



EUCIP - IT Administrator

Modulo 5 – Sicurezza IT

Versione 2.0

Modulo 5 : Obiettivi

Modulo 5 Il mdule 5, **Sicurezza IT**, richiede al candidato di avere familiarità con vari aspetti della sicurezza e della protezione dei dati sia in un singolo PC che in un ambiente di rete, anche connesso ad Internet. Più specificamente il candiadato dovrà essere in grado di proteggere dati e risorse della sua azienda da perdite, virus ed attacchi sapendo utiizzare gli strumenti normalmente disponibili per questo scopo.

| Categoria | Area | Riferim. | Argomento |
|---------------|--|----------|---|
| 5.1. Generale | 5.1.1. Principi di base | 5.1.1.1 | Conoscere i concetti fondamentali di: confidenzialità, integrità. |
| | | 5.1.1.2 | Essere al corrente degli obiettivi di: disponibilità, autenticità, non-ripudio. |
| | 5.1.2. Analisi e gestione del rischio | 5.1.2.1 | Conoscere i principali elementi di analisi del rischio (valore dei dati da proteggere, minacce, vulnerabilità del sistema, livello di rischio, violazione, impatto delle perdite). |
| | | 5.1.2.2 | Conoscere la classificazione convenzionale delle misure (funzioni di sicurezza) usate in tecniche di gestione del rischio (identificazione/autenticazione, controllo d'accesso, attribuzione di responsabilità, verifica (audit), riuso degli oggetti, accuratezza, affidabilità dei servizi critici, sicurezza d'interscambio dati). |
| | | 5.1.2.3 | Conoscere e distinguere i concetti di: funzionalità, garanzia. Capire l'importanza di entrambe nel quadro di un'efficace gestione del rischio. |
| | 5.1.3 Aspetti organizzativi della sicurezza | 5.1.3.1 | Conoscere il ruolo delle politiche di sicurezza nell'organizzazione dei sistemi di controllo. |
| | | 5.1.3.2 | Conoscere i processi fondamentali da instaurare in un'organizzazione che punti alla sicurezza informatica. |
| | | 5.1.3.3 | Essere consci della necessità di pianificare soluzioni di disaster recovery e business continuity. |
| | | 5.1.3.4 | Conoscere le responsabilità di tutti i soggetti coinvolti nella sicurezza aziendale (responsabili della sicurezza, amministratori/supervisor di sistema, utenti individuali). |
| | | 5.1.3.5 | Conoscere modalità e fasi d'interazione con i centri CSIRT (Computer Security Incident Response Team). |
| | 5.1.4 Norme ed autorità di standardizzazione | 5.1.4.1 | Essere informati su denominazione e ruolo delle principali autorità internazionali di standardizzazione. |

| Categoria | Area | Riferim. | Argomento |
|-------------------|---------------------------------|----------|--|
| | | 5.1.4.2 | Essere informati su criteri e standard per la valutazione dei livelli di garanzia (ITSEC, Common Criteria). |
| | | 5.1.4.3 | Conoscere gli elementi essenziali dei requisiti normativi (standard ISO/IEC 17799, BS 7799 parte 2) per la definizione d'infrastrutture e sistemi di gestione della sicurezza. |
| | | 5.1.4.4 | Conoscere i processi di standardizzazione relativi ad Internet . |
| 5.2. Crittografia | 5.2.1 Generale | 5.2.1.1 | Conoscere gli utilizzi base dellacrittografia: crittografia simmetrica, asimmetrica, algoritmi di hashing. |
| | 5.2.2 Crittografia simmetrica | 5.2.2.1 | Essere al corrente dei principi fondamentali di crittografia simmetrica. |
| | | 5.2.2.2 | Conoscere i principali algoritmi a chiave segreta, e le relative differenze (algoritmi DES, 3DES, AES etc). |
| | 5.2.3 Crittografia asimmetrica | 5.2.3.1 | Essere al corrente dei principi fondamentali di crittografia asimmetrica. |
| | | 5.2.3.2 | Conoscere i principali algoritmi a chiave pubblica. |
| | 5.2.4 Funzioni di hash e digest | 5.2.4.1 | Essere al corrente dei principi fondamentali delle funzioni di hash/digest. |
| | | 5.2.4.2 | Conoscere i principali algoritmi di hashing. |
| | 5.2.5 Confronto fra metodi | 5.2.5.1 | Conoscere i principali vantaggi/svantaggi dei sistemi di cifratura simmetrica e asimmetrica. |
| | | 5.2.5.2 | Essere in grado di distinguere i livelli di sicurezza e dimensione delle chiavi nella crittografia simmetrica ed asimmetrica.. |
| | | 5.2.5.3 | Conoscere il problema della distribuzione delle chiavi nei sistemi a cifratura simmetrica e asimmetrica. |
| | | 5.2.5.4 | Comprendere il ruolo del software "open source" nella diffusione e robustezza della crittografia. |
| | 5.2.6 Ambiti d'impiego | 5.2.6.1 | Sapere in che modo utilizzare i meccanismi di cifratura per garantire l'autenticità. |
| | | 5.2.6.2 | Essere al corrente dell'uso delle funzioni di hash/digest per consolidare l'integrità dei dati e l'autenticazione. |
| | | 5.2.6.3 | Conoscere i principali aspetti della firma digitale inerenti la non-ripudiabilità e autenticazione. |
| | | 5.2.6.4 | Conoscere le principali caratteristiche della crittografia inerenti la confidenzialità. |

