ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI AVELLINO

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI SALERNO

# CORSO PREPARATORIO AGLI ESAMI DI STATO

## I sessione 2025

**3 e 4 settembre 2025**

Relatore: Mario Di Mauro (mdimauro@unisa.it)

# Mobile Technology Evolution

**1G**

Analog

Voice only, Limited coverage and mobility. Example: AMPS

**2G**

Digital

Improved voice, security, coverage. SMS, data. Example GSM, CDMA

**3G**

Mobile Data

Higher data rates, smartphones, better voice. Example: HSPA / HSPA+

**4G**

Mobile Broadband

High speed data, better smartphones. Example: LTE / LTE-A

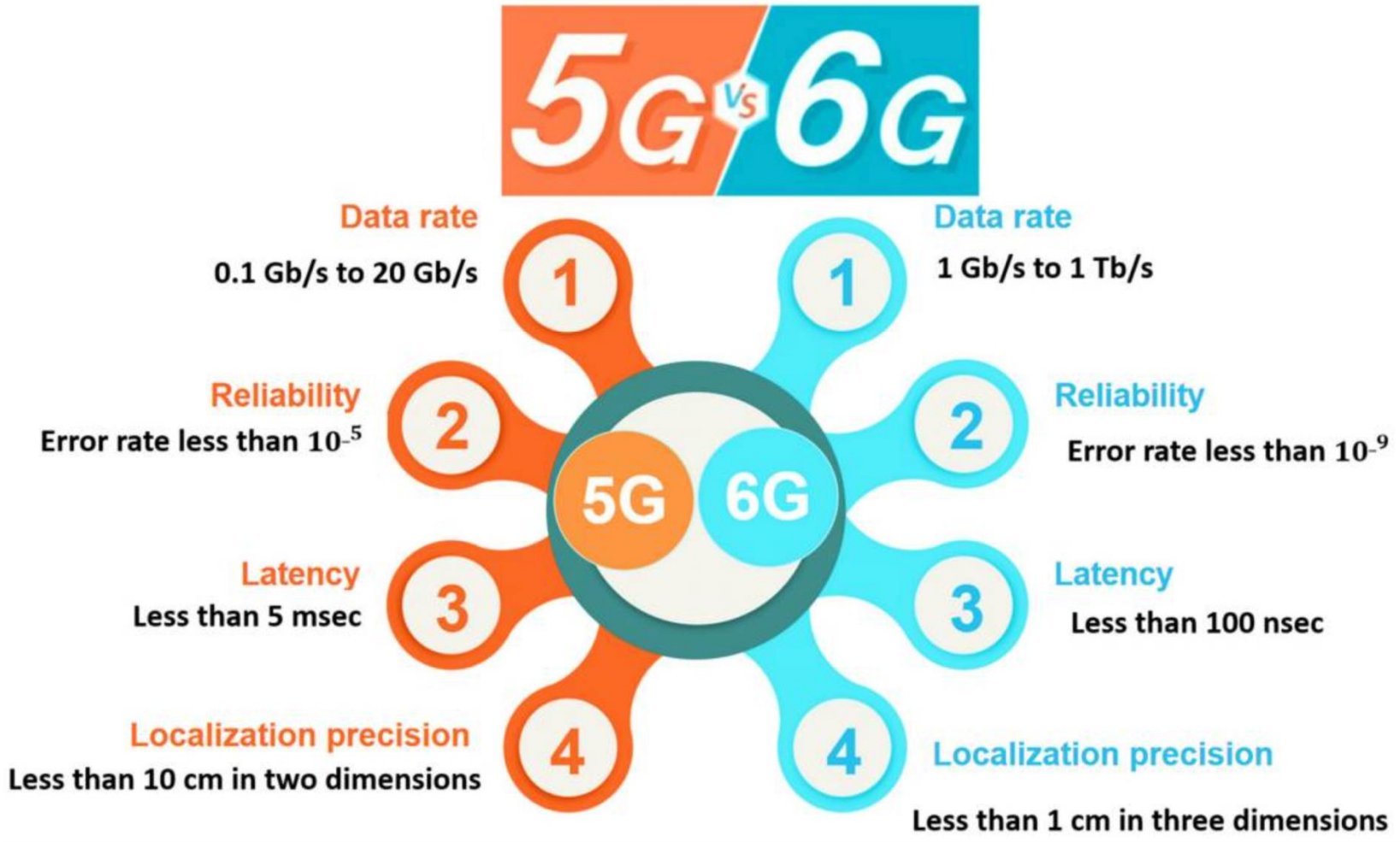
**5G**

eMBB, mMTC, URLLC

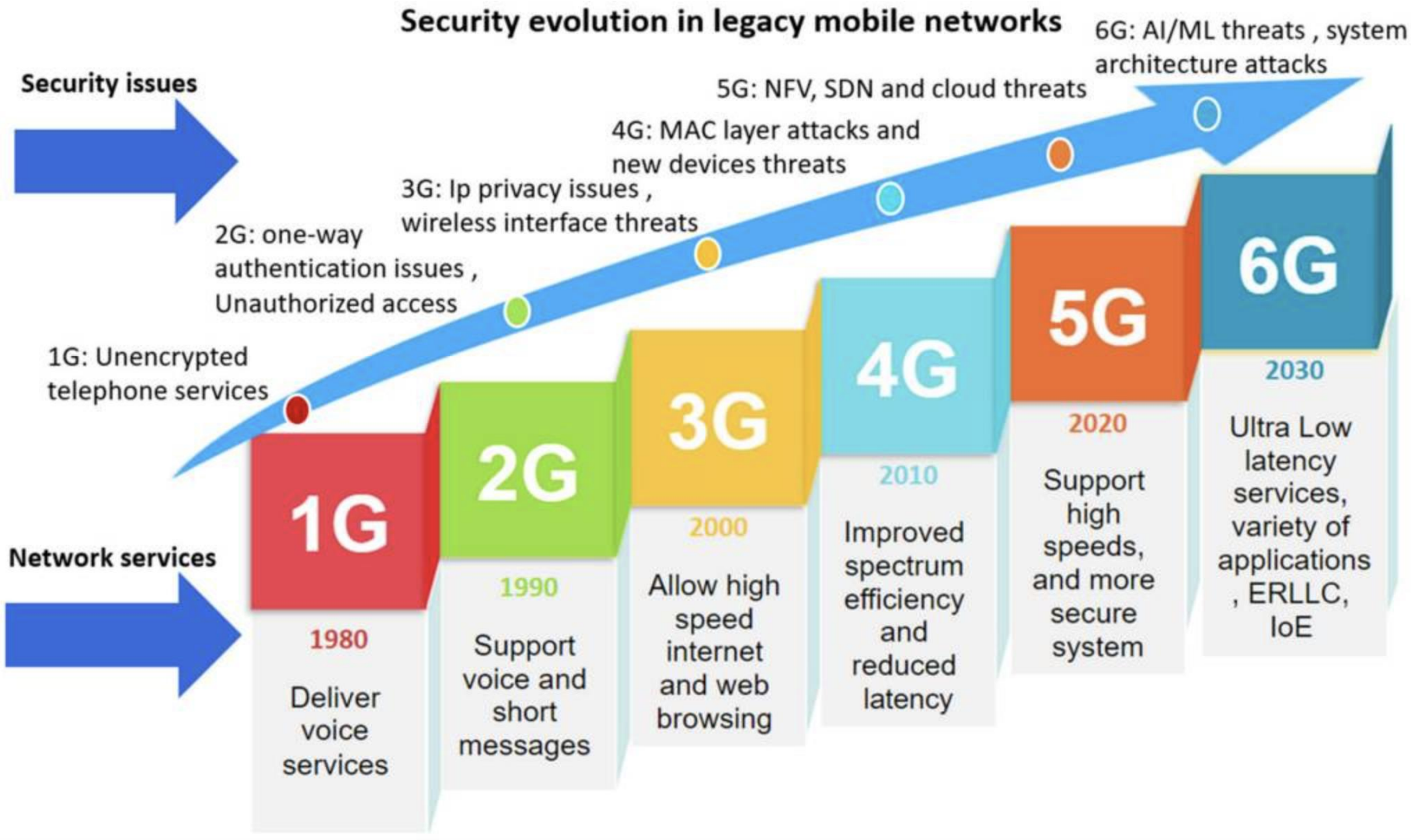
Even higher speeds, ultra-reliable, low latency, high connection density


