Ordine dei Dottori Commercialisti e degli Esperti Contabili di Torino

Fondazione Piero Piccatti e Aldo Milanese

ORDINE DOTTORI COMMERCIALISTI ED ESPERTI CONTABILI TORINO

CYBERSECURITY
una priorità per tutti

26 Marzo 2025

Matteo Malabaila

Ordine dei Dottori Commercialisti e degli Esperti Contabili di Torino

Fondazione Piero Piccatti e Aldo Milanese

ORDINE DOTTORI COMMERCIALISTI ED ESPERTI CONTABILI TORINO

Ci sono solo due tipi di aziende: quelle che sono state hackerate e quelle che non sanno di esserlo state."

— John Chambers, ex CEO di Cisco

PERCHE' SIAMO QUI OGGI

La cybersecurity non è solo un tema tecnico, ma è una responsabilità condivisa

Come professionisti siamo esposti su due fronti

- Personalmente
- Professionalmente

PERCHÉ I COMMERCIALISTI SONO A RISCHIO

- Accesso a dati fiscali, bancari e personali
- Sistema di fatturazione elettronica
- PEC, SPID, firma digitale

LA CYBERSECURITY NON È SOLO TECNOLOGIA, MA CULTURA

La vulnerabilità più grande: il fattore umano

Secondo numerosi studi, infatti, circa il 90% degli incidenti informatici è causato da errore umano o disattenzione. Un click distratto su un link sbagliato può causare danni enormi a uno studio, vanificando gli investimenti tecnologici fatti

L'importanza della sensibilizzazione e formazione interna

CYBERSECURITY: ALCUNI CONCETTI BASE

- **Cyber Security**

comprende l'insieme di **pratiche, tecnologie e processi** finalizzati a **proteggere sistemi informatici**, reti, dispositivi e dati da **attacchi esterni e interni**, danni accidentali e accessi non autorizzati, danni o furti.

L'obiettivo principale della cyber security è garantire la **riservatezza, integrità e disponibilità** delle informazioni, spesso abbreviato come **CIA (Confidentiality, Integrity, Availability).**

Si estende su vari livelli, includendo la protezione fisica e logica dei sistemi, la formazione del personale e la creazione di strategie preventive. La cyber security è una disciplina in continua evoluzione che mira a contrastare le minacce emergenti nel panorama digitale globale.

CYBERSECURITY: ALCUNI CONCETTI BASE

- **Malware** = software malevolo
- **Ransomware** = blocco dei dati in cambio di riscatto
- **Phishing** = inganno via email o sms
- **Data breach** = perdita o furto di dati

CYBERSECURITY: ALCUNI CONCETTI BASE

Malware

è un **software dannoso** creato con l'intento di **infiltrarsi, danneggiare o disabilitare sistemi informatic**i, spesso senza che l'utente se ne accorga. Può diffondersi attraverso e-mail, download, o exploit di vulnerabilità di sistema.

I malware possono variare in complessità e gravità, dai semplici virus ai più sofisticati trojan e ransomware. I malware possono variare in complessità e gravità, dai semplici virus ai più sofisticati trojan e ransomware.

CYBERSECURITY: ALCUNI CONCETTI BASE

Ransomware

Un virus che si diffonde tramite allegati e-mail infetti, infettando altri file di sistema e compromettendo le prestazioni complessive del computer.

Malware	Replica Autonoma	Necessita di Intervento Utente	Scopo Principale
Virus	No	Sì	Danneggiare file/sistema
Worm	Sì	No	Diffondersi rapidamente, bloccare reti
Trojan	No	Sì (inganno)	Creare accessi nascosti, rubare dati
Spyware	No	No	Spiare e raccogliere informazioni

CYBERSECURITY: ALCUNI CONCETTI BASE

Phishing

è una tecnica di ingegneria sociale che sfrutta l'inganno per ottenere informazioni sensibili come credenziali di accesso o dati finanziari. Gli attaccanti si fingono entità affidabili per indurre le vittime a rivelare informazioni personali.

