

CYBERSECURITY

Sicurezza informatica

Elena Maria Dal Santo

elenamaria.dalsanto@its-ictpiemonte.it

F.A.Q.

Who am I?

Elena

Cybersec?

Non lavoro nel campo cybersecurity, ma ho dedicato il mio percorso di studi e la mia tesi di laurea al mondo della crittografia.

Topics?

Cybersecurity, crittografia, sicurezza web/cloud/database

Handout?

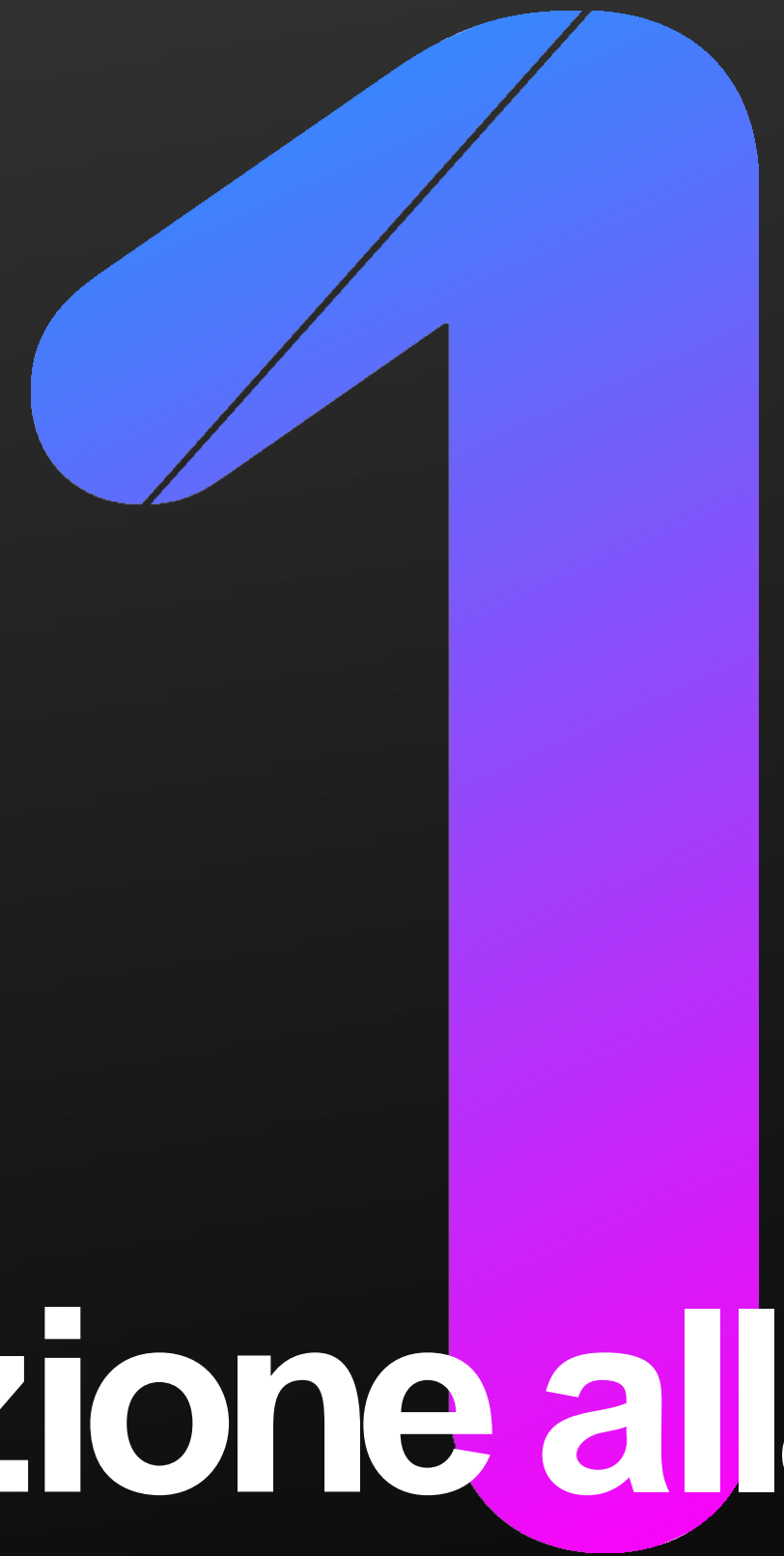
Slide a fine lezione

Exam?

Sulla teoria, a risposta chiusa

Questions?

Non esistono domande stupide.



Introduzione alla cybersecurity

Come definiamo il rischio?

