d EPICODE

S2 - L4

NIST, ENISAeITSRM2

7 maggio 2024

Manuel Di Gangi

INDICE

Traccia

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

https://csrc.nist.gov/pubs/sp/800/30/r1/final

1. Identificazione dello scenario

Supponiamo che un'azienda informatica fornisca servizi di hosting web per diverse aziende. Un potenziale scenario di rischio potrebbe riguardare una violazione dei dati a causa di un attacco informatico mirato ai server dell'azienda.

2. Threat source - Appendice D

Questo allegato fornisce:

I. una descrizione di input potenzialmente utili per l'identificazione delle fonti di minaccia;
II. una tassonomia esemplificativa delle fonti di minaccia per tipo, descrizione e fattori di rischio (ossia, caratteristiche) utilizzati per valutare la probabilità e/o l'impatto di tali fonti di minaccia nell'iniziare eventi di minaccia;
III. un insieme esemplificativo di scale di valutazione adattabili per valutare quei fattori di rischio; e
IV. modelli per riassumere e documentare i risultati del Task 2-1 di identificazione delle fonti di minaccia.

La tassonomia e le scale di valutazione in questo allegato possono essere utilizzate dalle organizzazioni come punto di partenza con una personalizzazione appropriata per adattarsi alle condizioni specifiche dell'organizzazione. Le tabelle D-7 e D-8, risultati del Task 2-1, forniscono input rilevanti alle tabelle di rischio nell'Allegato I.

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

TABLE D-7: IDENTIFICATION OF ADVERSARIAL THREAT SOURCES					
Minaccia	**Threat source**	**In Scope**	**Capability**	**Intent**	**Targeting**
Attacco informatico	Un attaccante compromette la sicurezza dei server aziendali attraverso vulnerabilità software o tecniche di phishing	Si	Alta: L'avversario ha un livello sofisticato di competenza, con risorse e opportunità significative per supportare più attacchi coordinati di successo.	Medio: L'avversario cerca di ottenere o modificare specifiche informazioni critiche o sensibili o di usurpare/interrompere le risorse informatiche dell'organizzazione stabilendo un punto d'appoggio nei sistemi informativi o nell'infrastruttura dell'organizzazione.	Alto: L'avversario analizza le informazioni ottenute tramite ricognizione per prendere di mira in modo persistente una specifica organizzazione, impresa, programma, missione o funzione aziendale, concentrandosi su specifiche informazioni, risorse, flussi di fornitura o funzioni di alto valore o mission-critical, dipendenti specifici che supportano tali funzioni, o posizioni chiave.

3. Threat events - Appendice E

Questo allegato fornisce:

I. una descrizione di potenziali input utili per l'identificazione degli eventi minacciosi;
II. esempi rappresentativi di eventi minacciosi avversari espressi come tattiche, tecniche e procedure (TTP) e eventi minacciosi non avversari;
III. una scala di valutazione esemplificativa per la rilevanza di tali eventi minacciosi; e
IV. modelli per riassumere e documentare i risultati del Task 2-2 di identificazione delle minacce.

Le organizzazioni possono eliminare certi eventi minacciosi dalla considerazione ulteriore se non è stato identificato alcun avversario con la capacità necessaria. Le organizzazioni possono anche modificare gli eventi minacciosi forniti per descrivere specifiche TTP con sufficiente dettaglio e al livello di classificazione appropriato. Le organizzazioni possono utilizzare gli eventi minacciosi rappresentativi e i valori predetti/previsti per la rilevanza di quegli eventi come punto di partenza, adattandoli per adattarsi a eventuali condizioni specifiche dell'organizzazione. La Tabella E-5, un output dal Task 2-2, fornisce input rilevanti per le tabelle di rischio nell'Allegato I.