1980 1990 2000 2010 2020

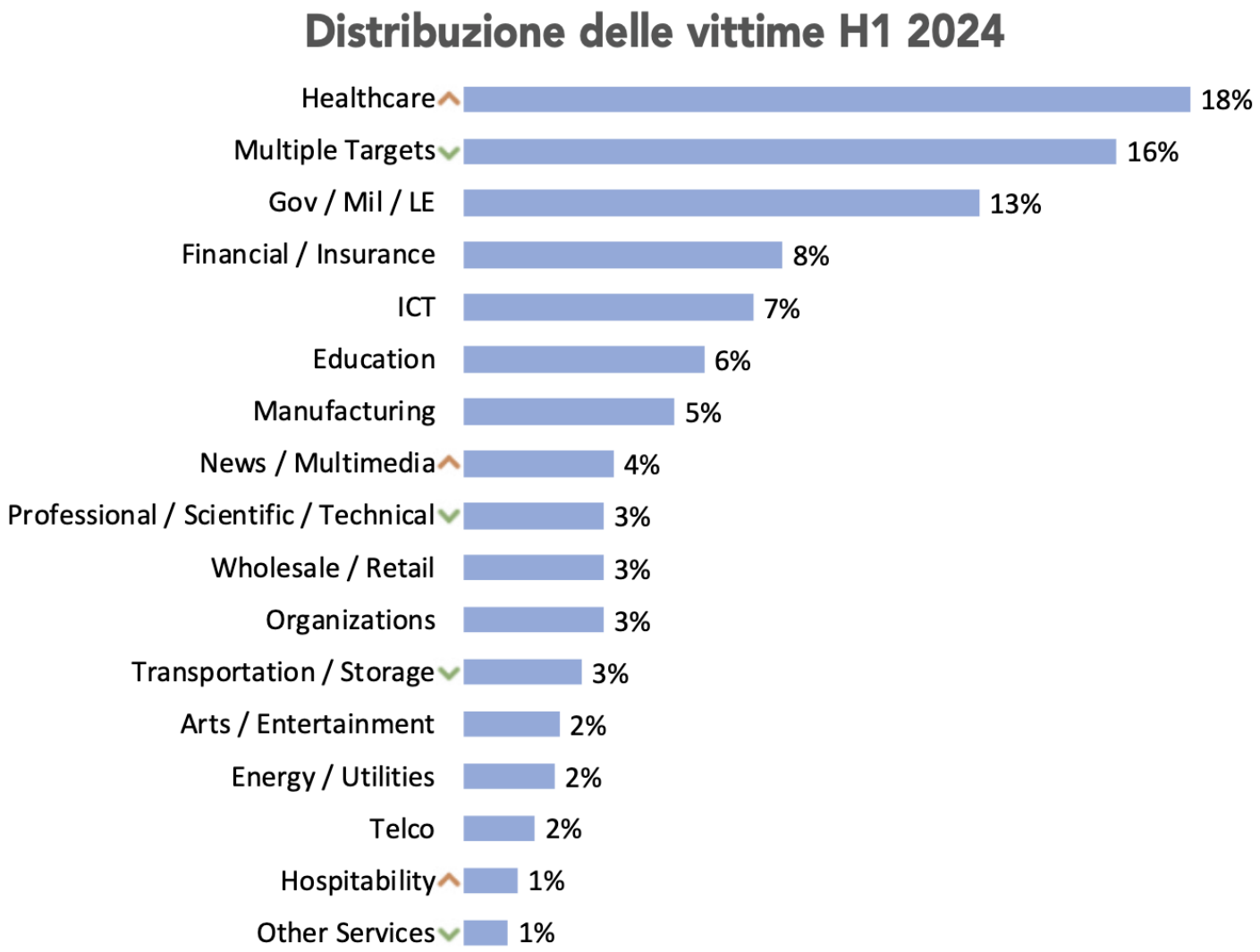
# L’avvento del 6G...



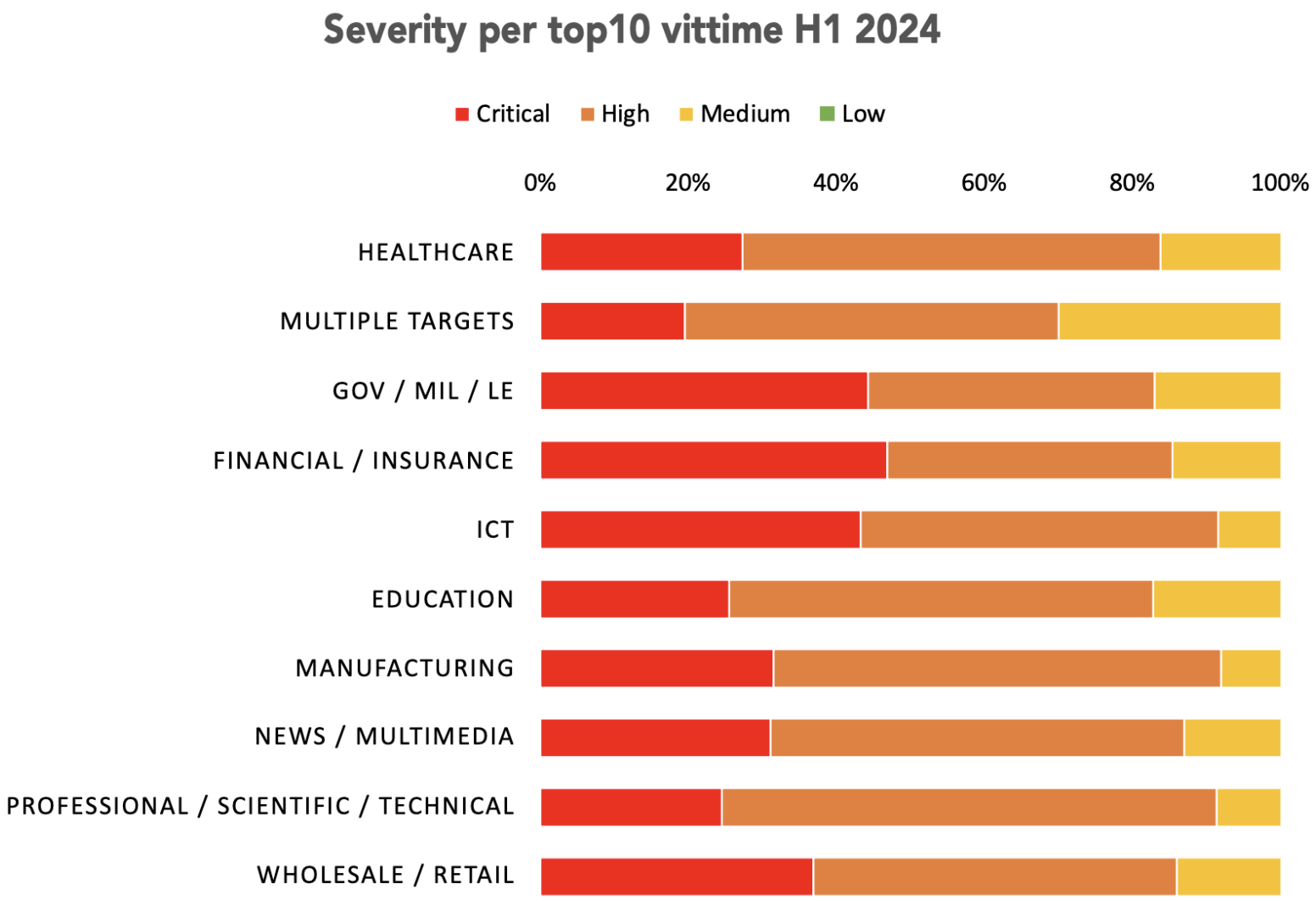
# Evoluzione delle minacce di rete



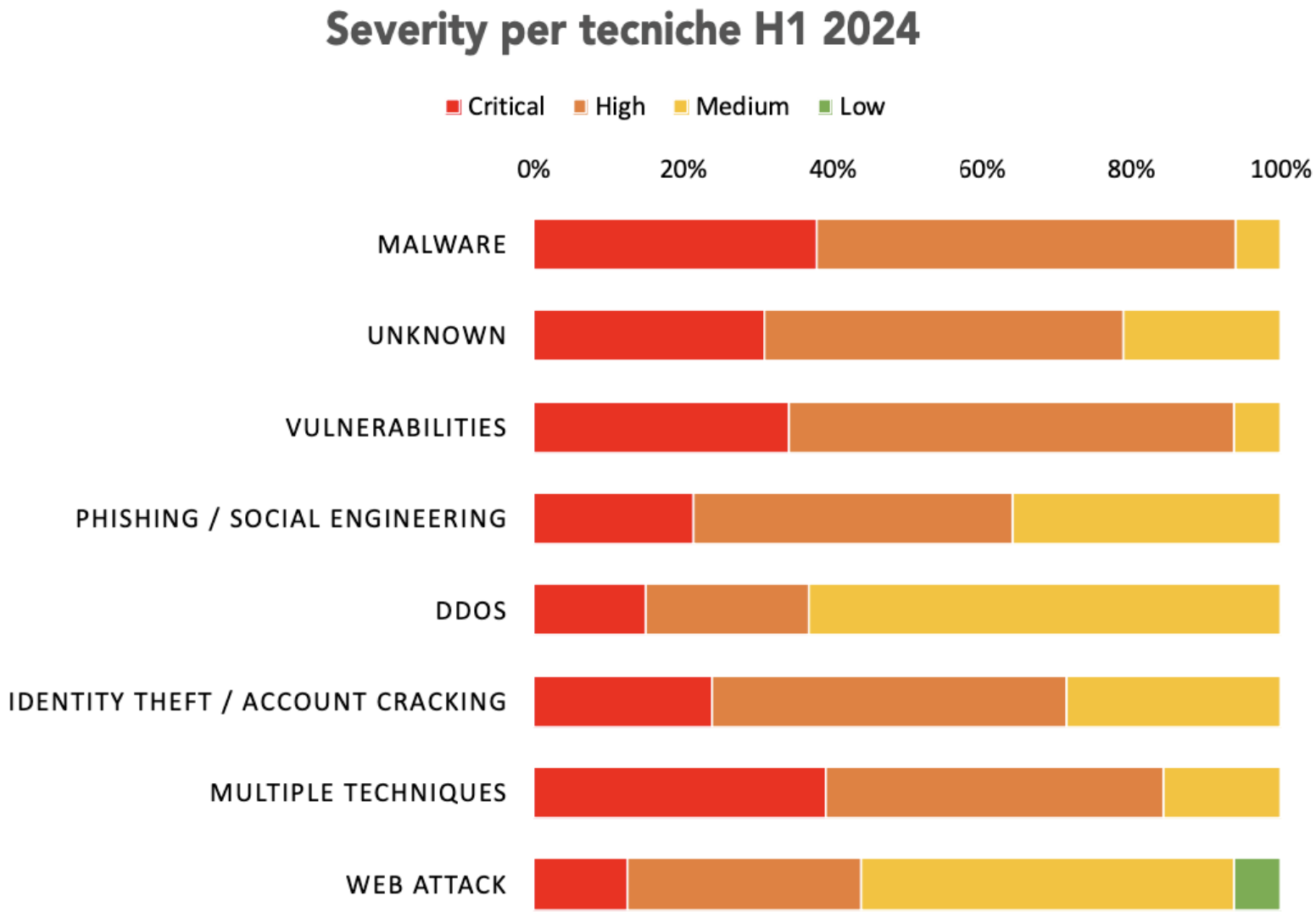
# Nuovi "trend" della cybersecurity (Clusit)



