AGID | Agenzia per l'Italia digitale

Linee Guida per la configurazione per adeguare la sicurezza del software di base

Sommario

LISTA DELLE TABELLE

LISTA DELLE FIGURE

1 INTRODUZIONE

1.1 Scopo

La sicurezza del software di base ed applicativo richiede di stabilire un processo volto ad identificare rischi e contromisure di sicurezza ad ogni livello (fisico, logico e organizzativo) del contesto in cui tali software operano e sono utilizzati.

Pertanto, nel fornire delle linee guida per la configurazione sicura di tali software (nel seguito tale attività viene spesso indicata con il termine "hardening"), è necessario considerare vari elementi, quali le protezioni perimetrali (fisiche e logiche), le architetture di rete (DMZ, segmentazioni, etc.), le procedure organizzative (perché dietro alle tecnologie operano le persone), i programmi formativi di "security awareness", ecc.

Partendo da questo presupposto, il presente documento si pone l'obiettivo di fornire un insieme di indicazioni per affrontare e risolvere correttamente le problematiche legate alla sicurezza del software di base e di individuare le misure da adottare per difendere ogni componente da possibili minacce accidentali e/o intenzionali.

1.2 Struttura del Documento

I paragrafi a seguire entrano nel dettaglio delle singole componenti (software di base, middleware, office automation, ecc.) oggetto di approfondita analisi dal punto di vista delle best practice di sicurezza, e per ognuna forniscono un elenco delle misure di sicurezza da adottare a fronte delle principali minacce, in modo da diminuire l'esposizione ai rischi per la sicurezza delle informazioni e dei servizi erogati.

Più nel dettaglio il documento è strutturato come segue:

- Il Capitolo 4 fornisce:
  - un catalogo delle minacce alla sicurezza delle informazioni ritenute applicabili nel contesto del presente documento (par. 4.1).
  - un catalogo delle principali tipologie di attacco rispetto al software di base, al middleware e al software applicativo più comune (par. 4.2).
- Il Capitolo 5 fornisce un insieme di raccomandazioni generali 'trasversali' che realizzano la base comune per affrontare le problematiche di sicurezza delle specifiche componenti.
- Il Capitolo 6 fornisce:
  - in una prima tabella, l'elenco dei riferimenti alle istruzioni operative di hardening (o benchmarks) messe a disposizione da enti/istituzioni preposte ed affermate a livello internazionale, operanti con il pieno supporto dei rispettivi vendor;
  - in una seconda tabella, l'elenco delle baseline di configurazione e alcuni strumenti software per l'hardening, messi a disposizione direttamente dai vendor.

1.3 Ambito di Applicabilità

Il presente documento si applica alle principali tipologie di software di base, middleware e applicativo in uso presso le pubbliche amministrazioni, ed in particolare:

- Principali Sistemi Operativi UNIX,
- Sistemi operativi Microsoft Windows Server,
- Sistemi operativi Windows Client,
- Web Browser,
- Postazioni di Lavoro,

- Web Application Server,
- DBMS/Data base server,
- Mail Server,
- Enterprise Service Bus,
- Principali applicativi di Office Automation (Microsoft Office e OpenOffice).

2 RIFERIMENTI

2.1 Documenti Applicabili

Rif.	Codice	Titolo

Tabella 1 - Documenti Applicabili

3 ACRONIMI

3.1 Acronimi

Codice	Titolo
AgID	Agenzia per l'Italia Digitale
ASLR	Address Space Layout Randomization
CAR	Committed Access Rate
CE	Contratto Esecutivo
CMDB	Configuration Management Data Base
COM	Component Object Model
COTS	Commercial Of The Shelf
CQ	Contratto Quadro
CRL	Liste di Revoca dei Certificati
CSRF	Cross-site request forgery
CVE	Common Vulnerabilities Exposures
DEP	Data Execution Prevention
DHA	Directory harvest attack
Dmz	De-militarized zone
DoS	Denial of Service
IDS	Intrusion Detection System
IM	Instant Messaging
IPS	Intrusion Prevention System
KRACK	Key Reinstallation Attacks
LDAP	Lightweight Directory Access Protocol
LLF	Low-level formatting
OCSP	Online Certificate Status Protocol
OSVDB	Open Source Vulnerability DataBase
PDL	Postazione di Lavoro
POODLE	Padding Oracle On Downgraded Legacy Encryption
PT	Penetration Test
QoS	Quality of Service
RFI	Remote File Inclusion
RTD	Real Time Data
RTI	Raggruppamento Temporaneo di Impresa

Codice	Titolo
SAML	Language Assertion Markup Language
Spim	Instant Messaging Spam
TLS	Transport Layer Security
VA	Vulnerability Assessment
VSTO	Visual Studio Tools per Office
WAF	Web Application Firewall
WOT	Web of Trust
WPA2	Wi-Fi Protected Access versione 2
XACML	EXtensible Access Control Markup Language
XKMS	XML Key Management Specification
XSS	Cross-site scripting

Tabella 2 - Acronimi

4 MINACCE E TIPOLOGIE DI ATTACCO

4.1 Catalogo delle Minacce

Di seguito viene fornito un catalogo di massima delle minacce correlate alle informazioni e ai servizi erogati. L'elenco è stato costruito seguendo le linee guida dettate dallo standard ISO/IEC 27005:2011 "Information technology — Security techniques — Information security risk management", e più in generale lo standard ISO/IEC 27001:2013.

Le minacce sono state individuate e selezionate in base alla loro effettiva applicabilità nel contesto del presente documento, escludendo quindi quelle ritenute non applicabili.

ID	Minaccia
M01	Abuso di privilegi da parte dell'utente.
M02	Abuso di risorse.
M03	Accesso non autorizzato ai sistemi (risorse di sistema, configurazioni, interfacce amministrative, ecc.).
M04	Accesso non autorizzato alle informazioni.
M05	Attacchi all'integrità dei sistemi (software e configurazioni).
M06	Attacchi all'integrità delle informazioni.
M07	Cancellazione dei log di accountability e/o ripudio di operazioni effettuate.
M08	Cancellazione o furto di informazioni (accidentale o da attacchi come ad es. il ransomware, ecc.).
M09	Compromissione delle comunicazioni.
M10	Crittografia debole o non validata.
M11	Divulgazione di informazioni riservate.
M12	Errori di amministrazione dei sistemi.
M13	Falsificazione di identità.
M14	Furto di credenziali di autenticazione.
M15	Generazione e/o gestione inadeguata delle chiavi crittografiche.
M16	Negazione dei servizi.
M17	Tentativi di frode.
M18	Uso non autorizzato di privilegi.
M19	Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (es. malware, ecc.)
M20	Violazione di leggi, di regolamenti, di obblighi contrattuali.
M21	Danneggiamento, perdita o furto di un asset fisico.

Tabella 3 - Catalogo delle Minacce

4.2 Catalogo delle tipologie di attacco

La tabella che segue fornisce una rassegna delle più note tipologie (meccanismi) di attacco.

Si sottolinea che i meccanismi di attacco sono sempre in evoluzione e spesso sfruttano vulnerabilità non note (i cosiddetti “zero-day”, descritti brevemente nel seguito), per cui un elenco di questo tipo, per sua stessa natura, non può ovviamente essere del tutto esaustivo.

ID	Tipologia	Descrizione
A01	BIOS rootkit attack	Un attacco di rootkit a livello di BIOS, noto anche come attacco persistente del BIOS, è un exploit in cui il BIOS viene aggiornato con codice dannoso. Il BIOS rootkit è un programma che risiede nella memoria fisica non volatile di un computer (in genera una EEPROM) e può consentire anche l'accesso e il monitoraggio del sistema da remoto.
A02	Brute Force Attack	Si definisce con il termine "Brute Force Attack" tratta di un attacco basato sul potere computazionale per decifrare le password o altre informazioni sensibili, o per “indovinare” password protette da hashing e crittografia.
A03	Buffer overflow	Si indica con il termine "Buffer overflow" tratta di una tecnica con cui un attaccante riesce ad eseguire uno “sfondamento” della memoria nel processo del sistema. Le vulnerabilità di buffer overflow possono portare ad attacchi di Denial of Service (DoS) o iniezione di codice (Code Injection). Un attacco di Denial of Service può causare un crash, uno stop o un rallentamento del processo; l'iniezione di codice invece, può modificare l'indirizzo di esecuzione del processo per eseguire il codice iniettato dall'aggressore.
A04	Cache poisoning	Il "cache poisoning", anche detto DNS poisoning o DNS cache poisoning, consiste nella compromissione di una tabella di sistema che memorizza gli indirizzi IP dei server internet dei nomi ottenuti dal server di dominio (DNS) Internet, sostituendo un indirizzo Internet corretto con quello di un altro indirizzo di un sito malevolo. Quando un utente Web cerca la pagina con tale indirizzo o nome host, la richiesta viene reindirizzata dalla voce all’indirizzo IP malevolo falsificato, presente nella tabella, verso un indirizzo diverso da quello reale. A quel punto è possibile che, un worm, uno spyware o un altro malware venga scaricato nel computer dell'utente direttamente dall'indirizzo malevolo, oppure è possibile che un sito contraffatto catturi le credenziali utente, eventualmente ponendosi come intermediario (man-in-the-middle) verso il sito legittimo.
A05	Clickjacking	Il Clickjacking (noto anche come reindirizzamento dell'interfaccia utente e “IFRAME overlay”) è un exploit in cui viene nascosto del codice dannoso nel codice dei pulsanti apparentemente innocui o di altri contenuti cliccabili presenti in un sito web.
A06	Clipboard hijacking	Il "clipboard hijacking" è un exploit in cui l'aggressore ottiene il controllo della clipboard della vittima e sostituisce i contenuti lì presenti con i propri dati, ad esempio un collegamento ad un sito Web dannoso.
A07	Code injection	È un attacco basato sull’inserimento nel codice dell’applicazione web di istruzioni, opportunamente modificate da un malintenzionato, finalizzate ad esempio, all'impersonificazione di un utente autenticato oppure nel furto di reperimento di credenziali di accesso.
A08	Cold boot attack	Un "cold boot attack" è un processo utilizzato per ottenere accesso non autorizzato alle chiavi di crittografia di un computer quando questo viene lasciato fisicamente incustodito. I ricercatori dell'Università di Princeton,

		della Electronic Frontier Foundation e Wind River Systems hanno scoperto che è possibile portare un attacco di questo tipo, dato che i chip di memoria ad accesso casuale dinamico (DRAM) conservano i dati per un breve periodo di tempo dopo lo spegnimento del computer su cui sono installate. Questa quantità di tempo può aumentare se i chip vengono rimossi dalla scheda madre e mantenuti a basse temperature. Ciò può essere fatto attraverso un raffreddamento con una canna invertita ad aria compressa. I chip possono quindi essere reinseriti rapidamente in un computer per poi leggerne il contenuto.
A09	Cracking	Con cracking si intende la modifica di un software per rimuovere la protezione dalla copia, oppure per ottenere accesso ad un'area altrimenti riservata. Per cracking si intende anche la violazione di sistemi informatici collegati ad Internet o ad un'altra rete, allo scopo di danneggiarli, di rubare informazioni oppure di sfruttare i servizi telematici della vittima (connessione ad Internet, traffico voce, sms, accesso a database etc..) senza la sua autorizzazione (thiefing).
A10	Cross-Frame Scripting (XFS)	Si tratta di un attacco che combina un codice JavaScript malizioso con un iframe che carica una pagina legittima allo scopo di rubare dati da un utente inconsapevole. In genere funziona in combinazione con il social engineering o il phishing. A titolo di esempio, un attaccante può convincere un utente a navigare su una pagina contenente il codice JavaScript e un iframe HTML che punta a un sito legittimo. Quando l'utente inserisce le credenziali sul sito legittimo, il codice JavaScript ne memorizza i caratteri.
A11	Cross-site request forgery (CSRF)	Un attacco "cross-site request forgery", detto anche brevemente CSRF e talvolta pronunciato "Sea-Surf", consiste nell'abuso della fiducia tra l'applicazione e un determinato client (la vittima) al fine di eseguire una transazione a livello applicativo, pilotata da un attaccante utilizzando l'identità del client. L'attacco è basato sull'incorporamento di URL, che rappresentano transazioni specifiche dell'applicazione di destinazione, all'interno di una pagina controllata dall' attaccante, che è già stata acceduta dalla vittima tramite browser dopo aver stabilito una relazione di fiducia con l'applicazione di destinazione (ad esempio tramite l'autenticazione). Esempi di tali richieste includono il trasferimento di fondi monetari e titoli, attività di provisioning, amministrazione di applicazioni e perfino operazioni di l'acquisto di beni e servizi.
A12	Cross-site scripting (XSS)	Esistono 3 tipi di Cross Site Scripting: - "Reflected": Il web server legge i dati dannosi (payload di attacco) direttamente dalla richiesta HTTP e li rimanda (riflette) indietro nella risposta HTTP (Il meccanismo più comune per distribuire i contenuti dannosi è quello di includerli come parametro in una URL che viene resa pubblica o inviata per e-mail direttamente alla vittima). - "Stored": Il web server memorizza i dati dannosi (payload di attacco) in un suo archivio. In un secondo momento, i dati dannosi vengono letti e inclusi in una risposta http. - "DOM based": A differenza dei due tipi precedenti, i dati dannosi (payload di attacco) non vengono inseriti nella risposta (a causa di un difetto lato server). L'attacco mira a modificare il DOM "environment" all'interno del browser della vittima in modo che uno script che gira lato client produca un esito diverso da quello atteso (a causa appunto della presenza dei dati dannosi che sono stati iniettati nel DOM

		"environment"). Ad esempio, lo script che gira lato client usa il "document.location" –ossia l'url- e l'attaccante inserisce opportunamente uno script nell'url.
A13	CSV Injection	Questo attacco, noto anche come Formula Injection, avviene quando un sito web inserisce input malevoli in dati e formule (o anche delle macro maliziose) in un file CSV che viene scaricato dagli utenti. Quando un programma come Excel (o LibreOffice Calc) apre tale foglio CSV, "valuta" le formule presenti nelle celle e contenenti valori "maliziosi". Ci sono tre tipi di attacco di questo tipo: - quelli che sfruttano le vulnerabilità del foglio elettronico, come quella descritta in CVE-2014-3524; - quelli che compromettono il computer dell'utente sfruttando la tendenza degli utenti a non effettuare controlli antivirus e a ignorare gli avvisi di sicurezza sui fogli CSV scaricati; - quelli mirati al furto di informazioni da altri fogli elettronici aperti dall'utente o da qualsiasi file presente sul suo computer.
A14	Denial of Service	È un attacco mirato a che si perpetra portando al limite delle prestazioni il funzionamento di un sistema (ad es., un sito web) al limite delle prestazioni, (ad es., un sito web) causando il blocco del servizio. La variante distribuita (DDoS) si attua, invece, generando un numero molto elevato di richieste simultanee da parte di più macchine (a volte decine di migliaia) generalmente controllati attraverso un malware specifico, contemporaneamente dirette tutte al medesimo server, in modo da esaurirne le risorse e renderlo non più in grado di erogare i propri servizi. Come conseguenza, il server vittima non risulta più raggiungibile dall'esterno.
A15	Dictionary Attack	Con l'attacco Dictionary, un aggressore utilizza un programma per l'iterazione di tutte le parole presenti in un dizionario (o più dizionari in diverse lingue) e calcola l'hash per ogni parola. L'hash risultante viene confrontato con il valore presente nell'archivio delle password. Le password deboli come una squadra preferita o un'auto preferita, verranno decifrate rapidamente. Le password più forti come ad esempio quelle che combinano sequenze di caratteri differenti ("? BiolLNessFiNdMeyePasSWirt!"), sono meno probabili da decifrare.
A16	Direct Dynamic Code Evaluation ('Eval Injection')	L'attacco colpisce gli script che non validano correttamente l'input utente usato nel parametro page. Un utente remoto può fornire un input una URL opportunamente formata, per passare codice arbitrario a un'istruzione eval().
A17	Directory harvest attack (DHA)	Un attacco "directory harvest" (DHA) è un tentativo di determinare gli indirizzi di posta elettronica validi associati a un server di posta elettronica in modo tale da poterli aggiungere a un database di spam. Attraverso un attacco di brute force (a volte più o meno selettivo e mirato a una specifica organizzazione/evoluto nella composizione degli usernames) indirizzato verso l'e-mail Mail Server, il programma DHA alimenta il database di spam secondo il seguente criterio: se l'e-mail Mail Server ritorna restituisce un messaggio di replica errore di tipo "Not found" allora l'indirizzo provato è inesistente e va scartato, se l'e-mail server invece non restituisce nulla allora l'indirizzo provato è valido e va aggiunto al database.
A18	Drive-by-Downloads attack	In un attacco "Drive-by-Download", l'applicazione web viene modificata (ad esempio iniettando codice HTML) in modo tale da istruire il browser

		del visitatore a scaricare il malware situato nel server controllato da un aggressore. Spesso, la manomissione non è visibile ai visitatori, quindi le vittime innocenti non sono a conoscenza dell'operazione di download che avviene in background. Pertanto l'attacco "Drive-by-Download" si svolge su 3 fronti: - compromissione di un web server legittimo per hostare il contenuto malevolo capace di avviare il download sul client della vittima o utilizzare, per lo stesso scopo, un *third party service* (ad es. un banner pubblicitario) che il web server legittimo (inconsapevolmente) espone; - compromissione del client per avviare il download del malware vero e proprio; - esecuzione del malware sul client.
A19	Esecuzione arbitraria di codice	Se un utente malintenzionato riesce a eseguire codice dannoso sul server, questo può compromettere le risorse del server o installare ulteriore software capace di portare attacchi contro i sistemi a valle dell'infrastruttura. I rischi derivanti dall'esecuzione arbitraria di codice aumentano se il processo server in cui viene eseguito il codice dell'attaccante ha privilegi elevati. Le vulnerabilità più comuni che consentono l'esecuzione arbitraria di codice sono legate a sistemi server mal configurati (privi di hardening) o non aggiornati (privi delle patch di sicurezza), oppure alla mancata validazione dell'input utente, specie in applicazioni scritte in linguaggi in cui la memoria dinamica non è gestita automaticamente e l'accesso diretto alla memoria tramite puntatori non viene impedito a causa di configurazioni deboli dell'application server e da server non sottoposti agli ultimi aggiornamenti che consentono l'attraversamento di percorsi non protetti (path traversal) e attacchi di buffer overflow, dove entrambi comunque, possono portare all'esecuzione di codice arbitrario.
A20	Format String Attack	Questo attacco si verifica quando i dati forniti in input e copiati in una stringa vengono in realtà "valutati" come un comando che viene eseguito dall'applicazione. In tal modo un attaccante può iniettare codice arbitrario, leggere lo stack o causare un "segmentation fault".
A21	Heap Overflow	Consiste in un tipo particolare di buffer overflow che avviene però nell'area di memoria dello "heap". La memoria nello heap è allocata dinamicamente dall'applicazione a run-time e tipicamente contiene le strutture dati allocate dinamicamente dal programma. L'attacco mira a corrompere queste strutture in vari modi, come ad es. sovrascrivendole attraverso i relativi puntatori, usati per accedere ad indirizzi che vanno oltre la fine di una determinata struttura memorizzata.
A22	Heartbleed	Si tratta di un attacco che sfrutta un bug della libreria crittografica fornita da OpenSSL, usata da innumerevoli applicazioni, compresi client e server Web, VPN, LDAP(S), IMAP(S), SMTP(S), SFTP, RDBMS, ecc. La vulnerabilità è dovuta a una impropria validazione dell'input da parte della libreria, in particolare nell'estensione TLS heartbeat, che comporta un "buffer over-read" in grado di esporre la chiave crittografica del server. È descritto in CVE-2014-0160.
A23	HTML Injection	L'HTML injection è una tecnica utilizzata per sfruttare input non validati al

		fine di modificare una pagina web fornita da un'applicazione web ai propri utenti. Gli aggressori sfruttano il fatto che il contenuto di una pagina web è spesso legato ad una precedente interazione con gli utenti. Quando l'applicazione non riesce a convalidare i dati forniti dall'utente, un utente malintenzionato può inviare un testo HTML opportunamente modificato per alterare quei contenuti del sito che vengono poi presentati ad altri utenti. Una query creata ad-hoc può portare all'inserimento nella pagina web di elementi HTML controllati dall'attaccante che modificano il modo in cui il contenuto dell'applicazione viene esposto sul web.
A24	HTTP response splitting	Un attaccante passa dati “maliziosi” a una applicazione che non li valida e li include immutati in una HTTP Response Header. L’applicazione è vulnerabile se consente l’input di caratteri contenenti CR (carriage return, ovvero %0d o \r) ed LF (line feed, ovvero %0a o \n) nell’header http e se contemporaneamente la piattaforma su cui gira il sistema è a sua volta vulnerabile alla injection di tali caratteri. Con questo attacco l’aggressore ha la possibilità di controllare le successive http response dell’applicazione, incluse l’HEADER e il BODY, e inoltre di creare altre response a suo piacimento.
A25	Infezione da malware	Per compromissione di un sistema di elaborazione causata da un software malevolo, si intende il malfunzionamento di un sistema di elaborazione causato da software che esegue funzioni "nocive" (ad esempio, virus, worm, cavalli di Troia).
A26	Information gathering	Si indica con il termine "Information gathering" una tecnica mirata a individuare, identificare e caratterizzare i dispositivi di rete che possono essere scoperti e profilati. Ciò avviene attraverso la scansione delle porte. Dopo aver identificato le porte aperte, si rilevano i tipi di periferica e si determinano le versioni del sistema operativo e delle applicazioni. Con queste informazioni, un aggressore può successivamente attaccare le vulnerabilità note che potrebbero non essere state risolte con patch di protezione.
A27	Integer Overflow	Un integer overflow avviene quando un’operazione aritmetica cerca di calcolare un valore numerico che supera il range che può essere rappresentato con un dato numero di bit. In tal modo si ottiene un risultato imprevisto che può compromettere la stabilità e l’integrità dell’applicazione, laddove l’errore non sia intercettato e gestito.
A28	Keylogging	Un keylogger è uno strumento hardware o software in grado di effettuare lo sniffing della registrazione dei caratteri premuti sulla della tastiera di un computer, cioè è in grado di intercettare e catturare segretamente tutto ciò che viene digitato sulla tastiera senza che l'utente si accorga di essere monitorato.
A29	KRACK	L’attacco Key Reinstallation AttaCK (KRACK), e un attacco di “replay” mirato allo standard Wi-Fi Protected Access protocol (WPA / WPA2), che si suppone metta in sicurezza le connessioni WiFi. L’attacco consiste nel resettare ripetutamente il “nonce” trasmesso in una specifica fase dell’handshake WPA2, consentendo di analizzare e decifrare gradualmente i pacchetti attraverso la comparazione con quelli precedenti, fino a ottenere la chiave crittografica utilizzata per cifrare il traffico. L’attacco sfrutta una vulnerabilità insita nello standard e non in specifici prodotti, e colpisce tutti i principali sistemi operativi compresi quelli usati

		da smartphone e tablet. Particolarmente grave è il fatto che sui sistemi linux-based, il client wpa-supplicant usato per connettersi alla rete WiFi con il WPA2 consente addirittura l'inserimento di una chiave "nulla".
A30	LDAP Injection	L'LDAP Injection è un tipo di attacco portato verso un'applicazione web dove gli hacker introducono del codice malevolo in un campo di input dell'interfaccia utente nel tentativo di ottenere accesso a informazioni non autorizzate. L'LDAP Injection utilizza i dati forniti nella richiesta proveniente dal client, nella costruzione di istruzioni LDAP (Lightweight Directory Access Protocol), quando questi non vengono controllati e validati al fine di rimuovere codice potenzialmente dannoso. Quando un'applicazione web non applica adeguati controlli sull'input fornito dall'utente, gli hacker possono essere in grado di modificare la costruzione di un'istruzione LDAP che verrà poi eseguita con le stesse autorizzazioni del componente destinato all'esecuzione del comando. Un LDAP Injection può causare seri problemi di protezione se le autorizzazioni consentono di interrogare, modificare o rimuovere qualsiasi oggetto presente all'interno dell'albero LDAP.
A31	Man-in-the-browser	È un attacco simile al man-in-the-middle, ma agisce all'interno del browser utente. Generalmente è basato su un "Trojan Horse" che si installa nel browser per intercettare e manipolare richieste e risposte http. Spesso questa tecnica è usata da malware mirati a specifici siti di Home Banking, in grado di rubare denaro modificando "al volo" le transazioni finanziarie (es. i bonifici). Il malware può insediarsi nei "Browser Helper Objects" di Internet Explorer (librerie caricate dinamicamente all'avvio del browser), nelle Estensioni dei browser più recenti o attraverso "API-Hooking" in un eseguibile o una libreria DLL, o ancora tramite Javascript (ad es. attraverso uno "worm" basato su Ajax).
A32	Man-in-the-middle	Questo attacco consiste nell'intercettare la comunicazione tra due sistemi ponendosi in mezzo e fingendo con ciascuno degli interlocutori di essere l'altro. Ad es. in una connessione http l'attaccante rompe la connessione originale in due parti: una connessione dal client a sé stesso (fingendosi il server) e una da sé stesso al server (fingendosi il client), inoltrando dopo averle intercettate ed eventualmente manipolate, le richieste del client al server e le risposte del server al client.
A33	Manipolazione dei campi di Form	I valori dei campi presenti in una form HTML vengono inviati in chiaro al server utilizzando il protocollo HTTP POST. Ciò può includere campi di form visibili e nascosti. Indipendentemente dalla tipologia, questi campi possono essere facilmente modificati ignorando le routine di convalida lato client. Di conseguenza, le applicazioni che si basano sui valori di input di un campo di una form per prendere decisioni di sicurezza lato server sono vulnerabili all'attacco in oggetto.
A34	Manipolazione dei Cookie	I cookie sono suscettibili a modifiche da parte del client. Ciò è vero sia per i cookie persistenti che per quelli che risiedono in memoria. Sono disponibili diversi strumenti per supportare un aggressore nella modifica del contenuto di un cookie residente in memoria. La manipolazione del cookie è l'attacco che si riferisce alla modifica di un cookie, si effettua di solito per

		ottenere un accesso non autorizzato ad un sito Web.
A35	Manipolazione della Query String	Gli utenti possono facilmente manipolare i valori della stringa di query passati tramite HTTP GET da client a server in quanto vengono visualizzati nella barra degli indirizzi URL del browser Web. Se l'applicazione si basa su valori della stringa di query per prendere decisioni di sicurezza o se i valori rappresentano dati sensibili o parametri critici di una transazione come importi monetari, l'applicazione è vulnerabile all'attacco in oggetto.
A36	Manipolazione dell'intestazione HTTP	Le headers HTTP passano le informazioni tra il client e il server. Il client costruisce le headers di richiesta mentre il server costruisce le headers di risposta. Se l'applicazione si basa sulle headers di richiesta per prendere una decisione, questa allora è vulnerabile all'attacco in oggetto.
A37	Memory dump attack	Un attacco di dump di memoria consiste nella cattura e nell'utilizzo di contenuti RAM che sono stati scritti su un'unità di memorizzazione durante un errore irreversibile (a scopo di diagnostica), tipicamente innescato dall'attaccante.
A38	Path Manipulation	Simile alla Resource Injection, salvo che si focalizza sul re-indirizzamento verso risorse di file system locali del server, forzandolo a caricare risorse diverse da quelle previste.
A39	Path traversal	Accesso alla struttura del file system non di pertinenza dell'applicativo web. Un aggressore avendo accesso alla gerarchia del file system (ad es. mediante la notazione "../") potrebbe prelevare informazioni riservate presenti all'interno della struttura di file e delle cartelle esterne all'applicazione.
A40	Pharming	Il phishing ed il pharming sono due tecniche utilizzate per ottenere l'accesso a informazioni personali o riservate. Nel primo caso un utente incauto viene indotto, tramite tecniche di social engineering, ad accedere ad un sito web contraffatto in modo tale da sembrare ufficiale ed a inserirvi dati personali e/o sensibili. Nel secondo caso, l'utente viene reindirizzato automaticamente, tramite alterazione delle richieste DNS (che possono coinvolgere direttamente il DNS server o la PdL vittima, tramite l'installazione di trojan) al sito web contraffatto, anche nel caso in cui digiti nel browser l'indirizzo corretto del server autentico.
A41	Phishing	Per "phishing" si intende un qualsiasi tentativo (per telefono, e-mail, messaggistica immediata o fax) di ottenere informazioni di identificazione personale a scopo di furto di identità. Un tipico attacco di phishing elettronico comprende due componenti: un messaggio e-mail dall'aspetto autentico e una pagina web fraudolenta. I collegamenti web inclusi in questi messaggi e-mail quasi sempre hanno l'aspetto e il funzionamento dei siti legittimi copiati, rendendo la frode quasi impossibile da rilevare.
A42	POODLE attack	Il POODLE (Padding Oracle On Downgraded Legacy Encryption) è una vulnerabilità che riguarda la sicurezza di una vecchia versione del protocollo SSL, la 3.0, che potrebbe essere sfruttata per intercettare i dati in transito fra client e server. La vulnerabilità, rivolta al lato client e non a quello server, potrebbe ad esempio consentire a un utente malintenzionato di decifrare i cookie che corrispondono a servizi come Twitter o Google, per entrare negli account degli utenti senza la necessità di conoscere la password di accesso. Il protocollo SSL 3.0, così come utilizzato in molti prodotti (es. OpenSSL 1.0.1i), usa un padding CBC non deterministico che consente a un attacco

		di tipo man-in-the-middle di decifrare facilmente i dati trasmessi utilizzando un attacco "padding-oracle". Il protocollo TLS (Transport Layer Security) ha largamente sostituito il protocollo SSL per la comunicazione sicura su Internet, ma molti browser tornano ad utilizzare SSL 3.0 quando non è disponibile una connessione TLS. Un aggressore che vuole sfruttare il POODLE approfitta di questa vulnerabilità inserendosi nella sessione di comunicazione e costringendo il browser a utilizzare SSL 3.0.
A43	Privilege horizontal escalation attack	Un attacco di "privilege escalation" è un tipo di intrusione di rete che sfrutta gli errori di programmazione o i difetti di progettazione per concedere all'attaccante un accesso privilegiato alla rete, ai dati e alle applicazioni ad essa associati. Nel caso di "horizontal esclation", per "accesso privilegiato" si intende un accesso nel quale un utente con certi privilegi accede alle funzioni e/o contenuti riservati a un altro utente che gode degli stessi privilegi.
A44	Privilege vertical escalation attack	Un attacco di "privilege escalation" è un tipo di intrusione di rete che sfrutta gli errori di programmazione o i difetti di progettazione per concedere all'attaccante un accesso privilegiato alla rete, ai dati e alle applicazioni ad essa associati. Nel caso di "vertical escalation", per "accesso privilegiato" si intende un accesso più alto di quello previsto dall'amministratore o dallo sviluppatore dell'applicazione.
A45	Proxy hijacking attack	Il "proxy hijacking" è una tecnica di attacco in cui il codice malevolo non installa un malware ma configura il browser presente sul sistema della macchina vittima per usare un web proxy controllato dall'attaccante stesso. Oltre a eseguire il deploy dei proxy settings fraudolenti, l'attacco installa un "self-signed root certificate" sul sistema in modo che l'attaccante possa leggere il traffico HTTPS che passa attraverso il proxy server fraudolento (man-in-the-middle MITM Attack). Tipicamente l'attacco parte da spam email con un attachment malevolo che esegue le operazioni di cui sopra.
A46	Remote File Inclusion (RFI)	Il "Remote File Inclusion (RFI)" è un attacco che punta ad un server di computer su cui sono in esecuzione siti e applicazioni web. Gli exploit RFI sono spesso attribuiti al linguaggio di programmazione PHP utilizzato da molte grandi aziende, tra cui Facebook e SugarCRM. Tuttavia, l'RFI può manifestarsi in altri ambienti ed è stato infatti introdotto inizialmente come "SHTML injection". RFI funziona sfruttando applicazioni che dinamicamente fanno riferimento a script esterni indicati da input dell'utente, senza adeguati controlli. Di conseguenza, l'applicazione può essere istruita per includere uno script ospitato su un server remoto e quindi eseguire codice controllato da un utente malintenzionato. Gli script eseguiti possono essere utilizzati per il furto temporaneo o l'accesso non autorizzato ai dati, la loro manipolazione o anche la loro sottrazione, per una acquisizione dati a lungo termine.
A47	Resource Injection	Questo attacco consiste nel modificare il tipo o l'identificatore di una risorsa usato da un'applicazione, attraverso un input non validato, i cui caratteri vengono usati dall'applicazione vulnerabile per determinare la risorsa da accedere (es. un nome file su uno share remoto, una porta TCP/IP, una URL, ecc.). In tal modo l'attaccante forza il server a caricare una risorsa arbitraria dalla rete, potenzialmente contenente codice dannoso, che in alcuni casi può essere persino memorizzato sul server ed essere inviato ad altri utenti.

A48	SEO poisoning attack	Il "SEO poisoning", noto anche come "search poisoning", è un metodo di attacco in cui i cyber criminali creano siti web dannosi e utilizzano tattiche di ottimizzazione dei motori di ricerca per renderli prominenti nei risultati della ricerca. Tali siti vengono associati a termini presumibilmente utilizzati nella ricerca da un numero elevato di persone in un dato momento, ad esempio frasi correlate a festività, news e video virali. Secondo i Websense Security Labs, in questi casi, fino ad un quarto della prima pagina dei risultati della ricerca, questi possono essere collegati a siti web dannosi. Gli aggressori creano siti web con nomi e descrizioni associate a temi popolari o ad argomenti di tendenza. Ad esempio, nelle settimane precedenti a Halloween, gli aggressori potrebbero attivare siti che offrono modelli gratuiti per i costumi di Halloween. Tuttavia, il vero scopo è quello di infettare i visitatori con malware o accedere in modo fraudolento a informazioni sensibili da utilizzare poi per il furto di identità.
A49	Sfruttamento delle sessioni	Ogni applicazione web che si avvale di un meccanismo di login di autenticazione, basato sul logon gestisce delle sessioni con le quali tracciare l'utente, che si attua con l'assegnazione di un token (ad es. un cookie, un parametro di sessione) univoco. L'attacco si perpetra dopo aver determinato il funzionamento dell'algoritmo di generazione del token e, in genere, comporta la sostituzione di identità, dando all'aggressore l'opportunità di accedere all'applicazione web poiché da essa ritenuto un utente accreditato.
A50	Shellcode	Uno shellcode è un programma in linguaggio assembly che tradizionalmente esegue una shell, come la shell Unix '/bin/sh' oppure la shell "command.com" sui sistemi operativi DOS e Microsoft Windows. Uno shellcode può essere utilizzato per sfruttare un bug mediante un exploit, consentendo ad un hacker o un cracker di acquisire l'accesso alla riga di comando di un computer, o più in generale di eseguire codice arbitrario.
A51	Spam	Il termine "spam" descrive una comunicazione non sollecitata (inviata per e-mail o messaggi/chat immediata) e destinata al lucro commerciale. Il termine spam comprende un'ampia gamma di attività, molte delle quali sono dannose (come la distribuzione di e-mail di phishing). Una variante di tale attacco è lo spam per immagini (spam in cui il messaggio è testo sotto forma di immagine, anziché testo effettivo) come mezzo usato per evadere il rilevamento.
A52	Spim (Instant Messaging Spam)	Lo Spim è una forma di spam distribuito tramite messaggistica istantanea (IM) anziché tramite messaggistica di posta elettronica. Anche se meno diffuso rispetto alla sua controparte di posta elettronica, lo Spim sta raggiungendo sempre più utenti. l'IM è un canale particolarmente adatto per gli spammer. Per prima cosa, l'immediatezza nello scambio di messaggi fornita dall'IM rende probabilmente gli utenti meno riflessivi nel cliccare sui link. Inoltre, con il fatto che l'IM bypassa il software antivirus e i firewall, questo rappresenta un mezzo facile per passare non solo messaggi commerciali, ma anche virus e altri malware.
A53	SQL injection	"SQL injection" è una tecnica di hacking che mira a colpire le applicazioni web connesse ad un database di tipo SQL. Tale attacco sfrutta l'inefficienza dei controlli sui dati ricevuti in input ed inserisce codice maligno all'interno di una query SQL. La tecnica permette al malintenzionato di autenticarsi con ampi privilegi in aree protette dell'applicazione e di visualizzare e/o alterare dati sensibili.
A54	Stack overflow	Lo stack overflow si verifica quando il puntatore di stack di chiamata,

		supera lo spazio di memoria associato allo stack. Lo stack delle chiamate può occupare uno spazio di memoria di dimensioni ridotte, in genere questa spesso viene determinata all'avvio del programma. La dimensione dello stack di chiamata dipende da molti fattori, tra cui il linguaggio di programmazione, l'architettura della macchina, il multi-threading e la quantità di memoria disponibile. Quando un programma tenta di utilizzare più spazio di quanto non sia disponibile nello stack di chiamata (ovvero quando tenta di accedere alla memoria oltre i limiti dello stack di chiamata, che è essenzialmente un buffer overflow), si parla di overflow dello stack, che porta al crash del programma. Questo si verifica in genere in caso di errori di programmazione quali la ricorsione infinita o l'uso di variabili di stack troppo grandi.
A55	XPath Injection	XPath è un linguaggio di query che consente di accedere a qualsiasi parte di un documento XML senza alcuna restrizione nel controllo di accesso (chi può accedere a cosa). Con un attacco di XPATH Injection, un malintenzionato può modificare una query XPATH per eseguire un'azione differente da quella prevista. La XPath Injection può essere usata per estrarre da un'applicazione, dati forniti dagli utenti, memorizzati in modo non sicuro. Questo può avvenire se l'applicazione non valida correttamente l'input usato per comporre una query XPATH.
A56	Zero-day exploit	Un exploit "zero-day" consiste nello sfruttamento di una vulnerabilità di sicurezza nello stesso giorno in cui questa generalmente diventa nota. Ci sono zero giorni tra il momento della scoperta della vulnerabilità e il primo attacco. Normalmente, quando qualcuno rileva che un programma software contiene un potenziale problema di sicurezza, la persona o l'azienda notificano il problema riscontrato alla società che ha realizzato il software (e talvolta al mondo in generale) in modo da poter intraprendere azioni di correzione. Passa del tempo prima che, la società che ha realizzato il software, possa correggere il codice e distribuire una patch o un aggiornamento software. Anche se potenziali aggressori sono a conoscenza della vulnerabilità, potrebbe essere necessario un certo tempo per poterla sfruttare a loro vantaggio. Nel frattempo, si spera che la soluzione di correzione sia disponibile prima che ciò avvenga.

5 BEST PRACTICES PER ADEGUARE E MANTENERE LA SICUREZZA DEL SOFTWARE DI BASE

L'apertura delle applicazioni verso fornitori, clienti, utenti remoti e mobili ha comportato la scomparsa di un perimetro aziendale definito e un'estrema diversificazione delle minacce. In questo nuovo scenario, le applicazioni sono diventate il **principale vettore di attacco** ed è sempre più difficile proteggerle. Lo studio presentato nel ***Rapporto OAD***[1] ***2017*** sugli attacchi applicativi in Italia, evidenzia come **principale causa degli attacchi** applicativi, sono le **vulnerabilità** delle infrastrutture ICT, del software di base e dei middleware usati dalle applicazioni (circa il 37%). Seguono poi le **vulnerabilità intrinseche all'applicativo** stesso quali, ad esempio, quelle dei sistemi di identificazione, autenticazione e controllo degli accessi. Nell'ultimo Rapporto Clusit del 2019[2] si evidenzia un trend di crescita degli attacchi sia in termini quantitativi che in termini di gravità dei danni prodotti. Il suddetto rapporto riporta quanto segue "Nell'ultimo biennio il tasso di crescita del numero di attacchi gravi è aumentato di 10 volte rispetto al precedente. Non solo, la Severity media di questi attacchi è contestualmente peggiorata, agendo da moltiplicatore dei danni.".

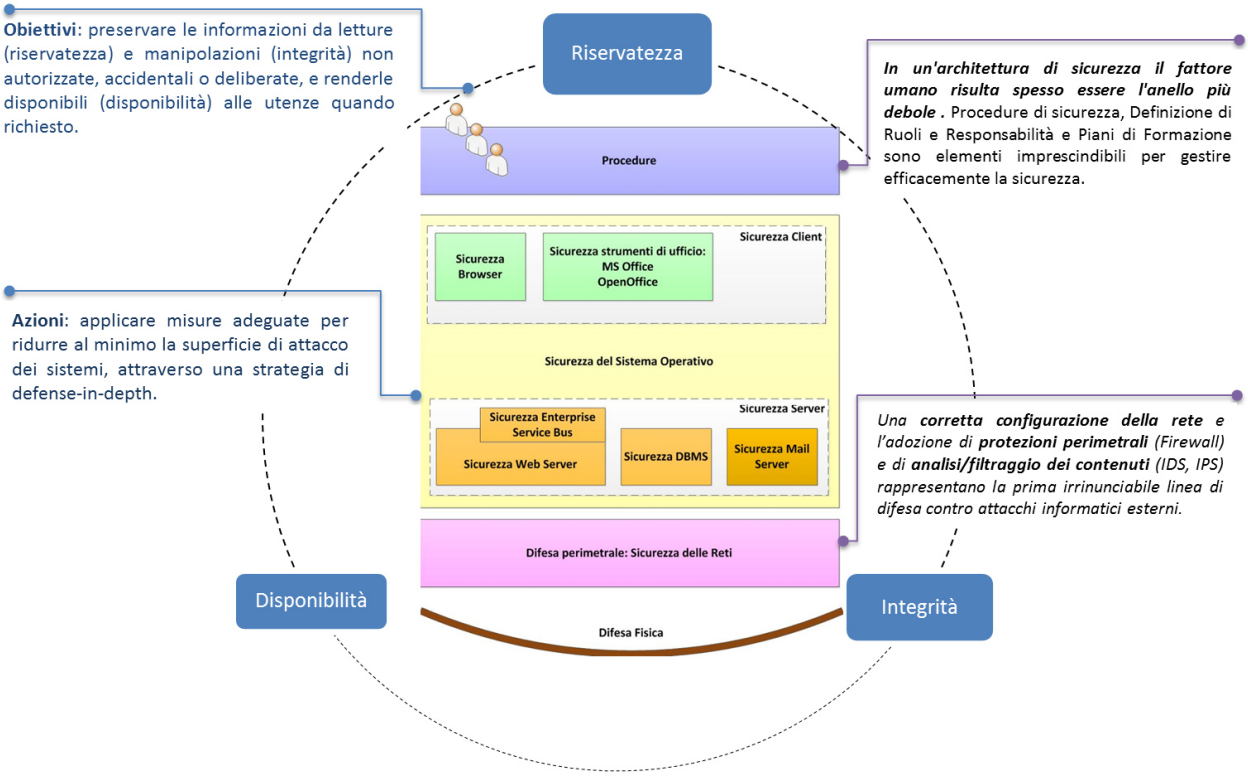


Figura 1 - Scenario - Sicurezza ad ogni livello (fisico, logico e organizzativo)

[1] Osservatorio Attacchi Digitali – https://www.malaboadvisoring.it/index.php?option=com_content&view=article&id=126:rapporto-2017-oad-attacchi-agli-applicativi-in-italia-&catid=13:oci-ed-oai-&Itemid=127

[2] https://clusit.it/rapporto-clusit/

5.1 Common Best Practice

Si forniscono nel seguito un insieme di raccomandazioni generali 'trasversali' che realizzano la base comune per affrontare le problematiche di sicurezza delle specifiche componenti.

Ogni argomento è strutturato in un paragrafo contenente una o più tabelle.

Ciascuna tabella riporta una problematica di sicurezza, le minacce che possono determinarla o comunque applicabili, e le contromisure generali suggerite per farvi fronte.

5.1.1 Utenze

Registrazione / Cancellazione utenti	
Minaccia	Abuso di privilegi da parte dell'utente.
Contromisure	Definire, per ogni sistema/piattaforma, un processo di registrazione/cancellazione degli utenti ai quali deve essere concesso/revocato un account. Il processo deve prevedere almeno: - l'uso di User ID individuali in modo che gli utenti possano essere resi responsabili delle proprie azioni. L'uso dell'ID di gruppo dovrebbe essere permessa solo per esigenze aziendali od operative previa approvazione e produzione della documentazione di supporto; - la verifica che il livello di accesso richiesto sia in linea con il principio del "need to know"; - l'obbligo di disabilitare o rimuovere immediatamente le UserId degli utenti che hanno cessato il rapporto di lavoro; - la verifica periodica (almeno trimestrale) dell'assenza di account inconsistenti, ridondanti o obsoleti e la loro eliminazione.

Assegnazione e revoca dei diritti di accesso degli utenti	
Minaccia	Abuso di privilegi da parte dell'utente.
Contromisure	Definire un processo che disciplini l'assegnazione e la revoca dei diritti di accesso dell'utente, identificato con UserId personale. L'accesso a ogni sistema/piattaforma da parte di persone fisiche deve essere soggetto a: - autenticazione, in modo univoca attraverso un identificativo personale (es. username o UserId) e credenziali private (es. password, PIN, token); - autorizzazione, nei limiti del principio del need-to-know ovvero attribuire il privilegio minimo necessario per svolgere l'attività lavorativa; - registrazione di tutti i diritti di accesso assegnati al sistema/piattaforma, in un sistema di anagrafica centralizzato. Verificare che il livello di accesso consentito sia coerente con le politiche di accesso e con il principio di separazione dei compiti. - i profili di accesso devono essere costantemente aggiornati; - eventuali deroghe ai criteri di assegnazione/revoca dei diritti di accesso dovrebbero essere limitate, registrate e approvate almeno dai responsabili del sistema/piattaforma e dai responsabili funzionali.

