MODULO 6 - IT SECURITY Versione 2

1 Concetti di sicurezza

1.1 Minacce ai dati

1.1.1 Distinguere tra dati e informazioni.

1.1.2 Comprendere i termini "crimine informatico" e "hacking".

1.1.3 Riconoscere le minacce dolose e accidentali ai dati provocate da singoli individui, fornitori di servizi, organizzazioni esterne.

1.1.4 Riconoscere le minacce ai dati provocate da circostanze straordinarie, quali fuoco, inondazioni, guerre, terremoti.

1.1.5 Riconoscere le minacce ai dati provocate dall'uso del cloud computing, quali: controllo sui dati, potenziale perdita di riservatezza (privacy).

1.2. Valore delle informazioni

1.2.1 Comprendere le caratteristiche fondamentali della sicurezza delle informazioni, quali: confidenzialità, integrità, disponibilità.

1.2.2 Comprendere i motivi per proteggere le informazioni personali, quali evitare il furto di identità o le frodi, mantenere la riservatezza.

1.2.3 Comprendere i motivi per proteggere informazioni di lavoro su computer e dispositivi mobili, quali: evitare furti, utilizzi fraudolenti, perdite accidentali di dati, sabotaggi.

1.2.4 Identificare i principi comuni per la protezione, conservazione e controllo dei dati e della riservatezza, quali: trasparenza, scopi legittimi, proporzionalità delle misure in rapporto ai danni.

1.2.5 Comprendere i termini "soggetti dei dati" e "controllori dei dati", e come si applicano nei due casi i principi di protezione, conservazione e controllo dei dati e della riservatezza.

1.2.6 Comprendere l'importanza di attenersi alle linee guida e alle politiche per l'uso dell'ICT e come fare per ottenerle.

1.3 Sicurezza personale

1.3.1 Comprendere il termine "ingegneria sociale" e le sue implicazioni, quali accesso non autorizzato a sistemi informatici, raccolta non autorizzata di informazioni, frodi.

1.3.2 Identificare i metodi applicati dall'ingegneria sociale, quali chiamate telefoniche, phishing, shoulder surfing (spiare alle spalle), al fine di carpire informazioni personali.

1.3.3 Comprendere il termine "furto di identità" e le sue implicazioni personali, finanziarie, lavorative, legali.

1.3.4 Identificare i metodi applicati per il furto di identità, quali acquisire informazioni a partire da oggetti e informazioni scartati (information diving); uso di dispositivi fraudolenti di lettura (skimming); inventare uno scenario pretestuoso (pretexting).

1.4 Sicurezza dei file

1.4.1 Comprendere gli effetti di attivare/disattivare le impostazioni di sicurezza relative alle macro.

1.4.2 Comprendere i vantaggi e i limiti della cifratura. Comprendere l'importanza di non divulgare o di non perdere la password, la chiave o il certificato di cifratura.

1.4.3 Cifrare un file, una cartella, una unità disco.

1.4.4 Impostare una password per file quali: documenti, fogli di calcolo, file compressi.

2 Malware

2.1 Tipi e metodi

2.1.1 Comprendere il termine "malware". Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor.

2.1.2 Riconoscere i tipi di malware infettivo e comprendere come funzionano, ad esempio virus e **worm**.

2.1.3 Riconoscere i tipi di malware usati per furto di dati, profitto/estorsione e comprendere come operano, ad esempio: **adware** (*proposta di pubblicità attraverso banner e popup*), **ransomware** (*blocco doloso di un programma con lo scopo di chiedere un riscatto per sbloccarlo*), spyware (*software che invia ad un server remoto i dati di navigazione*), **botnet** (*software capace di prendere il controllo di una rete di computer*), **keylogger** (*software capace di inviare ad un server remoto i caratteri digitati su una tastiera*) e **dialer** (*software capace di cambiare la connessione del modem da un provider ad un altro*).

2.2 Protezione

2.2.1 Comprendere come funziona il software antivirus e quali limitazioni presenta.

2.2.2 Comprendere che il software antivirus dovrebbe essere installato su tutti i sistemi informatici.

2.2.3 Comprendere l'importanza di aggiornare regolarmente vari tipi di software, quali: antivirus, browser web, plug-in, applicazioni, sistema operativo.

2.2.4 Eseguire scansioni di specifiche unità, cartelle, file usando un software antivirus. Pianificare scansioni usando un software antivirus.

2.2.5 Comprendere i rischi associati all'uso di software obsoleto e non supportato, quali: maggiori minacce da parte del malware, incompatibilità.

