For You Information Technologies Srl

piva / cf / reg. impr. ud
02102200306
rea 235449
info@4youit.net
www.4youit.net

RAPPORTO ANNUALE SULLA CYBERSECURITY 2025–2026

Minacce, evoluzione del rischio e resilienza digitale

Doc ID: 4YIT_000000000020.1.0

Data Pubblicazione: 26/04/2026

Autore: C.Lipone

Indice

1. Ruolo e approccio di For You Information Technologies (4YouIT)

4YouIT opera nel campo della gestione delle infrastrutture IT e dei servizi di sicurezza informatica, supportando organizzazioni pubbliche e private nella gestione operativa dei propri sistemi.

Nel contesto di una crescente esposizione ai rischi cyber, 4YouIT contribuisce alla sicurezza dei clienti attraverso attività di monitoraggio, gestione e supporto tecnico, operando nel rispetto delle responsabilità condivise e delle indicazioni fornite dalle organizzazioni servite.

4YouIT adotta un approccio basato su:

- tracciabilità delle attività;
- gestione strutturata delle richieste e degli interventi;
- allineamento a standard internazionali di qualità e sicurezza.

Il presente rapporto nasce con l'obiettivo di sintetizzare le principali evidenze emerse dai report delle agenzie di cybersecurity nazionali e internazionali, mettendole a disposizione di clienti e stakeholder in forma accessibile e strutturata.

2. Executive Summary

Il periodo 2025–2026 conferma in modo definitivo il passaggio da un modello di minacce episodiche a un ecosistema cyber strutturato e persistente.

Gli attacchi non si configurano più come eventi isolati, ma come fenomeni continui, distribuiti e sempre più industrializzati.

Secondo le analisi ENISA, il phishing rappresenta circa il 60% dei vettori di accesso iniziale, mentre lo sfruttamento delle vulnerabilità supera il 20% dei casi. Questo evidenzia come gli attacchi continuino a basarsi su tecniche consolidate ma altamente efficaci.

In parallelo, l'introduzione della direttiva NIS2 ha ampliato significativamente la visibilità sugli incidenti cyber, aumentando il numero di eventi rilevati e segnalati. Questo non rappresenta necessariamente un aumento degli attacchi, ma una maggiore capacità di rilevazione e consapevolezza del rischio.

3. Scenario delle minacce

Il contesto attuale è caratterizzato da campagne di attacco persistenti e distribuite nel tempo. Gli attori malevoli operano in modo strutturato, sfruttando strumenti automatizzati e modelli "as-a-service", rendendo gli attacchi più scalabili e accessibili.

ENISA ha analizzato circa 5.000 incidenti nel periodo recente, evidenziando un ecosistema ormai industrializzato, in cui le vulnerabilità vengono sfruttate rapidamente e le tecniche di attacco si diffondono velocemente tra gli attori.

La superficie di attacco continua ad ampliarsi a causa della digitalizzazione, del cloud e dell'interconnessione tra sistemi, aumentando il numero di possibili punti di ingresso.

Questo modello operativo rende il rischio meno visibile nel breve periodo, ma potenzialmente più impattante nel medio-lungo termine, in quanto contribuisce a una progressiva erosione della resilienza delle organizzazioni.

Il panorama delle minacce risulta ulteriormente confermato dalle analisi condotte da CISA (Cybersecurity and Infrastructure Security Agency) e dal FBI tramite l'Internet Crime Complaint Center (IC3), che evidenziano una crescita costante degli attacchi basati su vulnerabilità note e credenziali compromesse.

In particolare, il Known Exploited Vulnerabilities (KEV) Catalog di CISA rappresenta uno degli indicatori più rilevanti per comprendere il comportamento degli attaccanti: le vulnerabilità inserite nel catalogo sono quelle effettivamente sfruttate in attacchi reali. L'analisi di tali dati evidenzia come gli attaccanti privilegino vulnerabilità già documentate e per le quali esistono patch disponibili, ma non ancora applicate.

Questo conferma una dinamica già osservata nei report europei:

il fattore critico non è la scoperta di nuove vulnerabilità, ma la capacità delle organizzazioni di gestire quelle già note.

Parallelamente, i dati IC3 mostrano come le principali categorie di attacco continuino a includere:

- compromissione delle email aziendali (BEC – Business Email Compromise)
- ransomware
- frodi basate su social engineering

Questi attacchi, pur non essendo sempre tecnologicamente avanzati, risultano estremamente efficaci grazie alla combinazione tra fattore umano e debolezze organizzative.