# Nuovi "trend" della cybersecurity (Clusit)



# Nuovi "trend" della cybersecurity (Clusit)



# Reati contro i minori (Clusit)

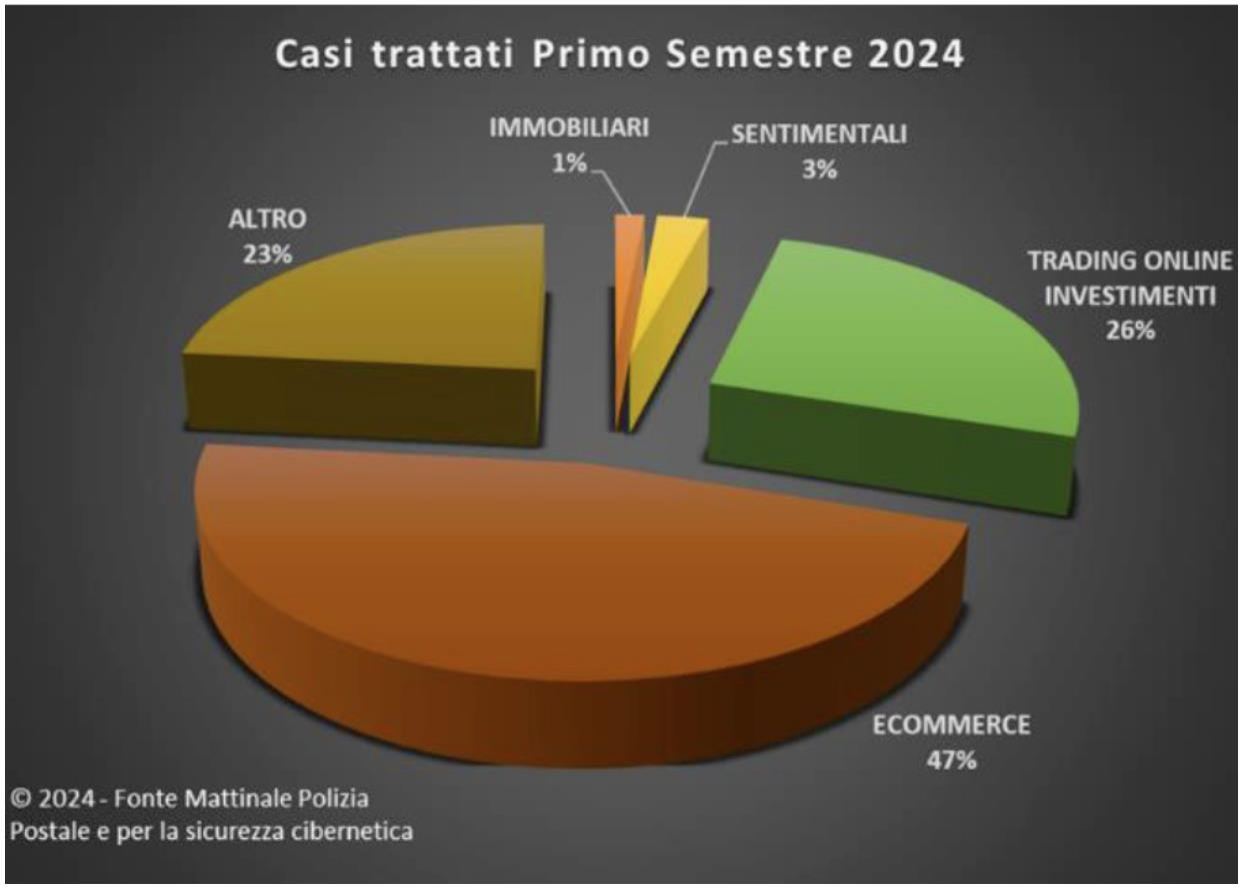
| CYBERBULLISMO Vittime minori | TOTALE casi trattati | Casi trattati vittime 0-9 anni | Casi trattati vittime 10-13 anni | Casi trattati vittime 14-17 anni |
|---|---|---|---|---|
| Primo semestre 2022 | 160 | 11 | 41 | 108 |
| Primo semestre 2023 | 164 | 5 | 35 | 124 |
| Primo semestre 2024 | 176 | 7 | 51 | 118 |

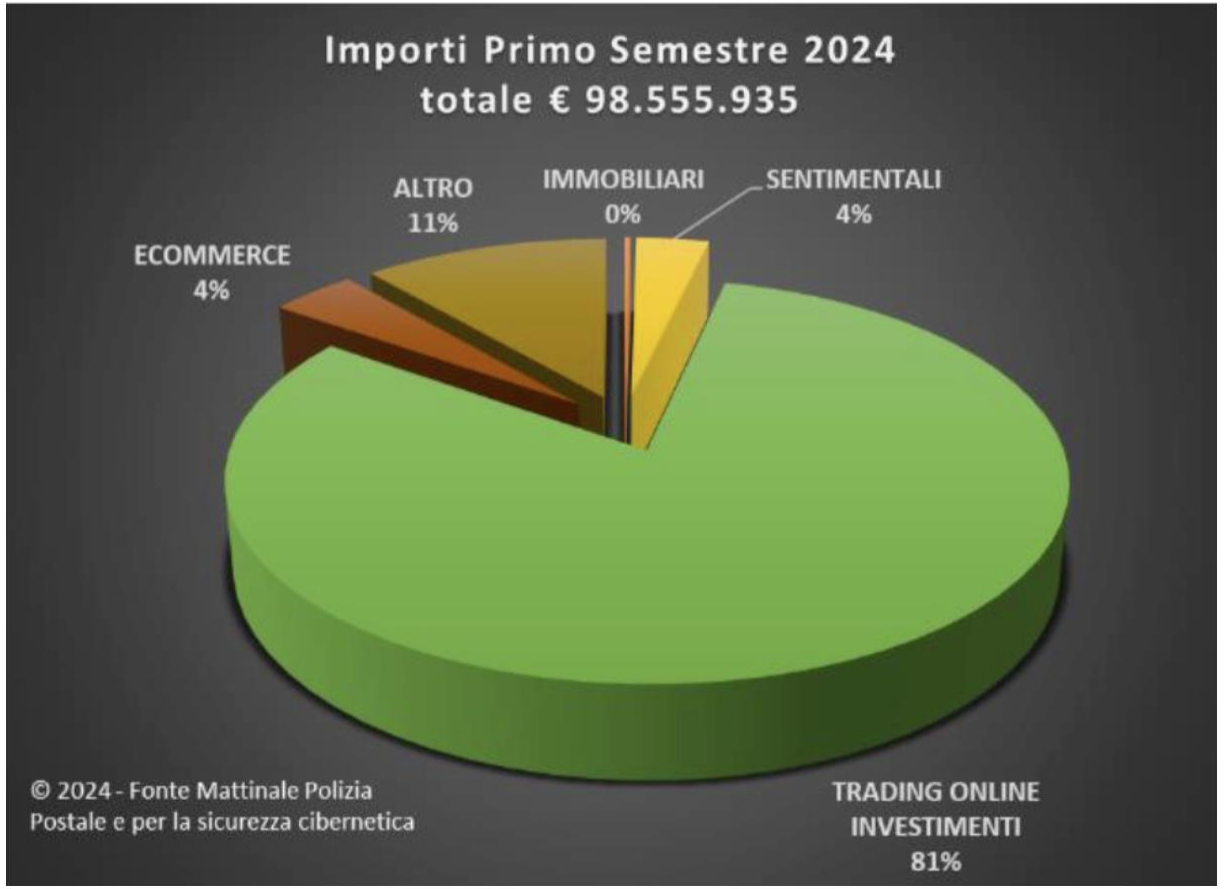
**Fonte** - Polizia Postale e per la sicurezza cibernetica © 2024

| SEXTORTION Vittime minori | TOTALE casi trattati | Casi trattati vittime 0-9 anni | Casi trattati vittime 10-13 anni | Casi trattati vittime 14-17 anni |
|---|---|---|---|---|
| Primo semestre 2022 | 41 | 0 | 8 | 33 |
| Primo semestre 2023 | 66 | 1 | 10 | 55 |
| Primo semestre 2024 | 59 | 0 | 5 | 54 |

**Fonte** - Polizia Postale e per la sicurezza cibernetica © 2024

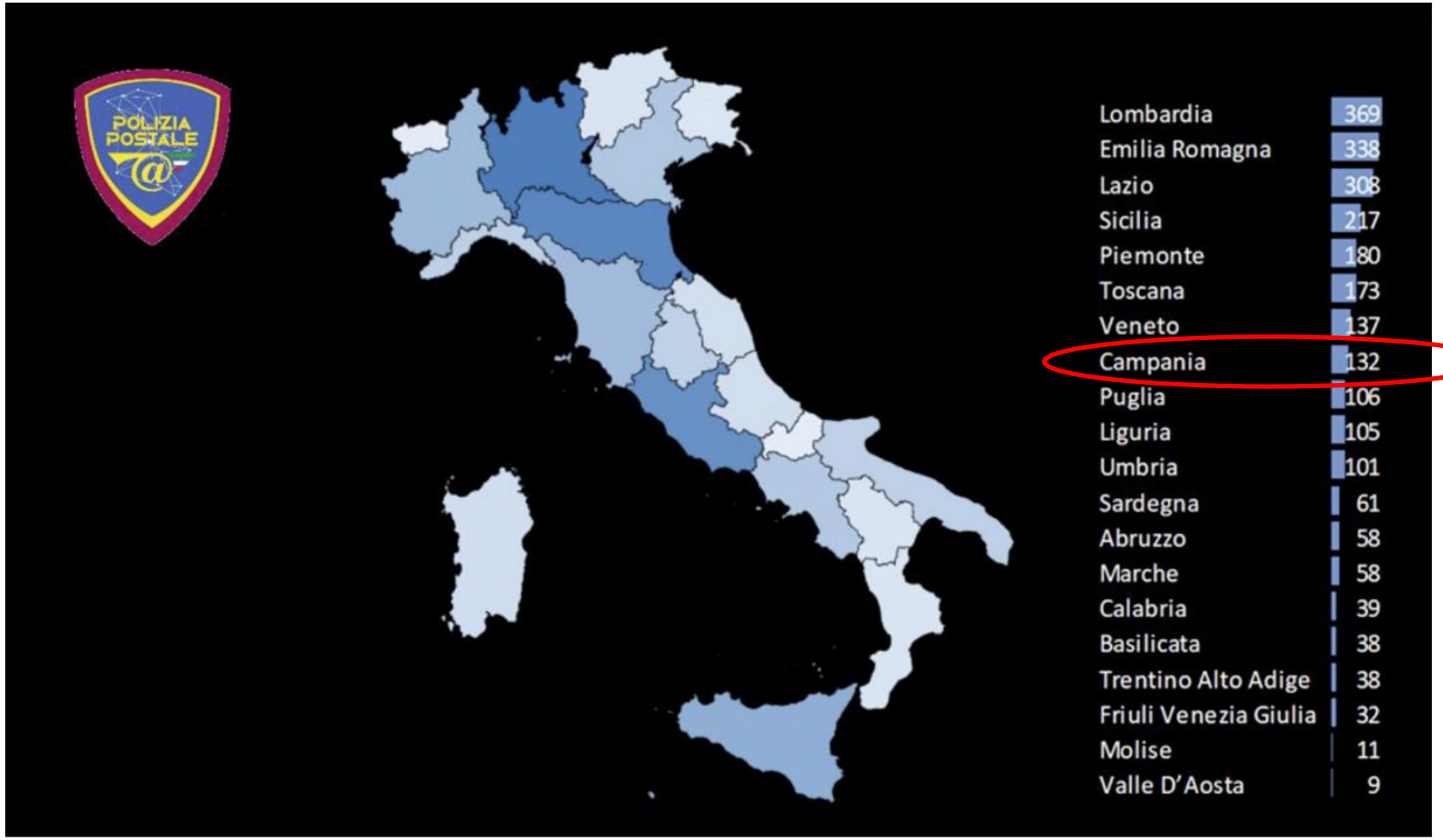
# Truffe Online (Clusit)