Autorizzazione all'assegnazione dei diritti di accesso privilegiato	
Minaccia	Abuso di privilegi da parte dell'utente.
Contromisure	L'assegnazione dei diritti di accesso privilegiato dovrebbe essere controllata attraverso un processo di autorizzazione che preveda: - l'identificazione dei diritti di accesso privilegiato relativi al sistema/piattaforma e gli utenti a cui è necessario assegnarli; applicazione principio della *segregation of duty* nel processo autorizzativo;

	- una registrazione di tutti i privilegi assegnati; - i requisiti per la scadenza dei diritti; - riesame regolare delle competenze degli utenti; - per le UserId amministrative generiche (da evitare se non indispensabile per l'esecuzione del servizio), dovrebbe essere mantenuta la riservatezza delle informazioni segrete di autenticazione quando questa è condivisa.

Riesame dei diritti di accesso degli utenti	
Minaccia	- Accesso non autorizzato alle informazioni. - Abuso di privilegi da parte dell'utente.
Contromisure	I diritti di accesso degli utenti dovrebbero essere riesaminati regolarmente (al massimo ogni sei mesi) e dopo ogni cambiamento (es. cessazione del rapporto di lavoro, cambio di ruolo, di mansione, all'interno dell'organizzazione). Le autorizzazioni per i diritti di accesso privilegiati dovrebbero essere riesaminate ad intervalli più frequenti e gli eventuali cambiamenti tracciati. Per ogni cambiamento di privilegi deve esserne registrato il richiedente, l'approvatore e la motivazione. In caso di cessazione del rapporto di lavoro, sia di personale interno sia esterno, è necessario verificare i requisiti per la rimozione, o sospensione dei diritti di accesso al sistema/piattaforma. Tali diritti dovrebbero essere ridotti o rimossi prima della cessazione o della variazione del rapporto di lavoro, a seconda della valutazione di fattori di rischio come: - criticità delle informazioni cui si accedeva; - ruolo della persona, - motivazione della cessazione/cambiamento. Prevedere controlli o misure di sicurezza per limitare il rischio che: - in caso di licenziamento o fine contratto, dei dipendenti scontenti o degli utenti di terze parti esterne possano deliberatamente corrompere informazioni o commettere illeciti; - in caso di persone dimissionarie o in uscita, esse possano essere tentate di recuperare/copiare informazioni per uso futuro.

Utenze tecniche

Protezione delle informazioni strumentali all'accesso	
Minaccia	- Divulgazione di informazioni riservate. - Accesso non autorizzato ai sistemi (risorse di sistema, configurazioni, ecc.). - Furto di credenziali di autenticazione.
Contromisure	- Utilizzare ACL forti per proteggere le risorse di sistema. - Utilizzare algoritmi standard di crittografia per memorizzare i dati sensibili nei file di configurazione (utenze tecniche, non legate a persone fisiche: processi di sistema, porzioni di DB, ecc.). - Utilizzare algoritmi di comprovata robustezza come. Ad esempio AES, l'algoritmo simmetrico ritenuto al momento più sicuro, consente di scegliere una chiave crittografica di 128, 192 o 256 bit. La scelta della lunghezza della chiave crittografica deve essere commisurata al tipo di algoritmo e al livello di riservatezza delle informazioni da proteggere. Per quanto riguarda AES, anche la chiave a 128 bit è considerata sicura. Algoritmi asimmetrici come RSA richiedono chaivi crittografiche più lunghe. Nel caso di RSA la lunghezza ad oggi considerata sicura e raccomandata dal NIST è 2048.

Terze parti

Identificazione dei requisiti di sicurezza per l'accesso di fornitori/clienti ad informazioni o beni aziendali	
Minaccia	Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione, ad opera di soggetti esterni.
Contromisure	Devono essere considerati e identificati tutti i requisiti di sicurezza prima di concedere ai partners, fornitori/clienti, anche in fase di trattativa, l'accesso a informazioni o beni dell'organizzazione ospitati nel sistema/piattaforma. Effettuare un'analisi dei rischi per valutare l'impatto sul business aziendale (a livello economico, d'immagine, di continuità operativa, eccetera) nel caso di violazioni della sicurezza, divulgazione non autorizzata (es. a concorrenti), illecito trattamento delle informazioni, effettuati da tali soggetti che accedono ad informazioni.

Identificazione dei requisiti di sicurezza negli accordi con i fornitori/clienti	
Minaccia	Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione, ad opera di soggetti esterni.
Contromisure	Gli accordi con terze parti che prevedono accesso, elaborazione, comunicazione, aggiunte o, in generale, gestione delle informazioni ospitate nel sistema/piattaforma dell'organizzazione, devono considerare tutti i requisiti di sicurezza pertinenti. Prevedere, in particolare, misure preventive per evitare violazioni o illeciti delle terze parti nella gestione delle informazioni. Definire con precisione le attività, le modalità, le responsabilità e la periodicità, per l'esercizio di diritti di audit o comunque di verifiche sull'attività dei fornitori/clienti. Gli accessi logici privilegiati da parte di soggetti esterni devono essere subordinati alla nomina di tali soggetti ad amministratori di sistema, e tale nomina deve essere a sua volta legata ad uno specifico contratto con la ditta di appartenenza comprendente accordi di riservatezza e regole per il corretto uso delle risorse informatiche vincolanti per il fornitore e per i suoi dipendenti. Ovviamente gli accessi logici devono essere monitorati da parte di fornitori devono essere completamente monitorati. In ogni caso gli accessi privilegiati da parte di soggetti esterni non devono mai avvenire da sedi esterne (es. sede fornitore).

5.1.2 Autenticazione

Gestione delle informazioni segrete di autenticazione degli utenti	
Minaccia	Accesso non autorizzato alle informazioni
Contromisure	L'assegnazione agli utenti delle informazioni segrete di autenticazione (es. password) deve essere controllata attraverso un processo di gestione. Il processo dovrebbe prevedere: - l'uso di user ID e password individuali per sostenere il principio di accountability; - le modalità di assegnazione temporanea delle informazioni segrete di autenticazione, da cambiare al primo uso; - procedure per verificare l'identità di un utente, prima di fornire, modificare o sostituire nuove informazioni; - le modalità per assicurare il rispetto dell'utente della riservatezza delle informazioni segrete di autenticazione. Per quest'ultimo punto l'organizzazione dovrebbe informare l'utente delle sue responsabilità ed acquisire dallo stesso un formale impegno a mantenere riservate le informazioni (ad es. mediante specifica lettera da sottoscrivere).

Criteri per l'autenticazione mediante password	
Minaccia	- Accesso non autorizzato alle informazioni. - Furto di credenziali di autenticazione (ad es. con attacchi in grado di sfruttare l'eventuale inadeguatezza delle password). - Uso non autorizzato di privilegi (ad es. mediante tecniche di "escalation" verticali su un target o orizzontali).
Contromisure	Configurare le funzioni di controllo della qualità delle password per l'accesso ai sistemi, affinché la composizione rispetti i criteri di lunghezza, complessità e univocità necessari per avere una robustezza elevata. Ovvero, la password: - deve essere composta da un numero crescente di caratteri (almeno 8) in funzione della criticità delle informazioni da difendere (es. 15 caratteri per utenze amministrative); - deve contenere caratteri di almeno tre delle quattro categorie seguenti: a. lettere maiuscole dell'alfabeto latino (dalla A alla Z); b. lettere minuscole dell'alfabeto latino (dalla a alla z); c. numeri in base 10 (da 0 a 9); d. caratteri speciali non alfanumerici, ad esempio punto esclamativo (!); - non si deve riferire a qualcosa che qualcun altro possa facilmente indovinare od ottenere utilizzando informazioni relative alla persona (ad esempio: nomi, numeri di telefono e date di nascita, etc.); Inoltre devono essere rispettate le seguenti regole: - Vietare nomi di account predefiniti e rinominare account standard come, ad esempio, l'account amministratore; - Non mostrare a video la password (ma neanche PIN, passphrase, ecc., in generale: chiavi segrete) quando viene inserita e non dare indicazioni sulla sua lunghezza; - La password temporanea deve essere obbligatoriamente cambiata al primo log-on; - Deve essere forzato per tutti gli utenti, e particolarmente per gli amministratori, il cambiamento periodico della password; - La procedura di cambiamento della password deve impedire il riutilizzo di tutte le password precedentemente utilizzate e includere una procedura efficace che tenga conto di errori di inserimento; - Limitare il numero di tentativi consentiti in un determinato periodo di tempo o, alternativamente, effettuare il blocco dell'account per l'accesso da parte degli utenti finali dopo un determinato numero di tentativi; - Non consentire l'accesso fino a quando il processo di log-on sia stato completato con successo; - Convalidare le informazioni del log-on solo al completamento di tutti i dati di input. Se una condizione di errore si presenta, il sistema non deve indicare quale dato è corretto o incorretto; - Limitare il tempo entro il quale la procedura di log-on deve ultimarsi. In caso di eccesso, la procedura deve terminare; - Considerare di visualizzare le informazioni seguenti a valle di log-on con successo: a. data e ora del precedente log-on di successo; b. dettagliare ogni tentativo di log-on di insuccesso dall'ultimo log-on di successo; - La persistenza e la trasmissione delle password deve avvenire in modo protetto. Per quanto concerne la persistenza, la forma "hash salted" rappresenta la best practices; - Per contrastare la possibilità fornita dalla cache del browser nel consentire l'accesso, implementare un criterio che consente all'utente di scegliere di non

	salvare le credenziali o di forzare tale criterio come predefinito; - Tracciare sia gli accessi riusciti sia i tentativi di accesso falliti; - Eseguire l'Audit degli accessi non andati a buon fine per rilevare tentativi di hacking delle password; - Controllare e validare sempre l'indirizzo IP sorgente del client usato dall'utente: a. Se l'applicazione è destinata alla sola intranet, impedire accessi provenienti da indirizzi IP esterni alla propria LAN; b. Se l'applicazione è destinata ad utenti Internet ma la connessione arriva da IP esteri, prevedere un livello di controllo maggiore (es. una convalida via SMS su un numero di cellulare italiano, oppure più in generale per applicazioni critiche l'uso di meccanismi di autenticazione a due fattori); c. Se l'applicazione è destinata ad utenti Internet italiani, quando risulti tecnicamente fattibile si dovrebbe rilevare e impedire l'eventuale accesso da IP esteri basato su un servizio di Proxy Server situato in Italia. Tali requisiti dovrebbero essere periodicamente riesaminati per mantenere o rendere più sicura la password.

Altri criteri per l'autenticazione	
Minaccia	Accesso non autorizzato alle informazioni.
Contromisure	La password costituisce la protezione minima obbligatoria per tutti gli accessi logici che richiedono l'identificazione dell'utente. Forme alternative più robuste di autenticazione quali one-time password o autenticazione forte a due fattori detta anche 2FA (pine e token o pin e impronta biometrica) o a tre fattori (pin, token e biometria) devono essere utilizzate per gli accessi amministrativi e per l'accesso a dati e sistemi critici secondo un approccio basato sull'analisi dei rischi. Per semplificare l'adozione dei meccanismi di autenticazione forte è possibile adottare soluzioni basate su sistemi gatekeepers che permettono di intermediare l'accesso privilegiato ai sistemi target senza che su di essi sia necessario alcun intervento. Per sistemi isolati o in ambiti IT ristretti, è opportuno preferire l'amministrazione di sistema esclusivamente attraverso l'accesso fisico locale al sistema, restringendo la possibilità di accesso remoto al minimo. In contesti più estesi la gestione remota è in genere indispensabile; in tal caso, a causa della sensibilità dei dati passati sulle interfacce amministrative, è necessario utilizzare canali crittografati, ad esempio, con tecnologia VPN o SSL, e nel caso del Remote Desktop di Windows è necessario abilitare la crittografia del protocollo RDP. Per ridurre ulteriormente il rischio, va considerato anche l'impiego di politiche IPSec per limitare la gestione remota dei computer collegati nella rete interna. In tutti i casi, il numero delle interfacce di amministrazione deve essere ridotto al minimo, disabilitando quelle non in uso.

Corretto utilizzo delle informazioni segrete di autenticazione	
Minaccia	Accesso non autorizzato alle informazioni
Contromisure	Tutti gli utenti devono essere informati dall'organizzazione sul corretto utilizzo delle informazioni segrete di autenticazione. Tutti gli utenti dovrebbero essere avvisati di: - evitare di tenere una registrazione (per esempio su carta, documenti software) delle informazioni segrete di autenticazione, salvo indicazione di un metodo di memorizzazione sicura; - modificare le informazioni segrete di autenticazione ogni qualvolta vi sia un'indicazione della loro possibile compromissione.

	L'organizzazione dovrebbe definire un processo affinché l'utente "proprietario" o altri utenti possano segnalare immediatamente - H24 - eventi/incidenti di sicurezza inerenti l'informazione segreta di autenticazione, quali: la divulgazione non autorizzata o la perdita di segretezza.

5.1.3 Autorizzazione

Definizione della politica di controllo accesso logico	
Minaccia	Accesso non autorizzato alle informazioni (ad es. causato dal personale utente per carenza di una politica per il controllo degli accessi che accoglie i requisiti di sicurezza).
Contromisure	Definire e documentare la politica che regola le autorizzazioni per ciascun utente e gruppo di utenti con una granularità che consenta un rigoroso rispetto del principio del ''need to know''. Deve essere soddisfatta la regola del ''tutto proibito tranne ciò che è espressamente concesso''. La politica deve tenere conto di: - requisiti di sicurezza delle applicazioni e dei rischi che le informazioni gestite da tali applicazioni possono incontrare; - leggi e obblighi contrattuali che riguardano la protezione degli accessi a dati e servizi; - gestione dei diritti di accesso in un ambiente distribuito e di rete che riconosce ogni tipo di connessione disponibile; - separazione dei ruoli riguardanti il controllo degli accessi (richiesta di accesso, autorizzazione degli accessi, amministrazione degli accessi); - rimozione dei diritti di accesso per le credenziali non utilizzate da almeno sei mesi.

Separazioni dei compiti e delle responsabilità	
Minaccia	Abuso di risorse.
Contromisure	I compiti e le aree di responsabilità in conflitto tra loro devono essere separati al fine di ridurre le possibilità di accedere, modificare o utilizzare asset dell'organizzazione impropriamente, senza autorizzazione o misure di controllo.

Definizione di regole di trattamento ed etichettatura	
Minaccia	Compromissione della sicurezza dell'informazione per carenza di regole di classificazione e trattamento delle informazioni
Contromisure	Definire criteri e procedure per la corretta etichettatura delle informazioni (non solo in forma elettronica, ma anche cartacea). Considerare le seguenti etichette: - Confidenziale (Informazione la cui impropria diffusione può provocare danni molto gravi, ad esempio: perdite economiche, conseguenze legali, conseguenze sul patrimonio, danno di immagine) - Riservata (Informazione la cui impropria diffusione può provocare danni gravi, ad esempio: perdita di vantaggio competitivo) - Interna (Informazione la cui diffusione può provocare danno lieve) - Pubblica (Informazione la cui diffusione non può provocare danno) Definire procedure che regolino come debba avvenire il trattamento delle informazioni ai vari livelli di classifica con riferimento alle attività di elaborazione, diffusione, utilizzo, custodia, riclassificazione, distruzione. Rendere disponibili le procedure a tutto il personale.

Definizione e assegnazione di ruoli e responsabilità	
Contromisura	Compromissione della sicurezza dell'informazione per carenza dell'organizzazione

	interna
Contromisure	Dare la responsabilità delle informazioni (insieme di dati) e delle risorse associate per la loro elaborazione (processo di business, gruppo specifico di attività, applicazioni) ad una determinata parte dell'organizzazione per assicurare l'appropriata classificazione e l'applicazione delle politiche di controllo degli accessi a tali risorse. In particolare: - identificare e definire chiaramente i vari beni (quali i server, le postazioni di lavoro client, gli apparati di rete e di sicurezza, i sistemi di storage, i dispositivi di stampa, i sistemi di continuità elettrica, ecc.) e i processi di sicurezza (es. gestione degli incidenti, gestione delle configurazioni di sistema, gestione degli aggiornamenti, gestione dei sistemi antivirus, gestione dei sistemi firewall, gestione delle verifiche tecniche di vulnerability assessment, gestione delle non conformità e monitoraggio dei rientri, ecc.); - nominare un responsabile della sicurezza di ciascun bene e un responsabile per ciascun processo di gestione della sicurezza e documentare in modo; dettagliato i processi, definendo in modo chiaro i ruoli e le responsabilità - definire chiaramente i livelli di autorizzazione per l'accesso o l'utilizzo di ciascun bene.

Protezione dell'accesso ai dati	
Minaccia	- Abuso di privilegi da parte dell'utente. Accesso non autorizzato ai sistemi (risorse di sistema, configurazioni, ecc.). - Accesso non autorizzato alle informazioni. - Furto di credenziali di autenticazione.
Contromisure	Per quanto riguarda il furto di credenziali di autenticazione e quel che ne consegue (accesso non autorizzato a sistemi e informazioni, furto d'identità, ecc.), è necessario stabilire meccanismi di autenticazione la cui robustezza sia adeguata alla criticità dell'applicazione e ancor più alla sensibilità dei dati che l'applicazione tratta. Ad es. per applicazioni critiche o dati particolarmente sensibili è necessario adottare meccanismi di autenticazione a due fattori, basati ad es. su SMS inviati su un numero di cellulare precedentemente "certificato", o codici inviati tramite una app per smartphone o altri metodi equivalenti. Tuttavia qualsiasi misura di sicurezza in tale ambito può risultare inefficace se non accompagnata da una appropriata campagna di diffusione della consapevolezza delle problematiche di sicurezza ("security awareness") verso gli utenti che devono essere informati e responsabilizzati verso un uso corretto delle credenziali di autenticazione con documenti (politiche di sicurezza) ed eventualmente corsi di formazione. Per impedire l'accesso non autorizzato ai dati, a riposo e/o in transito, da parte di utenti reali (ma non abilitati per i dati in oggetto) e per limitare le possibilità di accesso di eventuali utenti che abbiano ottenuto illecitamente delle credenziali valide non di propria pertinenza, i dati memorizzati all'interno dei sistemi (file e cartelle) devono essere adeguatamente protetti attraverso l'assegnazione di diritti di accesso il più possibile granulari e specifici (dal punto di vista delle risorse). Qualora i dati siano conservati in archivi elettronici (es. database) accertarsi che l'accesso ai dati avvenga mediante un'adeguata profilatura degli utenti e che le applicazioni che accedono ai database non utilizzino una singola utenza di "super-amministratore" per tutte le operazioni, dato che tale configurazione può essere sfruttata da un malintenzionato per prendere pieno possesso dell'archivio. L'organizzazione dovrebbe adottare controlli di accesso fisico e/o logico per l'isolamento di applicazioni, dati o sistemi critici o sensibili. Per l'accesso ai dati critici o sensibili definire requisiti di sicurezza più stringenti applicando tecniche di cifratura o altri meccanismi di sicurezza per rafforzare la protezione dell'accesso.

	Infine, per quanto riguarda l'abuso di privilegi da parte degli utenti, questo fenomeno può essere contrastato con un approccio basato su più aspetti: - Diffondere tra gli utenti un documento di politiche di sicurezza che spieghi qual è l'uso corretto delle risorse. - Impiegare meccanismi di tracciamento delle operazioni effettuate dagli utenti in grado di registrare i tentativi di accesso non riusciti a risorse per le quali non si dispone delle necessarie autorizzazioni, nei limiti imposti dalle leggi vigenti. - Informare gli utenti attraverso "banner" di accesso (oltre alle citate politiche di sicurezza) dell'esistenza di tali meccanismi di tracciamento. - Educare gli utenti ad un uso corretto delle risorse attraverso corsi di formazione.

5.1.4 Crittografia

Protezione delle informazioni strumentali all'accesso	
Minaccia	Crittografia debole o non validata.
Contromisure	- Non sviluppare e utilizzare algoritmi di crittografia personalizzati/propri. - Utilizzare servizi, funzioni e algoritmi crittografici la cui robustezza sia comprovata da certificazioni e standard riconosciuti a livello internazionale, e che risultino esenti da vulnerabilità note. A titolo esemplificativo e non esaustivo, per la crittografia deve essere usato quanto meno l'algoritmo AES a 128 bit (o meglio a 256 bit se possibile), per le funzioni di hashing quanto meno lo SHA-256 (MD5 e SHA-1 sono deprecati), per le connessioni internet sicure almeno TLS 1.2 (SSL e TLS precedenti alla 1.2 sono vulnerabili e deprecate). - Per quanto riguarda prodotti di crittografia a titolo esemplificativo devono disporre quanto meno di certificazione Common Criteria In genere EAL 4+ (ma a seconda dei casi possono essere richiesti livelli minori o anche superiori in base a regolamenti e norme di legge). - Mantenersi informati sugli algoritmi manomessi e sulle tecniche utilizzate per la manomissione, attraverso i bollettini di sicurezza emessi sia dai vendor sia da fonti internazionali autorevoli, sia dal CERT della PA.

Protezione dei dati di autenticazione (trasmissione)	
Minaccia	Crittografia debole o non validata.
Contromisure	Meccanismi, strumenti, procedure o abilità tecniche atti a prevenire l'accesso non autorizzato al sistema e a proteggere i dati di autenticazione quando memorizzati o trasmessi.

Protezione delle informazioni	
Minaccia	Crittografia debole o non validata.
Contromisure	I controlli crittografici devono essere utilizzati in conformità a tutti gli accordi, leggi e regolamenti pertinenti. Considerare di adeguarsi alle best practices di crittografia. Di seguito vengono indicate le principali: - Trasmissione dati: usare TLS 1.2 o 1.3. A partire dalla prima metà del 2020 le versioni 1.0 e 1.1 del protocollo, verranno considerate deprecate (viceversa SSL v2 e v3 sono considerate insicure). - Cifratura dati: usare AES con una chiave a 256 bit (3DES solo per backward compatibility, DES è considerato insicuro). - Hashing: usare SHA-256 (evitare SHA-1, mentre MD5 è considerato insicuro).

	- RSA: usare chiavi a 2048 bit. - Algoritmo di scambio chiavi: Utilizzare la feature "Forward Secrecy" conosciuta anche come "Perfect Forward Secrecy", per garantire che nel caso di compromissione di una chiave privata ciò non pregiudichi anche le chiavi delle altre sessioni. Per abilitare tale feature è necessario configurare TLS 1.2 in modo tale che venga adottato come algoritmo di scambio delle chiavi l'Elliptic Curve Diffie-Hellman (con Diffie-Hellman come algoritmo di fallback), ed evitare totalmente, se possibile, lo scambio chiavi tramite RSA. L'utilizzo di TLS 1.3 invece garantisce l'impiego della forward secrecy per tutte le sessioni TLS attraverso l'uso del protocollo di scambio chiavi Ephemeral Diffie-Hellman. - Ripristino della sessione TLS: Analogamente all'utilizzo del keepalives impiegato per mantenere le connessioni TCP persistenti attive, l'abilitazione del ripristino della sessione TLS "TLS Session Resumption" consente al server Web di tenere traccia delle ultime sessioni SSL/TLS negoziate e quindi di ripristinarle, scongiurando l'overhead computazionale dovuto alla negoziazione della chiave di sessione.

Protezione delle informazioni	
Minaccia	- Violazione di leggi, di regolamenti, di obblighi contrattuali. - Compromissione delle comunicazioni. - Falsificazione di identità.
Contromisure	I controlli crittografici devono essere utilizzati in conformità a tutti gli accordi, leggi e regolamenti pertinenti. Considerare di adeguarsi alle best practices di crittografia. Di seguito vengono indicate le principali: - Trasmissione dati: usare TLS 1.2 o 1.3 (viceversa SSL v2 e v3 sono considerate insicure). - Cifratura dati: usare AES con una chiave a 256 bit (3DES solo per retro-compatibilità, DES è considerato insicuro). - Hashing: usare SHA-256 (evitare SHA-1, mentre MD5 è considerato insicuro). - RSA: usare chiavi almeno a 2048 bit. - Algoritmo di scambio chiavi: Utilizzare la feature "Forward Secrecy" conosciuta anche come "Perfect Forward Secrecy", per garantire che nel caso di compromissione di una chiave privata ciò non pregiudichi anche le chiavi delle altre sessioni. Per abilitare tale feature è necessario configurare TLS 1.2 in modo tale che venga adottato come algoritmo di scambio delle chiavi l'Elliptic Curve Diffie-Hellman (con Diffie-Hellman come algoritmo di fallback), ed evitare totalmente, se possibile, lo scambio chiavi tramite RSA. L'utilizzo di TLS 1.3 invece garantisce l'impiego della forward secrecy per tutte le sessioni TLS attraverso l'uso del protocollo di scambio chiavi Ephemeral Diffie-Hellman. - Ripristino della sessione TLS: Analogamente all'utilizzo del keepalives impiegato per mantenere le connessioni TCP persistenti attive, l'abilitazione del ripristino della sessione TLS "TLS Session Resumption" consente al server Web di tenere traccia delle ultime sessioni SSL/TLS negoziate e quindi di ripristinarle, scongiurando l'overhead computazionale dovuto alla negoziazione della chiave di sessione.

Protezione delle informazioni strumentali all'accesso	
Minaccia	Generazione e/o gestione inadeguata delle chiavi crittografiche.
Contromisure	Utilizzare routine di crittografia integrate che includono la gestione delle chiavi

	protette. L'interfaccia di programmazione per la protezione dei dati applicativi (DPAPI) è un esempio di un servizio di crittografia fornito su sistemi operativi Windows 2000 e successivi in cui il sistema operativo gestisce la chiave. Se si utilizza un meccanismo di crittografia che richiede di generare o gestire la chiave, utilizzare algoritmi di generazione forti delle chiavi casuali e memorizzare la chiave in una posizione protetta. Ad esempio, in una chiave del Registro di sistema protetta con un ACL restrittivo. Crittografare la chiave di crittografia utilizzando DPAPI per una maggiore sicurezza. Impostare i limiti temporali di scadenza delle chiavi ad intervalli regolari.

5.1.5 Documentazione

Protezione della documentazione di sistema da accessi non autorizzati	
Minaccia	Accesso non autorizzato alle informazioni.
Contromisure	La documentazione di sistema (ad es. relativa al software del web server/DBMS, della piattaforma ospitante il web server/DBMS, ecc.) deve essere protetta da accessi non autorizzati e conservata in modo sicuro. In particolare, la documentazione cartacea, se non utilizzata, deve essere conservata e custodita all'interno di contenitori (es. armadi, cassettiere) chiusi a chiave e accessibile esclusivamente dai soggetti autorizzati. Per la documentazione memorizzata su supporto informatico l'accesso dovrebbe essere consentito ad una lista ridotta di utenti, mediante l'utilizzo di idonei sistemi di autenticazione e autorizzazione informatica.

5.1.6 Logging

Registrazione degli eventi (audit)	
Minaccia	- Abuso di privilegi da parte dell'utente - Cancellazione dei log di accountability e/o ripudio di operazioni effettuate. - Negazione dei servizi.
Contromisure	I log di audit che registrano le attività dell'utente, le eccezioni e gli eventi di sicurezza devono essere prodotti e conservati per essere utilizzati in indagini, come prove da esibire in caso di dispute, e monitoraggi, come elementi da considerare nell'identificazione di misure migliorative della sicurezza. Gli eventi che devono essere registrati includono: - log-on e log-off e durata dell'accesso dell'utente o applicazione software; - tentativi di accesso riusciti e falliti; - utilizzo di funzioni amministrative o di gestione; - avvio e arresto delle funzioni di audit; - errori del software. La registrazione dell'evento deve riportare almeno i seguenti dati: - identità dell'utente o l'identificativo del processo che ha scatenato l'evento; - indirizzo IP dell'utente nel caso di sessione remota; - data e ora dell'evento; - tipo dell'evento; - oggetti coinvolti dall'evento; - eventuali errori prodotti dall'evento. . Conservare i dati relativi agli eventi registrati per un periodo di tempo di almeno 5 anni.

Adozione di misure idonee a garantire inalterabilità e integrità dei log registrati	
Minaccia	- Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione. - Abuso di privilegi da parte dell'utente - Abuso di risorse. - Cancellazione dei log di accountability e/o ripudio di operazioni effettuate. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste; tale verifica avviene in conformità alla normativa in materia di protezione dei dati personali (Privacy) e dei principi di sicurezza. Proteggere i file di log utilizzando ACL restrittivi. Attraverso un processo automatico schedulato a intervalli regolari (ad es. ogni notte), spostare i file di log fin lì prodotti in una posizione diversa da quella predefinita e comprimerli. Predisporre un processo automatico per la raccolta dei log compressi e il loro trasferimento su un server centralizzato.

Registrazione e Analisi periodica dei log degli errori	
Minaccia	Accesso non autorizzato alle informazioni
Contromisure	Le segnalazioni di errori (es. di malfunzionamenti, di eventi anomali di sicurezza che possono essere segnali di un probabile attacco o palesi tentativi di intrusione) devono essere registrate cronologicamente nei file di log del sistema, archiviate centralmente su un sistema dedicato e analizzate periodicamente per rilevare prontamente eventuali segnali che possono indicare l'insorgenza di un malfunzionamento (che può portare a un disservizio) o per rilevare tentativi di attacco. I file di log raccolti sul sistema centralizzato devono essere mantenuti per un congruo periodi di tempo (in genere sei mesi), allo scopo di consentire analisi anche in tempi successivi e per analisi di tipo statistico. Si noti che i file di log relativi a transazioni bancarie, dati di traffico telematico e telefonico, dati personali, sensibili e giudiziari, sono soggetti a specifiche norme di legge che prescrivono tra l'altro tempi massimi consentiti di mantenimento, oltre i quali devono essere obbligatoriamente cancellati.

Conservazione dei log registrati degli amministratori di sistema	
Minaccia	- Cancellazione dei log di accountability e/o ripudio di operazioni effettuate. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione. - Violazione di leggi, di regolamenti, di obblighi contrattuali. - Abuso di privilegi da parte degli utenti. - Abuso di risorse.
Contromisure	- Tracciare eventi chiave come gli eventi di login e logout, i tentativi di login falliti, l'uso di privilegi elevati, le transazioni applicative critiche dal punto di vista della sicurezza, l'accesso e il tentativo fallito di accesso a oggetti e risorse critiche per la sicurezza. - Non utilizzare account condivisi o di ruolo poiché non è possibile determinare la vera identità dei soggetti. Gli accessi degli amministratori devono essere sempre nominativi e i relativi identificativi in caso siano revocati non devono più essere riassegnati ad altri utenti neppure in tempi diversi. - Salvare i log di accesso amministrativo ai sistemi e quelli di audit (operazioni che richiedono l'uso di privilegi) su sistemi di raccolta centralizzati.

	- Le registrazioni dei log degli amministratori devono essere conservate per un congruo periodo, non inferiore a sei mesi, in conformità alla normativa in materia di protezione dei dati personali (Privacy) e dei principi di sicurezza. - Tracciare le operazioni critiche eseguite a livello applicativo. - Eseguire un regolare backup dei file di log e analizzarli regolarmente per verificare la presenza di attività sospette.

Protezione log	
Minaccia	- Abuso di privilegi da parte dell'utente. - Negazione dei servizi (ad es. da errori hardware/software non rilevati in maniera tempestiva o corretta per carenze di monitoraggio nei sistemi ICT). - Accesso non autorizzato alle informazioni. - Accesso non autorizzato ai sistemi (risorse di sistema, configurazioni, ecc.). - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Controllare che le informazioni contenute nei file di log siano protette da manomissioni e accessi non autorizzati e che non ci siano problemi operativi con le logging facilities. In particolare, occorre verificare che non vi sia: - alterazione delle informazioni tracciate nel file di log; - discordanza fra il periodo di conservazione dei log e quanto indicato dalle policy di retention o specifiche disposizioni legali; - fallimento delle operazioni di registrazione degli eventi causato da un raggiungimento della dimensione massima del file di log; - sovrascrittura delle informazioni precedentemente tracciate causata da un raggiungimento della dimensione massima del file di log, nel caso in cui la scrittura dei log sia effettuata in modo ciclico sempre sullo stesso file.

Registrazione degli accessi logici da parte degli amministratori di sistema	
Minaccia	- Abuso di privilegi da parte dell'utente; - Cancellazione dei log di accountability e/o ripudio di operazioni effettuate.
Contromisure	Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) al sistema/piattaforma da parte degli amministratori di sistema. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate. Si tenga presente che il controllo e la registrazione possono essere aggirati da un account condiviso (questo vale sia per gli account amministrativi che per gli account utente / applicativi / di servizio): pertanto gli account amministrativi non devono essere condivisi. In generale, anche per gli account utente non privilegiati e per gli account usati dagli applicativi per l'esecuzione dei servizi in uno specifico contesto (es. account httpd per un server web in ambito UNIX), devono essere nominativi / specifici per l'utente o l'applicativo e non condivisi.

5.1.7 Procedure

Change management

Gestione dei cambiamenti	
Minaccia	- Accesso non autorizzato ai sistemi (risorse di sistema, configurazioni, ecc.). - Accesso non autorizzato alle informazioni. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione.

	- Negazione dei servizi.
Contromisure	Deve essere definito un processo di gestione dei cambiamenti (all'interno del ciclo di vita dei sistemi, nonché per i processi organizzativi di gestione della sicurezza) che tenga in considerazione l'identificazione delle esigenze che determinano il "change", l'analisi e la valutazione degli impatti del "change" (anche in termini di "non regressione"), la progettazione e la realizzazione, il testing, l'implementazione, la verifica, l'eventuale rollback in caso di errori nell'implementazione. La gestione dei cambiamenti può avere come oggetto un servizio, un sistema informativo, un'applicazione, un processo organizzativo o un processo di gestione della sicurezza, ecc. Quando vengono apportate delle modifiche a servizi, sistemi o processi, queste devono essere documentate in un registro, riportando informazioni dettagliate sui cambiamenti apportati.

Procedura di monitoraggio dei cambiamenti	
Minaccia	- Accesso non autorizzato ai sistemi (risorse di sistema, configurazioni, ecc.). - Accesso non autorizzato alle informazioni. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione. - Negazione dei servizi. - Attacchi all'integrità dei sistemi (software e configurazioni).
Contromisure	Definire delle formali procedure di controllo dei cambiamenti al fine di garantire l'integrità dei sistemi, delle applicazioni e dei prodotti. L'introduzione di nuovi sistemi e significativi cambiamenti sui sistemi esistenti dovrebbero seguire un processo formale di documentazione, specifica, test, controllo di qualità e gestione dell'implementazione. I cambiamenti non autorizzati o che comunque non hanno seguito un processo formali di "change" devono essere rilevati. Ad es. possono essere utilizzati sistemi cosiddetti "Configuration Management Data Base" o CMDB dotati di agent che rilevano le configurazioni dei sistemi e possono anche generare alert se tali configurazioni sono diverse da quelle stabilite. Funzionalità ancora più avanzate che comprendono la verifica anche su eseguibili e librerie installate nel sistema e controlli di integrità, possono essere ottenute con sistemi di controllo della compliance che generano delle "firme" per ciascuna componente software e le confrontano con quelle definite come "baseline" in fase di rilascio dell'ultimo "change" autorizzato.

Riesame tecnico a seguito di cambiamenti	
Minaccia	- Accesso non autorizzato ai sistemi (risorse di sistema, configurazioni, ecc.). - Accesso non autorizzato alle informazioni. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione. - Negazione dei servizi. - Attacchi all'integrità dei sistemi (software e configurazioni).
Contromisure	Definire un processo per il riesame tecnico delle applicazioni in seguito a cambiamenti apportati nelle piattaforme operative (quest'ultime includono i sistemi di produzione, i database e le piattaforme di middleware). Effettuare i necessari test applicativi per assicurare che non ci siano impatti negativi sull'operatività o sulla sicurezza dell'organizzazione.

Maintenance

Redigere e applicare le procedure operative	
Minaccia	- Abuso di privilegi da parte dell'utente. - Abuso di risorse. - Errori di amministrazione dei sistemi.
Contromisure	Le procedure operative concernenti la manutenzione delle strutture di elaborazione delle informazioni, quali: - installazione e configurazione iniziale dei sistemi; - backup e restore; - gestione delle vulnerabilità tecniche e aggiornamenti; - manutenzione delle apparecchiature; - sicurezza fisica delle apparecchiature e procedure per l'accesso fisico del personale tecnico addetto alla manutenzione; - elenco dei componenti hardware e delle parti di ricambio, dei relativi fornitori, dei livelli di servizio per l'assistenza (es. risposta e presa in carico h24 7x7, con risoluzione entro il next business day), dei riferimenti per la richiesta di intervento; - procedura per la corretta dismissione del sistema e delle sue componenti; devono essere formalmente documentate per iscritto, mantenute attive e aggiornate periodicamente al sopraggiungere di ogni cambiamento. Ciascuna procedura deve essere distribuita e resa nota ai soggetti interessati attraverso un portale documentale interno all'ente/organizzazione.

Backup delle informazioni e del software	
Minaccia	- Negazione dei servizi. - Cancellazione o furto di informazioni.
Contromisure	Effettuare periodicamente copie di backup delle informazioni e del software, in conformità alla politica per il salvataggio dei dati stabilita a livello aziendale. Verificare periodicamente, nel rispetto delle leggi, regolamenti, obblighi contrattuali, l'effettiva memorizzazione, "leggibilità" e integrità delle informazioni registrate, anche al fine di assicurare la pronta disponibilità delle stesse in caso di interruzione dei servizi informativi. Individuare le responsabilità per la gestione delle copie di backup.

Account dedicato al gruppo di manutenzione	
Minaccia	- Divulgazione di informazioni riservate. - Abuso di risorse. - Accesso non autorizzato ai sistemi (risorse di sistema, configurazioni, ecc.). - Accesso non autorizzato alle informazioni. - Uso non autorizzato di privilegi. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Affidare gli interventi di manutenzione che richiedono un accesso ai sistemi al solo personale formalmente autorizzato, appartenente a società fornitrici con le quali sono stati stipulati appositi contratti che vincolano il manutentore al corretto uso delle risorse informative e alla riservatezza. Il manutentore in tali casi dovrà essere munito di un apposito account amministrativo nominativo abilitato solo ai compiti stabiliti dal contratto di manutenzione. Impedire, se tecnicamente possibile, l'accesso con l'account del manutentore a cartelle, file, dati, interfacce applicative di esclusiva pertinenza degli utenti autorizzati. Gli interventi di manutenzione che avvengono attraverso un accesso remoto non devono mai avvenire dalla sede della società fornitrice, ma sempre dalla rete interna dell'ente/organizzazione. In ogni caso le sessioni di amministrazione remota devono

	usare protocolli autenticati e cifrati.

Manutenzione periodica dell'asset	
Minaccia	- Negazione dei servizi (per carenze di monitoraggio nei sistemi ICT). - Cancellazione o furto di informazioni. - Attacchi all'integrità delle informazioni. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Eseguire un'attività di manutenzione, con cadenza almeno semestrale, mediante procedure rigorose ed efficaci che prevedano una modulistica di intervento con esplicitazione dell'anomalia dichiarata, malfunzionamento accertato, intervento effettuato e parti sostituite. Effettuare delle statistiche sulla manutenzione di ogni singolo componente al fine di valutarne il livello di obsolescenza e definire un programma di manutenzione preventiva.

Regolamentazione della manutenzione dei dispositivi ICT	
Minaccia	- Divulgazione di informazioni riservate. - Accesso non autorizzato ai sistemi (risorse di sistema, configurazioni, ecc.). - Accesso non autorizzato alle informazioni. - Violazione di leggi, di regolamenti, di obblighi contrattuali
Contromisure	In generale, prima di affidare le apparecchiature a servizi esterni di manutenzione è necessario stabilire contrattualmente opportune clausole di riservatezza e di non divulgazione delle informazioni e valutare i rischi di sicurezza. In alcuni casi è necessario considerare la possibilità di sostituire le apparecchiature danneggiate, piuttosto che ripararle, per evitare il rischio di compromissione della riservatezza di informazioni particolarmente critiche. In tal caso prima di gettare tali apparecchiature è necessario distruggerle fisicamente. Naturalmente questo dipende dalla riservatezza dei dati contenuti. La regola da osservare è la seguente: I dispositivi di memorizzazione che contengono informazioni riservate come ad es. dati personali, sensibili o giudiziari, dati di traffico telematico e telefonico, dati relativi a transazioni bancarie, specie se tali dati risultino in chiaro (non cifrati), quando risultino danneggiati non possono essere inviati a società esterne per la riparazione, a meno che non sia possibile effettuare una cancellazione sicura dei dati memorizzati. Negli altri casi, e più in generale ogni volta che tali dispositivi devono essere dismessi, i dati in essi contenuti devono essere resi irrecuperabili con sistemi di smagnetizzazione o attraverso la distruzione fisica.

Regolamentazione della manutenzione della PdL	
Minaccia	- Negazione dei servizi (per impossibilità di amministrarli o monitorarli da parte del personale preposto). - Accesso non autorizzato ai sistemi (risorse di sistema, configurazioni, ecc.). - Accesso non autorizzato alle informazioni. - Divulgazione di informazioni riservate. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Definire una procedura relativamente alla manutenzione delle PdL che preveda: - solo il personale autorizzato alla manutenzione dovrebbe svolgere le riparazioni e le operazioni di servizio alle apparecchiature; - devono essere tenute le registrazioni di tutti i difetti presunti o reali, e di tutti gli interventi di manutenzione preventivi e correttivi; - devono essere adottati dei controlli appropriati quando si inviano all'esterno le

	apparecchiature in manutenzione, tenendo anche conto se tale manutenzione è fatta da personale in sito o all'esterno dell'organizzazione; - ove necessario, si dovrebbero eliminare le informazioni critiche dall'apparecchiatura oppure il personale di manutenzione dovrebbe essere sufficientemente selezionato;

Patching

Controllo di vulnerabilità tecniche	
Minaccia	- Abuso di risorse. - Accesso non autorizzato ai sistemi (risorse di sistema, configurazioni, ecc.). - Accesso non autorizzato alle informazioni. - Compromissione delle comunicazioni. - Crittografia debole o non validata. - Divulgazione di informazioni riservate. - Negazione dei servizi. - Cancellazione o furto di informazioni. - Attacchi all'integrità dei sistemi (software e configurazioni). - Attacchi all'integrità delle informazioni - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Ottenere tempestive informazioni sulle vulnerabilità tecniche dei sistemi di informazione in uso, valutare l'esposizione dell'azienda a tali vulnerabilità e prendere appropriate misure per indicare il rischio associato. A tale scopo è necessario mantenere un inventario aggiornato e completo dei beni quali il rivenditore del software, il numero della versione, i software installati e i sistemi su cui sono installati, e i referenti interni all'azienda responsabili del software. In particolare è necessario: - definire i ruoli e le responsabilità per la gestione delle vulnerabilità tecniche; - definire i mezzi di informazione che saranno usati per identificare le vulnerabilità tecniche; - identificare i rischi associati e le azioni da intraprendere una volta che una potenziale vulnerabilità tecnica è stata identificata; - gestire le patch disponibili valutando anche i rischi associati alla loro installazione; - controllare il processo di gestione delle vulnerabilità tecniche e valutare la sua efficacia ed efficienza.

Software Patching	
Minaccia	- Abuso di risorse. - Accesso non autorizzato ai sistemi (risorse di sistema, configurazioni, ecc.). - Accesso non autorizzato alle informazioni. - Compromissione delle comunicazioni. - Crittografia debole o non validata. - Divulgazione di informazioni riservate. - Negazione dei servizi. - Cancellazione o furto di informazioni. - Attacchi all'integrità dei sistemi (software e configurazioni). - Attacchi all'integrità delle informazioni - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Verificare che sia applicata una procedura di gestione delle patch composto almeno

	dalle fasi di seguito elencate: - Rilevamento, avvalersi di strumenti che verifichino l'eventuale mancanza di patch di protezione. Il rilevamento deve avvenire in modo automatico ed attivare il processo di gestione delle patch; - Valutazione, qualora sia riscontrata la mancanza di aggiornamenti utili, valutare la gravità delle problematiche risolvibili con l'applicazione delle patch; - Acquisizione, nel caso le misure di protezione applicate risultino insufficienti all'eliminazione della vulnerabilità, procedere con lo scaricamento della patch per sottoporla ad un'approfondita analisi; - Verifica, procedere con l'installazione della patch su un sistema di prova al fine di verificare l'impatto delle conseguenze dell'aggiornamento sulla configurazione dell'ambiente di produzione; - Gestione, eseguire la registrazione al servizio di notifica per segnalare eventuali vulnerabilità quando individuate; - Distribuzione, distribuire la patch sulle macchine interessate; prevedere, inoltre, l'adozione di un piano di ripristino o di backup. In presenza di "Zero-day exploit", per i quali non è ancora disponibile la patch, massimizzare la difesa perimetrale ed eseguire il patching appena disponibile e testato.

Secure testing

Vulnerability Assessment	
Minaccia	- Accesso non autorizzato ai sistemi (risorse di sistema, configurazioni, interfacce amministrative, ecc.). - Accesso non autorizzato alle informazioni; - Compromissione delle comunicazioni. - Divulgazione di informazioni riservate. - Negazione dei servizi. - Cancellazione o furto di informazioni. - Attacchi all'integrità dei sistemi (software e configurazioni). - Attacchi all'integrità delle informazioni. - Uso non autorizzato di privilegi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Effettuare almeno una volta l'anno un'attività di Vulnerability Assessment (VA) in modo da identificare le eventuali vulnerabilità che possono costituire un canale di accesso non autorizzato ad informazioni. Il VA deve verificare la corretta configurazione delle porte logiche affinché siano attive solo quelle strettamente necessarie. Inoltre, l'attività di VA deve essere condotta avendo come riferimento le ultime vulnerabilità note, pubblicate nelle banche dati di riferimento in tema di sicurezza informatica come, ad esempio, Open Source Vulnerability DataBase (OSVDB) e Common Vulnerabilities Exposures (CVE). In seguito all'attività di VA, per mitigare il rischio associato alle vulnerabilità identificate è necessario: - definire i ruoli e le responsabilità per la gestione delle vulnerabilità tecniche; - identificare le azioni da intraprendere (es. disabilitare le funzionalità non utilizzate, inclusi protocolli e servizi; rendere più sicure le impostazioni di configurazione predefinite, ridurre al minimo il numero delle interfacce di amministrazione, ecc.); - revisionare le funzionalità di failover del sistema.

