1. FONDAMENTI DI SICUREZZA DI RETE

Principi CIA (Confidenzialità, Integrità, Disponibilità)

Confidenzialità:

- **Definizione**: protezione delle informazioni dall'accesso non autorizzato
- **Tecniche**:
  - **Crittografia**: cifratura dei dati (simmetrica/asimmetrica)
  - **Controllo accessi**: autenticazione, autorizzazione, ACL
  - **Segmentazione reti**: VLAN, zone demilitarizzate (DMZ)
- **Esempi pratici**: VPN, HTTPS, crittografia end-to-end

Integrità:

- **Definizione**: garanzia che i dati non siano alterati durante trasmissione/archiviazione
- **Tecniche**:
  - **Hash**: MD5, SHA-256 (funzioni one-way)
  - **Firme digitali**: combinazione di hash e crittografia asimmetrica
  - **Checksum**: CRC (Cyclic Redundancy Check)
- **Esempi pratici**: TLS/SSL, HMAC, firme digitali nei certificati

Disponibilità:

- **Definizione**: garanzia di accesso ai sistemi e dati quando necessario
- **Tecniche**:
  - **Ridondanza**: sistemi duplicati, componenti spare
  - **Backup**: regolari, testati, geograficamente distribuiti
  - **Bilanciamento carico**: distribuzione traffico su più server
- **Esempi pratici**: cluster, CDN, sistemi RAID, disaster recovery

Principi complementari:

- **Autenticazione**: verifica dell'identità (chi sei)
- **Autorizzazione**: definizione dei permessi (cosa puoi fare)
- **Non-ripudio**: impossibilità di negare azioni compiute
- **Accounting**: tracciamento delle attività degli utenti

2. VULNERABILITÀ A LIVELLO DI RETE E TRASPORTO

Vulnerabilità a livello 2 (Data Link)

ARP spoofing/poisoning:

- **Tecnica**: falsificazione di messaggi ARP per associare l'indirizzo MAC dell'attaccante a un IP legittimo
- **Impatto**: intercettazione traffico (Man-in-the-Middle)
- **Mitigazione**: Inspection ARP, DHCP snooping, sistemi di rilevamento

MAC flooding:

- **Tecnica**: invio massivo di frame con indirizzi MAC diversi
- **Impatto**: saturazione tabelle CAM dello switch, conversione in hub
- **Mitigazione**: port security, limitazione MAC per porta

Rogue DHCP:

- **Tecnica**: installazione di server DHCP non autorizzato
- **Impatto**: reindirizzamento traffico attraverso gateway compromesso
- **Mitigazione**: DHCP snooping, autenticazione di rete 802.1X

Vulnerabilità a livello 3 (Network)

IP spoofing:

- **Tecnica**: falsificazione dell'indirizzo IP sorgente
- **Impatto**: aggiramento filtri IP, attacchi DDoS distribuiti
- **Mitigazione**: ingress/egress filtering, RPF (Reverse Path Forwarding)

ICMP attacks:

- **Tecniche**:
  - **Ping flood**: saturazione con richieste ICMP Echo
  - **Smurf attack**: amplificazione tramite broadcast
- **Mitigazione**: filtraggio ICMP, rate limiting, blocco broadcast diretti

Routing attacks:

- **Tecniche**:
  - **BGP hijacking**: annuncio di prefissi IP non propri
  - **Route poisoning**: manipolazione tabelle di routing
- **Mitigazione**: RPKI, filtri sui prefissi BGP, autenticazione routing

Vulnerabilità a livello 4 (Transport)

TCP SYN flood:

- **Tecnica**: invio massivo di pacchetti SYN senza completare handshake

- **Impatto**: esaurimento risorse server (tabelle connessioni)
- **Mitigazione**: SYN cookies, firewall stateful, rate limiting

Session hijacking:

- **Tecnica**: furto di sessioni TCP attive con spoofing di pacchetti
- **Impatto**: accesso non autorizzato a sessioni autenticate
- **Mitigazione**: cifratura, reset periodico sessioni, token imprevedibili

UDP flood:

- **Tecnica**: invio massivo di pacchetti UDP a porte diverse
- **Impatto**: saturazione della banda e risorse di elaborazione
- **Mitigazione**: rate limiting, firewall, filtri sul traffico