# Truffe Online (Clusit)

## CASI DI TRUFFE NEL TRADING ONLINE - Primo semestre 2024



# Modalità di attacco

- E’ molto più «comodo» attaccare un’organizzazione dal suo interno (es. attraverso phishing e tecniche similari) piuttosto che bypassare protocolli e/o dispositivi di sicurezza (HTTPS, Firewalls, etc.)

- Aumenta in maniera vertiginosa la «superficie di attacco» a disposizione dei cybercriminali dal momento che le reti 5G aprono la strada a qualsiasi oggetto che possa essere dotato  di una scheda di rete e di un indirizzo IP (un sensore, un elettrodomestico, una telecamera, dispositivi IoT in genere)

- La presenza massiccia di sistemi di virtualizzazione per ospitare risorse di rete apre la strada a nuovi scenari di attacco

# IoT come possible vettore di minacce

- I dispositivi IoT (sensori, telecamere, etc.) hanno una limitata capacità computazionale che può compromettere la sicurezza di alcune applicazioni

- I dispositivi IoT non riescono a gestire in maniera efficiente i protocolli crittografici

- I dispositivi IoT sono spesso accessibili dall'esterno per manutenzione, riavvii programmati, etc.

# Un caso emblematico: il malware Mirai

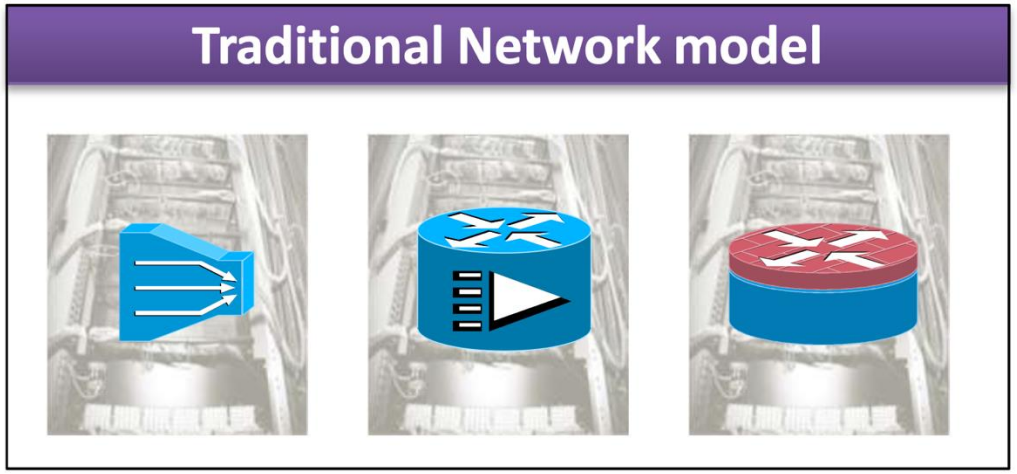
**Obiettivo principale:** infettare webcam, DVR, router sui quali sono installate determinate versioni di BusyBox per trasformarli in BOTS (membri di una botnet) in grado di sferrare un DDoS.

**Attacchi Conosciuti**

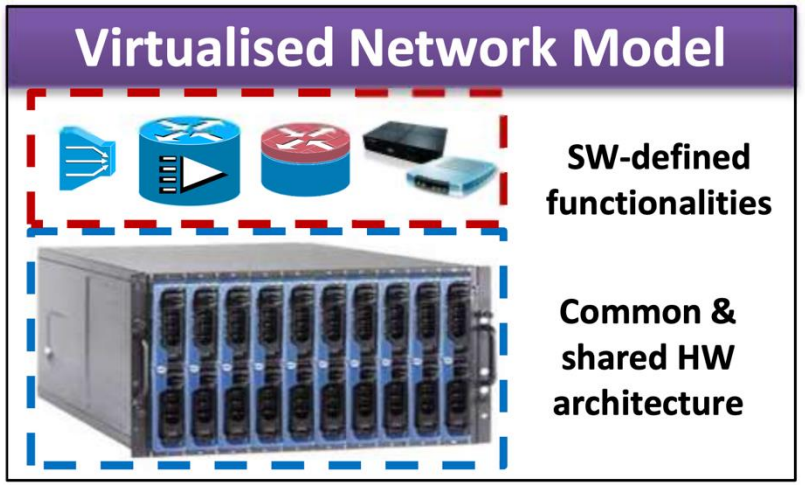
- **OVH - cloud provider francese (1.1 Tbps) – 2016**
- **Circa 900,000 router di Deutsche Tel. fuori uso – 2016**
- **DDoS di circa 54 hr ad un college americano – 2017**
- **Alcuni modelli di tv LG – 2018/2019**
- **Dispositivi di rete Akamai - 2023**

# Le tecnologie abilitanti come vettori di minacce

**NFV (Network Function Virtualization):** tecnologia che consente di trasformare i classici dispositivi di rete (es. router, firewall, etc.) in macchine virtuali (VNF – Virtual Network Function) attraverso il disaccoppiamento hardware/software




- Network functionalities are **based on specific HW&SW**
- **One physical node per role**




- Net functionalities are **SW-based over well-known HW**
- **Multiple roles** over **same HW**

# Le tecnologie abilitanti come vettori di minacce

**NFV (Network Function Virtualization):** tecnologia che consente di trasformare i classici dispositivi di rete (es. router, firewall, etc.) in macchine virtuali (VNF – Virtual Network Function) attraverso il disaccoppiamento hardware/software

**Vantaggi:**

- Riduzione di costi (CAPEX/OPEX)
- Incremento della velocità di rilascio di funzionalità
- Applicazioni di rete altamente personalizzate
- Flessibilità multi-operatore (multi-tenancy)

# Le tecnologie abilitanti come vettori di minacce

**Com’è fatta una VNF, ovvero, una funzionalità di rete realizzata in software?**

**E’ un’applicazione software (ovvero, un processo) che viene gestita da un ambiente virtuale oppure un ambiente a *container (virtualizzazione leggera)***

**Questa alta flessibilità consente di implementare in maniera semplice il paradigma del Network Slicing**

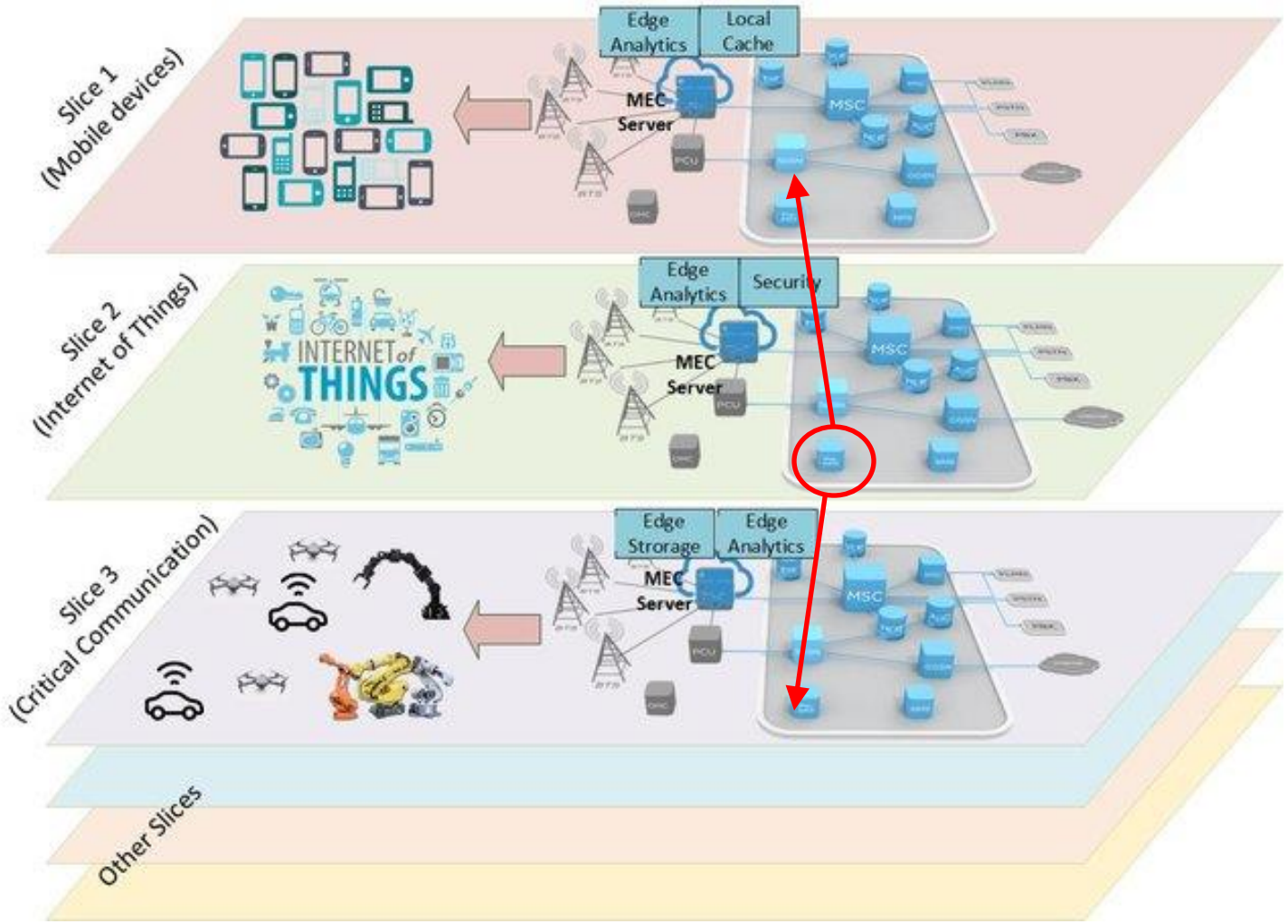
# Le tecnologie abilitanti come vettori di minacce

