L’Agenzia per la Cybersicurezza Nazionale e la minaccia cibernetica

Marco Valerio Cervellini

Viterbo, 4 ottobre 2024

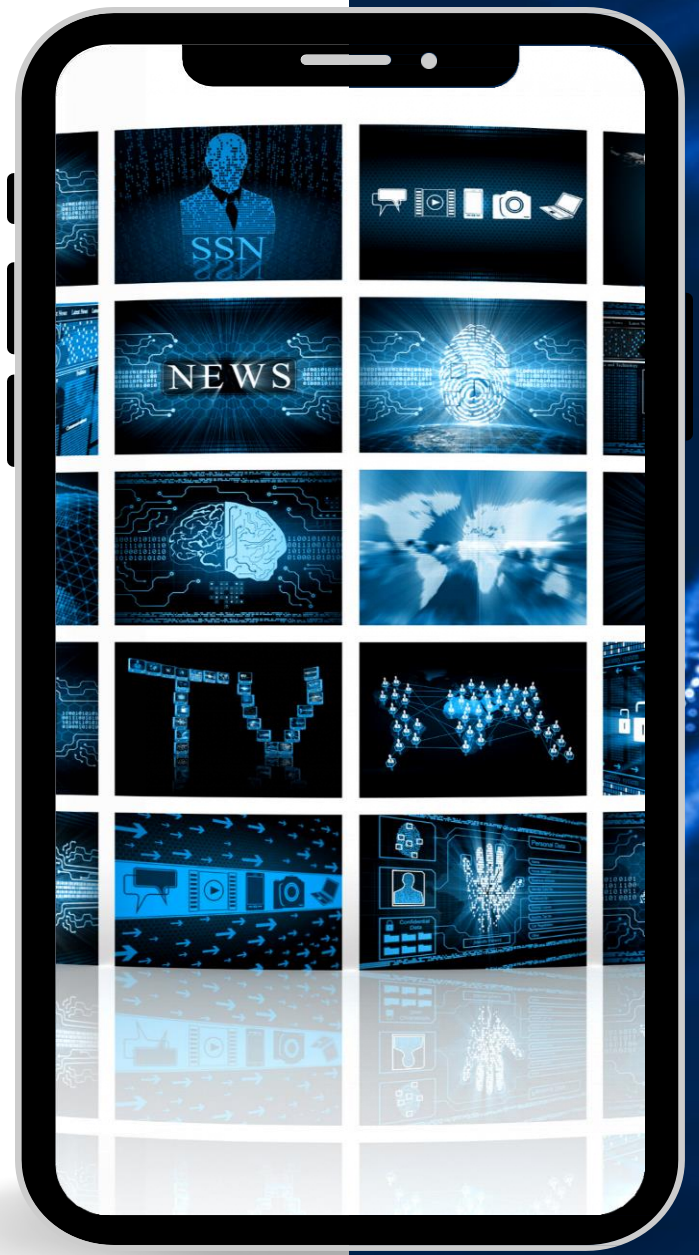
Dati in crescita continua

Fonte: Global Digital Report 2024

8,08 miliardi di persone!

5,61 miliardi di persone usano smartphone (69,4%).

5,04 miliardi di persone utenti attivi sui Social Media (62,3%)