| Categoria | Area | Riferim. | Argomento |
|---|------------------------------|----------|--|
| | 5.2.7 Applicazioni | 5.2.7.1 | Essere al corrente dell'uso della crittografia a protezione delle transazioni on-line, quali servizi di e-commerce ed e-banking. |
| | | 5.2.7.2 | Essere al corrente dell'uso della firma digitale per realizzare la non-ripudiabilità. |
| | | 5.2.7.3 | Conoscere gli aspetti essenziali del funzionamento di PGP. |
| | | 5.2.7.4 | Essere in grado d'installare e configurare un software di gestione del protocollo PGP. |
| | | 5.2.7.5 | Conoscere principi di funzionamento di SSH. |
| | | 5.2.7.6 | Essere in grado d'installare e configurare un software di gestione del protocollo SSH. |
| | | 5.2.7.7 | Conoscere i principi di funzionamento di S/MIME. |
| | | 5.2.7.8 | Conoscere i principi di funzionamento di SSL. |
| | | 5.2.7.9 | Essere al corrente dell'uso delle smartcard. |
| 5.3 Autenticazione e controllo di accesso | 5.3.1. Concetti generali | 5.3.1.1 | Conoscere differenti schemi di autenticazione. |
| | 5.3.2. Password | 5.3.2.1 | Conoscere i principi di creazione e amministrazione delle password. |
| | 5.3.3 Token | 5.3.3.1 | Conoscere i principi di autenticazione tramite token. |
| | 5.3.4 Biometria | 5.3.4.1 | Conoscere differenti schemi di autenticazione biometrica e la relativa efficacia. |
| | 5.3.5 Autenticazione in rete | 5.3.5.1 | Conoscere e differenti necessità e caratteristiche dell'autenticazione in rete rispetto all'autenticazione da host. |
| | | 5.3.5.2 | Conoscere differenti protocolli di rete per l'autenticazione utente (PAP, CHAP etc). |
| | | 5.3.5.3 | Conoscere differenti protocolli di rete per l'autenticazione di processi distribuiti. |
| | | 5.3.5.4 | Essere consci della complessità dei sistemi ad architettura "single sign-on". |
| | | 5.3.5.5 | Conoscere i principi generali di funzionamento del sistema di autenticazione Kerberos. |
| | 5.3.6 Controllo di accesso | 5.3.6.1 | Conoscere i principi concettuali alla base del controllo d'accesso. |
| | | 5.3.6.2 | Sapere cos'è l' Access Control List (ACL) e la List of Capabilities. |