## Network Slicing

Le «slice» condividono la stessa infrastruttura fisica

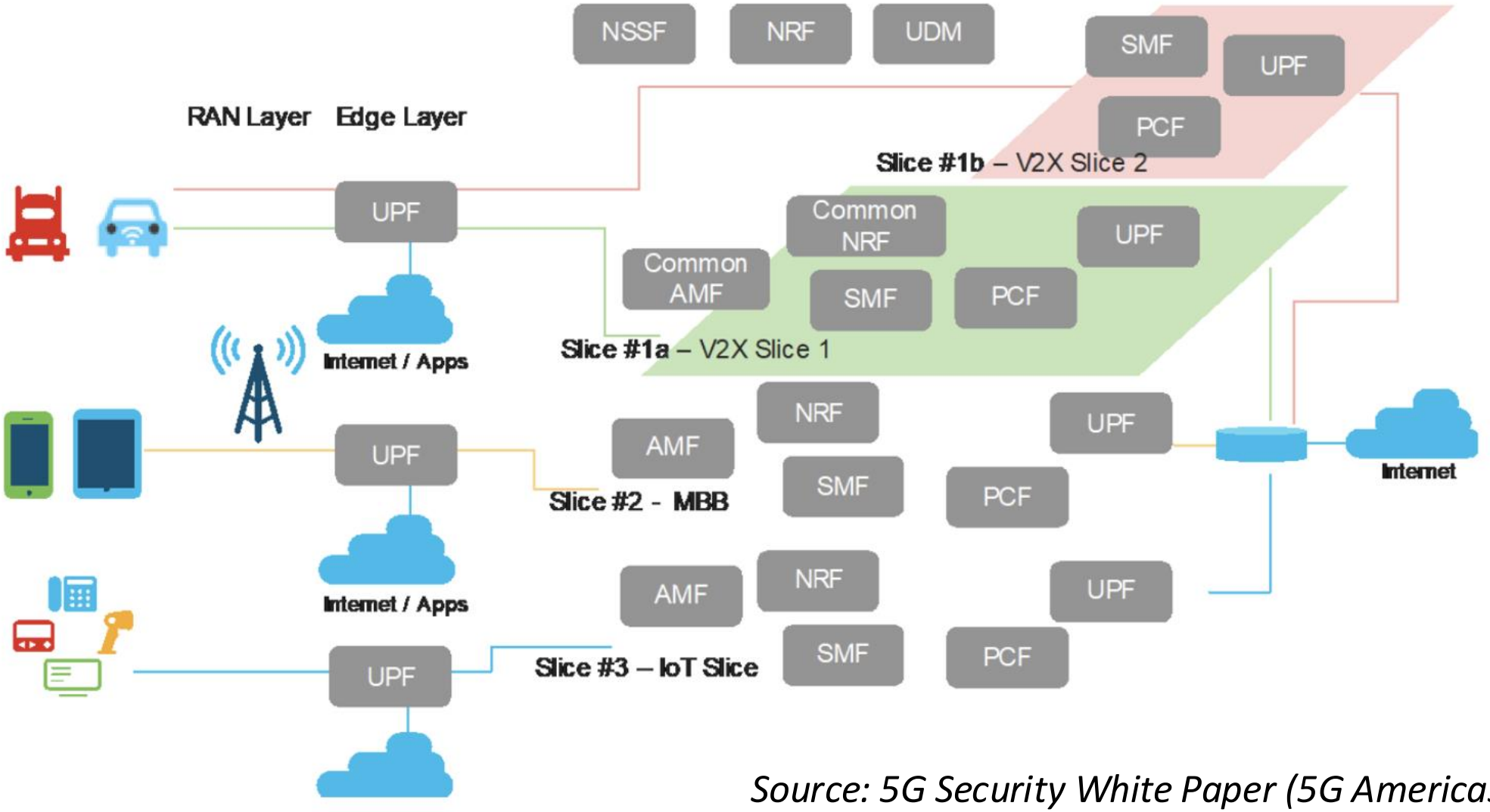
Ogni slice fornisce un servizio differente

Se una slice viene attaccata, c'è un alto rischio che la minaccia si propaghi in altre slice



# Le tecnologie abilitanti come vettori di minacce

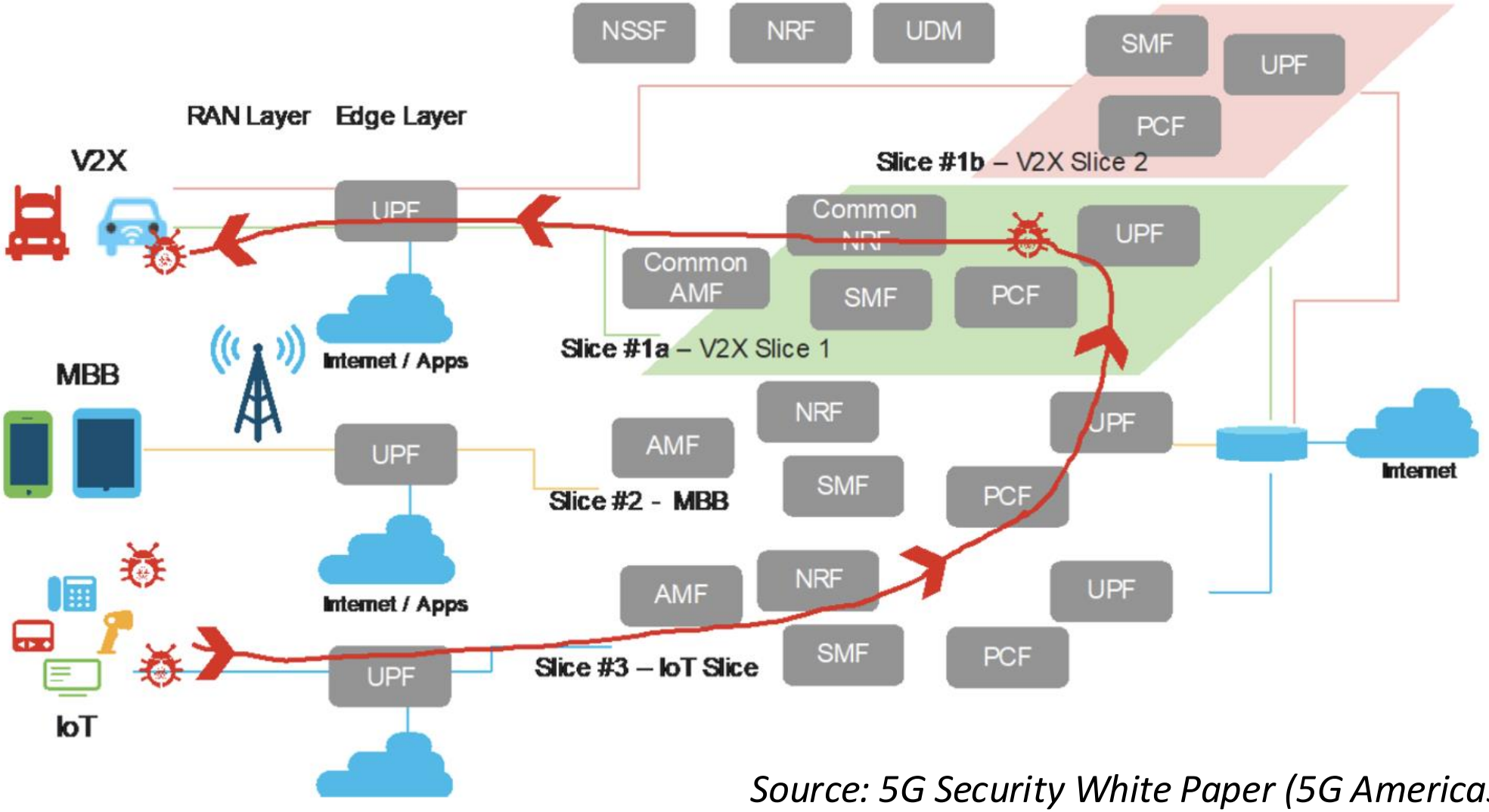
## Network Slicing




*Source: 5G Security White Paper (5G Americas)*

# Le tecnologie abilitanti come vettori di minacce

## Network Slicing




*Source: 5G Security White Paper (5G Americas)*

# Contromisure

- Potenziare le difese (antivirus di rete, IDS) all'*edge,* che rappresenta il punto più «vicino» in cui i dati dei dispositivi distribuiti sono raccolti ed elaborati)

- Adozione di *best practises* ben codificate ed eventualmente normate (es. GDPR)

- Intervento della *Robotic Process Automation* (RPA) nella gestione di attività di routine che comprendono anche processi di sicurezza e conformità

- Utilizzo di tecniche di *Artificial Intelligence* (AI) e *Machine Learning* (ML) a supporto dei sistemi di rilevazione e prevenzione delle intrusioni (IDS/IPS)

- Utilizzo di tecniche (statistiche/probabilistiche) di progettazione di rete per aumentare la resilienza delle infrastrutture ad eventi indesiderati (es. attacchi di rete)

# Contromisure

- Potenziare le difese (antivirus di rete, IDS) all'*edge,* che rappresenta il punto più «vicino» in cui i dati dei dispositivi distribuiti sono raccolti ed elaborati)

