CONSEGNA S2L4

INTRODUZIONE

Prendere familiarità con NIST SP 800-30, creando uno schema relazionale tra tutte le tabelle presenti nella pubblicazione.

1 - SCENARIO DEL RISCHIO

Un fornitore sanitario di medie dimensioni diventa bersaglio di un attacco di phishing, in cui un aggressore invia una falsa e-mail impersonando un amministratore IT interno. Questa e-mail contiene un link a un sito web dannoso, mascherato come un modulo di aggiornamento delle password. Un dipendente cade nella trappola e le sue credenziali vengono esposte. L'aggressore utilizza queste credenziali per accedere alla rete interna del fornitore sanitario e sottrae dati sensibili dei pazienti.

2 - THREAT SOURCES - APPENDIX D

L'**Appendice D - Fonti di Minaccia** della pubblicazione NIST Special Publication 800-30 si occupa dell'identificazione e caratterizzazione delle fonti di minaccia che possono innescare eventi di minaccia. Fornisce un insieme di tabelle esemplificative e scale di valutazione che possono essere personalizzate dalle organizzazioni per identificare e caratterizzare le fonti di minaccia rilevanti. Ecco una sintesi dei contenuti principali di quest'appenice:

1. **Tabella D-1 e D-2:** Offrono informazioni esemplificative per l'identificazione delle fonti di minaccia, inclusa una tassonomia che può essere utilizzata per identificare e caratterizzare le fonti di minaccia.
2. **Tabelle D-3, D-4 e D-5:** Forniscono scale di valutazione esemplificative per valutare le caratteristiche (capacità, intenzione e targeting) delle fonti di minaccia avversarie.
3. **Tabella D-6:** Presenta una scala di valutazione per valutare l'ampiezza degli effetti degli eventi di minaccia originati da fonti di minaccia non avversarie.
4. **Tabelle D-7 e D-8:** Sono modelli per riassumere e documentare i risultati dell'identificazione e della caratterizzazione delle fonti di minaccia.

Queste tabelle e scale di valutazione sono destinate ad essere adattate e personalizzate dalle organizzazioni in base alle specifiche condizioni e necessità organizzative .

TABLE D-7: TEMPLATE – IDENTIFICATION OF ADVERSARIAL THREAT SOURCES

Identifier	Threat Source Source of Information	In Scope	Capability	Intent	Targeting
Organization -defined	Table D-2 and Task 1-4 or Organization-defined	Yes / No	Table D-3 or Organization -defined	Table D-4 or Organization -defined	Table D-5 or Organization -defined

IDENTIFICATION OF ADVERSARIAL THREAT SOURCES

iDENTIFIER	THREAT SOURCE - SOURCE OF INFORMATION	iN SCOPE	CAPABILITY	INTENT	TARGETING
Pishing attack	Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies).	Yes	High	Modera te	Hight