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