APPUNTI RAPIDI MODULO 4

Cinque obiettivi dell'IT security:

integrità dei dati: devono effettivamente essere quelli che le parti in causa legittimamente sono convinti che siano;
confidenzialità: solo le persone autorizzate devono poter accedere alle risorse scambiate;
disponibilità: coloro che ne hanno diritto devono poter sempre accedere a un servizio o alle proprie risorse;
non ripudio: una transazione o un'azione svolta non può essere negata a posteriori dall'operatore;
autenticazione: assicura l'identità di un utente, garantendo a ciascun corrispondente che il suo partner sia effettivamente quello che crede.

Eventi accidentali: non ponderabili (non prevedibili, come alluvioni, terremoti …)
Eventi indesiderati: causati dall'uomo (malintenzionati)

AGID (Agenzia per l'Italia Digitale): definisce le linee guida per in ambito digitale.

Lo standard ISO/27001 è una norma internazionale che definisce lo standard per la sicurezza dei sistemi informatici.

AIDC (Automatic Identification and Data Capture): riconoscimento tramite dati biometrici (impronte, volto, iride ecc.)

GDPR (General Data Protection Regulation): si occupa della protezione dei dati personali.

Ingegneria sociale (social engineering): induce le vittime a comportarsi in un certo modo, ingannandole (manipolazione psicologica)

- Chiamate telefoniche
- Phishing (email e messaggi ingannevoli)
- Shoulder surfing (spia la vittima per rubare i dati, ad esempio il pin)

Macro: piccoli programmi per eseguire automaticamente delle operazioni. Per disattivarle in word vai su file – opzioni – centro protezione

---

Malware → malicious + software

Virus informatici: piccoli programmi (o sezioni di codice) che danneggiano i computer.
Trojan → si nascondono all'interno di altri programmi per rubare informazioni personali o permettere ad altri di controllare il computer.
Worm → inviano email fasulle con copie di sé stesso.
Spyware → installiamo involontariamente insieme ad altri programmi. Controllano le nostre attività in internet.
Adware → fanno comparire tante finestre che è difficile eliminare
Ransomware → bloccano il computer o rendono illeggibili i file. Chiedono un riscatto per il ripristino.
Rootkit → simile al Trojan. Prendono il controllo del computer

Backdoor → Controllare dall'esterno i dispositivi. Anche per scopi leciti (come assistenza da remoto)
Keylogger → registrano quello che viene digitato sulla tastiera (hardware e software)

Phishing: si finge un ente affidabile per farsi fornire informazioni personali; (carpire i dati di un utente attraverso una email che lo invita a visitare un sito o a rispondere lasciando i suoi dati). Se il messaggio arriva via SMS, si chiama **Smishing.**
Vishing: tramite telefono (VOIP)
Pharming: riproduzione identica di siti ufficiali
Sniffing: intercettazione passiva dei dati che transitano in rete

---

Antivirus: programma per rilevare ed eliminare i malware
Antispyware: programmi specifici per eliminare spyware, adware e spylogger

Analisi veloce: controlla solo le cartelle di sistema
Analisi completa: scansiona tutto il computer, richiede molto tempo
Analisi personalizzata: permette di scegliere quali file e percorsi analizzare
Analisi Offline: ricerca software particolarmente difficili da rimuovere

Per rispristinare un file in quarantena: pulsante "**cronologia della protezione**"
Per pianificare una scansione bisogna cercare, da start, "**Utilità di pianificazione**"
CERT: organizzazioni internazionali per la ricerca e catalogazione dei malware
Windows Update: possibilità di scaricare costantemente gli aggiornamenti rilasciati da windows

---

Rete: un gruppo di dispositivi collegati tra loro per poter condividere file e risorse (stampanti).
Rete LAN: pochi computer, vicini tra di loro. Di solito sono CABLATE e utilizzano il NIC (schede di rete). Se sono SENZA CAVI, quindi utilizzano la rete wi-fi, vengono chiamate **WLAN**

Reti LAN, MAN E WAN: sono l'una più grande dell'altra.
VPN: rete privata virtuale. L'accesso è consentito soltanto alle persone autorizzate.
Reti P2P: i dispositivi sono tutti allo stesso livello.
Reti client/server: c'è un server centrale che fornisce i dati ai vari client
Firewall: controlla il traffico dati sia in ingresso che in uscita dai dispositivi connessi a una rete locale o a Internet (simile alla dogana)

Attacchi alle reti wireless

- Eavesdropping (origliare): ascoltano e intercettano le conversazioni
- Jamming (interferire): è un disturbo della rete wifi
- network hijacking (dirottamento di rete): reindirizzano verso siti carichi di malware
- Man in the middle (uomo nel mezzo): inserirsi in una conversazione private per leggere e modificare i messaggi

Protocolli di sicurezza reti wireless: WEP (1999), WPA (2003), **WPA2** (2004, **il più usato** ancora oggi), WPA3 (2018, ma non ancora diffuso)

Modalità personal > reti domestiche
Modalità enterprise > reti aziendali

Mail_To: posta elettronica (sottoinsieme della rete internet)
ProtonMail: servizio di posta elettronica per cifrare le mail (renderle illeggibili ad altri)
Firma digitale: garantisce l'identità del mittente (sostituisce quella cartacea e ha valore legale)

Social Network Poisoning: profilo artefatto
Man In The Middle (MITM): gli hacker si inseriscono nelle comunicazioni tra due utenti per rubare le loro informazioni personali. Per evitare ciò si usa la **Crittografia end to end (E2E)**