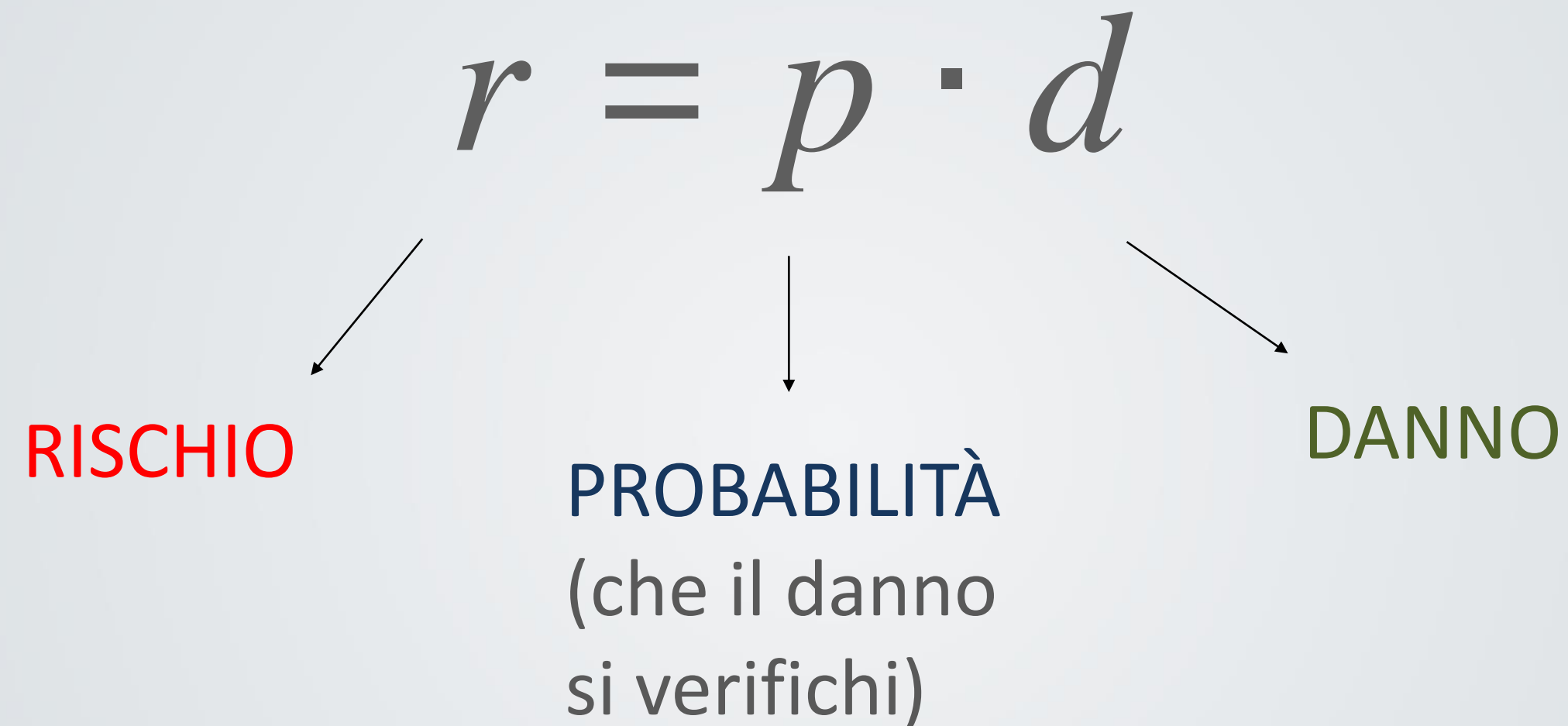


Valutazione del rischio

Il rischio è la **probabilità** di subire una perdita in seguito a un attacco.

È implicata l'esistenza di una sorgente di pericolo, detta **minaccia**, e delle possibilità che essa si trasformi in un **danno**.

Come definiamo il rischio?



Es. è poco probabile che cada un aereo, ma se cade il danno è molto grande.
Quanto è grande il RISCHIO?

Cos'è la sicurezza?

«**Sicurezza**» è la conoscenza (si spera, precisa) che l'evoluzione di un sistema non produrrà stati indesiderati.

Analisi del
rischio



Raggiungere il
maggior livello di
sicurezza possibile



Eliminare il più
possibile le
vulnerabilità.

Perché ci interessa?

VEDIAMO INSIEME UN PO' DI DATI...

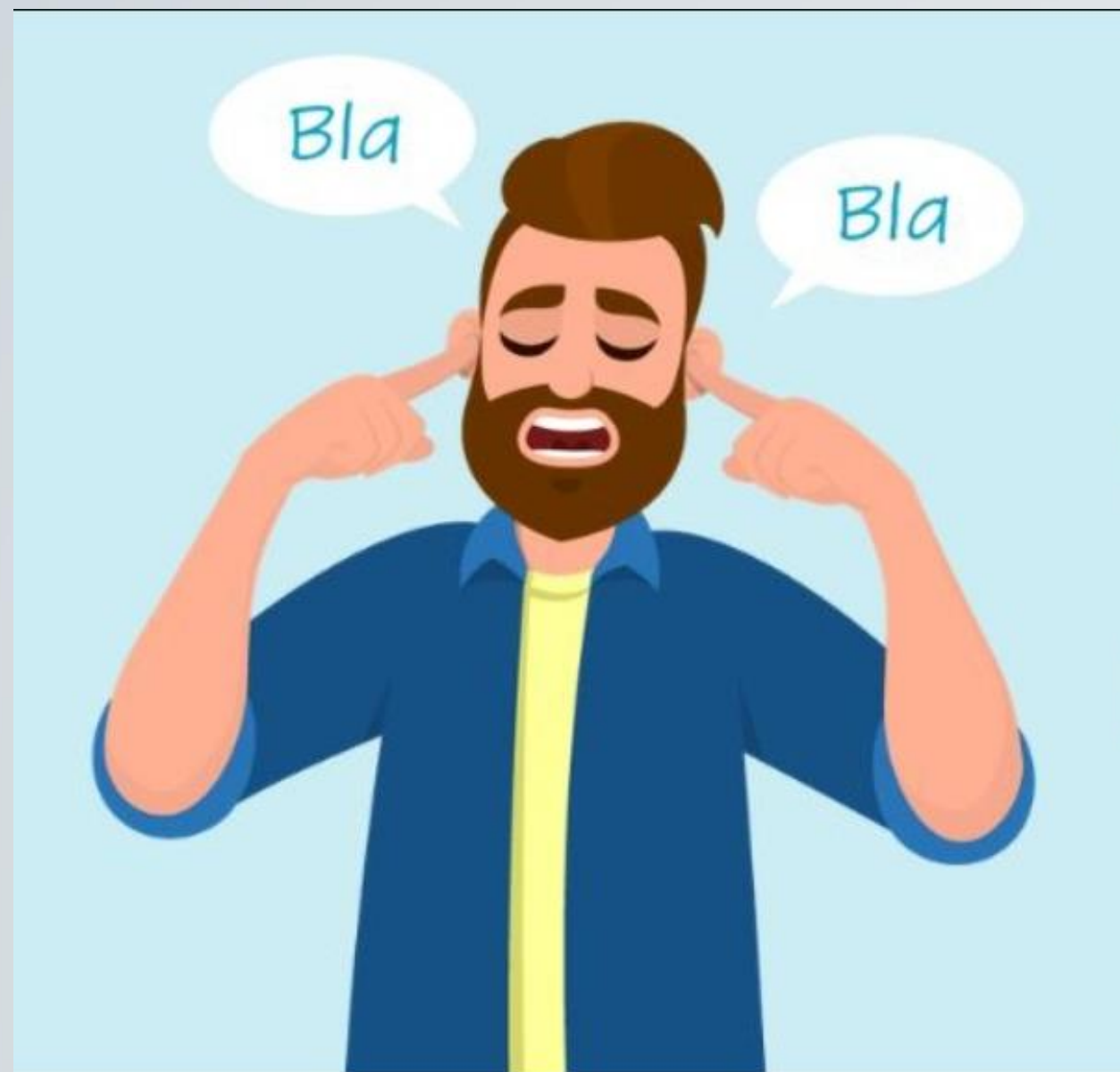
Per gli eventuali curiosi:
trovate i link alle fonti
nelle ultime slide