2.3 Risoluzione e rimozione

2.3.1 Comprendere il termine "quarantena" e l'effetto di messa in quarantena file infetti/sospetti.

2.3.2 Mettere in quarantena, eliminare file infetti/sospetti.

2.3.3 Comprendere che un attacco da malware può essere diagnosticato e risolto usando risorse online quali: siti web di sistemi operativi, antivirus, fornitori di browser web, siti web di autorità preposte.

MODULO 6 - IT SECURITY Versione 2

3 Sicurezza in rete

3.1 Reti e connessioni 3.1.1 Comprendere il termine "rete" e riconoscere i più comuni tipi di rete, quali LAN (rete locale), WLAN (rete locale wireless), WAN (rete geografica), VPN (rete privata virtuale).

3.1.2 Comprendere che la connessione ad una rete ha implicazioni di sicurezza, quali malware, accessi non autorizzati ai dati, difesa della riservatezza.

3.1.3 Comprendere il ruolo dell'amministratore di rete nella gestione delle operazioni di autenticazione, autorizzazione e assegnazione degli account all'interno di una rete; verifica e installazione di patch e aggiornamenti di sicurezza importanti; controllo del traffico di rete e trattamento del malware rilevato su una rete.

3.1.4 Comprendere la funzione e i limiti di un firewall in ambiente domestico e di lavoro.

3.1.5 Attivare, disattivare un firewall personale. Consentire o bloccare l'accesso attraverso un firewall personale a un'applicazione, servizio/funzione.

3.2 Sicurezza su reti wireless

3.2.1 Riconoscere diversi tipi di sicurezza per reti wireless e i loro limiti, quali: WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) / WPA2

(Wi-Fi Protected Access 2), filtraggio MAC (Media Access Control), SSID nascosto (Service Set Identifier).

3.2.2 Essere consapevoli che usando una rete wireless non protetta si va incontro ad attacchi da parte di intercettatori (eavesdropping), dirottatori di rete (network hijacking), violatori di comunicazioni private (man in the middle).

3.2.3 Comprendere il termine "hotspot personale". RIF. Argomento

3.2.4 Attivare, disattivare un hotspot personale sicuro, connettere in modo sicuro e disconnettere dispositivi informatici.

4 Controllo di accesso

4.1 Metodi

4.1.1 Identificare i metodi per impedire accessi non autorizzati ai dati, quali: nome utente, password, PIN, cifratura, autenticazione a più fattori.

4.1.2 Comprendere il termine "one-time password" e il suo utilizzo tipico.

4.1.3 Comprendere lo scopo di un account di rete.

4.1.4 Comprendere che per accedere alla rete sono necessari un nome utente e una password, e che è importante disconnettere l'account, al termine del collegamento.

4.1.5 Identificare le comuni tecniche di sicurezza biometrica usate per il controllo degli accessi, quali impronte digitali, scansione dell'occhio, riconoscimento facciale, geometria della mano.

4.2 Gestione delle password

4.2.1 Riconoscere buone linee di condotta per la password, quali scegliere le password di lunghezza adeguata e contenenti un numero sufficiente di lettere, numeri e caratteri speciali; evitare di condividerle, modificarle con regolarità, scegliere password diverse per servizi diversi.

4.2.2 Comprendere la funzione e le limitazioni dei software di gestione delle password.

5 Uso sicuro del web

5.1 Impostazioni del browser

5.1.1 Selezionare impostazioni adeguate per attivare, disattivare il completamento automatico, il salvataggio automatico quando si compila un modulo.

5.1.2 Eliminare dati privati da un browser, quali cronologia di navigazione, cronologia di scaricamento, file temporanei di internet, password, cookie, dati per il completamento automatico.

5.2 Navigazione sicura in rete

5.2.1 Essere consapevoli che alcune attività in rete (acquisti, transazioni finanziarie) devono essere eseguite solo su pagine web sicure e con l'uso di una connessione di rete sicura.

5.2.2 Identificare le modalità con cui confermare la autenticità di un sito web, quali: qualità del contenuto, attualità, validità URL, informazioni sulla società o sul proprietario, informazioni di contatto, certificato di sicurezza, validazione del proprietario del dominio.

5.2.3 Comprendere il termine "pharming".

5.2.4 Comprendere la funzione e i tipi di software per il controllo del contenuto, quali software per il filtraggio di internet, software di controllo genitori.

