



# Cybersecurity: meglio pensarci prima

**Roberto Caldelli**

Prof. Associato di Sicurezza delle Reti e Cybersecurity



Università telematica delle  
Camere di Commercio Italiane



# Sommario



- Concetti introduttivi di cybersecurity
- La sicurezza di un sistema informatico
- Gli hacker
- Tipologie di attacchi informatici
- Alcuni dati statistici
  
- Cyber risk management
- Rischi aziendali
- Possibili soluzioni e buone pratiche

# Introduzione: una possibile definizione



## Cybersicurezza (Cybersecurity):

l'insieme delle attività necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità, e garantendone altresì la resilienza.

*DECRETO-LEGGE 14 giugno 2021, n. 82*

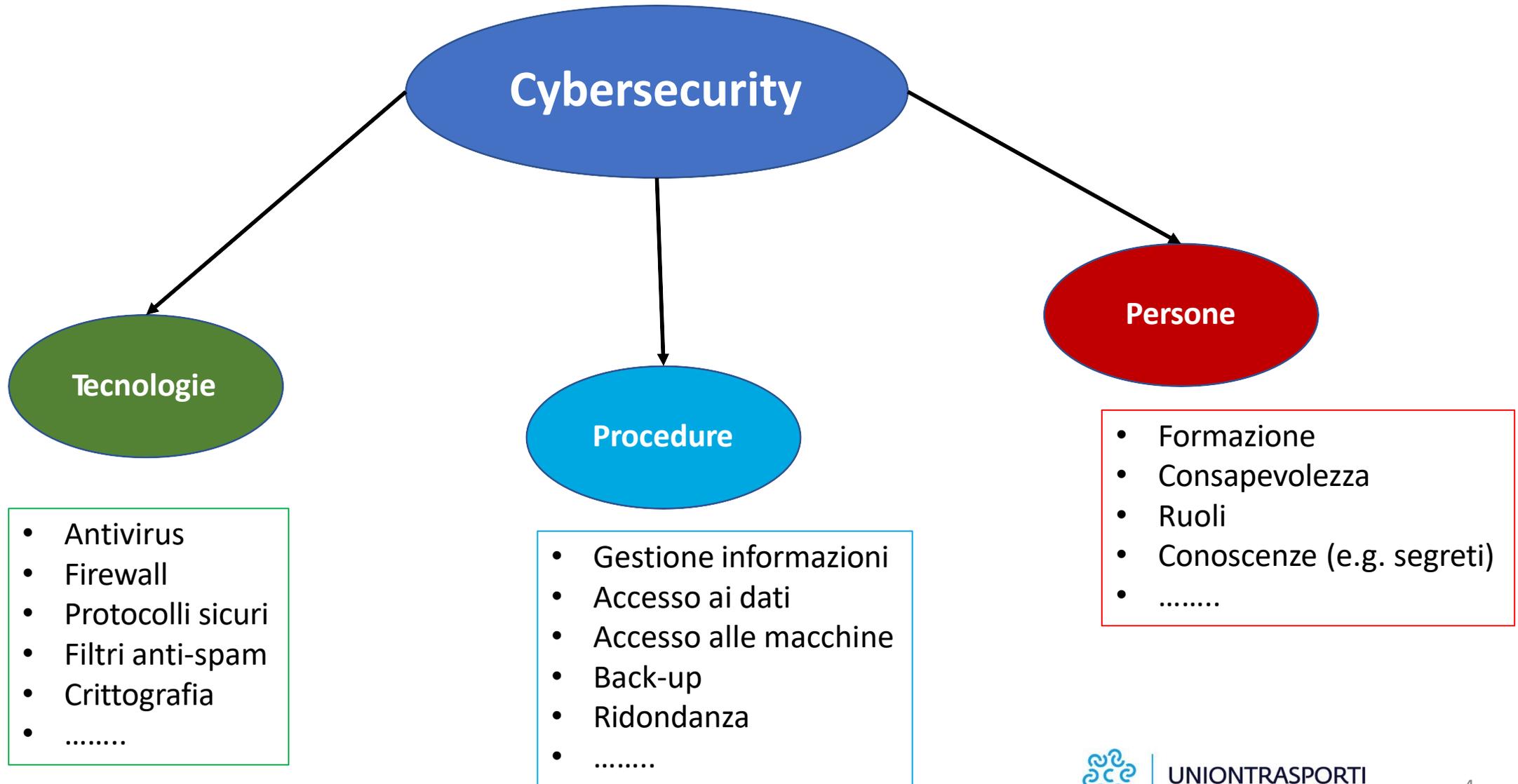


## Cybersicurezza vs Sicurezza Informatica.....

La Sicurezza Informatica si riferisce a mezzi, tecnologie e procedure  
La Cybersicurezza si riferisce alle tecnologie



