



Angelo di mauro

RISK ASSESSMENT

EPICODE - BCC ICCREA

Nist 800-30r1

Qualitative

Agenda

- 01** Traccia
- 02** Risk Frame
- 03** Identify threat sources
- 04** Identify threat events
- 05** Identify vulnerabilities and predisposing conditions
- 06** Determine likelihood
- 07** Determine Impact
- 08** Determine Risk
- 09** Gap Analysis

Traccia

L'azienda Alpha è un fornitore leader di servizi sanitari online che gestisce un'ampia infrastruttura IT che include sistemi basati su cloud, applicazioni web e dispositivi mobili. L'azienda gestisce anche dati sanitari sensibili per i propri pazienti.

- L'organizzazione si è resa conto di essere target di un gruppo criminale organizzato con un buon livello di preparazione e delle significative risorse per condurre attacchi coordinati. Dai sistemi di monitoraggio, è emerso che solo questa azienda è continuamente sorvegliata dal gruppo criminale. Da ulteriori analisi, si arriva alla conclusione che il gruppo criminale vuole esfiltrare delle informazioni all'azienda sui dati sanitari degli utenti per rivenderli, creando una persistenza all'interno dell'organizzazione e non facendosi rilevare
- In questo momento la sorgente delle minaccie è alla fase di ricognizione esterna con diversi metodi (scanning, sniffing, OSINT, sorveglianza), non si rilevano ricognizioni interne
- L'organizzazione non ha abilitato MFA e non effettua regolarmente Vulnerability Assessment.
- L'organizzazione tratta informazioni personali e il loro software deve consentire la condivisione delle informazioni tra gli utenti, ciò si applica alla maggior parte dei loro sistemi
- Tutte le attività di ricognizioni sono attive, però lo scanning e sniffing portano a degli impatti bassi perché presente un firewall e WAF su cloud, invece gli effetti potrebbero essere moderati nella ricerca open source o nella sorveglianza di alcuni target particolari
- Consideriamo solamente il danneggiamento degli asset dovuto a perdita o danneggiamento degli asset informativi, con un impatto alto

Risk Frame

1

Lo scopo:

è identificare e comprendere i potenziali danni agli asset informativi ad alto impatto causati dalla perdita o danneggiamento, al fine di proteggere le informazioni sensibili dei pazienti gestite dall'azienda Alpha e mitigare le vulnerabilità

2

Ipotesi:

- Il gruppo criminale organizzato ha accesso a risorse significative e un alto livello di preparazione per condurre attacchi coordinati
- L'azienda Alpha è l'unico target continuamente sorvegliato dal gruppo criminale, indicando un interesse specifico per i dati sanitari dei pazienti
- La mancanza di abilitazione del Multi-Factor Authentication (MFA) e la mancata esecuzione regolare di Vulnerability Assessment potrebbero lasciare l'azienda vulnerabile ad attacchi informatici
- L'azienda Alpha tratta informazioni personali e richiede la condivisione di informazioni tra gli utenti, aumentando il rischio di esfiltrazione di dati sensibili

3

Vincoli:

- L'azienda deve garantire la condivisione delle informazioni tra gli utenti senza compromettere la sicurezza dei dati sensibili
- Le attività di monitoraggio come lo scanning e lo sniffing sono ostacolate dalla presenza di un firewall e WAF su cloud, tuttavia, la ricerca open source e la sorveglianza di target specifici possono ancora rappresentare un rischio moderato
- La mitigazione dei rischi deve essere realizzata senza compromettere l'accessibilità e l'utilità dei servizi sanitari online offerti dall'azienda Alpha

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

IDENTIFIER	THREAT SOURCE SOURCE OF INFORMATION	IN SCOPE	CAPABILITY	INTENT	TARGETING
D-7/1	ADVERSARIAL	YES	HIGH	HIGH	HIGH

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

IDENTIFIER	THREAT EVENT SOURCE OF INFORMATION	THREAT SOURCE	RELEVANCE
E-5/1	PERFORM PERIMETER NETWORK RECONNAISSANCE/SCANNING.	D-7/1	CONFIRMED
E-5/2	PERFORM NETWORK SNIFFING OF EXPOSED NETWORKS	D-7/1	CONFIRMED
E-5/3	GATHER INFORMATION USING OPEN SOURCE DISCOVERY OF ORGANIZATIONAL INFORMATION.	D-7/1	CONFIRMED
E-5/4	PERFORM RECONNAISSANCE AND SURVEILLANCE OF TARGETED ORGANIZATIONS.	D-7/1	CONFIRMED

