FORUM 2024
CYBER 4.0

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

LUISS

Interviene:

Nicola Vanin

CISO, Cassa Depositi e Prestiti

Megatrend di Cybersecurity in Italia e nel mondo

Megatrend di Cybersecurity in Italia e nel mondo

OVERVIEW TREND CYBER SECURITY

Gli scenari politici, l'evoluzione normativa e le nuove tecnologie stanno creando un forte impatto sulla capacità delle **organizzazioni**, del settore **finanziario** e **pubblico**, di garantire la propria **cyber resilience** e di affrontare le minacce relative alla sicurezza.

Impatto della Geopolitica

Minaccia dei conflitti che porta ad attacchi informatici sia sponsorizzati dallo Stato sia collaterali che richiedono misure di sicurezza informatica rafforzate.

Focus in Slide successive

Tecnologie Emergenti

Attacchi come deepfakes, phishing e malware tramite l'utilizzo di tecnologie emergenti come l'Intelligenza Artificiale, Quantum Computing e Cloud computing.

Focus in Slide successive

Evoluzione Normativa

Normative in evoluzione come DORA, CRA, NIS 2, AI Act e crittografia post-quantistica portano a sfide di conformità per le organizzazioni.

Skill Gap

Carenza di professionisti qualificati che comporta maggiore vulnerabilità agli attacchi informatici e tempi di risposta più lenti agli incidenti di sicurezza

Politica dei Costi

Continuo aumento degli investimenti in presenza di esigenze di consolidamento e di efficienza dei costi.

70% delle strategie di cyber security delle organizzazioni sono influenzate dai cambiamenti geopolitici.

66% delle società FS ritiene che l'IA generativa fornirà un vantaggio agli attaccanti rispetto ai difensori.

50% delle organizzazioni FS hanno subito un impatto rilevante da un incidente causato da terzi.

20 % del Top Management aziendale ha denunciato la mancanza di figure qualificate.

14% aumento della spesa per la sicurezza informatica nel 2024.

Fonte: *Global Cybersecurity Outlook*

FOCUS: TECNOLOGIE EMERGENTI

È diffuso il timore che l'utilizzo di tecnologie emergenti come l'intelligenza artificiale generativa, l'informatica quantistica, e l'edge computing farà avanzare rapidamente le capacità di attacchi cyber.

Tecnologie Emergenti

GenAI

Informatica Quantistica

Edge Computing

Principali Rischi Cyber

- **DeepFake:** diffusione di informazioni e contenuti falsi.
- **Phishing e social engineering:** divulgazione informazioni sensibili.
- **Math Washing:** deresponsabilizzazione dell'individuo nelle scelte e presa di decisioni.
- **Privacy e protezione dei dati:** diffusione dei dati personali e sensibili.

- **Cracking Crittografia**: decifrazione della crittografia grazie alla potenza di calcolo dei computer quantistici.
- **Backdoor Quantistiche**: accessi non autorizzati a sistemi protetti.

- **Edge Device Attack**: accessi non autorizzati agli edge devices (componenti di rete responsabili della connessione della rete locale a una rete esterna)
- **Attack Surface Management**: aumento dei punti di ingressi per gli attachi.

Considerazioni

A prescindere dai Rischi Cyber, le tecnologie emergenti potrebbero tagliare fuori dal mercato le organizzazioni soprattutto quelle meno resilienti in quanto:

Controllo Governativo: : sviluppo di tecnologie avanzate per scopi strategici e di sicurezza nazionale che potrebbero non essere rese disponibili al settore privato per motivi di sicurezza

Costi Elevati: investimenti significativi in termini di ricerca, sviluppo e infrastruttura. Questo può renderle non accessibili per diverse organizzazioni.

Accesso Limitato: restrizioni sull'accesso per motivi di licenze, proprietà intellettuale o esigenze strategiche del fornitore.

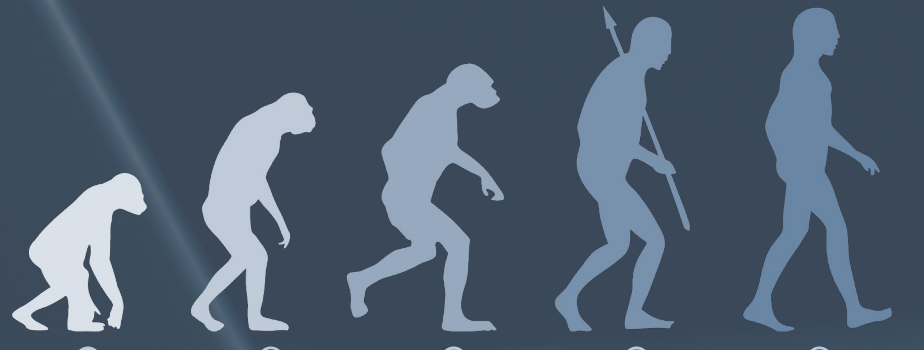
Competizione e Disuguaglianza: vantaggi competitivi significativi, per le organizzazioni con accesso a questa tecnologia indietro le restanti.