| Categoria | Area | Riferim. | Argomento |
|--------------------|------------------|----------|--|
| | | 5.3.6.3 | Conoscere le modalità di gestione dell'accesso per i file system correnti. |
| | | 5.3.6.4 | Conoscere le modalità di gestione dell'accesso ai RDBMS. |
| 5.4 Disponibilità | 5.4.1 Generale | 5.4.1.1 | Conoscere i diversi tipi di esigenze di disponibilità dei dati. |
| | | 5.4.1.2 | Conoscere i diversi tipi di esigenze infrastrutturali dei sistemi informatici (gruppi di continuità, climatizzazione, cablaggi etc). |
| | 5.4.2 Resilienza | 5.4.2.1 | Essere al corrente delle diverse metodologie di replicazione in tempo reale delle unità disco (RAID etc). |
| | | 5.4.2.2 | Essere al corrente delle diverse metodologie di replicazione host e meccanismi di distribuzione e bilanciamento del carico (load distribution e load balancing). |
| | | 5.4.2.3 | Conoscere diversi tipi d'infrastrutture per la disponibilità della rete (per LAN, WAN, WLAN etc). |
| | 5.4.3 Backup | 5.4.3.1 | Essere in grado di definire ed utilizzare efficaci procedure di backup (locali e di rete). |
| | | 5.4.3.2 | Saper verificare il buon esito di un processo di backup. Conoscere le procedure per il ripristino. |
| 5.5 Codice maligno | 5.5.1. Programmi | 5.5.1.1 | Sapere con quali strumenti è possibile controllare direttamente un computer: sistema operativo, programmi, comandi di shell, macro. |
| | | 5.5.1.2 | Essere al corrente delle esigenze di filtraggio e validazione dell'input ai fini della sicurezza. |
| | | 5.5.1.3 | Essere al corrente dei differenti tipi di overflow e le possibilità di sfruttamento per l'esecuzione di codice. |
| | | 5.5.1.4 | Essere al corrente della possibilità di attacchi "cross-site scripting". |
| | | 5.5.1.5 | Essere al corrente della possibilità di attacchi "denial-of-service" (DoS), e come i diversi ambienti e risorse ne risultino affetti. |
| | | 5.5.1.6 | Conoscere le vie d'accesso ad un sistema informatico: floppy, CD-ROM, email, navigazione web, client di chat. |
| | | 5.5.1.7 | Sapere quali buone prassi (good practices) considerare negli accessi ad Internet. |
| | | 5.5.1.8 | Conoscere i rischi legati ai programmi adware e agenti spyware. |

| Categoria | Area | Riferim. | Argomento |
|--------------------------------------|--------------------------|-----------------|---|
| | 5.5.2 Tipi di file | 5.5.2.1 | Sapere in che modo l'interfaccia grafica (GUI) riconosce l'azione da eseguire su un file tramite l'estensione e tipo MIME associati. |
| | | 5.5.2.2 | Sapere in che modo il client di posta riconosce l'azione da eseguire su un allegato tramite l'estensione e tipo MIME associati. |
| | 5.5.3 Codice scaricabile | 5.5.3.1 | Sapere che le applicazioni possono gestire più di semplice testo eseguendo comandi di SO tramite le macro. |
| | | 5.5.3.2 | Sapere in che modo i malintenzionati possono far uso illecito dei tipi MIME, e le possibili contromisure. |
| | | 5.5.3.3 | Sapere in che modo i malintenzionati possono far uso illecito delle macro, e le possibili contromisure. |
| | | 5.5.3.4 | Sapere in che modo i malintenzionati possono far uso illecito di applet, e le possibili contromisure. |
| | 5.5.4 Codice virale | 5.5.4.1 | Conoscere le principali categorie di codici virali (trojan, virus propriamente detti, worm, etc). |
| | | 5.5.4.2 | Conoscere i principi essenziali di funzionamento di un programma antivirus. |
| | | 5.5.4.3 | Essere al corrente dei limiti e delle fallacità dei programmi antivirus. |
| | | 5.5.4.4 | Essere in grado d'installare, configurare, mantenere aggiornato un programma antivirus. |
| | | 5.5.4.5 | Sapere quali buone prassi (good practices) considerare nel proteggere e utilizzare postazioni workstation. |
| 5.6 Infrastruttura a chiave pubblica | 5.6.1 PKI | 5.6.1.1 | Essere al corrente delle problematiche di distribuzione della chiave pubblica, anche riguardo l'identificazione del possessore. |
| | | 5.6.1.2 | Conoscere il significato di: certificato, liste dei certificati revocati (CRL). |
| | | 5.6.1.3 | Conoscere i certificati X.509.V3. |
| | | 5.6.1.4 | Conoscere il significato dell'acronimo PKI e le relative componenti fondamentali: Certification Authority, Registration Authority, etc. |
| | | 5.6.1.5 | Essere in grado d'utilizzare un browser per generare le chiavi e la richiesta di certificazione a una CA. |
| | | 5.6.1.6 | Essere in grado d'importare/esportare un certificato in un browser. |