4. Vettori di attacco e tecniche operative

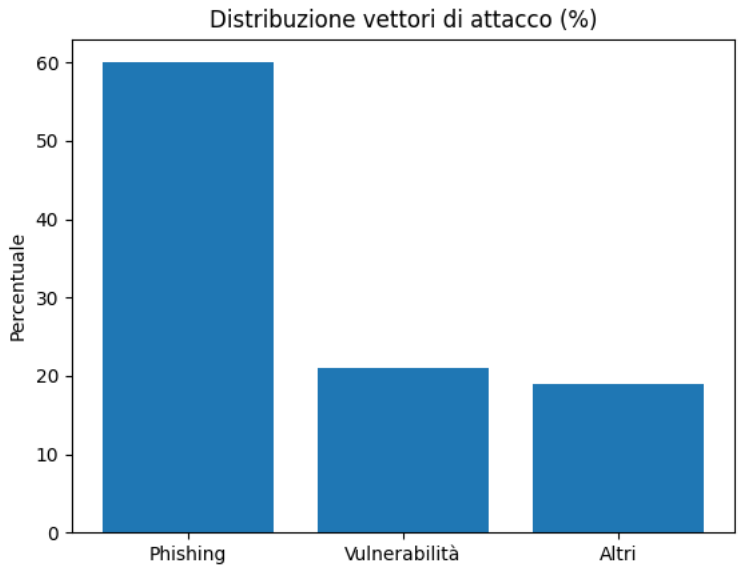
Il phishing si conferma come il principale vettore di accesso iniziale, grazie alla sua capacità di sfruttare il fattore umano e alla diffusione di strumenti automatizzati.

Lo sfruttamento delle vulnerabilità rappresenta il secondo vettore principale, con tempi sempre più ridotti tra la pubblicazione di una vulnerabilità e il suo utilizzo attivo.

Gli attacchi seguono schemi ricorrenti: accesso iniziale, acquisizione delle credenziali, movimento laterale e compromissione finale dei sistemi o dei dati.

5. Distribuzione dei vettori di attacco

La distribuzione dei vettori evidenzia la predominanza del phishing, seguito dallo sfruttamento delle vulnerabilità.



Fonte elaborazione su dati ENISA Threat Landscape - I valori rappresentano una sintesi aggregata dei principali report ENISA e possono variare in funzione del campione analizzato.

6. Vulnerabilità e superficie di attacco

Il numero di vulnerabilità pubblicate è in costante crescita, con migliaia di nuove CVE ogni mese. La disponibilità di exploit pubblici riduce drasticamente il tempo di intervento.

Questo fenomeno evidenzia come la gestione delle vulnerabilità sia uno degli elementi più critici nella strategia di sicurezza.

7. Supply chain e interdipendenze

Gli attacchi alla supply chain rappresentano una delle principali evoluzioni del panorama cyber. La compromissione di un fornitore può avere effetti a cascata su più organizzazioni.

Questo scenario richiede un approccio alla sicurezza esteso all'intero ecosistema digitale.

8. Sicurezza nelle PMI

Le piccole e medie imprese rappresentano uno dei segmenti più esposti al rischio cyber, non tanto per la presenza di vulnerabilità tecnologiche differenti rispetto alle grandi organizzazioni, quanto per limiti strutturali nella gestione della sicurezza.

A differenza delle grandi aziende, le PMI operano spesso con:

- risorse IT limitate
- assenza di ruoli dedicati alla sicurezza
- elevata concentrazione di responsabilità su poche figure
- forte dipendenza da fornitori esterni

Questo contesto rende difficile l'adozione completa dei modelli teorici di sicurezza, in particolare per quanto riguarda la segregazione dei ruoli e la separazione dei domini operativi.

Un elemento critico è rappresentato dalla crescente integrazione tra sistemi:

- cloud
- gestione remota
- sicurezza endpoint
- infrastruttura di rete

In molti casi, questi sistemi vengono gestiti all'interno dello stesso ambiente o con gli stessi privilegi amministrativi. Questo approccio, sebbene efficiente dal punto di vista operativo, introduce un rischio sistemico significativo.

Infatti:

la compromissione di un singolo account privilegiato può determinare accesso trasversale all'intera infrastruttura.

In questo scenario, per le PMI risulta spesso irrealistico replicare modelli di sicurezza basati su una rigida separazione dei ruoli. Tuttavia, è possibile adottare un approccio alternativo basato su una sicurezza a più livelli (defense-in-depth), che prevede:

- utilizzo di soluzioni diverse e indipendenti
- separazione logica dei controlli
- monitoraggio incrociato tra sistemi
- limitazione dei privilegi operativi
- tracciabilità completa delle attività

Questo modello consente di ridurre il rischio anche in contesti con risorse limitate, aumentando la resilienza complessiva del sistema.

9. Caso reale – Attacco a STRYKER – Lezione appresa

Il recente attacco che ha coinvolto Stryker rappresenta un esempio significativo delle criticità legate alla gestione integrata della sicurezza.