***Fonte**: ISF Threat Horizon 2026*

FOCUS: EVOLUZIONE NORMATIVA

L'introduzione e l'evoluzione di normative come DORA, CRA, NIS 2, AI Act aiutano a proteggere i dati sensibili, ridurre le minacce cibernetiche, promuovere la fiducia degli utenti e standardizzare le pratiche di sicurezza ma allo stesso tempo possono generare una "*ipertrofia normativa*" in materia di innovazione digitale

Evoluzione Normativa



- **DORA** entrata in vigore il 17/01/2023
- **NIS 2** entrata in vigore il 17/01/2023
- **CRA** pubblicato il 20/12/2023
- **AI Act** approvata il 13/03/2024
- **DDL AI** Varato il 23/04/2024

Necessità

- Contrasto alle minacce informatiche derivanti dallo sviluppo delle tecnologie emergenti.
- Protezione dei diritti e della privacy dei cittadini, garantendo che le tecnologie emergenti siano utilizzate in modo etico e sicuro.
- Aumento della fiducia degli utenti nelle tecnologie emergenti e nei sistemi digitali.

Azioni

- Armonizzare le normative esistenti, riducendo le ridondanze.
- Definire le regole più chiare e accessibili per le organizzazioni.

Nonostante il rischio di incorrere in un' "*ipertrofia normativa*" e di generare confusione all'interno delle organizzazioni **la proliferazione normativa** è **la risposta necessaria** al rapido sviluppo e diffusione delle tecnologie emergenti ed ai nuovi potenziali rischi ne scaturiscono.

Fonte: *Piano triennale per l'informatica 2024-2026 – Cyber360*

FOCUS: INVESTIMENTI E CRESCITA MERCATO CYBER

Gli investimenti e la crescita del mercato Cyber, in Italia, hanno l'obiettivo strategico di posizionare il Paese come leader nell'innovazione digitale e raggiungere **l'autonomia tecnologica**.

da **190,4** Miliardi di $ nel 2023

Crescita del mercato globale della sicurezza informatica

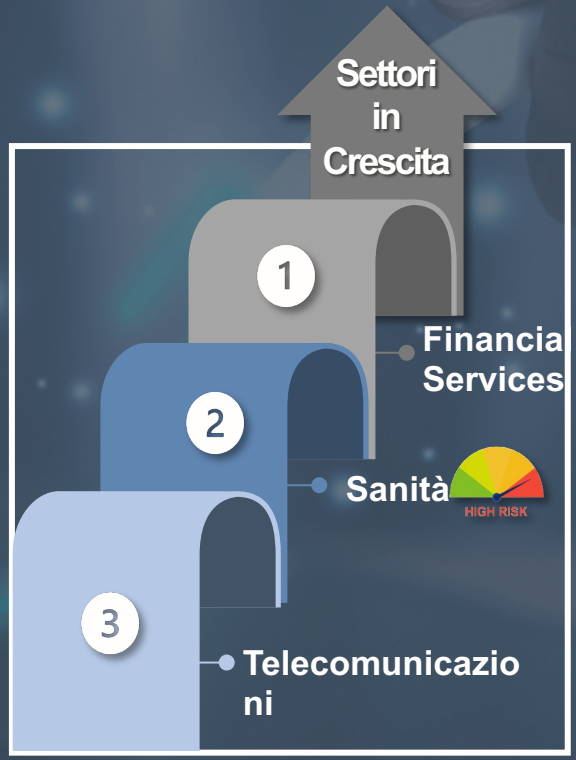
a **298,5** miliardi di $ entro il 2028 con un Cagr* del 9,4% sino al 2028

spesa a **2,15** di Miliardi di € in Italia

+16% rispetto2022

Crescita del mercato globale della sicurezza informatica

Il **62%** delle grandi aziende italiane ha investito di più in difesa digitale delle infrastrutture



Fonti: Rapporto di ricerca Mercato della sicurezza informatica, ilsole24ore,

Note: CAGR - Compound annual growth rate - tasso di crescita annuo composto (CAGR) misura il tasso di rendimento di un investimento*