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

IDENTIFIER	VULNERABILITY SOURCE OF INFORMATION	VULNERABILITY SEVERITY
F-3/1	MFA NON ABILITATO, AUMENTANDO IL RISCHIO DI ACCESSI NON AUTORIZZATI DURANTE LA RICOGNIZIONE ESTERNA.	HIGH
F-3/2	VULNERABILITY ASSESSMENT NON ESEGUITO REGOLARMENTE, AUMENTANDO LA VULNERABILITÀ DEL GRUPPO A POTENZIALI MINACCE INFORMATICHE DURANTE LA FASE DI RICOGNIZIONE ESTERNA.	MODERATE

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

IDENTIFIER	PREDISPOSING CONDITION SOURCE OF INFORMATION	PERVASIVENESS OF CONDITION
F-6/1	INFORMATION-RELATED: PERSONALLY IDENTIFIABLE INFORMATION	HIGH
F-6/2	TECHNICAL -- ARCHITECTURAL : SOLUTIONS FOR AND/OR APPROACHES TO USER-BASED COLLABORATION AND INFORMATION SHARING	HIGH

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

TYPE OF IMPACT	IMPACT AFFECTED ASSET	MAXIMUM IMPACT
HARM TO ASSETS	DAMAGE TO OR LOSS OF INFORMATION SYSTEMS OR NETWORKS.	HIGH

TABLE I-5: TEMPLATE – ADVERSARIAL RISK

TYPE OF IMPACT	THREAT SOURCES	CAPABILITY	INTENT	TARGETING	RELEVANCE	LIKELIHOOD OF ATTACK INITIATION	VULNERABILITIES AND PREDISPOSING CONDITIONS	SEVERITY AND Pervasiveness	Likelihood Initiated Attack Succeeds	Overall Likelihood	Level of Impact	Risk
E-5/1	D-7/1	HIGH	HIGH	HIGH	CONFIRMED	VERY HIGH	F-3/2	Moderate	LOW	Moderate	HIGH	Moderate
E-5/2	D-7/1	HIGH	HIGH	HIGH	CONFIRMED	VERY HIGH	F-3/2	Moderate	LOW	Moderate	HIGH	Moderate
E-5/3	D-7/1	HIGH	HIGH	HIGH	CONFIRMED	VERY HIGH	F-3/1	HIGH	Moderate	HIGH	HIGH	HIGH
E-5/4	D-7/1	HIGH	HIGH	HIGH	CONFIRMED	VERY HIGH	F-3/1	HIGH	Moderate	HIGH	HIGH	HIGH

Gap analysis

Situazione desiderata:

- MFA è implementato su tutti i sistemi critici e sensibili del gruppo, garantendo un'ulteriore protezione contro l'accesso non autorizzato
- Viene condotta una valutazione regolare delle vulnerabilità su tutti i sistemi e le reti del gruppo, garantendo che le vulnerabilità siano identificate e corrette tempestivamente

Situazione corrente:

- MFA non è abilitato su nessun sistema del gruppo, aumentando il rischio di compromissione delle credenziali e accessi non autorizzati
- Nessuna valutazione regolare delle vulnerabilità viene effettuata, questo aumenta il rischio di sfruttamento delle vulnerabilità da parte degli attaccanti

Piano d'azione MFA:

- Identificare e selezionare una soluzione MFA adatta ai bisogni e ai sistemi del gruppo
- Pianificare e comunicare il processo di implementazione di MFA a tutti gli utenti
- Implementare gradualmente MFA su tutti i sistemi critici e sensibili, monitorando attentamente il processo per garantire una transizione senza problemi
- Garantire che tutti gli utenti comprendano e utilizzino correttamente l'MFA per migliorare la sicurezza degli account

Piano d'azione VULNERABILITY:

- Selezionare uno strumento o un servizio per la valutazione delle vulnerabilità adatto alle esigenze del gruppo
- Pianificare e condurre scansioni periodiche delle reti, dei sistemi e delle applicazioni per identificare e documentare le vulnerabilità
- Priorizzare le vulnerabilità identificate in base al loro impatto potenziale e alla loro criticità per l'azienda
- Implementare un processo per correggere le vulnerabilità identificate in modo tempestivo, monitorando il progresso e garantendo che tutte le vulnerabilità critiche siano affrontate prioritariamente