Più risorse ma più confini

OPPORTUNITÀ

Crescita economica, sociale e culturale

MINACCE

Più diffuse, più diversificate, più sofisticate

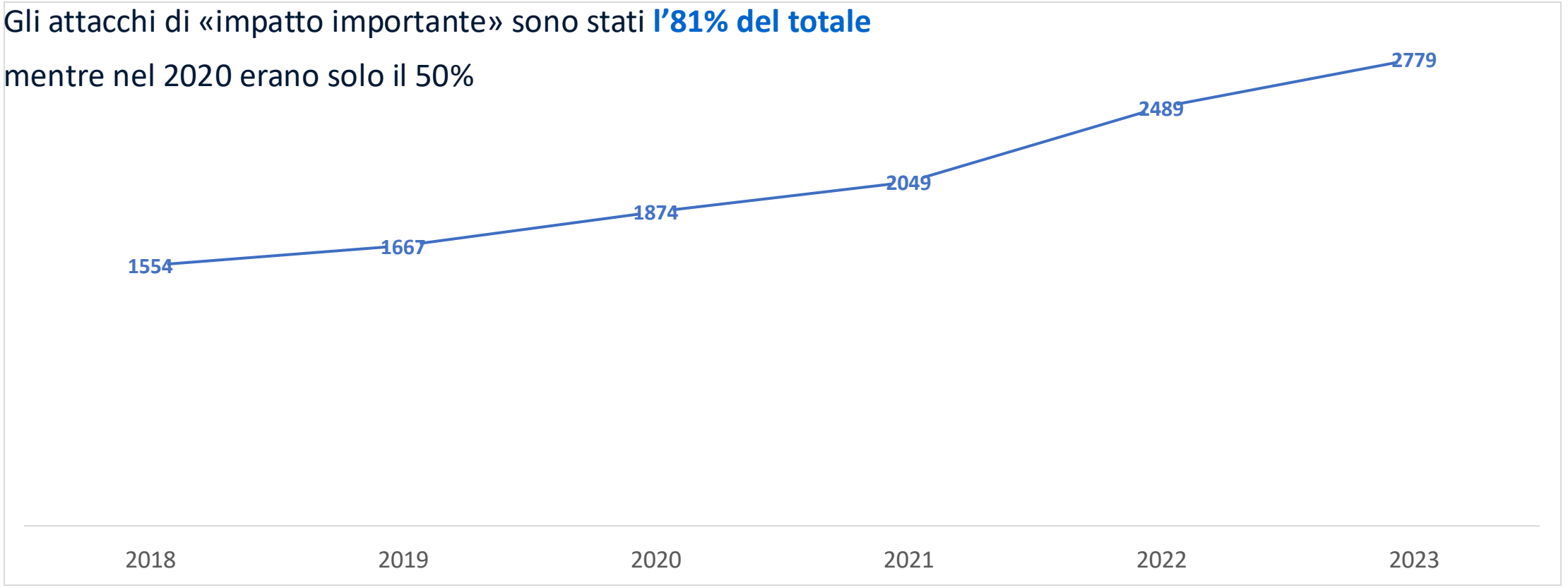
La situazione mondiale

DATI STATISTICI GLOBALI 2023 - Fonte Clusit – Rapporto 2024

Nel 2023 il trend degli attacchi si conferma in forte crescita (+12%).

Gli attacchi di «impatto importante» sono stati **l'81% del totale**

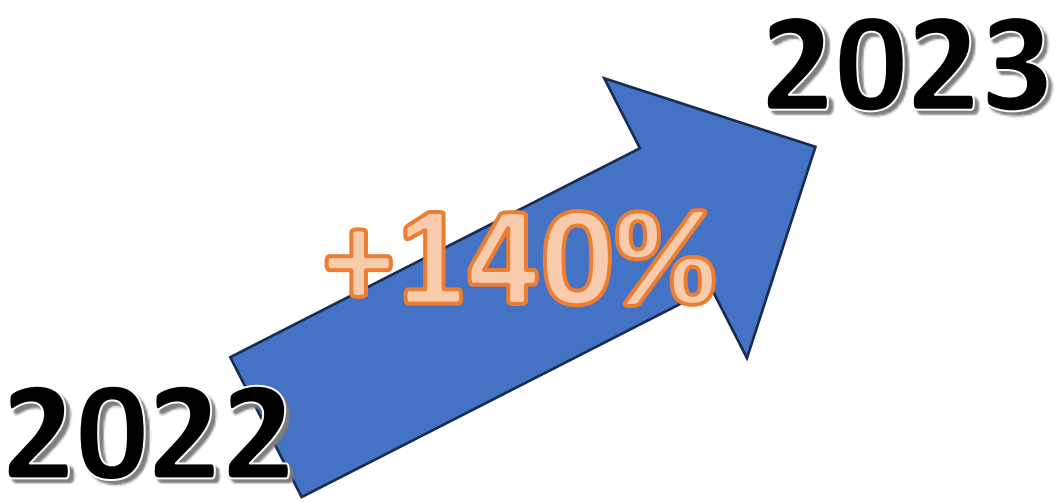
mentre nel 2020 erano solo il 50%



La situazione italiana

DATI STATISTICI ITALIANI 2023 - **Fonte ACN**

Secondo le rilevazioni di ANC in Italia abbiamo avuto nel 2023 rispetto al 2022 un aumento del 140% degli “incidenti”, cioè eventi cyber con impatto confermato dalla vittima.



