ALLEGATO "1"

[K1.8] ESPERTO IN SICUREZZA INFORMATICA

Descrizione sintetica:
L'Esperto/a in sicurezza informatica opera in autonomia nell'analisi dei sistemi digitali hardware e software e nella valutazione di possibili vulnerabilità e rischi alla sicurezza dei sistemi. In tale ambito, l'Esperto/a in sicurezza informatica agisce, secondo i principi di security by design per un'efficace ed efficiente gestione della sicurezza informatica. Inoltre, testa la sicurezza dei sistemi contro intrusioni, virus e minacce - intenzionali o accidentali - la recuperabilità di dati e operazioni, a seguito di incidenti o malfunzionamenti e la corretta funzione di protezione delle informazioni, mediante opportune tecniche di crittografia. Individua soluzioni per la mitigazione dei possibili rischi, tramite opportune misure di sicurezza dei sistemi e supporta nelle attività di ripristino delle corrette funzionalità dei sistemi.

SISTEMI DI REFERENZIAZIONE	
Sistema di riferimento	**Denominazione**
Settore economico-professionale (S.E.P.)	14. Servizi digitali
Area/e di Attività (AdA) del Repertorio nazionale delle qualificazioni regionali a cui il profilo afferisce	AdA.14.01.22 - Gestione della Sicurezza dell'Informazione
Livello E.q.f.	6
Posizione classificatoria ISTAT CP 2011	2.1.1.5.4 - Specialisti in sicurezza informatica
Posizione/i classificatoria/e ISTAT ATECO 2007	62.01.00 - Produzione di software non connesso all'edizione 62.02.00 - Consulenza nel settore delle tecnologie dell'informatica 62.03.00 – Gestione di strutture e apparecchiature informatiche hardware – housing (esclusa la riparazione) 62.09.09 - Altre attività dei servizi connessi alle tecnologie dell'informatica nca 63.11.20 - Gestione database (attività delle banche dati) 63.11.30 – Hosting e fornitura di servizi applicativi (ASP) 63.12.00 – Portali web

UNITÀ DI COMPETENZA – Analisi delle vulnerabilità software e hardware e della conformità alla normativa vigente
RISULTATO ATTESO DALL'ESERCIZIO DELLA COMPETENZA Analizzare sistemi digitali, per le componenti hardware e software, dati ed operazioni, al fine di rilevarne rischi di sicurezza e vulnerabilità rispetto alle possibili minacce ed alla continuità di funzionamento ed integrità, individuando ed applicando metodi e norme di riferimento e supportando i relativi processi decisionali di adeguamento
LIVELLO E.q.f.: 6

CONOSCENZE

- Architettura hardware e software dei sistemi digitali
- Sistemi digitali ed ingegneria del software
- Fondamenti teorici della sicurezza dei sistemi digitali
- Evoluzione ed attuale scenario delle principali vulnerabilità note
- Metodologie e framework di riferimento per la misurazione vulnerabilità (es. CVSS, NVD) e conseguenti strategie di mitigazione
- Metodi e strumenti per attività di Penetration Testing
- Application Security tools (Static and Dynamic Application Security Testing)
- Awareness, Red Teaming e Lesson Learned Techniques
- Metodi di valutazione dei rischi per la sicurezza legati alle componenti hardware e software del sistema digitale
- Metodi di valutazione di rischi per la sicurezza legati alle componenti del sistema digitale dedicate al networking (protocolli, connessioni, apparecchiature di rete)
- Quadro normativo nazionale e comunitario in materia di sicurezza informatica, cybersecurity
- Quadro normativo nazionale: Perimetro di Sicurezza Nazionale Cibernetica
- Quadro normativo nazionale e comunitario in materia di protezione dei dati personali
- Standard e framework nazionali ed internazionali in ambito cybersecurity (Security by design, Sistema di Gestione per la Sicurezza delle Informazioni – ISO 27001, Sistemi di gestione per la continuità operativa ISO 22301, NIST, Framework Nazionale per la Cybersecurity e la data protection – FNCS, NIST SP800-9
- Standard e framework di riferimento per la definizione del processo di gestione della qualità dei dati (Data Quality Management)
- Fondamenti di organizzazione aziendale
- Fondamenti di project management
- Inglese tecnico per l'informatica

ABILITA'

- Analizzare l'architettura del sistema digitale, per individuare i possibili punti di accesso al sistema o alle informazioni in esso contenute
- Analizzare i requisiti richiesti al sistema digitale dalle previsioni normative vigenti in materia di privacy e sicurezza informatica
- Individuare le vulnerabilità dell'architettura, delle apparecchiature hardware, del software e dei processi di gestione del sistema digitale
- Elaborare documenti di valutazione dei rischi per la sicurezza del sistema digitale, contenenti l'analisi delle minacce e delle vulnerabilità individuate
- Interagire con i responsabili dei vari livelli decisionali, supportando le scelte strategiche in materia di sicurezza dei sistemi digitali