3. SOCIAL ENGINEERING E ATTACCHI A LIVELLO UMANO

Definizione: manipolazione psicologica per indurre le persone a compiere azioni o rivelare informazioni

Perché funziona:

- Fiducia naturale delle persone
- Paura e senso di urgenza
- Desiderio di essere d'aiuto
- Curiosità innata

Tipi di attacchi di ingegneria sociale:

Phishing:

- **Definizione**: invio di comunicazioni fraudolente che sembrano provenire da fonti legittime
- **Varianti**:
  - **Spear phishing**: attacco mirato a specifici individui/organizzazioni
  - **Whaling**: targeting di figure senior (CEO, dirigenti)
  - **Vishing**: phishing via telefono
  - **Smishing**: phishing via SMS
- **Indicatori**: URL sospetti, errori grammaticali, richieste urgenti, mittenti generici

Pretexting:

- **Definizione**: creazione di uno scenario fittizio per ottenere informazioni
- **Esempio**: finto tecnico IT che chiama per "risolvere un problema"

- **Efficacia**: costruzione di una storia credibile che giustifica la richiesta

Baiting:

- **Definizione**: offrire qualcosa di allettante per indurre azioni rischiose
- **Esempi**: chiavette USB infette lasciate in luoghi pubblici, software "gratuito"
- **Sfrutta**: curiosità e desiderio di ottenere qualcosa di gratuito

Quid pro quo:

- **Definizione**: offrire un servizio in cambio di informazioni o accesso
- **Esempio**: supporto tecnico fasullo che richiede credenziali
- **Differenza dal baiting**: promessa di un servizio specifico anziché un'esca generica

Contromisure:

- **Formazione continua**: consapevolezza delle tecniche e red flags
- **Verifica attraverso canali alternativi**: conferma richieste via telefono/di persona
- **Politiche organizzative**: procedure chiare per richieste sensibili
- **Tecnologie**: filtri email, sandboxing, autenticazione multi-fattore
- **Simulazioni**: test periodici di phishing per misurare consapevolezza

4. MALWARE E MINACCE SOFTWARE

Definizione: software malevolo progettato per danneggiare, compromettere o accedere illegalmente a sistemi

Tipologie di malware:

Virus:

- **Caratteristiche**: necessita di un host (file eseguibile) per diffondersi
- **Funzionamento**: si attacca a file legittimi e si attiva quando questi vengono eseguiti
- **Tipi**: virus di boot, virus di macro, virus polimorfi
- **Esempio**: ILOVEYOU, Melissa

Worm:

- **Caratteristiche**: si propaga autonomamente senza host
- **Funzionamento**: sfrutta vulnerabilità di rete per replicarsi
- **Impatto**: consumo banda, crash di servizi
- **Esempio**: WannaCry, Slammer, Stuxnet

Trojan:

- **Caratteristiche**: si presenta come software legittimo ma contiene funzionalità malevole

- **Funzionamento**: spesso usato come "porta d'ingresso" per altri attacchi
- **Tipi**: RAT (Remote Access Trojan), trojan bancari, backdoor
- **Esempio**: Zeus, DarkComet

Ransomware:

- **Caratteristiche**: cifra i dati delle vittime e richiede riscatto per la chiave
- **Funzionamento**: utilizza algoritmi di crittografia forti (RSA, AES)
- **Evoluzione**: dal semplice blocco schermo alla crittografia completa
- **Esempio**: CryptoLocker, Ryuk, Petya

Spyware:

- **Caratteristiche**: raccoglie informazioni senza consenso
- **Funzionamento**: monitora attività, registra input, cattura schermate
- **Tipi**: keylogger, screen scraper, tracker
- **Esempio**: Pegasus, FlexiSpy

Vettori di diffusione:

- **Email**: allegati infetti, link malevoli
- **Download**: software da fonti non affidabili
- **Vulnerabilità**: exploit di bug nei sistemi operativi/applicazioni
- **Dispositivi rimovibili**: USB infetti
- **Social engineering**: induzione dell'utente a installare malware

Contromisure base:

- **Antivirus/antimalware**: rilevamento basato su firme e comportamento
- **Patch regolari**: aggiornamenti tempestivi di OS e applicazioni
- **Sandbox**: esecuzione del codice in ambiente isolato
- **Whitelisting**: esecuzione solo di applicazioni approvate
- **Backup**: copie regolari dei dati su supporti offline
- **User training**: educazione sulla sicurezza digitale