+625%

Qualche spunto di analisi sui dati di ACN

DDOS

Phishing

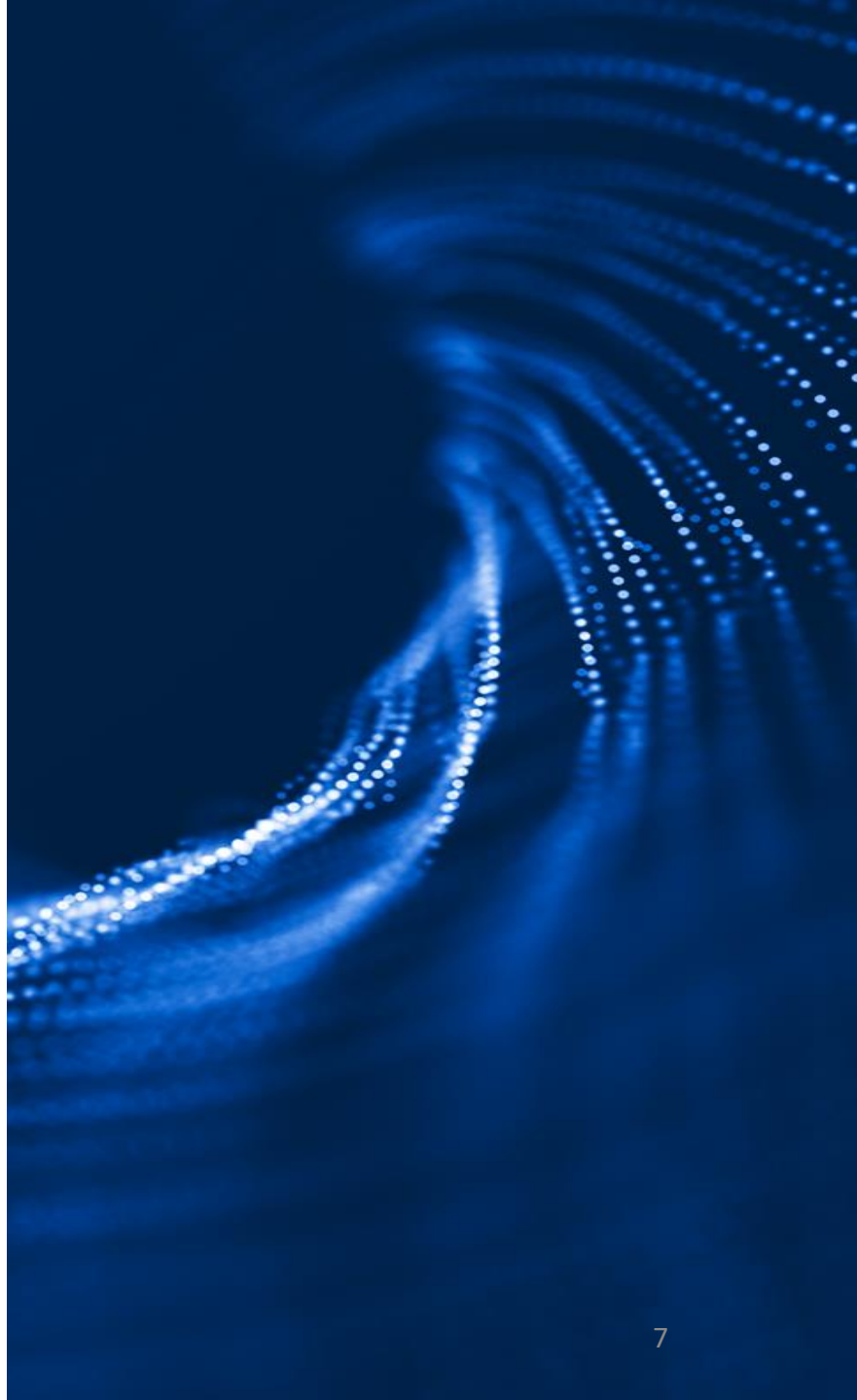
Sfruttamento delle vulnerabilità

Conseguenze meno gravi?

E il 2024?