| Categoria | Area | Riferim. | Argomento |
|-----------------------|----------------------------|-----------------|---|
| | | 5.6.1.7 | Essere in grado d'accedere alle liste CRL dal browser, e sapere effettuare controlli sulla validità dei certificati tramite OCSP (Online Certificate Status Protocol). |
| | | 5.6.1.8 | Essere in grado d'importare una lista CRL nel browser, e sapere effettuare controlli sulla validità dei certificati tramite OCSP (Online Certificate Status Protocol). |
| | 5.6.2 Servizi di directory | 5.6.2.1 | Conoscere i server LDAP. |
| | | 5.6.2.2 | Utilizzare il browser per effettuare un'interrogazione a un server LDAP che restituisca i dati relativi a uno specifico DN (Distinguished Name). |
| | | 5.6.2.3 | Conoscere il significato di: Common Name, Distinguished Name, attributo. |
| | | 5.6.2.4 | Conoscere il significato di X509. |
| | | 5.6.2.5 | Sapere in che modo i server LDAP possono supportare la gestione e autenticazione dei profili utente. |
| 5.7 Sicurezza di rete | 5.7.1. Concetti di base | 5.7.1.1 | Essere al corrente dei fondamenti di comunicazione analogica/digitale. Conoscere i principi di base relativi alla sicurezza nell'architettura ISO/OSI. |
| | | 5.7.1.2 | Conoscere la differenza fra comunicazioni continue e comunicazioni a pacchetto. |
| | | 5.7.1.3 | Conoscere le modalità di funzionamento di Ethernet (indirizzo MAC, CSMA/CD). |
| | | 5.7.1.4 | Comprendere i principali aspetti del protocollo TCP/IP (indirizzi, numeri di porta, principali operazioni). |
| | | 5.7.1.5 | Conoscere l'incapsulamento di TCP/IP in Ethernet. |
| | | 5.7.1.6 | Comprendere i servizi di rete effettuati in ambiente TCP/IP. |
| | | 5.7.1.7 | Essere in grado d'installare e far funzionare un analizzatore di rete. |
| | | 5.7.1.8 | Essere al corrente delle principali tipologie di attacco allo stack TCP/IP: sniffing di pacchetti, IP spoofing, rerouting, TCP hijacking, attacco DOS multi-IP (DDOS, Distributed Denial Of Service) etc. |
| | | 5.7.1.9 | Sapere in che modo il ricorso allo switching e reti locali virtuali può migliorare la sicurezza della LAN. |
| | 5.7.2 Reti wireless | 5.7.2.1 | Conoscere le principali tecnologie wireless. |
| | | 5.7.2.2 | Conoscere i problemi di sicurezza relativi alle differenti tecnologie wireless, e le possibili soluzioni. |

