

Dispensa di Sicurezza Informatica (parte 1)

CAPITOLO 1 – CONCETTI DI SICUREZZA

- **Dati e Informazioni**

- Le **informazioni** nelle attività umane semplici sono rappresentate da lingua, disegni, numeri, ecc..
- Nei sistemi informatici, le informazioni sono rappresentate da **dati** (numeri, testo, immagini, ecc.) che di per sé non hanno significato.
- Le informazioni si ottengono **organizzando e interpretando i dati**.

- **Crimine Informatico e Hacking**

- Il **crimine informatico** è l'attività criminale che usa strumenti informatici come computer e internet per scopi illeciti.
- L'**hacking** è la pratica di accedere illegalmente a sistemi altrui per carpire dati, danneggiare o trovarne le falle di sicurezza. I professionisti della sicurezza eseguono test di hacking per valutarne l'affidabilità.
- Nel crimine informatico rientrano: **intercettazione di dati, interferenza sui dati** (danneggiamento, cancellazione, ecc.), **duplicazione non autorizzata e diffusione di virus/malware**.

- **Minacce ai Dati**

- **Minacce dolose e accidentali:** Attacchi esterni, spesso sofisticati (dolose). Persone che chiedono credenziali o accedono senza permesso. Utenti non tecnici o ospiti che accedono a reti senza sicurezza (accidentali).
- **Minacce da circostanze straordinarie:** Eventi naturali (incendi, terremoti) o causati dall'uomo (guerre, attacchi terroristici). Possono causare danni a computer, perdita di dati e interruzione dei servizi. Si affrontano con piani di ripristino e emergenza.
- **Minacce dall'uso del Cloud Computing:** La delega della gestione dei dati a un provider introduce rischi. L'utente ha meno controllo sui dati fisici. C'è il rischio di violazione, uso scorretto o furto dei dati personali/aziendali. La crittografia è utile in questo contesto.

- **Caratteristiche Fondamentali della Sicurezza delle Informazioni**

- Modello **C.I.A. (Confidenzialità, Integrità, Disponibilità)** o C.I.D..
- **Confidenzialità:** Accesso ai dati solo per gli autorizzati. Protezione durante la trasmissione.
- **Integrità:** I dati non devono essere manomessi o modificati senza autorizzazione.
- **Disponibilità:** L'informazione deve essere accessibile quando necessario agli autorizzati.

- **Protezione delle Informazioni**
 - **Informazioni personali:** Importante proteggerle, soprattutto su dispositivi mobili. Rischi di furto di credenziali (email, social, banking) e dati carta di credito. Possibili danni economici e di reputazione.
 - **Informazioni di lavoro:** Cruciali per un'azienda. Vanno protette per ragioni commerciali, legali e per mantenere i rapporti con i partner. Particolarmente importanti i dati dei clienti finanziari. Misure per prevenire furto, perdita, uso improprio, sabotaggio.
- **Principi di Protezione, Conservazione e Controllo dei Dati**
 - La normativa (basata su Direttiva 95/46/CE e D.L. 196/2003 "Codice della privacy") stabilisce principi per il trattamento dei dati personali.
 - Principi chiave: **Trasparenza, Legittimità, Proporzionalità.**
 - Principio di **Conservazione:** Dati conservati per il tempo necessario, in modo sicuro e protetto. Richiede protezioni fisiche, procedurali, logiche, da intrusioni, da perdite.
- **Linee Guida e Politiche per l'Uso dell'ICT**
 - È importante conoscere i pericoli legati all'uso dell'ICT.
 - Le aziende dovrebbero avere **procedure integrate e politiche di sicurezza.**
 - Tali documenti dovrebbero essere resi disponibili a tutto il personale (es. sull'intranet aziendale).
- **Ingegneria Sociale**
 - L'arte di **manipolare psicologicamente** le persone per fargli compiere azioni o rivelare informazioni. Sfrutta fiducia o ignoranza.
 - Implicazioni: **raccolta di informazioni, frode, accesso non autorizzato** (con credenziali rubate).
- **Metodi per il Furto di Identità**
 - Ottenere informazioni personali per sostituirsi alla vittima o agire in suo nome.
 - Tecniche: **Dumpster diving** (rifiuti), **Eavesdrop** (origliare), **Wiretap** (intercettazione comunicazioni), **Phishing** (email ingannevoli), **Shoulder surfing** (spiare alle spalle), **Skimming** (clonazione carta di credito).
- **Sicurezza delle Macro**
 - Le macro possono automatizzare azioni ma anche contenere codice malevolo.
 - L'impostazione di sicurezza raccomandata è **"Disattiva tutte le macro con notifica"** per essere avvisati e scegliere.
- **Crittografia**
 - Tecnica per rendere i dati illeggibili (cifrati) senza la chiave. Protegge da accesso e manomissione non autorizzati.

- **Crittografia simmetrica:** singola chiave (es. Office).
- **Crittografia asimmetrica:** due chiavi (pubblica e privata) per cifrare/decifrare (es. identificazione, firma digitale).
- **Importante:** Non perdere o divulgare la password/chiave. La perdita implica la perdita dei dati.
- **Cifrare File, Cartelle, Unità**
 - Funzionalità disponibile in molti sistemi operativi. Su Windows, si può cifrare un file tramite "Attributi avanzati" nelle proprietà.
 - Per cifrare un'intera unità, si usa la funzionalità **BitLocker** (su alcune versioni di Windows).
- **Impostare Password per File Office**
 - Nel menu File > Informazioni > Proteggi documento > Crittografia con password. Richiede l'inserimento e conferma della password.