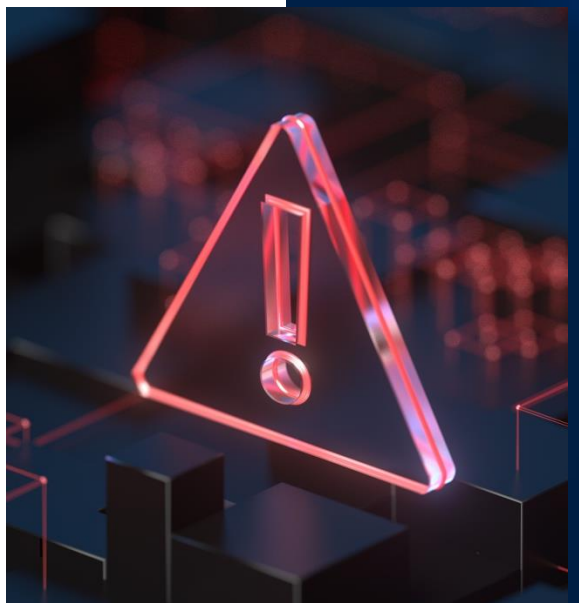
Attacchi più diffusi

- **Phishing:** Gli attaccanti inviano email o messaggi fraudolenti che sembrano provenire da fonti legittime al fine di ottenere informazioni personali o finanziarie.
- **Malware:** Software dannoso progettato per danneggiare o infiltrarsi nei sistemi informatici. Questo include virus, worm, trojan e **ransomware**.
- **Attacchi di DDoS** (Distributed Denial of Service): Gli attaccanti sovraccaricano i server o le reti di destinazione con un enorme volume di traffico, rendendoli inaccessibili agli utenti legittimi.
- **Attacchi di Iniezione di Codice**: Gli attaccanti inseriscono codice dannoso in applicazioni web o database per ottenere accesso non autorizzato o compromettere i dati.
- **Attacchi di Password Cracking**: Gli attaccanti cercano di indovinare o decifrare le password degli utenti per accedere a sistemi o account protetti.
- **Attacchi di Phishing a Ingegneria Sociale**: Gli attaccanti manipolano le persone attraverso tecniche di persuasione psicologica per ottenere informazioni riservate o l'accesso ai sistemi.
- **Attacchi Zero-Day**: Gli attaccanti sfruttano vulnerabilità di sicurezza non ancora note o non corrette nei software per ottenere l'accesso non autorizzato ai sistemi.
- **Man-in-the-Middle** (MitM): Gli attaccanti intercettano e manipolano la comunicazione tra due parti legittime per rubare informazioni o compromettere la sicurezza.
- **Attacchi di Smishing e Vishing**: Simili al phishing, ma condotti attraverso SMS (smishing) o chiamate telefoniche (vishing).
- **Attacchi a dispositivi IoT** (Internet of Things): Gli attaccanti prendono di mira dispositivi IoT non sicuri per compromettere la rete o raccogliere informazioni sensibili.



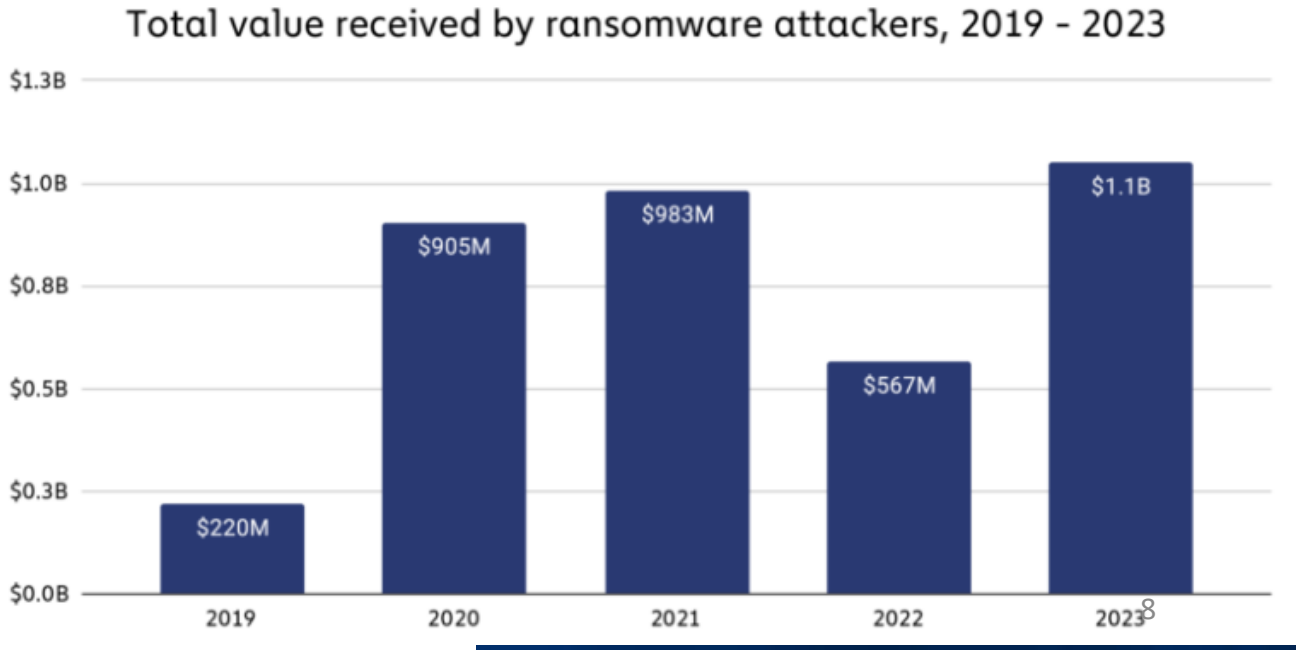
Ransomware: attacco globale ai sistemi informatici

