DECRETI E DELIBERE DI ALTRE AUTORITÀ

AGENZIA PER LA CYBERSICUREZZA NAZIONALE

DETERMINA 3 gennaio 2023.

Tassonomia degli incidenti che debbono essere oggetto di notifica.

IL DIRETTORE GENERALE

Visto il decreto-legge 14 giugno 2021, n. 82, convertito, con modificazioni, dalla legge 4 agosto 2021, n. 109, recante «Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale»;

Visto il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, recante «Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica» e, in particolare, l'art. 1, comma 3-*bis*;

Visto il decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131, recante «Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'art. 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133»;

Visto il decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81, recante «Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'art. 1, comma 2, lettera *b)*, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza»;

Ritenuto di dover dare attuazione a quanto previsto dal citato art. 1, comma 3-*bis*, del decreto-legge n. 105 del 2019, indicando la tassonomia di incidenti che devono essere notificati ai sensi del medesimo comma 3-*bis*;

Sentito il vice direttore generale;

Determina:

Art. 1.

Definizioni

1. Ai fini del presente provvedimento si intende per:

a) «decreto-legge», il decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133;

b) «DPCM 2», il decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81, recante «Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'art. 1, comma 2, lettera *b)*, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza»;

c) «perimetro», il perimetro di sicurezza nazionale cibernetica istituito ai sensi dell'art. 1, comma 1, del decreto-legge;

d) «soggetti inclusi nel perimetro», i soggetti di cui all'art. 1, comma 2-*bis*, del decreto-legge;

e) «bene ICT» (*Information and communication technology*), un insieme di reti, sistemi informativi e servizi informatici, o parti di essi, incluso nell'elenco di cui all'art. 1, comma 2, lettera *b)*, del decreto-legge;

f) «incidente», ogni evento di natura accidentale o intenzionale che determina il malfunzionamento, l'interruzione, anche parziali, ovvero l'utilizzo improprio delle reti, dei sistemi informativi o dei servizi informatici;

g) «impatto sul bene ICT», limitazione della operatività del bene ICT, ovvero compromissione della disponibilità, integrità, o riservatezza dei dati e delle informazioni da esso trattati, ai fini dello svolgimento della funzione o del servizio essenziali.

Art. 2.

Oggetto

1. Il presente provvedimento indica la tassonomia degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici diversi dai beni ICT di pertinenza dei soggetti inclusi nel perimetro, che i soggetti medesimi sono tenuti a notificare ai sensi dell'art. 1, comma 3-*bis*, del decreto-legge.

Art. 3.

Tassonomia degli incidenti

1. Nella sezione 1 della tabella di cui all'allegato A al presente provvedimento sono classificati, in categorie, gli incidenti di cui all'art. 2, comma 1, indicando, per ciascuna tipologia di incidente, un codice identificativo e la corrispondente categoria, accompagnata dalla descrizione di ciascuna tipologia di incidente.

2. Al fine di fornire all'Agenzia per la cybersicurezza nazionale un quadro di valutazione della minaccia più completo, nella sezione 2 della tabella di cui all'allegato A al presente provvedimento sono, altresì, descritti gli eventi che i soggetti inclusi nel perimetro potranno notificare, con le medesime modalità previste dall'art. 1, comma 3-*bis*, del decreto-legge.

Art. 4.

Disposizioni finali

1. La presente determina ha efficacia dal quindicesimo giorno successivo alla sua pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana e sarà disponibile, dopo la pubblicazione, sui siti istituzionali dell'Agenzia per la cybersicurezza nazionale (https://www.acn.gov.it e https://www.csirt.gov.it).

Roma, 3 gennaio 2023

Il direttore generale: BALDONI

ALLEGATO *A*

(articolo 3)

TASSONOMIA DEGLI INCIDENTI

(in attuazione dell'articolo 1, comma 3-*bis*, del D.L. n. 105/2019)