Tipo di Attacco	Canale di Attacco	Esempio Comuni
Phishing	E-mail	E-mail da "banca" con link fraudolenti.
Smishing	SMS/Messaggi	SMS con link di "corriere" o "premio vinto".
Vishing	Telefonata	Chiamata di falso operatore bancario.

CYBERSECURITY: ALCUNI CONCETTI BASE

Ordine dei Dottori Commercialisti e degli Esperti Contabili di Torino

Fondazione Piero Piccatti e Aldo Milanese
ORDINE DOTTORI COMMERCIALISTI ED ESPERTI CONTABILI TORINO

Data breach

è una violazione della sicurezza in cui **dati sensibili, riservati o protetti vengono esposti, rubati o consultati da persone non autorizzate**. I dati compromessi possono includere **informazioni personali, credenziali di accesso, dati finanziari o proprietà intellettuale**.

CYBERSICURITY IN NUMERI

Geografia delle vittime 2024

Continente Americano

Continente Europeo

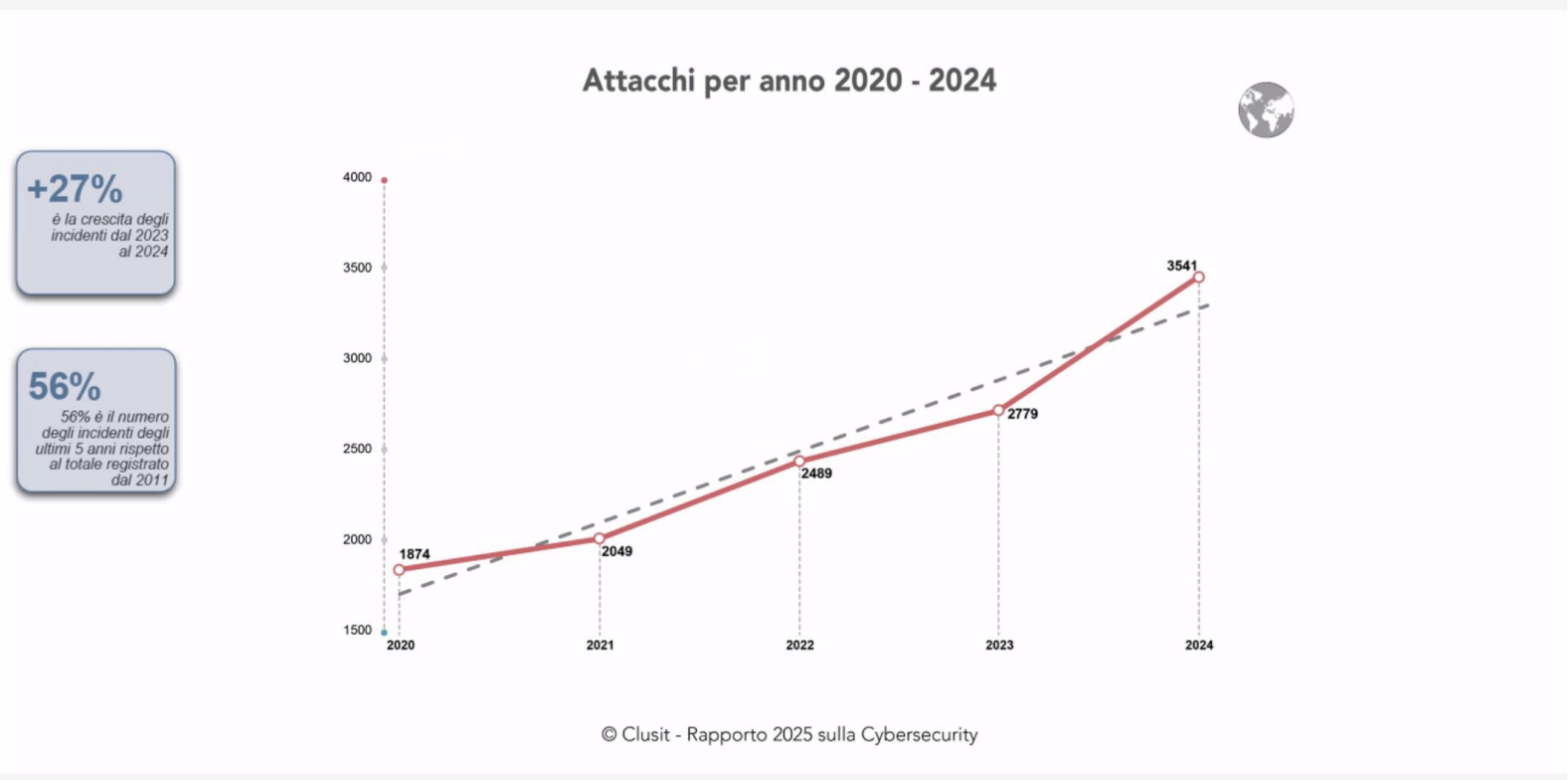
36.914 miliardi US$*	**PIL**	18.590 miliardi US$*	[-50% circa PIL AM]
> 1.000.000.000	**Popolazione**	> 700.000.000	[-30% circa pop. AM]
1.235	**N° Incidenti Cyber**	1.075	[-12% incidenti AM]
35%	**% Incidenti vs. Mondo**	30%	