# Le componenti fondamentali



# Il Cyber risk



## **Minaccia (Threat):**

potenziale azione malevola volta a determinare un funzionamento anomalo o non autorizzato

## **Vulnerabilità (Vulnerability):**

caratteristica di un componente/sistema/procedura di essere suscettibile a guasti o malfunzionamenti

## **Rischio (Risk):**

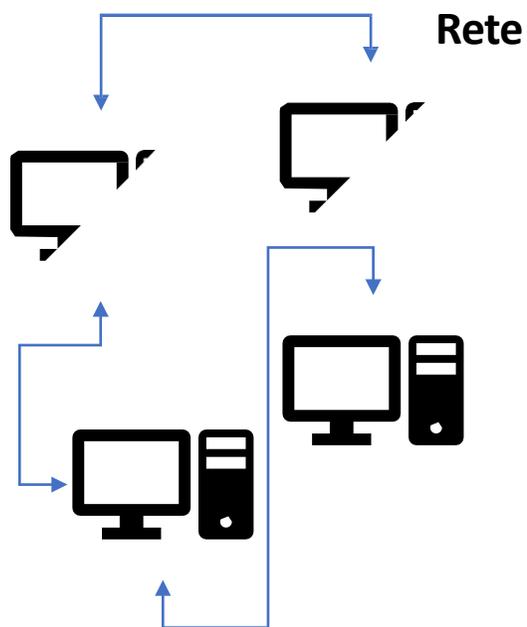
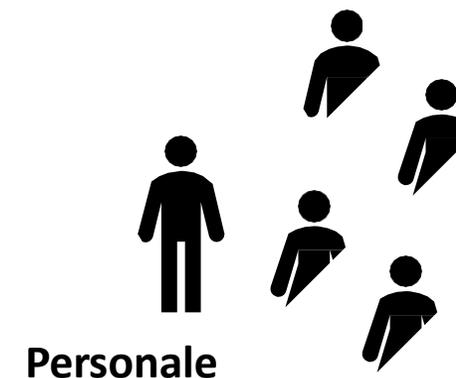
probabilità che una vulnerabilità sia individuata da una minaccia e utilizzata a scopo malevolo

# Cosa si intende per «superficie di attacco»

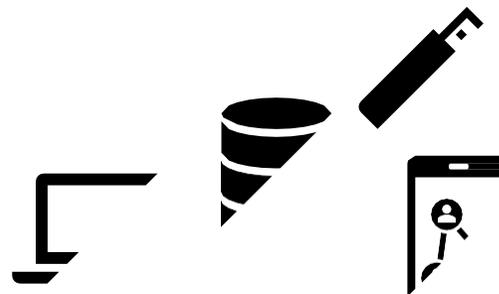


## Superficie di attacco (Attack surface)

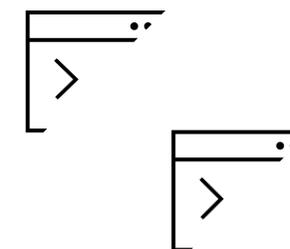
Porzione di un sistema informatico (in senso generale) esposta ad accesso o modifica non autorizzata.



Accesso fisico a dispositivi



Software



# La sicurezza dipende da....



**La sicurezza assoluta non esiste  
ma dipende da vari fattori**



**Misure di protezione  
(tecnologiche, procedurali,  
infrastrutturali, ...)**

**Importanza dei  
dati e dell'utente**

**Rapporto tra costo-  
tempo e benefici**



# Quando un sistema informatico è sicuro....



Un sistema informatico si definisce sicuro se salvaguarda i requisiti di:

- **Disponibilità (Availability)**: accessibilità continua ai sistemi e ai servizi
- **Riservatezza (Confidentiality)**: accesso autorizzato alle informazioni e ai dati
- **Integrità (Integrity)**: i dati non sono modificabili (cancellabili) da soggetti non autorizzati

# Chi sono gli hacker



## Hacker (Cracker tende a generare effetti dannosi)

- Script Kiddie
- Hactivist >>> ideologia politico-religiosa
- Industrial Spy
- Cyber Terrorist (danni fisici)
- E-Mugger
- Heavyweight Ninja
- Cyber soldier (reparti militari, stati)
- Ethical hacker

### Attaccante (Hacker):

persona (software) che cerca di acquisire informazioni o di accedere in maniera non autorizzata a un servizio/sistema.