Penetration Test

Minaccia	- Accesso non autorizzato ai sistemi (risorse di sistema, configurazioni, interfacce amministrative, ecc.). - Accesso non autorizzato alle informazioni; - Compromissione delle comunicazioni. - Divulgazione di informazioni riservate. - Negazione dei servizi. - Cancellazione o furto di informazioni. - Attacchi all'integrità dei sistemi (software e configurazioni). - Attacchi all'integrità delle informazioni. - Uso non autorizzato di privilegi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Effettuare, almeno una volta l'anno, un'attività di Penetration Test (PT) sui sistemi più critici, simulando dall'esterno un'azione di intrusione al sistema/piattaforma. L'attività deve prevedere degli opportuni scenari d'intrusione affinché siano evidenziate la presenza di vulnerabilità nel sistema, e la conseguente possibilità di ottenere accessi non autorizzati a funzioni ed informazioni riservate.

Fuzzing Test	
Minaccia	- Divulgazione di informazioni riservate. - Negazione dei servizi. - Cancellazione o furto di informazioni. - Attacchi all'integrità dei sistemi (software e configurazioni). - Attacchi all'integrità delle informazioni.
Contromisure	Eseguire test regolari di tipo fuzzing per rilevare e correggere eventuali malfunzionamenti causati da mancata validazione dell'input (es. buffer overflow).

Disposal

Protezione dei dati personali in caso di reimpiego o riciclo dell'apparecchiatura elettronica	
Minaccia	- Accesso non autorizzato alle informazioni. - Divulgazione di informazioni riservate. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Chi procede al reimpiego o al riciclaggio di rifiuti di apparecchiature elettriche ed elettroniche o di loro componenti è comunque tenuto ad assicurarsi dell'inesistenza o della non intelligibilità di dati personali sui supporti, acquisendo, ove possibile, l'autorizzazione a cancellarli o a renderli non intelligibili.

Protezione dei dati personali in caso di smaltimento dell'apparecchiatura elettronica	
Minaccia	- Accesso non autorizzato alle informazioni. - Divulgazione di informazioni riservate. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	In caso di smaltimento di rifiuti elettrici ed elettronici, l'effettiva cancellazione dei dati personali dai supporti contenuti nelle apparecchiature elettriche ed elettroniche può anche risultare da procedure che, nel rispetto delle normative di settore, comportino la distruzione dei supporti di memorizzazione di tipo ottico o magneto-ottico in modo da impedire l'acquisizione indebita di dati personali. La distruzione dei supporti prevede il ricorso a procedure o strumenti diversi a secondo del loro tipo, quali: - sistemi di punzonatura o deformazione meccanica;

	- distruzione fisica o di disintegrazione (usata per i supporti ottici come i cd-rom e i dvd); - demagnetizzazione ad alta intensità.

5.2 Sicurezza dei Sistemi Operativi

Di seguito viene fornita una vista delle principali minacce e delle relative contromisure da adottare.

Sono fornite dapprima una serie di indicazioni generiche, valide per qualsiasi sistema operativo moderno ma con un focus particolare per sistemi destinati ad un ruolo di server, e successivamente una serie di indicazioni specifiche (in paragrafi dedicati) per i sistemi operativi più diffusi, ovvero Windows, Mac OS X e Linux.

5.2.1 Architettura

Architettura	
Minaccia	Accesso non autorizzato alle informazioni.
Contromisure	- Utilizzare un sistema di protezione del perimetro (Firewall). - Segmentare la rete: creare segmenti di rete distinti per le diverse tipologie di sistemi dotate di caratteristiche diverse di sensibilità e tipologia. Ad es. creare un segmento o layer dati, un layer per i server di front-end, un layer per le postazioni di lavoro, un segmento per la rete di amministrazione (da cui gli amministratori accedono alle interfacce amministrative dei server e degli apparati di rete e di sicurezza). - Non usare le VLAN per separare i layer: attestare ogni layer/segmento su una diversa interfaccia del firewall. - Installare un IDS (intrusion detection system) o IPS (intrusion prevention system) - Impiegare VPN terminate sul firewall perimetrale (o su host specifici e dedicati, attestati su una apposita DMZ), per la connessione di utenti remoti e di altre reti appartenenti a diverse sedi dell'ente/organizzazione. - Utilizzare un sistema di controllo accessi alla rete (NAC basato su protocollo 802.1x e Server RADIUS) per prevenire l'accesso tramite cavo da parte di sistemi fraudolenti. - Individuare e rimuovere eventuali punti di accesso wireless non autorizzati e utilizzare su quelli leciti il sistema di protezione Wi-Fi Protected Access versione 2 (WPA2) per la massima protezione dagli attacchi wireless, avendo cura di aggiornare il firmware all'ultima versione disponibile (fine Ottobre 2017 o successiva), in grado di eliminare la vulnerabilità denominata KRACK (Key Reinstallation Attacks) (cfr. https://www.krackattacks.com/). - Collocare i computer e i supporti esterni di memorizzazione dei dati in luoghi sicuri. - Adottare sistemi di controllo basato su ruolo per l'accesso ai computer e ai dati, separando gli utenti in più gruppi con distinto livello di autorizzazione per la lettura e la scrittura dei dati.

Architettura	
Minaccia	- Negazione dei servizi. - Cancellazione di informazioni (accidentale).
Contromisure	Al fine di garantire la continuità operativa del sistema, configurare i dischi in modalità RAID-1 o RAID-5, in modo che i dati presenti su ciascun disco siano replicati. In questo modo in caso di guasto di un disco, sarà possibile continuare ad utilizzare il

	sistema senza perdita di informazione o interruzione di servizi, procedendo tempestivamente alla sostituzione del disco guasto. Ciò si applica sia ai dischi locali al sistema, sia a quelli disponibili in rete attraverso sistemi di Storage Area Networks.

5.2.2 Hardening

Hardening del sistema	
Minaccia	- Accesso non autorizzato ai sistemi (risorse di sistema, configurazioni, interfacce amministrative, ecc.). - Accesso non autorizzato alle informazioni. - Furto di credenziali di autenticazione (ad es. con tecniche di brute-force o password crackers). - Negazione dei servizi. - Cancellazione o furto di informazioni. - Attacchi all'integrità dei sistemi (BIOS, software di base, configurazioni). - Attacchi all'integrità delle informazioni - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Consolidare la sicurezza di base del sistema implementando dei meccanismi di protezione atti a contrastare in maniera più efficace eventuali attacchi e limitarne la capacità di azione. I principali interventi da intraprendere sono: - attivare una password a protezione del BIOS in modo da prevenire alterazioni alla configurazione di avvio del sistema; - impedire l'uso di password vuote; - configurare il sistema affinché obblighi all'uso di password "robuste" (es. almeno una maiuscola, una minuscola, un numero e un carattere speciale, e almeno 8 caratteri di lunghezza); - cambiare le password di default delle utenze di sistema e di quelle applicative in uso; - disabilitare le utenze di sistema e quelle applicative predefinite e non utilizzate; - installare gli aggiornamenti di sicurezza più recenti sia durante la fase di installazione iniziale, prima di iniziare ad utilizzare il sistema, sia regolarmente e periodicamente, quando il sistema è in uso; - disattivare o rimuovere le funzionalità non utilizzate, inclusi protocolli di comunicazione, servizi, software, interfacce di rete, interfacce hardware (es. porte seriali e parallele, cd-rom se non usati, porte usb se non permesse, ecc.); - assicurarsi che i permessi d'accesso (lettura, scrittura, modifica, etc.) al file system siano concessi secondo la profilatura degli utenti accreditati, evitando la presenza di condivisioni accessibili indiscriminatamente da tutti gli utenti dell'organizzazione, o senza autenticazione, o scrivibili da chiunque; - bloccare tutte le porte di comunicazione non utilizzate sul firewall di rete e su quelli degli host server (se presenti).

Hardening del sistema	
Minaccia	- Negazione dei servizi (es. fault per buffer overflows). - Attacchi all'integrità dei sistemi (BIOS, software di base, configurazioni).
Contromisure	- Rendere certe pagine di memoria, come quelle contenenti stack e heap, non eseguibili. In generale, utilizzare un meccanismo di Data Execution Prevention (DEP) o l'opzione kernel ExecShield per limitare attacchi di iniezione di codice.

	- Utilizzare meccanismi di address space layout randomization (ASLR) o l'opzione del kernel per il Randomized Virtual Memory Region Placement, nelle modalità più restrittive supportata da ciascun sistema operativo.

Hardening del protocollo TCP/IP	
Minaccia	Negazione dei servizi (Denial of Service).
Contromisure	- Disabilitare l'IP forwarding al fine di impedire che il server in esame possa essere utilizzato come "testa di ponte" per attacchi verso ulteriori sistemi nella rete interna. - Disabilitare il source routing, inibendo la possibilità ad un utente malintenzionato di specificare le rotte da percorrere in fase di connessione verso un sistema. - Abilitare i log per i pacchetti di rete ricevuti aventi un indirizzo di origine non-routable (privo di una rotta in tabella di routing). Questa contromisura aiuta ad individuare attacchi basati sull'IP spoofing. - Abilitare i TCP SYN cookies per la gestione efficiente dell'handshake TCP SYN/ACK, in presenza di attacchi DOS specifici. - Disattivare la funzione di risposta alle richieste ICMP via broadcast. - Filtrare i pacchetti IP in modo che siano consentite solo le richieste ICMP provenienti da indirizzi IP appartenenti al piano d'indirizzamento aziendale. - Attivare la funzione di Quality of Service (QoS) e limitare, con valori idonei, l'ampiezza della banda di rete destinata al protocollo ICMP, ad esempio mediante tecniche di Committed Access Rate (CAR).

Hardening del sistema	
Minaccia	Accesso non autorizzato alle informazioni (es. da Memory dump attack).
Contromisure	Sui sistemi operativi server è necessario, se possibile tecnicamente e se consentito dalle regole del supporto tecnico dei fornitori, disabilitare la generazione dei dump di memoria di sistema ("core dump"). Laddove ciò non fosse possibile, è necessario configurare i sistemi in modo che i dump contengano la minor quantità possibile di informazioni sensibili. In ogni caso, i dump di memoria possono essere inviati ai fornitori solo in presenza di un accordo di riservatezza e con modalità di trasmissione atte a garantirne la riservatezza.

Hardening del sistema	
Minaccia	- Compromissione delle comunicazioni. (es. Cache poisoning) - Falsificazione di identità. - Furto di credenziali di autenticazione. - Negazione dei servizi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (da Malware).
Contromisure	- Assicurarsi di utilizzare versioni di software DNS più recenti ed installare tutte le patch di sicurezza disponibili; - Rimuovere dal server DNS qualsiasi altro servizio e software non necessari al suo funzionamento; - Proteggere i server DNS con un firewall perimetrale; - Configurare i server DNS in modo tale da fare il meno affidamento possibile nei rapporti di fiducia con altri server DNS; - Configurare il DNS server in modo tale da limitare query ricorsive, memorizzare solo i dati relativi a domini richiesti e limitare la risposta al fine di fornire

	informazioni inerenti al solo dominio richiesto. Assicurarsi che non ci siano servizi attivi sul DNS che non sono utilizzati; - Utilizzare DNSSEC; - Utilizzare ARP e tabelle IP statiche sul server DNS; - Utilizzare comunicazioni crittografate con SSH per accedere al server DNS.

Hardening del sistema	
Minaccia	- Perdita di riservatezza delle informazioni sulla rete e sui sistemi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (attacchi da Malware).
Contromisure	Configurare i sistemi operativi, in particolare quelli che ospitano il software di rete (ad esempio il firewall) o esposti sulla rete, per impedire il footprinting disabilitando i protocolli e le porte inutilizzate che possono rivelare informazioni sul sistema, sui servizi installati, sulle versioni utilizzate, sul posizionamento dei sistemi e sulla logistica degli uffici, ecc.

Hardening del sistema	
Minaccia	Negazione dei servizi.
Contromisure	- Configurare le applicazioni, i servizi e il sistema operativo tenendo sempre presente le possibili esposizioni ad attacchi DoS. - Ad es. è opportuno utilizzare estesamente architetture di tipo "stateless" o "RESTful" perché l'esaurimento delle risorse di sistema creando un numero elevato di false sessioni su sistemi che memorizzano lo stato di ciascuna di esse è una tecnica di attacco molto diffusa. - Assicurarsi che i criteri di blocco dell'account predisposti non possano essere sfruttati per bloccare service accounts ben noti (quindi il blocco di un account in caso di ripetuti tentativi di accesso deve essere temporaneo, e tra un tentativo e l'altro deve essere imposto un ritardo dell'ordine dei secondi). - Assicurarsi che il sistema sia in grado di gestire alti volumi di traffico e che le soglie massime per le risorse siano opportunamente impostate per gestire carichi anormalmente elevati. A tale scopo è necessario effettuare periodicamente il monitoraggio del carico sull'applicazione in condizioni realistiche per verificare il corretto dimensionamento del sistema in termini di risorse quali memoria RAM e CPU, numero di sessioni concorrenti gestite e tempi di connessione e di risposta effettivi in presenza di picchi di carico.

Hardening del sistema	
Minaccia	- Negazione dei servizi (es. fault per buffer overflows). - Attacchi all'integrità dei sistemi.
Contromisure	Disabilitare tutti i protocolli e i servizi legacy non sicuri, quali ad es. Telnet, FTP, r-commands, SNMP v1, ecc.

Hardening del sistema	
Minaccia	- Negazione dei servizi (es. fault per buffer overflows). - Attacchi all'integrità dei sistemi (software e configurazioni). - Cancellazione o furto di informazioni (accidentale o da attacchi come ad es. il ransomware, ecc.). - Uso non autorizzato di privilegi.
Contromisure	Assicurarsi che la variabile d'ambiente PATH (usata su UNIX e Windows per accedere

	alle utilità di sistema da una finestra di terminale interattivo), non contenga percorsi sospetti né percorsi scrivibili da chiunque, ma solo quelli standard previsti dallo specifico sistema operativo. In particolare il PATH non deve mai contenere il percorso "." che rappresenta la directory corrente. Su UNIX e Linux in particolare, l'utenza di root deve avere la variabile di ambiente PATH definita ad esempio come *PATH="/usr/bin:/usr/sbin:/sbin"*.

Disabilitazione delle interfacce di rete inutilizzate	
Minaccia	- Negazione dei servizi (es. fault per buffer overflows). - Attacchi all'integrità dei sistemi. - Accesso non autorizzato ai sistemi.
Contromisure	Disabilitare le interfacce wireless non necessarie al corretto funzionamento del server. Ciò include le interfacce WiFi, Bluetooth e di altri protocolli wireless, ivi compresi quelli proprietari usati da mouse e tastiere wireless, su sistemi server e su Workstation critiche. Per quanto riguarda tastiere e mouse wireless sulle postazioni desktop (non server) è preferibile usare dispositivi bluetooth che consentano di utilizzare l'autenticazione e la crittografia della comunicazione.

Anti-spam	
Minaccia	- Negazione dei servizi (es. fault per buffer overflows). - Abuso di risorse.
Contromisure	Sui sistemi Linux e UNIX in genere, i Mail Transfer Agents o MTA (ad es. Sendmail e Postfix) sono usati per ricevere email in entrata e trasferire I messaggi all'utente o al mail server di destinazione. Se il sistema non è un mail server o un SMTP relay, l'MTA deve essere configurato per processare solo le mail generate localmente al sistema (ad es. da applicative che generano un errore e inviano un messaggio a root per scopi di diagnostica).

Hardening del sistema	
Minaccia	- Accesso non autorizzato alle informazioni - Cold boot attack - Accesso non autorizzato ai sistemi
Contromisure	- Utilizzare meccanismi di crittografia dei dischi di sistema (es. BitLocker); - Assicurarsi che tutti i dischi crittografati siano smontati (protetti) quando il computer è in una posizione in cui può essere rubato. Tipicamente ciò non è possibile con il disco su cui il sistema operativo è in esecuzione; - Impiegare un meccanismo di autenticazione a due fattori per l'avvio del sistema, ad esempio un PIN di pre-avvio o un dispositivo USB rimovibile contenente una chiave di avvio; - Assicurarsi che il computer abbia completato la procedura di arresto prima di lasciarlo incustodito; - Sui sistemi UNIX inserire un controllo di autenticazione per accedere in single user mode e disabilitare il boot interattivo (che consente di presentare un prompt interattivo di amministratore senza autenticazione); - Quando è previsto che il Sistema Operativo passi in modalità di sospensione a seguito di un periodo di inutilizzo, configurarlo invece per l'arresto completo; - Applicare le patch per kernel Linux quali TRESOR e Loop-Amnesia che modificano il

	kernel del sistema operativo in modo tale da utilizzare i registri della CPU (nel caso TRESOR registri di debug x86 e, in caso di Loop-Amnesia, i registri di profilazione AMD64 o EMT64) per memorizzare le chiavi di crittografia, piuttosto che memorizzarle in RAM; - Seguire l'approccio denominato "frozen cache" conosciuto anche come "cache as RAM", con il quale si disattiva la cache L1 della CPU per poterla utilizzare come supporto di memorizzazione delle chiavi di crittografia. Ovviamente questo approccio è oneroso dal punto di vista delle performance, ma si può ovviare a ciò utilizzando CPU multicore in cui tale cache viene disattivata per un solo core; Impiegare hardware in cui i moduli di memoria RAM sono saldati o incollati nel socket della scheda madre.

Inibizione dei terminali non in uso	
Minaccia	Accesso non autorizzato ad informazioni, causato dal personale utente per inadeguati meccanismi, strumenti, procedure o abilità tecniche atti a prevenire l'accesso non autorizzato al sistema.
Contromisure	Tutti gli utenti devono essere sensibilizzati sui requisiti e sulle procedure di sicurezza per proteggere le apparecchiature incustodite. Le postazioni di lavoro e i sistemi informativi di qualsiasi tipo dotati di un terminale video e una tastiera, devono essere configurati in modo da bloccare la sessione di login e richiedere la password utente quando il sistema viene lasciato incustodito o inattivo per oltre 5 minuti. Ciò si applica specialmente ai sistemi server, anche se posizionati in data center o in zone ad accesso ristretto.

Limitazione del tempo di connessione	
Minaccia	- Accesso non autorizzato ad informazioni. - Abuso di privilegi.
Contromisure	Sui sistemi più critici, laddove sia prevista una durata massima per lo svolgimento di determinati compiti, o quando l'uso di tali sistemi sia consentito solamente in certi orari, alla scadenza temporale prevista deve essere effettuato un logout automatico.

Limitazione dell'uso delle utility/servizi di sistema	
Minaccia	- Accesso non autorizzato ad informazioni. - Abuso di privilegi. - Errori di amministrazione dei sistemi. - Uso non autorizzato di privilegi.
Contromisure	Limitare l'uso delle utility/servizi di sistema attraverso: - sistemi di identificazione e autenticazione per l'uso delle utility/servizi; - separazione delle utility di sistema dalle applicazioni; - autorizzazione all'uso delle utility/servizi solo per chi ne ha la reale necessità (compreso l'orologio di sistema); - tracciamento di ogni operazione privilegiata svolta con l'uso delle utility/servizi; - rimozione di tutte le utility/servizi non strettamente necessarie (in particolare i servizi di RAS o dial-up, gestione remota, ecc.); - disabilitazione di tutte le porte non necessarie; - rimozione di tutti gli strumenti di sviluppo (compilatori e interpreti) su sistemi destinati ad ambienti di test, collaudo, certificazione e produzione.

Presentazione di messaggi di avvertimento	
Minaccia	Accesso non autorizzato ad informazioni causato dal personale utente per inadeguati meccanismi, strumenti, procedure o abilità tecniche atti a prevenire l'accesso non autorizzato al sistema o a proteggere i dati di autenticazione quando memorizzati o trasmessi.
Contromisure	Includere nella schermata di log-on l'avvertimento che l'accesso è consentito ai soli utenti autorizzati. Richiamare nella schermata le norme interne o di legge che verrebbero violate in caso di accesso non autorizzato e le relative sanzioni. Informare chi si accinge ad accedere al sistema che le attività saranno monitorate e che ogni accesso non autorizzato ed ogni abuso saranno perseguiti a norma di legge.

Sincronizzazione degli orologi	
Minaccia	- Accesso non autorizzato al sistema (macchina, configurazione, ecc.). - Abuso di privilegi da parte degli utenti.
Contromisure	Sincronizzare l'orologio interno di tutti i sistemi e gli apparati di rete attraverso il protocollo NTP con un server "fidato" posizionato sulla propria intranet. Laddove tecnicamente possibile (sistemi UNIX e apparati di rete evoluti) abilitare l'autenticazione verso il server NTP. Laddove tecnicamente realizzabile, il server NTP deve a sua volta ottenere l'ora esatta attraverso un segnale radio proveniente da stazione terrestre o satellitare (GPS). Per le reti di piccole dimensioni, laddove non sia possibile avere un server NTP proprio, utilizzare comunque un server NTP "fidato" unico per tutti i sistemi, come ad es. quello dell'Istituto Nazionale di Ricerca Metrologica (INRIM) (ex Istituto Elettrotecnico Nazionale Galileo Ferraris).

5.2.3 Utenze

Accesso privilegiato nominativo	
Minaccia	- Abuso di privilegi da parte degli utenti. - Abuso di risorse. - Accesso non autorizzato alle informazioni. - Cancellazione dei log di accountability e/o ripudio di operazioni effettuate.
Contromisure	Disabilitare la possibilità di accesso ai sistemi (locale o remoto) utilizzando utenze amministrative impersonali come "root" o "Administrator". Gli amministratori devono accedere con utenze nominative abilitate ai rispettivi compiti (ad es. abilitate all'uso del comando "su" su Unix, o appartenenti al gruppo Administrators su Windows).

Valgono inoltre i principi generali già introdotti nel paragrafo [rif. 5.1.1].

5.2.4 Autenticazione

Ai principi generali introdotti nel paragrafo [rif. 5.1.2], si aggiungono le indicazioni, di cui di seguito:

Identificazione e autenticazione degli utenti a livello di sistema	
Minaccia	- Abuso di privilegi da parte dell'utente. - Accesso non autorizzato alle informazioni. - Falsificazione di identità.

	- Tentativi di frode. - Uso non autorizzato di privilegi.
Contromisure	Richiedere l'autenticazione per svolgere qualsiasi tipo di attività di rilievo (compreso lo shutdown del sistema). Utilizzare tecniche di identificazione e autenticazione a due fattori, ad es. basate su pin e token o su pin e impronta biometrica, non solo per l'accesso amministrativo a sistemi critici ed apparati di rete e di sicurezza, ma anche per l'accesso ad applicativi che trattano dati personali sensibili, dati di traffico telematico e telefonico, dati bancari.

5.2.5 Autorizzazione

Ai principi generali introdotti nel paragrafo [rif. 5.1.3], si aggiungono le indicazioni, di cui di seguito:

Gestione delle informazioni segrete di autenticazione degli utenti	
Minaccia	- Perdita di riservatezza delle informazioni. - Furto di credenziali di autenticazione. - Falsificazione di identità.
Contromisure	Per i file contenenti le password e altre informazioni riservate relative agli account utente, valgono le seguenti restrizioni: - Possono essere salvati solo su file system che supportano meccanismi di controllo accessi a livello di singolo utente. - Devono essere protetti con diritti di accesso il più possibile restrittivi. - Devono contenere le password in formato hashed (non invertibile) protetto con un codice ("salt") e non tramite crittografia reversibile. L'hash non deve essere basato su MD5, né SHA-1. Preferibilmente deve essere usato l'algoritmo SHA-2 512. Questa impostazione ad es. è possibile per il file delle password sui moderni sistemi operativi UNIX-like e Linux.

Autorizzazioni basate sui ruoli	
Minaccia	Perdita di riservatezza delle informazioni
Contromisure	Per le informazioni di autorizzazione valgono le seguenti regole: - Utilizzare meccanismi autorizzazione di sistema e applicativa basata sui ruoli per garantire che solo gli utenti con il livello appropriato di autorizzazione siano autorizzati ad accedere a dati sensibili e che tali autorizzazioni discendano da un ruolo organizzativo e non da una abilitazione "ad hoc" che è spesso sinonimo di eccezione non tracciata e non autorizzata formalmente. - Utilizzare la protezione basata sui ruoli con il massimo livello possibile di granularità, per distinguere tra utenti che possono creare, visualizzare, aggiornare e cancellare dati, distinguendo anche tra le diverse tipologie di dati e di funzionalità applicative. - A livello di sistema, utilizzare ruoli distinti per diversi compiti amministrativi come il backup, l'esecuzione di applicativi, l'avvio di specifici servizi di rete, la configurazione dell'audit e la visualizzazione dei log, ecc.

5.2.6 Crittografia

Valgono i principi generali introdotti nel paragrafo [rif. 5.1.4].

5.2.7 Documentazione

Valgono i principi generali introdotti nel paragrafo [rif. 5.1.5].

5.2.8 Logging

Valgono i principi generali introdotti nel paragrafo [rif.5.1.6].

5.2.9 Antivirus

Prevenzione e individuazione di codice malevolo sul sistema operativo	
Minaccia	- Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione, causata da Malware. - Negazione dei servizi causata da Malware. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Su sistemi sia client sia server è necessario installare un software antivirus e antimalware di riconosciuta efficacia, in grado di rilevare e rimuovere keylogger, spyware, trojans, worms, ransomware ed ogni altro tipo di malware conosciuto. I sistemi devono essere configurati in modo che l'antivirus/antimalware: - sia eseguito in modo automatico all'avvio della macchina senza possibilità di disattivazione da parte di utenti non autorizzati; - esegua in automatico l'aggiornamento della lista di definizione dei virus (DAT) anche più volte al giorno mediante un'infrastruttura di sistemi dedicati alla distribuzione del DAT; - esegua una scansione approfondita del disco fisso almeno una volta alla settimana, in orari che riducano l'impatto sulle attività lavorative (ad es. durante la pausa pranzo); - esegua una scansione anche dei file compressi fino a 3 livelli di nidificazione; - preveda una gestione remota per la segnalazione di infezioni virali; - abbia funzionalità di tipo euristico per la rilevazione dei virus che consenta di inserire in "quarantena" tutti i file ritenuti sospetti dal motore euristico; - si integri nel sistema operativo al livello di file system e nel software di gestione della posta; - notifichi, durante la fase di shutdown, se è presente un dispositivo removibile. L'amministratore di sistema deve verificare (e se necessario effettuare manualmente) l'effettivo aggiornamento dei sistemi anti-virus con cadenza almeno mensile.

5.2.10 Procedure

Alle linee guida 'Procedure generali' (Change management, Maintenance, Patching, Secure testing, Disposal) introdotti nel paragrafo [rif. 5.1.7], si aggiungono, per l'ambito specifico, le indicazioni di cui di seguito:

Controlli sulla regolamentazione dell'uso del codice mobile per Sistemi Operativi	
Minaccia	- Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione, causata da Malware. - Negazione dei servizi causata da Malware. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Nel caso in cui si utilizzi "mobile code" (ad es. JavaScript / VBScript scaricati da siti web, Java applets, controlli ActiveX, codice Adobe Flash o Shockwave, documenti PDF attivi

	o anche semplici macro VBA trasferite attraverso documenti Microsoft Office), è necessario controllare che il "mobile code" non effettui operazioni non autorizzate. In particolare è necessario predisporre il maggior numero possibile di controlli tra quelli di seguito elencati: - esecuzione del mobile code in un ambiente di test isolato logicamente (sistemi di malware analysis in grado di analizzare il mobile code); - blocco di ogni utilizzo di mobile code sulle postazioni di lavoro e sui server; - blocco della ricezione di mobile code da internet (operato dai firewall perimetrali); - attivazione delle misure tecniche disponibili sul browser in uso per bloccare o quanto meno mettere in sicurezza l'utilizzo del mobile code, ad es. impedendo che il mobile code possa eseguire qualsiasi operazione sul sistema operativo, o all'esterno di una "sandbox" predisposta dal browser; - limitazione delle risorse di sistema che possono essere utilizzate dal mobile code; - attivazione di controlli crittografici per autenticare il mobile code (firma digitale del codice).

Controlli dell'installazione di software sui sistemi in funzione	
Minaccia	- Negazione dei servizi. - Attacchi all'integrità dei sistemi (software e configurazioni).
Contromisure	Devono essere in vigore procedure per controllare l'installazione ed i cambiamenti del software sui sistemi di produzione. L'installazione deve essere effettuata seguendo scrupolosamente le indicazioni scritte fornite dal produttore e rispettando l'ordine delle operazioni da compiere. Nelle procedure devono essere indicate le istruzioni per i controlli che possono variare in relazione alla tipologia di ambiente/sistema operativo.

Autorizzazione per trasferimento di informazioni, strumenti elettronici e supporti all'esterno	
Minaccia	- Accesso non autorizzato alle informazioni. - Divulgazione di informazioni riservate. - Uso non autorizzato di privilegi. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Il trasferimento all'esterno del sito aziendale o dell'organizzazione di informazioni contenute su strumenti o supporti elettronici, oppure in altre tipologie di supporti (es. atti e documenti cartacei) deve avvenire mediante preventiva autorizzazione dei soggetti responsabili. Per il trasferimento di archivi contenenti dati personali presso fornitori esterni operanti nell'Unione Europea, è necessaria l'autorizzazione del Titolare e può richiedere l'aggiornamento dell'informativa agli utenti laddove necessario. Il fornitore esterno deve essere formalmente nominato responsabile del trattamento. Il trasferimento di tali archivi all'esterno dell'Unione Europea deve essere impedito.

Security awareness: come combattere il phishing/pharming	
Minaccia	- Divulgazione di informazioni riservate. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Sensibilizzare il personale sui rischi del phishing/pharming (divulgazione non autorizzata a terzi di informazioni riservate o critiche, perdita delle informazioni ad es. da ransomware, ecc.). Istruire il personale sulle norme di comportamento cui attenersi per diminuire i rischi di phishing/pharming. Tali norme dovrebbero, almeno, indicare di: - non fare affidamento sull'intuito per distinguere tra richieste legittime e illegali di

	informazioni riservate, ma piuttosto di tentare di comprendere appieno ogni richiesta ricevuta prima di effettuare qualsiasi scelta; - non consegnare mai informazioni personali o riservate a individui o aziende sconosciuti; - eliminare messaggi e-mail che richiedono informazioni riservate o l'. Se la richiesta appare legittima, verificatene telefonicamente l'autenticità; - non disabilitare le protezioni aziendali antivirus, anti-phishing/pharming o altre misure di sicurezza (ad esempio quelle del browser); - contattare l'assistenza IT nel caso di comunicazioni ricevute per e-mail, telefono, fax o messaggistica immediata, che richiedono informazioni aziendali o personali.

Security awareness: prevenzione infezioni da malware	
Minaccia	- Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione. - Violazione di leggi, di regolamenti, di obblighi contrattuali. - Compromissione delle comunicazioni. - Furto di credenziali di autenticazione (es. keylogger).
Contromisure	Verificare il contenuto della clipboard prima di incollarlo su un terminale o sulla barra degli indirizzi del browser web o all'interno di un messaggio di posta elettronica; Scaricare e installare software solo da siti web riconosciuti e certificati; Non aprire file o archivi sospetti; Su Windows non aprire file eseguibili (EXE) privi di firma digitale, né file CMD, BAT, REG. Su sistemi Windows o anche UNIX (dotati di interfaccia grafica tipo KDE o GNOME), non aprire mai i file con un doppio click in base all'icona visualizzata: visualizzare e controllare sempre l'estensione del file, perché un eseguibile contenente un malware può celarsi dietro l'icona falsificata di un file PDF o altro; Indipendentemente dalla piattaforma in uso, Linux o Windows, controllare i file di installazione software attraverso l'uso di programmi capaci di rilevare la presenza di malware.

5.2.11 Sicurezza di macOS

La sicurezza del sistema operativo macOS è importante, ma spesso trascurata. Mantenere la privacy e proteggere i dati è estremamente importante per ogni utente del sistema. Eppure, molte volte si dedica poca attenzione a tali aspetti e si fa poco più del minimo indispensabile, se non altro per garantire che gli hacker, e terze parti, siano in grado di accedere il meno possibile ai dati personali presenti nel sistema. Tuttavia, macOS rende la sicurezza dei dati molto semplice, grazie a una serie di strumenti disponibili nelle "Preferenze di sistema" e in Safari, nonchè in diverse applicazioni distribuite da terze parti. Apple solitamente reagisce in modo rapido quando emergono nuovi malware per il sistema, e dispone di diverse misure messe in atto al fine di proteggere il proprio software dalle minacce conosciute. Tuttavia, è possibile in taluni casi che compaiano dei malware non riconosciuti e pertanto potrebbe essere necessario apportare le opportune modifiche al modo in cui si utilizza il sistema, in attesa che si renda disponibile la necessaria protezione. Esistono tre fonti distinte da cui è possibile che provengano delle minacce: via Internet, via e-mail o da qualcuno che ha accesso diretto alla postazione di lavoro. In linea generale, adottando le opportune misure di protezione verranno ridotti al minimo i rischi.

Segue un elenco di best practices generali per la sicurezza di questo sistema:

- Impostazioni di sicurezza e privacy. Partendo dalle impostazioni di base del Mac che dovrebbero essere controllate al fine di garantire la adeguata sicurezza, verificare le impostazioni presenti nella finestra di "Sicurezza e privacy" disponibile nelle "Preferenze" di sistema. Ivi sono presenti quattro

schede (Generale, FileVault, Firewall e Privacy) che controllano i vari aspetti della sicurezza del sistema. In primo luogo abilitare il firewall, che blocca qualsiasi connessione di rete in entrata indesiderata. Si potrebbe pensare che il firewall sia abilitato per impostazione predefinita, ma spesso non lo è. È importante notare che il Firewall di macOS, sebbene utile, offre solo una protezione limitata dal malware. Questo perché protegge il sistema solo dal traffico in entrata. Il suo compito è quello di limitare le applicazioni e servizi nell'accettazione delle connessioni in entrata. Non fornisce alcun controllo sulle connessioni in uscita, vale a dire le applicazioni e i servizi che istaurano una connessione. Così, ad esempio, se si scarica del malware, il firewall di macOS non interromperà la connessione a Internet. A volte si sceglie di bloccare anche le connessioni di rete in uscita in modo che alcune applicazioni non possano "comunicare indebitamente con l'esterno". Ciò significa anche che un eventuale malware installato accidentalmente non è in grado di sottrarre impropriamente dati senza venirne a conoscenza.

- Utilizzo di una password. Nella sezione Generale della finestra "Sicurezza e Privacy", sono presenti tre impostazioni a cui si dovrebbe prestare particolare attenzione: La prima è quella che ci consente di impostare una password per l'account in uso, se non lo si abbia già fatto, o di cambiarla se lo si ritiene necessario. La seconda ci permette di specificare se è necessaria una password per sbloccare la postazione Mac, quando questa va in standby o quando parte uno screen saver. È possibile scegliere di richiederla immediatamente, o dopo un certo tempo prestabilito di inattività successivo all'avvio o un certo numero di screen saver. Se si lavora in un ufficio con altre persone, è opportuno considerare la possibilità di attivare tale impostazione. Esiste anche un'opzione per disattivare il login automatico, cosa che si dovrebbe fare. Si può anche scegliere di consentire ad un dispositivo "Apple Watch" di sbloccare la postazione Mac. Con questa opzione abilitata tutto ciò che è necessario fare è indossare l'Apple Watch. In tal caso la postazione Mac si sblocca automaticamente quando ci si trova nelle vicinanze. (Non è possibile utilizzare questa impostazione se la Condivisione Internet è attiva). Parlando di password, dobbiamo ricordare che una buona password dovrebbe essere difficile da ricordare. Inoltre, queste non devono essere assolutamente scritte. Fortunatamente, Apple fornisce "iCloud Keychain" come modo per ricordare le password e suggerirne di nuove da utilizzare tramite il generatore di password casuale incorporato. Con "iCloud Keychain" attivo è sufficiente effettuare il login con l'Apple ID per inserire automaticamente la password richiesta per accedere a qualsiasi servizio o sito web. L' "iCloud Keychain" può memorizzare tutti i dati dell'account, numeri di carta di credito e altre informazioni personali (comprese le impostazioni per le e-mail, contatti, calendari e servizi di social network) rendendoli automaticamente disponibili in caso di necessità di accesso attraverso una qualsiasi postazione Mac o dispositivo iOS.
- Impostazioni di download delle App. Nella parte inferiore della scheda "Generale" della finestra "Sicurezza e Privacy" sono presenti due opzioni che definiscono le modalità di download ed esecuzione delle applicazioni sulla postazione Mac. L'opzione più sicura, ma più limitativa, è quella di consentire l'esecuzione solo alle app scaricate dell'App Store. L'altra opzione è comunque un buon compromesso, in quanto consente di eseguire applicazioni scaricate dall'App Store e da fonti di sviluppo note ad Apple. Nelle vecchie versioni di MacOS esisteva un'opzione per consentire l'esecuzione di applicazioni provenienti da qualsiasi fonte. Se si dispone di tale opzione è fortemente sconsigliato usarla. Sarà comunque possibile eseguire un'applicazione che non provenga dall'App Store o da una fonte di sviluppo riconosciuta, ma sarà necessario fornire l'approvazione prima che questa possa essere eseguita.
- Abilitazione del FileVault. Con FileVault attivo, tutti i file dell'account utente verrano criptati. Per poterli decriptare, è necessario digitare la password dell'account o la chiave di recupero creata all'atto dell'attivazione di FileVault. Per la maggior parte degli utenti, l'inconveniente di dover digitare una password per aprire un file, insieme al tempo inizialmente necessario per crittografare tutti i file presenti sulla postazione Mac, supera i vantaggi della sicurezza. Nonostante ciò, se si intende mantenere il più possibile sicuri i dati memorizzati sulla postazione, è consigliabile attivare tale funzionalità.

- Impostazioni relative alla privacy. La scheda "Privacy" presente nella finestra di "Sicurezza e Privacy", copre una serie di diversi controlli e impostazioni. Questi sono: "Servizi di localizzazione" che consente di controllare quali applicazioni hanno accesso ai dati di localizzazione. È possibile disattivare completamente i Servizi di localizzazione o impedire alle singole applicazioni di accedere a tali dati. Allo stesso modo, "Contatti", "Calendario" e "Promemoria" consentono di specificare quali app installate sulla postazione Mac possono accedere alle informazioni memorizzate dalle relative app di default dell'OS X. Inoltre è presente la sezione "Accessibilità". In questa sezione è possibile impostare quali applicazioni in qualche modo possono controllare la postazione Mac. Ad esempio, Deeper e Onyx consentono di modificare le impostazioni di sistema che normalmente richiederebbero gli opportuni comandi da terminale. Infine, l'opzione "Analytics" è stata aggiunta in macOS “High Sierra”, la quale consente agli sviluppatori di Apple e alle app in generale di migliorare i propri prodotti sulla base delle informazioni raccolte riguardo l'utilizzo delle app stesse. In tal senso, è possibile scegliere di non condividere tali informazioni.
- Verifica delle impostazioni di privacy in Safari. A differenza delle "Preferenze di Sistema", Safari dispone di diverse impostazioni che permettono di controllare gli aspetti di privacy. La prima è la finestra "Privacy", accessibile dal menu "File" (o Shift+comando+N), che consente di visitare siti web, senza che questi vengano registrati nel menu "Cronologia" o in qualsiasi altro punto del sistema. La seconda è "Clear History", accessibile dal menu "Safari", che cliccata periodicamente, cancella i cookie e altri dati memorizzati nella cache dei siti visitati rimuovendoli anche dal menu "Cronologia". Nelle "Preferenze di Safari", la sezione "Privacy" permette di evitare il tracciamento da parte dei siti web durante la navigazione in rete e di controllare quali siti possono memorizzare i cookie nel sistema. In passato era possibile specificare come i dati relativi alla posizione potevano essere resi disponibili tramite questa finestra, ma dalla versione “High Sierra”, tali impostazioni sono state trattate in una scheda separata, ovvero in "Siti web" > "Posizione". Qui è possibile scegliere di impostare Safari per negare come impostazione predefinita il rilascio di informazioni sulla posizione o consentire a siti web specifici di accedere alla posizione della postazione di lavoro. Relativamente alle impostazioni di archiviazione delle credenziali di accesso per un sito web, o dei dati personali, nelle sezioni "Riempimento automatico e Password" togliere la spunta sulle caselle che abilitano tali servizi.
- Verifica di ciò che viene condiviso. Il sistema operativo Mac è in grado di condividere file con altri sistemi Mac e può condividere dati in diversi altri modi, inclusa la condivisione dell'intero schermo per facilitare l'attività lavorativa da remoto. Ad esempio, per poter utilizzare la condivisione dello schermo, è necessaria una password, e questo potrebbe portare a considerare sicuro il servizio, ma esiste comunque la possibilità in cui la presenza di una difettosità nel servizio di condivisione potrebbe renderlo vulnerabile da un punto di vista della sicurezza. In generale, è buona pratica disattivare qualsiasi servizio di condivisione che non viene utilizzato. Nello specifico:
    - Condivisione dello schermo - Utilizzato principalmente in ambienti aziendali per consentire agli addetti all'assistenza tecnica di vedere o controllare lo schermo di una macchina remota, e di eseguire correzioni e/o aggiornamenti. Anche le macchine Windows e Linux, attraverso l’uso del servizio VNC, possono controllare lo schermo di un computer Mac. In tal caso assicurarsi che questo venga disattivato.
    - Condivisione di file – questo servizio consente ad altri computer in rete di accedere al file system del computer Mac. Tecnicamente parlando, abilita la condivisione del file system di Windows (SMB), Apple Filing Protocol (AFP) e Network File Service (NFS). Il sistema di file sharing del Mac veniva utilizzato nel passato dal servizio “Back To My Mac”, integrato in iCloud, ma Apple lo rimosse con l’uscita della versione di sistema “Mojave”. “Back To My Mac” consentiva di accedere da un sistema Mac, via Internet (anche se non ha assolutamente nulla a che fare con iCloud Drive, che svolge una funzione simile), ai file di un altro sistema Mac. Se non si ha la necessità di condividere file in rete e non si utilizza la feature “Back To My Mac”, allora questo servizio dovrebbe essere disattivato.

  - Condivisione delle stampanti – il servizio consente di condividere qualsiasi stampante collegata al sistema Mac, con altri computer presenti sulla rete. Se non si hanno stampanti collegate alla postazione Mac o non si ha la necessità di condividere alcuna stampante, questo servizio dovrebbe essere disattivato.
  - Condivisione della connessione Internet – il servizio consente a un sistema Mac di condividere una connessione di rete con altri Mac. Questo servizio fu concepito ai tempi delle connessione Internet in dial-up. È improbabile che al giorno d'oggi possa essere utilizzata una connessione di questo tipo, visto che oramai si dispone di banda larga e router Wi-Fi. Pertanto questo servizio dovrebbe essere disattivato.
  - Condivisione tramite Bluetooth – il servizio consente a un sistema Mac di inviare e ricevere file da e verso un altro dispositivo abilitato Bluetooth, come un telefono cellulare. L'iPhone e l'iPad non possono condividere file in questo modo, quindi è probabile che lo si possa utilizzare solo con un dispositivo Android. A meno di specifiche esigenze, questo servizio dovrebbe essere disattivato.
- Login remoto. Questo servizio abilita le connessioni al sistema Mac via SSH/SFTP, che per lo più viene utilizzato dai tecnici per operare tramite "command shell" da remoto. A meno di specifiche esigenze, questo servizio dovrebbe essere disattivato.
- Gestione remota. Questo servizio viene solitamente utilizzato in un ambiente aziendale per consentire agli amministratori di accedere al sistema Mac da remoto per poter eseguire le necessarie operazioni di manutenzione del sistema. Nei casi in cui non esiste tale necessità, questo servizio dovrebbe essere spento.
- Eventi remoti Apple. Questo servizio consente ad un sistema Mac di controllarne un altro per stampare, o fare qualsiasi altra cosa, difatti, grazie all'integrazione con AppleScript, è possibile utilizzare gli eventi remoti Apple per far eseguire comandi su un sistema Mac controllati da un altro sistema Mac attraverso sintesi vocale. Utilizzando questo servizio, un programma AppleScript in esecuzione su un sistema Mac può interagire con un altro Mac. Ad esempio, il programma potrebbe aprire e stampare un documento che si trova sul sistema remoto. Normalmente questo servizio dovrebbe essere spento a meno di particolari necessità.
- Applicare una password per l'accesso al firmware. Il sistema Mac è predisposto per utilizzare di default la crittografia di FileVault, il che significa che l'intero disco di avvio viene crittografato ed è impossibile accedervi a meno che non venga sbloccato al login utilizzando la password dell'utente. Tuttavia, ciò non impedisce a chiunque di poter utilizzare una chiavetta di memoria USB per avviare la postazione e potenzialmente cancellare tutti i dati presenti nel disco rigido, o semplicemente reinstallare il sistema operativo. La soluzione è quella di applicare una password per l'accesso al firmware. A differenza della cosiddetta password del BIOS di un PC, la richiesta della password del firmware del sistema Mac appare solo nel momento in cui si tenta di avviare il Mac in modo non standard, vale a dire, tramite una chiavetta USB, o se si tenta di avviare il Mac in Recovery Console. Per attivare la password del firmware è necessario farlo dalla Recovery Console. Da tener presente che, se si dimentica tale password, solo Apple è in grado di sbloccare la postazione.
- Abilitazione dell'utente "guest". L'account "Guest" è essenziale per l'utilizzo del servizio "Trova il Mio Mac", presente in iCloud e che permette di rintracciare un computer Mac smarrito o rubato. Pertanto, non disattivare l'account Guest se è abilitata l'opzione "Trova il Mio Mac" in iCloud.
- Disabilitare il "Security Hole" in FileVault. Quando il sistema Mac entra in modalità sleep (per esempio se si chiude il coperchio di un MacBook Pro), esiste un potenziale problema di sicurezza dovuto al fatto che la chiave necessaria per decriptare con FileVault viene mantenuta in memoria. Anche se molto difficile, in teoria qualcuno potrebbe riattivare il computer e in qualche modo recuperare questa chiave, e quindi avere accesso all'intero contenuto del disco senza la necessità di una password di login. Tuttavia, è possibile impedire che la chiave FileVault venga mantenuta in memoria, anche se questo comporterà a volte la richiesta di digitare due volte la password di accesso alla riattivazione della postazione Mac, e un rallentamento in fase di riattivazione dalla modalità sleep.