5. PRIVACY E ANONIMATO NELLE RETI

Come i protocolli di rete rivelano informazioni personali

Indirizzo IP:

- **Rivela**: posizione geografica approssimativa, ISP
- **Tracciamento**: può essere usato come identificatore tra siti diversi
- **Persistenza**: spesso statico per connessioni fisse

DNS:

- **Rivela**: tutti i domini visitati
- **Problema**: query spesso non cifrate
- **Raccolta**: ISP e provider DNS possono registrare tutte le richieste

HTTP e Header:

- **User-Agent**: rivela browser, sistema operativo, dispositivo
- **Referer**: indica la pagina di provenienza
- **Cookie**: permettono il tracciamento cross-site
- **ETag**: persistenza anche dopo cancellazione cookie

Informazioni di livello 2:

- **MAC address**: identificatore hardware unico
- **Probe request Wi-Fi**: rivelano SSIDs precedentemente connessi
- **Bluetooth**: dispositivi in modalità discoverable

Metadati delle comunicazioni:

- **Pattern di comunicazione**: chi parla con chi
- **Timing**: quando avvengono le comunicazioni
- **Volume**: quantità di dati scambiati
- **Significatività**: i metadati spesso rivelano più dei contenuti

Tecniche di base per la protezione della privacy

VPN (Virtual Private Network):

- **Funzionamento**: tunnel cifrato tra client e server VPN
- **Protegge da**: ISP, reti locali, siti web visitati
- **Limiti**: il provider VPN può vedere il traffico non cifrato
- **Considerazioni**: giurisdizione provider, policy di logging

Proxy:

- **Tipi**: HTTP, SOCKS, web proxy
- **Differenze da VPN**: solo specifiche applicazioni, spesso senza cifratura
- **Use case**: mascheramento IP per specifiche attività
- **Considerazioni**: spesso più veloci ma meno sicuri delle VPN

DNS over HTTPS/TLS (DoH/DoT):

- **Funzionamento**: cifratura delle query DNS

- **Protezione**: impedisce intercettazione e modifica delle query
- **Implementazioni**: Firefox (Cloudflare), Chrome (Google)
- **Considerazioni**: centralizzazione verso grandi provider

Navigazione anonima/incognito:

- **Funzionalità**: non salva cronologia, cookie, form data localmente
- **Non protegge da**: tracciamento IP, fingerprinting
- **Utilizzo corretto**: privacy locale (stesso dispositivo)

Blocco dei tracker:

- **Estensioni**: uBlock Origin, Privacy Badger
- **Funzionalità**: blocco di script di tracciamento, pixel, fingerprinting
- **A livello di rete**: Pi-hole (DNS filtering)
- **Browser privacy-focused**: Firefox con hardening, Brave

6. RETI DOMESTICHE E SMART HOME

Architettura di una rete domestica moderna

Componenti principali:

- **Router/gateway**: connessione a Internet, NAT, DHCP, firewall
- **Access point Wi-Fi**: copertura wireless (possibilmente mesh)
- **Switch**: connessioni cablate ad alta velocità
- **NAS**: archiviazione centralizzata
- **Smart hub**: controllo dispositivi domotici

Topologia tipica:

- **Modem ISP → Router principale → Switch/AP/Dispositivi**
- **Segmentazione**: rete principale, guest, IoT (ideale)
- **Cablaggio**: Cat5e/Cat6 per connessioni principali
- **Wireless**: copertura completa con sistemi mesh

Tecnologie di connettività:

- **Cablata**:
  - **Ethernet**: 1/2.5/5/10 Gbps
  - **MoCA**: networking su cavi coassiali
- **Wireless**:
  - **Wi-Fi 5/6/6E**: 802.11ac/ax/ax 6GHz
  - **Mesh**: sistemi con nodi multipli coordinati

- **Powerline**: comunicazione attraverso rete elettrica
- **Tecnologie IoT**: Zigbee, Z-Wave, Thread

Gestione e monitoraggio:

- **Interfacce**: web admin, app mobile
- **QoS**: prioritizzazione traffico (gaming, streaming, VoIP)
- **Parental control**: filtri contenuti, limiti tempo
- **Security**: aggiornamenti firmware, log, alert