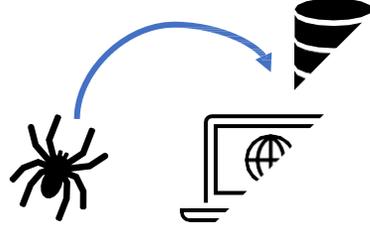
# Tipologie di cyber attacchi



**Malware** 

**Social Hacking** 

**DOS/DDOS** 

**SQL Injection** 

**Brute force** 

**....?!?**



# Tipologie di cyber attacchi: malware



Le minacce più sofisticate contro i computer e le reti di computer sono senza dubbio costituite dal **software doloso (malevolo)**, *malware*.

**Malware**: un programma che è inserito in maniera nascosta all'interno di un altro oppure indipendente, creato con l'intento di distruggere dei dati, lanciare programmi dannosi o compromettere la segretezza, l'integrità o la disponibilità di dati e applicazioni della vittima dell'attacco.

Esistono sostanzialmente due categorie di malware:

- richiede un programma ospite (frammenti di codice in un programma applicativo o di sistema)
- opera in modo indipendente (programmi completi eseguiti dal sistema operativo come *worm*).

I malware possono anche essere distinti diversamente:

- Software che si replicano ovvero quando attivati generano più copie di se stessi (*virus e worm*)
- Software che non si replicano (*trojan*)



# Tipologie di cyber attacchi: alcuni malware



- **Exploit:** Codice specifico che sfrutta una particolare vulnerabilità di un programma
- **Trojan:** programma che appare avere una certa utilità (e.g. un gioco) ma ha nascosto al suo interno un codice doloso che una volta richiamato svolge azioni dannose
- **Backdoor:** punto di accesso o meccanismo segreto in un programma che permette di entrare in un sistema evitando le normali procedure di sicurezza
- **Keylogger:** programma che inserito in un sistema compromesso cattura i caratteri immessi da tastiera
- **Ransomware:** malware che cifra i dati dell'utente e richiede un pagamento per rivelare la chiave di decifratura per recuperare i file
- .....??!???

# Tipologie di cyber attacchi: social hacking



## Social hacking (social engineering attacks):

Tecnica che fa leva sulla psicologia umana e usa l'inganno (amicizia, solidarietà, fornitura dispositivi, ecc.) per ottenere dalla vittima dati confidenziali come una password, il codice fiscale, ecc..

1. **Footprinting** (analisi/ricerca dati disponibili): profili social, account, numeri di telefono, nominativi, ecc.
2. **Contatto**: creazione del rapporto con la vittima
3. **Manipolazione psicologica**: azione di recupero informazioni
4. **Cancellazione tracce**



Phishing



# Il Phishing



## Phishing:

Truffa perpetrata attraverso l'invio di e-mail per convincere la vittima a compiere un'azione (click) o rivelare un segreto