- Verificare la presenza di applicazioni persistenti. Alcune applicazioni per il sistema Mac sono progettate per essere esguite in modo silente ad ogni avvio rimanendo invisibili durante l'utilizzo del computer. Queste vengono chiamate applicazioni persistenti, come ad esempio le app di controllo degli aggiornamenti che Google e Microsoft installano per garantire che Google Chrome e Microsoft Office siano sempre aggiornati. Anche Adobe installa alcune applicazioni persistenti come parte del pacchetto "Creative Cloud". Tuttavia, questa tipologia di applicazioni può contenere del malware, e a peggiorare le cose, esistono diverse posizioni all'interno del file system in cui il malware stesso può nascondersi con il fine di essere eseguito in modo del tutto invisibile ad ogni avvio. Riguardo tale problema, esistono due applicazioni gratuite che possono essere utilizzate come supporto per contrastare questo tipo di minaccia. La prima è KnockKnock la quale analizza queste posizioni sul file system, dando evidenza di cosa è presente. Non è uno scanner di malware, quindi non fornisce alcuna indicazione in merito alla pericolosità di ciò che viene rilevato. La seconda applicazione si chiama BlockBlock. Questa viene eseguita in background nel sistema Mac e verifica tutte le posizioni in cui vengono installate le applicazioni persistenti. Se un'applicazione tenta di installare qualsiasi cosa in modo persistente, viene mostrata una finestra di dialogo con una richiesta di conferma per poter procedere. Anche in questo caso, BlockBlock non è uno strumento anti-malware, quindi non è in grado di riconoscere cosa è legittimo è cosa non lo è. Queste applicazioni non risolvono definitivamente il problema, ma impiegate come mezzi di protezione dal malware risultano essere piuttosto efficaci.
- Eseguire le scansioni malware. Poiché OS X/macOS dispone già di un potente strumento anti-malware chiamato Xprotect, il quale è sempre in funzione, non è necessario eseguire alcuna azione in tal senso.
- Abilitare ovunque l'autenticazione a due fattori. L'autenticazione in due fasi è un sistema in cui l'accesso a servizi o siti web richiede più di un semplice nome utente e password. Questa richiede un codice numerico aggiuntivo. Tale codice viene inviato come messaggio di testo o viene generato da una particolare applicazione in esecuzione su un dispositivo mobile (esistono numerose applicazioni di questo tipo, ma per l'iPhone si consiglia Authy). La verifica in due fasi dell'identità viene a volte indicata con il suo nome più tecnico di autenticazione a due fattori, o TFA (two-factor authentication). Questa feature dovrebbe essere abilitata per tutti i siti e servizi a cui si accede. Ad esempio, se si utilizza un qualsiasi servizio di Google come ad esempio Gmail, è possibile abilitare il TFA per accedervi. E' possibile abilitare tale feature anche per i servizi e i siti Microsoft e Dropbox. Ovviamente, non tutti i siti o servizi supportano il TFA. Esistono alcuni siti come "https://twofactorauth.org" i quali forniscono un elenco continuamente aggiornato di quei siti/servizi che supportano tale feature. L'impostazione del TFA è piuttosto semplice. Alcuni siti e servizi inviano un codice all'atto della connessione, che poi deve essere fornito quando richiesto dal servizio stesso, a tal fine è necessario impostare in fase di configurazione del servizio, il numero del dispositivo mobile autorizzato. Per quei servizi o siti che utilizzano un'applicazione come sistema di verifica, come il suddetto Authy, quando si sceglie di configurare il TFA, è necessario utilizzare l'applicazione installata sul cellulare o tablet, quindi scegliere nel servizio di aggiungere un codice e puntare semplicemente la fotocamera del dispositivo mobile verso il codice a barre o QR mostrato nella schermata del sito. Se il dispositivo mobile non è provvisto di fotocamera, è possibile digitare manualmente il codice di autenticazione, che solitamente viene mostrato sotto il codice a barre o QR. Successivamente all'accesso al servizio, terminata la configurazione del TFA, l'applicazione installata nel dispositivo mobile viene avviata richiedendo a sua volta la digitazione del codice visualizzato (solitamente dopo aver inserito la password di accesso all'applicazione stessa), oppure rimanendo in attesa della ricezione di un messaggio di testo/chiamata vocale, prevedendo successivamente la digitazione del codice ricevuto quando richiesto.
- Crittografare le ricerche sulle pagine web. Il Domain Name System, o DNS, converte gli indirizzi basati su nomi di dominio che un essere umano può leggere e ricordare, come ad esempio "www.nomedominio.it", in indirizzi internet numerici IP, maggiormente comprensibili da un computer, come ad esempio "192.161.1.1". Tutti i computer collegati a Internet interagiscono con i

server DNS. Questi vengono resi disponibili dall'Internet Service Provider come parte del pacchetto complessivo dei servizi di rete. Il problema è che, come la maggior parte delle risorse disponibili online, anche i servizi DNS non sono in alcun modo sicuri. In altre parole, tutte le richieste che viaggiano da e verso siti web e che transitano per un DNS possono essere spiate. L'applicazione e il progetto DNSCrypt risolve tale problema semplicemente crittografando le richieste DNS sia da che verso il server DNS. È possibile scaricare questa applicazione dalla home page del progetto e la configurazione, una volta installata, è piuttosto semplice. Con DNSCrypt in esecuzione le ricerche eseguite dalle pagine web divengono immediatamente più sicure.

- Utilizzare una VPN. Non dare mai per scontato che un sistema Mac sia al sicuro quando si utilizza una rete condivisa. Sfortunatamente, è estremamente facile per un malintenzionato spiare i dati trasmessi da e verso i siti web. E' buona pratica utilizzare un servizio di rete privata virtuale (VPN). Questo ha la capacità di cifrare i dati di una comunicazione e di indirizzarli verso un end-point gestito dal servizio VPN. Azioni come la navigazione e il download non hanno alcun effetto sull'utente finale, ma chiunque si trovi sulla stessa rete fisica - come ad esempio un altro computer connesso sulla stessa rete Wi-Fi - viene completamente bloccato per contrastare qualsiasi forma di sniffing sui dati trasmessi o ricevuti dal sistema Mac. In genere, i servizi VPN sono dotati di un'applicazione che viene eseguita quando si desidera utilizzare la connessione VPN, anche se OS X/macOS è dotato di uno strumento VPN built-in che è possibile utilizzare.
- Utilizzare ovunque l'HTTPS. Per ragioni storiche, la maggior parte dei dati viene trasmessa sul web in forma semplice e ciò significa che chiunque li può intercettare durante il transito. Fanno eccezione le connessioni sicure come quelle adottate dalle banche, dai servizi di webmail e dai siti di shopping online. Questi normalmente utilizzano l'HTTP sicuro, e si riconoscono dal fatto che l'indirizzo del sito web inizia con "https://". Se si utilizza un browser che non è Safari - come Chrome o Firefox - installando l'estensione "HTTPS Everywhere" e possibile navigare utilizzando automaticamente l'HTTPS. Questo software è in grado di consultare un database di siti che sono opzionalmente disponibili in HTTPS cambiando automaticamente il protocollo di accesso da HTTP a HTTPS (se disponibile) in fase di accesso. Purtroppo, a causa della modalità di funzionamento di Safari, non è possibile implementare una vera estensione "HTTPS Everywhere" da utilizzare con tale browser e capace di garantirne la massima sicurezza. Tuttavia, l'estensione "SSL Everywhere" disponibile per il browser Apple, consente di ottenere risultati molto simili a "HTTPS Everywhere". L'unica differenza sta nel fatto che quando si accede a un sito web la trasmissione iniziale dei dati non viene crittografata, il che può fornire agli hacker o agli snoop interessati qualche informazione ad essi utile. Tuttavia, una volta che si è passati all'HTTP sicuro - cosa che in sostanza avviene immediatamente dal punto di vista dell'utente finale - tutti i dati vengono ovviamente criptati.
- Verificare i certificati digitali. Se viene mostrato un lucchetto accanto all'indirizzo web presente nella barra degli indirizzi di Safari, è possibile cliccare su di esso per visualizzare le informazioni sul Certificato digitale in uso. In Safari 11, introdotto nel 2017, Apple ha apportato dei miglioramenti nell'interfaccia utente relativamente alla visualizzazione di tali informazioni. Utilizzando l'ultima versione di Safari si dispone di un meccanismo potenziato di "Warnings" riguardo i certificati digitali in uso. Tali "Warnings" indicano chiaramente se una connessione non è privata. Si consiglia pertanto di usare l'ultima versione disponibile di Safari.

Alle linee guida generali, riportate nei paragrafi precedenti e valide per tutti i sistemi operativi, si aggiungono, per l'ambito specifico dei sistemi Mac OS X (con un focus per la versione 10.12), le indicazioni seguenti:

Controlli utente	
Minaccia	- Accesso non autorizzato al sistema. - Accesso non autorizzato alle informazioni. - Uso non autorizzato di privilegi.
Contromisure	È necessario assicurare che siano impostati i seguenti controlli sulle utenze:

	- L'utente root deve essere disabilitato (default). - L'accesso all'utente Guest deve essere disabilitato. - Il login automatico al desktop deve essere disabilitato. - La schermata di login deve essere configurata per richiedere l'inserimento manuale di nome utente e password (anziché visualizzare le immagini relative agli utenti presenti sul sistema). - La visualizzazione dei "suggerimenti" per la password deve essere disabilitata. - L'accesso dell'utente Guest alle cartelle condivise degli altri utenti deve essere disabilitata. - Bloccare lo schermo dopo 15 minuti di inattività e richiedere la password per sbloccarlo. - Richiedere la password quando il Mac si riattiva da una sospensione.

Servizi di condivisione file obsoleti	
Minaccia	- Accesso non autorizzato alle informazioni. - Furto di credenziali di autenticazione.
Contromisure	È necessario disabilitare, sui computer Mac, i servizi legacy FTP e NFS che consentono di accedere ai file e alle cartelle del Mac da remoto con protocolli obsoleti e altamente insicuri. In particolare si ricorda che il protocollo FTP richiede l'invio delle credenziali di autenticazione in chiaro sulla rete.

Funzionalità di condivisione	
Minaccia	- Accesso non autorizzato ai sistemi. - Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi (software e configurazioni). - Negazione dei servizi. - Furto di credenziali di autenticazione.
Contromisure	Mac OS X dispone di numerose funzionalità di condivisione che devono essere disattivate se non effettivamente necessarie. In particolare è necessario disattivare: - "Apple Events" Remoti, per impedire a programmi in esecuzione su Mac remoti di eseguire programmi sul sistema locale. - Condivisione Internet (Internet Sharing), per ridurre la superficie d'attacco del sistema. - Condivisione dello schermo (Screen Sharing), per prevenire il rischio di connessioni remote in grado di visualizzare le operazioni svolte dall'operatore sul sistema locale, a sua insaputa. - Login remoto (Remote Login), per impedire l'accesso remoto al sistema attraverso una sessione terminale all'insaputa dell'utente del sistema locale. In questo caso si disabilita il server SSH, ovviamente solo per i sistemi client dato che sui server, probabilmente, tale servizio risulterà necessario. - Condivisione Bluetooth (Bluetooth Sharing), per ridurre la superficie d'attacco del sistema. - Condivisione File (File Sharing), per disabilitare i servizi SMB (Samba) e AFP, in modo da impedire ogni tentativo di accesso remoto a cartelle e file del Mac. - Gestione Remota (Remote Management), per impedire ogni tentativo di accesso remoto al sistema attraverso il protocollo Apple Remote Desktop (ARD). Tale protocollo dovrebbe essere attivato solo se effettivamente in uso, in abbinamento con controlli di autenticazione basati su un Directory Server, e solo su una rete assolutamente "trusted".

Protocollo Bonjour	
Minaccia	- Accesso non autorizzato al sistema. - Negazione dei servizi.
Contromisure	Se non strettamente necessario (ad es. per un Mac che espone servizi di rete legittimamente), è necessario disabilitare il meccanismo di "advertising" del protocollo Bonjour. Il Bonjour è un protocollo di auto-discovery che consente di enumerare dispositivi e servizi TCP/IP in una rete locale. Un attaccante potrebbe utilizzare le funzionalità di multicast DNS di Bonjour per individuare la presenza di un servizio vulnerabile o non correttamente configurato, o per collezionare informazioni sui servizi esposti da un sistema target. Si noti che alcune applicazioni (come ad es. Final Cut Studio e AirPort Base Station management) potrebbero non funzionare se si disabilita Bonjour.

Estensioni dei nomi file	
Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (es. malware, ecc.).
Contromisure	Il Mac OS X non mostra di default l'estensione associata ai nomi dei file. In tal modo l'utente è portato a credere che il tipo file sia quello associato all'icona visualizzata sulla scrivania per quel file. Per evitare che un programma malevolo possa mascherare la sua vera natura attraverso l'icona contenuta nel file stesso, e per evitare errori, è necessario istruire Mac OS (nelle preferenze del Finder) affinché visualizzi sempre l'estensione associata al nome file (es. ".pdf", o ".doc").

Crittografia del disco di avvio	
Minaccia	- Accesso non autorizzato ai sistemi. - Accesso non autorizzato alle informazioni - Attacchi all'integrità dei sistemi (software e configurazioni). - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Per i computer Mac portatili che contengono informazioni riservate, oppure dati personali sensibili, è necessario proteggere il disco di avvio con il FileVault (impostazioni di Sicurezza & Privacy di sistema). Si tratta di un meccanismo di crittografia del disco di boot (analogo al bitlocker di Windows) che richiede all'avvio una password o una "recovery key". In tal modo in caso di smarrimento o furto del portatile, i dati resteranno protetti. Ovviamente la password e la recovery key NON devono essere trascritte (ad es. su un foglio custodito nella valigetta del Mac), né comunicate a terzi.

Crittografia dei volumi di backup e dei dischi esterni	
Minaccia	- Accesso non autorizzato alle informazioni. - Divulgazione di informazioni riservate. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Quando si utilizza Time Machine (o altri strumenti di terze parti) per creare volumi di back-up, è necessario abilitare sempre l'opzione che richiede la crittografia di tali

	volumi. Questo controllo va sempre applicato, ma è particolarmente importante nel caso di backup su dischi rimovibili dato che essi possono essere smarriti o rubati. Si pensi ad es. ad un Mac portatile con disco di avvio crittografato con FileVault. Se nella stessa borsa è presente un disco esterno con un volume di back-up Time Machine in chiaro, le informazioni riservate presenti nel Mac sono fortemente a rischio. Più in generale, i dischi esterni rimovibili contenenti informazioni riservate devono essere inizializzati con un file system HFS crittografato (usando lo strumento Disk Utility di Apple).

Controllo sull'origine degli applicativi	
Minaccia	- Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (es. malware, ecc.) - Cancellazione o furto di informazioni (accidentale o da attacchi come ad es. il ransomware, ecc.). - Attacchi all'integrità dei sistemi (software e configurazioni).
Contromisure	Per prevenire la possibile introduzione di malware sui Mac è necessario abilitare la funzionalità denominata Gatekeeper. Il Gatekeeper è un meccanismo di controllo di tipo white-listing che impedisce l'esecuzione di applicazioni scaricate, quando sono state rilasciate da fonti sconosciute o non autorizzate.

Host Firewall	
Minaccia	- Accesso non autorizzato ai sistemi. - Negazione dei servizi.
Contromisure	È necessario abilitare l'host firewall integrato nel Mac OS X (preferenze di sistema, sicurezza e privacy). Nelle opzioni del firewall, abilitare inoltre la modalità stealth, in modo da rendere il sistema meno riconoscibile e più difficilmente individuabile da parte di software di scansione di rete.

Sicurezza del terminale	
Minaccia	- Accesso non autorizzato alle informazioni. - Furto di credenziali di autenticazione.
Contromisure	Quando si utilizza l'utility di sistema "Terminale" del Mac, è necessario utilizzare sempre la modalità "Input da tastiera sicuro" (Secure Keyboard Entry), visibile nel menù "Terminale" dell'utility. Questo impedisce ad altre applicazioni sul sistema e in rete di leggere o registrare i caratteri digitati sul terminale.

"Safe Files" in Safari	
Minaccia	- Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (es. malware, ecc.) - Attacchi all'integrità dei sistemi (software e configurazioni). - Accesso non autorizzato ai sistemi - Cancellazione o furto di informazioni (accidentale o da attacchi come ad es. il ransomware, ecc.).
Contromisure	Un file, la cui tipologia è considerata sicura (Safe Files), viene automaticamente eseguito da SAFARI al termine del download.

	Questo comportamento deve essere necessariamente disabilitato, dato che tra i "Safe Files" ci sono immagini e file di installazione di applicazioni, oltre che video, immagini, file archivio e testo. Tali file vengono aperti nel contesto del sistema operativo anziché in un contesto isolato nel browser e dunque rappresentano gravi rischi per la sicurezza del sistema. La funzionalità è configurabile nelle preferenze generali di Safari.

Plug-ins di Safari	
Minaccia	- Accesso non autorizzato ai sistemi. - Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Cancellazione o furto di informazioni (accidentale o da attacchi come ad es. il ransomware, ecc.). - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (es. malware, ecc.).
Contromisure	A partire da Safari 10, è possibile abilitare o disabilitare i plug-in in base a uno specifico sito oltre che globalmente (come in passato). Per ovvi motivi di sicurezza, è necessario, quindi, con Safari versione 10 o successivo, disabilitare la configurazione che abilita globalmente i plug-in, optando invece per una configurazione in cui i plug-in sono globalmente disabilitati. All'accesso a un sito che richiede un certo plug-in, Safari chiederà all'utente se abilitare o no il plug-in per quel sito.

Java Virtual Machine	
Minaccia	- Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (es. malware, ecc.) - Attacchi all'integrità dei sistemi (software e configurazioni). - Accesso non autorizzato alle informazioni.
Contromisure	Apple, in passato, inseriva Java come parte del sistema operativo "core", ma sfortunatamente non fornisce più i relativi aggiornamenti rilasciati da Oracle. La versione più recente di Java, rilasciata da Apple, contiene peraltro numerosi difetti e vulnerabilità e pertanto non deve essere registrata come default runtime delle Applet Java. È necessario quindi disinstallare del tutto Java se non in uso, o altrimenti assicurarsi di aver installato la versione più recente fornita da Oracle.

5.2.12 Sicurezza di Linux

Il primo passo necessario per l'hardening di un server GNU/Linux è determinare la funzione che il server è chiamato a svolgere, e che stabilisce quali servizi necessariamente devono essere installati. Per esempio, se il server è usato come server web, si potrebbero installare i servizi Linux, Apache, MySQL e Perl/ PHP/ Python etc. Se invece il server viene utilizzato per i servizi di directory, le uniche applicazioni e servizi che dovrebbero essere disponibili e pertanto installati sono quelli necessari per il compito prestabilito. Non dovrebbe essere installato altro per due principali motivi:

1. L'installazione di software extra o l'esecuzione di servizi extra potenzialmente espone il sistema a inutili vulnerabilità. Ad esempio, se si installa e si usa un servizio Lightweight Directory Access Protocol (LDAP) su un server per servizi di directory, sia il sistema operativo che LDAP dovrebbero essere regolarmente aggiornati con le relative patch di sicurezza e bug fixing. Ciò sarebbe necessario anche se si installasse qualsiasi altro software, a prescindere dal fatto che questo venga usato o meno, e tale software dovrebbe essere sottoposto comunque a regolari aggiornamenti. La

semplice presenza sul server di software non necessario, fornisce ad un attaccante un'altra via d'accesso al sistema.

2. Installare software extra su un server significa che qualcuno potrebbe essere tentato di usare il server per qualcosa di diverso dall'uso previsto. L'utilizzo del server per compiti diversi da quello principale sottrae risorse al compito per cui è destinato e nel contempo lo espone a potenziali minacce.

In linea generale, le pratiche più comuni indicate nelle diverse linee guida di hardening dei sistemi GNU/Linux, includono:

- la cifratura dei dati nelle comunicazioni,
- l'esclusione di protocolli insicuri che trasportano informazioni o password in chiaro,
- la riduzione della presenza di software non necessario sul sistema,
- la disattivazione di file eseguibili/binari o directory indesiderati con permessi speciali come SUID e SGID,
- il mantenimento dello stato di aggiornamento del sistema operativo, con particolare riguardo alle patch di sicurezza,
- l'utilizzo di estensioni di sicurezza come valore aggiuntivo,
- l'adozione di SELinux come sistema di controllo accessi,
- l'uso di account con password molto robuste,
- il regolare cambiamento delle password e il non riutilizzo di password recenti,
- il blocco degli account che presentano numerosi errori di login,
- l'impossibilità di utilizzare password vuote,
- l'hardening del protocollo e dei servizi SSH,
- la disabilitazione dei servizi non necessari,
- il rafforzamento in termini di sicurezza dei percorsi /tmp, /var/tmp e /dev/shm,
- l'occultazione delle versioni del BIND DNS server e dell'Apache server,
- l'hardening del sysctl.conf,
- l'installazione di Root Kit Hunter e ChrootKit Hunter,
- la riduzione al minimo delle porte di rete aperte nel sistema,
- la configurazione del firewall di sistema,
- la separazione delle partizioni in modo da rendere il sistema maggiormente sicuro,
- la disattivazione di file binari indesiderati,
- la gestione dei log del sistema; con l'esecuzione del mirroring dei log su un server di log separato,
- l'installazione di Logwatch con una revisione giornaliera delle e-mail inviate da tale sistema,
- l'utilizzo di sistemi di rilevamento di attacchi di forza bruta e delle intrusioni,
- l'installazione di Linux Socket Monitor,
- l'installazione di Mod_security,
- l'hardening dell'installato Php,
- la limitazione per gli account ad accedere solo a ciò di cui questi hanno bisogno,
- l'adeguata gestione dei backup,
- la sicurezza fisica del server.

In informatica, solitamente il termine hardening identifica il processo di sicurezza atto a ridurre in un sistema la superficie vulnerabile. Il suo obiettivo principale è quello di ridurre il rischio per la sicurezza eliminando i potenziali vettori di attacco e riducendo la superficie di attacco del sistema stesso. A tale scopo, con un livello maggiore di dettaglio, si riportano alcune buone pratiche di hardening nell'ottica di sicurezza, specifiche dei sistemi GNU/Linux. Nel descrivere tali pratiche, ci si avvale di un indice di obbligatorietà implementativa o livello di priorità della specifica, che è necessario considerare al fine di garantire il giusto livello di sicurezza. Tale livello di priorità può assumere i seguenti valori in relazione alle relative specifiche:

- BASSO - indica che la specifica ha una priorità bassa,

- MEDIO - indica che la specifica ha una priorità media. Anche se non obbligatoria, è comunque opportuno prenderla in considerazione.
- ALTO - indica che la specifica ha una priorità alta e come tale è necessario seguire l'indicazione fornita nella specifica e implementare/apportare le modifiche consigliate.

PARTIZIONAMENTO	
Separazione delle partizioni	
Specifica	**Livello di priorità**
Garantire che "*/tmp*" e "*/var/tmp*" siano collocate su partizioni separate.	ALTO
Garantire che "*/var/log*" e "*/var/log/audit*" siano collocate su partizioni separate.	ALTO
Garantire che "*/var*" sia collocata su una partizione separata.	MEDIO
Garantire che "*/usr*" sia collocata su una partizione separata.	BASSO
Garantire che "*/home*" sia collocata su una partizione separata.	BASSO
Garantire che "*/boot*" sia collocata su una partizione separata.	BASSO
Uso delle opzioni di limitazione nei mount (/etc/fstab)	
Specifica	**Livello di priorità**
Limitare la partizione di mount "*/dev/shm*" nel seguente modo: *tmpfs /dev/shm tmpfs rw,nodev,nosuid,noexec,size=1024M,mode=1777 0 0*	MEDIO
Limitare la partizioni di mount "*/var*" e "*/var/tmp*" nel seguente modo: *mv /var/tmp /var/tmp.old* *ln -s /tmp /var/tmp* *cp -prf /var/tmp.old/* /tmp && rm -fr /var/tmp.old* *UUID=<...> /tmp ext4 defaults,nodev,nosuid,noexec 0 2*	MEDIO
Limitare la partizione di mount "*/home*" nel seguente modo: *UUID=<...> /home ext4 defaults,nodev,nosuid 0 2*	MEDIO
Limitare la partizione di mount "*/boot*" nel seguente modo: *LABEL=/boot /boot ext2 defaults,nodev,nosuid,noexec,ro 1 2*	MEDIO
Limitare la partizione di mount "*/proc*" nel seguente modo: *proc /proc proc defaults,hidepid=2 0 0*	BASSO
Limitare la partizioni di mount "*/var/log*" e "*/var/log/audit*" nel seguente modo: *UUID=<...> /var/log ext4 defaults,nosuid,noexec,nodev 0 2* *UUID=<...> /var/log/audit ext4 defaults,nosuid,noexec,nodev 0 2*	BASSO
Limitare la partizione di mount "*/var*" nel seguente modo: *UUID=<...> /var ext4 defaults,nosuid 0 2*	BASSO
Limitare la partizione di mount "*/usr*" nel seguente modo: *UUID=<...> /usr ext4 defaults,nodev,ro 0 2*	BASSO
Condivisione della memoria	
Specifica	**Livello di priorità**
Impostare il gruppo per "*/dev/shm*" come segue: *tmpfs /dev/shm tmpfs rw,nodev,nosuid,noexec,size=1024M,mode=1770,uid=root,gid=shm 0 0*	BASSO
Cifratura delle partizioni	
Specifica	**Livello di priorità**
Cifrare la partizione di "*swap*" come segue: *# Impostare in /etc/crypttab:* *sdb1_crypt /dev/sdb1 /dev/urandom cipher=aes-xts-plain64,size=256,swap,discard* *# Impostare in /etc/fstab:* */dev/mapper/sdb1_crypt none swap sw 0 0*	BASSO

ACCESSO FISICO	
Specifica di una password per il "Single User Mode"	
Specifica	**Livello di priorità**
Proteggere il "*Single User Mode*" con la password di root, come di seguito mostrato: *# Impostare in /etc/sysconfig/init.* *SINGLE=/sbin/sulogin*	BASSO
BOOTLOADER	
Protezione dei file di configurazione del "bootloader"	
Specifica	**Livello di priorità**
Assicurarsi che i file di configurazione del bootloader siano impostati correttamente. Segue un esempio: *# Impostare l'owner e group di /etc/grub.conf con quelli dell'utente root:* *chown root:root /etc/grub.conf* *chown -R root:root /etc/grub.d* *# Impostare i permessi sui file /etc/grub.conf o /etc/grub.d in modo tale che solo root può leggere e scrivere:* *chmod og-rwx /etc/grub.conf* *chmod -R og-rwx /etc/grub.d*	BASSO
KERNEL LINUX	
Log del kernel	
Specifica	**Livello di priorità**
Limitare l'accesso ai logs del kernel nel seguente modo: *echo "kernel.dmesg_restrict = 1" > /etc/sysctl.d/50-dmesg-restrict.conf*	BASSO
Kernel pointers	
Specifica	**Livello di priorità**
Limitare l'accesso ai "*kernel pointers*" nel seguente modo: *echo "kernel.kptr_restrict = 1" > /etc/sysctl.d/50-kptr-restrict.conf*	BASSO
Exec Shield	
Specifica	**Livello di priorità**
Proteggere "Exec Shield" come segue: *echo "kernel.exec-shield = 2" > /etc/sysctl.d/50-exec-shield.conf*	BASSO
Protezione della memoria	
Specifica	**Livello di priorità**
Randomizzare lo spazio di memoria nel seguente modo: *echo "kernel.randomize_va_space=2" > /etc/sysctl.d/50-rand-va-space.conf*	BASSO
LOGGING	
Syslog	
Specifica	**Livello di priorità**
Assicurarsi che il servizio *syslog* sia abilitato ed in esecuzione. A tal fine, procedere come segue: *systemctl enable rsyslog* *systemctl start rsyslog*	MEDIO
Inviare i dati *syslog* a un server esterno. Ad esempio: *# ELK* *# Logstash* *# Splunk* *# ...*	MEDIO
UTENTI E GRUPPI	
Password	
Specifica	**Livello di priorità**

Aggiornare la "*password policy*" (PAM) utilizzando il comando che segue: *authconfig --passalgo=sha512 * *--passminlen=14 * *--passminclass=4 * *--passmaxrepeat=2 * *--passmaxclassrepeat=2 * *--enablereqlower * *--enablerequpper * *--enablereqdigit * *--enablereqother * *--update*	MEDIO
Limitare il riuso delle password (PAM) nel seguente modo: *# Modificare /etc/pam.d/system-auth* *# Nel caso di pam_unix.so impostare:* *password sufficient pam_unix.so ... remember=5* *# nel caso di pam_pwhistory.so impostare:* *password requisite pam_pwhistory.so ... remember=5*	MEDIO
Rafforzare le impostazioni relative alla politica sulle password presenti nel file "*/etc/login.defs*". Procedere come segue: *# Impostare in /etc/login.defs* *PASS_MIN_LEN 14* *PASS_MIN_DAYS 1* *PASS_MAX_DAYS 90* *PASS_WARN_AGE 14*	MEDIO
Logon Access	
Specifica	**Livello di priorità**
Bloccare gli account dopo un certo numero di tentativi di accesso falliti (PAM). A tal fine procedere come segue: *# Modificare /etc/pam.d/system-auth e /etc/pam.d/password-auth* *# Aggiungere la seguente linea immediatamente prima dello statement pam_unix.so presente nella sezione AUTH:* *auth required pam_faillock.so preauth silent deny=3 unlock_time=never fail_interval=1800* *# Aggiungere la seguente linea immediatamente dopo lo statement pam_unix.so presente nella sezione AUTH:* *auth [default=die] pam_faillock.so authfail deny=3 unlock_time=never fail_interval=1800* *# Aggiungere la seguente linea immediatamente prima lo statement pam_unix.so presente nella sezione ACCOUNT:* *account required pam_faillock.so*	MEDIO
Impostare l'auto logout per inattività dell'utente. Procedere nel seguente modo: *echo "readonly TMOUT=900" >> /etc/profile.d/idle-users.sh* *echo "readonly HISTFILE" >> /etc/profile.d/idle-users.sh* *chmod +x /etc/profile.d/idle-users.sh*	BASSO
Impostare la notifica per l'ultima operazione di logon/accesso. Procedere nel seguente modo: *# Impostare in /etc/pam.d/system-auth* *session required pam_lastlog.so showfailed*	BASSO
FILESYSTEM	
Hardlinks e Symlinks	
Specifica	**Livello di priorità**
Abilitare la protezione per gli hard/soft link nel seguente modo: *echo "fs.protected_hardlinks = 1" > /etc/sysctl.d/50-fs-hardening.conf* *echo "fs.protected_symlinks = 1" >> /etc/sysctl.d/50-fs-hardening.conf*	BASSO

Mount e Unmount dinamico	
Specifica	**Livello di priorità**
Disattivare i file system non di uso comune, come segue: *echo "install cramfs /bin/false" > /etc/modprobe.d/uncommon-fs.conf* *echo "install freevxfs /bin/false" > /etc/modprobe.d/uncommon-fs.conf* *echo "install jffs2 /bin/false" > /etc/modprobe.d/uncommon-fs.conf* *echo "install hfs /bin/false" > /etc/modprobe.d/uncommon-fs.conf* *echo "install hfsplus /bin/false" > /etc/modprobe.d/uncommon-fs.conf* *echo "install squashfs /bin/false" > /etc/modprobe.d/uncommon-fs.conf* *echo "install udf /bin/false" > /etc/modprobe.d/uncommon-fs.conf* *echo "install fat /bin/false" > /etc/modprobe.d/uncommon-fs.conf* *echo "install vfat /bin/false" > /etc/modprobe.d/uncommon-fs.conf* *echo "install nfs /bin/false" > /etc/modprobe.d/uncommon-fs.conf* *echo "install nfsv3 /bin/false" > /etc/modprobe.d/uncommon-fs.conf* *echo "install gfs2 /bin/false" > /etc/modprobe.d/uncommon-fs.conf*	MEDIO
SELINUX E AUDITD	
Utilizzo di SELinux in modalità "Enforcing"	
Specifica	**Livello di priorità**
Impostare SELinux in modalità "*Enforcing*" nel modo che segue: *# Impostare in /etc/selinux/config.* *SELINUXTYPE=enforcing*	ALTO
RETE	
TCP/SYN	
Specifica	**Livello di priorità**
Abilitare la protezione dei cookie TCP/SYN nel modo che segue: *echo "net.ipv4.tcp_syncookies = 1" > /etc/sysctl.d/50-net-stack.conf*	MEDIO
Routing	
Specifica	**Livello di priorità**
Disabilitare il routing dell'IP sorgente nel modo che segue: *echo "net.ipv4.conf.all.accept_source_route = 0" > /etc/sysctl.d/50-net-stack.conf*	MEDIO
Protocollo ICMP	
Specifica	**Livello di priorità**
Disattivare l'accettazione del re-indirizzamento nel protocollo ICMP. A tal fine, procedere come segue: *echo "net.ipv4.conf.all.accept_redirects = 0" > /etc/sysctl.d/50-net-stack.conf*	MEDIO
Consentire di ignorare le richieste ICMP. A tal fine procedere come segue: *echo "net.ipv4.icmp_echo_ignore_all = 1" > /etc/sysctl.d/50-net-stack.conf*	MEDIO
Broadcast	
Specifica	**Livello di priorità**
Consentire di ignorare le richieste in broadcast. A tal fine procedere come segue: *echo "net.ipv4.icmp_echo_ignore_broadcasts = 1" > /etc/sysctl.d/50-net-stack.conf*	MEDIO

Seguono alcuni riferimenti utili per la Policy Compliance e la protezione delle informazioni:

- Center of Internet Security (CIS) - CIS Bemchmarks (https://www.cisecurity.org/cis-benchmarks/) - Il Center for Internet Security (CIS) è un'organizzazione senza scopo di lucro. La sua missione è di "identificare, sviluppare, convalidare, promuovere e sostenere soluzioni di best practice per la difesa informatica".
- Security Technical Implementation Guide (STIG) - Stigviewer (https://www.stigviewer.com/stigs) - Le Security Technical Implementation Guides (STIGs) sono gli standard di configurazione creati dalla Defense Information Systems Agency (DISA) per i sistemi del Dipartimento della Difesa Statunitense. Le STIG contengono una guida tecnica

per proteggere informazioni, sistemi e software, che altrimenti potrebbero essere vulnerabili a attacchi informatici dannosi in termini di diniego.

- National Institute of Standards and Technology (NIST) - National Checklist Program (NCP) (https://nvd.nist.gov/ncp/repository) - trattasi di un documento contenente istruzioni o procedure di configurazione di un prodotto informatico (IT) in un ambiente operativo, utili a verificare la corretta configurazione del prodotto stesso e/o a identificare eventuali modifiche non autorizzate a quest'ultimo.
- Payment Card Industry Data Security Standard (PCI-DSS) (https://www.pcisecuritystandards.org/pci_security/) - Il Payment Card Industry Data Security Standard (PCI DSS) è uno standard di sicurezza informatica per le organizzazioni che gestiscono carte di credito. Tale standard è stato creato per aumentare i controlli sui dati dei titolari delle carte di credito al fine di ridurne le frodi.
- Security Content Automation Protocol (SCAP) - Il Security Content Automation Protocol (SCAP) è una metodologia per l'utilizzo di specifici standard che consentono la gestione automatizzata delle vulnerabilità, la misurazione e la valutazione della conformità alle policy dei sistemi presenti in un'organizzazione, ivi inclusa, ad esempio, la conformità FISMA. Il National Vulnerability Database (NVD) rappresenta il content repository del governo statunitense per lo SCAP. Un esempio di implementazione dello SCAP è OpenSCAP.
  - SCAP Security Policies (https://www.open-scap.org/security-policies/) - insieme di regole interpretabili da una macchina a cui l'infrastruttura deve conformarsi.
  - OpenSCAP Base (https://www.open-scap.org/tools/openscap-base/) - Il tool di scansione OpenSCAP è uno strumento capace di scansionare il sistema, convalidare i contenuti di conformità alla sicurezza e generare report e indicazioni basate su tali scansioni.
  - SCAP Workbench (https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/sect-using_scap_workbench) - SCAP Workbench è un'utilità che consente di eseguire facilmente le comuni operazioni oscap su sistemi locali o remoti.
  - OpenSCAP Static (https://static.open-scap.org/) – documentazione OpenSCAP suddivisa in tre distinte sezioni: "API Documentation", User Manuals" e "SCAP Security Guides".
- DevSec Hardening Framework (https://dev-sec.io/) - Il progetto tratta alcuni aspetti di hardening che possono essere automatizzati (ad esempio l'impostazione della password di grub o il rafforzamento dei permessi delle directory di uso comune).

Alle linee guida generali riportate nei paragrafi precedenti e valide per tutti i sistemi operativi, si aggiungono, per l'ambito specifico dei sistemi Linux, le indicazioni seguenti:

BIOS Protection	
Minaccia	Possibilità di cambiare o sovrascrivere le caratteristiche di sicurezza del BIOS.
Contromisure	- È necessario proteggere il BIOS dell'host con una password in modo che l'utente finale non sia in grado di modificare e sovrascrivere le impostazioni di sicurezza nel BIOS; è importante mantenere quest'area protetta da eventuali modifiche. Ogni produttore di computer ha un set diverso di modalità di accesso al BIOS che dovrebbe essere comunque protetto utilizzando queste modalità. Proteggere GRUB con password per limitare l'accesso fisico al sistema. - Inoltre, è necessario disabilitare l'avvio da dispositivi multimediali esterni (USB / CD / DVD). Se si omette di modificare questa impostazione, chiunque può utilizzare una chiavetta USB che contenga un sistema operativo avviabile e accedere ai dati del sistema operativo. - I server linux più recenti dispongono di applicazioni Web attraverso le quali è

	possibile, accedendo da remoto, configurare le caratteristiche di sistema. Bisogna assicurarsi di cambiare la password predefinita o, eventualmente, disattivare questa possibilità.

Hard disk encryption	
Minaccia	Possibilità di accedere, ad esempio, tramite boot da sistema operativo esterno ai dati presenti sui dischi della macchina linux.
Contromisure	La maggior parte delle distribuzioni Linux consentono di crittografare i dischi prima dell'installazione o successivamente tramite software opportuni. La crittografia del disco è importante in caso di furto o di accesso fraudolento perché il malintenzionato non sarà in grado di leggere le informazioni presenti sui dischi stessi anche collegando il disco rigido ad un altro computer.

Lock boot directory	
Minaccia	La "boot directory" contiene file importantissimi relativi al kernel Linux, quindi è necessario assicurarsi che questa directory sia bloccata con autorizzazioni di sola lettura.
Contromisure	Il lock della boot directory va eseguito seguendo alcuni semplici passaggi. Aprire con un editor il file “fstab” (path usuale /etc/fstab) e aggiungere la riga LABEL=/boot /boot ext2 defaults 1 2 (i valori di riferimento ext2 possono variare a seconda della configurazione del sistema linux). Al termine della modifica del file, è necessario impostare il proprietario eseguendo il seguente comando: #chown root:root /etc/fstab Successivamente, vanno impostate alcune autorizzazioni per la protezione delle impostazioni di avvio: Come già indicato nelle pratiche precedentemente descritte, impostare il proprietario e il gruppo di /etc/grub.conf all'utente root: #chown root: root /etc/grub.conf Impostare il permesso sul file /etc/grub.conf per leggere e scrivere solo per root: #chmod og-rwx /etc/grub.conf Richiedere l'autenticazione per la modalità "single user": #sed -i "/ SINGLE / s / sushell / sulogin /" / etc / sysconfig / init #sed -i "/ PROMPT / s / yes / no /" / etc / sysconfig / init

Disabilitare l'utilizzo di device USB	
Minaccia	Attraverso l'uso di device USB un utente malintenzionato potrebbe accedere al sistema linux come utente amministratore oppure potrebbe accedere a informazioni o dati sensibili del sistema stesso.
Contromisure	A seconda della criticità del sistema, a volte è necessario disabilitare l'uso delle chiavette USB sull'host Linux. Esistono diversi modi per bloccare l'utilizzo di un device USB. Di seguito viene descritto uno dei metodi principali: - Aprire con un editor e modificare il file “blacklist.conf” (path usuale /etc/modprobe.d/blacklist.conf) come indicato. - Aggiungere alla fine del file la riga: - blacklist usb_storage - Salvare e chiudere il file blacklist.conf. - Aprire con un editor e modificare il file rc.local (path usuale /etc/rc.local) - Aggiungere alla fine del file le due righe seguenti: - modprobe -r usb_storage

	- exit 0 - Salvare e chiudere il file rc.local. Eseguire la ripartenza della macchina per rendere effettive le modifiche.

Aggiornamenti di Sistema	
Minaccia	Avere un Sistema non aggiornato può rendere vulnerabile la macchina da attacchi di utenti malintenzionati.
Contromisure	La prima cosa da fare dopo il primo avvio è aggiornare il sistema operativo. La procedura in genere non è complessa e può essere fatta sia da una finestra terminale che per la maggior parte dei sistemi linux anche tramite tool grafici di amministrazione del sistema.

Controllo dei pacchetti installati	
Minaccia	La presenza di servizi non necessari può rappresentare un rischio per la sicurezza del sistema.
Contromisure	Successivamente all'installazione del sistema operativo deve essere effettuato dagli amministratori della macchina un elenco di tutti i pacchetti installati sul SO Linux. Vanno quindi rimossi tutti i pacchetti non necessari. La selezione deve essere molto approfondita per le macchine con tipologia di server perché i server hanno bisogno di un minor numero di applicazioni e servizi installati. Nel caso di server Linux, in particolare, è importante rimuovere i seguenti servizi perché non necessari per il normale utilizzo di un server linux: - Telnet server - RSH server - NIS server TFTP server TALK server

Secure Shell (SSH)	
Minaccia	Secure Shell (SSH) è un protocollo utilizzato per fornire comunicazioni sicure e crittografate su una rete. È più utilizzato dagli amministratori di sistema Linux per la gestione remota dei server. Può anche essere utilizzato per trasferire file su una rete. Per queste caratteristiche la sicurezza SSH è molto importante.
Contromisure	Il protocollo SSH, pur essendo abbastanza sicuro, necessita di una corretta e approfondita configurazione per poter essere utilizzato senza rischi. A tal fine vanno eseguiti tutta una serie di passi sul file file di configurazione "sshd_config" (path usuale /etc/ssh). Tra i principali settaggi di seguito ne verranno elencati i principali: - Cambio delle porte di default del servizio SSH - Configurare SSH per autenticarsi tramite delle chiavi SSH invece di password - Usare il protocollo SSH2 invece di SSH1 - Usare una lista predefinita di possibili accessi di utenti ("User Whitelist") o in alternativa usare delle "Blacklist" di utenti bloccati. - Disabilitare l'accesso tramite root login Se non strettamente necessario è possibile anche eliminare la possibilità di accesso tramite SSH.

