

SCHEDA DI CASO

RISULTATO ATTESO 2 - Implementare politiche di sicurezza informativa e tendere al loro miglioramento nel tempo anche effettuando analisi comparative e realizzando audit, test e simulazioni

1 - INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

Grado di complessità 4

1.4 MIGLIORAMENTO ISMS

Analizzare i rischi per il miglioramento delle procedure di gestione della sicurezza definendo un Security KPI report nell'ISMS e identificando soluzioni e tecnologie di sicurezza per la protezione del sistema informativo a seguito della S.W.O.T. analysis sulla sicurezza dei sistemi e delle applicazioni

Grado di complessità 3

1.3 RISK INVENTORY

Predisporre e utilizzare un Risk Inventory dentro l'ISMS analizzando rischi, minacce, vulnerabilità e impatto

Grado di complessità 2

1.2 PIANI DI RIPRISTINO (INFORMATION SECURITY RISK TREATMENT)

Creare piani di ripristino (Information Security Risk Treatment Plan) nell'ISMS definendo la policy di gestione del rischio (Risk Management Policy)

Grado di complessità 1

1.1 GESTIONE ISMS

Identificare le soluzioni e le tecnologie di sicurezza per la protezione del sistema informativo aziendale applicando Best practices, standards, frameworks e principi dell'information security management (ISO/IEC 27001, GDPR) definendo e realizzando l'ISMS (Information Security Management System) comprensivo di tutte le componenti di gestione della sicurezza (Information Security Strategy, Information Security Policy and organization, Security KPI report, Security measures and controls, Data Protection Policy, Security operations and incident management)

2 - AUDIT DI SICUREZZA: TEST RESILIENZA / TEST DI VULNERABILITÀ

Grado di complessità 4

ADA.14.01.22 - GESTIONE DELLA SICUREZZA DELL'INFORMAZIONE

2.4 PIANIFICAZIONE E GESTIONE AUDIT INFRASTRUTTURE COMPLESSE E DISTRIBUITE

Pianificare i controlli di sicurezza atti a identificare e prevenire le minacce di sicurezza, interne ed esterne all'azienda in piani ciclici definiti nell'ISMS nel contesto 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.)

Grado di complessità 3

2.3 PIANIFICAZIONE AUDIT

Pianificare i controlli di sicurezza atti a identificare e prevenire le minacce di sicurezza, interne ed esterne all'azienda aggiornando gli interventi in piani ciclici definiti nell'ISMS

Grado di complessità 2

2.2 VALUTAZIONE RISULTATI AUDIT

Fornire approfondimenti oggettivi sull'esistenza di vulnerabilità e sull'efficacia delle difese analizzando le vulnerabilità ed individuando soluzioni di sicurezza per mitigarle

Grado di complessità 1

2.1 ATTIVITÀ DI AUDIT

Effettuare Vulnerability Assessment applicativi e infrastrutturali, Penetration test e attività di remediation updates 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.

SCHEDA RISORSE A SUPPORTO DELLA VALUTAZIONE DEL RISULTATO ATTESO 2

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

- Tipologie di rischi, di minacce, vulnerabilità e impatto
- Tipologie di infrastruttura digitale (semplice e localizzata; complessa distribuita e innovativa - numerosità asset, numerosità utenze e accessi, rete web, tecnologie IoT, Big Data, A.I., Cloud, Mobile, NFC - Near Field Communication, Wearable Technology, ecc.)
- Tipologie di processi funzionali (semplici e vitali - VBF) con esigenze di ripristino nel minor tempo possibile
- Requisiti di riservatezza, integrità e disponibilità
- Strumenti tecnologici per la verifica tecnica delle vulnerabilità e degli attacchi di rete
- Information Security Strategy, Information Security Policy and organization, Best practices, standards, frameworks and principles of information security management, Security KPI report, Security measures and controls, Data Protection Policy, Security operations and incident management, Codici deontologici e codice etico (es.: ACM, IEEE, IS-SA)
- Risk Management policy
- Processo e procedure di audit interno dell'ICT
- Problematiche di sicurezza legate al cloud computing (es.: rischi di sistema/virtualizzazione hardware)
- 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.)
- Tipologie di problemi di sicurezza dei dispositivi mobili (es.: vulnerabilità Bluetooth)
- BYOD Policies
- Architetture di Information and Communication Security

TECNICHE TIPICHE DI REALIZZAZIONE/CONDUZIONE DELLE ATTIVITÀ

- Best practices, standards, frameworks e principi dell'information security management (ISO/IEC 27001, GDPR)
- Tecniche di "hacking" e di analisi statica e dinamica
- Analisi dei rischi di Sicurezza, Best practices, standards, frameworks and principles of information security management, Common threats, attacks, vulnerabilities, and their consequences,
- Tecniche di forensics, threat intelligence e intrusion detection
- Tecniche di rilevamento della sicurezza, incluse quelle mobili e digitali
- Tecniche di security by design & by default, in linea con i requisiti normativi di protezione del software e del dato
- Tecniche di Social Engineering
- 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

ADA.14.01.22 - GESTIONE DELLA SICUREZZA DELL'INFORMAZIONE

anomalie, incidenza dei falsi positivi e dei falsi negativi, NIDS basati sulla firma, tecniche di decodifica del protocollo, deep-packet inspection)

- Tecniche del Digital Forensics Process (Data Collection, Examination and Analysis, Reporting)

OUTPUT TIPICI DELLE ATTIVITÀ

- ISMS (Information Security Management System) definito, comprensivo di tutte le componenti di gestione della sicurezza (Information Security Strategy, Information Security Policy and organization, Security KPI report, Security measures and controls, Data Protection Policy, Security operations and incident management)
- Risk Inventory e Piani di ripristino (Information Security Risk Treatment Plan) nell'ISMS con policy di gestione del rischio (Risk Management Policy) definiti
- Security KPI report nell'ISMS e soluzioni e tecnologie di sicurezza per la protezione del sistema informativo con S.W.O.T. analysis sulla sicurezza dei sistemi e delle applicazioni definiti
- Vulnerability Assessment applicativi e infrastrutturali, Penetration test e attività di remediation updates svolte,
- Soluzioni di sicurezza per le vulnerabilità individuate
- Controlli di sicurezza atti a identificare e prevenire le minacce di sicurezza, interne ed esterne svolti
- Attacchi sulla disponibilità dei servizi causati da tecniche di denial-of-service semplice (DOS) e distribuito (DDOS) prevenuti
- Accessi illegali (es.: backdoor, trojan, spyware, ransomware) prevenuti
- Supporto e consulenza per il Social Engineering erogate

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

ESTENSIONE SUGGERITA DI VARIETÀ PRESTAZIONALE

1. Le tipologie di ISMS
2. L'insieme dei metodi di audit
3. L'insieme dei metodi di Risk inventory e piani di ripristino (Information Security Risk Treatment) in contesti funzionali vitali per il business (VBF)
4. Un set di infrastrutture tecnologiche complesse e distribuite con tecnologie digitali innovative e altamente vulnerabili

DISEGNO TIPO DELLA VALUTAZIONE

1. Prova prestazionale: sulla base del set dato, definizione di un ISMS con Risk Inventory e piani di ripristino e la realizzazione di Audit con analisi dei risultati e preparazione di un piano di miglioramento e di intervento sull'ISMS definito.
2. Colloquio tecnico: Contenuti di un ISMS, gestione e preparazione di un Audit

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/>