- **85%** delle violazioni della sicurezza informatica sono causati da errori umani. ([Verizon](#))
- **94%** di tutti i malware viene consegnato tramite e-mail. ([CSO online](#))
- Gli attacchi ransomware si verificano ogni **10 secondi**. ([Gruppo InfoSecurity](#))
- **71%** di tutti gli attacchi informatici sono motivati finanziariamente (seguiti dal furto di proprietà intellettuale e quindi dallo spionaggio). ([Verizon](#))
- Si stima che il costo globale annuo del crimine informatico sia **\$ 10.5 trilioni** entro il 2025. ([Cybersecurity Ventures](#))

Il COSTO dei danni da criminalità informatica è intorno ai 6 trilioni ("6 con 18 zeri") di dollari l'anno...

190mila dollari AL SECONDO

Droga + traffico di essere umani + furto di petrolio + estrazione mineraria e pesca illegale + traffico d'armi generano «solo» 2 trilioni di dollari l'anno

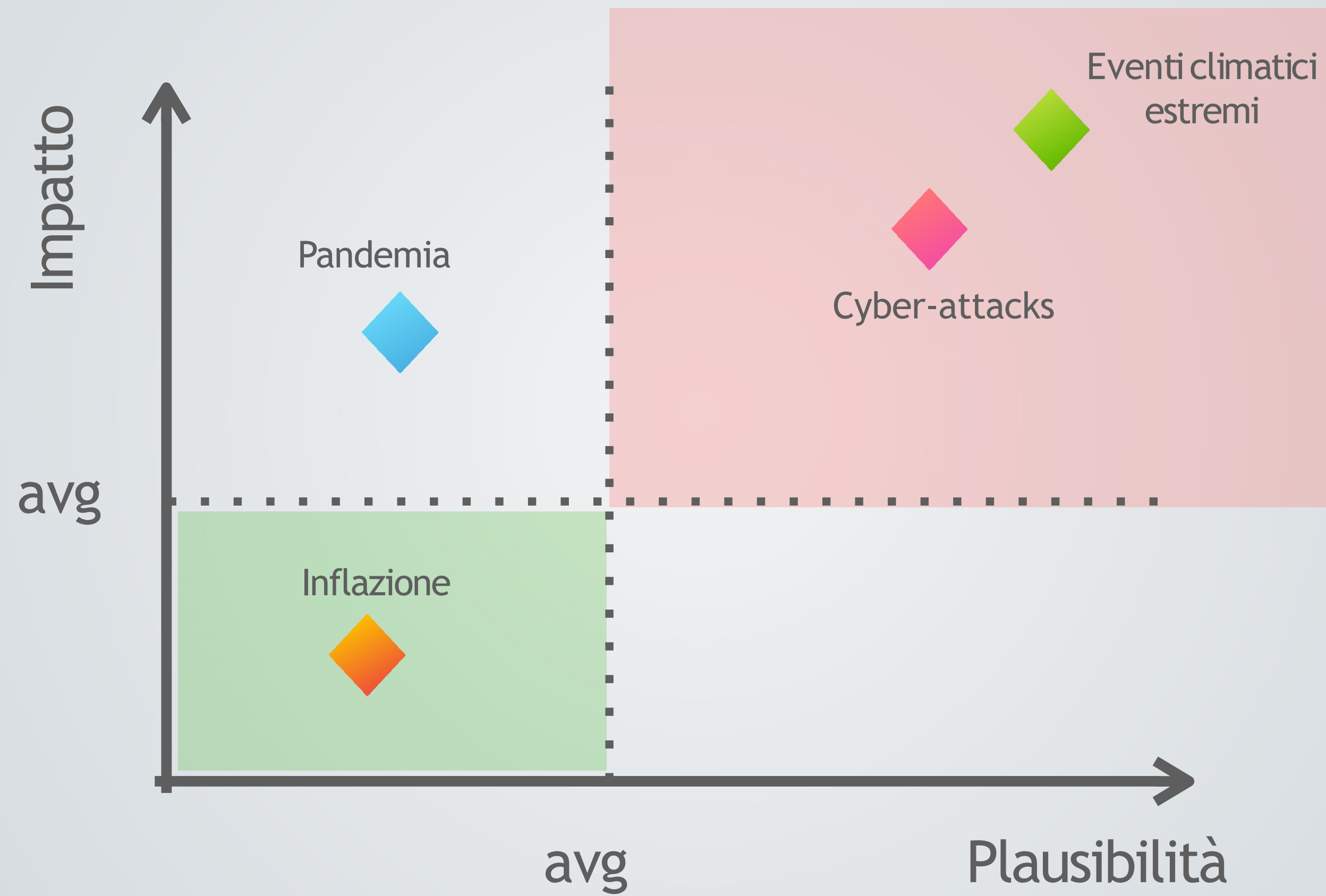


«Tanto a me non succede...»