Controllo delle porte aperte su linux

Minaccia	La gestione delle porte aperte su linux ed in particolare delle connessioni Internet aperte è fondamentale su linux ai fini della sicurezza del sistema in merito a possibili attacchi di malintenzionati.
Contromisure	Vanno verificate tutte le porte aperte con attenzione particolare a porte nascoste. Su molte versioni di linux, ad esempio, è possibile individuare eventuali porte aperte nascoste tramite il comando: `#netstat –antp` Dopo aver configurato i servizi della rete, è quindi molto importante sapere quali porte sono in ascolto sulle interfacce di rete del sistema. Qualsiasi porta aperta può essere segno di una intrusione. Sono presenti due approcci di base per poter elencare le porte in ascolto sulla rete. L'approccio meno affidabile è quello di interrogare lo stack della rete, inserendo dei comandi del tipo `netstat –an o lsof –i`. Questo metodo è meno affidabile in quanto questi programmi non si collegano alla macchina dalla rete, ma cercano di sapere cosa viene eseguito sul sistema. Per questa ragione, queste applicazioni sono bersaglio da parte di aggressori. In questo modo, i cracker cercano di coprire le loro tracce nel caso in cui essi aprono delle porte di una rete non autorizzata. Il modo più affidabile di controllare quali sono le porte in ascolto sulla rete, è quello di usare uno scanner del tipo nmap. Il seguente comando emesso dalla console, determina quali sono le porte in ascolto dalla rete per collegamenti TCP: `nmap –sT –O localhost`

Password policies	
Minaccia	Una gestione non corretta nella gestione delle "Password policies" aziendali può rappresentare una possibile falla nella sicurezza del sistema.
Contromisure	Una possibile fonte di criticità nella sicurezza nei sistemi operativi è rappresentata dal fatto che le persone spesso riutilizzano le loro password, consuetudine che rappresenta una cattiva pratica di sicurezza. Questa modalità può essere controllata e ed eventualmente impedita tramite interventi sui file di configurazione di sistema. Un'altra politica sulle password che dovrebbe essere forzata è obbligare ad usare solo password con certi regole. Esistono moduli o utility che proteggono il server tramite l'uso di dizionari e metodologie contro attacchi di tipo brute-force. Sarebbe opportuno anche assicurarsi di definire un algoritmo di hashing della password sicuro ad esempio di tipo SHA512. Un'altra funzionalità interessante è bloccare l'account dopo cinque tentativi falliti. Inoltre, un'altra buona pratica è impostare la scadenza della password dopo 90 giorni. Queste attività possono essere eseguite in varie modalità sui sistemi linux. Per esempio: settare il parametro PASS_MAX_DAYS a 90 nel file "/etc/login.defs". E' possibile anche modificare dinamicamente il parametro con il comando linux: #change --maxdays 90 <user>

Partizionamento	
Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Negazione dei servizi.
Contromisure	Come precedentemente illustrato nelle pratiche di sicurezza, in fase di installazione del sistema Linux, è necessario creare delle partizioni distinte per i seguenti percorsi: - / - /boot

	- /home - /tmp - /var/log - /var/log/audit Queste partizioni devono essere utilizzate nel seguente modo: - Sulla partizione di boot devono esser salvati tutti i file necessari ad un corretto avvio del sistema - Sulla partizione /tmp devono esser salvati tutti i file temporanei necessari al corretto funzionamento del sistema e il path /var/tmp dovrà esser collegato, tramite link e irreversibilmente, alla partizione /tmp - Sulla partizione /home devono esser salvati tutti i dati relativi alle utenze presenti sul sistema e ai loro ambienti - Sulle partizioni /var/log* devono esser salvati tutti i file di log e auditing Altri applicativi particolarmente esigenti in termini di spazio e non inclusi nella distribuzione Linux, devono essere installati in partizioni separate (es. Oracle, DB2, ecc.). L'utilizzo di diverse partizioni permette di salvaguardare l'integrità e la riservatezza dei file di configurazione, dei file di log e dei dati applicativi.

Opzioni di mount delle partizioni	
Minaccia	- Abuso di privilegi da parte dell'utente. - Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Errori di amministrazione dei sistemi. - Negazione dei servizi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (es. malware, ecc.). - Cancellazione o furto di informazioni (accidentale o da attacchi come ad es. il ransomware, ecc.).
Contromisure	Specificare le seguenti opzioni di mounting per la partizione /tmp: - nodev - nosuid - noexec - strictatime (visualizzato come relatime dall'output comando "mount") Specificare la seguente opzione di mounting per la partizione /home: - nodev Non devono esser utilizzate periferiche esterne removibili. Nel caso se ne renda necessario l'utilizzo, specificare le seguenti opzioni di mounting in /etc/fstab: - nodev - nosuid - noexec Utilizzare le seguenti opzioni di mounting per il path relativo alla memoria condivisa: - nodev - nosuid - noexec L'utilizzo di questi parametri evita l'esecuzione di file malevoli e l'escalation dei privilegi sul server, o l'accesso non autorizzato a periferiche di sistema.

Cartelle scrivibili da chiunque	
Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Negazione dei servizi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (es. malware, ecc.). - Cancellazione o furto di informazioni (accidentale o da attacchi come ad es. il ransomware, ecc.).
Contromisure	Sul sistema non dovrebbero esistere cartelle scrivibili da chiunque, modificare, per tali cartelle, i permessi di scrittura per OTHER in modo più restrittivo. Nel caso in cui tale configurazione dei diritti di accesso sia strettamente necessaria, configurare i permessi di tutte le cartelle riscrivibili da tutti per far sì che nessun utente possa cancellare e modificare i file di cui non è proprietario. Impostare di conseguenza lo "sticky bit", su tutte le cartelle riscrivibili da tutti.

UMASK	
Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Negazione dei servizi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (es. malware, ecc.). - Cancellazione o furto di informazioni (accidentale o da attacchi come ad es. il ransomware, ecc.).
Contromisure	Configurare la umask di default sia per root sia per gli altri utenti in modo che: - Ogni nuovo file creato possa essere modificato o cancellato esclusivamente dal suo owner - Ogni nuovo file creato possa esser acceduto solo da parte degli utenti appartenenti al gruppo dell'owner stesso Questa configurazione permette di avere un controllo nativo sulla riservatezza e sull'integrità di tutti i nuovi file.

Single User Mode e Boot Interattivo	
Minaccia	- Abuso di privilegi da parte dell'utente. - Accesso non autorizzato ai sistemi. - Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi (software e configurazioni). - Attacchi all'integrità delle informazioni. - Cancellazione dei log di accountability e/o ripudio di operazioni effettuate. - Uso non autorizzato di privilegi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (es. malware, ecc.). - Violazione di leggi, di regolamenti, di obblighi contrattuali. - Danneggiamento, perdita o furto di un asset fisico.
Contromisure	Abilitare il controllo di autenticazione per l'accesso alla modalità single-user al fine di impedire la compromissione del sistema da parte di utenti non autorizzati in grado di accedere fisicamente alla console del sistema. Disabilitare il boot interattivo per gli utenti di sistema (tasto I al boot) al fine di

	contrastare l'utilizzo improprio di comandi sistemistici in fase di avvio del sistema operativo.

Sicurezza TCP/IP	
Minaccia	- Negazione dei servizi. - Compromissione delle comunicazioni.
Contromisure	È necessario mettere in sicurezza lo stack TCP/IP attraverso le seguenti impostazioni: - Disabilitare l'IP forwarding al fine di impedire che il server in esame funga come base di attacco verso ulteriori sistemi nella rete. - Disabilitare l'invio e l'accettazione di pacchetti ICMP Redirect. - Disabilitare l'accettazione di pacchetti ICMP Redirect anche se questi provengono da gateway trusted (ICMP Secure Redirect). - Disabilitare i pacchetti "source routed". - Abilitare i log per i pacchetti di rete ricevuti, aventi un indirizzo di origine non-routable (privo di una rotta in tabella di routing). - Ignorare i pacchetti ICMP Echo inviati in broadcast. - Disabilitare il logging nel caso di ricezione di pacchetti broadcast non conformi allo standard RFC-1122 al fine di impedire la saturazione dello spazio destinato ai file di log. - Abilitare il "reverse path filtering". - Abilitare i "SYN cookies" per la gestione dell'handshake TCP SYN/ACK. - Disabilitare l'IPv6 (se non utilizzato) in modo da ridurre la superficie di attacco del sistema.

Utenti e gruppi di default	
Minaccia	Accesso non autorizzato ai sistemi.
Contromisure	Disabilitare le utenze di default non utilizzate ma definite sul sistema quali: - lp - news - uucp - games - gopher - ftp - vcsa - rpc - smmsp - pcap - desktop Disabilitare i gruppi di default non utilizzati quali: - lp - news - uucp - games

PATH di root	
Minaccia	- Attacchi all'integrità dei sistemi. - Errori di amministrazione dei sistemi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (es. malware, ecc.).

Contromisure	L'utenza root deve avere la variabile di ambiente PATH definita con i soli percorsi necessari all'esecuzione delle operazioni di default. Definire, ad esempio, PATH="/usr/bin:/usr/sbin:/sbin" e non inserire in alcun caso il path "." . Nel caso in cui siano presenti specifiche directory, diverse da quelle standard, per esigenze particolari, tali directory devono risultare scrivibili solo da root ed eventualmente dall'utente proprietario, se diverso da root.

Accessi amministrativi impersonali	
Minaccia	- Violazione di leggi, di regolamenti, di obblighi contrattuali. - Uso non autorizzato di privilegi. - Cancellazione dei log di accountability e/o ripudio di operazioni effettuate.
Contromisure	Disabilitare il login remoto per l'utenza amministrativa root e per altre utenze impersonali (es. "oracle", ecc.), al fine di assicurare il corretto tracciamento delle attività svolte dagli amministratori di sistema e la corretta associazione tra le attività svolte e le persone fisiche che le hanno effettivamente attuate. Gli amministratori di sistema dovranno accedere con utenze personali univoche e successivamente utilizzare il comando "sudo" per effettuare operazioni privilegiate. Le utenze personali possono essere definite sul sistema, o per maggiore praticità il sistema può essere integrato con un server di autenticazione centralizzato basato su LDAP o Active Directory, ad es. tramite moduli PAM.

Tentativi di accesso ripetuti	
Minaccia	- Accesso non autorizzato ai sistemi. - Negazione dei servizi.
Contromisure	Impostare un limite per i tentativi di accesso remoto al sistema (3 tentativi) e un blocco temporaneo (generalmente 30 minuti) al raggiungimento di tale limite.

Minimizzazione dei servizi	
Minaccia	- Abuso di risorse. - Accesso non autorizzato ai sistemi. - Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Negazione dei servizi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (es. malware, ecc.).
Contromisure	Disabilitare tutti i servizi non necessari, al fine di ridurre i vettori di attacco al sistema e il numero di vulnerabilità associate a servizi non necessari e insicuri. In particolare. Disabilitare X-Windows se non necessario, e tutti i servizi legacy basati su inetd e non utilizzati, ovvero chargen, daytime, discard, echo, time, tftp. Disabilitare inoltre I seguenti servizi autonomi: - avahi-daemon - cups (server di stampa) - dhcpd (server DHCP) - slapd (server LDAP) - nfs - rpcbind - named (server DNS)

	- vsftpd (server FTP di default) - httpd (server Web di default) - dovecot (servizi IMAP e POP3) - smb (server Samba) - squid (Web Proxy Server) - snmpd (SOLO SE SNMP NON E' IN USO) - ypserv (server NIS) - rsh.socket (rsh) - rlogin.socket (rlogin) - rexec.socket (rexec) - ntalk (server Talk) - telnet.socket (server Telnet) - tftp.socket (server TFTP) - rsyncd (server rsync) - finger-server

Configurare il Mail Transfer Agent (MTA) in modalità locale	
Minaccia	- Abuso di risorse. - Negazione dei servizi.
Contromisure	Gli MTA (ad es. Sendmail e Postfix) sono usati per ricevere email in entrata e trasferire I messaggi all'utente o al mail server di destinazione. Se il sistema non è un mail server o un SMTP relay, l'MTA deve essere configurato per processare solo le mail generate localmente al sistema (ad es. da applicative che generano un errore e inviano un messaggio a root per scopi di diagnostica).

Controllo automatico di integrità dei sistemi	
Minaccia	Attacchi all'integrità dei sistemi (software e configurazioni).
Contromisure	Per sistemi particolarmente critici, installare e configurare un File Integrity Monitor tool, al fine di garantire l'integrità dei file di configurazione e di sistema. Tale strumento deve permettere l'invio di alert configurabili, qualora siano rilevate delle modifiche non autorizzate eseguite da utenti malevoli. Esempi di tali strumenti sono AIDE (Advanced Intrusion Detection Environment), TripWire File Integrity Manager e OSSEC[3].

5.2.13 Sicurezza di Windows

La versione di default di un server o una workstation Windows potrebbe non disporre di tutte le misure di sicurezza necessarie per essere impiegato direttamente in un contesto di produzione, anche se Microsoft negli ultimi anni ha notevolmente migliorato la configurazione predefinita in ciascuna versione del sistema operativo. Segue una sintesi in termini di raccomandazioni di carattere generale, alcune valide anche per altri sistemi e altre specifiche per Windows, utili a rafforzare la resilienza del sistema operativo alla maggior parte degli attacchi informatici:

- Tenere aggiornata l'installazione di Windows - Probabilmente il passo più importante da fare è controllare la presenza degli ultimi aggiornamenti di sicurezza e le patch disponibili per il sistema

[3] https://www.ossec.net

operativo Windows. E' possibile in Windows ottenere automaticamente gli aggiornamenti di sicurezza. Dopo aver verificato la disponibilità di aggiornamenti, tenere attivo l'aggiornamento automatico al fine di scaricare e installare gli aggiornamenti maggiormente importanti che possono essere di aiuto a proteggere la postazione di lavoro/server da possibili nuovi virus o malware. Ricordare sempre di mantenere aggiornato il sistema operativo applicando l'ultima patch di sicurezza disponibile. Il patching del software rimane una chiave essenziale per migliorare la sicurezza online.

- Aggiornare il software installato - Non è necessario aggiornare solo il sistema operativo, ma anche il software in esso installato. Pertanto, anche in questo caso è opportuno assicurarsi che vengano installati gli ultimi aggiornamenti e le patch di sicurezza per i programmi e le applicazioni principali presenti nel sistema. Inutile dire che i software più diffusi (come Java, Adobe Flash, Adobe Shockwave, Adobe Acrobat Reader), in particolare quelli obsoleti, sono sempre oggetto di minaccia da parte di attori malintenzionati che intendono sfruttarli per ottenere un accesso più facile ai dati sensibili. Poiché questi software sono sempre sotto attacco, è importante non limitarsi a fare affidamento sulla propria memoria per aggiornare manualmente ciascun programma o applicazione installata nel sistema.
- Creare un punto di ripristino - Se si sono già installati gli aggiornamenti di sicurezza per il sistema operativo, il passaggio successivo è creare un punto di ripristino di Windows. Dopo aver installato Windows, è possibile creare il punto di ripristino e denominarlo "Installazione pulita" e continuare con l'installazione dei driver e delle applicazioni necessarie alla destinazione d'uso della macchina. Se uno dei driver o applicazione causa problemi al sistema, è sempre possibile tornare al punto di ripristino ripartendo dall'installazione pulita.
- Installare un software antivirus - Nel prendere in considerazione l'installazione di un programma antivirus, assicurarsi di utilizzarne uno certificato da una azienda riconsciuta, in quanto si potrebbe incorrere in programmi antivirus falsi. È importante disporre sul sistema di una soluzione di sicurezza affidabile, che dovrebbe prevedere la scansione in tempo reale, l'aggiornamento automatico del software e delle ultime vulnerabilità/minacce nonché di un firewall. Se si sceglie di installare un software antivirus che non dispone di un firewall, assicurarsi quantomeno di aver attivato il firewall di Windows.
- Adottare una soluzione di sicurezza proattiva per una protezione a più livelli - L'utilizzo di un antivirus tradizionale non è più la soluzione ideale, semplicemente perché non riesce a tenere il passo con l'ascesa di nuove e avanzate minacce presenti online. In particolare, il malware di carattere finanziario viene prodotto per sottrarre illecitamente dati sensibili e informazioni riservate impiegando metodi sofisticati per farlo. Il malware di nuova generazione di solito ha la capacità di eludere il rilevamento e aggirare il software antivirus che gli utenti hanno installato sulle proprie postazioni di lavoro al fine di mantenere i propri dati al sicuro. Con l'aiuto di una soluzione di sicurezza informatica proattiva, è possibile ottenere una migliore protezione contro malware di carattere finanziario e di furto di dati, come Zeus o Cryptolocker. Ad esempio, per migliorare il controllo finanziario di un conto bancario online, è sempre possibile impostare degli avvisi inviati dalla banca per tenere traccia dell'attività svolta sul conto, applicando questo semplice ed efficace criterio come misura proattiva di sicurezza.
- Eseguire il backup del sistema - Le pratiche precedentemente descritte hanno lo scopo di proteggere il sistema da software dannoso e minacce online, ma si potrebbero comunque riscontrare problemi hardware che potrebbero mettere in pericolo le informazioni riservate presenti nel sistema stesso. Per garantire che i dati rimangano al sicuro, si dovrebbe utilizzare una duplice strategia, che dovrebbe includere la combinazione di un utilizzo di un disco rigido esterno con un servizio di backup online. E' opportuno sottolineare l'importanza di disporre di una soluzione di backup capace di fornire stabilità, facile da usare, che consenta di sincronizzare i file di sistema con un server di backup online e che disponga di capacità di sicurezza, come la crittografia. A prescindere, è sempre comunque possibile utilizzare il sistema di backup di Windows.
- Utilizzare account di utente standard - Windows fornisce un certo livello di diritti e privilegi a seconda del tipo di account utente in uso. È possibile utilizzare un account utente standard o un

account utente amministratore. Al fine di proteggere il sistema, è consigliabile l'utilizzo di account standard per impedire agli utenti di apportare modifiche che interesserebbero tutti coloro che utilizzano la macchina, come ad esempio la cancellazione di importanti file di Windows necessari per il sistema. Con un account utente standard, si hanno diritti limitati e non è possibile ad esempio, cambiare le impostazioni di sistema o installare nuove applicazioni software, cambiare il nome dell'utente e la relativa password. Questo il motivo per cui si dovrebbe usare un account di questo tipo. Se è necessario installare un'applicazione o apportare modifiche di sicurezza, ciò lo si dovrebbe fare solo con un account amministratore. E' inoltre una buona pratica di sicurezza impostare una password complessa per ciascun account di Windows.

- Mantenere abilitato il controllo dell'account - Lo "User Account Control" anche detto UAC è una funzionalità di sicurezza essenziale di Windows che impedisce modifiche non autorizzate al sistema operativo. Spesso si ha la tendenza a disabilitarlo dopo aver installato/reinstallato il sistema operativo. Come si può ben comprendere, non è consigliabile disattivarlo. Invece di disabilitare l'UAC, è possibile ridurre il livello di notifica usando un cursore presente nelle impostazioni di controllo dell'account utente di Windows. L'UAC controlla quali modifiche potranno essere apportate al computer. Quando viene rilevata una modifica importante, come l'installazione di un programma o la rimozione di un'applicazione, viene visualizzato l'UAC che richiede un'autorizzazione a livello di amministratore. Nel caso in cui l'account utente sia infetto da malware, l'UAC aiuta a impedire che programmi e attività sospette apportino modifiche al sistema.
- Proteggere il browser web predefinito prima di connettersi a internet - Un'altra cosa da fare dopo l'installazione di Windows è quella di prestare particolare attenzione alla sicurezza del browser web. Poiché il browser Web è lo strumento principale utilizzato per accedere a Internet, è importante tenerlo al sicuro prima di connettersi online. Le vulnerabilità presenti nel browser web sono come una porta aperta verso il sistema per i criminali informatici che trovano sempre modi creativi per raccogliere dati significativamente importanti. Ad esempio, se si utilizza Adobe Flash, prestare attenzione alle difettosità di sicurezza di quest'ultimo e al modo in cui può esporre il sistema agli attacchi. Per rimanere al sicuro durante la navigazione sul Web, attenersi in generale alle seguenti regole:
    - Scegliere l'ultima versione del browser in uso.
    - Tenere il software del browser aggiornato.
    - Scegliere una sessione di navigazione privata quando si accede a un sito Web di cui non si è sicuri. La scelta di tale modalità impedirà che le credenziali (o i cookie) di autenticazione vengano archiviate e sottratte indebitamente dagli aggressori.
    - Poiché un eventuale malware capace di sottrarre dati potrebbe diffondersi anche nei siti Web legittimi attraverso del codice dannoso presente all'interno delle finestre popup, è buona norma assicurarsi che il browser web sia preimpostato per bloccare i popup.
- Utilizzare uno strumento software per crittografare il disco rigido - Anche se si imposta una password di account per l'accesso al sistema, soggetti malintenzionati possono comunque ottenere l'accesso non autorizzato ai file e documenti privati dell'account. Questi vi possono accedere semplicemente avviando la macchina con un proprio sistema operativo, ad esempio Linux, da un disco esterno o un'unità flash USB. In tal caso, una delle possibili soluzioni è quella di crittografare il disco rigido in modo tale da proteggere i file sensibili in esso memorizzati. Si consiglia di utilizzare tale livello di sicurezza se si dispone di un laptop, che può essere facilmente prelevato. La stessa cosa vale per un computer desktop. Uno strumento di crittografia gratuito che è possibile utilizzare è BitLocker, disponibile anche per le ultime versioni di Windows. Dopo aver abilitato la protezione BitLocker, non si noterà alcuna differenza e si potrà semplicemente accedere al sistema inserendo la normale password dell'account utente di Windows. I vantaggi apportati dall'utilizzo di questo strumento di crittografia sono:
    - la possibilità di cifrare l'intero disco, il che rende impossibile per i soggetti malintenzionati prelevare il laptop per rimuovere il disco rigido e leggere i file.

- la facilità d'uso e la totale integrazione con il sistema operativo Windows, quindi non è necessario aggiungere altro software crittografico.

Alle linee guida generali riportate nei paragrafi precedenti e valide per tutti i sistemi operativi, si aggiungono, per l'ambito specifico dei sistemi Windows (con un focus per Windows 7 Professional Edition), le indicazioni seguenti:

Controlli utente	
Minaccia	- Accesso non autorizzato al sistema. - Accesso non autorizzato alle informazioni. - Uso non autorizzato di privilegi.
Contromisure	È necessario assicurare che i seguenti controlli sulle utenze siano impostati: - L'utente Administrator deve essere disabilitato: questo avviene di default in fase di installazione e pertanto si raccomanda di non riattivarlo. - L'utente Administrator deve essere rinominato. - L'utente Guest deve essere disabilitato. - Il login automatico al desktop deve essere disabilitato. - La schermata di login deve essere configurata per richiedere l'inserimento manuale di nome utente e password (anziché visualizzare le immagini relative agli utenti presenti sul sistema). - La visualizzazione dei "suggerimenti" per la password deve essere disabilitata. - Bloccare lo schermo dopo 15 minuti di inattività e richiedere la password per sbloccarlo. - Richiedere la password quando il PC si riattiva da una sospensione. - L'utente che utilizza normalmente il PC non deve essere un amministratore, ma un utente comune (gruppo Users). - Il sistema Windows deve essere parte di un dominio di Active Directory dell'organizzazione. In conseguenza di ciò, la maggior parte dei controlli indicati nel seguente paragrafo, potranno e dovranno essere applicati ai sistemi sotto forma di Group Policy attuate automaticamente. - Sul sistema non devono essere presenti amministratori locali. Gli unici amministratori abilitati sul sistema devono essere quelli di dominio.

Policy di gruppo	
Minaccia	Accesso non autorizzato alle informazioni sensibili del sistema.
Contromisure	Adottare le seguenti impostazioni di Policy di gruppo, oltre a quelle specificamente menzionate in altre aree del presente documento, per attuare un insieme completo di politiche sui permessi degli utenti ed adeguato dal punto di vista della sicurezza. A tal fine procedere come segue: - Aprire lo strumento di sistema "Group Policy Management Editor". - Navigare fino al nodo "Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment" e selezionarlo. - Nel riquadro dei dettagli mostrato, modificare i permessi utente predefiniti impostando i valori delle opzioni come segue: o "Access Credential Manager as a trusted caller" con il valore "<blank>", o "Act as part of the operating system" con il valore "<blank>", o "Allow log on locally" con il valore "Administrators, Users", o "Create a pagefile" con il valore "Administrators", o "Create a token object" con il valore "<blank>",

	○ "Create global objects" con il valore "Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE", ○ "Create permanent shared objects" con il valore "<blank>", ○ "Create symbolic links" con il valore "Administrators", ○ "Debug programs" con il valore "Administrators", ○ "Enable computer and user accounts to be trusted for delegation" con il valore "<blank>", ○ "Force shutdown from a remote system" con il valore "Administrators", ○ "Impersonate a client after authentication" con il valore "Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE", ○ "Increase scheduling priority" con il valore "Administrators", ○ "Load and unload device drivers" con il valore "Administrators", ○ "Lock pages in memory" con il valore "<blank>", ○ "Modify an object label" con il valore "<blank>", ○ "Modify firmware environment values" con il valore "Administrators", ○ "Perform volume maintenance tasks" con il valore "Administrators", ○ "Profile single process" con il valore "Administrators", ○ "Take ownership of files or other objects" con il valore "Administrators".

Controlli di base	
Minaccia	- Attacchi all'integrità dei sistemi (software e configurazioni). - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (es. malware, ecc.). - Cancellazione dei log di accountability e/o ripudio di operazioni effettuate (in assenza di un SIEM).
Contromisure	È necessario assicurare che i seguenti controlli di base siano attivati: - Abilitare Windows Update e configurare il sistema per l'aggiornamento automatico. - Disabilitare l'auto-play per supporti removibili quali CD/DVD, chiavette USB, schede di memoria, ecc. - Installare e configurare una soluzione per la raccolta, la gestione centralizzata e l'analisi dei log di sicurezza (SIEM – Security Information and Event Management). - Installare una soluzione anti-malware e aggiornarla regolarmente in automatico. Per la gestione centralizzata della sicurezza di una rete Windows complessa, si raccomanda l'uso di adeguati strumenti di gestione basati su template rilasciati da Microsoft, come ad es. Microsoft Security Compliance Manager.

Crittografia del disco di avvio	
Minaccia	- Accesso non autorizzato ai sistemi. - Accesso non autorizzato alle informazioni - Attacchi all'integrità dei sistemi (software e configurazioni). - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Per i computer Windows portatili che contengono informazioni riservate, oppure dati personali sensibili, è necessario proteggere il disco di avvio con BitLocker. Si tratta di un meccanismo di crittografia del disco di boot che richiede all'avvio una password o una "recovery key" (o una smart card).

	In tal modo in caso di smarrimento o furto del portatile, i dati resteranno protetti. Ovviamente la password e la recovery key NON devono essere trascritte (ad es. su un foglio custodito nella valigetta del PC), né comunicate a terzi.

Crittografia dei dischi di ripristino e dei dischi esterni	
Minaccia	- Accesso non autorizzato alle informazioni. - Divulgazione di informazioni riservate. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Quando si utilizza una unità removibile per creare dischi di ripristino, è necessario abilitare la crittografia BitLocker del disco. Questo controllo è particolarmente importante nel caso di backup su dischi rimovibili dato che essi possono essere smarriti o rubati. Più in generale, i dischi esterni removibili contenenti informazioni riservate devono essere inizializzati con un file system crittografato con BitLocker.

Partizionamento	
Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Negazione dei servizi.
Contromisure	In fase di installazione del sistema Windows, è necessario assicurarsi che la partizione di sistema sia di tipo NTFS e non FAT. Se il sistema precede la presenza di una partizione di ripristino del sistema operativo, si consiglia di rimuoverla e di recuperare il relativo spazio. Infatti l'eventuale reinstallazione del sistema operativo deve avvenire partendo da supporti originali non riscrivibili (DVD), o da altri supporti la cui integrità sia garantita.

Accesso al PC dalla rete	
Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Attacchi all'integrità delle informazioni.
Contromisure	La policy di sicurezza 'Access this computer from the network' deve essere ristretta al solo gruppo Administrators, a meno che l'utente (gruppo Users) non debba davvero accedere a questa postazione anche da altri sistemi.

Blocchi per il gruppo Guests	
Minaccia	- Accesso non autorizzato ai sistemi. - Accesso non autorizzato alle informazioni.
Contromisure	Le seguenti policy di sicurezza che impediscono determinate funzionalità sul sistema a certi utenti e gruppi, devono includere esplicitamente il gruppo Guests: - Deny log on as a batch job - Deny log on as a service - Deny log on locally - Deny log on through Remote Desktop Services

Logon Interattivo	
Minaccia	Accesso non autorizzato ai sistemi.
Contromisure	Quando un sistema, facente parte di un dominio, non riesce a raggiungere il server

	Active Directory in fase di accesso, consente comunque di effettuare il login all'utente ma solo per un certo numero di volte (default 10). Tale numero deve essere ridotto a 4 per sistemi particolarmente critici. La relativa policy è denominata: Interactive logon: "Number of previous logons to cache". Inoltre, è necessario disattivare la visualizzazione del nome utente che ha effettuato l'ultimo login, attraverso la policy "Interactive logon: Do not display last user name".

Enumerazione di utenze e condivisioni	
Minaccia	- Accesso non autorizzato ai sistemi. - Accesso non autorizzato alle informazioni. - Attacchi all'integrità delle informazioni.
Contromisure	Per impedire agli utenti anonimi di enumerare le utenze di dominio, le utenze locali e le condivisioni presenti sul sistema, abilitare la policy "Network access: Do not allow anonymous enumeration of SAM accounts and shares".

Null Session	
Minaccia	- Accesso non autorizzato ai sistemi. - Accesso non autorizzato alle informazioni. - Attacchi all'integrità delle informazioni.
Contromisure	Quando alcuni servizi che "girano" come Local System si connettono a sistemi legacy (Windows Vista / Windows Server 2008), utilizzano una Null Session priva dei più elementari controlli di sicurezza. Per impedire questo comportamento ed utilizzare un meccanismo più robusto basato sulla "computer identity", abilitare la policy "Network security: Allow Local System to use computer identity for NTLM".

Sicurezza del protocollo NTLM	
Minaccia	- Accesso non autorizzato ai sistemi. - Accesso non autorizzato alle informazioni. - Attacchi all'integrità delle informazioni.
Contromisure	Se tutti i sistemi Windows in rete supportano NTLMv2, è necessario abilitare questo protocollo come mandatario. Ciò è sicuramente possibile in modo del tutto affidabile solo se in rete vi sono unicamente sistemi Windows 7 / Windows Server 2008 e successivi. A tale scopo devono essere abilitate le seguenti policy: - "Network security: LAN Manager authentication level" → "Send NTLMv2 response only. Refuse LM & NTLM" - "Network security: Minimum session security for NTLM SSP based (including secure RPC) clients" → "Require NTLMv2 session security, Require 128-bit encryption" - "Network security: Minimum session security for NTLM SSP based (including secure RPC) servers" → "Require NTLMv2 session security, Require 128-bit encryption"

Sicurezza del protocollo SMB	
Minaccia	- Accesso non autorizzato ai sistemi. - Accesso non autorizzato alle informazioni. - Attacchi all'integrità delle informazioni.

	- Negazione dei servizi
Contromisure	Per prevenire lo spoofing dell'identità del client, su tutti i sistemi Windows deve essere abilitata la seguente policy per SMB: - "Microsoft network server: Server SPN target name validation level" → "Accept if provided by client" (o più stringente). Quando risulti possibile, è però consigliabile di impostare questa funzionalità come obbligatoria ("Required from client"). Tale impostazione è supportata da tutte le versioni di Windows ma deve essere comunque verificata attentamente prima di essere introdotta. Inoltre, il protocollo SMB nella configurazione di default (che consente la compatibilità con sistemi Windows legacy), è vulnerabile ad attacchi di session hijacking, che consentono ad un utente malevolo, della rete, di interrompere una sessione SMB o di carpire i dati della sessione per introdursi in essa in maniera non autorizzata. Per impedire questa evenienza, è necessario configurare una serie di policy di sicurezza che richiedono la firma digitale e l'encryption del protocollo SMB. Tuttavia tali policy possono bloccare il funzionamento della rete in presenza di sistemi legacy, e quando i sistemi Windows non sono TUTTI configurati nello stesso modo. Se i sistemi presenti sono tutti basati su Windows 7 / Windows Server 2012 (oppure Windows Server 2008 con una hotfix, cfr. Microsoft Knowledge Base KB 950876) e successive versioni, e se è possibile configurare TUTTI questi sistemi allo stesso modo ad es. attraverso una Group Policy, è necessario abilitare le seguenti policy di sicurezza: - "Microsoft network client: Digitally sign communications (always)" → ENABLED - "Microsoft network server: Digitally sign communications (always)" → ENABLED - "Microsoft network server: Digitally sign communications (if client agrees)" → ENABLED Per completezza si nota che sistemi server con ruoli multipli (es. Domain Controller e File Server) fortemente utilizzati e dotati di processori obsoleti, risentiranno necessariamente di un calo delle performance dato che la firma digitale apposta ai pacchetti pone un carico non trascurabile sulla CPU.

Sicurezza del protocollo WS-Management	
Minaccia	- Accesso non autorizzato ai sistemi. - Accesso non autorizzato alle informazioni. - Attacchi all'integrità delle informazioni. - Negazione dei servizi
Contromisure	Windows Remote Management (WinRM) è l'implementazione Microsoft del protocollo WS-Management che è stato sviluppato come standard pubblico per lo scambio remoto di dati di gestione tra i dispositivi che lo implementano. Se per tale protocollo non viene attuata un'adeguata autenticazione e crittografia, il traffico può essere soggetto ad attacchi da parte di un avversario. Per ridurre questo rischio, Windows Remote Management dovrebbe essere configurato in modo sicuro adottando le adeguate impostazioni dei criteri di gruppo. A tal fine procedere come segue: - Aprire lo strumento di sistema "Group Policy Management Editor". - Navigare fino al nodo "Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Client" e selezionarlo. - Nel riquadro dei dettagli mostrato, modificare i permessi utente predefiniti impostando i valori delle opzioni come segue:

	○ "Allow Basic authentication" con il valore "Disabled", ○ "Allow unencrypted traffic" con il valore "Disabled", ○ "Disallow digest authentication" con il valore "Enabled". - Navigare poi fino al nodo "Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service" e selezionarlo. - Nel riquadro dei dettagli mostrato, modificare i permessi utente predefiniti impostando i valori delle opzioni come segue: ○ "Allow Basic authentication" con il valore "Disabled", ○ "Allow unencrypted traffic" con il valore "Disabled", ○ "Disallow WinRM from storing RunAs credentials" con il valore "Enabled".

Disattivazione degli accessi tramite Windows Remote Shell	
Minaccia	- Accesso non autorizzato ai sistemi. - Accesso non autorizzato alle informazioni. - Attacchi all'integrità delle informazioni. - Negazione dei servizi
Contromisure	Quando Windows Remote Shell è abilitato, può consentire ad un avversario di eseguire a distanza script e comandi sulle workstation. Per ridurre questo rischio, Windows Remote Shell dovrebbe essere disabilitato. Per disabilitare l'accesso a Windows Remote Shell, è possibile attuare una specifica impostazione di policy di gruppo procedendo come segue: - Aprire lo strumento di sistema "Group Policy Management Editor". - Navigare fino al nodo "Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Shell" e selezionarlo. - Nel riquadro dei dettagli mostrato, modificare i permessi utente predefiniti impostando i valori delle opzioni come segue: ○ "Allow Remote Shell Access" con il valore "Disabled".

POSIX Subsystem	
Minaccia	Attacchi all'integrità dei sistemi.
Contromisure	Per ridurre la superficie d'attacco del sistema, è necessario disabilitare il sotto-sistema POSIX a meno che non sia effettivamente utilizzato. A tale scopo impostare la policy di sicurezza: - "System settings: Optional subsystems" → "Defined: (blank)"

User Account Control	
Minaccia	- Attacchi all'integrità dei sistemi. - Uso non autorizzato di privilegi. - Errori di amministrazione dei sistemi. - Furto di credenziali di autenticazione (es. da keylogger).
Contromisure	È necessario abilitare il meccanismo "User Account Control" per l'utente Administrator, built-in utilizzando la policy di sicurezza: - "User Account Control: Admin Approval Mode for the Built-in Administrator account" → ENABLED Si raccomanda, inoltre, di impedire agli utenti standard la possibilità di inserire credenziali amministrative per ottenere un token di amministratore, lasciando le operazioni privilegiate ai soli amministratori del dominio. In tal modo gli utenti non potranno, ad es., installare autonomamente software o driver di periferiche né

	eseguire software che richiede l'accesso amministrativo al sistema. Il comportamento normale di Windows quando un utente non amministratore lancia un'applicazione che tenta di ottenere privilegi amministrativi è di richiedere l'immissione delle credenziali amministrative. Se si abilita la seguente policy invece, non apparirà alcuna richiesta di credenziali dato che l'operazione amministrativa sarà automaticamente negata: - "User Account Control: Behavior of the elevation prompt for standard users" → "Automatically deny elevation requests"

Windows Firewall	
Minaccia	- Accesso non autorizzato ai sistemi. - Negazione dei servizi.
Contromisure	Il firewall di Windows è attivo di default. Si raccomanda di non disattivarlo e di non modificare in senso più permissivo le impostazioni di default. Pertanto, a meno che il firewall di Windows non sia stato sostituito da un altro prodotto commerciale (ad es. come parte di una soluzione anti-malware adottata dall'ente/organizzazione), si raccomanda di assicurare tramite Group Policy le seguenti politiche di sicurezza, in modo da impedirne la disattivazione: - "Windows Firewall: Domain: Firewall state" → "ON" - "Windows Firewall: Domain: Inbound connections" → "Block (default)" - "Windows Firewall: Domain: Outbound connections" → "Allow (default)" - "Windows Firewall: Domain: Settings: Apply local firewall rules" → "Yes (default)" - "Windows Firewall: Domain: Settings: Apply local connection security rules" → "Yes (default)" - "Windows Firewall: Domain: Logging: Log dropped packets" → "'Yes" (default: NO) - "Windows Firewall: Domain: Logging: Size limit (KB)" → "16,384 KB" (default 4.096 KB). Identiche impostazioni devono essere applicate alle stesse policy di sicurezza per i profili di rete PRIVATE e PUBLIC del Firewall.

Audit degli accessi	
Minaccia	- Accesso non autorizzato ai sistemi. - Cancellazione dei log di accountability e/o ripudio di operazioni effettuate.
Contromisure	Per abilitare l'auditing (logging) degli accessi sia riusciti che falliti, impostare la seguente policy di sicurezza: - "Audit Credential Validation" → "Success and Failure" In tal modo saranno generate più informazioni di auditing sull'account logon, tra cui: - 4774: An account was mapped for logon. - 4775: An account could not be mapped for logon. - 4776: The domain controller attempted to validate the credentials for an account. - 4777: The domain controller failed to validate the credentials for an account Inoltre, impostare anche le seguenti policy di audit per l'accounting: - "Audit Logon" → "Success and Failure" - "Audit Logoff" → "Success" - "Audit Other Logon/Logoff Events" → "Success and Failure" - "Audit Special Logon" → "Success" - "Audit Account Lockout" → "Success"

Audit degli eventi di sicurezza	
Minaccia	- Accesso non autorizzato ai sistemi. - Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi (software e configurazioni). - Uso non autorizzato di privilegi.
Contromisure	È necessario impostare le seguenti policy di audit, in modo da tracciare nei log di sistema i principali eventi di sicurezza: - "Audit Application Group Management" → "Success and Failure" - "Audit Computer Account Management" → "Success and Failure" - "Audit Other Account Management Events" → "Success and Failure" - "Audit Security Group Management" → "Success and Failure" - "Audit User Account Management" → "Success and Failure" - "Audit Policy Change" → "Success and Failure" - "Audit Authentication Policy Change" → "Success" - "Audit Security State Change" → "Success" - "Audit Security System Extension" → "Success and Failure" - "Audit System Integrity" → "Success and Failure"

Pass the Hash	
Minaccia	- Accesso non autorizzato ai sistemi. - Accesso non autorizzato alle informazioni. - Falsificazione di identità.
Contromisure	Per mitigare la vulnerabilità "pass-the-hash" è necessario adottare, come minimo, le impostazioni di sicurezza fornite dall'apposito template di Microsoft Security Compliance Manager. Da ciò consegue l'impostazione delle seguenti policy: - "Apply UAC restrictions to local accounts on network logons" → "Enabled" - "WDigest Authentication" → "Disabled"

Visualizzazione delle password immesse	
Minaccia	Furto di credenziali di autenticazione.
Contromisure	Generalmente le applicazioni e i servizi di Windows utilizzano le librerie di sistema per visualizzare le finestre di dialogo per l'immissione di username e password. In questo tipo di finestre è presente un "check-box" che consente di visualizzare la password in chiaro. Tale check-box deve essere disattivato a livello globale sul sistema, per impedire che la password possa essere vista da persone diverse dall'utente legittimo. A tale scopo, impostare la seguente policy di sicurezza: - "Do not display the password reveal button" → "Enabled"

Path UNC di NETLOGON e SYSVOL	
Minaccia	- Accesso non autorizzato ai sistemi. - Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Attacchi all'integrità delle informazioni.
Contromisure	Nel febbraio 2015, Microsoft ha rilasciato un nuovo meccanismo di controllo ("Hardened UNC Paths") per mitigare un rischio di sicurezza nelle Group Policy. Il

relativo bollettino di sicurezza è MS15-011 / KB 3000483.
Questo meccanismo richiede sia l'installazione di un aggiornamento di sicurezza, sia l'applicazione di specifiche impostazioni di Group Policy su TUTTI i computer del dominio che devono essere necessariamente basati su Windows Vista / Windows Server 2008 o versioni successive.
L'aggiornamento di sicurezza comprende anche un nuovo template di Group Policy (NetworkProvider.admx/adml) che indirizza i parametri da impostare.
Una volta applicato l'aggiornamento e il template di Group Policy, l'impostazione minima per mitigare il rischio in oggetto è la seguente:

"Hardened UNC Paths" → ENABLED, impostato come segue:

*\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1

*\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1

5.3 Sicurezza del Web Browser

Di seguito viene fornita una vista delle principali minacce e delle relative contromisure da adottare.

5.3.1 Architettura

Architettura	
Minaccia	- Accesso non autorizzato al sistema. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	- Utilizzare un sistema di protezione del perimetro (Firewall) in grado di effettuare Web Application Firewalling, posizionato tra la rete dei client e tutte le altre. - Installare un IDS (intrusion detection system) o IPS (intrusion prevention system) in grado di analizzare le richieste Web. - Impedire la manipolazione DNS: utilizzare DNS attendibile e protetto. - Bloccare i punti di accesso wireless e utilizzare un sistema di protezione come Wi-Fi Protected Access 2 e access point non vulnerabili (con firmware aggiornato) rispetto all'attacco KRACK precedentemente citato. **Nota Bene.** Si tenga presente che i dispositivi portatili personali possono eludere tali contromisure.

5.3.2 Hardening

Hardening del browser	
Minaccia	- Accesso non autorizzato al sistema. - Compromissione delle comunicazioni. - Furto di credenziali di autenticazione (es. keylogger). - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	- Utilizzare il browser con un account utente a bassi privilegi (ovvero senza privilegi di amministratore) in modo da limitare le possibilità di un attacco (security exploit) di compromettere l'intero sistema operativo. - Impostare il browser in modo da controllare la validità dei certificati presentati dai server, utilizzando le liste di revoca dei certificati (CRL), l'Online Certificate Status

	Protocol (OCSP), o altri meccanismi equivalenti. - Limitare/Disabilitare/Condizionare l'uso di: • Controlli ActiveX • Add-ons • Estensioni del browser (plug-ins) • JavaScript e Flash • Java Applets e applicazioni Silverlight. • "Mobile code" in generale. - Ad esempio, su Internet Explorer esiste la possibilità di esprimere delle white list e/o delle black list per controlli ActiveX, add-ons, ed estensioni del browser. - Abilitare (se disponibili) meccanismi di sandbox integrati nel browser. Ad esempio a partire da IE 7 è disponibile il "*protected mode*", una tecnologia che sfrutta i meccanismi di sandboxing chiamati "*Mandatory Integrity Control*". Anche Google Chrome fornisce una sandbox che limita l'accesso al sistema operativo da parte delle pagine web. - Valutare la possibilità di eseguire il browser all'interno di un software di una sandbox selezionata e approvata dall'organizzazione. - Valutare l'adozione di estensioni e plugin di terze parti create a scopo di hardening del browser. A titolo di esempio: - il software "NoScript" che consente l'esecuzione di contenuti web basati su JavaScript, Java, Flash, Silverlight e altri plug-in solo se il sito è considerato attendibile ossia è stato precedentemente aggiunto a una white list. - Valutare l'adozione del software "MyWOT/WOT" (Web of Trust) che fornisce un servizio di reputazione sul livello di trust dei siti web. - Considerare di utilizzare il browser all'interno di un LiveCD. I LiveCD, che forniscono un sistema operativo da una sorgente non scrivibile e sono tipicamente dotati di browser Internet. Se l'immagine originale LiveCD è priva di malware, tutto il software utilizzato, incluso il browser Internet, verrà caricato malware-free ogni volta che viene eseguito il boot dall'immagine LiveCD. Prestare però attenzione ad altro genere di pericoli: Qualsiasi traffico web non protetto (ad esempio, non utilizzando https) o verso siti web vulnerabili potrebbe ancora essere soggetto ad attacchi man-in-the-middle o altre manipolazioni basate sul traffico di rete.

Hardening del browser	
Minaccia	- Accesso non autorizzato alle informazioni. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (phishing e malware). - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	- Disabilitare la memorizzazione di password nel browser. Quasi tutti i browser e molti siti web in genere offrono la possibilità di ricordare le password per uso futuro. L'attivazione di questa funzionalità memorizza le password in un'unica posizione sul computer, rendendo più facile per un aggressore scoprirle se il sistema venisse compromesso. Se questa funzionalità risulta abilitata, è necessario disattivarla e cancellare le password memorizzate. - Attivare il blocco dei popup del browser. Le finestre di popup sono una notevole tecnica di "phishing". Il blocco dei popup è oggi una funzionalità standard dei browser e dovrebbe essere abilitato ogni volta che si naviga sul web. Può essere utilizzata anche su siti web specifici e non su altri, dove i popup potrebbero invece essere necessari.

Privacy durante la navigazione web	
Minaccia	Divulgazione di informazioni riservate.
Contromisure	Adottare le seguenti misure a salvaguardia della privacy degli utenti, rispetto ai siti Web che monitorano le attività utente: - Impostare una routine specifica per eliminare i cookie regolarmente. Alcuni cookie possono costituire un rischio per la privacy in quanto tengono traccia dei siti visitati. Non sempre è possibile bloccare i cookie, ma è opportuno eliminarli (diversamente i cookie possono rimanere memorizzati nel sistema per settimane o più) - Attivare funzionalità "Do Not Track". "Do Not Track" è un header HTTP che comunica ai siti visitati e alle terze parti i cui contenuti sono ospitati in tali siti che le proprie attività non devono essere tracciate. **Nota Bene.** L'invio di una richiesta "Do Not Track" ai siti non garantisce la protezione della privacy. I siti possono scegliere di rispettare la richiesta o continuare a eseguire attività che potrebbero essere considerate di monitoraggio anche se è stata espressa questa preferenza. - Utilizzare la navigazione anonima. **Nota Bene**. Il livello di protezione è diverso a seconda dei browser. In certi casi si tratta fi una difesa da attacchi locali: alcune info, come le password, la cronologia di ricerca e la cronologia delle pagine, vengono eliminate alla chiusura della scheda. In altri casi si tratta della difesa dall'attaccante esterno ossia viene protetto l'**anonimato durante la navigazione**. - Disattivare la condivisione della posizione geografica.