IoT e interconnessione di dispositivi

Dispositivi smart comuni:

- **Entertainment**: TV, altoparlanti, streaming devices
- **Controllo ambientale**: termostati, illuminazione, tende
- **Sicurezza**: videocamere, serrature, sensori
- **Elettrodomestici**: frigoriferi, lavatrici, robot aspirapolvere
- **Assistenti vocali**: Amazon Echo, Google Home, HomePod

Protocolli di comunicazione IoT:

- **Zigbee**:
  - **Caratteristiche**: basso consumo, mesh, 2.4 GHz
  - **Range**: 10-100m
  - **Uso**: home automation, lighting
- **Z-Wave**:
  - **Caratteristiche**: frequenze sub-GHz (minori interferenze)
  - **Range**: 30-100m
  - **Uso**: controllo, sicurezza
- **Bluetooth LE**:
  - **Caratteristiche**: basso consumo, corto raggio
  - **Range**: 10-30m
  - **Uso**: wearable, sensori
- **Wi-Fi**:
  - **Caratteristiche**: alta banda, consumo elevato
  - **Range**: 30-50m
  - **Uso**: streaming, dispositivi alimentati

Architetture IoT:

- **Cloud-centric**: dispositivi → cloud → app
- **Edge computing**: elaborazione locale dei dati

- **Fog computing**: elaborazione distribuita
- **Hub-based**: dispositivi → hub locale → cloud

Problematiche di interoperabilità:

- **Ecosistemi chiusi**: vendor lock-in
- **Standard multipli**: frammentazione protocolli
- **Gateway di traduzione**: bridge tra protocolli diversi
- **Standard emergenti**: Matter/CHIP per unificazione

7. SICUREZZA NELLE RETI DOMESTICHE E IOT

Vulnerabilità comuni

Password di default o deboli:

- **Problema**: molti dispositivi mantengono credenziali predefinite
- **Impatto**: facilmente trovabili online (manuali, database)
- **Esempio**: fotocamere IP con admin/admin, admin/password

Mancanza di aggiornamenti:

- **Problema**: dispositivi senza patch o supporto EOL
- **Impatto**: vulnerabilità note non corrette
- **Esempio**: router con firmware obsoleto

Comunicazioni non cifrate:

- **Problema**: dati trasmessi in chiaro
- **Impatto**: intercettazione, modifica dati
- **Esempio**: telecamere che trasmettono video senza TLS

Scarsa segmentazione di rete:

- **Problema**: dispositivi IoT sulla stessa rete di PC/smartphone
- **Impatto**: compromissione IoT → accesso alla rete principale
- **Esempio**: frigorifero smart che può accedere al NAS con dati personali

Minacce principali

Accesso non autorizzato:

- **Tecnica**: exploit vulnerabilità, credenziali deboli
- **Impatto**: controllo dispositivi, accesso alla rete
- **Esempio**: controllo remoto di termostati, serrature

Botnet IoT:

- **Tecnica**: compromissione massiva di dispositivi IoT
- **Impatto**: DDoS, mining cryptocurrency, spam
- **Esempio**: Mirai botnet (2016) - attacco a Dyn DNS

Esfiltrazione dati:

- **Tecnica**: invio non autorizzato di dati a server esterni
- **Impatto**: violazione privacy, spionaggio
- **Esempio**: smart TV che raccolgono dati di visione

Violazione privacy:

- **Tecnica**: accesso a microfoni/telecamere smart home
- **Impatto**: sorveglianza non autorizzata
- **Esempio**: hacking di baby monitor, altoparlanti smart

Strategie di mitigazione

Segmentazione della rete:

- **Tecnica**: VLAN dedicata per IoT
- **Implementazione**: router con supporto VLAN o router separato
- **Beneficio**: isolamento in caso di compromissione

Aggiornamenti regolari:

- **Approccio**: firmware update automatici o schedulati
- **Considerazioni**: verificare supporto prima dell'acquisto
- **Beneficio**: correzione vulnerabilità note

Autenticazione forte:

- **Implementazione**: password uniche e complesse, 2FA ove disponibile
- **Gestione**: password manager per dispositivi
- **Considerazioni**: rotazione periodica credenziali

Monitoraggio del traffico:

- **Strumenti**: IDS/IPS domestici, log analysis
- **Approccio**: stabilire baseline di comportamento normale
- **Alert**: notifiche per traffico anomalo
- **Esempio**: Pi-hole con monitoraggio DNS

8. IMPATTO AMBIENTALE DELLE INFRASTRUTTURE DI RETE

Consumo energetico di data center e reti

Dati sul consumo globale:

- Data center: 1-2% del consumo energetico mondiale
- Singola ricerca Google: 0,2-7g CO2
- Traffico Internet globale: ~1 miliardo tonnellate CO2/anno
- Crescita annuale: 10-15% (pre-ottimizzazione)

Componenti ad alto consumo:

- **Server**: CPU, RAM, storage (60-70% energia totale)
- **Cooling**: raffreddamento (20-30%)
- **Power delivery**: UPS, trasformatori (10-15%)
- **Networking**: router, switch, transceivers (5-10%)

Metriche di efficienza:

- **PUE (Power Usage Effectiveness)**: energia totale / energia IT
  - PUE ideale = 1.0 (impossibile nella pratica)
  - PUE medio = 1.5-2.0
  - PUE inefficiente > 2.5
- **WUE (Water Usage Effectiveness)**: consumo acqua
- **CUE (Carbon Usage Effectiveness)**: emissioni CO2
- **ERF (Energy Reuse Factor)**: energia riutilizzata

Cause di inefficienza:

- **Bassa utilizzazione**: server al 10-20% di capacità
- **Sovradimensionamento**: eccesso di ridondanza
- **Raffreddamento inadeguato**: temperature troppo basse
- **Hardware obsoleto**: minore efficienza energetica
- **Architetture non ottimizzate**: mancata virtualizzazione

Green networking

Efficienza hardware:

- **CPU efficienti**: architetture ARM, design a basso consumo
- **Raffreddamento innovativo**: liquido, immersione
- **Virtualizzazione**: consolidamento server

- **Sleep mode**: spegnimento componenti non utilizzati
- **Storage tiering**: SSD per dati attivi, HDD per archiviazione

Software e protocolli efficienti:

- **Energy-aware routing**: percorsi ottimizzati per efficienza
- **SDN**: gestione centralizzata e ottimizzata
- **NFV**: virtualizzazione di funzioni di rete
- **Adaptive Link Rate**: adattamento velocità link al traffico
- **Efficienza algoritmica**: ottimizzazione codice

Design dei data center:

- **Free cooling**: utilizzo aria esterna per raffreddamento
- **Hot/cold aisle containment**: separazione flussi d'aria
- **Localizzazione strategica**: climi freddi, fonti rinnovabili
- **Recupero calore**: riutilizzo per riscaldamento edifici
- **Modularità**: scalabilità efficiente

Energie rinnovabili:

- **On-site generation**: fotovoltaico, eolico in loco
- **PPA (Power Purchase Agreement)**: acquisto diretto
- **Grid matching**: bilanciamento con produzione rinnovabile
- **Carbon offsetting**: compensazione emissioni
- **24/7 carbon-free energy**: nuovo standard emergente

E-waste e gestione sostenibile dell'hardware

Dimensione del problema:

- 53,6 milioni tonnellate e-waste globale (2019)
- Solo 17,4% riciclato correttamente
- Hardware di rete: ~10% dell'e-waste totale
- Crescita annuale: 3-4% (più rapida di altri rifiuti)

Componenti critici:

- **Metalli rari**: terre rare, oro, argento, palladio
- **Materiali tossici**: piombo, mercurio, ritardanti di fiamma
- **Batterie**: rischio incendio/esplosione
- **Plastica**: difficile da riciclare completamente

Ciclo di vita dell'hardware di rete:

- **Durata media**: 3-5 anni consumer, 5-7 enterprise
- **Obsolescenza**: nuovi standard, vulnerabilità, performance
- **Second life**: riuso in ambienti meno esigenti
- **Refurbishing**: ricondizionamento
- **End-of-life**: smaltimento o riciclo

Strategie di gestione sostenibile:

- **Ecodesign**: progettazione modulare, riparabile
- **Estensione vita utile**: aggiornamenti firmware
- **Ritiro programmato**: trade-in, buy-back
- **Riciclo certificato**: standard R2, e-Stewards
- **Economia circolare**: recupero materiali per nuova produzione