| Categoria | Area | Riferim. | Argomento |
|-----------|--|----------|---|
| | 5.7.3 Servizi | 5.7.3.1 | Essere informati dei servizi di rete offerti dalle applicazioni sui punti d'accesso ai server. |
| | | 5.7.3.2 | Conoscere quale insieme minimo e più sicuro di servizi è prudente abilitare su server Internet. |
| | | 5.7.3.3 | Conoscere quale insieme di servizi è di prassi abilitato sui server locali (non-Internet). |
| | | 5.7.3.4 | Essere al corrente dei più noti impieghi illeciti: utilizzi abusivi, denial of service, contraffazione dei dati etc. |
| | | 5.7.3.5 | Conoscere i rischi legati all'utilizzo fraudolento di DNS. |
| | | 5.7.3.6 | Essere al corrente dei comuni schemi di autenticazione e delle rispettive vulnerabilità. |
| | | 5.7.3.7 | Essere consci che debolezze dei protocolli o vulnerabilità nel software possono essere sfruttate per attaccare un server in rete. |
| | | 5.7.3.8 | Essere consci che la potenziale vulnerabilità dei client è pari a quella dei server. |
| | | 5.7.3.9 | Essere al corrente dei rischi legati alle tecnologie e programmi peer-to-peer. |
| | | 5.7.3.10 | Sapere quali buone prassi(good practices) considerare per proteggere e utilizzare un server locale (non-Internet). |
| | | 5.7.3.11 | Sapere quali buone prassi(good practices) considerare nel proteggere e utilizzare un server Internet. |
| | 5.7.4 Controllo d'accesso | 5.7.4.1 | Essere al corrente delle modalità di autenticazione alla rete, e sapere in che modo gestirle. |
| | | 5.7.4.2 | Conoscere l'autenticazione alla rete mediante chiave cifrata, e sapere in che modo gestirla. |
| | | 5.7.4.3 | Conoscere l'autenticazione al dominio. |
| | 5.7.5 Gestione dei log | 5.7.5.1 | Ricavare dai log di sistema le informazioni maggiormente rilevanti per la sicurezza. |
| | | 5.7.5.2 | Sapere in che modo configurare il logging delle applicazioni. |
| | | 5.7.5.3 | Sapere in che modo predisporre un servizio di log centralizzato. |
| | | 5.7.5.4 | Sapere in che modo proteggere i log di sistema da manomissioni. |
| | 5.7.6 Controllo d'accesso dei servizi HTTP | 5.7.6.1 | Conoscere la differenza fra siti web HTTP e HTTPS. |

| Categoria | Area | Riferim. | Argomento |
|-----------|--|----------|---|
| | | 5.7.6.2 | Sapere in che modo l'interazione fra il servizio web e le altre componenti di sistema influenza la sicurezza. |
| | | 5.7.6.3 | Essere in grado d'implementare una versione sicura di un sito web non protetto, generando chiavi e richiesta di certificazione, e inserendo chiavi e certificati. |
| | | 5.7.6.4 | Essere in grado di configurare un sito web per l'identificazione e autorizzazione dei client tramite password in formato testo. |
| | | 5.7.6.5 | Essere in grado di configurare un sito web per l'identificazione e autorizzazione dei client tramite certificato, come in SSL V.3. |
| | | 5.7.6.6 | Sapere quale tipo d'accesso sugli oggetti d'una directory può essere controllato nei siti web. |
| | | 5.7.6.7 | Essere in grado d'applicare le corrette limitazioni d'accesso su specifiche directory di un sito web. |
| | 5.7.7 Controllo d'accesso dei servizi di posta elettronica | 5.7.7.1 | Essere consci delle possibilità di contraffare il mittente ed altre informazioni relative ad un messaggio di posta elettronica, |
| | | 5.7.7.2 | Essere in grado d'impostare l'accesso ai servizi email POP/IMAP con semplice autenticazione password. |
| | | 5.7.7.3 | Essere in grado d'impostare l'accesso ai servizi email POP/IMAP con autenticazione cifrata e certificato. |
| | | 5.7.7.4 | Sapere in che modo abilitare l'autenticazione SMTP utilizzando SASL. |
| | | 5.7.7.5 | Essere in grado d'impostare l'accesso ai servizi email POP/IMAP tramite un canale cifrato. |
| | | 5.7.7.6 | Conoscere il significato del termine SPAM e le possibili contromisure. |
| | 5.7.8 Firewall | 5.7.8.1 | Sapere cos'è un firewall, le relative limitazioni e potenzialità, le differenti architetture (gateway, circuiti etc). |
| | | 5.7.8.2 | Essere al corrente del significato del termine: DMZ. |
| | | 5.7.8.3 | Sapere cos'è un proxy, e le relative modalità di funzionamento. |
| | | 5.7.8.4 | Essere al corrente dell'utilizzo del proxy per limitare l'utilizzo di indirizzi IP e proteggere i sistemi interni della rete. |
| | | 5.7.8.5 | Sapere cos'è la traduzione d'indirizzo di rete (NAT), e come influenza la sicurezza. |