- Adozione di *best practises* ben codificate ed eventualmente normate (es. GDPR)

- Intervento della *Robotic Process Automation* (RPA) nella gestione di attività di routine che comprendono anche processi di sicurezza e conformità

- Utilizzo di tecniche di *Artificial Intelligence* (AI) e *Machine Learning* (ML) a supporto dei sistemi di rilevazione e prevenzione delle intrusioni (IDS/IPS)

- Utilizzo di tecniche (statistiche/probabilistiche) di progettazione di rete per aumentare la resilienza delle infrastrutture ad eventi indesiderati (es. attacchi di rete)

# Tecniche di apprendimento automatico (Machine Learning)

**Dispositivi «Classici»:**

- **Firewall**
- **Switch**
- **Router**
- **Intrusion Detection/Prevention Systems**

Questi potrebbero non essere sufficienti a fronteggiare minacce avanzate (es. 0-day attacks)…

# Tecniche di apprendimento automatico (Machine Learning)

## Imparare…da chi?

ML: dall'esperienza passata, ovvero da dati esistenti

## Perchè imparare in maniera «automatica»?

- Mancanza di «human expertise»
- Presenza di fenomeni variabili nel tempo (es. mercati azionari)
- Eterogeneità dei dati

# Tecniche di apprendimento automatico (Machine Learning)

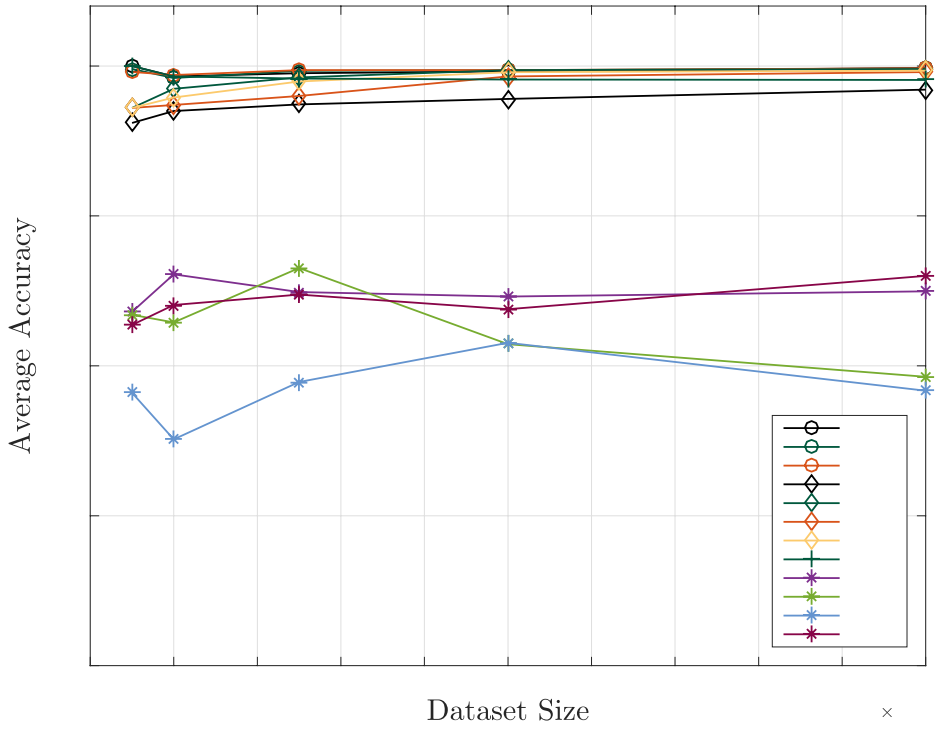
## Supervised Learning (classificazione di traffico dati)

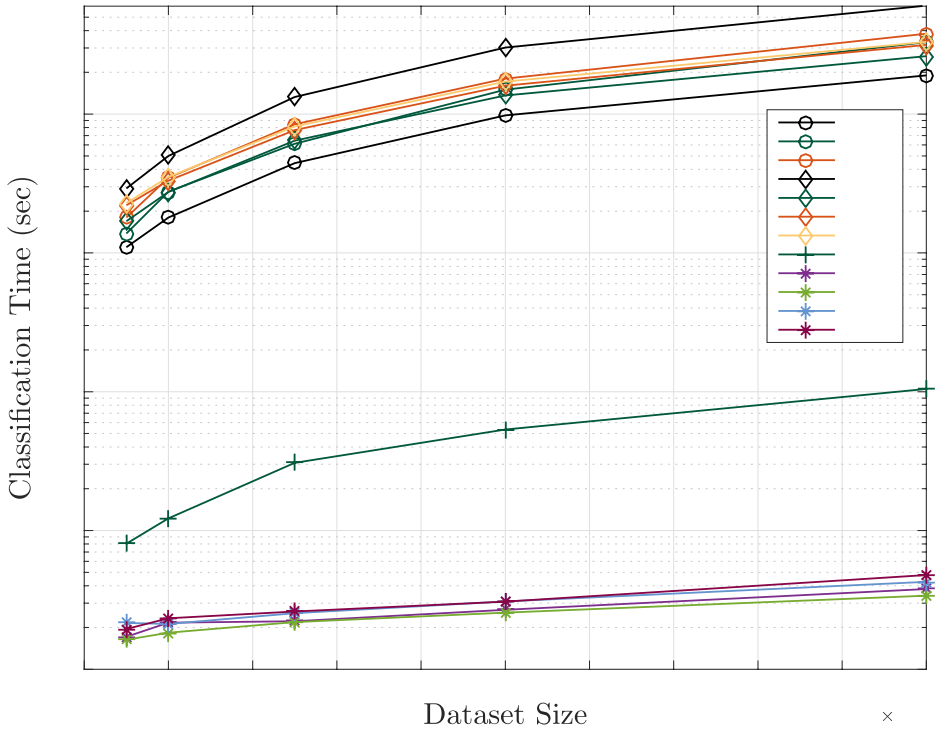
Step 1: **Training** → il sistema «si allena» sui dati esistenti

Step 2: **Classification** → il sistema prova a classificare i dati nuovi sulla base di ciò che ha imparato prima

# Machine Learning (ML) concepts

**Esistono svariati algoritmi di «Classification» che si differenziano per accuracy (una misura dell'efficacia di un algoritmo a classificare bene un dato) e per complessità temporale (una misura di quanto impiega un algoritmo a classificare un dato).**




Di Mauro et al. «*Experimental Review of Neural-Based Approaches for Network Intrusion Management*», IEEE Transactions on Network and Service Management (Sept. 2020)

# Contromisure

- Potenziare le difese (antivirus di rete, IDS) all'*edge,* che rappresenta il punto più «vicino» in cui i dati dei dispositivi distribuiti sono raccolti ed elaborati)

- Adozione di *best practises* ben codificate ed eventualmente normate (es. GDPR)

- Intervento della *Robotic Process Automation* (RPA) nella gestione di attività di routine che comprendono anche processi di sicurezza e conformità

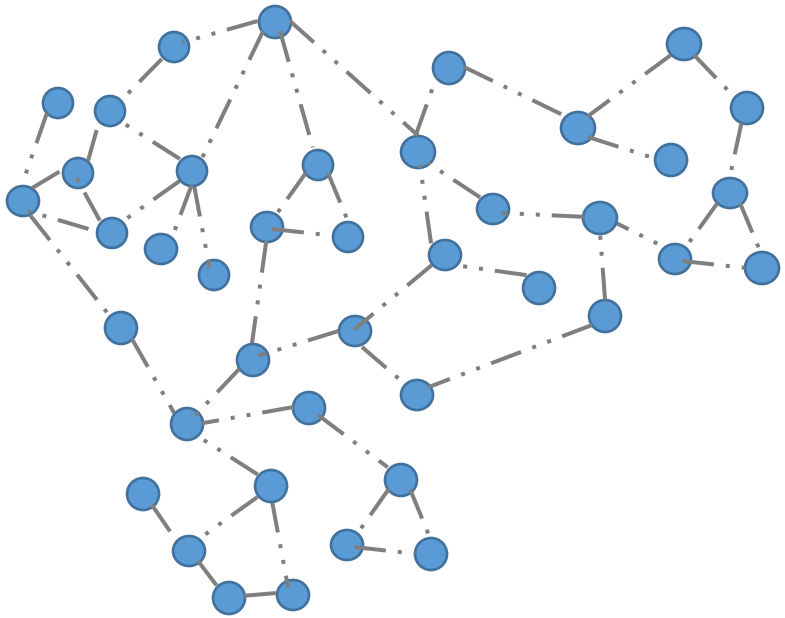
- Utilizzo di tecniche di *Artificial Intelligence* (AI) e *Machine Learning* (ML) a supporto dei sistemi di rilevazione e prevenzione delle intrusioni (IDS/IPS)

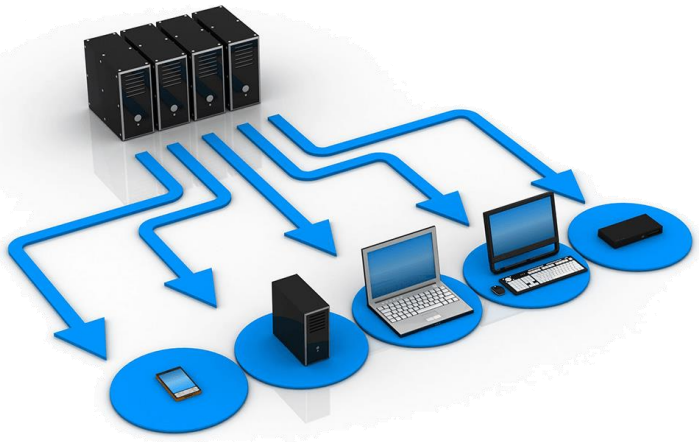
- Utilizzo di tecniche (statistiche/probabilistiche ) di progettazione di rete per aumentare la resilienza delle infrastrutture ad eventi indesiderati (es. attacchi di rete)

# Resilienza contro attacchi di rete

**I moderni attacchi alle reti presentano spesso due caratteristiche:**

- Sono in grado di emulare traffico dati non sospetto, e quindi possono eludere anche i più sofisticati sistemi di intrusion detection (anche quelli che applicano tecniche di ML…)
- Riescono a creare disservizi (es. congestione di rete, saturazione di risorse) in un arco temporale limitatissimo (dell'ordine di poche decine di minuti)