La stima degli attacchi informatici è di

1 attacco ogni 10 secondi

In media, ci vogliono 280 giorni per rilevare e fermare
un attacco informatico



Cosa vogliamo proteggere?

- A livello PERSONALE
- A livello AZIENDALE
- A livello STATALE
- A livello GLOBALE
- ... altre idee?

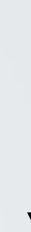
La SICUREZZA INFORMATICA

È



L'insieme dei prodotti, dei servizi, delle regole organizzative e dei comportamenti individuali che proteggono i sistemi informatici (di un'azienda)

Serve a



Garantire la triade

Confidentiality

Integrity

Availability

Confidenzialità



Integrità



Disponibilità



2

Vulnerabilità

Vulnerabilità

È un punto debole del sistema in cui le misure di sicurezza sono assenti, ridotte o compromesse. Può essere sfruttata per compromettere il sistema stesso.



Anche il software migliore contiene delle vulnerabilità!

Vulnerabilità

Un **exploit** è un attacco che sfrutta una vulnerabilità

PER

Creare comportamenti
imprevisti nel sistema

Eseguire un **rootkit**

Insieme di software o
strumenti che vengono
usati per dare pieni poteri
sulla modifica di un
sistema.

Vulnerabilità

I rootkit possono essere usati per aprire delle **backdoor**



Accessi privilegiati in grado di superare le procedure di sicurezza attivate su un sistema informatico. Spesso usate per lanciare attacchi di tipo DoS.



Le backdoor possono essere create anche dagli amministratori di sistema per agevolare la manutenzione del software stesso!

Vulnerabilità

Grande minaccia costituiscono le **0-day vulnerability**

- È nota all'attaccante, ma non allo sviluppatore
- Lo sviluppatore ha 0 giorni per riparare la falla prima che possa essere utilizzata per un exploit
- OIS Guidelines for Security Vulnerability Reporting and Response (lo sviluppatore deve avere un tempo sufficiente a rilasciare la fix prima che la vulnerabilità venga divulgata)

3

**Attacks &
attackers**

Un **attacco** è un accesso non autorizzato al sistema, con conseguente utilizzo dei dati contenuti al suo interno.

Un attacco può compromettere confidenzialità, integrità e disponibilità (CIA) dei dati o del sistema stesso.



Tipologie di attacchi

Attivi

Integrità e disponibilità

- MASCHERAMENTO
- RIPETIZIONE
- MODIFICA
- DoS e DDoS

Passivi

Autenticazione e riservatezza

- INTERCETTAZIONE
- SNIFFING



NON implicano alterazione dei dati (→complicati da riconoscere)

Attacchi ATTIVI

MASCHERAMENTO

Un'entità finge di essere un'altra.

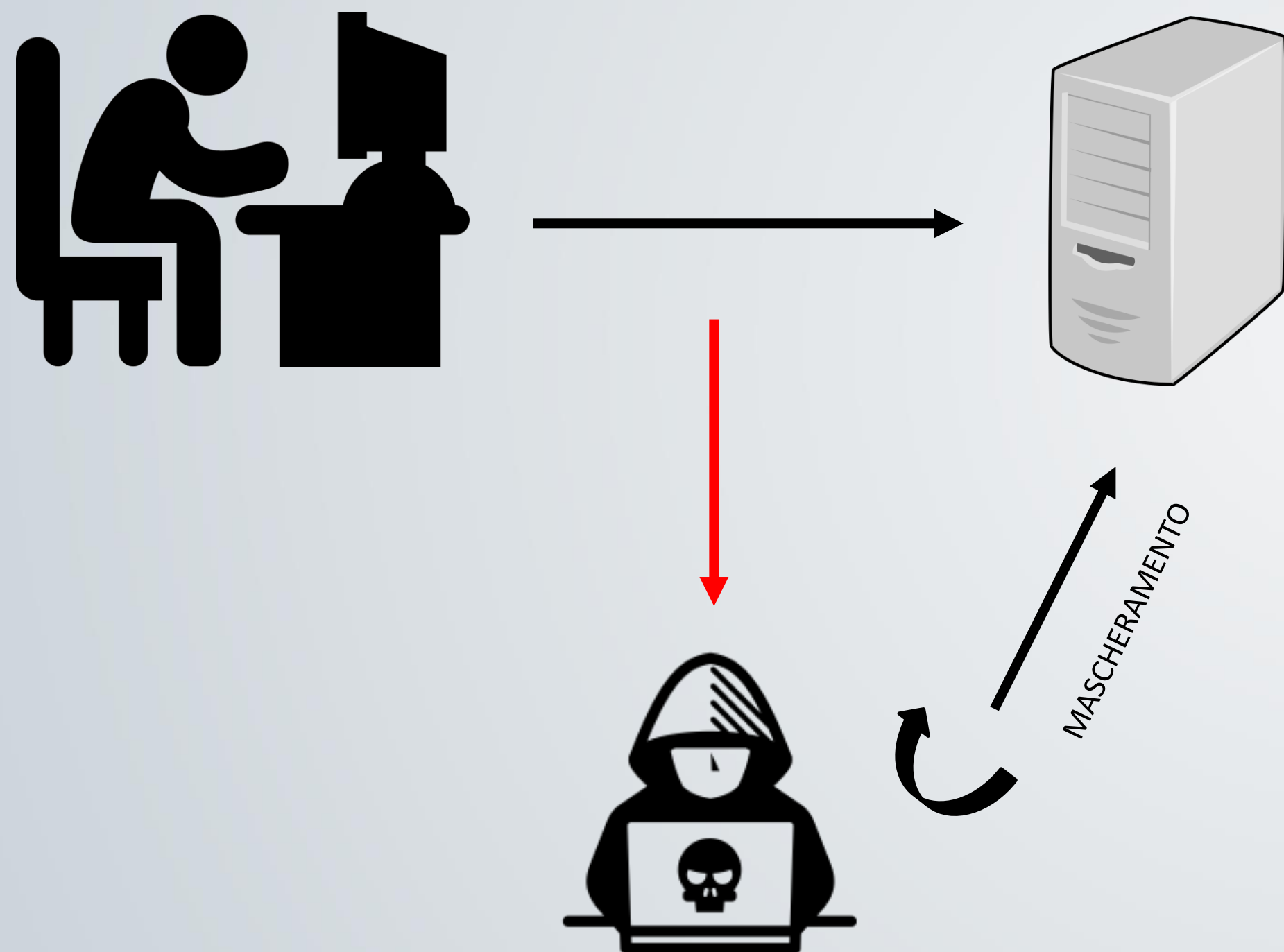
Es. inserisco le mie credenziali di accesso a un account, ma username e password vengono intercettati. Chi effettua l'attacco può ora mascherarsi da entità autorizzata all'accesso.