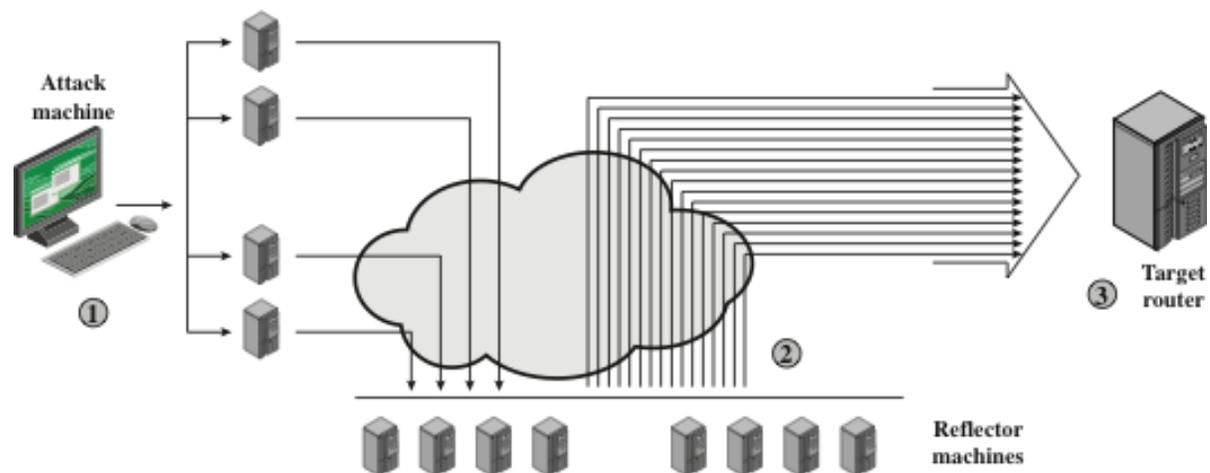
- Spray Phishing: si tratta di un'azione non mirata
- Spear Phishing: azione mirata ad una vittima (utente/azienda)
- Whaling: phishing orientato ai vertici aziendali (e.g. CEO)
- Vishing: voice phishing, truffa via telefonica
- Smishing: SMS phishing

# Tipologie di attacchi: DOS (DDOS)



## DOS (DDOS): (Distributed) Denial Of Service

- Attacco volto ad indurre un malfunzionamento su un sistema o su un server esaurendone le risorse computazionali o di banda
- Rende un sistema inaccessibile inondando i server, la rete e i terminali con traffico inutile
- Se l'attacco proviene da un unico computer si parla di *DoS*, quando invece si usano un gran numero di host compromessi si parla di *DDoS*

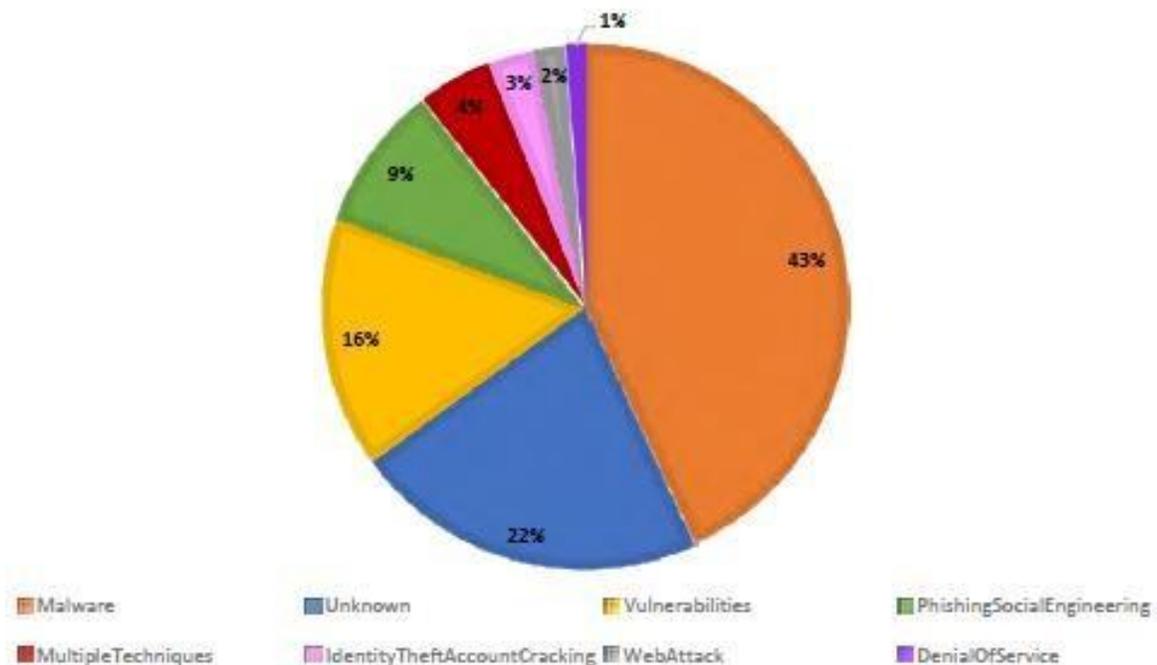


# Panoramica sulle tipologie di cyber attacchi



Panoramica dei cyber attacchi più significativi del 2018-2020 e del primo semestre 2021