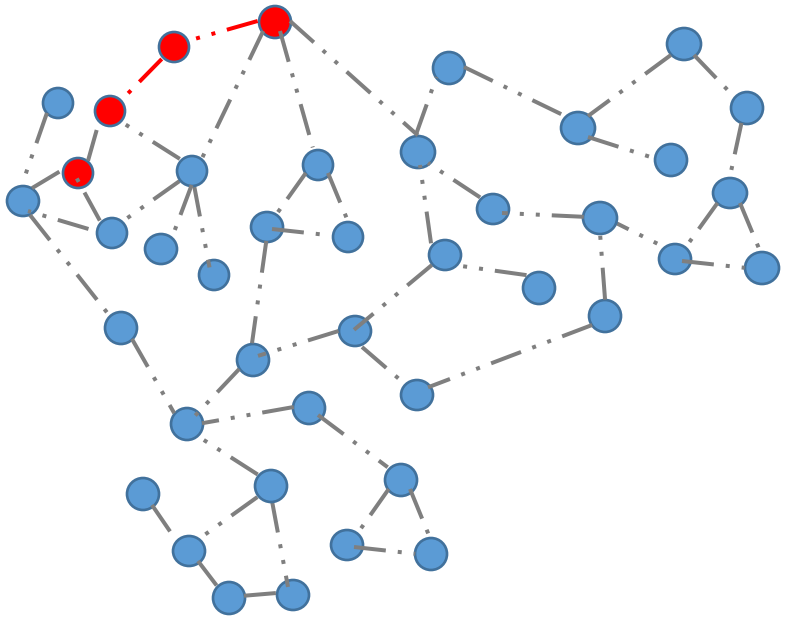


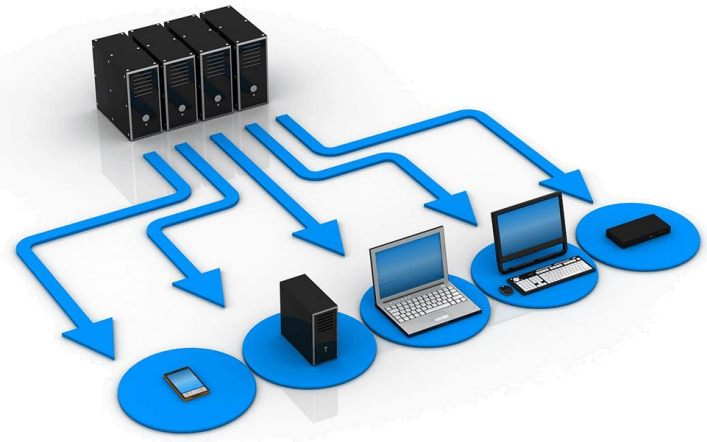


# Resilienza contro attacchi di rete

**I moderni attacchi alle reti presentano spesso due caratteristiche:**

- Sono in grado di emulare traffico dati non sospetto, e quindi possono eludere anche i più sofisticati sistemi di intrusion detection (anche quelli che applicano tecniche di ML…)
- Riescono a creare disservizi (es. congestione di rete, saturazione di risorse) in un arco temporale limitatissimo (dell'ordine di poche decine di minuti)

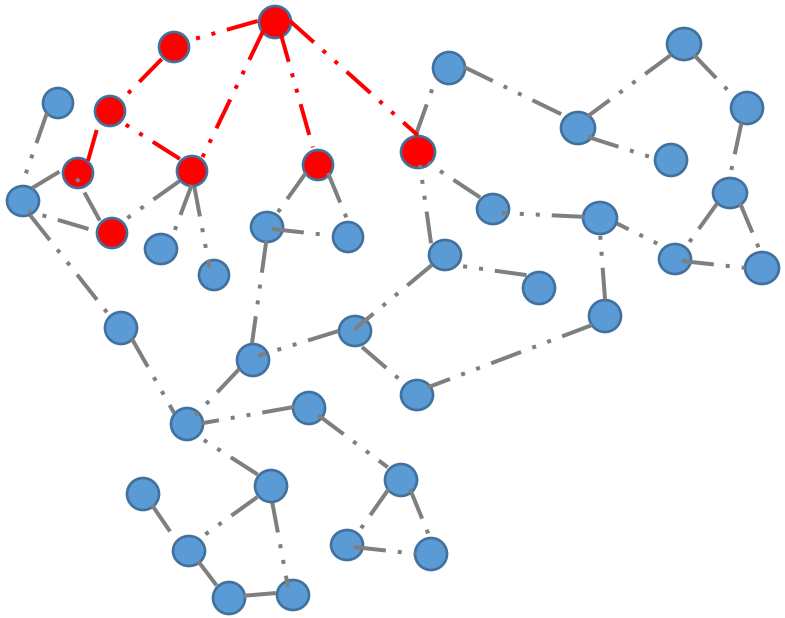


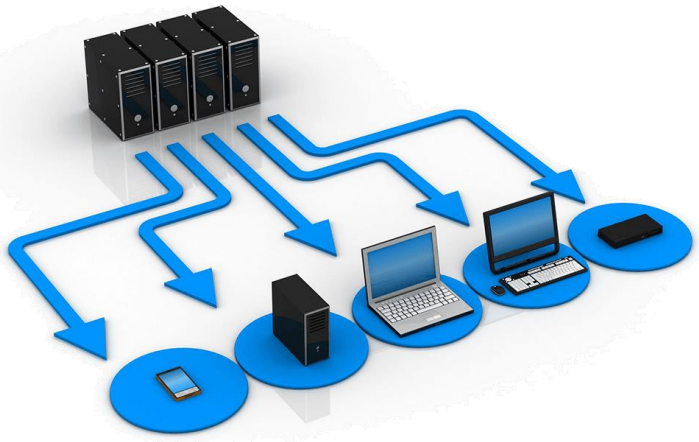


# Resilienza contro attacchi di rete

**I moderni attacchi alle reti presentano spesso due caratteristiche:**

- Sono in grado di emulare traffico dati non sospetto, e quindi possono eludere anche i più sofisticati sistemi di intrusion detection (anche quelli che applicano tecniche di ML…)
- Riescono a creare disservizi (es. congestione di rete, saturazione di risorse) in un arco temporale limitatissimo (dell'ordine di poche decine di minuti)

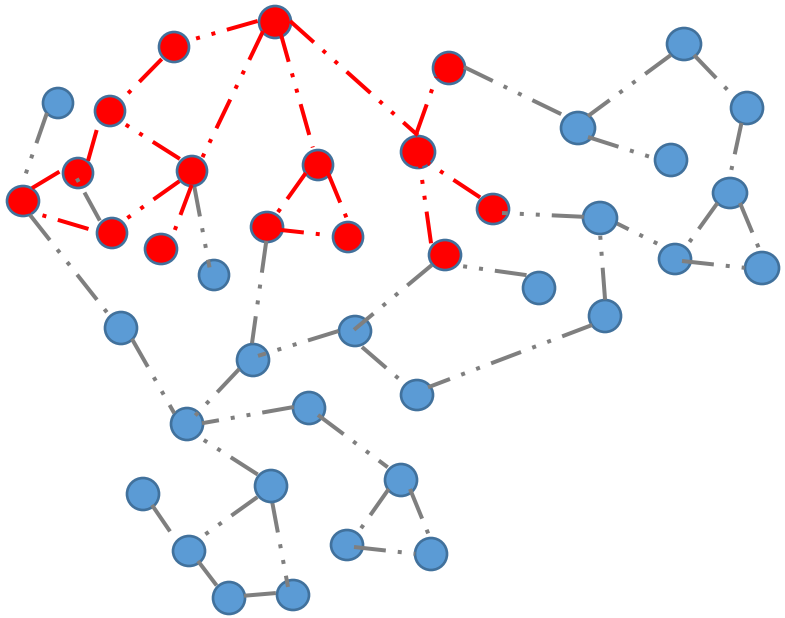


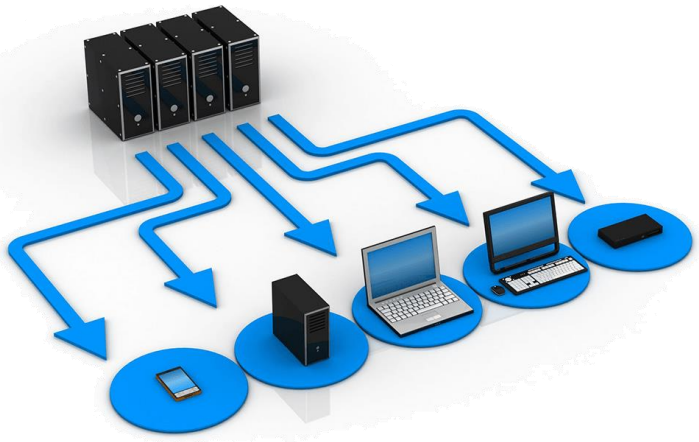


# Resilienza contro attacchi di rete

**I moderni attacchi alle reti presentano spesso due caratteristiche:**

- Sono in grado di emulare traffico dati non sospetto, e quindi possono eludere anche i più sofisticati sistemi di intrusion detection (anche quelli che applicano tecniche di ML…)
- Riescono a creare disservizi (es. congestione di rete, saturazione di risorse) in un arco temporale limitatissimo (dell'ordine di poche decine di minuti)