TABLE E-5: TEMPLATE – IDENTIFICATION OF THREAT EVENTS

Identifier	Threat Event Source of Information	Threat Source	Relevance
Organization-defined	Table E-2, Table E-3, Task 1-4 or Organization-defined	Table D-7, Table D-8 or Organization-defined	Table E-4 or Organization-defined

TABELLA E-5: IDENTIFICAZIONE DEGLI EVENTI DI MINACCIA			
Minaccia	**Threat event**	**Threat Source**	**Relevance**
Mancanza di aggiornamenti regolari	Sfruttamento delle vulnerabilità sui sistemi informativi interni dell'organizzazione: L'avversario cerca vulnerabilità note nei sistemi informativi interni dell'organizzazione e sfrutta tali vulnerabilità.	Un attaccante compromette la sicurezza dei server aziendali attraverso vulnerabilità software o tecniche di phishing	Confermato: L'evento di minaccia o TTP è stato rilevato dall'organizzazione

4. Identificazione delle vulnerabilità - Appendice F

Questo allegato fornisce:

I. una descrizione di potenziali input utili per l'identificazione delle vulnerabilità e delle condizioni predisponenti;
II. una tassonomia esemplificativa delle condizioni predisponenti;
III. scale di valutazione esemplificative per valutare la gravità delle vulnerabilità e la pervasività delle condizioni predisponenti; e
IV. un insieme di modelli per riassumere e documentare i risultati dell'attività di identificazione delle vulnerabilità e delle condizioni predisponenti.

La tassonomia e le scale di valutazione in questo allegato possono essere utilizzate dalle organizzazioni come punto di partenza con l'adeguata personalizzazione per adattarsi a eventuali condizioni specifiche dell'organizzazione. Le Tabelle F-3 e F-6, output dalla Task 2-3, forniscono input rilevanti alle tabelle del rischio nell'Allegato I.

TABLE F-3: TEMPLATE – IDENTIFICATION OF VULNERABILITIES

Identifier	Vulnerability Source of Information	Vulnerability Severity
Organization-defined	Task 2-3, Task 1-4 or Organization-defined	Table F-2 or Organization-defined

TABELLA F-3: IDENTIFICAZIONE DELLE VULNERABILITA’		
Minaccia	**Vulnerabilità**	**Gravità delle vulnerabilità**
Mancanza di aggiornamenti regolari	La versione attuale dell’applicazione non gestisce correttamente le credenziali di accesso.	Alta: La vulnerabilità è estremamente preoccupante, in base all'esposizione della vulnerabilità e alla facilità di sfruttamento e/o alla gravità degli impatti che potrebbero derivare dal suo sfruttamento. Sono pianificati ma non implementati i relativi controlli di sicurezza o altri interventi correttivi; i controlli compensativi sono in atto e sono almeno minimamente efficaci.

TABLE F-6: TEMPLATE – IDENTIFICATION OF PREDISPOSING CONDITIONS

Identifier	Predisposing Condition Source of Information	Pervasiveness of Condition
Organization-defined	Table F-4, Task 1-4 or Organization-defined	Table F-5 or Organization-defined

TABELLA F-6: IDENTIFICAZIONE DELLE CONDIZIONI PREDISPOSTE		
Minaccia	**Condizione predisposta**	**Pervasività* della condizione** (*Diffusione/estensione)
Mancanza di aggiornamenti regolari	Informazioni di identificazione personale: Ha bisogno di utilizzare le tecnologie in modi specifici.	Molto alta: Si applica a tutte le missioni organizzative/funzioni aziendali (Livello 1), missione/processi aziendali (Livello 2) o sistemi informativi (Livello 3).

5. Identificazione degli impatti negativi - Appendice H

Questa appendice fornisce:

I. una descrizione di input utili per il compito di determinazione dell'impatto;
II. esempi rappresentativi di impatti negativi sulle operazioni e gli asset organizzativi, sugli individui, su altre organizzazioni o sulla Nazione;
III. scale di valutazione esemplificative per valutare l'impatto degli eventi minacciosi e la gamma di effetti degli eventi minacciosi; e
IV. un modello per riassumere e documentare i risultati del compito di determinazione dell'impatto 2-5.