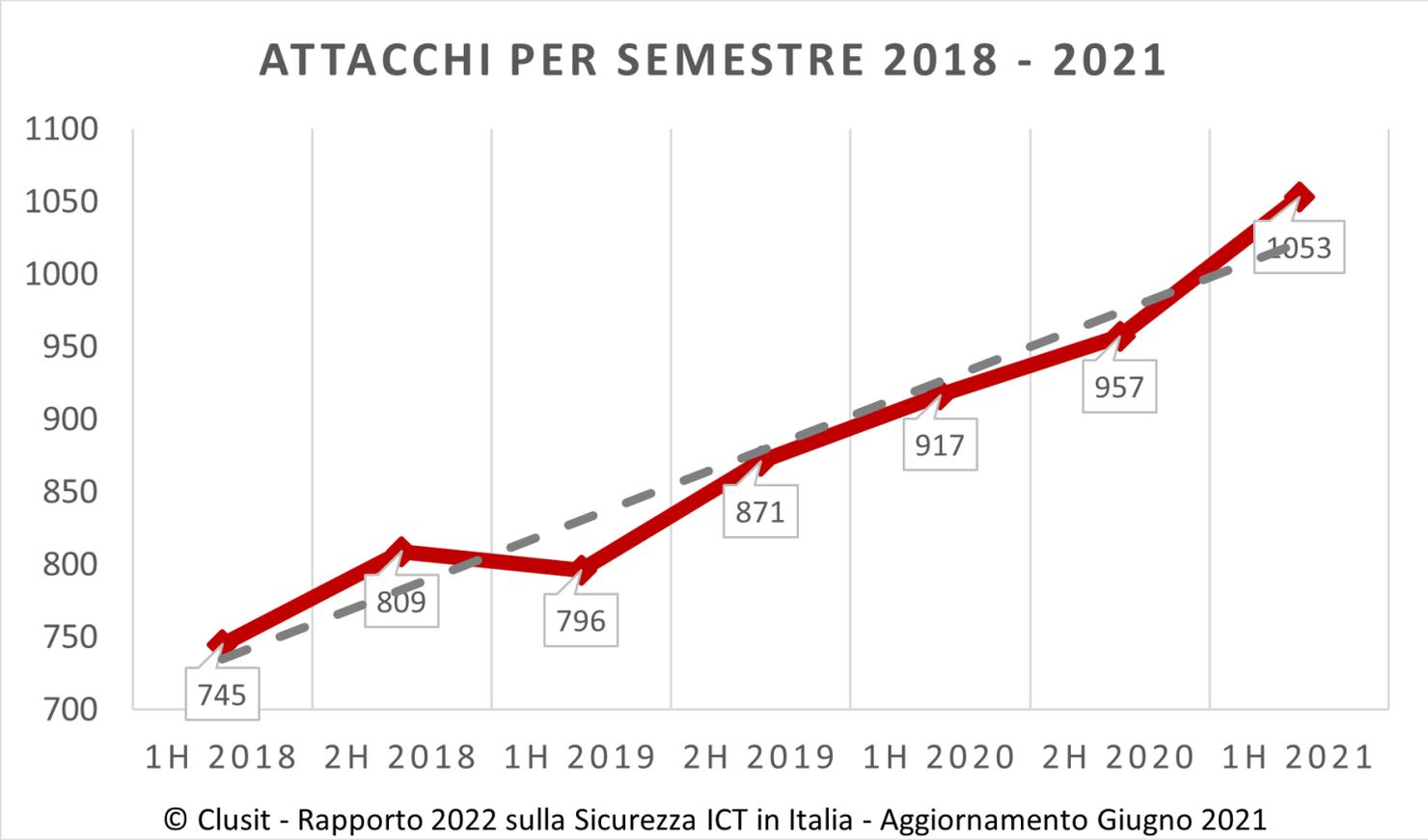
Tecniche di attacco - 1H 2021



© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia - aggiornamento giugno 2021