Solitamente questo tipo di attacco implica mosse successive

Attacchi ATTIVI

RIPETIZIONE



Serie di azioni volte a catturare dei dati, con l'obiettivo di ritrasmetterli e ottenere effetti dannosi.

Es. accedo al mio account, un nemico mi ruba la password. Quando faccio logout, il nemico usa le mie credenziali per fare login e sfruttare i servizi.

Attacchi ATTIVI

MODIFICA

Cambiamento, totale o parziale, di uno o più messaggi al fine di generare caos, ritardi, mancate evasioni.

Gli effetti non sono prevedibili a priori.



«Ti diamo un aumento!»

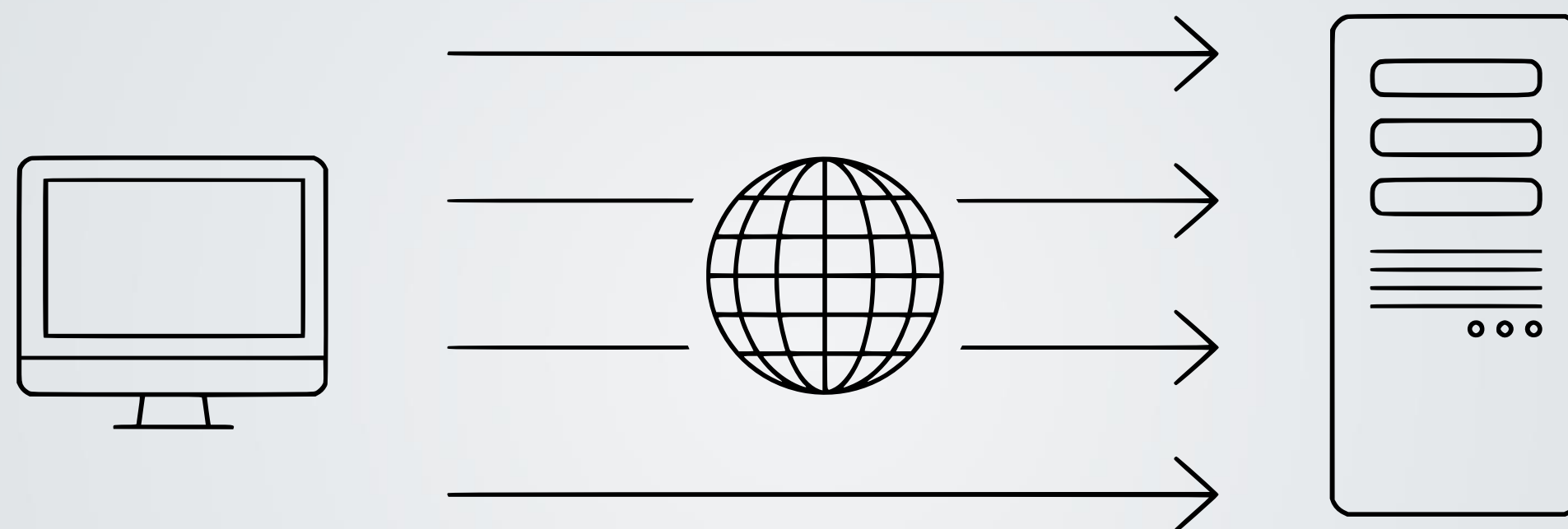


«Notifica di licenziamento?!»



Attacchi ATTIVI

DENIAL OF SERVICE (DoS)



Esaurimento delle risorse del sistema informatico che fornisce un servizio (es. sito web) fino a renderlo non più in grado di erogare il servizio stesso.