DATI STATISTICI GLOBALI 2023 - Chainanalisys



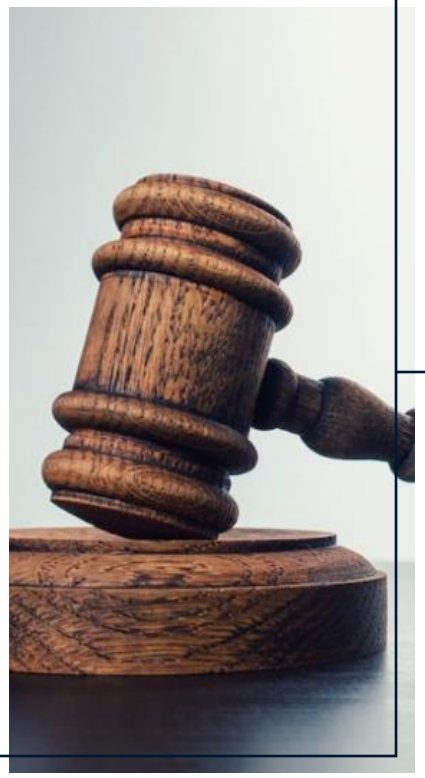
Nel 2023 gli attacchi di tipo **Ransomware** sono tornati a crescere dopo l'anomalo calo del 2022.

I pagamenti dei riscatti dovuti a ransomware nel 2023 hanno superato la soglia del miliardo di dollari (1,1 B$), la cifra più alta mai osservata.

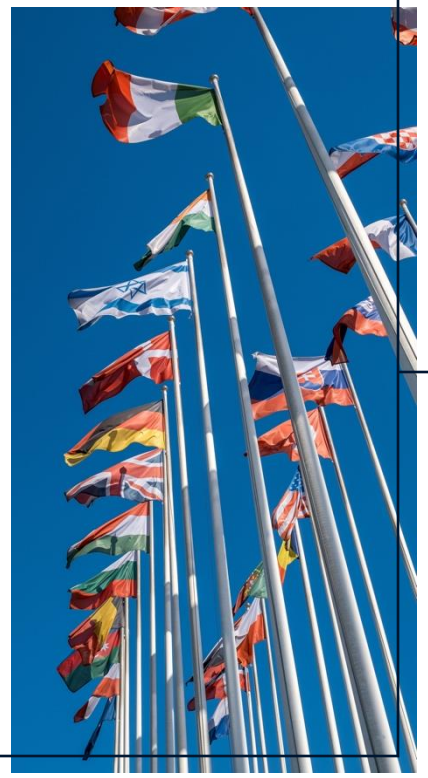


Perché c’è un costante aumento degli attacchi?