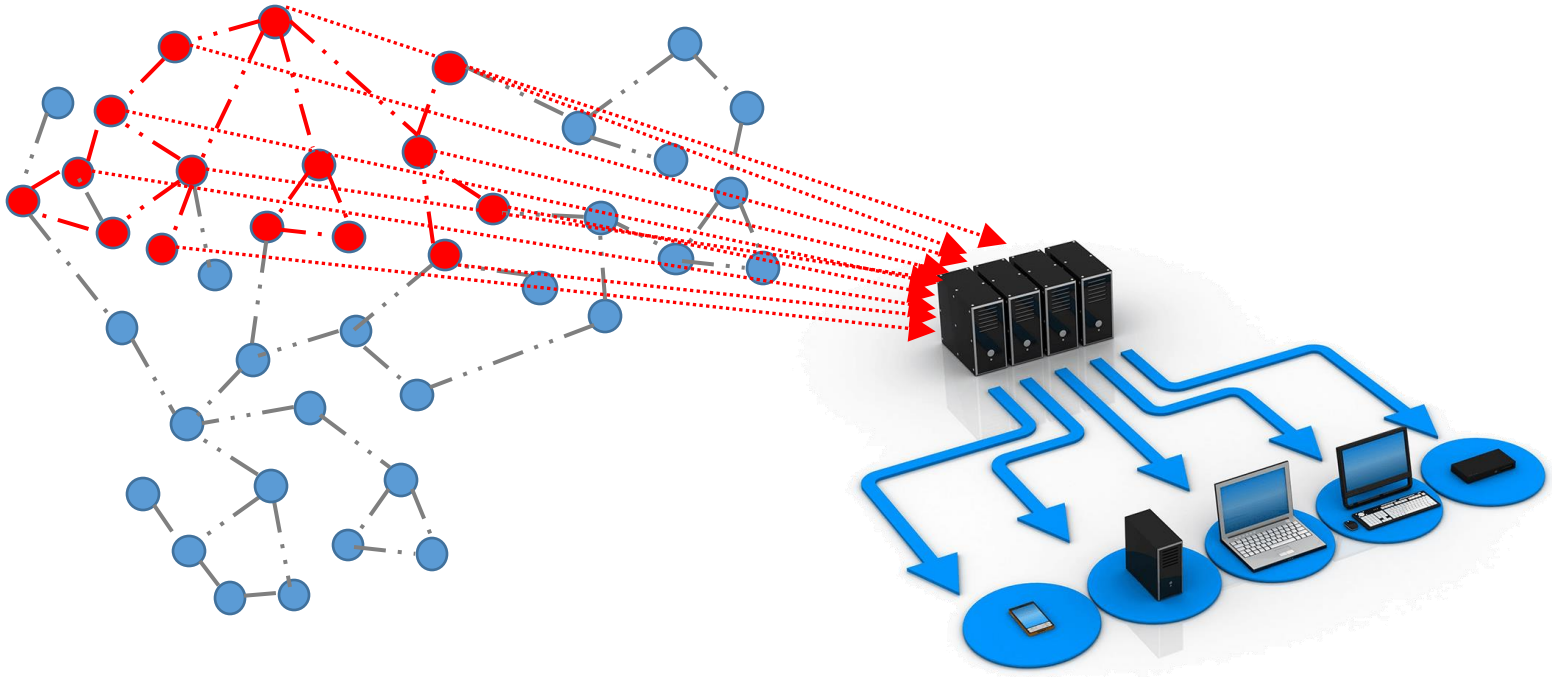




# Resilienza contro attacchi di rete

**I moderni attacchi alle reti presentano spesso due caratteristiche:**

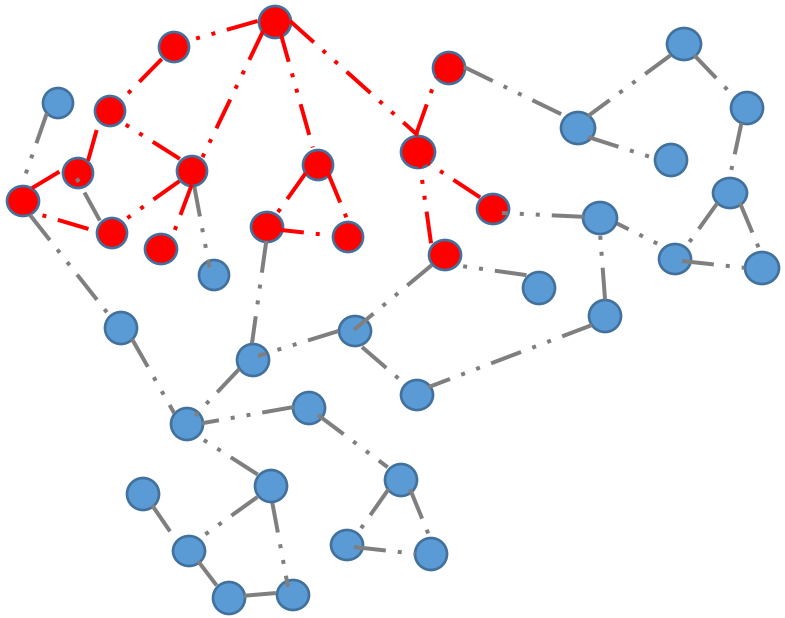
- Sono in grado di emulare traffico dati non sospetto, e quindi possono eludere anche i più sofisticati sistemi di intrusion detection (anche quelli che applicano tecniche di ML…)
- Riescono a creare disservizi (es. congestione di rete, saturazione di risorse) in un arco temporale limitatissimo (dell'ordine di poche decine di minuti)

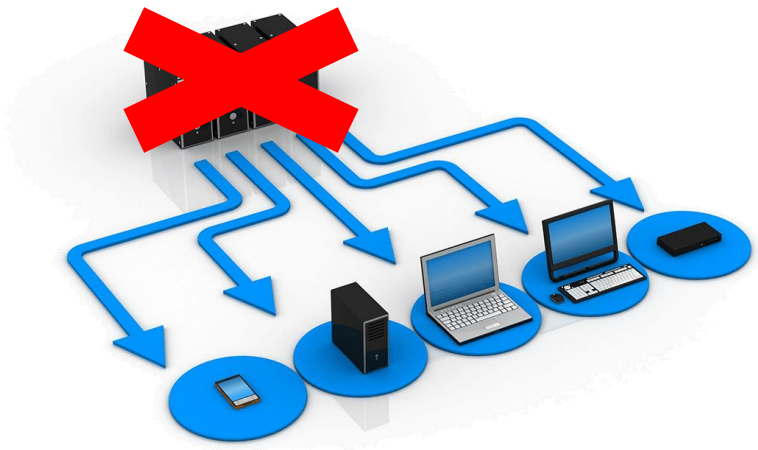


# Resilienza contro attacchi di rete

**I moderni attacchi alle reti presentano spesso due caratteristiche:**

- Sono in grado di emulare traffico dati non sospetto, e quindi possono eludere anche i più sofisticati sistemi di intrusion detection (anche quelli che applicano tecniche di ML…)
- Riescono a creare disservizi (es. congestione di rete, saturazione di risorse) in un arco temporale limitatissimo (dell'ordine di poche decine di minuti)

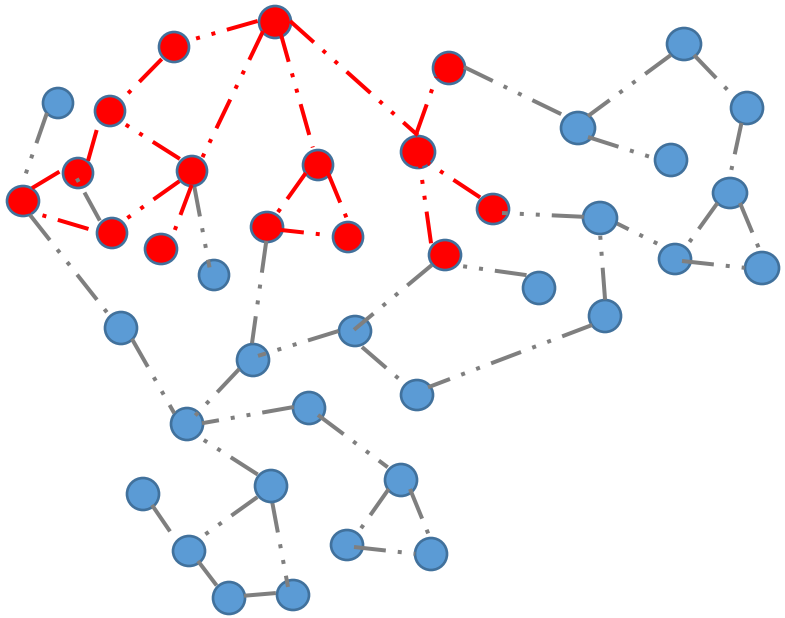


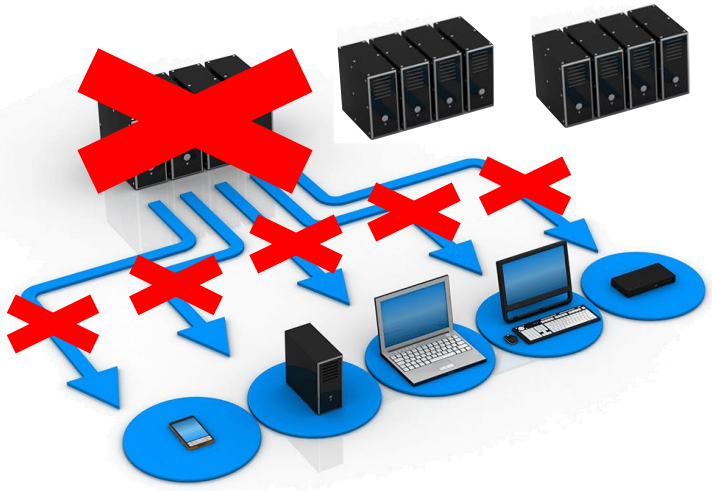


# Resilienza contro attacchi di rete

**Possibile soluzione:**
**Ridondanza Controllata con algoritmi di ottimizzazione**

- Ridondare «troppo poco» vuol dire essere inefficaci nei confronti dell'attacco
- Ridondare «troppo» vuol dire affrontare costi troppo elevati





# Resilienza contro attacchi di rete

**Come si implementa un modello a ridondanza controllata?**

1. Creare un modello probabilistico di failure/repair di un sistema

2. Risolvere il modello probabilistico e ricavare una misura di resilienza, per es., l'affidabilità (capacità di un sistema di essere «up» quando viene richiesto un servizio)

3. Costruire un modello di ridondanza sulla base di una soglia di affidabilità, es., affidabilità «five nines»: il sistema non può essere fuori servizio più di 5 minuti e 15 secondi all'anno (*Prob di funzionamento*=0.99999)

# Resilienza contro attacchi di rete

**Una rete può essere considerata sicura al 100%?**

**Certo! Basta eliminare tutte le connessioni! ☺**

# Grazie per l'attenzione!