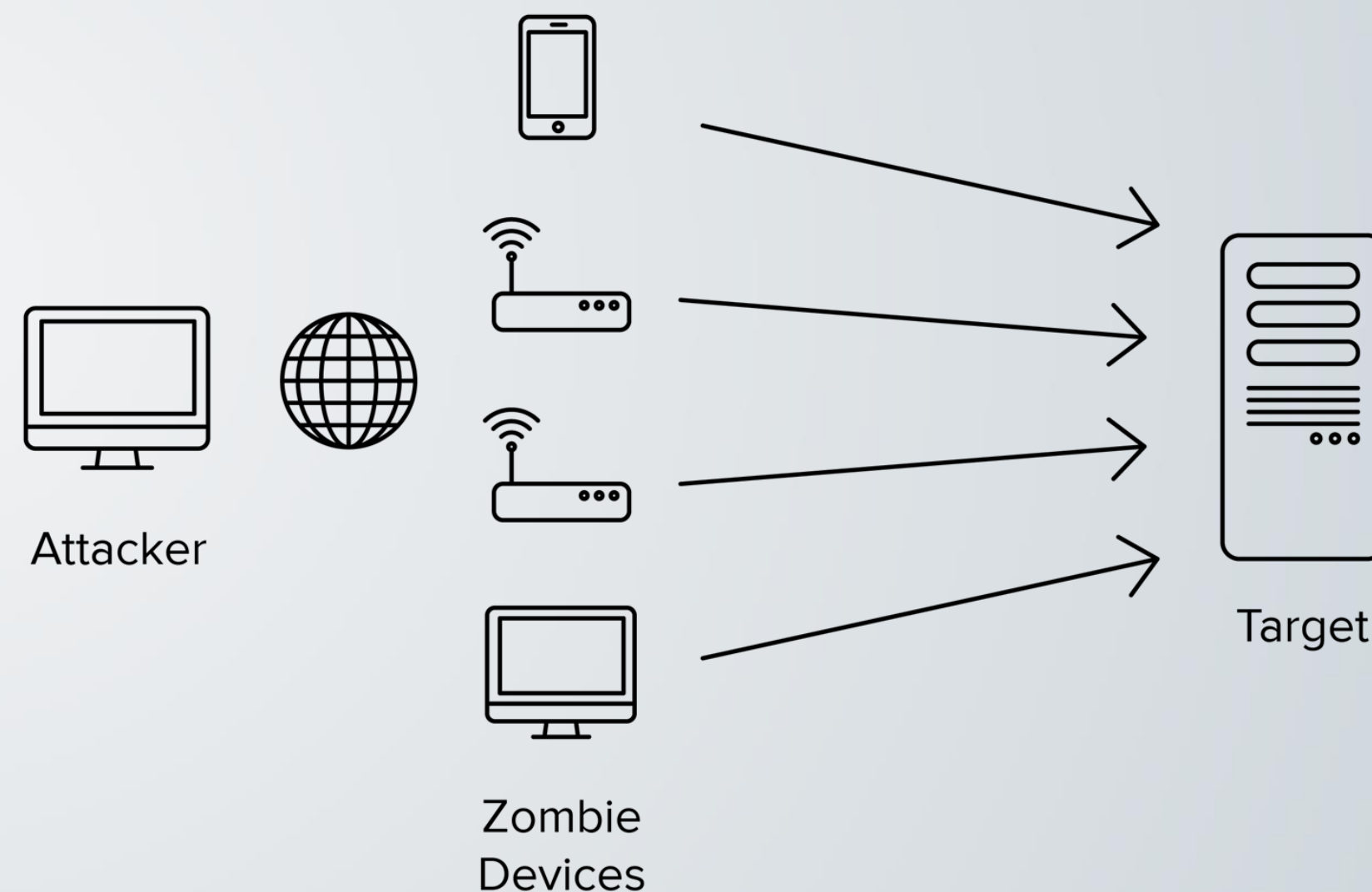
Il traffico “inonda” la vittima.

Attacchi ATTIVI

DISTRIBUTED DENIAL OF SERVICE (DDoS)

Il traffico che inonda la vittima proviene da molte fonti diverse.

L'attacco non si può più fermare "facilmente"
(bloccando una singola fonte)



Attacchi ATTIVI

DoS e DDoS



Es. Avete provato a comprare i biglietti per il Lucca Comics il giorno dell'apertura della vendita generale?



Attacchi PASSIVI

INTERCETTAZIONE



Attacchi PASSIVI

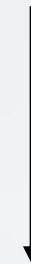
SNIFFING

Analisi del traffico dati, con attacchi rivolti alla **crittografia** dei messaggi (i messaggi sono “nascosti”, ma io li intercetto, li capisco e li posso usare).



Malware

Sono strumenti con cui può essere sferrato un attacco.



Un malware è un software maligno che può essere usato per ottenere dati sensibili e/o cancellare, modificare, corrompere dati e software.

Malware

Qual è l'obiettivo dei malware?

Risposta: c'è l'imbarazzo della scelta

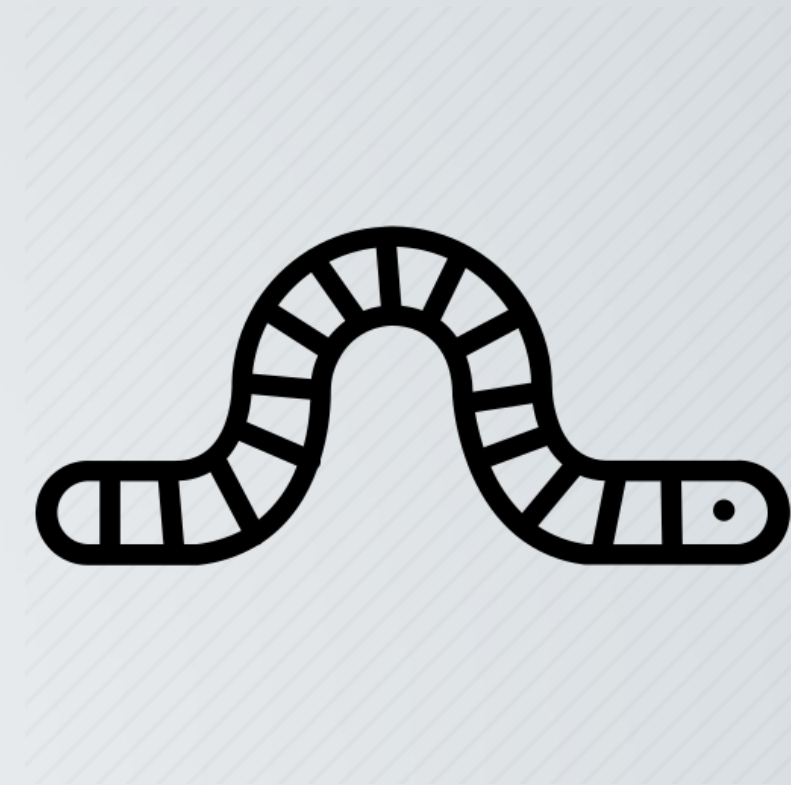


Malware



Virus

Si **attacca** a un codice eseguibile, si moltiplica all'interno dei vari file del programma per compiere il suo lavoro