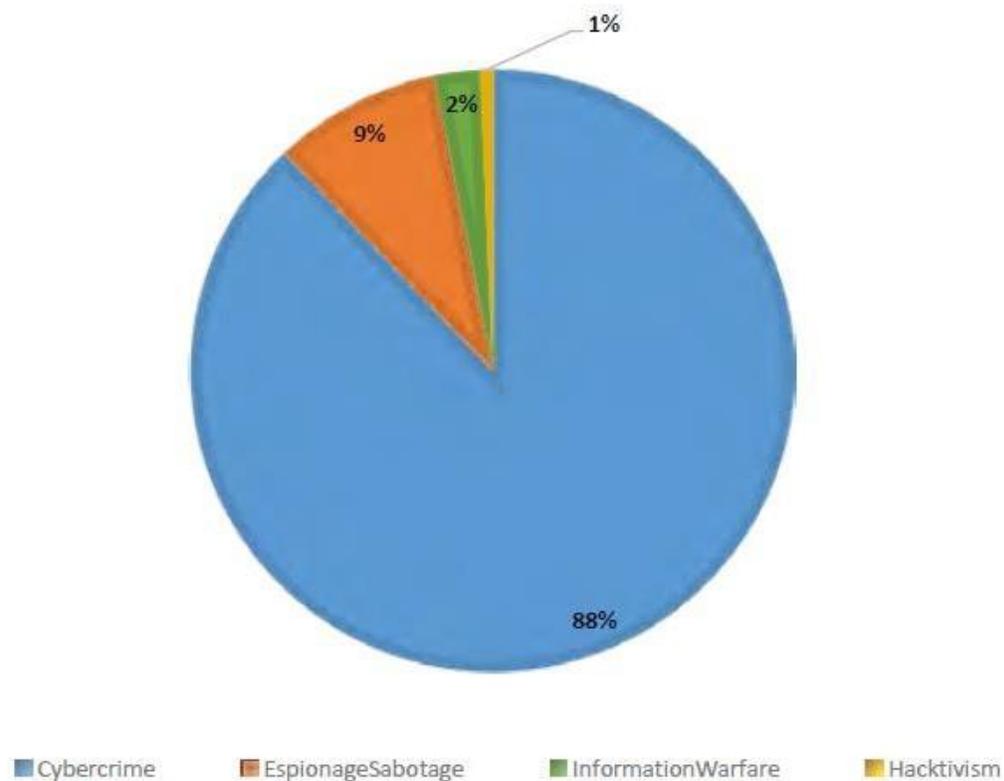
# Trend dei cyber attacchi



# Tipologie dei cyber attaccanti



Tipologia e distribuzione attaccanti 1H 2021



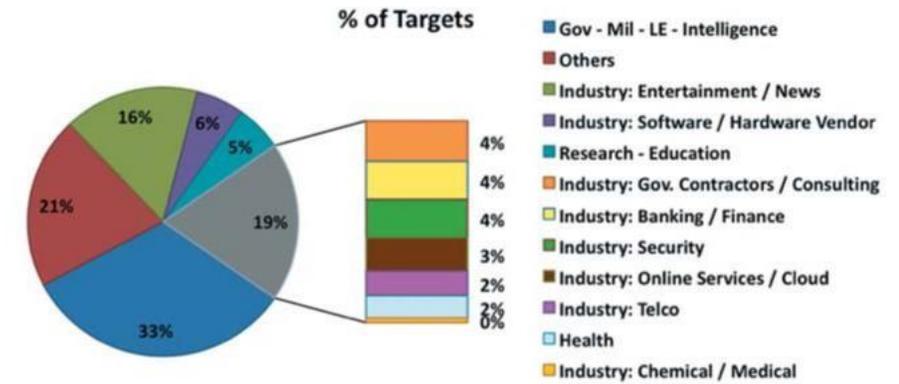
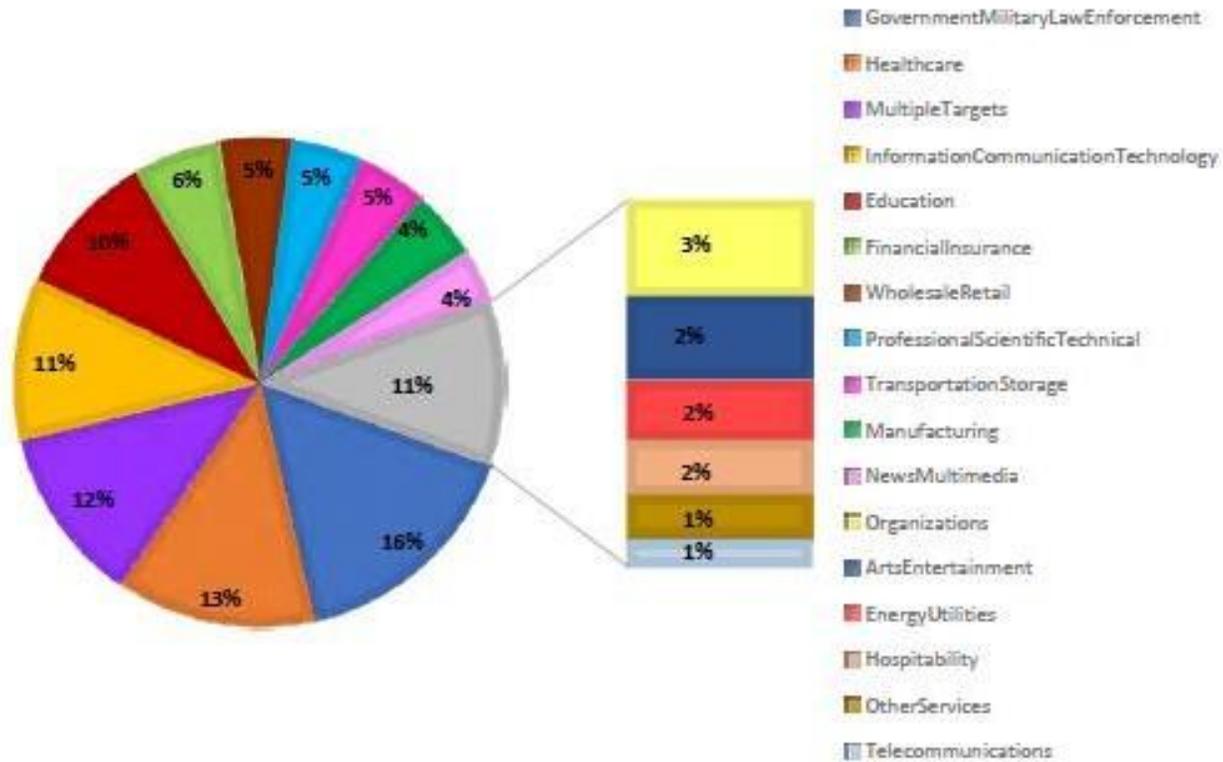
© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia - aggiornamento giugno 2021



# Vittime di cyber attacchi 2012 vs 2021



Distribuzione delle vittime - 1H 2021



Rapporto Clusit 2012

© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia - aggiornamento giugno 2021



# Cyber risk management



## MINACCIA

Cosa potrebbe succedere?

Ad esempio un attacco cyber portato da una comunità di hacker.



## PROBABILITÀ

Quanto è probabile che succeda?

La probabilità coincide con il livello di esposizione all'attacco (fate benchmark, derivante da analisi statistica, su attacchi analoghi verificatisi in passato).



## VULNERABILITÀ

Quanto sono esposto e/o in grado di difendermi?

La vulnerabilità è la parziale realizzazione o l'assenza di misure di sicurezza atte a prevenire/contenere/impedire l'attacco.



## IMPATTO

Che tipo di danni provocherebbe?

L'impatto è il danno derivante dalla compromissione della riservatezza, integrità e disponibilità dell'informazione del sistema informativo, di un applicativo, un servizio o una piattaforma



## CONTROMISURA

Come posso proteggermi da quel che potrebbe succedere?

Con metodologie e iniziative di prevenzione e gestione del rischio dell'oggetto di attacco.