** Fonte: World Bank Group*

CYBERSICURITY IN NUMERI

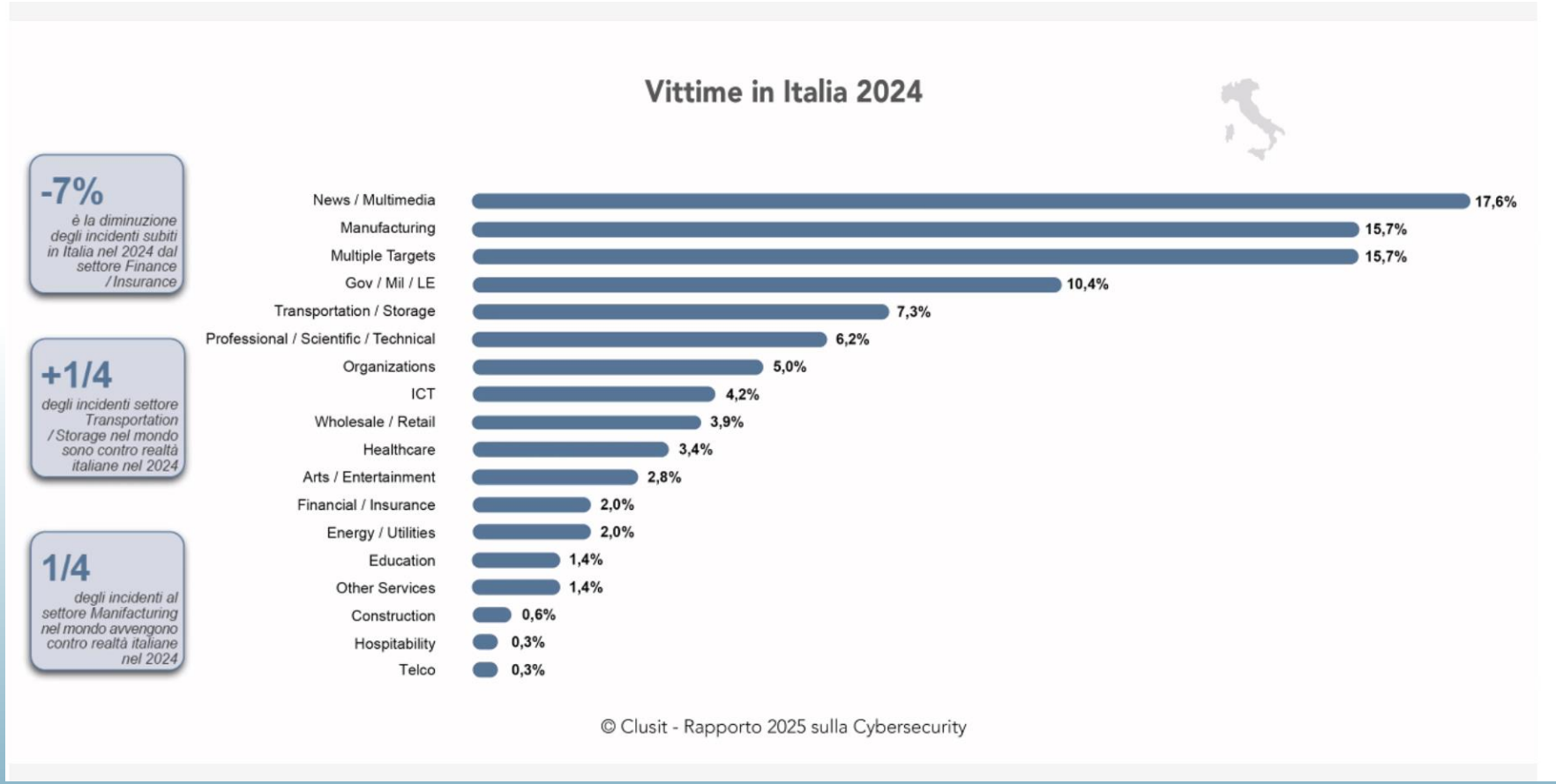
- Investimenti globali in aumento
- Gap tra Italia e media europea
- PMI e studi professionali: ancora poca protezione