| Categoria | Area | Riferim. | Argomento |
|------------------------------------|--|----------|---|
| | | 5.7.8.6 | Conoscere i principi di funzionamento dei firewall IP nel filtrare l'accesso ai servizi IP. |
| | | 5.7.8.7 | Conoscere i principi di funzionamento dei 'proxy firewall' nel filtrare i protocolli. |
| | | 5.7.8.8 | Essere in grado d'installare un firewall e un proxy server. Sapere implementare una politica di sicurezza. |
| | | 5.7.8.9 | Essere in grado di mascherare gli indirizzi IP mediante il firewall. |
| | | 5.7.8.10 | Essere in grado di configurare il NAT sul firewall. |
| | | 5.7.8.11 | Essere in grado d'impostare delle regole d'accesso sul firewall. |
| | 5.7.9 Rilevamento delle intrusioni (IDS) | 5.7.9.1 | Conoscere le principali tipologie di Intrusion Detection Systems (IDS). |
| | | 5.7.9.2 | Sapere in che modo monitorare i log di sicurezza e eventi di sistema. |
| | | 5.7.9.3 | Essere informati sui sistemi di prevenzione delle intrusioni (Intrusion Prevention Systems). |
| | | 5.7.9.4 | Essere in grado di allestire e configurare in maniera essenziale un sistema di Intrusion Prevention System (IDS). |
| | 5.7.10 Reti private virtuali | 5.7.10.1 | Conoscere i protocolli IPSEC/IKE. |
| | | 5.7.10.2 | Conoscere le reti private virtuali basate su tecnologia MPLS. |
| | | 5.7.10.3 | Sapere quale livello di sicurezza è garantito dalle differenti tecnologie. |
| | | 5.7.10.4 | Conoscere altri protocolli d'incapsulamento (PPTP, IP over UDP etc), e il relativo impiego. |
| | | 5.7.10.5 | Essere in grado d'installare un client VPN. |
| 5.8 Aspetti sociali, etici, legali | 5.8.1 Principi di base | 5.8.1.1 | Conoscere il significato di: riservatezza (privacy), anonimato, diritto allo pseudonimo. |
| | 5.8.2 PET | 5.8.2.1 | Conoscere l'equilibrio fra esigenze di autenticazione e diritto alla privacy. |
| | | 5.8.2.2 | Conoscere le tecnologie per l'incremento della privacy (PET) |
| | | 5.8.2.3 | Conoscere i cookie e le relative modalità di gestione. |
| | | 5.8.2.4 | Essere consapevoli delle implicazioni etiche (controlli nel lavoro, sorveglianza). |

| Categoria | Area | Riferim. | Argomento |
|-----------|-------------------------|----------|--|
| | | 5.8.2.5 | Conoscere i principali codici di riferimento: codici deontologici, codici etici (casi studiati: ACM, BCS, IEEE, etc). |
| | | 5.8.2.6 | Conoscere terminologia e aspetti essenziali dell'etica hacker |
| | | 5.8.2.7 | Conoscere le principali forme di crimini informatici. |
| | | 5.8.2.8 | Conoscere le mailing-list e URL principali relativi alle aree della sicurezza informatica |
| | | 5.8.2.9 | Essere consapevoli degli aspetti etici e di tutela della privacy relativi alla biometria. |
| | 5.8.3 Normative europee | 5.8.3.1 | Conoscere gli aspetti legali della firma digitale, anche in relazione alle direttive della Comunità Europea. |
| | | 5.8.3.2 | Conoscere la legge a tutela e trattamento dei dati personali (Direttiva Europea 95/46), e relative implicazioni. |
| | | 5.8.3.3 | Conoscere gli aspetti legali generali relativi all'evidenza di reato e alle perizie informatiche giudiziarie (Computer Forensics). |