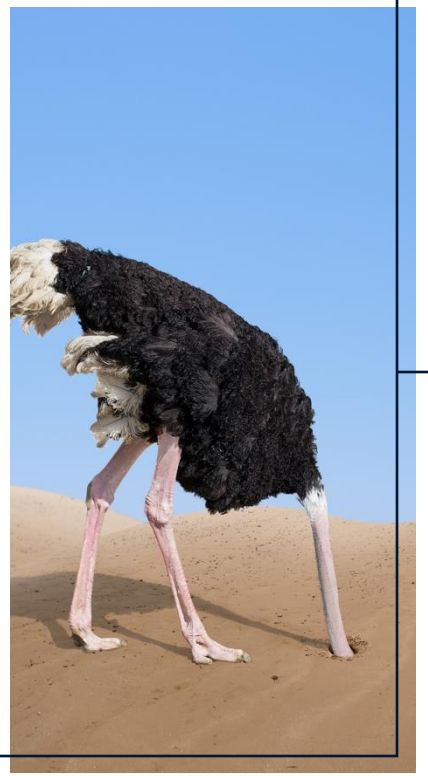
Anonimato in rete



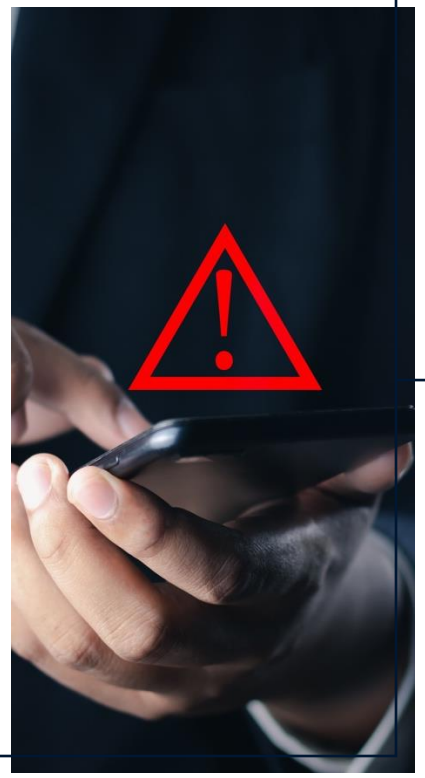
Strumenti normativi inidonei



Difficoltà di cooperazione internazionale

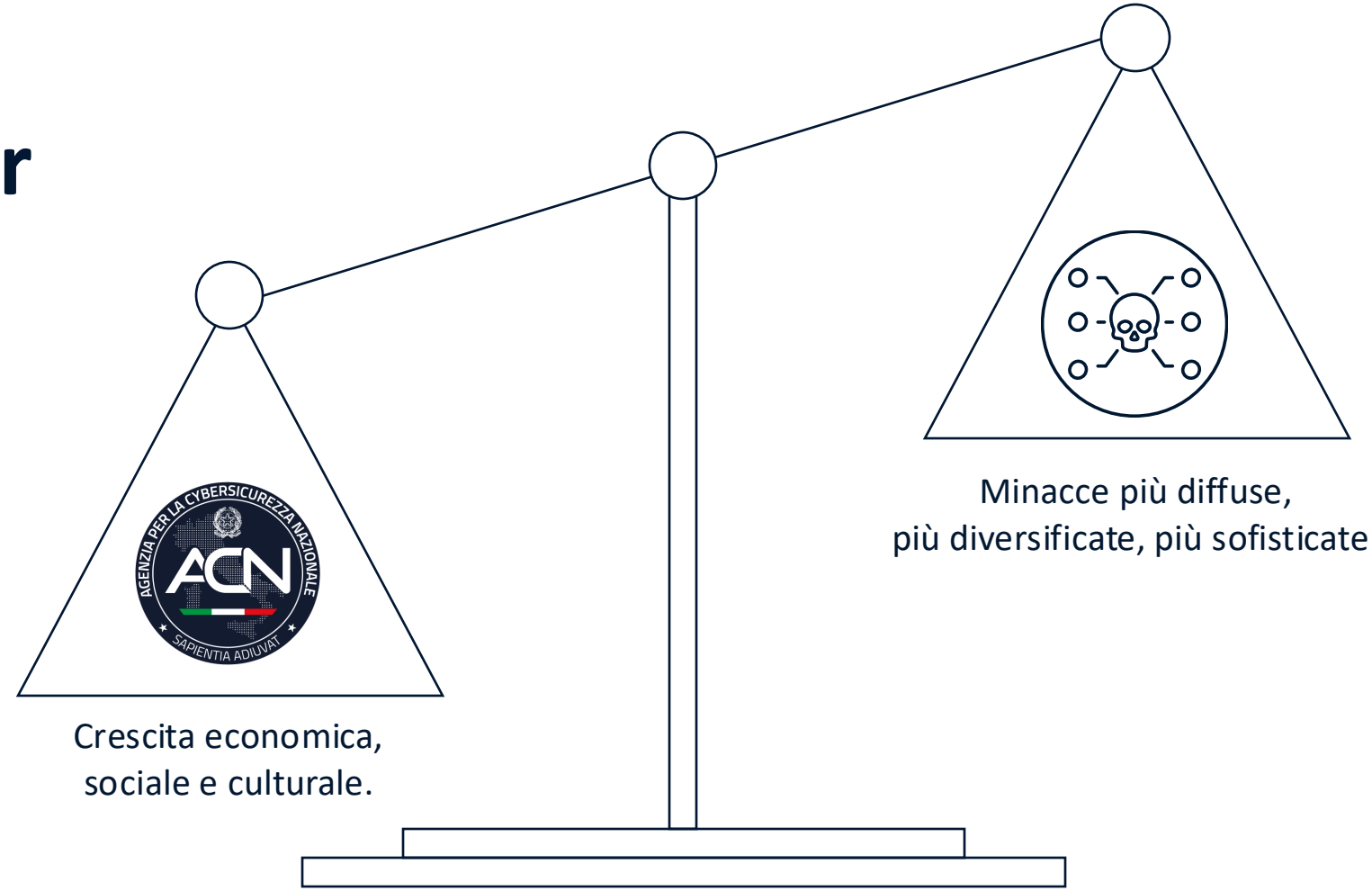


Mancata percezione del problema



Sicurezza informatica inadeguata

Come facciamo a far pendere la bilancia dal lato giusto?



Crescita economica,
sociale e culturale.

Minacce più diffuse,
più diversificate, più sofisticate.

Per liberare il potenziale dell'innovazione tecnologica servono:

+ STRUMENTI
Normativi, di policy e tecnologici.

+ CAPACITÀ

+ RISORSE

+ ISTITUZIONI

L'AGENZIA PER LA CYBERSICUREZZA NAZIONALE

ARCHITETTURA NAZIONALE DI CYBERSICUREZZA

L’ACN ha il compito di implementare la cyber-resilienza del sistema-paese

La **cyber-resilienza** è la capacità di un’organizzazione di gestire al meglio la propria attività durante una violazione dei dati o un cyber attacco, in modo da garantire **l’availability** dell’intero sistema ICT.

