

ADA.14.01.22 - GESTIONE DELLA SICUREZZA DELL'INFORMAZIONE

SCHEDA DI CASO

RISULTATO ATTESO 1 - Applicare protocolli di controllo e affrontamento di criticità relative alla sicurezza del sistema informativo, dando corso all'esecuzione di piani di ripristino in caso di crisi

1 - SECURITY ASSESSMENT

Grado di complessità 3

1.3 VALUTAZIONE VULNERABILITÀ INFRASTRUTTURE COMPLESSE E DISTRIBUITE

Analizzare le vulnerabilità di una infrastruttura tecnologica complessa e distribuita (numerosità asset, numerosità utenze e accessi, rete web, tecnologie IoT, Big Data, A.I., Cloud, Mobile, NFC - Near Field Communication, Wearable Technology, ecc.) individuando soluzioni di sicurezza per mitigarle

Grado di complessità 2

1.2 VALUTAZIONE VULNERABILITÀ

Analizzare le vulnerabilità presenti individuando soluzioni di sicurezza per mitigarle

Grado di complessità 1

1.1 ASSESSMENT

Effettuare attività di Vulnerability Assessment e Penetration Test utilizzando strumenti tecnologici ed approcci metodologici per la verifica tecnica delle vulnerabilità e applicando tecniche di "hacking" e di analisi statica e dinamica per testare il livello di sicurezza dei sistemi, delle applicazioni e dei servizi.

1.1 DOCUMENTAZIONE VERIFICHE

Produrre la documentazione relativa ai risultati delle verifiche monitorando la chiusura delle vulnerabilità identificate

2 - SITUAZIONE DI CRISI

Grado di complessità 4

2.4 PRESIDIO GESTIONE INCIDENTI DI SICUREZZA

Presidiare il processo di gestione degli incidenti di sicurezza, coordinando tutte le azioni necessarie per una risposta immediata in caso di incidente

ADA.14.01.22 - GESTIONE DELLA SICUREZZA DELL'INFORMAZIONE

Grado di complessità 3

2.3 RECOVERY DI UNA VBF

Provvedere alla recovery con il minimo tempo di fermo applicando piani di ripristino (Information Security Risk Treatment Plan) o di work-around riferiti alla causa di un incidente di sicurezza che compromette una VBF (Vital Business Function) dell'organizzazione

Grado di complessità 2

2.2 RECOVERY INCIDENTE DI SICUREZZA

Provvedere alla recovery con il minimo tempo di fermo applicando piani di ripristino (Information Security Risk Treatment Plan) riferiti alla causa dell'incidente di sicurezza

Grado di complessità 1

2.1 ANALISI INCIDENTE DI SICUREZZA

Condurre attività di analisi atte a identificare le cause scatenanti di un incidente di sicurezza identificando rapidamente la causa e selezionando tra diverse alternative come riparare, sostituire e riconfigurare

3 - INFORMATION SECURITY RISK ASSESSMENT

Grado di complessità 4

3.4 VALUTAZIONE IMPATTO DATA BREACH NELLA GESTIONE DI EX-DATI SENSIBILI

Valutare gli impatti dovuti alla compromissione dei dati (data breach) nell'ambito della gestione di dati personali ed ex-dati sensibili nelle attività dell'organizzazione

Grado di complessità 3

3.3 VALUTAZIONE IMPATTO DATA BREACH

Valutare gli impatti dovuti alla compromissione dei dati (data breach)

Grado di complessità 2

3.2 ANALISI

Condurre attività di analisi atte a identificare le cause scatenanti di un "data breach"

Grado di complessità 1

ADA.14.01.22 - GESTIONE DELLA SICUREZZA DELL'INFORMAZIONE

3.1 ASSESSMENT DPIA

Effettuare attività di valutazione di impatto in materia di protezione dei dati personali (DPIA)

ADA.14.01.22 - GESTIONE DELLA SICUREZZA DELL'INFORMAZIONE

SCHEDA RISORSE A SUPPORTO DELLA VALUTAZIONE DEL RISULTATO ATTESO 1

RISORSE FISICHE ED INFORMATIVE TIPICHE (IN INPUT E/O PROCESS ALLE ATTIVITÀ)