6 Comunicazioni

6.1 Posta elettronica

6.1.1 Comprendere lo scopo di cifrare, decifrare un messaggio di posta elettronica.

6.1.2 Comprendere il termine "firma digitale".

6.1.3 Identificare i possibili messaggi fraudolenti o indesiderati.

6.1.4 Identificare le più comuni caratteristiche del phishing, quali: uso del nome di aziende e di persone autentiche, collegamenti a falsi siti web, uso di loghi e marchi falsi, incoraggiamento a divulgare informazioni personali.

6.1.5 Essere consapevoli che è possibile denunciare tentativi di phishing alle organizzazioni competenti o alle autorità preposte.

6.1.6 Essere consapevoli del rischio di infettare un computer o un dispositivo con malware attraverso l'apertura di un allegato contenente una macro o un file eseguibile.

6.2 Reti sociali

6.2.1 Comprendere l'importanza di non divulgare su siti di reti sociali informazioni riservate o informazioni personali che permettono l'identificazione.
6.2.2 Essere consapevoli della necessità di applicare e di rivedere con regolarità le impostazioni del proprio account su una rete sociale, quali riservatezza dell'account e propria posizione.
6.2.3 Applicare le impostazioni degli account di reti sociali: riservatezza dell'account e propria posizione.
6.2.4 Comprendere i pericoli potenziali connessi all'uso di siti di reti sociali, quali cyber bullismo, adescamento (grooming), divulgazione dolosa di informazioni personali, false identità, link o messaggi fraudolenti o malevoli.
6.2.5 Essere consapevoli che è possibile denunciare usi o comportamenti inappropriati della rete sociale al fornitore del servizio o alle autorità preposte.

6.3 VoIP e messaggistica istantanea

6.3.1 Comprendere le vulnerabilità di sicurezza della messaggistica istantanea e del VoIP (Voice over IP), quali malware, accesso da backdoor, accesso a file, intercettazione (eavesdropping).
6.3.2 Riconoscere i metodi per assicurare la confidenzialità durante l'uso della messaggistica istantanea e del VoIP (Voice over IP), quali cifratura, non divulgazione di informazioni importanti, limitazione alla condivisione di file.

6.4 Dispositivi mobili

6.4.1 Comprendere le possibili implicazioni dell'uso di applicazioni provenienti da "app store" non ufficiali, quali malware per dispositivi mobili, utilizzo non necessario delle risorse, accesso a dati personali, bassa qualità, costi nascosti.
6.4.2 Comprendere il termine "autorizzazioni dell'applicazione".
6.4.3 Essere consapevoli che le applicazioni mobili possono estrarre informazioni private dal dispositivo mobile, quali dettagli dei contatti, cronologia delle posizioni, immagini.
6.4.4 Essere consapevoli delle misure precauzionali e di emergenza da adottare in caso di perdita di un dispositivo mobile, quali disattivazione remota, cancellazione remota dei contenuti, localizzazione del dispositivo.

7 Gestione sicura dei dati

7.1 Messa in sicurezza e salvataggio di dati
7.1.1 Riconoscere i modi per assicurare la sicurezza fisica di computer e dispositivi mobili, quali non lasciarli incustoditi, registrare la collocazione e i dettagli degli apparati, usare cavi antifurto, controllare gli accessi alle sale dei computer.
7.1.2 Riconoscere l'importanza di avere una procedura di copie di sicurezza per ovviare alla perdita di dati da computer e da dispositivi mobili.
7.1.3 Identificare le caratteristiche di una procedura di copie di sicurezza, quali regolarità/frequenza, pianificazione, collocazione del supporto dei dati salvati, compressione dei dati.
7.1.4 Effettuare la copia di sicurezza di dati su un supporto quale: unità disco/dispositivo locale, unità esterna, servizio su cloud.
7.1.5 Ripristinare i dati da una copia di sicurezza su unità disco/dispositivo locale, unità esterna, servizio su cloud.
7.2 Cancellazione e distruzione sicura
7.2.1 Distinguere tra cancellare i dati ed eliminarli in modo permanente.
7.2.2 Comprendere i motivi per eliminare in modo permanente i dati dalle memorie di massa o dai dispositivi mobili.
7.2.3 Essere consapevoli che l'eliminazione del contenuto dai servizi potrebbe non essere permanente, come nel caso dei siti di reti sociali, blog, forum su internet, servizi su cloud.
7.2.4 Identificare i metodi più comuni per distruggere i dati in modo permanente, quali uso di trita documenti, distruzione di memorie di massa/dispositivi, smagnetizzazione, uso di software per la cancellazione definitiva dei dati.