Ma è anche intesa come misura preventiva e proattiva: tutte quelle attività che possono evitare un attacco prima che avvenga.

Di cosa ci occupiamo

PREVENZIONE E MITIGAZIONE

Supporta i soggetti pubblici e privati nazionali, che esercitano funzioni ed erogano servizi essenziali, nella prevenzione e mitigazione degli incidenti, nonché ai fini del ripristino dei sistemi.

CERTIFICAZIONE E VIGILANZA

Valuta prodotti e servizi informatici e conduce attività ispettive e di verifica per gli adempimenti normativi nel campo della cybersicurezza.

AUTONOMIA STRATEGICA

Persegue l'autonomia strategica nazionale ed europea nel settore del digitale, in sinergia con il sistema produttivo e con il mondo della ricerca.

CULTURA CYBER

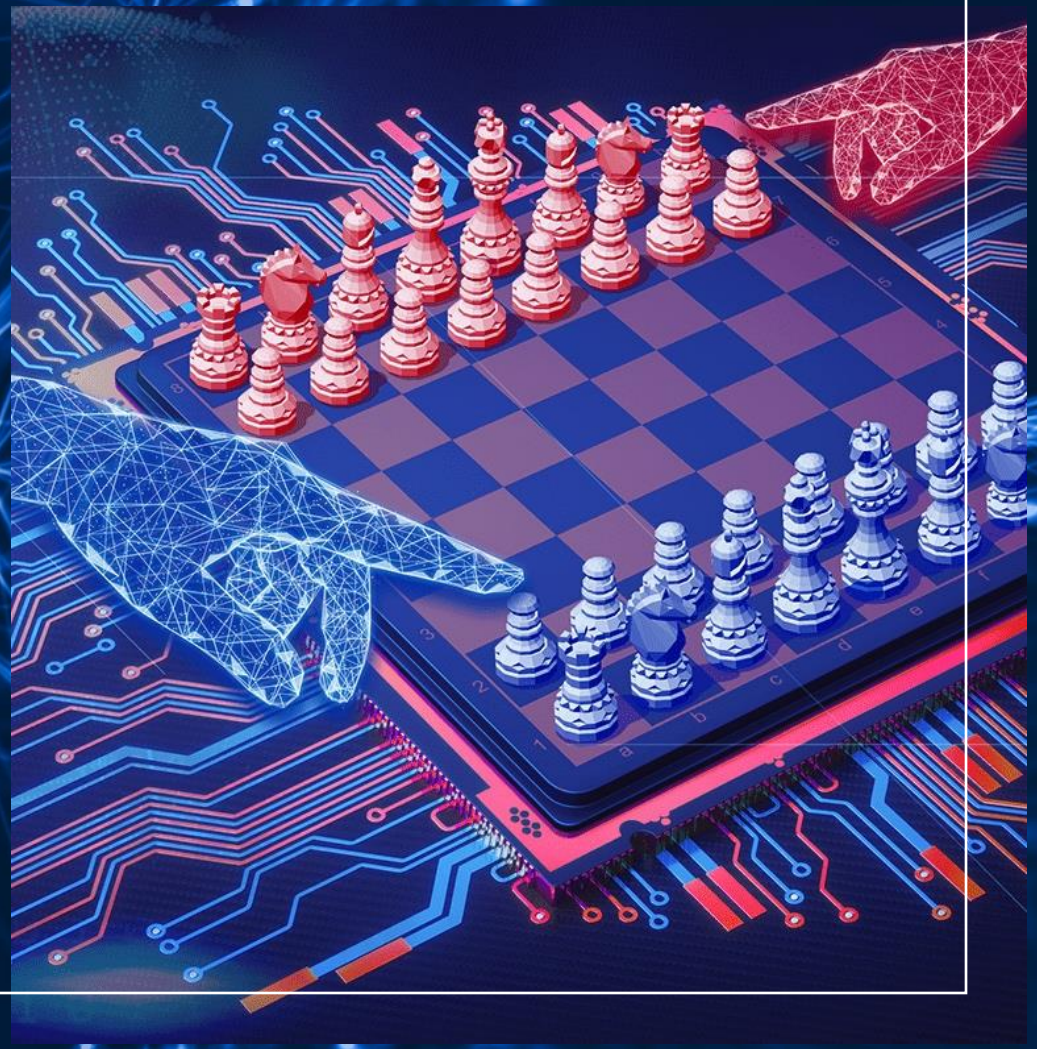
Favorisce percorsi formativi per lo sviluppo della forza lavoro di settore e promuove campagne di sensibilizzazione e diffusione della cultura della cybersicurezza.