Le scale di valutazione in questa appendice possono essere utilizzate come punto di partenza con la personalizzazione appropriata per adattarsi a eventuali condizioni specifiche dell'organizzazione. La Tabella H-4, un output del compito 2-5, fornisce input rilevanti per le tabelle dei rischi nell'Appendice I.

TABLE H-4: TEMPLATE – IDENTIFICATION OF ADVERSE IMPACTS

Type of Impact	Impact Affected Asset	Maximum Impact
Table H-2 or Organization-defined	Table H-2 or Organization-defined	Table H-3 or Organization-defined

TABELLA H-4: IDENTIFICAZIONE DEGLI IMPATTI NEGATIVI		
Tipo di impatto	**Impatto Asset interessati**	**Impatto massimo**
Danno alle operazioni; Danno agli individui	Incapacità di svolgere missioni/funzioni aziendali attuali. - In modo sufficientemente tempestivo. - Con sufficiente sicurezza e/o correttezza. - Entro i limiti delle risorse pianificate. Furto d'identità e perdita di informazioni di identificazione personale.	Moderato: Si potrebbe prevedere che l'evento di minaccia abbia un grave effetto negativo sulle operazioni organizzative, sui beni organizzativi, sugli individui, su altre organizzazioni o sulla Nazione. Un effetto avverso grave significa che, ad esempio, l'evento di minaccia potrebbe: (i) causare un significativo degrado della capacità della missione in una misura e una durata tali da consentire all'organizzazione di svolgere le sue funzioni primarie, ma l'efficacia delle funzioni è significativamente ridotta ; (ii) comportare danni significativi al patrimonio organizzativo; (iii) comportare perdite finanziarie significative; o (iv) provocare danni significativi a individui che non comportino la perdita della vita o lesioni gravi mortali.

6. Adversarial risk - Appendice I

Questo allegato fornisce:

I. una descrizione dei potenziali input utili per il compito di determinazione del rischio, inclusi considerazioni per l'incertezza delle determinazioni;
II. scale di valutazione esemplificative per valutare i livelli di rischio;
III. tabelle per descrivere il contenuto (cioè, input di dati) per le determinazioni di rischio avversarie e non avversarie; e
IV. modelli per riassumere e documentare i risultati del compito di determinazione del rischio 2-6.
V. Le scale di valutazione in questo allegato possono essere utilizzate come punto di partenza con una personalizzazione appropriata per adattarsi a eventuali condizioni specifiche dell'organizzazione. La Tabella I-5 (rischio avversario) e la Tabella I-7 (rischio non avversario) sono risultati dal Compito 2-6.

TABLE I-5: TEMPLATE – ADVERSARIAL RISK

1	2	3	4	5	6	7	8	9	10	11	12	13
Threat Event	Threat Sources	Threat Source Characteristics			Relevance	Likelihood of Attack Initiation	Vulnerabilities and Predisposing Conditions	Severity and Pervasiveness	Likelihood Initiated Attack Succeeds	Overall Likelihood	Level of Impact	Risk
		Capability	Intent	Targeting								

TABELLA I-5: RISCHIO CONTROVERSO												
1	2	3	4	5	6	7	8	9	10	11	12	13
Treat event	Threat source	Threat source Characteristics			Relevance	Likleihood of attack initiation	Vulnerabilities and predisposing conditions	Likelihood Initialited Attack Successeds	Severity and pervasiveness	Overall likelihood (G-5)	Level of Impact	Risk (I-2)
		Capability	Intent	Targeting								
Sfruttamento delle vulnerabilità sui sistemi informativi interni dell'organizzazione	Un attaccante compromette la sicurezza dei server aziendali attraverso vulnerabilità software o tecniche di phishing	Alta	Medio	Alto	Confermato	Alta	La versione attuale dell'applicazione non gestisce correttamente le credenziali di accesso.	Medio	Molto alta	Medio	Medio	Medio