Hardening del browser: configurazione di base per la sicurezza	
Minaccia	- Attacchi all'integrità dei sistemi. - Cancellazione o furto di informazioni (accidentale o da attacchi come ad es. il ransomware, ecc.). - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (es. malware, ecc.).
Contromisure	La configurazione di default per molti browser web non è sicura. Si raccomandano i passaggi a seguire per rendere maggiormente sicuro il browser web in uso. Tali impostazioni assumono particolare importanza nel caso in cui si utilizza il browser per accedere a sistemi aziendali o più in generale se si utilizza il browser per accedere, inviare o ricevere informazioni sensibili. - Impostare il browser di default: o Firefox: sia per Mac che per Windows - andare nel menu Firefox > Preferenze (Mac) Opzioni (Windows) > scheda Generale. Selezionare la casella "Controlla sempre se Firefox è il browser predefinito". o Safari: andare nel menu Safari > Preferenze > scheda Generale e clicca sul pulsante "Imposta predefinito....". o Internet Eplorer: si raccomanda di non utilizzare IE come browser predefinito. o Google Chrome: andare sulle impostazioni nella sezione "Browser predefinito" e cliccare sul pulsante "Imposta come predefinito" in corrispondenza della voce "Imposta Google Chrome come browser predefinito". - Mantenere il software del browser aggiornato. - Abilitare nel browser gli aggiornamenti automatici e mantenerli in tale stato: o Firefox: sia per Mac che per Windows - vai al menu Firefox >

Preferenze (Mac), scheda Opzioni (Windows), scheda Generale > sezione Aggiornamenti di Firefox. Selezionare "Installare automaticamente gli aggiornamenti (consigliato)".
    - Safari: gli aggiornamenti in Safari sono gestiti nel menu Apple in Preferenze di sistema > Aggiornamento software. Impostare su Aggiornamenti giornalieri.
    - Google Chrome: a garanzia di protezione, Google Chrome si aggiorna automaticamente ogni volta che rileva che è disponibile una nuova versione del browser. Il processo di aggiornamento avviene in background e non richiede alcuna azione manuale.
- Bloccare l'accesso ai pop-up, plug-in e ai siti di phishing:
    - Firefox: per il blocco dei pop-up indesiderati, sia per Mac che per Windows – andare nel menu Firefox > Preferenze (Mac) Opzioni (Windows) > Privacy e sicurezza > sezione Permessi. Selezionare "Blocca le finestre pop-up".
    - Firefox: per il blocco delle estensioni del browser indesiderate, sia per Mac che per Windows – andare nel menu Firefox > Preferenze (Mac) Opzioni (Windows) > Privacy e sicurezza > sezione Permessi. Seleziona "Avvisa se un sito web tenta di installare un componente aggiuntivo".
    - Safari: per il blocco dei pop-up indesiderati, andare nel menu Safari > Preferenze > scheda Siti web, fare clic su "Finestre di pop-up" dal pannello di sinistra e impostare "Quando si visitano altri siti web:" su "Blocca e notifica".
    - Safari: per il blocco del phishing e delle estensioni del browser indesiderate, andare nel menu Safari > Preferenze > Scheda Siti Web e deselezionare i plug-in installati indesiderati presenti nel pannello di sinistra.
    - Edge: per il blocco dei pop-up indesiderati, andare su Impostazioni > Impostazioni avanzate > Blocca popup e impostarlo a Attivato.
    - Internet Explorer: per il blocco dei pop-up indesiderati, andare nel menu Strumenti > Opzioni Internet > scheda Privacy. Selezionare la casella di controllo "Attiva Blocco popup".
    - Internet Explorer: per il blocco delle estensioni del browser indesiderate, andare nel menu Strumenti > Opzioni Internet > scheda Avanzate e scorrere verso il basso fino a "Elementi multimediali". Deselezionare se selezionate, "Riproduci animazioni" e "Riproduci suoni" in pagine web.
    - Google Chrome: per il blocco dei pop-up indesiderati, andare su Impostazioni > Avanzate > Privacy e sicurezza > Impostazioni sito > Pop-up e reindirizzamenti e impostare su "Bloccato".
    - Google Chrome: per il blocco delle estensioni del browser indesiderate, andare su Impostazioni > Avanzate > Privacy e sicurezza > Impostazioni sito > Accesso al plugin senza sandbox e impostare su "Chiedi conferma quando un sito vuole utilizzare un plug-in per accedere al tuo computer (opzione consigliata)".
- Impostare il browser in modo tale da non salvare le password. Diversamente se strettamente necessario, utilizzare un meccanismo di master password conforme allo standard UCSC[4]:
    - Firefox: sia per Mac che per Windows - andare nel menu Firefox >

[4] https://its.ucsc.edu/security/passwords.html

Preferenze (Mac) Opzioni (Windows) > Privacy e sicurezza > sezione Privacy del browser > Credenziali e password. Deselezionare la casella di controllo "Chiedi se salvare le credenziali di accesso ai siti Web".

- Firefox: per l'utilizzo di una master password, se è necessario salvare le password, impostare una password Master in modo che le password salvate non siano facilmente accessibili a chiunque abbia accesso al sistema. Sia per Mac che per Windows- andare nel menu Firefox > Preferenze (Mac) Opzioni (Windows) > Privacy e sicurezza > sezione Privacy del Browser > Credenziali e password. Selezionare "Utilizza una password principale".
- Safari: andare nel menu Safari > Preferenze > Scheda Riempimento automatico e deselezionare la casella "Nomi utente e password".
- Edge: andare nel menu Impostazioni > Impostazioni avanzate > Privacy e servizi > "Offri la possibilità di salvare le password" e impostare a Disattivato e "Salva i dati immessi nei moduli" a Disattivato.
- Internet Explorer: andare nel menu Strumenti > Opzioni Internet > Scheda Contenuto e fare clic sul pulsante Impostazioni di "completamento automatico" e deselezionare la casella "Nome utente e password sui moduli".
- Internet Explorer: IE non ha una funzione master password, ma sarebbe opportuno disabilitare la funzione di completamento automatico per le password. Vedere l'indicazione precedente.
- Google Chrome: andare nel menu Impostazioni > Compilazione automatica > Password e disattivare "Chiedi di salvare le password".

- Disabilitare i third-party cookie.
  - Firefox: sia per Mac che per Windows - andare nel menu Firefox > Preferenze (Mac) Opzioni (Windows) > Privacy e sicurezza > Blocco contenuti. Seleziona "Personalizzato" e imposta i cookie per bloccare "Traccianti di terze parti". Abilitare anche i controlli per bloccare i criptominer e le Fingerprinter.
  - Edge: andare nel menu Impostazioni > Impostazioni avanzate > "Privacy e servizi" quindi attivare "Invia richieste Do Not Track", disattivare "Mostra suggerimenti per la ricerca e i siti durante la digitazione", impostare i Cookie su "Blocca solo i cookie di terze parti", disattivare "Usa la previsione della pagina per velocizzare l'esplorazione, migliorare la lettura e migliorare l'esperienza nel complesso" e abilitare "Proteggi il PC da siti e download dannosi con il filtro SmartScreen".
  - Internet Explorer: andare nel menu Strumenti > Opzioni Internet > scheda Privacy e fare clic sul pulsante "Avanzate". Selezionare la casella "Accetta" per i cookie dei siti Web visualizzati e il pulsante "Chiedi conferma" per i cookie di terze parti. Il pulsante "Accetta sempre i cookie della sessione" non dovrebbe essere selezionato. Fare clic su OK. Al termine, fare clic sul pulsante Applica.
  - Google Chrome: andare nel menu Impostazioni > Avanzate > Privacy e sicurezza > Impostazioni sito > Cookie > e attivare "Consenti ai siti di salvare e leggere i dati dei cookie (opzione consigliata)" e "Blocca cookie di terze parti".
- Impostazioni specifiche per tipologia di browser:
  - Firefox: installare l'estensione del browser "uBlock Origin" per il blocco degli annunci.
  - Firefox: contenuto ingannevole e protezione da software pericoloso -

sia per Mac che per Windows - andare nel menu Firefox > Preferenze (Mac) Opzioni (Windows) > Privacy e sicurezza > sezione Sicurezza. Spuntare "Blocca contenuti a rischio e ingannevoli", "Blocca download a rischio" e "Avvisa in caso di software indesiderato e non scaricato abitualmente".

- Firefox: raccolta e utilizzo dei dati Firefox – sia per Mac che per Windows - andare nel menu Firefox > Preferenze (Mac) Opzioni (Windows) > Privacy e sicurezza > Raccolta e utilizzo dati di Firefox. Deselezionare "Consenti a Firefox di inviare a Mozilla dati tecnici e relativi all'interazione con il browser", "Consenti a Firefox di installare e condurre studi" e "Consentire a Firefox di inviare segnalazioni di arresto anomalo in sospeso".
- Safari: disabilitare Java. Andare nel menu Safari > Preferenze > Scheda Sicurezza e impostare il segno di spunta per abilitare "Avvisa quando visiti un sito web fraudolento" e un segno di spunta per "Abilita JavaScript".
- Safari: privacy - andare nel menu Safari > Preferenze > scheda Privacy e selezionare "Prevent cross-site tracking".
- Safari: apertura in modo sicuro dei file scaricati - andare nel menu Safari > Preferenze > scheda Generale. Deselezionare la casella di controllo che indica "Open 'safe' files after downloading".
- Edge: disattivare Flash – andare nel menu Impostazioni > Impostazioni avanzate > "Usa Adobe Flash Player" e impostare su Disattivato.
- Internet Explorer: impostare le security zones, ovvero i livelli di sicurezza per le aree "Internet", "Intranet locale", "Siti attendibili" e "Siti con restrizioni".
- Internet Explorer: disattivare il filtro ActiveX - aprire IE, premere il tasto Alt, aprire il menu Strumenti, e cliccare su "ActiveX Filtering", se non è già spuntato.
- Internet Explorer: suggerimenti aggiuntivi – IE dispone di zone di sicurezza che possono essere impostate per diversi livelli di protezione. Aprire IE, premere il tasto Alt, aprire il menu Strumenti, e cliccare su "Opzioni Internet", selezionare la scheda "Sicurezza". Si consiglia di impostare il livello di sicurezza per l'area "Internet" su ALTA. È inoltre possibile identificare i "Siti attendibili" e impostarli su MEDIO-ALTA.
- Google Chrome: andare nel menu Impostazioni > Avanzate > Privacy e sicurezza > Impostazioni sito > JavaScript e attivare "Consentita (opzione consigliata)".
- Google Chrome: fare in modo che per l'esecuzione di contenuti Flash venga chiesto il consenso - andare nel menu Impostazioni > Avanzate > Privacy e sicurezza > Impostazioni sito > Flash > e impostare su "Chiedi prima".
- Google Chrome: download automatici - andare in Impostazioni > Avanzate > Privacy e sicurezza > Impostazioni sito > Download automatici e impostare su "Chiedi conferma quando un sito tenta di scaricare automaticamente file dopo il primo file (opzione consigliata)".
- Google Chrome: accesso alla videocamera - andare nel menu Impostazioni > Avanzate > Privacy e sicurezza > Impostazioni sito > Videocamera e impostare su "Chiedi prima di accedere (opzione consigliata)".
- Google Chrome: accesso al microfono: andare nel menu Impostazioni

	> Avanzate > Privacy e sicurezza > Impostazioni sito > Microfono e impostare su "Chiedi prima di accedere (opzione consigliata)".

Hardening del browser: MIME Sniffing	
Minaccia	- Attacchi all'integrità dei sistemi. - Cancellazione o furto di informazioni (accidentale o da attacchi come ad es. il ransomware, ecc.). - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (es. malware, ecc.).
Contromisure	Abilitare la barra delle informazioni per consentire all'utente di visualizzare il risultato di un'azione (es. cliccare su un link) prima di effettuarla. Disabilitare la possibilità per i siti web di iniziare un download senza l'accettazione esplicita dell'utente, ad es. da codice (Internet Explorer). Abilitare le funzionalità di MIME Sniffing che consentono di "marcare" un file collegato a un download attraverso il suo MIME Type, per evitare che un codice eseguibile venga visualizzato come testo o altro documento (es. PDF) per invogliare l'utente ad aprirlo.

Hardening del browser: segnalazione errori	
Minaccia	Divulgazione di informazioni riservate.
Contromisure	Limitare/Disabilitare i servizi di "segnalazione automatica degli errori", al fine di evitare la divulgazione di dati personali e di altre informazioni riservate.

Hardening del sistema operativo che ospita il browser	
Minaccia	Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione.
Contromisure	Eseguire l'hardening del sistema operativo che ospita il browser. L'hardening del sistema operativo è oggetto di un paragrafo specifico [rif. 5.2.2]

5.3.3 Autorizzazione

Ai principi generali introdotti nel paragrafo [rif.5.1.3], si aggiungono le indicazioni, di cui di seguito:

Autorizzazione	
Minaccia	Accesso non autorizzato al sistema (macchina, configurazione, etc.)
Contromisure	Proteggere i parametri di sicurezza dagli utenti finali: essi devono essere modificabili solo da un'utenza amministrativa.

5.3.4 Crittografia

Ai principi generali introdotti nel paragrafo [rif. 5.1.4], si aggiungono le indicazioni, di cui di seguito:

Crittografia	
Minaccia	- Accesso non autorizzato alle informazioni. - Divulgazione di informazioni riservate. - Crittografia debole o non validata. - Generazione e/o gestione inadeguata delle chiavi crittografiche.
Contromisure	Valgono i principi generali introdotti nel paragrafo [rif. 5.1.4].

5.3.5 Procedure

Alle linee guida 'Procedure generali' (Change management, Maintenance, Patching, Secure testing, Disposal) introdotti nel paragrafo [rif. 5.1.7], si aggiungono, per l'ambito specifico, le indicazioni di cui di seguito:

Patching	
Minaccia	- Accesso non autorizzato ai sistemi (risorse di sistema, configurazioni, interfacce amministrative, ecc.). - Accesso non autorizzato alle informazioni. - Cancellazione o furto di informazioni (ad es. da ransomware, ecc.). - Compromissione delle comunicazioni. - Negazione dei servizi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (malware) - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	È necessario controllare periodicamente il sito web del fornitore per gli aggiornamenti. A tal fine si fa notare che: - Alcuni browser controllano automaticamente gli aggiornamenti disponibili - Alcuni fornitori offrono la notifica automatica degli aggiornamenti tramite una mailing list.

Sensibilizzare il personale sui rischi che la navigazione in Internet via Browser comporta	
Minaccia	Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (es. malware, ecc.).
Contromisure	Sensibilizzare il personale sui rischi che la navigazione in Internet via Browser comporta. Di seguito le principali norme comportamentali da seguire: - Non fare clic su collegamenti senza considerare i rischi che ne potrebbero derivare (evitare di cliccare su link sospetti presenti nelle pagine). - Prestare attenzione al fatto che gli indirizzi di pagine Web potrebbero essere mascherati e portare in un sito imprevisto. - Considerare che ogni volta che un sito web richiede che vengano abilitate determinate funzionalità o installati software e aggiornamenti, si mette a rischio il computer. Ad es. non aggiornare mail il Flash Player su richiesta di una pagina web ma solo da pannello di controllo. - Non riutilizzare la stessa password per siti diversi. - Non fornire mai online informazioni personali a meno di non essere certi che il sito sia valido e le transazioni sicure: prima di inserire qualsiasi informazione personale, controllare la barra degli URL del browser al fine di accertarsi che il sito sia quello atteso e che sia presente la dicitura "https:" e un'icona a forma di lucchetto ad indicare che la connessione al sito è protetta e che il certificato server è valido. - Evitare Wi-Fi pubblici o gratuiti: l'attaccante spesso utilizza sniffers wireless per rubare le informazioni degli utenti quando vengono inviate su reti non protette. Il modo migliore per proteggersi da questo attacco è evitare di utilizzare queste reti, oppure utilizzarle solo con una VPN che incapsuli tutto il traffico in un tunnel cifrato. - In caso di individuazione di una "falsa" pagina di autenticazione segnalarla al team di sicurezza interna all'organizzazione per procedere all'oscuramento della medesima e possibilmente all'individuazione dei responsabili.

5.3.6 Informazioni addizionali

Riferimenti CERT	
CERT/CC	- Technical Trends in Phishing Attacks, https://www.us-cert.gov/sites/default/files/publications/phishing_trends0511.pdf
US-CERT	- Evaluating Your Web Browser's Security Settings, http://www.us-cert.gov/ncas/tips/st05-001 - Browsing Safely: Understanding Active Content and Cookies, http://www.us-cert.gov/ncas/tips/st04-012 - Understanding Website Certificates, http://www.us-cert.gov/ncas/tips/st05-010 - Understanding Internationalized Domain Names, http://www.us-cert.gov/ncas/tips/st05-016 - Avoiding Social Engineering, http://www.us-cert.gov/ncas/tips/st04-014

Riferimenti Prodotti	
Microsoft Edge	Edge è il browser presentato da Microsoft con il sistema operativo Windows 10 e rappresenta il successore di Internet Explorer (MSIE). Nato come browser integrato con Windows 10 (tecnicamente un'app UWP, ossia Universal Windows Platform), recentemente è stato ricostruito a partire da Chromium, diventando un applicativo a se stante. https://docs.microsoft.com/it-it/deployedge/security-overview
Mozilla Firefox	Mozilla Firefox è un popolare browser di terze parti per Windows, Mac e Linux. Per informazioni su come mantenere i dati protetti e al sicuro con la navigazione privata di Firefox, le funzioni di password e altre impostazioni di protezione, visitare il sito: https://support.mozilla.org/en-US/products/firefox/privacy-and-security
Apple Safari	È il browser più usato nel sistema operativo macOS. Per informazioni visitare la pagina: https://www.apple.com/it/safari/
Google Chrome	Per informazioni sulla sicurezza di Chrome (caratteristiche e funzionalità) si rinvia alla pagina (selezionare le opzioni visualizzate nell'argomento): https://www.google.com/intl/it/chrome/security
Opera	Browser snello che nella sua ultima versione è stato costruito sulla base di Chromium. Ne esiste una versione per le pattaforme "mobile", chiamato Opera Mini. Per informazioni relative a privacy e sicurezza visitare la pagina: https://help.opera.com/en/latest/security-and-privacy
Chromium	Chromium è un progetto open source volto a realizzare un browser sicuro, veloce e stabile per tutti gli utenti di Internet. Per informazioni relative alla sicurezza visitare la seguente pagina: https://www.chromium.org/Home/chromium-security

5.4 Sicurezza delle Postazioni di lavoro

5.4.1 Architettura

Protezione reti extranet (ad es., Internet)	
Minaccia	Furto di credenziali di autenticazione
Contromisure	Provvedere ad un'adeguata protezione dell'infrastruttura di rete nella quale è operativa la PdL, mediante la configurazione di uno o più dispositivi (firewall, proxy server, etc.) di protezione dalle reti esterne (Internet e reti di partner e fornitori). Prevedere inoltre una segmentazione della rete interna che isoli tramite firewall le PdL

	in una apposita sezione di rete.

Continuità elettrica delle PdL	
Minaccia	Negazione dei servizi - Black out elettrico o mancanza improvvisa di energia elettrica
Contromisure	Verificare che sia garantita l'alimentazione delle PdL in caso di interruzione della corrente elettrica, tramite l'utilizzo di dispositivi UPS che garantiscano anche la protezione dalle sovratensioni, prevedendo uno shutdown automatico allo scadere del periodo di autonomia dell'UPS. Effettuare un monitoraggio delle batterie degli UPS e prevederne la sostituzione qualora si ravvisi un degrado della loro capacità.

Protezione fisica dei dispositivi (fissi e mobili)	
Minaccia	- Cancellazione o furto di informazioni. - Danneggiamento, perdita o furto di un asset fisico. - Negazione dei servizi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione.
Contromisure	Assicurare un cavo di acciaio galvanizzato, non meno di 3,5 mm di spessore, munito di chiusura a chiave o a combinazione al computer da proteggere o, in alternativa, utilizzare delle gabbie di sicurezza facilmente ancorabili, in cui riporre i dispositivi. Accertare che il cavo sia assicurato ad un elemento fisso non smontabile, facendone passare un'estremità nell'occhiello posto ad un capo del cavo ed inserire il lucchetto di sicurezza nell'apposito foro presente nel computer.

5.4.2 Hardening

Hardening del sistema operativo installato sulla PDL	
Minaccia	- Accesso non autorizzato ai sistemi (risorse di sistema, configurazioni, interfacce amministrative, ecc.). - Accesso non autorizzato alle informazioni. - Cancellazione o furto di informazioni (accidentale o da attacchi come ad es. il ransomware, ecc.). - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (malware).
Contromisure	Eseguire l'hardening del sistema operativo che gira sulla PDL [rif. 5.2.2].

Hardening del/i web browser/s installato/i sulla PDL	
Minaccia	- Accesso non autorizzato alle informazioni. - Cancellazione o furto di informazioni (accidentale o da attacchi come ad es. il ransomware, ecc.). - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (malware)
Contromisure	I principi per la sicurezza del web browser sono oggetto di un paragrafo precedente. Effettuare controlli periodici al fine di verificare che i browser installati sulle PdL siano effettivamente quelli autorizzati e con le configurazioni di sicurezza previste (es. funzionalità di blocco dei popup, degli script, ecc.).

Hardening del sistema	
Minaccia	Negazione dei servizi (per spam su sistemi di messaggistica).
Contromisure	Se è autorizzato l'uso di sistemi di messaggistica immediata, dotarsi di strumenti specifici "IM spam blockers".

5.4.3 Utenze

Valgono i principi generali già introdotti nel paragrafo [rif. 5.1.1].

5.4.4 Autenticazione

Valgono i principi generali già introdotti nel paragrafo [rif. 5.1.2].

5.4.5 Autorizzazione

Valgono i principi generali già introdotti nel paragrafo [rif.5.1.3].

5.4.6 Crittografia

Ai principi generali introdotti nel paragrafo [rif. 5.1.1.4], si aggiungono le indicazioni, di cui di seguito:

Crittografia	
Minaccia	Accesso non autorizzato alle informazioni
Contromisure	Per l'accesso ai dati critici o sensibili definire requisiti di sicurezza più stringenti applicando tecniche di cifratura o altri meccanismi di sicurezza per rafforzare la protezione dagli accessi non autorizzati.

5.4.7 Documentazione

Valgono i principi generali già introdotti nel paragrafo [rif. 5.1.1.5].

5.4.8 Logging

Valgono i principi generali già introdotti nel paragrafo [rif. 5.1.1.6].

5.4.9 Procedure

Ai principi generali introdotti nel paragrafo [rif. 5.1.7], si aggiungono le indicazioni, di cui di seguito:

Politica per la gestione delle postazioni di lavoro	
Minaccia	- Abuso di privilegi da parte dell'utente. - Abuso di risorse. - Accesso non autorizzato ai sistemi (risorse di sistema, configurazioni, interfacce amministrative, ecc.). - Accesso non autorizzato alle informazioni. - Danneggiamento, perdita o furto di un asset fisico. - Uso non autorizzato di privilegi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (es. malware, ecc.) - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Verificare l'esistenza e l'applicazione di una formale politica di sicurezza che specifichi dei principi e delle linee guida per il corretto utilizzo delle postazioni di lavoro (workstation, desktop, notebook) da parte degli utenti, al fine di garantire la salvaguardia dell'informazione aziendale. Tale politica di sicurezza deve, nel rispetto della politica di sicurezza generale dell'azienda, specificare: - i requisiti di sicurezza fisica da soddisfare durante l'utilizzo dei dispositivi (ad

	esempio, il corretto posizionamento delle PdL); - i requisiti relativi alla corretta gestione della password, al backup, alla protezione contro i virus, alla configurazione del sistema operativo e delle applicazioni; - gli utilizzi non consentiti, estranei agli incarichi lavorativi, della propria postazione di lavoro; - i requisiti relativi al riutilizzo o alla rottamazione della PdL; - i requisiti relativi alla restituzione della PdL in caso di cessazione del rapporto di lavoro e/o cambio mansione. Eseguire delle attività di controllo e degli audit periodici sull'utilizzo della PdL da parte degli utenti, anche tramite tecnologie di controllo compatibili con quanto disposto dalle norme di legge.

Misure tecniche di garanzia di effettiva cancellazione dei dati o di loro non intellegibilità in caso di reimpiego o riciclo dell'apparecchiatura elettronica	
Minaccia	Accesso non autorizzato alle informazioni / ai dati personali contenuti in apparecchiature elettroniche dismesse.
Contromisure	Adottare misure tecniche che garantiscano la non intellegibilità dei dati o l'effettiva cancellazione. Le prime possono consistere, tra l'altro, nella cifratura di singoli file o gruppi di file, di volta in volta protetti con parole-chiave riservate, note al solo utente proprietario dei dati, che può con queste procedere alla successiva decifratura. La cancellazione sicura delle informazioni, è ottenibile mediante misure tecniche consistenti in: - utilizzo di programmi informatici (quali wiping program o file shredder); - demagnetizzazione (degaussing) dei dispositivi di memoria basati su supporti magnetici o magneto-ottici (dischi rigidi, floppy-disk, nastri magnetici); - distruzione fisica dei dispositivi di memoria dismessi.

Politica di protezione da accesso fisico non autorizzato	
Minaccia	- Accesso non autorizzato alle informazioni. - Danneggiamento, perdita o furto di un asset fisico. - Violazione della sicurezza (riservatezza, integrità, disponibilità) delle informazioni.
Contromisure	Deve essere adottata una politica di sospensione della sessione per inattività su PC e notebook che preveda almeno che i terminali: - non debbano essere lasciati incustoditi durante e fuori orario di lavoro; - siano protetti da accessi non autorizzati con la sospensione della sessione mediante un salva-schermo che richieda l'autenticazione per continuare. Le informazioni critiche, riportate su carta o su supporti informatici e i dispositivi critici quando non utilizzati, dovrebbero essere chiusi a chiave (in cassaforte o armadio o altri mobili con caratteristiche di sicurezza) soprattutto quando l'ufficio è vuoto. Devono essere adottate regole e accorgimenti per evitare il danneggiamento/ distruzione delle apparecchiature.

Sensibilizzazione del personale sui rischi di divulgazione di informazioni riservate	
Minaccia	- Divulgazione di informazioni riservate (codici di accesso). - Furto di credenziali di autenticazione.
Contromisure	Effettuare opere di sensibilizzazione nei confronti del personale perché non divulghi a terze parti informazioni riservate o critiche quali, ad esempio, dati personali e password.

5.5 Sicurezza dei Web Application Server

Il componente estende l'analisi sulla sicurezza dei sistemi informativi che adottano tecnologia web based.

5.5.1 Architettura

Isolamento dei sistemi critici	
Minaccia	Accesso non autorizzato alle informazioni
Contromisure	I sistemi critici come i Web Server devono avere un ambiente di elaborazione dedicato, strettamente controllato e monitorato. Tipicamente è necessaria una protezione perimetrale fisica (CED) e logica (firewall). Il web Server va collocato in un segmento di rete di front-end isolato tramite regole firewall dagli altri segmenti interni.

Failover	
Minaccia	Negazione dei servizi.
Contromisure	Prevedere meccanismi di failover del sistema. Ad es. alimentatori, ventole, schede di rete e hard disk devono essere in configurazione ridondata. I sistemi middleware più critici dal punto di vista della disponibilità devono utilizzare meccanismi di clustering applicativo. I sistemi di front-end web più critici per la disponibilità o particolarmente impegnati per un elevato numero di connessioni devono usare meccanismi di clustering applicativo oppure devono essere posti alle spalle di sistemi di bilanciamento del carico. In tutti i casi, in presenza di un fault di un sistema, deve essere presente un processo di controllo (watchdog) in grado di rilevare il fault, generare un alert verso i sistemi di monitoraggio e gestire il carico esistente attraverso gli altri sistemi, eventualmente attivando sistemi di riserva configurati in modalità "hot-standby".

Protezione dei servizi web	
Minaccia	Attacchi all'integrità dei sistemi (software e configurazioni).
Contromisure	Laddove sia necessario pubblicare in front-end web una serie di servizi che risiedono su molteplici server della rete interna, anziché esporre tutti questi server verso l'esterno è necessario invece installare un unico sistema di front-end opportunamente hardenizzato e posizionato su un segmento di rete dedicato, protetto dal firewall perimetrale e controllato da una sonda di intrusion detection. Tale sistema conterrà un servizio di "reverse proxy" o "portale" in grado di presentare in un'unica interfaccia l'insieme dei vari servizi interni, in modo controllato. Su tale sistema è necessario definire opportune politiche di controllo accessi e di autorizzazione, per consentire l'accesso alle varie sezioni del sito (corrispondenti ai diversi servizi interni) ai soli utenti autorizzati.

Sicurezza nelle connessioni nei sistemi web	
Minaccia	- Accesso non autorizzato alle informazioni. - Accesso non autorizzato al sistema. - Attacchi all'integrità dei sistemi (software e configurazioni). - Attacchi all'integrità delle informazioni.
Contromisure	L'eventuale reverse proxy o portale di front-end deve essere configurato in modo da

	concentrare l'accesso solo a determinati server interni senza consentire ad es. la manipolazione delle URL o dei parametri di una richiesta http POST in modo tale da ottenere una connessione verso un indirizzo arbitrario della intranet. In conformità al principio della defense-in-depth, il firewall che protegge tale sistema deve essere configurato in maniera puntuale per consentire unicamente le connessioni previste da internet verso il server e dal server verso gli altri server interni (indirizzi ip e porte dei soli server effettivamente previsti). In tal modo l'accesso al portale non deve permettere accessi non autorizzati a reti a cui il sistema è inter-connesso.

Controllo del traffico dati	
Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità delle informazioni. - (esempi: Zero-day exploit, Remote File Inclusion)
Contromisure	Impiegare un Web Application Firewall (WAF): - Il web application firewall consente il controllo di tutti i tipi di richiesta HTTP (URL, form, cookie, query string, hidden field e parametri). - L'impiego di una blacklist di URL referenziate consente al WAF di bloccare exploit basati su vulnerabilità applicative "zero-day" (portate lo stesso giorno in cui la vulnerabilità diventa nota).

Controllo del traffico dati	
Minaccia	Accesso non autorizzato alle informazioni - HTML Injection
Contromisure	Utilizzare un Web Application Firewall capace di monitorare la comunicazione tra gli utenti e l'applicazione e creare profili di interazioni HTML consentite.

Controllo del traffico dati	
Minaccia	- Furto di credenziali di autenticazione - Negazione del servizio
Contromisure	Attivare, a livello perimetrale, un dispositivo di sicurezza intelligente di tipo IDS (Intrusion Detection System) o IPS (Intrusion Prevention System) per individuare (IDS) la presenza di codice malevolo e bloccare (IPS) le intrusioni.

Comunicazioni sicure tra differenti Application Server	
Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità delle informazioni.
Contromisure	Quando un servizio web utilizza un'architettura distribuita, composta da server web di front-end e application server, ciascun server deve essere dotato di un certificato digitale e deve comunicare con gli altri in HTTPS attraverso TLS 1.2 o successivo. Sui sistemi maggiormente critici ed esposti come front-end su Internet, o usati per transazioni commerciali, la chiave privata deve essere custodita su un dispositivo hardware esterno (HSM).

5.5.2 Hardening

Hardening della piattaforma web	
Minaccia	- Abuso di privilegi - Abuso di risorse - Accesso non autorizzato alle informazioni

	- Accesso non autorizzato al sistema (macchina, configurazione, ecc.)
Contromisure	- Concedere al Web Server i privilegi minimi necessari per completare le operazioni richieste. In particolare dovrà utilizzare un account nominativo diverso da “root” o “administrator”. - Disabilitare gli script, le applicazioni d'esempio, i servizi, le utility non strettamente necessari ed ogni altra funzionalità non pertinente agli scopi della piattaforma web, proposti dalle configurazioni di base del web server. - Limitare l'accesso al file system da parte del web server separando la root directory e le directory virtuali dal resto del file system, facendole puntare su partizioni / mount dedicate. - Disattivare sul web server la possibilità di navigazione del file system. - Disabilitare il “Directory Listing”. - Proteggere con opportune ACL su file system, i file di configurazione e le directory contenenti i siti web i log del server, i suoi eseguibili e i suoi file temporanei. - Modificare i messaggi di sistema eliminando tutte le informazioni atte ad identificare il tipo di server, la versione e la build. - Isolare il servizio web dal sistema che lo ospita e da altri servizi web utilizzando tecniche di “jail” o “chroot”, oppure containers Docker o altre tecniche di virtualizzazione in grado di fornire un efficace isolamento. - Se l’application server lo consente, eseguirlo attraverso una sandbox per proteggere il codice da errori, trojans e codice malizioso (es. eseguire Apache Tomcat attraverso il Security Manager). - Proteggere l’accesso all’interfaccia di amministrazione dell’application server attraverso un firewall o una VPN, in modo da restringere tale accesso ai soli indirizzi IP e utenti autorizzati. Forzare inoltre l’interfaccia amministrativa all’utilizzo di TLS 1.2 o successivi escludendo il semplice http.

Hardening della piattaforma web	
Minaccia	- Accesso non autorizzato alle informazioni - Path traversal - Violazione della sicurezza, rispetto alle politiche di sicurezza dell’organizzazione - esecuzione arbitraria di codice
Contromisure	- Configurare l'application server in modo tale da rifiutare le URL con sequenze "../", al fine di impedire l'attraversamento di percorsi non protetti. - Bloccare i comandi e le utility di sistema con ACL restrittive.

Hardening della piattaforma web	
Minaccia	Negazione dei servizi.
Contromisure	- Configurare le applicazioni, i servizi e il sistema operativo tenendo sempre presente le possibili esposizioni ad attacchi DoS. - Assicurarsi che i criteri di blocco dell'account predisposti non possano essere sfruttati per bloccare service accounts ben noti. - Assicurarsi che il sistema sia in grado di gestire alti volumi di traffico e che le soglie siano opportunamente impostate per gestire carichi anormalmente elevati. - Configurare il sistema operativo e il server web in modo da evitare il rischio di esaurimento di risorse in presenza di un elevato numero di connessioni non completate (es. TCP SYN COOKIES su kernel Linux/Unix e configurazione opportuna dei timeout sul server web). - Su server web soggetti ad un elevatissimo numero di connessioni, utilizzare applicativi con logica RESTful di tipo connectionless, o affidare l’onere di gestire i parametri della sessione al client attraverso l’inclusione dei parametri di sessione

	in cookies cifrati e non predicibili né manipolabili lato client. - Alcuni Application Server e Web Server espongono semplici interfacce amministrative per lo shutdown remoto che devono essere disabilitate (es. Apache Tomcat sulla porta TCP 8005).

Hardening della piattaforma web	
Minaccia	- Accesso non autorizzato alle informazioni. - Compromissione delle comunicazioni. - Falsificazione di identità. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (Cross-site scripting, Clickjacking, Hijacking, ecc.).

Contromisure	Configurare sempre una dimensione massima accettabile per l'Header http.
	
	Inoltre, considerare l'adozione di http security headers. Di seguito i principali:
	
	- HttpOnly: istruisce il browser ad impedire che i cookies siano acceduti lato client a mezzo di script;
	- strict-transport-security: forza il browser a comunicare solo su HTTPS;
	- cache-control: impostato a "no-cache, no-store, must-revalidate" (laddove sono in gioco dati sensibili);
	- expires: impostato a 0 (laddove sono in gioco dati sensibili);
	- content-security-policy: definisce quali sono le sorgenti attendibili dei contenuti (script) e quindi caricabili dal browser;
	- x-xss-protection: abilita un filtro sul browser che previene i XSS di tipo reflected;
	- x-frame-options: mette al riparo da un particolare tipo di attacco: il "clickjacking". Di fatto impedisce agli iframes di caricare il sito;
	- public-key-pins: istruisce il browser di associare una opportuna public key con un certo web server. Ciò mette al riparo:
	  o da Man-In-The-Middle attack (tentato con un certificate falso) o
	  o dall'eventualità in cui la certification authority fosse compromessa.
	- x-content-type: impostato a nosniff: mette al riparo da un particolare tipo di attacco: il "mime based attacks". Di fatto impone al browser di attenersi rigorosamente al content type specificato (es. se il server imposta il content come text/html, il browser ne farà il rendering come text/html).
	- expect-ct: impedisce l'utilizzo di certificati emessi in modo errato, consentendo ai siti web di segnalare e, facoltativamente, di imporre i requisiti di trasparenza dei certificati. Quando questa intestazione è abilitata, il sito web richiede al browser di verificare se il certificato appare o meno nei log pubblici della CT[5] (Certificate Transparency).
	- Feature-policy: conferisce la possibilità di consentire o negare l'utilizzo delle funzioni del browser, sia nel proprio frame che nel contenuto di un elemento iframe (<iframe>).
	NB. Non tutti i browser supportano gli http security headers di cui sopra. Anche la scelta del browser è importante.

Hardening della piattaforma web	
Minaccia	Accesso non autorizzato alle informazioni - Remote File Inclusion (RFI)
Contromisure	L'utilizzo di blacklist di IP costruiti sulla base di osservazioni eseguite su avvenuti attacchi (es. di tipo RFI), potrebbero essere usati per bloccare altri tipi di attacchi

[5] https://www.certificate-transparency.org/known-logs

	portati dalla stessa origine. Ove possibile, limitare gli accessi a indirizzi IP o Reti specifiche.

Hardening della piattaforma web	
Minaccia	Crittografia debole o non validata.
Contromisure	Non consentire il fallback a SSL (qualsiasi versione) né a TLS 1.1 o versioni inferiori. Deve essere richiesto l'uso obbligatorio almeno di TLS 1.2.

Hardening della piattaforma web	
Minaccia	Divulgazione di informazioni riservate.
Contromisure	Rimuovere HTTP Response Headers che espongono informazioni sul web server. A titolo di esempio, in ambiente Microsoft, rimuovere: - Server– Specifica la versione del web server version. - X-Powered-By- Indica che il website è "powered by ASP.NET." - X-AspNet-Version- Specifica la versione di ASP.NET usata. Disabilitare il metodo HTTP TRACE. A titolo di esempio: - in ambiente Microsoft, impostare la chiave di registro "EnableTraceMethod" (sotto HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters) a 0 (zero) - in ambiente Apache, configurare "TraceEnable off" in http.conf. - In Apache Tomcat disabilitare l'attributo allowTrace per ogni connettore. Su Apache Tomcat disabilitare inoltre lo Stack Tracing sul client.

Hardening della piattaforma web	
Minaccia	Negazione dei servizi (Buffer overflows).
Contromisure	- Utilizzare linguaggi di programmazione che forniscono controlli automatici sulla dimensione dei buffer di memoria (o a tempo di compilazione o a runtime) come Java, Python o Perl. - Utilizzare le safe libraries (ad es. in C e C++), ovvero librerie di funzioni che implementano protezioni contro il buffer overflow quando tale protezione non è nativamente supportata dal linguaggio di programmazione. - Prevedere che sia il compilatore ad inserire le verifiche sulla dimensione di tutti i buffer nel codice compilato senza richiedere alcuna modifica al codice sorgente (a titolo di esempio, utilizzare il flag /GS per compilare codice sviluppato con Microsoft Visual C ++ ®. Il flag / GS fa sì che il compilatore inietti controlli di sicurezza nel codice compilato).

Integrità del software e dei dati nei sistemi web	
Minaccia	Attacchi all'integrità dei sistemi (software e configurazioni).
Contromisure	Il web server deve proteggere il software, i dati e le informazioni memorizzate sul sistema con meccanismi appropriati per garantire un alto livello di integrità attraverso l'uso di firma digitale o MAC (message authentication codes).

Hardening del sistema operativo che ospita la piattaforma web	
Minaccia	- Accesso non autorizzato al sistema. - Compromissione delle comunicazioni. - Furto di credenziali di autenticazione (es. keylogger). - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione. - Violazione di leggi, di regolamenti, di obblighi contrattuali.

Contromisure	Eseguire l'hardening del sistema operativo che ospita il Web Server [rif. 5.2.2].

5.5.3 Utenze

Valgono i principi generali già introdotti nel paragrafo [rif. 5.1.1].

5.5.4 Autenticazione

Valgono i principi generali già introdotti nel paragrafo [rif. 5.1.2].

5.5.5 Autorizzazione

A i principi generali già introdotti nel paragrafo [rif. 5.1.3], si aggiungono le seguenti indicazioni per il contesto specifico:

Autorizzazione	
Minaccia	- Accesso non autorizzato ai sistemi (macchina, configurazione, ecc.). - Accesso non autorizzato alle informazioni.
Contromisure	Utilizzare e configurare opportunamente i meccanismi di controllo di accesso alle risorse esposte dal web server (a titolo di esempio l'autorizzazione di accesso a livello di specifiche URL fornita dal Framework .NET).

5.5.6 Crittografia

Valgono i principi generali già introdotti nel paragrafo [rif. 5.1.4].

5.5.7 Documentazione

Valgono i principi generali già introdotti nel paragrafo [rif. 5.1.5].

5.5.8 Logging

Valgono i principi generali già introdotti nel paragrafo [rif. 5.1.6].

5.5.9 Sessioni

Contrasto delle riproduzioni di sessione	
Minaccia	- Accesso non autorizzato alle informazioni. - Compromissione delle comunicazioni. - Falsificazione di identità. - Uso non autorizzato di privilegi.
Contromisure	Verificare che siano adottate le seguenti best practices: - Utilizzare token di sessione (ad es. cookie o sessionID) difficilmente predicibili (ossia random) - Configurare l'applicativo web in modo che venga verificata la validità e l'integrità di ciascun token di sessione (ad es. cookie o sessionID) associato ad una richiesta di accesso.

	- Generare un nuovo identificativo di sessione dopo il login (per evitare il session fixation ossia che il session ID sia forzato dall'esterno). - Limitare il periodo di scadenza del token di sessione in modo da limitare il tempo disponibile per sferrare un attacco. - Utilizzare un protocollo di comunicazione cifrato (TLS 1.2 o successivo) per la creazione di un canale di comunicazione protetto, e configurare il protocollo in modo che i cookie di autenticazione transitino solo mediante connessione HTTPS; - Configurare il client web (browser) in modo da consentire di non archiviare i dati di sessione sulla postazione di lavoro; - Prevedere un meccanismo che imponga di terminare una sessione qualora ne venga avviata una nuova con le medesime credenziali di autenticazione della precedente. - Attivare un meccanismo per la disconnessione automatica delle sessioni di lavoro dopo un periodo di inattività inferiore ai 5 minuti.

Gestione delle informazioni segrete di autenticazione degli utenti	
Minaccia	- Accesso non autorizzato alle informazioni. - Crittografia debole o non validata. - Falsificazione di identità. - Uso non autorizzato di privilegi.
Contromisure	Mentre l'SSL/TLS protegge i cookie in rete, non impedisce loro di essere modificati nel computer del client. Per contrastare la minaccia di manipolazione dei cookie, crittografare i cookie utilizzando un HMAC.

5.5.10 Procedure

A i principi generali già introdotti nel paragrafo [rif. 5.1.7], si aggiungono le seguenti indicazioni per il contesto specifico:

Controlli sulla regolamentazione dell'uso del codice mobile per Web Server	
Minaccia	- Negazione dei servizi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione.
Contromisure	Controllare che nel caso in cui si sia concesso l'utilizzo del mobile code (codice, come Java Applet, che è trasmesso via rete e eseguito su una macchina remota, "a fianco" di altro mobile code, potenzialmente malevolo) non siano effettuate operazioni non autorizzate rispetto alla politica definita per l'utilizzo del codice mobile. In particolare, controllare il rispetto delle politiche riguardanti: - esecuzione del mobile code in un ambiente isolato logicamente; - blocco di ogni utilizzo di mobile code; - blocco della ricezione di mobile code dall'esterno; - attivazione di controlli crittografici per autenticare univocamente il mobile code. - rispetto delle security guidelines di programmazione sicura per il per mobile code.

Inventario piattaforma web	
Minaccia	- Attacchi all'integrità dei sistemi (software e configurazioni). - Errori di amministrazione dei sistemi. - Negazione dei servizi.
Contromisure	Mantenere un inventario aggiornato che evidenzi: - Le date di pubblicazione dei dati forniti dal servizio web; - La release software del servizio web con l'indicazione, nelle Release Notes, di tutte

	le modifiche introdotte (come nuove funzionalità, plug-in, etc.); - I sistemi su cui è implementato il servizio web; - L'owner o funzione responsabile dei servizi web e dei relativi sistemi.

Collaudo del servizio web	
Minaccia	- Accesso non autorizzato alle informazioni. - Uso non autorizzato di privilegi. - Negazione dei servizi.
Contromisure	Effettuare un collaudo del servizio web prima di renderlo operativo, a tal proposito: - Svolgere il test in un ambiente diverso da quello dello sviluppo; - Considerare, nelle specifiche di collaudo, le tipologie di browser maggiormente diffuse e le versioni più recenti; - Assicurarsi che durante la fase di testing siano predisposte verifiche mirate non solo alla componente funzionale ma si attui anche una mirata attività dedicata alle eventuali falle di sicurezza. A questo riguardo: • Utilizzare specifici software per il controllo della qualità del codice (analisi statica) che tenga conto dei princìpi di sicurezza della programmazione (SAST). • Utilizzare specifici software per l'analisi dinamica del codice (DAST).