- Tipologie di sistemi, applicazioni e servizi a differente livello di complessità
- Tipologie di incidenti di sicurezza
- Tipologie di incidenti di sicurezza che compromettono una VBF (Vital Business Function)
- Tipologie di Data breach presenti o possibili
- Piani di ripristino (Information Security Risk Treatment Plan)
- GDPR Privacy by design e DPIA (protezione dei dati personali), Information Security Policy e procedure di sicurezza delle informazioni, Data Protection Policy, Confidentiality, integrity and availability of information, Codici deontologici e codice etico (es.: ACM, IEEE, ISSA)
- Strumenti tecnologici per la verifica tecnica delle vulnerabilità e degli attacchi di rete
- Minacce alla privacy e alla sicurezza dell'informazione con i dispositivi e le nuove tecnologie (IoT, Big Data, A.I., Cloud, Mobile, NFC - Near Field Communication, Wearable Technology, ecc.)
- Codici deontologici e codice etico (es.: ACM, IEEE, ISSA)
- Tipologie di problemi di sicurezza dei dispositivi mobili (es.: vulnerabilità Bluetooth)

TECNICHE TIPICHE DI REALIZZAZIONE/CONDUZIONE DELLE ATTIVITÀ

- Tecniche di Vulnerability Assessment e Penetration Test
- Tecniche di "hacking" e di analisi statica e dinamica
- Operatività di gestione degli incidenti di sicurezza
- Tecniche di rilevamento e prevenzione delle intrusioni, forensics, threat intelligence e intrusion detection
- Tecniche per limitare lo spoofing nelle sue varie versioni (es.: IP, ARP, e-mail)
- Tecniche di Social Engineering
- Tecniche di rilevazione di un attacco alla rete (es.: ricognizione, scansione, intrusione)
- Tecniche di prevenzione da attacchi di rete (es.: rischi e tecniche di social engineering, strumenti di ricognizione, mappatura, scansione delle porte, fingerprinting di OS, scanner di vulnerabilità)
- Metodi di rilevamento e prevenzione delle intrusioni (es.: uso improprio e rilevamento delle anomalie, incidenza dei falsi positivi e dei falsi negativi, NIDS basati sulla firma, tecniche di decodifica del protocollo, deep-packet inspection)
- Operatività di gestione reporting e analisi degli incidenti di sicurezza

OUTPUT TIPICI DELLE ATTIVITÀ

- Documentazione relativa ai risultati delle verifiche con chiusura delle vulnerabilità identificate redatta
- Vulnerabilità presenti individuate e soluzioni di sicurezza per mitigarle definite
- Vulnerabilità di una infrastruttura tecnologica complessa e distribuita individuata e soluzioni di sicurezza definite
- Recovery svolto

ADA.14.01.22 - GESTIONE DELLA SICUREZZA DELL'INFORMAZIONE

- Piani di ripristino (Information Security Risk Treatment Plan) e work-around definiti ed applicati
- Valutazione sulla protezione dei dati personali (DPIA) svolta
- Valutazione di impatto dovuti alla compromissione dei dati (data breach) svolta
- Valutazione di impatto alla compromissione dei dati (data breach) nell'ambito della gestione di dati personali ed ex-dati sensibili svolta

INDICAZIONI A SUPPORTO DELLA SCELTA DEL METODO VALUTATIVO E DELLA PREDISPOSIZIONE DELLE PROVE

ESTENSIONE SUGGERITA DI VARIETÀ PRESTAZIONALE

1. L'insieme delle tipologie di sistemi, applicazioni e servizi a differente livello di complessità
2. L'insieme delle tipiche casistiche di incidenti di sicurezza
3. L'insieme delle tipologie di security assessment in una infrastruttura tecnologica complessa e distribuita
4. L'insieme delle tecniche gestione dei dati generali, dati personali e dati ex-sensibili

DISEGNO TIPO DELLA VALUTAZIONE

1. Prova prestazionale: Per almeno una tipologia di security assessment e un incidente di sicurezza, definizione di un piano di ripristino in situazioni di crisi effettuando il DPIA e l'analisi di data breach in contesti di trattamento dei dati

ADA.14.01.22 - GESTIONE DELLA SICUREZZA DELL'INFORMAZIONE

ADA.14.01.22 - GESTIONE DELLA SICUREZZA DELL'INFORMAZIONE

FONTI

Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali - Garante per la protezione dei dati personali (www.garanteprivacy.it)

Repertorio Qualificazioni regione FVG

Norma ISO/IEC 27001, 27002

Standard of Good Practice for Information Security 2020 (SOGP 2020)

The Cyber Security Body of Knowledge v.1.0 2019

COBIT 5 for Information Security

CIS Controls IoT Companion Guide

Tutti i reports su malware, attacchi, 5G, Artificial Intelligence, etc. sul sito ENISA (European Union Agency for Cybersecurity)

<https://www.iso.org/isoiec-27001-information-security.html>

<https://www.itgovernance.eu/it-it/iso-27001-it>

<https://www.cybok.org/>

<https://www.cisecurity.org/>

<https://www.enisa.europa.eu/>