Allegato A, articolo 3, comma 1

		SEZIONE 1
Identificativo	**Categoria**	**Descrizione**
ICP-C-1	Accesso iniziale (*Initial exploitation*)	Accesso iniziale (*Initial access*). Il soggetto ha evidenza dell'effettivo accesso non autorizzato all'interno della rete attraverso vettori di infezione, lo sfruttamento di vulnerabilità di risorse esposte pubblicamente o qualsiasi altra tecnica nota.
ICP-C-2	Esecuzione (*Execution*)	Esecuzione (*Execution*). Il soggetto ha evidenza dell'effettiva esecuzione non autorizzata di codice o malware all'interno della rete aziendale.
ICP-C-3	Installazione (*Establish persistence*)	Ottenimento di privilegi di livello superiore (*Privilege Escalation*). Il soggetto ha evidenza dell'impiego non autorizzato di tecniche, condotte dall'interno della rete, utili ad ottenere permessi di livello superiore su un sistema o una rete.
ICP-C-4		Persistenza (*Persistence*). Il soggetto ha evidenza dell'impiego non autorizzato di tecniche, condotte su un sistema o all'interno della rete, utili ad ottenere persistenza di codice malevolo o a garantire un accesso.
ICP-C-5		Evasione delle difese (*Defence Evasion*). Il soggetto ha evidenza dell'impiego non autorizzato di tecniche, di elusione di politiche e/o sistemi di sicurezza, volte ad evitare il rilevamento durante un tentativo di compromissione.
ICP-C-6		Comando e Controllo (*Command and Control*). Il soggetto ha evidenza di comunicazioni non autorizzate verso l'esterno della rete.
ICP-C-7	Movimenti laterali (*Lateral Movement*)	Esplorazione (*Discovery*). Il soggetto ha evidenza dell'impiego non autorizzato di tecniche, condotte dall'interno della rete, utili a effettuare attività di ricognizione per acquisire conoscenze sul sistema e sulla rete interna.
ICP-C-8		Raccolta di credenziali (*Credential Access*). Il soggetto ha evidenza dell'impiego non autorizzato di tecniche utili ad acquisire, dall'interno della rete, credenziali valide per l'autenticazione alle risorse di rete o ne rinviene copie non autorizzate.
ICP-C-9		Movimenti laterali (*Lateral Movement*). Il soggetto ha evidenza dell'impiego non autorizzato di tecniche utili ad accedere, controllare o eseguire codice tra le risorse interne della rete.
ICP-C-10	Azioni sugli obiettivi (*Actions on objectives*)	Raccolta (*Collection*). Il soggetto ha evidenza dell'impiego non autorizzato di tecniche utili a ricercare e/o raccogliere, dall'interno della rete, dati riservati e/o sensibili ovvero ne rilevi la presenza al di fuori dei sistemi autorizzati alla trattazione degli stessi.
ICP-C-11		Esfiltrazione (*Exfiltration*). Il soggetto ha evidenza dell'impiego non autorizzato di tecniche utili ad esfiltrare dati dall'interno della rete verso risorse esterne.
ICP-C-12		Inibizione delle funzioni di risposta (*Inhibit Response Function*). Il soggetto ha evidenza dell'impiego non autorizzato di tecniche utili a inibire l'intervento delle funzioni di sicurezza, di protezione e di "*quality assurance*" dei sistemi di controllo industriale predisposte per rispondere a un disservizio o a uno stato anomalo.
ICP-C-13		Compromissione dei processi di controllo (*Impair Process Control*). Il soggetto ha evidenza dell'impiego non autorizzato di tecniche utili a manipolare, disabilitare o danneggiare i processi di controllo fisico di sistemi di controllo industriale.
ICP-C-14		Disservizio intenzionale (*Impact*). Il soggetto ha evidenza dell'impiego non autorizzato di tecniche utili a manipolare, degradare, interrompere o distruggere i sistemi, i servizi o i dati. In tale ambito rientrano ad esempio gli eventi di tipo *Denial of Service/Distributed Denial of Service* che hanno impatto sui beni ICT.

Allegato A, articolo 3, comma 2

		SEZIONE 2
Identificativo	**Categoria**	**Descrizione**
ICP-C -15	Ricognizione (*Reconnaissance*) riferita ad attività di *spearphishing*	La ricognizione consiste in tecniche che gli avversari adottano per raccogliere, attivamente o passivamente, informazioni potenzialmente sfruttabili per successive attività. Nella specifica categoria sono da ricomprendere le campagne, ancorché prive di impatto su assetti aziendali, rilevate via posta elettronica (PEO e/o PEC) e costituite da messaggi, altamente personalizzati (*spearphishing*), indirizzati a utenti multipli della stessa organizzazione e finalizzati alla cattura di informazioni ad esempio tramite l'uso di allegati malevoli o collegamenti *web*.

23A00114