Procedura di monitoraggio sull'uso del web server	
Minaccia	- Accesso non autorizzato ai sistemi (risorse di sistema, configurazioni, interfacce amministrative, ecc.). - Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi (software e configurazioni). - Negazione dei servizi.
Contromisure	Definire procedure che specifichino le modalità con cui monitorare il web server per garantirne la funzionalità e l'uso corretto. La procedura deve specificare cosa monitorare (ambito del monitoraggio) e quando eseguire l'audit rimanendo conformi ai requisiti di legge e alle policy in vigore nell'organizzazione. Gli aspetti da considerare sono: - accessi autorizzati, includendo dettagli quali: • user ID; • indirizzo IP del client; • data e ora degli eventi chiave; • i tipi di eventi; • indirizzo delle risorse accedute; - tutte le operazioni privilegiate, come: • l'uso di account privilegiati (supervisor, root, administrator); • avvio e arresto del sistema; • collegamento e scollegamento di dispositivi di input/output; - tentativi di accesso non autorizzato, come: • azioni degli utenti falliti o rifiutati; • azioni fallite o rifiutate che coinvolgono dati o altre risorse; • violazioni della policy di accesso e notifiche generate da gateway e firewall; • alert da sistemi di intrusion detection; - alert o avaria dei sistemi come: • alert o messaggi inviati alle console di amministrazione; • eccezioni dei log dei sistemi; • allarmi provenienti da sistemi di gestione della rete;

	• allarmi generati dai sistemi di controllo degli accessi; - cambiamenti o tentativi di cambiamento delle configurazioni di sicurezza del sistema. La procedura deve specificare la frequenza con cui effettuare l'audit ogni qual volta sussista la necessità e comunque non oltre il termine di 1 mese.

Rimozione delle vulnerabilità nei sistemi web	
Minaccia	- Accesso non autorizzato ai sistemi (risorse di sistema, configurazioni, interfacce amministrative, ecc.). - Accesso non autorizzato alle informazioni. - Negazione dei servizi.
Contromisure	- Il web server deve essere accuratamente testato prima che le informazioni siano rese disponibili affinché vulnerabilità e malfunzionamenti siano rimossi. - Aggiornamenti o patch rilevanti la sicurezza devono essere installati dove ritenuto necessario. Se aggiornamenti o patch sono indisponibili, devono essere adottate contromisure addizionali per la riduzione della vulnerabilità (massimizzare la difesa perimetrale) - Il web server deve essere soggetto ad una analisi delle vulnerabilità tramite strumenti automatici di vulnerability assessment e le vulnerabilità specifiche per la sicurezza ritenute critiche e riscontrate devono essere rimosse. - L'analisi delle vulnerabilità deve essere eseguita ogni qual volta sussista la necessità e comunque non oltre il termine di 1 mese.

Accordi con i fornitori di servizi internet per scoprire l'attacco	
Minaccia	- Negazione dei servizi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione.
Contromisure	Prevedere accordi contrattuali con il proprio Provider di servizi internet (Internet Service Provider "ISP") perché, soprattutto in fase di attacco in corso, sia possibile effettuare un'attività di tracciamento degli indirizzi di rete (IP) per tentare di individuare l'aggressore mediante un percorso a ritroso e provare a fermare l'attacco.

5.5.11 Programmazione e Configurazione

Convalida dell'input	
Minaccia	Accesso non autorizzato alle informazioni.
Contromisure	- Evitare di utilizzare parametri nella stringa di query che contengono dati sensibili o dati che possono in qualche modo influenzare la logica di protezione sul server. Utilizzare invece un identificativo di sessione per identificare il client e memorizzare sul server gli elementi sensibili nell'archivio di sessione. - Preferire l'utilizzo di HTTP POST piuttosto che HTTP GET per inviare form di dati. - Adottare un processo di serializzazione (anche noto come deflating o marshalling) in modo da convertire i dati in una sequenza di bit da trasmettere sulla rete - Crittografare i parametri passati nella query string. - Validare tutti i parametri di input al fine di garantire la conformità allo standard adottato in termini di lunghezza minima e massima consentita, range di valori numerici consentiti, sequenze di caratteri e patterns ammessi e se e quando sono consentiti valori nulli. - Utilizzare un meccanismo di Whitelisting nella validazione dei parametri di query.

Convalida dell'input	
Minaccia	Compromissione delle comunicazioni - Cross-site request forgery (CSRF)
Contromisure	- Aggiungere a ciascuna transazione un valore numerico casuale di lunghezza elevata (da usare come token). Tale valore allegato alla richiesta viene convalidato rispetto al valore dato per quella specifica sessione utente. Pertanto, un aggressore non potrà incorporare una URL che rappresenta una transazione valida nella pagina controllata dall'attaccante. Richiedere un'interazione umana aggiuntiva per le transazioni sensibili in forma di autenticazione ripetuta o risposta a CAPTCHA.

Convalida dell'input	
Minaccia	Compromissione delle comunicazioni - Manipolazione dell'intestazione HTTP
Contromisure	Non basare le decisioni di sicurezza sulle intestazioni HTTP. Ad esempio, non fidarsi di quanto riportato nell'intestazione "HTTP Referer" per determinare la provenienza di una richiesta in quanto facilmente falsificabile.

Convalida dell'input	
Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi - Negazione dei servizi. - (Ad es. per attacchi di injection ed esecuzione arbitraria di codice).
Contromisure	Configurare il web service in modo da garantire l'attuazione di specifici controlli dei dati in ingresso. In particolare determinare: - Il set di caratteri consentito; - La lunghezza minima e massima dei dati; - L'intervallo numerico (range) dei dati; - Quali valori sono ammessi; - Se è previsto il tipo "NULL"; - Se sono consentiti duplicati; - Il formato consentito dei nomi dei file, nel caso siano accettati come input, e verificarne la presenza nella gerarchia di directory dell'applicazione.

Convalida dell'input	
Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi - Negazione dei servizi. - (Ad es. con Cross-site scripting - XSS).
Contromisure	Eseguire una convalida completa dell'input. Il sistema deve garantire che l'input da query strings, i campi delle form e i cookie siano validi. Considerare tutti gli input da parte degli utenti come potenzialmente dannosi, pertanto è necessario filtrare o sanitizzare l'input lato server. Validare tutti gli input per valori validi noti e quindi rifiutare tutti gli altri input. Utilizzare espressioni regolari per convalidare i dati di input ricevuti tramite i campi di form HTML, cookie e query strings. Utilizzare le funzioni HTMLEncode e URLEncode per codificare qualsiasi output che contiene l'input dell'utente. Questo converte gli script eseguibili in HTML innocuo.

Convalida dell'input	
Minaccia	Negazione dei Servizi (Buffer overflows)
Contromisure	- Eseguire una convalida completa dell'input. Questa è la prima linea di difesa contro

	il buffer overflow. Sebbene possa esistere un bug nel processo che consente all'input atteso di sconfinare le aree di memoria allocate, gli input inattesi sono in genere la causa principale di questa vulnerabilità. Filtrare l'input convalidandolo per tipo, lunghezza, formato e range. - Quando possibile, limitare l'utilizzo di codice unmanaged (es. C, C++) da parte dell'applicazione e verificare accuratamente le API che usano codice unmanaged per garantire che l'input venga correttamente convalidato. - Esaminare i casi in cui il codice managed chiama API che usano codice unmanaged al fine di assicurare che solo parametri appropriati possano essere passati come parametri all'API. - Utilizzare specifici flag di compilazione del codice sorgente per verificare staticamente le formattazioni di stringhe e produrre eventuali avvisi di pericolo o di sospetto.

Convalida dell'input	
Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi - Negazione dei servizi. - (Ad es. da esecuzione arbitraria di codice).
Contromisure	- Evitate di utilizzare i nomi dei file come input dove possibile e utilizzare invece percorsi di file assoluti che non possono essere modificati dall'utente finale. Assicurarsi che i nomi dei file seguano gli standard di formato consentiti dal file system (se si deve accettare i nomi dei file come input) e convalidarli nel contesto dell'applicazione. Ad esempio, verificare che siano all'interno della gerarchia di directory dell'applicazione. - Assicurarsi che la codifica dei caratteri sia impostata correttamente per limitare il modo in cui l'input può essere rappresentato (canonicalizzazione).

Convalida dell'input	
Minaccia	Accesso non autorizzato alle informazioni (manipolazione dei campi di un Form).
Contromisure	Invece di utilizzare i campi nascosti di una form, utilizzare gli identificativi di sessione allo stato di riferimento mantenuto nell'archivio di stato lato server. Validate tutti i campi di input al fine di garantire la conformità allo standard adottato in termini di lunghezza minima e massima consentita, range di valori numerici consentiti, sequenze di caratteri e patterns ammessi e se e quando sono consentiti valori nulli. Utilizzare un meccanismo di Whitelisting nella validazione dei campi di input. Usare e configurare in modo appropriato un firewall per l'applicazione web in uso.

Convalida dell'input	
Minaccia	Accesso non autorizzato alle informazioni (HTML Injection).
Contromisure	Validare gli elementi HTML nel flusso HTTP in entrata che contiene i dati forniti dall'utente. Impiegando una convalida nativa dell'input dell'utente è possibile rimuovere qualsiasi sottostringa di sintassi HTML (come tag e link) dai contenuti testuali forniti dall'utente stesso.

Convalida dell'input	
Minaccia	Accesso non autorizzato alle informazioni (Path traversal).
Contromisure	Validare l'input proveniente dal browser web attraverso l'uso di white list. Verificare che non esistano file documentali facilmente raggiungibili o il cui percorso

	sia intuitivo (ad es., solo digitando l'url corretto). Mascherare il percorso dei file documentali memorizzati nelle applicazioni web (ad esempio, con la conversione in hash dei nomi dei file o la visualizzazione del percorso con sequenze di lettere e numeri) provvedendo ad inserirli all'interno di specifici repository, utilizzando percorsi di tipo semantico complessi non facilmente riproducibili nell'url.

Convalida dell'input	
Minaccia	Negazione dei servizi.
Contromisure	- Validare l'input proveniente dal browser web attraverso l'uso di white list. - Valutare accuratamente tutti i dati di input sul server. - Gestire le eccezioni nel codice dell'applicazione.

Personalizzazione dei messaggi di errore del web server	
Minaccia	Divulgazione di informazioni riservate (Attacchi che rivelano dettagli implementativi).
Contromisure	Gestire le eccezioni nel codice dell'applicazione. Codificare e registrare le eccezioni che possono essere propagate all'esterno dell'applicazione. In caso di eccezione, restituire al client messaggi di errore generici (ad es., 404 Not Found, 408 Request Timeout) e/o codificati che non rivelino dettagli interni del sistema.

Password in memoria RAM	
Minaccia	Divulgazione di informazioni riservate (Memory dump attack).
Contromisure	Il Web Server deve utilizzare le password hash invece di memorizzare il testo delle password in chiaro. Il Web Server può utilizzare la Tokenizzazione in modo che solo i dati rappresentativi saranno in memoria mentre i dati sensibili vengono memorizzati altrove; I Web Server basati su .NET e su Java possono utilizzare il tipo SecureString/GuardedString per limitare il tempo in cui le password non crittografate sono disponibili in memoria.

5.6 Sicurezza dei DBMS/Database Server

5.6.1 Architettura

Isolamento dei sistemi critici	
Minaccia	Accesso non autorizzato alle informazioni
Contromisure	I sistemi critici come i DBMS devono avere un ambiente di elaborazione dedicato, strettamente controllato e monitorato. Per tali sistemi vale quanto segue: - Devono essere posti su un sistema dedicato che ospita solo il DB (e non ad es. un Web Server, un Application Server, un Directory Server e o altri servizi importanti). - Devono essere posti su un "layer dati" (segmento) di rete diverso da quello dei sistemi di front-end e da quello delle postazioni di lavoro client. - I diversi layer di rete devono essere posti su interfacce diverse di un firewall - Il firewall deve consentire unicamente le comunicazioni strettamente necessarie da e per i DB rispetto agli altri sistemi (Web Server, Application Server, client interni). - Non deve essere consentita dai firewall nessuna connessione diretta da internet o

	altre reti esterne all'organizzazione, verso il layer dati che ospita i DBMS.

Firewall per il server di database	
Minaccia	Accesso non autorizzato alle informazioni
Contromisure	I sistemi critici come i DBMS devono essere protetti da firewall opportunamente configurati. Per tali sistemi vale quanto segue: - Il server del database deve essere posizionato dietro un firewall le cui regole predefinite sono impostate per negare tutto il traffico. - Il firewall del server del database deve essere aperto solo a specifiche applicazioni o server web, e le regole del firewall non devono consentire l'accesso diretto da parte dei client. Se l'ambiente di sviluppo non può soddisfare tale requisito, in tal caso quei dati con particolari restrizioni non devono essere memorizzati nel server del database di sviluppo utilizzando in sostituzione dati falsi. La scelta di offuscare eventualmente i dati reali di produzione non sarebbe sufficiente, pertanto viene sconsigliata. - Adottare le opportune procedure di controllo riguardo le modifiche apportate alle regole dei firewall notificando le modifiche alle regole agli amministratori di sistema (SA) e agli amministratori di database (DBA). - Le regole Firewall per i server di database devono essere regolarmente manutenute e revisionate dai SA e dai DBA. Tali regole devono essere regolarmente riesaminate anche dall'Ufficio per la sicurezza delle informazioni. - Verificare regolarmente i criteri di hardening delle macchine e le regole dei firewall tramite scansioni di rete, o consentendo scansioni da parte dell'ufficio per la sicurezza delle informazioni attraverso il firewall.

Failover	
Minaccia	Negazione dei servizi.
Contromisure	Prevedere meccanismi di failover del sistema DB per i database più critici dal punto di vista della disponibilità del servizio. In tali casi, è necessario utilizzare architetture DBMS in cluster applicativi, scegliendo se possibile i sistemi di clustering nativi dello specifico prodotto piuttosto che soluzioni di terze parti. Quando un DBMS del cluster va in fault, un processo di controllo (watchdog) deve rilevare il problema, generare un alert verso i sistemi di monitoraggio e ripartire il carico di lavoro sui sistemi restanti, eventualmente attivando sistemi di riserva posti in configurazione "hot-standby". Il cluster deve essere in grado di salvaguardare l'integrità dei dati dal punto di vista delle transazioni, attraverso opportuni meccanismi di replica in grado di avere i dati sempre coerenti rispetto all'ultima operazione di "commit" eseguita.

Controllo del traffico dati	
Minaccia	- Accesso non autorizzato ai sistemi. - Negazione dei servizi.
Contromisure	Attivare, a livello perimetrale, un dispositivo di sicurezza intelligente di tipo IDS (Intrusion Detection System) o IPS (Intrusion Prevention System) per individuare (IDS) la presenza di codice malevolo e bloccare (IPS) le intrusioni.

5.6.2 Hardening

Hardening della piattaforma DBMS	
Minaccia	- Accesso non autorizzato alle informazioni. - Accesso non autorizzato ai sistemi. - Negazione dei servizi. - Uso non autorizzato di privilegi.
Contromisure	Concedere al DBMS i privilegi minimi necessari per completare le operazioni richieste. In particolare i processi del DB devono essere eseguiti sul sistema nel contesto di una utenza non privilegiata (diversa da root/Administrator e dotata dei privilegi minimi necessari). Disinstallare o disabilitare tutte le componenti opzionali / aggiuntive del DBMS non strettamente necessarie (es. Reporting Services, Debugging, interfacce amministrative, servizi di replica o backup, servizi di ricerca Full Text, interfacce web o Web Services, ecc.). Prestare particolare attenzione a quelle componenti aggiuntive che espongono servizi o interfacce amministrative su specifiche porte TCP/IP. Rimuovere gli "schema" e i DB di default presenti al termine dell'installazione standard e non utilizzati. Dopo la creazione del database, rimuovere gli eventuali script utilizzati per la creazione o, come minimo, spostarli su un repository "sicuro" (quanto meno dotato di controllo accessi) ed esterno al sistema. Quando si avviano processi o tools legati al DBMS, evitare di fornire a linea di comando informazioni sensibili quali ad es. username e password o chiavi crittografiche, perché tali parametri possono essere visualizzati da tutti gli utenti del sistema, anche in remoto, esaminando l'elenco dei processi in esecuzione. Analogamente, tali informazioni non devono essere memorizzate neppure in variabili d'ambiente né come testo in chiaro in file batch, ma piuttosto fornite a mano dall'operatore, o memorizzate in file di configurazione crittografati o come minimo offuscati. I file temporanei prodotti dal processo di installazione che possono contenere password devono essere rimossi.

Hardening della piattaforma DBMS	
Minaccia	Abuso di risorse.
Contromisure	Disabilitare gli script, le applicazioni d'esempio, le utility non strettamente necessari ed ogni altra funzionalità non pertinente agli scopi della piattaforma DBMS, proposti dalle configurazioni di base del DBMS.

Protezione delle informazioni strumentali all'accesso	
Minaccia	Accesso non autorizzato ai sistemi.
Contromisure	Non utilizzare nomi di account predefiniti e rinominare account standard come l'account amministratore del DB. Non utilizzare password nulle. Tutti gli accessi al sistema operativo e ai server di database, avvenuti con o senza successo, devono essere registrati. I log contenenti tali informazioni devono essere conservati per almeno un anno. Gli oggetti del database contenenti dati con particolari restrizioni, lì dove tecnicamente possibile, devono essere predisposti per l'auditing. I dati di log devono essere regolarmente esaminati da persone esperte e indipendenti designate dal titolare dei dati per soddisfare le proprie esigenze. Tali requisiti e il processo di revisione devono essere ben documentati. Eseguire l'Audit degli accessi non andati a buon fine per intercettare tentativi di indovinare le password.

Accesso a dati sensibili su memoria di massa	
Minaccia	Accesso non autorizzato alle informazioni.
Contromisure	Utilizzare ACL restrittive per tutti i data stores e in particolare per quelli che contengono dati sensibili. Memorizzare i data store che contengono dati sensibili o comunque riservati su file system crittografati.

Hardening della piattaforma DBMS	
Minaccia	Negazione dei servizi.
Contromisure	Configurare le applicazioni, i servizi e il sistema operativo che compongono / ospitano il DBMS, tenendo sempre presente le possibili esposizioni ad attacchi DoS. Assicurarsi che i criteri di blocco dell'account predisposti non possano essere sfruttati per bloccare account di servizio ben noti. Assicurarsi che il DBMS sia in grado di gestire alti volumi di traffico e che le soglie siano opportunamente impostate per gestire carichi anormalmente elevati.

Hardening del sistema operativo che ospita il DBMS	
Minaccia	- Accesso non autorizzato al sistema. - Compromissione delle comunicazioni. - Furto di credenziali di autenticazione (es. keylogger). - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione.
Contromisure	Eseguire l'hardening del sistema operativo che ospita il DBMS. L'hardening del sistema operativo è oggetto di un paragrafo specifico [rif. 5.2.2].

Patching del DBMS	
Minaccia	- Accesso non autorizzato al sistema. - Accesso non autorizzato alle informazioni. - Compromissione delle comunicazioni. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione.
Contromisure	Eseguire il patching iniziale (prima di mettere in uso i sistemi DBMS) e successivamente in maniera regolare e periodica, installando tutti gli aggiornamenti suggeriti e di sicurezza rilasciati dal produttore. Verificare che la versione del software del database sia attualmente supportata dal fornitore o dal progetto open source, come richiesto dagli standard minimi di sicurezza. Il software del database deve essere aggiornato per includere tutte le patch di sicurezza ultime. Predisporsi per applicare le nuove patch di sicurezza in modo tempestivo.

Disabilitazione delle interazioni con il sistema operativo	
Minaccia	- Accesso non autorizzato al sistema. - Attacchi all'integrità dei sistemi (software e configurazioni). - Compromissione delle comunicazioni. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione.
Contromisure	Molti DBMS, tra cui Microsoft SQL Server (attraverso alcune Extended Stored Procedure come *xp_cmdshell*, *xp_dirtree*, *xp_servicecontrol*, ecc.) e Oracle (con altri meccanismi) consentono di interagire in modo molto stretto con il sistema operativo, ad es. richiamando eseguibili sul sistema, navigando sul file system, avviando/arrestando servizi o eseguendo altre operazioni anche privilegiate. Tali meccanismi, quando non effettivamente necessari, devono essere disabilitati.

5.6.3 Utenze

Valgono i principi generali già introdotti nel paragrafo [rif. 5.1.15.1.1].

5.6.4 Autenticazione

Valgono i principi generali già introdotti nel paragrafo [rif. 5.1.2].

5.6.5 Autorizzazione

A i principi generali già introdotti nel paragrafo [rif. 0], si aggiungono le seguenti indicazioni per il contesto specifico:

Autorizzazione	
Minaccia	Accesso non autorizzato alle informazioni.
Contromisure	Utilizzare e configurare opportunamente i meccanismi di controllo di accesso alle risorse (tabelle, viste, procedure, ecc.) gestite dal DBMS (a titolo di esempio l'istruzione "grant" fornita da Oracle), fornendo a ciascun utente o utenza applicativa i minimi diritti effettivamente necessari al corretto funzionamento, secondo il principio del *least privilege*. Ad es., evitare l'accesso di un application server al DBMS con utenza di amministratore globale del database, anche quando un utente non privilegiato deve effettuare compiti di ordinaria operatività.

5.6.6 Crittografia

Ai principi generali già introdotti nel paragrafo [rif. 5.1.4], si aggiungono le seguenti indicazioni per il contesto specifico:

Protezione delle informazioni riservate	
Minaccia	- Crittografia debole o non validata. - Accesso non autorizzato alle informazioni.
Contromisure	- Per la protezione delle informazioni riservate custodite nel database, all'interno di campi specifici di tabelle specifiche, utilizzare tecniche di crittografia dei dati a livello di colonna fornite nativamente dallo specifico DBMS, evitando l'uso di soluzioni custom o di terze parti, evitando così tutta una serie di problemi che possono sorgere (ad es. quando la colonna cifrata è parte di un indice: in tal caso solitamente si indicizza il valore cifrato anziché quello in chiaro); - Per la protezione delle informazioni riservate custodite nel database, all'interno di righe specifiche di una tabella, utilizzare tecniche di crittografia dei dati a livello di riga fornite nativamente dallo specifico DBMS, evitando l'uso di soluzioni custom o di terze parti; - In presenza di dati particolarmente sensibili, valutare se vi sia davvero la necessità di custodirli all'interno del DBMS, e in caso contrario, evitare la loro memorizzazione permanente; - I dati sensibili presenti sui DBMS di produzione non devono mai essere trasferiti su sistemi di sviluppo, test e collaudo, se non dopo essere stati sottoposti ad un

	processo di “anonimizzazione” o “tokenizzazione”.

Protezione delle informazioni strumentali all'accesso	
Minaccia	Crittografia debole o non validata. Accesso non autorizzato alle informazioni.
Contromisure	Per la memorizzazione sicura delle chiavi applicative di accesso e/o di cifratura utilizzare funzionalità o prodotti di tipo “wallet” native o aggiuntive ma comunque certificate dal vendor dello specifico database.

5.6.7 Documentazione

Valgono i principi generali già introdotti nel paragrafo [rif. 5.1.5].

5.6.8 Logging

Valgono i principi generali già introdotti nel paragrafo [rif. 5.1.6].

5.6.9 Sessioni

Protezione delle sessioni di lavoro	
Minaccia	Accesso non autorizzato alle informazioni.
Contromisure	Attivare un meccanismo per la disconnessione automatica delle sessioni di lavoro dopo un periodo di inattività inferiore ai 5 minuti

5.6.10 Procedure

Ai principi generali già introdotti nel paragrafo [rif. 5.1.7], si aggiungono le seguenti indicazioni per il contesto specifico:

Limitare e controllare l'uso dei programmi di utilità	
Minaccia	Accesso non autorizzato ai sistemi.
Contromisure	Limitare e tenere sotto controllo l'uso di programmi di utilità, considerando le seguenti linee guida: - utilizzo di procedure di identificazione, autenticazione e autorizzazione per i programmi di utilità; - limitazione della disponibilità e tracciamento di tutti gli utilizzi dei programmi di utilità; - rimozione o disabilitazione di tutti i programmi di utilità non necessari.

Tecniche di programmazione SQL sicura e protezione degli accessi	
Minaccia	- Accesso non autorizzato alle informazioni. - Cancellazione o furto di informazioni.
Contromisure	Alcuni prodotti di mercato (es. Oracle Database 12c) forniscono un “database firewall” specializzato per monitorare le istruzioni SQL dirette al DBMS. Ciò corrobora le best practices di programmazione sicura, difendendo il DBMS da vari tipi di attacchi.

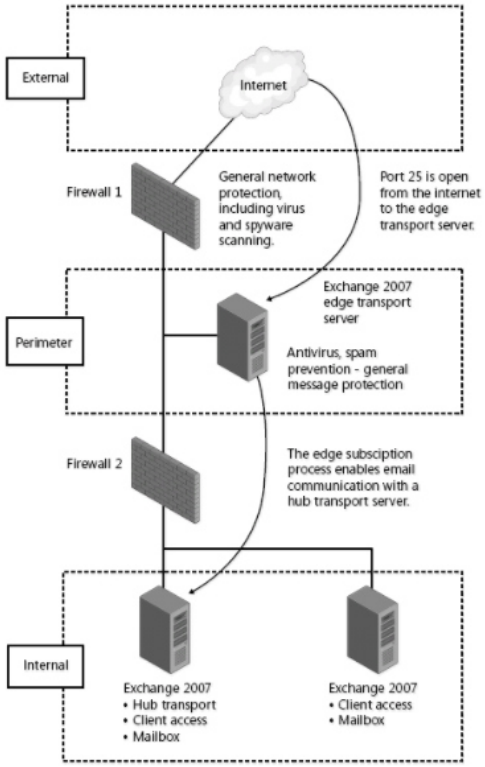
5.6.11 Informazioni addizionali

Riferimenti

Oracle Database 12c	Per informazioni aggiornate sulle impostazioni di protezione e privacy per Oracle Database 12c, scaricare il documento: http://www.oracle.com/us/products/database/securing-oracle-database-primer-2522965.pdf.
Microsoft SQL Server 2012	Per informazioni aggiornate sulle impostazioni di protezione e privacy per Microsoft SQL Server 2012, visitare il sito: https://docs.microsoft.com/en-us/sql/relational-databases/security/securing-sql-server.

5.7 Sicurezza del Mail Server

5.7.1 Architettura

Isolamento dei sistemi critici	
Minaccia	Accesso non autorizzato alle informazioni
Contromisure	I sistemi critici come il Mail Server devono avere un ambiente di elaborazione dedicato, strettamente controllato e monitorato. Tipicamente è necessaria una protezione perimetrale fisica (CED) e logica (firewall). Occorrono in linea di principio: - un SMTP server hardenizzato collocato in DMZ che si limita ad accettare le connessioni in ingresso provenienti da Internet, con funzione di "relay"; - uno o più mail server interni anch'essi opportunamente messi in sicurezza (vedi best practices successive) a cui l'SMTP server in DMZ inoltra (relay) le mail ricevute dall'esterno e da cui riceve quelle provenienti dall'interno. Inoltre si può considerare di installare un Application Layer inspection firewall a protezione del server SMTP in DMZ. Si consideri, a titolo di esempio, il seguente schema (con 2 firewall) in ambiente Microsoft:  [Fonte: https://msdn.microsoft.com/en-us/library/cc505927.aspx]

Failover	
Minaccia	Negazione dei servizi.
Contromisure	Prevedere meccanismi di failover dei sistemi di posta elettronica.

Controllo del traffico dati	
Minaccia	- Accesso non autorizzato alle informazioni. - Compromissione delle comunicazioni. - Negazione dei servizi.
Contromisure	Attivare, a livello perimetrale, un dispositivo di sicurezza intelligente di tipo IDS (Intrusion Detection System) o IPS (Intrusion Prevention System) per individuare (IDS) la presenza di codice malevolo e bloccare (IPS) le intrusioni.

Hardening del MailServer	
Minaccia	- Accesso non autorizzato alle informazioni. - Accesso non autorizzato ai sistemi. - Negazione dei servizi.
Contromisure	Concedere al Mail Server i privilegi minimi necessari per completare le operazioni richieste. In particolare i processi del server devono essere eseguiti nel contesto di una utenza non privilegiata.

Hardening del MailServer	
Minaccia	- Accesso non autorizzato ai sistemi. - Compromissione delle comunicazioni.
Contromisure	Customizzare opportunamente le configurazioni di base del mail server. In particolare, cambiare i nomi degli account di default e degli alias pre-definiti.

Hardening del MailServer	
Minaccia	Negazione dei servizi.
Contromisure	Configurare le applicazioni, i servizi e il sistema operativo tenendo sempre presente le possibili esposizioni ad attacchi DoS. Assicurarsi che i criteri di blocco dell'account predisposti non possano essere sfruttati per bloccare service accounts ben noti. Assicurarsi che il sistema sia in grado di gestire alti volumi di traffico e che le soglie siano opportunamente impostate per gestire carichi anormalmente elevati.

Hardening del MailServer	
Minaccia	- Compromissione delle comunicazioni. - Negazione dei servizi.
Contromisure	L'utilizzo di black-list di IP/indirizzi mail costruite sulla base di osservazioni su attacchi avvenuti in passato, può ridurre notevolmente i rischi derivanti da attacchi di vario tipo (es. spam). Tali liste sono disponibili in internet oppure sono incluse in prodotti commerciali di protezione dei mail server. Ove possibile, limitare gli accessi a indirizzi IP/indirizzi mail presenti in queste black-list.

Hardening del MailServer	
Minaccia	Divulgazione di informazioni riservate.

Contromisure	Configurare opportunamente i messaggi prodotti dal mail server (messaggi di Hello, risposte automatiche ad es. per i messaggi non consegnabili, messaggi di errore, funzionalità diagnostiche, ecc.) in modo da non rivelare nessuna informazione ad un eventuale aggressore, quali ad es. indirizzi email degli amministratori o di altri utenti o di caselle di risposta automatica, versione del software, ecc. Infatti un malintenzionato potrebbe indurre il sistema in errore per ottenere indirizzi email validi da usare ad es. in una campagna di phishing o spamming.

Hardening del MailServer	
Minaccia	- Accesso non autorizzato ai sistemi (risorse di sistema, configurazioni, interfacce amministrative, ecc.). - Attacchi all'integrità dei sistemi (software e configurazioni). - Furto di credenziali di autenticazione (es. keylogger). - Negazione dei servizi. - Tentativi di frode. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (es. malware, ecc.). - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Filtrare gli Attachments. Installare un software antivirus e implementare filtri per bloccare attachment sospetti o potenzialmente pericolosi.

Hardening del MailServer	
Minaccia	- Accesso non autorizzato alle informazioni. - Compromissione delle comunicazioni.
Contromisure	Utilizzare solo protocolli sicuri per l'accesso alla posta elettronica: - Client POP3: Solo se si utilizza con SSL/TLS, altrimenti usare IMAP4. - Client IMAP4: Configurare sempre l'uso di SSL/TLS. - Server SMTP: Configurare sempre l'uso di SSL/TLS. Utilizzare solo TLS 1.2, evitando SSL e le versioni precedenti di TLS, in quanto vulnerabili a diverse tipologie di attacchi.

Hardening del MailServer	
Minaccia	- Accesso non autorizzato alle informazioni. - Compromissione delle comunicazioni.
Contromisure	Webmail Access. Se il MailServer supporta la Webmail, è necessario adottare tutte le misure di sicurezza previste nel presente documento per i server web. In particolare però il server di webmail deve obbligatoriamente utilizzare HTTPS con TLS 1.2 o superiore, per l'intera durata della sessione.

Hardening del MailServer	
Minaccia	Negazione dei servizi.
Contromisure	Limitare sempre la dimensione massima dei messaggi e degli attachments sia per i messaggi in ingresso sia per quelli in uscita, utilizzando valori considerati accettabili per l'organizzazione. Ciò protegge da situazioni potenzialmente pericolose (degrado prestazioni, crash, esaurimento disco, SPAM e attacchi DOS verso terzi) in cui messaggi con allegati di grandi dimensioni sono inviati a molteplici destinatari. Configurare anche un numero massimo ragionevole di destinatari per i messaggi in uscita o in fase di relay. Configurare una dimensione massima ragionevole per le mailbox degli utenti e per le

	cartelle pubbliche / condivise.

Hardening del MailServer	
Minaccia	- Divulgazione di informazioni riservate. - Negazione dei servizi (Spam).
Contromisure	Disabilitare il comando "VRFY" (che consente di verificare se un account di email esiste sul server).

Hardening del MailServer	
Minaccia	Negazione dei servizi.
Contromisure	Limitare il numero di messaggi di posta elettronica per minuto o per ora che un server può ricevere, legittimare o altro.

Hardening del MailServer	
Minaccia	- Attacchi all'integrità dei sistemi. - Negazione dei servizi.
Contromisure	Il mobile code può essere scaricato ed eseguito su PC utente anche via email. Oltre al download via attachment (ad esempio: macro in un file Word), si consideri anche il caso di body HTML della mail (ad esempio: JavaScript). In generale, a livello di mail client occorre: - Assicurarsi che il "reading pane", se presente, non attivi script e/o apra attachment automaticamente; - Bloccare contenuti esterni in HTML (es. immagini o altri elementi multimediali).

Hardening del sistema operativo che ospita il Mail Server	
Minaccia	- Accesso non autorizzato alle informazioni. - Accesso non autorizzato al sistema. - Compromissione delle comunicazioni. - Furto di credenziali di autenticazione (es. keylogger). - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Eseguire l'hardening del sistema operativo che ospita il Mail Server [rif. 5.2.2].

5.7.2 Utenze

Valgono i principi generali già introdotti nel paragrafo [rif. 5.1.1].

5.7.3 Autenticazione

Valgono i principi generali già introdotti nel paragrafo [rif. 5.1.2].

5.7.4 Autorizzazione

A i principi generali già introdotti nel paragrafo [rif. 5.1.3], si aggiungono le seguenti indicazioni per il contesto specifico:

Autorizzazione	
Minaccia	Negazione dei servizi.

Contromisure	- Attivare la “Relaying Protection” in modo che solo gli utenti identificati ed autorizzati possano collegarsi per l’invio di email. Disabilitare il funzionamento come "open relay". - Configurare inoltre il server in modo da accettare (in ingresso) o effettuare il relay (in uscita) solo per le email rispetto alle quali è autoritativo (per il dominio) e solo da e per caselle di posta effettivamente esistenti all’interno dell’organizzazione. - Infine quando il server è un relay host (il cui compito è di inoltrare i messaggi ad un altro SMTP server), utilizzare sempre l’autenticazione per la connessione tra i diversi server SMTP dell’architettura, utilizzando su ogni host il TLS 1.2 o successivo.

5.7.5 Crittografia

Ai principi generali già introdotti nel paragrafo [rif. 5.1.4], si aggiungono le seguenti indicazioni per il contesto specifico:

Protezione delle informazioni strumentali all'accesso	
Minaccia	- Attacchi all’integrità delle informazioni. - Compromissione delle comunicazioni. - Divulgazione di informazioni riservate. - Falsificazione di identità.
Contromisure	A livello di client mail, si tengano presenti: - L’utilizzo di meccanismi per la protezione dell'integrità e dell’autenticità delle informazioni trasmesse e/o ricevute via e-mail che prevedano utilizzo di strumenti crittografici, quali ad esempio la firma digitale. - L’utilizzo di meccanismi per la protezione della confidenzialità delle informazioni trasmesse e/o ricevute via e-mail eseguendo la cifratura dei messaggi end-to-end (cioè a livello dei client), con strumenti idonei ammessi dalla politica aziendale.

5.7.6 Documentazione

Valgono i principi generali già introdotti nel paragrafo [rif. 5.1.5].

5.7.7 Logging

Valgono i principi generali già introdotti nel paragrafo [rif. 5.1.6].

5.7.8 Anti-Phishing

Software anti-phishing	
Minaccia	- Attacchi all’integrità dei sistemi. - Furto di credenziali di autenticazione. - Negazione dei servizi.
Contromisure	Mail Server: Installare sul Mail Server un modulo aggiuntivo anti-phishing che aggiorni il proprio database delle “firme” (pattern riconosciuti come pericolosi) almeno una volta al giorno. Mail Client: Prevedere per i client di posta aziendali, come Microsoft Outlook, un modulo aggiuntivo con il quale possano essere rilevati i collegamenti sospetti di un e-mail. Webmail: Utilizzare un browser recente e aggiornato, dotato di funzionalità di filtro

	anti-phishing native, o in alternativa utilizzare un software anti-malware dotato di estensioni anti-phishing per i browser adottati dall'organizzazione.

5.7.9 Anti-Spam

Software anti-Spam	
Minaccia	Negazione dei servizi.
Contromisure	Installare sul Mail Server un software anti-spam che aggiorni il proprio database delle "firme" almeno una volta al giorno. Il software deve avere la funzione di auto-apprendimento in modo da incrementare l'accuratezza del filtraggio, e deve eseguire il filtraggio dei messaggi sospetti mediante analisi di tipo: - Semantico, ovvero la rilevazione in base a parole chiavi (ad es. Viagra, sesso, Prozac, etc.); - Euristico, ovvero individuare la posta ricevuta con comportamento anomalo (ad esempio con un numero insolitamente elevato di destinatari, con l'assenza dell'indirizzo del mittente o con l'indirizzo del mittente identico a quello del destinatario). Inoltre il software deve usare una specifica tecnica di blocco dei messaggi sospetti in base al mail server di provenienza come, ad esempio, la tecnica DNSBL (DNS-based Blackhole Lists) che si avvale dell'ausilio di una lista pubblicata su internet, che viene manutenuta costantemente da terze parti ed in cui sono elencati i servers che favoriscono lo spam (ad es. server SMTP Open Relay, server che emettono spam, ISP che supportano lo spam, etc.).

5.7.10 Procedure

A i principi generali già introdotti nel paragrafo [rif. 5.1.7] (i principi generali si applicano sia ai MailServer quanto che ai Mail Client), si aggiungono le seguenti indicazioni per il contesto specifico:

Uso corretto della posta elettronica	
Minaccia	- Abuso di risorse. - Attacchi all'integrità dei sistemi. - Compromissione delle comunicazioni. - Furto di credenziali di autenticazione.
Contromisure	- Evitare l'uso dell'e-mail a fini diversi da quelli strettamente aziendali (ad esempio, per iscriversi a mailing list, forum, chat, blog, etc.) che non siano attinenti alla funzione svolta. - Non cliccare mai direttamente su un link presente in una e-mail per accedere a un sito web contenente informazioni sensibili. Copiare e incollare il testo del collegamento in una nuova finestra del browser e verificare l'URL per assicurarsi che la sessione inizi dall'indirizzo autentico conosciuto del sito, senza che vengano aggiunti altri caratteri. - Controllare che la pagina web del sito dell'eventuale istituto creditizio a cui conduce un link presente in una e-mail, disponga di un certificato digitale attendibile, ovvero appartenente al legittimo proprietario, e che tale certificato sia ancora valido. Ad esempio, nelle versioni più recenti di diversi browser comunemente disponibili è sufficiente cliccare con il pulsante destro del mouse in un punto qualsiasi della finestra del browser e selezionare "Proprietà" dal menu a comparsa, dopo aver visualizzato la finestra "Proprietà", occorre cliccare su "Certificati" per controllarne la validità ed attendibilità.

Sensibilizzazione del personale sui rischi di infezione da malware	
Minaccia	- Attacchi all'integrità dei sistemi. - Furto di credenziali di autenticazione. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (malware).
Contromisure	Sensibilizzare il personale sui rischi di infezione da malware. Ad esempio, informare sui rischi derivanti dal phishing/pharming (divulgazione a terze parti d'informazioni riservate o critiche quali, ad esempio, dati personali, password, numeri di conto o carta di credito) sui sintomi di infezione e sulla protezione di PC e dispositivi portatili. Istruire il personale sulle norme di comportamento cui attenersi per diminuire i rischi di phishing/pharming. Tali norme dovrebbero, almeno, indicare di: - non fare affidamento sull'intuito per distinguere tra richieste legittime e illegali di informazioni riservate; - non consegnare mai informazioni personali o riservate a individui o aziende sconosciuti; eliminare messaggi e-mail che richiedono informazioni riservate. Se la richiesta appare legittima, verificatene telefonicamente l'autenticità; - non disabilitare le protezioni aziendali antivirus, anti-phishing/pharming o altre misure di sicurezza (ad esempio quelle del browser); - contattare l'assistenza IT nel caso di comunicazioni ricevute per e-mail, telefono, fax o messaggistica immediata, che richiedono informazioni aziendali o personali.

Procedura di monitoraggio sull'uso del mail server	
Minaccia	- Abuso di risorse. - Negazione dei servizi.
Contromisure	Definire procedure che specifichino le modalità con cui monitorare il mail server per garantirne la funzionalità e l'uso corretto. La procedura deve specificare cosa monitorare (ambito del monitoraggio) e quando eseguire l'audit rimanendo conformi ai requisiti di legge e alle politiche aziendali. Un monitoraggio di base dovrebbe considerare i carichi medi del traffico email e delle risorse del sistema: analizzando in tempo reale tali parametri e le loro deviazioni rispetto ai valori attesi, si possono trovare indizi di problemi e attacchi. La procedura deve specificare la frequenza con cui effettuare i controlli ogni qual volta sussista la necessità (non meno di una volta al giorno).

Accordi con i Service Provider	
Minaccia	Negazione dei servizi.
Contromisure	Considerare le seguenti linee guida per i contratti con i service provider di posta elettronica: - stabilire livelli di servizio garantiti, accettabili per l'organizzazione; - ottenere la garanzia di ottenere dal provider il massimo supporto in caso di attacco, per individuare gli indirizzi di rete (IP) degli aggressori mediante un percorso a ritroso, e per bloccare l'attacco.

5.8 Sicurezza dei Enterprise Service Bus (ESB)

5.8.1 Architettura

Isolamento dei sistemi critici	
Minaccia	- Accesso non autorizzato alle informazioni. - Negazione dei servizi.
Contromisure	I sistemi critici come l'ESB devono avere un ambiente di elaborazione dedicato, strettamente controllato e monitorato. Tipicamente è necessaria una protezione perimetrale fisica (CED) e logica (firewall). Occorrono in linea di principio: - un "external ESB" collocato in DMZ che agisce come Security Gateway (Security Enforcement Point – es. gestione identità) e un "internal ESB" opportunamente messo in sicurezza (vedi best practices successive) a cui l'"external ESB" passa le chiamate esterne e da cui riceve le risposte (ed eventuali chiamate verso l'esterno). Oltre al routing dei messaggi, è qui che avviene la conversione dei messaggi ed è qui che risiedono i business workflow. - Un "Security Decision Service", interno (ossia non in DMZ), cui i 2 ESB si riferiscono come repository unico delle security policies.

5.8.2 Hardening

Hardening del sistema operativo che ospita l'ESB	
Minaccia	- Accesso non autorizzato al sistema. - Compromissione delle comunicazioni. - Furto di credenziali di autenticazione (es. keylogger). - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Eseguire l'hardening del sistema operativo che ospita l'ESB [rif. 5.2.2]. Tipicamente è necessaria una protezione perimetrale fisica (CED) e logica (firewall).

Hardening della piattaforma web che ospita l'ESB	
Minaccia	- Accesso non autorizzato al sistema. - Compromissione delle comunicazioni. - Furto di credenziali di autenticazione (es. keylogger). - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione. - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Siccome SOA sfrutta e si basa sulle tecnologie Web, le vulnerabilità associate a tali tecnologie influenzano anche SOA. Pertanto, deve essere eseguito l'hardening della piattaforma web che ospita l'ESB [rif. 5.3.2].

Hardening del Web Services Layer	
Minaccia	- Accesso non autorizzato alle informazioni. - Divulgazione di informazioni riservate.
Contromisure	Utilizzare adeguati meccanismi di controllo dell'accesso per separare "operazioni interne" da "operazioni esterne" come: - un firewall XML che "tagli" le operazioni interne o - spostare le operazioni interne su servizi Web privati e ospitarle sui server Web interni. Il WSDL di un Web Service pubblica le sue operazioni, i parametri e le associazioni di

	rete. Alcune di queste (operazioni interne) devono essere utilizzate solo dal fornitore di servizi, tipicamente le operazioni amministrative. Il resto delle operazioni (operazioni esterne) può essere richiamato dal consumatore di servizi. Ora un attaccante può tentare di indovinare le operazioni interne e invocarle tramite l'endpoint (che è disponibile nel WSDL). Tale attacco è chiamato scansione WSDL.

Hardening del Web Services Layer	
Minaccia	Compromissione delle comunicazioni.
Contromisure	Verificare l'autenticità dei metadati del servizio Web (si tenga presente che non esistono meccanismi standard per verificare l'autenticità dei metadati). Un attaccante che, ad esempio, riesca a modificare l'endpoint del servizio può mettere in atto un man-in-the-middle attack per l'intercettazione o la modifica dei dati del servizio Web.

Hardening del Web Services Layer	
Minaccia	Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione.
Contromisure	La validazione dello schema del contenuto cifrato va eseguita dopo la decifratura e non prima. Gli standard di XML Encryption e XML Signature, utilizzati per fornire servizi di crittografia e firma digitale sui messaggi scambiati via Web Services (ad esempio SOAP), possono essere utilizzati da un attaccante per nascondere codice malevolo che va in esecuzione durante la decifratura (Attack obfuscation).