L'attacco ha comportato la compromissione di un account privilegiato, attraverso il quale è stato possibile eseguire comandi ad alto impatto sull'infrastruttura. In particolare, è stata avviata una procedura di cancellazione massiva che ha interessato circa 200.000 dispositivi, tra server e dispositivi mobili, inclusi smartphone.

L'incidente ha evidenziato come la mancanza di una chiara separazione tra:

- sistemi operativi
- strumenti di gestione
- controlli di sicurezza
- accessi amministrativi

possa amplificare l'impatto di una compromissione.

In contesti altamente integrati, la presenza di un unico dominio di controllo o di credenziali condivise tra più sistemi può trasformare una violazione iniziale in un incidente sistemico.

Questo tipo di scenario è particolarmente rilevante per le PMI e per i fornitori di servizi gestiti, dove:

- gli strumenti di gestione sono centralizzati
- gli accessi amministrativi sono estesi
- le piattaforme cloud integrano più funzioni

La lezione principale che emerge è chiara:

la sicurezza non deve essere solo efficace, ma anche resiliente alla compromissione dei suoi stessi controlli.

In questo senso, l'adozione di un'architettura basata su più livelli indipendenti rappresenta una delle strategie più efficaci per ridurre il rischio

10. Approfondimento: Direttiva NIS2

La Direttiva NIS2 (UE 2022/2555) rappresenta un pilastro della strategia europea di cybersecurity. L'obiettivo è rafforzare la resilienza delle infrastrutture critiche e migliorare la gestione del rischio cyber a livello sistemico.
La direttiva amplia il numero di soggetti coinvolti, includendo organizzazioni essenziali e importanti, e introduce obblighi in materia di gestione del rischio, notifica degli incidenti e sicurezza della supply chain.

L'impatto principale è il passaggio da una sicurezza tecnica a una sicurezza di governance aziendale, con responsabilità dirette per il management.

10.1. NIS2: cosa cambia realmente per le organizzazioni

La Direttiva NIS2 (Network and Information Security), formalmente Direttiva (UE) 2022/2555, rappresenta uno dei principali strumenti normativi con cui l'Unione Europea sta affrontando l'evoluzione del rischio cyber.

Recepita in Italia con il D.Lgs. 138/2024, la NIS2 introduce un modello più strutturato e pervasivo di gestione della sicurezza informatica.

10.1.1. Obiettivo della NIS2

L'obiettivo della direttiva non è esclusivamente tecnico, ma sistemico:

- aumentare il livello medio di sicurezza informatica nell'UE
- ridurre il rischio di incidenti con impatto su servizi essenziali
- migliorare la capacità di prevenzione, rilevazione e risposta
- rafforzare la resilienza delle infrastrutture critiche

10.1.2. Chi è coinvolto

Le organizzazioni vengono suddivise in:

Soggetti Essenziali:

- energia, trasporti, sanità, telecomunicazioni, PA, infrastrutture digitali

Soggetti Importanti:

- manifatturiero, servizi digitali, rifiuti, alimentare, fornitori ICT e cloud

10.1.3. Obblighi principali

- gestione del rischio cyber
- notifica degli incidenti
- sicurezza della supply chain
- governance e responsabilità del management

10.1.4. Tempistiche in Italia

- 2022 approvazione
- 2024 recepimento
- 2025-2026 operatività

10.1.5. Impatto

La NIS2 introduce un cambio di paradigma:

- da sicurezza tecnica a sicurezza di governance
- maggiore responsabilità del management
- maggiore formalizzazione dei processi

11. Considerazioni conclusive

Il panorama della cybersecurity evidenzia un rischio sempre più sistemico. Gli attacchi sono continui e sfruttano vulnerabilità note.

Le organizzazioni devono adottare un approccio strutturato e continuo alla sicurezza, basato su monitoraggio, gestione delle vulnerabilità e controllo degli accessi.

La cybersecurity rappresenta oggi un fattore strategico per la resilienza e la continuità operativa.

12. Fonti

Il presente rapporto si basa sull'analisi e sintesi delle principali pubblicazioni istituzionali in ambito cybersecurity:

ENISA – Threat Landscape - https://www.enisa.europa.eu
ACN – Relazione annuale sulla sicurezza nazionale - https://www.acn.gov.it
CLUSIT – Rapporto sulla sicurezza ICT in Italia - https://www.clusit.it
CISA – Cybersecurity and Infrastructure Security Agency - https://www.cisa.gov
CISA – Known Exploited Vulnerabilities (KEV) Catalog - https://www.cisa.gov/known-exploited-vulnerabilities-catalog
FBI / IC3 – Cybersecurity Advisories - https://www.ic3.gov

Le informazioni sono state rielaborate in forma sintetica per finalità divulgative e di sensibilizzazione.