Worm

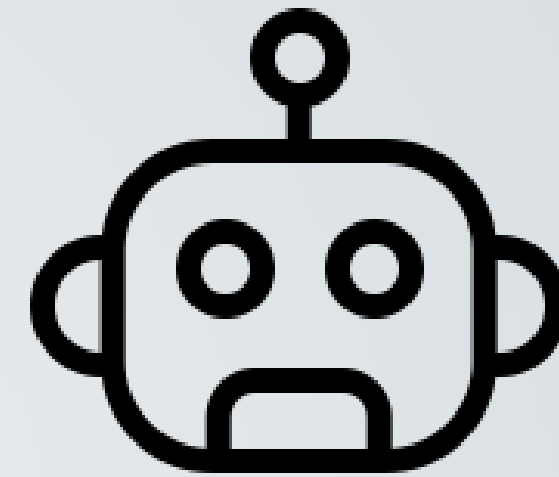
Non si attacca, vive **da sé** e può diffondersi (ad esempio attraverso la rete aziendale)

Malware



Trojan

Malware che **sembra una cosa** ma in realtà ne fa un'altra



Botnet

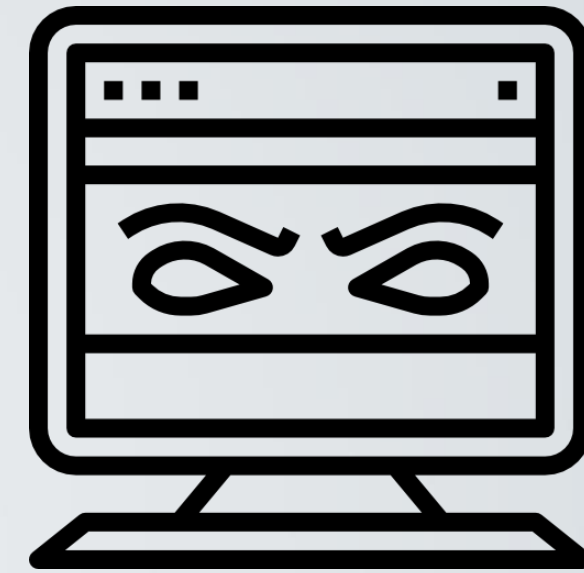
A compiere l'attacco è una **macchina diversa** da quella dell'attaccante (comunque controllata dall'attaccante). Sfruttano le potenzialità di macchine connesse in rete per eseguire funzioni distribuite tra queste.

Malware



Ransomware

I dati rubati vengono tenuti in **ostaggio** e solitamente viene chiesto un ricatto.



Spyware

Costruiti apposta per **spiare** le azioni e i comportamenti della vittima.

Social Engineering

Insieme di tecniche rivolte a spingere le persone a fornire informazioni personali o a consentire l'accesso a un computer.

“È più facile spingere una persona a rivelare le proprie password, che cercare di scoprirle con metodi di hacking”



Cyber attackers

Minacce interne

Malicious insider

Impiegati o partner che usano i loro accessi legittimi per accedere ai dati confidenziali per un vantaggio personale.

Inside agent

Dipendenti malintenzionati neoassunti, ma alle reali dipendenze di una parte esterna che ruba, altera o cancella dati riservati.

Emotional employees

Dipendenti emotivi che causano danno all'azienda per vendetta in seguito ad un torto subito (a ragione o meno).

Reckless employees

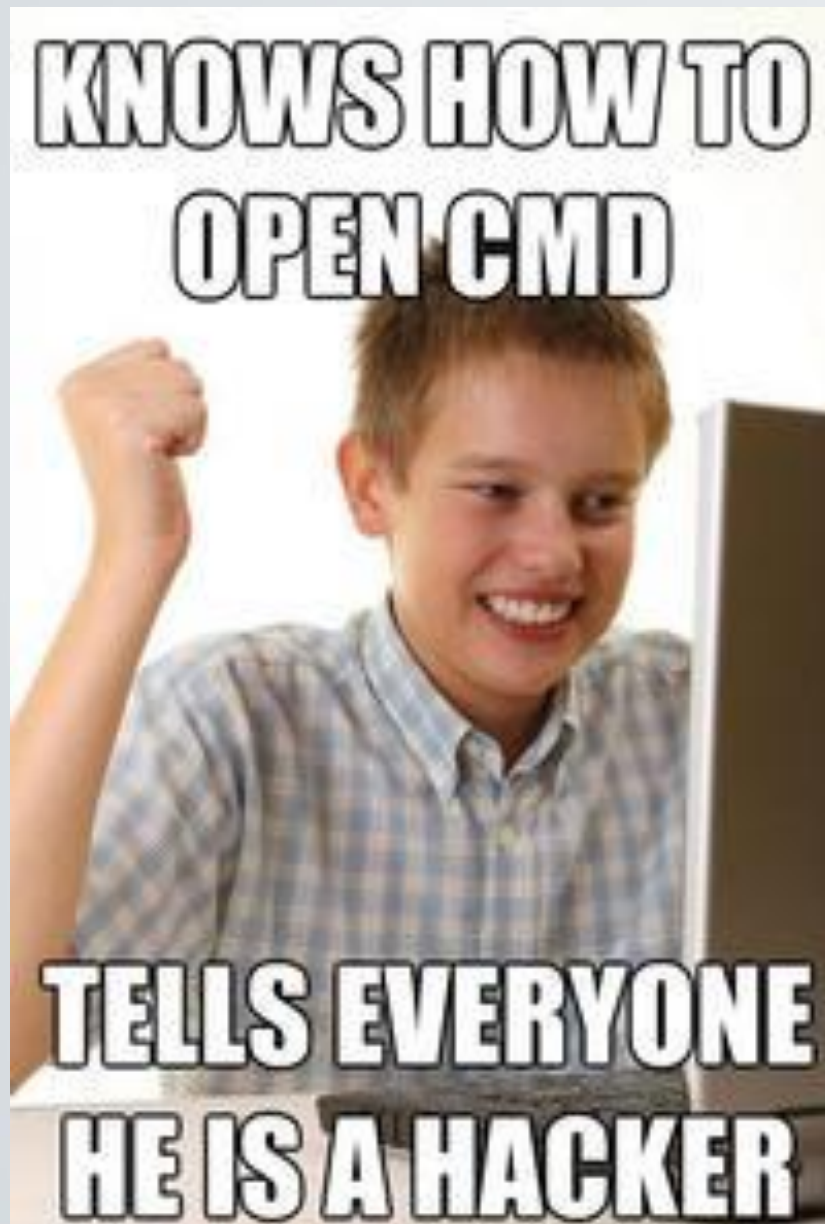
Dipendenti o terze parti che non accettano le regole delle policy di sicurezza dell'azienda.