Hardening del Web Services Layer	
Minaccia	Negazione dei servizi.
Contromisure	Le richieste dei service consumer devono essere elaborate solo se gli elementi del security header del messaggio SOAP in entrata corrispondono esattamente ai requisiti imposti dallo schema della security policy. Diversamente vanno scartati. Lo standard WS-Security non impone restrizioni né su quali parti del security header di un messaggio SOAP possono essere crittografate né sulla dimensione massima di un messaggio crittografato. Ciò significa che un attaccante è in grado di provocare un denial of service inviando a un servizio Web dei security headers crittografati di grandi dimensioni. Le operazioni di decifratura causano un carico elevato sulla CPU del server che ospita il Web Service, carico che a sua volta crea problemi di disponibilità.

Hardening del Business Processes Layer	
Minaccia	- Accesso non autorizzato alle informazioni. - Divulgazione di informazioni riservate.
Contromisure	Estendere i meccanismi di controllo dell'accesso per separare “operazioni interne” da “operazioni esterne” a livello BPEL. Un WS-BPEL (BPEL) di un processo di business può essere sottoposto ad un attacco di "BPEL scanning" analogo al “WSDL scanning” (ma portato su un layer diverso).

Hardening del Business Processes Layer	
Minaccia	Compromissione delle comunicazioni. - Metadata spoofing
Contromisure	Verificare l'autenticità dei metadati a livello BPEL. Un attaccante, ad esempio, potrebbe modificare a suo vantaggio i riferimenti di endpoint del processo aziendale nella dichiarazione BPEL.

BPEL state deviation	
Minaccia	Negazione dei servizi. - Metadata spoofing
Contromisure	Un attaccante può inondare (flood) il motore BPEL con molti messaggi BPEL che sono conformi allo schema ma non hanno alcun contenuto significativo. Le risorse computazionali del motore BPEL potrebbero esaurirsi producendo un attacco di denial of service. Per rifiutare i messaggi non validi, l'approccio migliore è quello di utilizzare un application level firewall.

Hardening del Business Processes Layer	
Minaccia	Negazione dei servizi - Instantiation flooding (diretto e indiretto)
Contromisure	I motori BPEL istanziano un nuovo processo quando ricevono un "receive message" (che istanzia un processo BPEL). Quando viene ricevuto un "receive message", il motore BPEL sospende l'esecuzione corrente finché il messaggio entrante è completamente ricevuto. Un attaccante può sfruttare questo comportamento dei motori BPEL inondandoli di "receive message" non validi, producendo un attacco di denial of service. L'attacco può avvenire anche in modo indiretto: si colpisce un motore BPEL per attaccarne un altro che interagisce con il primo. La protezione dei motori BPEL contro questa tipologia di attacchi di flooding è complessa: occorrerebbe un'analisi semantica per individuare i messaggi non validi. E ciò esula dalle possibilità di un application level firewall. In caso di attacco occorre intervenire a livello di difesa perimetrale in modo mirato.

Hardening del Business Processes Layer	
Minaccia	Compromissione delle comunicazioni - WS-Addressing spoofing
Contromisure	Verificare la validità degli endpoint prima che il processo venga eseguito dal motore BPEL (caso di endpoint non validi o pericolosi) La specifica WS-Addressing descrive come indirizzare in modo standard gli endpoint di un web service o di un business process. Un attaccante può modificare gli header WS-Addressing facendo puntare il motore BPEL agli endpoint di servizi o di processi non validi o pericolosi.

Hardening del Business Processes Layer	
Minaccia	Negazione dei servizi - Workflow engine hijacking
Contromisure	Verificare la validità degli endpoint prima che il processo venga eseguito dal motore BPEL (caso di endpoint a un sistema di destinazione esistente, che fornisce un servizio reale all'URL specificato). In caso contrario, un attaccante può utilizzare il WS-Addressing spoofing per provocare il denial of service di un servizio legittimo attraverso un attacco di flooding. L'endpoint di cui l'attaccante esegue lo spoofing è quello di un servizio legittimo (il target dell'attacco). Il sistema attaccato tenta di elaborare una grande quantità di messaggi che gli pervengono come risultato del WS-Addressing spoofing e, se non ci riesce, i suoi utenti legittimi subiscono un Denial of Service.

Hardening del protocollo SOAP	
Minaccia	Attacchi all'integrità dei sistemi - Harmful SOAP attachments
Contromisure	I messaggi SOAP possono contenere allegati di dimensione arbitraria. Pertanto un

	attaccante può allegare un virus a un messaggio SOAP e inviarlo per l'elaborazione al sistema di destinazione. Gestire gli allegati SOAP secondo le seguenti modalità: - bloccarli se non previsti o sospetti; - filtrarli in base al MIME-type; - analizzarli con un anti-malware.

Hardening del protocollo SOAP	
Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità delle informazioni. - Negazione dei servizi. - (SOAPAction spoofing).
Contromisure	Verificare rigorosamente se l'azione specificata nel SOAP body corrisponde all'azione specificata nell'HTTP header. Se non corrispondono, il messaggio in arrivo deve essere rifiutato. Non utilizzare mai il campo SOAPAction nell'intestazione HTTP come identificativo dell'operazione del servizio. Un malintenzionato potrebbe facilmente modificare l'elemento "SOAPAction" nell'intestazione HTTP per eseguire un'azione diversa da quella specificata nel SOAP body.

Hardening dei documenti XML	
Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità delle informazioni. - (XPath injection).
Contromisure	È necessario utilizzare un'interfaccia XPath parametrizzata (se disponibile) oppure eseguire la sanitizzazione dell'input utente prima di includerlo in una query costruita dinamicamente (in analogia con le tecniche per evitare la SQL Injection). La specifica XPath viene utilizzata per navigare nel contenuto di un documento XML. Un attacco di XPath injection (simile all'attacco SQL injection) inietta un'espressione XPath all'interno di quella predisposta dal programmatore al fine di accedere a informazioni non autorizzate in un documento XML.

Hardening dei documenti XML	
Minaccia	Negazione dei servizi.
Contromisure	Limitare la dimensione dei messaggi SOAP in arrivo per contrastare un attacco di payload di grandi dimensioni. Si tenga presente che l'approccio Document Object Model (DOM) per l'analisi e l'elaborazione di XML consuma una grande quantità di memoria. Ciò è dovuto al fatto che è necessaria una rappresentazione in memoria ad oggetti dell'intero documento XML, che richiede molto più spazio di memoria rispetto al documento XML stesso. Payload di grandi dimensioni possono essere ottenuti ad esempio: - Abusando della proprietà di nesting di elementi, inserendo a piacimento molteplici elementi nel documento. - Abusando della funzionalità di DTD (Document Type Definitions) per creare ricorsivamente entità all'interno del documento fino a farlo "esplodere".

Hardening dei documenti XML	
Minaccia	Negazione dei servizi.
Contromisure	Considerare l'impiego di session tokens univoci nei messaggi SOAP come i nonces

	(ossia numeri univoci usati una sola volta). Messaggi XML completamente validi possono essere usati per causare un attacco DoS chiamato "replay attack". Un attaccante può inviare messaggi SOAP ripetitivi contenenti payload XML validi e richieste ben formate replicando messaggi precedentemente osservati, per portare un attacco DoS.

Hardening dei documenti XML	
Minaccia	Negazione dei servizi (es. Coercive parsing).
Contromisure	Verificare che l'input XML sia sempre validato attraverso il corrispondente schema XML.

Hardening dei documenti XML	
Minaccia	Negazione dei servizi - Schema poisoning
Contromisure	Proteggere gli schemi XML contro modifiche non autorizzate. Un attaccante può intercettare uno schema XML prima di raggiungere un service consumer e modificarlo con uno "Schema poisoning". In tal modo, AD ESEMPIO, è possibile compromettere, lato web service, l'elaborazione dell'XML parser (che può andare in hang, crash o in uno stato inconsistente), producendo un denial of service.

5.8.3 Utenze

Ai principi generali già introdotti nel paragrafo [rif. 5.1.1], si aggiungono le seguenti indicazioni per il contesto specifico:

Utenze	
Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità delle informazioni. - Divulgazione di informazioni riservate.
Contromisure	Nel contesto ESB, sistemi e utenze applicative (non assegnate a persone fisiche) dovranno essere chiaramente identificati e autenticati.

5.8.4 Autenticazione

Ai principi generali già introdotti nel paragrafo [rif. 5.1.2], si aggiungono le seguenti indicazioni per il contesto specifico:

Autenticazione	
Minaccia	- Abuso di privilegi da parte dell'utente. - Accesso non autorizzato alle informazioni.
Contromisure	Lo standard SAML è una specifica di protezione basata su XML per scambiare informazioni di autenticazione e autorizzazione su un utente o un soggetto. Definisce uno XML schema e le asserzioni di sicurezza. Le asserzioni sono di tre tipi e riguardano: - l'autenticazione - gli attributi relativi alla sicurezza per il soggetto - le decisioni di autorizzazione adottate. Laddove si debbano realizzare applicazioni interoperabili (tra differenti application server) o web services richiamabili da molteplici operazioni (si pensi ad es. ad un servizio di CRM che espone i suoi metodi tramite web services ad un gran numero di altre applicazioni interne), è necessario utilizzare SAML per la gestione delle autorizzazioni applicative del soggetto che richiede i servizi in base agli attributi di sicurezza di cui dispone.

5.8.5 Autorizzazione

Ai principi generali già introdotti nel paragrafo [rif. 5.1.3], si aggiungono le seguenti indicazioni per il contesto specifico:

Autorizzazione	
Minaccia	- Accesso non autorizzato alle informazioni. - Uso non autorizzato di privilegi. - Crittografia debole o non validata. - Falsificazione di identità.
Contromisure	Si considerino i seguenti standard: - XML Signature: definisce la sintassi della firma digitale nell'ambito dei documenti XML e le regole per il suo processing. - XML Encryption: si avvale di una tecnologia a chiave condivisa. Il motivo per cui è richiesta la crittografia a livello XML (al di sopra di quella di trasporto, ad esempio SSL) è che la riservatezza dei messaggi deve essere mantenuta quando un messaggio attraversa più nodi nel suo percorso verso la destinazione. Inoltre XML Encryption conserva anche la riservatezza dei messaggi a riposo (quando cioè un messaggio XML viene memorizzato sulla destinazione finale). - XML Key Management Specification (XKMS): completa gli standard XML Signature e XML Encryption, specificando i protocolli per la distribuzione e la registrazione di chiavi pubbliche (crittografia a chiave pubblica) che possono essere utilizzate con XML Signature e XML Encryption. - WS-Security: definisce le estensioni per il protocollo SOAP per realizzare messaggistica sicura ovvero tale da garantire l'integrità, la riservatezza, l'autenticazione dei messaggi. È un meccanismo di uso generale per associare i token di sicurezza ai messaggi SOAP. Si basa su XML Signature e XML Encryption. Le funzionalità descritte, laddove richieste da un'applicazione, non devono essere implementate autonomamente partendo da zero c con librerie generiche, ma devono necessariamente utilizzare gli standard sopra elencati.

5.8.6 Crittografia

Ai principi generali già introdotti nel paragrafo [rif. 5.1.1], si aggiungono le seguenti indicazioni per il contesto specifico:

Utenti	
Minaccia	- Accesso non autorizzato ai sistemi. - Accesso non autorizzato alle informazioni.
Contromisure	Per la definizione delle politiche di controllo di accesso e per valutare le richieste di autorizzazione, utilizzare lo standard XACML o eXtensible Access Control Markup Language, basato su XML.

5.8.7 Documentazione

Valgono i principi generali già introdotti nel paragrafo [rif. 5.1.5].

5.8.8 Logging

Valgono i principi generali già introdotti nel paragrafo [rif. 5.1.6].

5.8.9 Procedure

Valgono i principi generali già introdotti nel paragrafo [rif. 5.1.7].

5.8.10 Informazioni addizionali

Gli standard citati per mettere in sicurezza l'ESB (Security Assertion Markup Language (SAML), WS-Security, eXtensible Access Control Markup Language (XACML), ecc.) sono implementati e resi fruibili da soluzioni COTS (Commercial Of The Shelf), la cui adozione indirizza molte delle best practices descritte.

Riferimenti	
SAML, XACML, etc	Gli standard citati per mettere in sicurezza l'ESB (SAML - Security Assertion Markup Language, WS-Security, XACML - eXtensible Access Control Markup Language, ecc.) sono implementati e resi fruibili da soluzioni **COTS** (Commercial Of The Shelf), la cui adozione indirizza molte delle best practices descritte nei paragrafi precedenti.
Web Services	Per informazioni sulle problematiche di sicurezza relative alla tecnologia dei Web Services, visitare il sito: https://www.us-cert.gov/bsi/articles/best-practices/assembly-integration-and-evolution--security-concept-challenge-and-design-considerations-web-services-integration.

5.9 Sicurezza del pacchetto MS Office

5.9.1 Hardening

Hardening della suite Office	
Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (malware).
Contromisure	Limitare/Disabilitare/Condizionare l'uso di contenuti attivi. Per contenuti attivi si intendono: - i controlli ActiveX, - i componenti aggiuntivi quali, ad esempio: • Componenti aggiuntivi COM (Component Object Model) • Componenti aggiuntivi Visual Studio Tools per Office (VSTO) • Componenti aggiuntivi di automazione • Server RTD (RealTimeData) • Componenti aggiuntivi di applicazioni, ad esempio file con estensioni wll, xll e xlam • Pacchetti di espansione XML • Fogli di stile XML • Macro VBA
Riferimenti	- Pianificare le impostazioni di sicurezza per i controlli ActiveX in Office 2013, https://technet.microsoft.com/it-it/library/cc179076.aspx - Pianificare le impostazioni di protezione per i componenti aggiuntivi per Office

	2013, https://technet.microsoft.com/it-it/library/ee857086.aspx - Pianificare le impostazioni di protezione per le macro VBA per Office 2013, https://technet.microsoft.com/it-it/library/ee857085.aspx

Hardening della suite Office	
Minaccia	Accesso non autorizzato alle informazioni. Attacchi all'integrità dei sistemi. Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (malware).
Contromisure	Bloccare i contenuti esterni, come: Immagini, elementi multimediali, Hyperlinks, Connessioni dati, Templates, etc. I contenuti esterni possono nascondere Web beacons (che minano la privacy) o malware (con svariati esiti).
Riferimenti	- Blocco o sblocco di contenuti esterni in documenti di Office, https://support.office.com/en-us/article/Block-or-unblock-external-content-in-Office-documents-10204ae0-0621-411f-b0d6-575b0847a795?CorrelationId=2589076c-bc38-4c1e-bac5-317c19aed229&ui=en-US&rs=en-US&ad=US&ocmsassetID=HA010065176

Hardening della suite Office	
Minaccia	Divulgazione di informazioni riservate.
Contromisure	I documenti possono contenere grandi quantità di informazioni nascoste: - Nome utente, organizzazione - Storia delle modifiche, aggiunte, cancellazioni - Note, Commenti - Testo nascosto - Un intero foglio di calcolo "dietro" a un semplice diagramma (con cifre confidenziali!) - A volte anche blocchi casuali di memoria - Proprietà del server di documenti (se il documento fosse stato salvato in un server di gestione dei documenti, che ad esempio si basa su Microsoft Windows SharePoint Services, il documento potrebbe contenere informazioni aggiuntive relative a quel server). Per rimuovere tali informazioni, utilizzare lo strumento di Office denominato "Document Inspector".
Riferimenti	- Remove hidden data and personal information by inspecting documents, https://support.office.com/en-us/article/Remove-hidden-data-and-personal-information-by-inspecting-documents-356b7b5d-77af-44fe-a07f-9aa4d085966f - Using the document inspector, https://msdn.microsoft.com/en-us/vba/office-shared-vba/articles/using-the-document-inspector

Hardening della suite Office	
Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione. - (Zero-day-exploits).
Contromisure	- Bloccare (in via temporanea) l'apertura e/o il salvataggio di certi di tipi di file. Ciò attenua il rischio di attacchi alla sicurezza di tipo zero-day, impedendo temporaneamente agli utenti di aprire tipi di file specifici, nell'attesa di

	aggiornamento software o un Service Pack. - Attivare la funzionalità "Convalida file di Office". Tale funzionalità consente di individuare e prevenire un tipo di exploit noto come "file format attack" o "file fuzzing attack" (la struttura del file viene modificata al fine di aggiungere malware). In pratica se "Convalida file di Office" determina che la struttura di un file (prima ancora di essere aperto) non è conforme a tutte le regole descritte nello schema, il file non supera la convalida.
Riferimenti	- Pianificare le impostazioni di blocco dei file per Office, https://technet.microsoft.com/it-it/library/cc179230.aspx

Hardening della suite Office	
Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (malware).
Contromisure	- Limitare/Disabilitare i servizi, basati su Internet, che contribuiscono a proteggere e migliorare le applicazioni di Office (ad esempio quelli che inviano le informazioni dei messaggi di errore a Microsoft), al fine di controllare la divulgazione di informazioni private (privacy). - Attivare la funzionalità di "Visualizzazione protetta". La "Visualizzazione protetta" protegge da diversi tipi di exploit poiché apre i documenti in una sandbox (un ambiente isolato da dove risulta difficile sferrare attacchi). In Visualizzazione protetta: • i contenuti attivi non sono abilitati • gli utenti possono visualizzare il contenuto di un file ma non possono eseguire operazioni di modifica, salvataggio o stampa, né visualizzare le eventuali firme digitali del file. - Limitare/Disabilitare l'uso dei meccanismi: • Trusted Documents • Trusted Locations • Trusted Publishers Tali meccanismi infatti by-passano molti controlli di sicurezza. In particolare tutti i contenuti di un "trusted document" o di un documento preso da una "trusted location", o firmati da un "Trusted Publisher" sono immediatamente attivi all'apertura del documento.
References	- Pianificare le impostazioni di Visualizzazione protetta per Office 2013, https://technet.microsoft.com/it-it/library/ee857087.aspx - Trusted documents, https://support.office.com/en-us/article/Trusted-documents-cf872bd8-47ec-4c02-baa5-1fdba1a11b53 - Pianificare e configurare le impostazioni di Percorsi attendibili per Office 2013, https://docs.microsoft.com/it-it/previous-versions/office/office-2013-resource-kit/cc179039(v=office.15)?redirectedfrom=MSDN

Hardening del sistema operativo che ospita la suite	
Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (malware).
Contromisure	Eseguire l'hardening del sistema operativo che ospita la suite Office. L'hardening del sistema operativo è oggetto di un paragrafo specifico [rif. 5.2.2].

	Installare sul sistema software anti-malware in grado di: - analizzare i "contenuti attivi" presenti nei documenti Office rilevando la presenza di malware; - rimuovere dai documenti di Office i "contenuti attivi" in base a specifiche politiche configurabili, ad es. In base alla tipologia (macro, scripts, oggetti "embedded", applets, etc.), e altre caratteristiche.

5.9.2 Autorizzazione

A i principi generali già introdotti nel paragrafo [rif. 5.1.3], si aggiungono le seguenti indicazioni per il contesto specifico:

Autorizzazione	
Minaccia	- Attacchi all'integrità dei sistemi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (malware).
Contromisure	Proteggere i parametri di sicurezza e la definizione delle "trusted location" da eventuali cambiamenti apportati dagli utenti finali. Tali configurazioni devono essere impostabili solo da un'utenza amministrativa.

5.9.3 Crittografia

A i principi generali già introdotti nel paragrafo [rif. 5.1.4], si aggiungono le seguenti indicazioni per il contesto specifico:

Crittografia	
Minaccia	- Accesso non autorizzato alle informazioni - Attacchi all'integrità delle informazioni. - Falsificazione di identità.
Contromisure	Si tengano presenti i seguenti strumenti integrati in Office: - L'utilizzo di firma digitale per la protezione dell'integrità dei documenti prodotti (Gli utenti possono firmare digitalmente un documento di Excel, PowerPoint o Word); - L'utilizzo di meccanismi per la protezione della confidenzialità dei documenti prodotti eseguendone la cifratura. Sono disponibili impostazioni che consentono di imporre l'utilizzo di password complesse, ad esempio regole relative alla complessità e alla lunghezza.
References	- Pianificare le impostazioni della firma digitale per Office 2013, https://docs.microsoft.com/it-it/previous-versions/office/office-2013-resource-kit/cc545900(v=office.15)?redirectedfrom=MSDN - Pianificare le impostazioni di complessità delle password per Office 2013, https://technet.microsoft.com/it-it/library/ff657853.aspx

Crittografia	
Minaccia	Disponibilità dei servizi.
Contromisure	Valutare l'adozione dello strumento DocRecrypt che funziona sul principio del Key escrow, ovvero un accordo in cui le chiavi necessarie per decifrare i dati crittografati sono detenuti in un "deposito" (escrow) in modo che, in determinate circostanze, una terza parte autorizzata, ad esempio un apposito incaricato appartenente alla Security dell'organizzazione, possa accedere a tali chiavi. - Pro: si può recuperare il contenuto di un file cifrato anche nell'eventualità che il

	detentore della password la smarrisca o lasci l'organizzazione. - Contro: occorre affidarsi a un soggetto fidato.
References	- Rimuovere o reimpostare le password dei file in Office, https://docs.microsoft.com/it-it/previous-versions/office/office-2013-resource-kit/jj923033(v=office.15)?redirectedfrom=MSDN

5.9.4 Procedure

A i principi generali già introdotti nel paragrafo [rif. 5.1.7], si aggiungono le seguenti indicazioni per il contesto specifico:

Patching	
Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (malware). - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Per quanto concerne il Patching, il Microsoft Security Response Center rilascia mensilmente dei bollettini sulla sicurezza che descrivono gli aggiornamenti di sicurezza pubblicati nel mese corrente. Essi risolvono le vulnerabilità legate alla sicurezza del software Microsoft, i relativi rimedi e forniscono i collegamenti agli aggiornamenti applicabili per il software interessato.
References	- Security Bulletins, https://docs.microsoft.com/en-us/security-updates/securitybulletins/securitybulletins

Procedura	
Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (malware).
Contromisure	Visto che: A partire da Office 2013 si distinguono 2 tipi di documenti: "normal" e "macro-enabled": - Normal (default): .docx, .xlsx e .pptx - Macro-enabled: .docm, .xlsm, .pptm I documenti "normal" ('x') non hanno macro abilitate, mentre i documenti "macro-enabled" hanno le macro abilitate La regola più sicura è che si dovrebbe usare sempre documenti di tipo "normal" ('x' finale), evitando di aprire quelli contenenti macro.

5.9.5 References and additional information

I riferimenti sono già stati riportati all'interno delle singole best practices.

5.10 Sicurezza del pacchetto OpenOffice

5.10.1 Hardening

Hardening della suite OpenOffice	
Minaccia	- Accesso non autorizzato alle informazioni.

	- Attacchi all'integrità dei sistemi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (malware).
Contromisure	Limitare/Disabilitare/Condizionare l'uso di contenuti attivi. Per contenuti attivi si intendono: - EXE, COM, PIF, SCR, etc.: Binary code; - BAT, CMD, VBS, JS, etc.: Commands, Scripts; - HTML, XML, XHTML: Scripts; - PDF: Scripts, Embedded files, Commands - Word, Excel, PowerPoint, Access, … : Macros, OLE objects, Embedded files, Commands; - URLs. OpenOffice offre una certa difesa a livello di: - esecuzione delle macro (4 modalità -low, medium, high, very high- e possibilità di definizione di "trusted sources"); - navigazione degli hyperlinks (attraverso Ctrl-click).
References	- Security options, https://wiki.openoffice.org/wiki/Documentation/OOo3_User_Guides/Getting_Started

Hardening della suite OpenOffice	
Minaccia	Divulgazione di informazioni riservate.
Contromisure	I documenti possono contenere grandi quantità di informazioni nascoste: - Nome utente, organizzazione; - Storia delle modifiche, aggiunte, cancellazioni; - Note, Commenti; - Testo nascosto; - Un intero foglio di calcolo "dietro" a un semplice diagramma (con cifre aziendali confidenziali!) ; - A volte anche blocchi casuali di memoria. Se si registrano le modifiche al documento o si includono informazioni o commenti nascosti nei documenti, per evitare la diffusione incontrollata di tali informazioni utilizzare i meccanismi messi a disposizione da OpenOffice che consentono di: - impostare warnings per ricordare (in fase di firma, esportazione PDF e salvataggio) di rimuovere tali informazioni oppure; - rimuovere automaticamente alcune informazioni.
References	- Security options and warnings, https://wiki.openoffice.org/wiki/Documentation/OOo3_User_Guides/Getting_Started

Hardening del sistema operativo che ospita la suite OpenOffice	
Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (malware).
Contromisure	Eseguire l'hardening del sistema operativo che ospita la suite [rif. 5.2.2]. Installare sul sistema software anti-malware in grado di: - analizzare i "contenuti attivi" presenti nei documenti OpenOffice rilevando la presenza di malware; - rimuovere dai documenti OpenOffice i "contenuti attivi" in base a specifiche

	politiche configurabili, ad es. In base alla tipologia (macro, scripts, oggetti "embedded", applets, etc.), e altre caratteristiche.

5.10.2 Autorizzazione

Ai principi generali già introdotti nel paragrafo [rif. 5.1.3], si aggiungono le seguenti indicazioni per il contesto specifico:

Autorizzazione	
Minaccia	- Attacchi all'integrità dei sistemi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (malware).
Contromisure	Proteggere i parametri di sicurezza e la definizione delle "trusted location" da eventuali cambiamenti apportati dagli utenti finali. Tali configurazioni devono essere impostabili solo da un'utenza amministrativa.

5.10.3 Crittografia

Ai principi generali già introdotti nel paragrafo [rif.5.1.4], si aggiungono le seguenti indicazioni per il contesto specifico:

Crittografia	
Minaccia	- Accesso non autorizzato alle informazioni - Attacchi all'integrità delle informazioni. - Falsificazione di identità.
Contromisure	Si tengano presenti i seguenti strumenti integrati in OpenOffice: - L'utilizzo di firma digitale per la protezione dell'integrità dei documenti prodotti (attraverso l'azione "File → Digital Signatures"); - L'utilizzo di meccanismi per la protezione della confidenzialità dei documenti prodotti eseguendone la cifratura (attraverso l'azione "Save With Password").

5.10.4 Procedure

Ai principi generali già introdotti nel paragrafo [rif. 5.1.7], si aggiungono le seguenti indicazioni per il contesto specifico:

Patching	
Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (malware). - Violazione di leggi, di regolamenti, di obblighi contrattuali.
Contromisure	Dalla versione 2.1, OpenOffice ha incluso una funzionalità che segnala se è disponibile una nuova versione. Per attivare questa opzione: *Tools → Options → Online Update → Check for updates automatically* È possibile ricevere alerts via email su vulnerabilità di sicurezza risolte (vedi references: [1]); È possibile ricevere informazioni complete sugli alert per tutte le vulnerabilità di sicurezza risolte (vedi references: [2]). Tutte le patch di sicurezza devono essere installate prontamente.
References	[1] Security Alerts, https://www.openoffice.org/security/alerts.html [2] Security Bulletin, https://www.openoffice.org/security/bulletin.html

Limitare e controllare l'uso di open source "spurio"	
Minaccia	Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (malware).
Contromisure	Poiché l'open source rende il codice sorgente disponibile a chiunque, un attaccante potrebbe: - progettare e distribuire alcuni malware incorporando codice dannoso nella distribuzione originale open source (al fine di lasciare backdoor o eseguire l'upload di dati sensibili o informazioni aziendali) - mostrare alcune caratteristiche interessanti della distribuzione malevola attirando così alcuni utenti finali. L'organizzazione deve definire una chiara politica di sicurezza sull'utilizzo di open source, per evitare che vengano scaricate e installate customizzazioni di software open source da fonti non attendibili, considerando le seguenti linee guida: - utilizzo di procedure di identificazione, autenticazione e autorizzazione per il software open source; - limitazione della disponibilità e tracciamento di tutti gli utilizzi di software open source; - rimozione o disabilitazione di tutti i programmi open source non necessari e non ammessi.

Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (malware).
Contromisure	Assicurarsi che la copia di OpenOffice sia genuina: - scaricata da un sito attendibile (https://www.openoffice.org/download/); - acquisita da uno distributore ufficiale. Verificare il checksum per assicurarsi che la copia non sia stata danneggiata prima di installarla.

Minaccia	- Accesso non autorizzato alle informazioni. - Attacchi all'integrità dei sistemi. - Falsificazione di identità. - Violazione della sicurezza, rispetto alle politiche di sicurezza dell'organizzazione (malware).
Contromisure	Una macro può essere collegata a qualsiasi file OpenOffice (documento, foglio di lavoro, ecc.). Ogni volta che OpenOffice rileva le macro in un documento aperto, gestirà/eseguirà la macro come impostato a livello di "Security options → Macro security", che offre una protezione limitata. La regola più sicura è di non aprire alcun file OpenOffice a meno che non si abbia sicurezza della provenienza e fiducia del mittente, tanto più se contiene delle macro. Pertanto, se è necessario scambiare regolarmente documenti con soggetti ben individuati, si consiglia l'uso di firme digitali per certificare l'autenticità e l'integrità del documento.

Minaccia	Divulgazione di informazioni riservate.
Contromisure	Definire la modalità di segnalazione di eventuali vulnerabilità sospette o errori di OpenOffice al team di Sicurezza dell'organizzazione o dell'eventuale provider (in caso di servizi di sicurezza gestita) o a fornitori che erogano servizi di supporto tecnico, al fine di impedire la divulgazione di informazioni riservate. Occorre definire: - Quali informazioni si possono fornire. - Gli accordi di riservatezza.

6 RIFERIMENTI A ISTRUZIONI OPERATIVE E TOOLS DI HARDENING

6.1 Istruzioni operative (benchmarks) di terze parti

Si riporta nel seguito l'elenco completo dei riferimenti alle istruzioni operative di hardening (o benchmarks) delle varie componenti (sistemi operativi, middleware, office automation, ecc.) che sono state oggetto di analisi nei capitoli precedenti.

Fonte	Categoria	Famiglia	Target	Titolo
CIS Benchmarks	Sistemi Operativi	Linux	Ubuntu	Securing Ubuntu Linux - An objective, consensus-driven security guideline for the Ubuntu Linux Operating Systems. https://www.cisecurity.org/benchmark/ubuntu_linux/
CIS Benchmarks	Sistemi Operativi	Linux	CentOS	Securing CentOS Linux - An objective, consensus-driven security guideline for the CentOS Linux Operating Systems. https://www.cisecurity.org/benchmark/centos_linux/
CIS Benchmarks	Sistemi Operativi	Linux	Red Hat	Securing Red Hat Linux - An objective, consensus-driven security guideline for the Red Hat Linux Operating Systems. https://www.cisecurity.org/benchmark/red_hat_linux/
CIS Benchmarks	Sistemi Operativi	Linux	Debian	Securing Debian Linux - An objective, consensus-driven security guideline for the Debian Linux Operating Systems. https://www.cisecurity.org/benchmark/debian_linux/
CIS Benchmarks	Sistemi Operativi	Linux	Oracle Linux	Securing Oracle Linux - An objective, consensus-driven security guideline for the Oracle Linux Operating Systems. https://www.cisecurity.org/benchmark/oracle_linux/
CIS Benchmarks	Sistemi Operativi	Linux	SUSE	Securing SUSE Linux - An objective, consensus-driven security guideline for the SUSE Linux Operating Systems. https://www.cisecurity.org/benchmark/suse_linux/
CIS Benchmarks	Sistemi Operativi	UNIX	AIX 7.1	CIS IBM AIX 7.1 Benchmark https://www.cisecurity.org/benchmark/ibm_aix
CIS Benchmarks	Sistemi Operativi	UNIX	Solaris 11.1	CIS Oracle Solaris 11.1 Benchmark https://www.cisecurity.org/benchmark/oracle_solaris
CIS Benchmarks	Sistemi Operativi	UNIX	Solaris 11	CIS Oracle Solaris 11 Benchmark https://www.cisecurity.org/benchmark/oracle_solaris
CIS Benchmarks	Sistemi Operativi	UNIX	Solaris 10	CIS Oracle Solaris 10 Benchmark https://www.cisecurity.org/benchmark/oracle_solaris
CIS Benchmarks	Sistemi Operativi	Windows Desktop	Windows 10	CIS Benchmarks for CIS Microsoft Windows 10 Enterprise: Securing Microsoft Windows Desktop - An objective, consensus-driven security guideline for the Microsoft Windows Desktop Operating Systems - For Microsoft Windows Desktop 10 https://www.cisecurity.org/benchmark/microsoft_windows_desktop/
CIS Benchmarks	Sistemi Operativi	Windows Desktop	Windows 8.1	CIS Microsoft Windows 8.1 Workstation Benchmark https://www.cisecurity.org/benchmark/microsoft_windows_desktop/
CIS Benchmarks	Sistemi Operativi	Windows Desktop	Windows 8	CIS Microsoft Windows 8 Benchmark https://www.cisecurity.org/benchmark/microsoft_windows_desktop/

CIS Benchmarks	Sistemi Operativi	Windows Desktop	Windows 7	CIS Microsoft Windows 7 Workstation Benchmark https://www.cisecurity.org/benchmark/microsoft_windows_desktop/
CIS Benchmarks	Sistemi Operativi	Windows Desktop	Windows XP	CIS Microsoft Windows XP Benchmark https://www.cisecurity.org/benchmark/microsoft_windows_desktop/
CIS Benchmarks	Sistemi Operativi	Windows Server	2016	CIS Microsoft Windows Server 2016 RTM Benchmark https://www.cisecurity.org/benchmark/microsoft_windows_server/
CIS Benchmarks	Sistemi Operativi	Windows Server	2012 R2	CIS Microsoft Windows Server 2012 R2 Benchmark https://www.cisecurity.org/benchmark/microsoft_windows_server/
CIS Benchmarks	Sistemi Operativi	Windows Server	2012	CIS Microsoft Windows Server 2012 (non-R2) Benchmark https://www.cisecurity.org/benchmark/microsoft_windows_server/
CIS Benchmarks	Sistemi Operativi	Windows Server	2008 R2	CIS Microsoft Windows Server 2008 R2 Benchmark https://www.cisecurity.org/benchmark/microsoft_windows_server/
CIS Benchmarks	Sistemi Operativi	Windows Server	2008	CIS Microsoft Windows Server 2008 (non-R2) Benchmark https://www.cisecurity.org/benchmark/microsoft_windows_server/
CIS Benchmarks	Sistemi Operativi	Windows Server	2003	CIS Microsoft Windows Server 2003 Benchmark https://www.cisecurity.org/benchmark/microsoft_windows_server/
CIS Benchmarks	Collaboration Server	Microsoft SharePoint	2019	CIS Microsoft SharePoint 2019 Benchmark https://www.cisecurity.org/benchmark/microsoft_sharepoint/
CIS Benchmarks	Collaboration Server	Microsoft SharePoint	2016	CIS Microsoft SharePoint 2016 Benchmark https://www.cisecurity.org/benchmark/microsoft_sharepoint/
CIS Benchmarks	Web / Application Server	Microsoft IIS	IIS 10	CIS Microsoft IIS 10 Benchmark https://www.cisecurity.org/benchmark/microsoft_iis/
CIS Benchmarks	Web / Application Server	Microsoft IIS	IIS 8	CIS Microsoft IIS 8 Benchmark https://www.cisecurity.org/benchmark/microsoft_iis/
CIS Benchmarks	Web / Application Server	Microsoft IIS	IIS 7	CIS Microsoft IIS 7 Benchmark https://www.cisecurity.org/benchmark/microsoft_iis/
CIS Benchmarks	Web / Application Server	Apache HTTP	2.4	CIS Apache HTTP Server 2.4 Benchmark https://www.cisecurity.org/benchmark/apache_http_server/
CIS Benchmarks	Web / Application Server	Apache HTTP	2.2	CIS Apache HTTP Server 2.2 Benchmark https://www.cisecurity.org/benchmark/apache_http_server/
CIS Benchmarks	Web / Application Server	Apache Tomcat	9	CIS Apache Tomcat 9 Benchmark https://www.cisecurity.org/benchmark/apache_tomcat/
CIS Benchmarks	Web / Application Server	Apache Tomcat	8	CIS Apache Tomcat 8 Benchmark https://www.cisecurity.org/benchmark/apache_tomcat/
CIS Benchmarks	Web / Application Server	Apache Tomcat	7	CIS Apache Tomcat 7 Benchmark https://www.cisecurity.org/benchmark/apache_tomcat/
CIS Benchmarks	DBMS	Microsoft SQL Server	2016	CIS Microsoft SQL Server 2016 Benchmark https://www.cisecurity.org/benchmark/microsoft_sql_server/

CIS Benchmarks	DBMS	Microsoft SQL Server	2014	CIS Microsoft SQL Server 2014 Benchmark https://www.cisecurity.org/benchmark/microsoft_sql_server/
CIS Benchmarks	DBMS	Microsoft SQL Server	2012	CIS Microsoft SQL Server 2012 Benchmark https://www.cisecurity.org/benchmark/microsoft_sql_server/
CIS Benchmarks	DBMS	Microsoft SQL Server	2008 R2	CIS Microsoft SQL Server 2008 R2 Benchmark https://www.cisecurity.org/benchmark/microsoft_sql_server/
CIS Benchmarks	DBMS	Oracle DB	12c	CIS Oracle Database 12c Benchmark https://www.cisecurity.org/benchmark/oracle_database/
CIS Benchmarks	DBMS	Oracle DB	11g R2	CIS Oracle Database 11g R2 Benchmark https://www.cisecurity.org/benchmark/oracle_database/
CIS Benchmarks	DBMS	Oracle DB	11 – 11g	CIS Oracle Database Server 11 - 11g Benchmark https://www.cisecurity.org/benchmark/oracle_database/
CIS Benchmarks	DBMS	Oracle MySQL	5.7 EE	CIS Oracle MySQL Enterprise Edition 5.7 BenchmarK https://www.cisecurity.org/benchmark/oracle_mysql/
CIS Benchmarks	DBMS	Oracle MySQL	5.7 CE	CIS Oracle MySQL Community Server 5.7 Benchmark https://www.cisecurity.org/benchmark/oracle_mysql/
CIS Benchmarks	DBMS	Oracle MySQL	5.6 EE	CIS Oracle MySQL Enterprise Edition 5.6 Benchmark https://www.cisecurity.org/benchmark/oracle_mysql/
CIS Benchmarks	DBMS	Oracle MySQL	5.6 CE	CIS Oracle MySQL Community Server 5.6 Benchmark https://www.cisecurity.org/benchmark/oracle_mysql/
CIS Benchmarks	DBMS	IBM DB2	10	CIS IBM DB2 10 Benchmark https://www.cisecurity.org/benchmark/ibm_db2/
CIS Benchmarks	DBMS	IBM DB2	9	CIS IBM DB2 9 Benchmark https://www.cisecurity.org/benchmark/ibm_db2/
CIS Benchmarks	DBMS	IBM DB2	8	CIS IBM DB2 Benchmark https://www.cisecurity.org/benchmark/ibm_db2/
CIS Benchmarks	DNS Server	BIND	9.9	CIS ISC BIND DNS Server 9.9 Benchmark https://www.cisecurity.org/benchmark/bind/
CIS Benchmarks	Mail Server	Microsoft Exchange Server	2016	CIS Microsoft Exchange Server 2016 Benchmark https://www.cisecurity.org/benchmark/microsoft_exchange_server/
CIS Benchmarks	Mail Server	Microsoft Exchange Server	2013	CIS Microsoft Exchange Server 2013 Benchmark https://www.cisecurity.org/benchmark/microsoft_exchange_server/
CIS Benchmarks	Mail Server	Microsoft Exchange Server	2010	CIS Microsoft Exchange Server 2010 BenchmarK https://www.cisecurity.org/benchmark/microsoft_exchange_server/
CIS Benchmarks	Office Automation	Microsoft Office	Office 365 2016 2013	CIS Microsoft Office 365 Benchmark CIS Microsoft Office Word 365 Benchmark CIS Microsoft Office Excel 365 Benchmark CIS Microsoft Office PowerPoint 365 Benchmark

				CIS Microsoft Office Access 365 Benchmark CIS Microsoft Office Outlook 365 Benchmark CIS Microsoft Office 2016 Benchmark CIS Microsoft Office Word 2016 Benchmark CIS Microsoft Office Excel 2016 Benchmark CIS Microsoft Office PowerPoint 2016 Benchmark CIS Microsoft Office Access 2016 Benchmark CIS Microsoft Office Outlook 2016 Benchmark CIS Microsoft Office 2013 Benchmark CIS Microsoft Office Word 2013 Benchmark CIS Microsoft Office Excel 2013 Benchmark CIS Microsoft Office PowerPoint 2013 Benchmark CIS Microsoft Office Access 2013 Benchmark CIS Microsoft Office Outlook 2013 Benchmark https://www.cisecurity.org/benchmark/microsoft_office/
CIS Benchmarks	Web Browser	Internet Explorer	11	CIS Microsoft Internet Explorer 11 Benchmark https://www.cisecurity.org/benchmark/microsoft_internet_explorer/
CIS Benchmarks	Web Browser	Internet Explorer	10	CIS Microsoft Internet Explorer 10 Benchmark https://www.cisecurity.org/benchmark/microsoft_internet_explorer/
CIS Benchmarks	Web Browser	Mozilla Firefox		CIS Mozilla Firefox 38 ESR Benchmark https://www.cisecurity.org/benchmark/mozilla_firefox/
CIS Benchmarks	Web Browser	Mozilla Firefox		CIS Mozilla Firefox 24 ESR Benchmark https://www.cisecurity.org/benchmark/mozilla_firefox/
CIS Benchmarks	Web Browser	Google Chrome		CIS Google Chrome Benchmark https://www.cisecurity.org/benchmark/google_chrome/
CIS Benchmarks	Networking	Cisco IOS	IOS 15	CIS Cisco IOS 15 Benchmark https://www.cisecurity.org/benchmark/cisco/
CIS Benchmarks	Networking	Cisco IOS	IOS 12	CIS Cisco IOS 12 Benchmark https://www.cisecurity.org/benchmark/cisco/

6.2 Tools di hardening e baseline di sicurezza fornite dai vendor

Si riporta nel seguito un elenco di strumenti software (laddove disponibili) e baseline di sicurezza, per la configurazione sicura (hardening) dei principali sistemi target.

Fonte	Categoria	Famiglia	Target	Titolo
Microsoft	Sistemi Operativi	Windows	Windows Server & Client	Microsoft Security Compliance Manager (SCM) È uno strumento gratuito di Microsoft che consente di gestire correttamente e agilmente la sicurezza dell'infrastruttura IT e delle applicazioni, analizzando la propria infrastruttura e configurandola seguendo le raccomandazioni di Microsoft. Consente una gestione centralizzata dell'insieme delle baseline di sicurezza, con la possibilità di gestire specifiche personalizzazioni in base a specifiche esigenze di certi sistemi. Consente inoltre di esportare le configurazioni in vari formati tra cui XLS (Excel) e GPO (Group Policy Objects). Supporta i sistemi operativi Windows Server e Windows Client. https://www.microsoft.com/en-us/download/details.aspx?id=53353
Microsoft	Web Server	IIS	8	Security Best Practices for IIS 8 https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/jj635855(v=ws.11)?redirectedfrom=MSDN
Microsoft	DBMS	SQL Server	20108-2016	Non è disponibile ad oggi un tool specifico ma esiste una pagina di riferimento di Microsoft aggiornata che contiene opportune indicazioni per la configurazione sicura di SQL Server: https://docs.microsoft.com/en-us/sql/relational-databases/security/securing-sql-server#sql-server-security-tools-utilities-views-and-functions Esiste inoltre una pagina ulteriore di supporto per specifici task di configurazione sicura che riguardano non solo SQL Server ma più in generale l'accesso ai dati: Security Checklists for the Database Engine: • Checklist: Database Engine Security Configuration • Checklist: Enhancing the Security of Database Engine Connections • Checklist: Limiting Access to Data • Checklist: Encrypting Sensitive Data https://docs.microsoft.com/en-us/previous-versions/sql/sql-server-2008-r2/ff848778(v=sql.105)?redirectedfrom=MSDN
Bastille	Sistemi Operativi	Linux (RedHat, SUSE, Debian, Ubuntu) e HP-UX	Vari	Bastille Linux è un tool gratuito per l'hardening di vari sistemi operative Linux (RedHat, Debian, SUSE, ecc.) e HP-UX. Sulla maggior parte dei sistemi operativi supportati fa parte della distribuzione standard ed è quindi immediatamente disponibile per l'uso. http://bastille-linux.sourceforge.net/
Apache Software Foundation	Web Server	Apache HTTP	2.4	Security Tips - Apache HTTP Server Version 2.4 https://httpd.apache.org/docs/2.4/misc/security_tips.html
Apache Software Foundation	Web Server	Tomcat	8	Apache Tomcat 8 Security Considerations https://tomcat.apache.org/tomcat-8.0-doc/security-howto.html

Oracle	DBMS	Oracle Database	12c 11g	Oracle Database 12c Security and Compliance https://www.oracle.com/webfolder/s/delivery_production/docs/FY15h1/doc6/security-compliance-wp.pdf Cost Effective Security and Compliance with Oracle Database 11g http://www.oracle.com/technetwork/database/security/owp-security-database-11gr2-134651.pdf L'elenco del software Oracle legato alla sicurezza del prodotto Oracle Database è disponibile a questo indirizzo: Oracle Database Security Products https://www.oracle.com/database/security/products.html
Oracle	Database	Oracle MySQL	5.7	MySQL Security Guide, parte di MySQL Reference Manual Un estratto è disponibile a questo link: https://dev.mysql.com/doc/mysql-security-excerpt/5.7/en/
McAfee	Database	Oracle MySQL	Varie	McAfee MySQL Database Security Tool (gratuito): https://www.mcafee.com/content/enterprise/en-us/downloads/trials.html?query=database
Microsoft	Mail Server	Exchange Server	2016 2013 2010	Offline Assessment for Exchange Server Security http://download.microsoft.com/download/1/C/1/1C15BA51-840E-498D-86C6-4BD35D33C79E/Prerequisites_Offline_EXCHSec.pdf