INDICATORI DI VALUTAZIONE DEL POSSESSO DELLA COMPETENZA

Sulla base di indicazioni relative a tipologie di sistemi digitali, all'insieme delle tipologie di potenziali minacce, considerando la criticità dei dati e delle operazioni processate da un determinato sistema, analizzarne i livelli di sicurezza– per le componenti hardware e software –,e identificare il livello di analisi del rischio informatico potenziale

PRESTAZIONE MINIMA ATTESA IN ESITO ALLA VALUTAZIONE

Per almeno una tipologia di sistema digitale e con riferimento all'insieme delle potenziali minacce, sulla base delle indicazioni date, identificazione del livello di rischio potenziale e predisposizione e condivisione della reportistica associata

MODALITÀ DI VALUTAZIONE DEL POSSESSO DELLA COMPETENZA

Audizione, colloquio tecnico e/o prova prestazionale

UNITÀ DI COMPETENZA – Individuazione di soluzioni per la sicurezza dei sistemi hardware e software

RISULTATO ATTESO DALL'ESERCIZIO DELLA COMPETENZA

Individuare, considerando l'esito delle analisi dei rischi e delle vulnerabilità tecniche, processi e soluzioni a protezione del sistema digitale, agendo sulle diverse componenti e funzioni, mediante tecniche di configurazione degli specifici applicativi

LIVELLO E.q.f.: 6

CONOSCENZE

- Principali caratteristiche e funzionalità dei programmi di network scanning ed intrusion detection
- Principali caratteristiche e funzionalità dei proxy e del controllo di connessioni e traffico TCP/IP da client a server
- Tipologie e logiche di funzionamento dei programmi informatici creati per diffondersi e sottrarre informazioni o danneggiare sistemi digitali (virus, worm, trojan, malware, ransomware, ecc…)
- Tipologie e caratteristiche degli attacchi al sistema digitale a livello di IP, TCP/UDP, protocollo applicativo, applicazione, utente
- Caratteristiche e funzionalità dei firewall
- Algoritmi crittografici specifici (SHA, AES, RSA, ecc.) e loro applicazione alla trasmissione sicura dei dati e alla conservazione su file system
- Principali metodi e tecniche di configurazione del sistema di protezione e del firewall
- Elementi di metodologie, tecniche e strumenti in ambito asset management
- Autenticazione federata basata su Single Sign-On (SSO) e Identity Provider
- Sistemi per la creazione e gestione di password complesse
- Principali tipologie e funzionalità di un Security Operation Center
- Sistemi di controllo degli accessi al sistema digitale ed alle reti: Architettura IAM (Identity Access Management), meccanismi di autenticazione distribuita, meccanismi di Strong Authentication
- Elementi di architettura Zero Trust e cenni sull'autenticazione in ambito IoT
- Inglese tecnico per l'informatica

ABILITA'

- Contribuire alle procedure per allestire e mantenere un asset inventory
- Utilizzare programmi di crittografia e cifratura per la protezione dei dati contenuti nel sistema digitale e per la loro comunicazione
- Installare e configurare sistemi di protezione della rete, per garantire la sicurezza, la riservatezza e l'integrità delle connessioni tra client e server
- Installare e configurare un efficace ed efficiente software di protezione dai malware sui dispositivi digitali, per l'individuazione e la rimozione dei programmi informatici finalizzati all'attacco dei sistemi digitali
- Installare e configurare sistemi di controllo degli accessi (IAM), basati su identificazione, autenticazione e autorizzazione, che garantiscano, in modo sostenibile per gli utenti, un uso più sicuro dei sistemi digitali
- Configurare e aggiornare le regole di firewall
- Definire profili di accesso selettivi, individuali o per ruoli (configurazione dello IAM), basati su effettive necessità operative o su una politica di controllo degli accessi preventivamente approvata
- Definire le credenziali di autenticazione per l'identificazione degli utenti autorizzati ad accedere al sistema digitale, prevedendo l'utilizzo delle tecniche più appropriate (user-id, password, smart card, sistemi biometrici, etc.)
- Definire politiche per la creazione e aggiornamento delle password
- Contribuire all'elaborazione di documentazione relativa all'implementazione delle politiche di sicurezza