Third-party users

Un collaboratore che si avvantaggia dell'accesso ai dati per compromettere la sicurezza delle informazioni.

Cyber attackers

"Script kiddies"



Abilità limitate

Uso di tool professionali

Danni potenzialmente devastanti

Tracce spesso non coperte

Mafiaboy (2000): 15 anni, DDoS, causa 1,7\$ miliardi di danni.



Cyber attackers

White hat

Classe

Legale buono

Allineamento

Comunemente conosciuto come hacker etico, è uno dei lavori più ricercati negli ultimi anni.



- Usa le sue abilità per scopi leciti e legali.
- Conduce **penetration-test** per scoprire vulnerabilità delle reti o dei sistemi informatici.
- Lavora sotto contratto e stila report
- Es. **Log4j vulnerability** (2021 – Chen Zhaojun) – «La vulnerabilità più critica dell'ultimo decennio»



Cyber attackers

Gray hat

Classe

Caotico buono

Allineamento

Spinto dalla curiosità si aggira
nel meandri del web alla ricerca
di vulnerabilità zero-day.



- Guidati dalla curiosità
- Le vulnerabilità vengono scoperte illegalmente o con metodi non etici.
- Risolvono le vulnerabilità scoperte sotto compenso oppure divulgano le informazioni nel web senza venderle.
- Es. Khalil Shreath— 2013 — **Facebook**



Cyber attackers

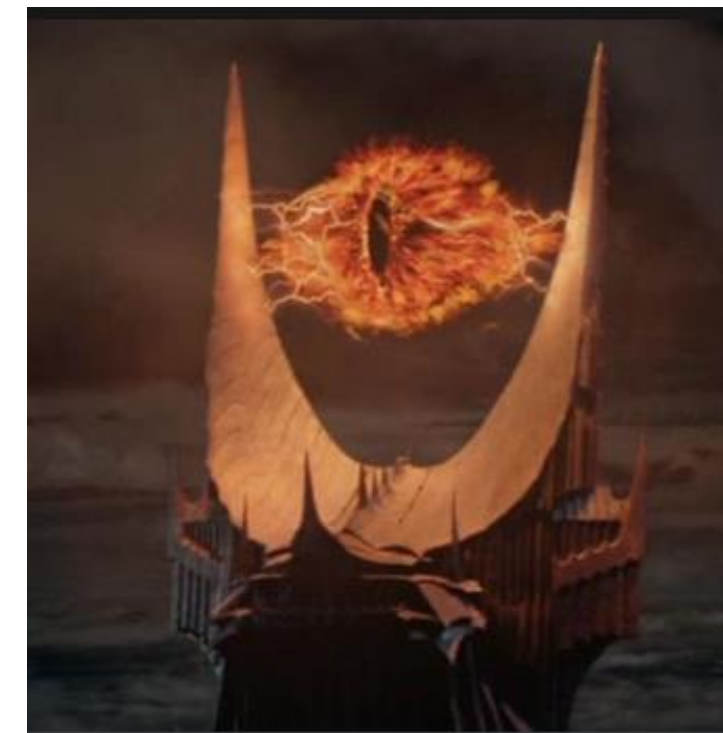
Black hat

Classe

Caotico malvagio

Allineamento

Il dark web è l'habitat naturale in cui mietono vittime senza pietà.



- Lavora per causare un danno, o per prelevare informazioni private e confidenziali, con o senza vantaggio personale (profitto economico o politico).
- Può vendere i propri servizi sul dark web.

Es. **Kevin Mitnick** – Nel 1995 era l'hacker più ricercato del mondo – danni a oltre 40 compagnie

Cyber attackers

Organized hackers



Organizzazioni
criminali

Es. DarkSide



Hacktivist

Es. Anonymous,
Black Reward,
donk_enby



State- sponsored

Es. Lazarus Group

Link utili

- OLTRE 40 STATISTICHE E FATTI SULLA SICUREZZA INFORMATICA PER IL 2022, <https://www.websiterating.com/it/research/cybersecurity-statistics-facts/>
- Cyberattacks 2021: Phishing, Ransomware & Data Breach Statistics From the Last Year, <https://spanning.com/blog/cyberattacks-2021-phishing-ransomware-data-breach-statistics/>

