

APPUNTI RAPIDI MODULO 4

Eventi accidentali: non ponderabili (non prevedibili, come alluvioni, terremoti ...)

Eventi indesiderati: causati dall'uomo (malintenzionati)

Minaccia -> azione capace di nuocere

Vulnerabilità -> livello di esposizione rispetto alla minaccia

Contromisura -> azioni per prevenire la minaccia

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.

Google Authenticator: applicazione per doppia autenticazione

Social engineering: manipolazione psicologica

Man-in-the-middle-attack: interpersi in una comunicazione per carpire informazioni

Social Network Poisoning: profili artefatti e relazioni inesistenti sui social network

Hijacking: digitando una pagina si viene indirizzati su un altro sito o cambia la pagina iniziale

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)

Thiefing: sfruttare l'assenza di adeguate misure per sottrarre servizi informatici (rubare la wifi)

Jamming: creare interferenze via radio

Pharming: riprodurre un sito web ufficiale

Eavesdropping: intercettazione non autorizzata delle conversazioni private

Zip bomb disattiva le difese di un pc

Trojan horse: programma "maligno" con funzioni utili e desiderate

Worm: rallenta il sistema con operazioni inutili e dannose.

Keylogger: intercetta tutto ciò che si digita sulla tastiera

phracher: furto di programmi che offrono servizi telefonici gratuiti

phreaker: utilizzano numeri telefonici o carte telefoniche per accedere ad altri computer.

Poisoning: profili artefatti

Modalità personal > reti domestiche

Modalità enterprise > reti aziendali

Lan mesh: i nodi sono collegati senza un ordine preciso, essendo sia server e client

Lan ad anello: l'ultimo si connette al primo

Lan a stella: i nodi sono collegati allo stesso dispositivo

Lan a bus: tutti i nodi sono agganciati al medesimo cavo fisico

Cinque aspetti dell'ICT: Integrità, confidenzialità, disponibilità, non ripudio e autenticazione.

Firewall: filtraggio di pacchetti (rapidi) e a livello di circuiti (lenti ma più sicuri)

ProtonMail: servizio gratuito per email criptate

Scansione antivirus

- **completa:** tutte le unità del computer.
- **su misura o personalizzata:** selezionare unità e le cartelle
- **rapida:** all'avvio del sistema operativo e la memoria di sistema.
- **intelligente:** aree più soggette a infezione.

Antivirus real-time: istantaneamente

social engineering: manipolazione psicologica

WI-FI: comunicare senza cavi

protocolli di sicurezza wi-fi: il più sicuro è WPA2