CYBERSICURITY IN NUMERI



Il 2024 ha segnato un nuovo record negativo per la cybersecurity globale. Secondo i dati presentati, lo scorso anno si sono registrati **3.541 attacchi informatici noti**, con un incremento del **27%** rispetto al 2023.
Questo dato conferma una tendenza costante di crescita che, negli ultimi cinque anni, ha visto avvenire **oltre la metà (56%) di tutti gli incidenti mappati dal 2011 ad oggi**.

CYBERSICURITY IN NUMERI



CYBERSICURITY IN NUMERI

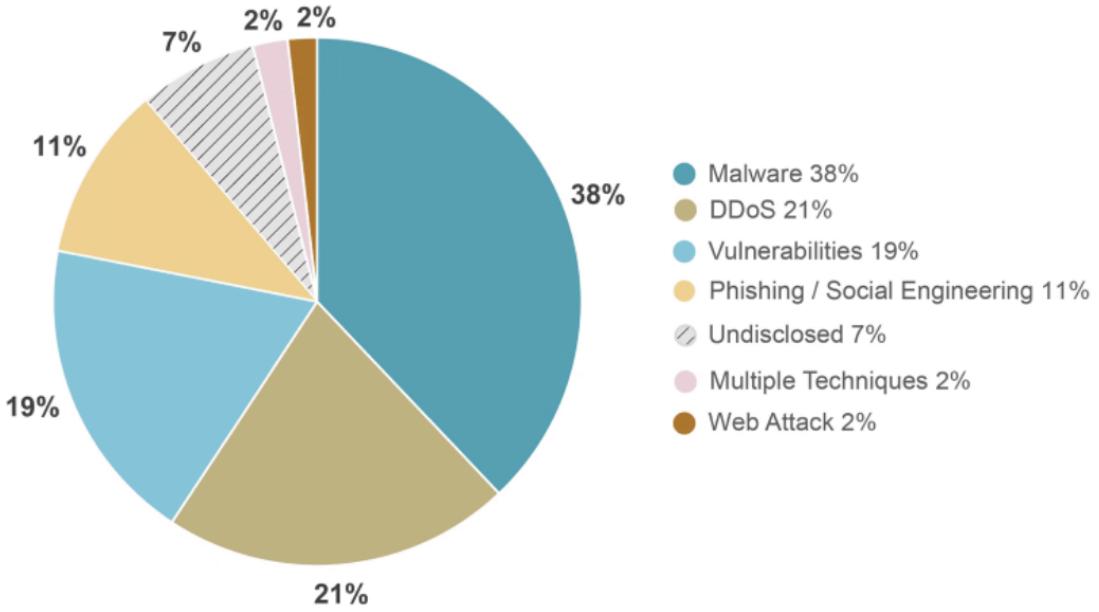
+35%
è la crescita degli incidenti in Italia basati su phishing e ingegneria sociale, dal 2023 al 2024