INDICATORI DI VALUTAZIONE DEL POSSESSO DELLA COMPETENZA
Sulla base di indicazioni relative a tipologie di sistemi digitali ed all'insieme delle minacce applicabili, in coerenza con il piano di trattamento del rischio, in conformità con le normative cogenti ed i regolamenti interni, identificare le soluzioni ed i meccanismi per la protezione della rete
PRESTAZIONE MINIMA ATTESA IN ESITO ALLA VALUTAZIONE
Per almeno una tipologia di sistema digitale e con riferimento all'insieme delle potenziali minacce, sulla base delle regole e dei processi interni, identificare, implementare, configurare e mantenere aggiornato un sistema per il controllo degli accessi e/o un sistema di protezione dei sistemi digitali o delle reti
MODALITÀ DI VALUTAZIONE DEL POSSESSO DELLA COMPETENZA
Audizione, colloquio tecnico e/o prova prestazionale

UNITÀ DI COMPETENZA – Monitoraggio e supporto al ripristino della sicurezza dei sistemi hardware e software

RISULTATO ATTESO DALL'ESERCIZIO DELLA COMPETENZA

Monitorare lo stato di sicurezza dei sistemi digitali, verificando l'efficacia delle soluzioni di protezione adottate e intervenendo in caso di attacchi o malfunzionamenti, supportando il team nella fase di ripristino

LIVELLO E.q.f.: 6

CONOSCENZE

- Principali strumenti e tecniche per l'analisi e gestione degli incidenti informatici: monitoraggio, analisi valutazione e gestione degli eventi informatici (SIEM), individuazione di anomalie
- Principali metodi e tecniche per la classificazione degli eventi ed incidenti informatici (es. tassonomie nazionali/comunitarie, il framework MITRE ATT&CK™)
- Principali metodi, per infrastrutture con soluzioni in locale o su cloud, e strumenti per implementare una politica di backup e restore dei sistemi digitali
- Cenni sulle metodologie e strumenti per la protezione fisica dei sistemi e delle reti
- Fondamenti di crisis management
- Elementi sulle tecniche e infrastrutture di disaster recovery
- Elementi di sistemi di gestione per la continuità aziendale (ISO 22301)
- Cenni sulle metodologie e tecniche di simulazione e role playing per lo svolgimento di test e simulazioni del sistema di gestione della continuità operativa (test di DR e BC)
- Cenni su metodi e tecniche per lo svolgimento di Business Impact Analysis
- Principali standard e framework di riferimento in ambito gestione degli incidenti informatici
- Cenni sul funzionamento e organizzazione del CERT e dei SOC e sul sistema di alert dello CSIRT nazionale
- Fondamenti di organizzazione aziendale
- Fondamenti di project management
- Inglese tecnico per l'informatica

ABILITA'

- Collaborare per il ripristino dell'integrità e del funzionamento delle strutture informatiche di riferimento, danneggiate a seguito di una violazione tentata o riuscita
- Controllare il rispetto delle misure di sicurezza progettate
- Supportare le procedure per il test dei piani di business continuity e disaster recovery
- Configurare strumenti per riconoscere e mitigare attacchi denial of service
- Monitorare il traffico interno ed esterno, riconoscendo potenziali minacce alla sicurezza del sistema digitale
- Monitorare e valutare gli eventi informatici e dei log dei sistemi digitali
- Supportare l'implementazione delle politiche di backup e restore
- Collaborare alla definizione ed esecuzione dei piani di ripristino
- Supportare nell'elaborazione dei piani di Disaster Recovery e Business Continuity che, in caso di incidente grave o interruzione per cause non controllabili, consentano il mantenimento o il ripristino, nel più breve tempo possibile, della corretta funzionalità del sistema digitale
- Monitorare ed interpretare log (server, dispositivi di rete, applicazioni, ecc.)
- Configurare strumenti per l'individuazione e la segnalazione di malware (spyware, backdoor, trojans, ecc.) nei sistemi digitali
- Supportare il design e lo sviluppo di un incident response playbook

INDICATORI DI VALUTAZIONE DEL POSSESSO DELLA COMPETENZA

Sulla base di indicazioni relative a tipologie di sistemi digitali e all'insieme delle minacce applicabili, in coerenza con il piano di gestione del rischio, individuare una procedura di esecuzione, mantenimento e restore dei backup in conformità con i piani di BC e/o DR qualora previsto e in particolare considerando l'esito della B.I.A.

PRESTAZIONE MINIMA ATTESA IN ESITO ALLA VALUTAZIONE Per almeno una tipologia di sistema digitale, considerando il contesto ed il processo di riferimento anche in coerenza con quanto previsto dalla B.I.A., eseguire un test dei piani di Business Continuity o Disaster Recovery, precedentemente forniti, nonché le operazioni e le tecniche per il ripristino dei dati, tenendo in considerazione la normativa di riferimento, valutandone l'esito e identificando eventuali piani di rimedio
MODALITÀ DI VALUTAZIONE DEL POSSESSO DELLA COMPETENZA Audizione, colloquio tecnico e/o prova prestazionale