CAPITOLO 2 – MALWARE

- **Malware**
 - Software creato per causare danni a sistemi o dati. Significa "programma malevolo". Storicamente chiamato "Virus".
- **Occultamento del Malware**
 - Modi per nascondersi: **Trojan** (fingono di essere utili), **Rootkit** (nascondono processi), **Backdoor** (bypassano la sicurezza).
- **Tipi di Malware e Funzionamento**
 - **Virus:** Si copiano in altri programmi (host), si diffondono all'esecuzione dell'host.
 - **Worm:** Si diffondono autonomamente (es. via rete).
 - **Spyware:** Raccolgono informazioni sull'utente (navigazione, password).
 - **Adware:** Mostrano pubblicità indesiderate (popup).
 - **Keylogger:** Registrano la digitazione sulla tastiera.
 - **Dialer:** Modificano la connessione internet per chiamare numeri a tariffazione speciale.
 - **Botnet:** Reti di computer infetti controllati da un attaccante.
 - **Ransomware:** Bloccano l'accesso a dati/sistema e chiedono un riscatto.
- **Software Anti-virus**
 - Funzioni: Analisi della memoria (cerca comportamenti anomali/firme) e scansione file/cartelle (individua codice virale).
 - Limitazioni: Non offre protezione totale. Necessita di essere **aggiornato** regolarmente. Possibili "falsi positivi".
 - Dovrebbe essere installato su **tutti i sistemi informatici** (PC, dispositivi mobili).

- **Aggiornamento Software**
 - Essenziale aggiornare regolarmente: sistema operativo, antivirus, browser web, plugin, applicazioni. Combatte i nuovi rischi e le vulnerabilità.
- **Scansioni Antivirus**
 - È possibile eseguire e **pianificare scansioni** di unità, cartelle e file specifici. Permette un controllo regolare.
- **Quarantena**
 - L'antivirus sposta i file infetti/sospetti in una cartella apposita. Il file viene reso inerte e non può causare danni. Permette il ripristino o l'eliminazione successiva. I file in quarantena vengono solitamente cancellati dopo un periodo.
- **Eliminazione File Infetti/Sospetti**
 - Dopo la quarantena, è possibile eliminare definitivamente i file infetti.
- **Rischi Software Obsoleto/Non Supportato**
 - Software vecchio non riceve aggiornamenti di sicurezza, lasciando vulnerabilità sfruttabili dagli hacker.
- **Risorse Online per Malware**
 - Si possono usare scanner antivirus online gratuiti o tool dai produttori di sistemi operativi per diagnosticare e risolvere attacchi.

CAPITOLO 3 – SICUREZZA IN RETE

- **Reti di Computer**
 - Insieme di elaboratori interconnessi per scambiare informazioni.
 - Tipi comuni in base all'estensione: **LAN** (area limitata, cablata o wireless), **WLAN** (LAN wireless, Wi-Fi), **MAN** (area cittadina), **WAN** (area estesa, internet), **VPN** (rete privata virtuale su internet pubblico, sicura con crittografia).
- **Implicazioni di Sicurezza della Connessione in Rete**
 - La connessione espone a rischi di sicurezza. Possibili infezioni malware e accesso non autorizzato a dati.
- **Ruolo dell'Amministratore di Rete**
 - Gestisce tecnicamente la rete. Responsabile di progettazione, realizzazione, controllo di LAN/WAN. Include monitoraggio, aggiornamenti, sicurezza, gestione accessi (Access Control List).
- **Firewall**

- Componente che filtra il traffico tra una rete/computer e l'esterno (es. internet). Evita intrusioni/accessi non autorizzati.
- Tipi: **perimetrale** (aziende) e **personale** (software sul singolo PC).
- Funzione: **filtrare il traffico** in entrata/uscita, bloccando ciò che è pericoloso.
- Limiti: La configurazione può renderli poco flessibili. Se mal configurato/disattivato non protegge. Malware può manipolarlo.
- Windows Firewall è integrato in Windows ed è attivo di default. Si può attivare/disattivare dal Pannello di controllo.
- **Sicurezza Reti Wireless**
 - Meno sicure delle reti cablate. Richiedono crittografia.
 - Standard di sicurezza: **WEP** (debole, superato), **WPA** (migliore del WEP), **WPA2** (più sicuro del WPA, raccomandato).
- **Metodi di Accesso non Autorizzato (in rete)**
 - Tecniche per intercettare traffico wireless non protetto: **Wardriving** (cercare reti aperte/deboli in giro), **Leavesdropping** (ascoltare/decodificare passivamente i segnali).
 - Altri attacchi: **Network hijacking** (controllo account), **Man in the middle** (intercettare e modificare comunicazione).
- **Hotspot Personale**
 - Funzionalità (chiamata anche "tethering") che permette a uno smartphone di diventare un punto di accesso internet per altri dispositivi (via Bluetooth o Wi-Fi).
- **Scopo di un Account di Rete**
 - Identificare l'utente e regolare il suo accesso alle risorse di rete (file, stampanti, internet) in base alle politiche (Access Control List). Composto da User ID e password.