PREVENZIONE E MITIGAZIONE DEGLI INCIDENTI (CSIRT Italia)

- Individuazione dei soggetti critici per il sistema Paese
- Gestione degli incidenti di sicurezza critici e di potenziali crisi che colpiscano i soggetti individuati.
- Monitoraggio volto alla raccolta di informazioni utili a rilevare anomalie che possano prevenire e/o individuare attacchi cibernetici.
- Diffusione selezionata di informazioni in merito a minacce e vulnerabilità di sicurezza che possano coinvolgere il perimetro dei soggetti.
- Gestione del rischio e della crisi a rilevanza sistemica per il sistema Paese.

L'AUTONOMIA STRATEGICA IN AMBITO TECNOLOGICO

- La sovranità tecnologica ha un ruolo cruciale per l'indipendenza economica e l'autonomia strategica dell'Italia e dell'Unione europea. L'abilità di generare conoscenza tecnologica e scientifica autonomamente o di utilizzare capacità tecnologiche sviluppate altrove, attraverso l'attivazione di partnership, è di vitale importanza per il sistema Paese.
- L'Agenzia attraverso la strategia nazionale di Cybersicurezza e la gestione di fondi europei e nazionali collabora al finanziamento di progetti e start up volti al miglioramento della postura cyber delle pubbliche amministrazioni e delle aziende.
- Investe in programmi di ricerca e sviluppo da svolgere in collaborazione con l'accademia e altre istituzioni di ricerca.



CERTIFICAZIONE E VIGILANZA

- Esercita le funzioni di Autorità Nazionale di Certificazione della Cybersicurezza (NCCA), ai sensi del Cybersecurity Act.
- Verifica la sicurezza e l'assenza di vulnerabilità note in beni, sistemi e servizi ICT, con l'obiettivo di innalzare il livello di cybersicurezza e di resilienza delle infrastrutture da cui dipendono le funzioni e i servizi essenziali del Paese.
- Gestisce lo schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione.
- Svolge tutte le attività di verifica tecnico documentale e ispezione concernenti gli adempimenti di cybersicurezza attribuiti all'Agenzia dalla normativa vigente.

CONSAPEVOLEZZA E COMPETENZA

- Diffondere conoscenze e competenze nella gestione del rischio cyber alle istituzioni e ai vertici aziendali.
- Promozione dell'awareness e della cultura cyber attraverso attività e progetti di awareness, formazione e educazione.
- Formazione diretta a moltiplicare i professionisti del settore per I quali c'è una ernorme carenza, sia a livello mondiale che a livello italiano.
- Ancora putroppo forte gender-gap.

acn.gov.it