+90%
è la crescita degli incidenti in Italia basati su Vulnerabilities, dal 2023 al 2024

-36%
è la riduzione dal 2023 al 2024 degli attacchi DDOS in Italia

+1/3
degli incidenti in Italia nel 2024 sono causati da Malware

Tecniche di attacco in Italia 2024



© Clusit - Rapporto 2025 sulla Cybersecurity

Intelligenza artificiale e nuovi attacchi

Aumento degli attacchi IA

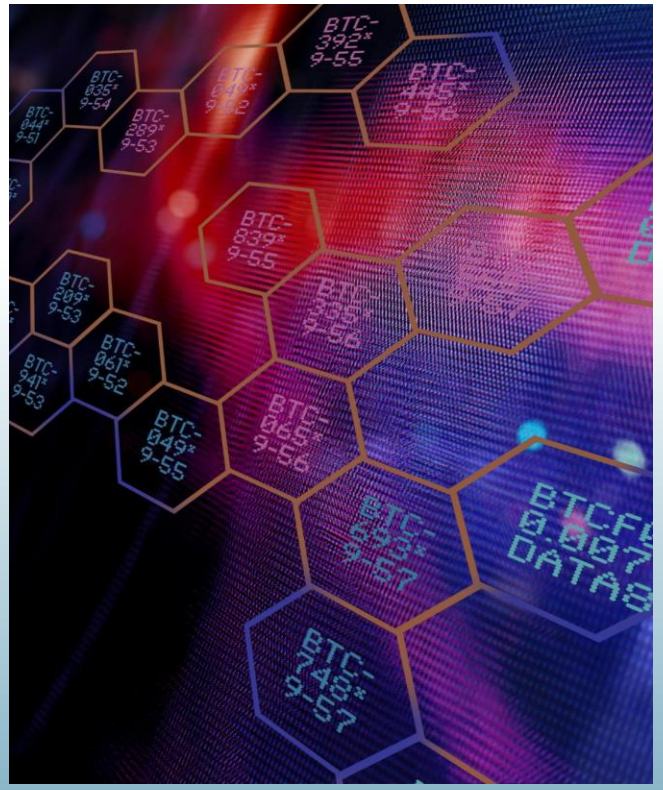
Prevediamo un aumento degli attacchi informatici sfruttando l'intelligenza artificiale generativa, con nuove modalità di aggressione.

Difficoltà di individuazione

Gli attacchi che sfruttano l'IA diventeranno più difficili da rilevare, aumentando il rischio di violazioni della sicurezza.

Malware e phishing sofisticati

L'uso dell'IA permetterà la creazione di malware e attacchi di phishing sempre più avanzati e personalizzati.



Deepfake: minacce emergenti

Minaccia emergente

I deepfake rappresentano una nuova minaccia emergente, con il potenziale di ingannare le persone in vari contesti.

Fiducia e inganno

La crescente fiducia nel riconoscere i deepfake è preoccupante, poiché molte persone potrebbero essere facilmente ingannate.

Consequenze aziendali

Le aziende possono subire gravi perdite finanziarie a causa di truffe basate su deepfake, come dimostrato da recenti attacchi.

Deepfake: Esempi Recenti

Ordine dei Dottori Commercialisti e degli Esperti Contabili di Torino

Fondazione Piero Piccatti e Aldo Milanese

ORDINE DOTTORI COMMERCIALISTI ED ESPERTI CONTABILI TORINO

Deepfake nelle Elezioni

- Gennaio 2024: chiamata automatizzata ai elettori del New Hampshire;
- la chiamata sembrava provenire dal presidente Joe Biden

Deepfake nel contesto B2B

- Febbraio: truffa basata su deepfake a Hong Kong
- Multinazionale ha perso 200 milioni di dollari
- Impiegato ingannato durante una riunione virtuale
- Partecipanti alla riunione erano tutti deepfake, incluso il CFO

“La cybersecurity non è un’opzione. È una responsabilità.”

Grazie per l’attenzione.

www.odcec.torino.it
www.linkedin.com/company/odcec-torino/
www.youtube.com/channel/UCBUHnLEOEHA6YY-MLr8vG8A/videos