[sicurezzait.gov.it](https://sicurezzait.gov.it)



# Rischi legati al personale aziendale (1/2)



**Molti dei rischi sono legati ai comportamenti e alle azioni del personale aziendale**

- Uso di dispositivi personali in attività di lavoro
  - Lavoro da remoto (Covid19)
  - BYOD (Bring Your Own Device)
- Smart working e DAD/DDI
  - Configurazioni di accesso non controllate
  - Accesso su rete (server) aziendale (VPN)
  - E-mail e cloud aziendale

# Rischi legati al personale aziendale (2/2)



**Molti dei rischi sono legati ai comportamenti e alle azioni del personale aziendale**

- Personale malevolo interno o ex-dipendenti
  - Aziende competitor
  - Comportamenti rischiosi non volontari
- Informazioni personali sui social
  - Password, nickname, domande segrete per recupero credenziali
- Esposizione a social hacking

# Soluzioni di difesa



Esistono vari tipi di soluzioni di difesa che possono essere messi in campo

- Difesa Passiva (*Cyber Threat Intelligence*)
  - Analisi delle minacce
  - Conoscenze, informazione e aggiornamento
  - Esperienza
  - Capacità di limitare/risolvere possibili attacchi
- Difesa Attiva (*Esperto di Cybersecurity*)
  - Implementazione di meccanismi informatici (firewall, antivirus, crittografia...)
  - Strumenti per il controllo degli accessi
  - Analisi continua degli indicatori di comportamento (download file, variazione permessi, tentativi di accesso)
- Difesa Pro-Attiva (*Preventiva*)
  - Analisi delle vulnerabilità e Penetration test
  - Ethical hacking
  - Sandbox, Honeypot

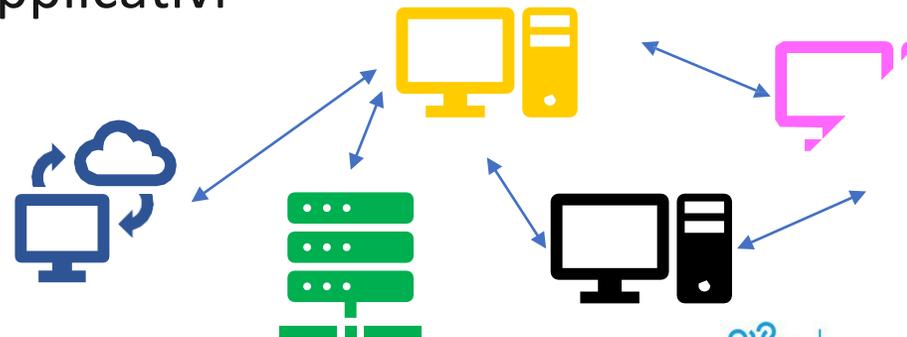


# Alcune....buone pratiche tecniche (1/2)



Le soluzioni di cybersecurity sono molteplici e devono perciò essere valutate e implementate in relazione alle specifiche esigenze di un'azienda.

- Consapevolezza e conoscenza delle minacce informatiche
- Corretta gestione password: non semplici e aggiornate
- Ridondanza dati, server e applicativi

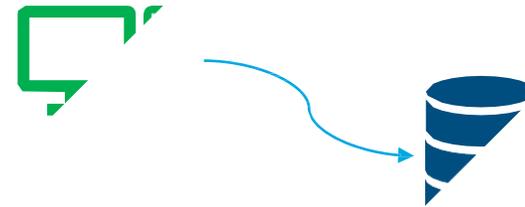


# Alcune....buone pratiche tecniche (2/2)



Le soluzioni di cybersecurity sono molteplici e devono perciò essere valutate e implementate in relazione alle specifiche esigenze di un'azienda.

- Back-up periodici e automatici



- Aggiornamento programmi, tool e sistemi operativi

- Penetration test (periodico)



- Accesso a dati strategici tramite MFA (Multi-Factor Authentication)

# Alcune.....buone pratiche aziendali



- Dotarsi di un ICT security manager/team
  - Interno (esterno?)
- Formare e responsabilizzare il personale sui rischi
- Ridondanza ruoli strategici per il personale adibito alla sicurezza informatica
- Gestione adeguata delle conoscenze segrete (accessi, credenziali, ecc.)
- Revisione periodica
  - Profili del personale
  - Log accessi
- Approccio Zero-Trust
  - Limitare uso dispositivi personali
  - Verificare autorizzazioni

# Conclusioni



- Cybersecurity: definizioni e terminologia
- Hacker e tipologie di attacchi
- Analisi dei rischi
- Soluzioni di difesa
- Buone pratiche aziendali



**Grazie!!**

**[roberto.caldelli@unimercatorum.it](mailto:roberto.caldelli@unimercatorum.it)**

