COMUNICATO STAMPA

Pubblicato Rapporto OAD 2025 di AIPSI



AIPSI ha pubblicato il **Rapporto 2025 OAD**, Osservatorio Attacchi Digitali in Italia, arrivato alla 18° anno consecutivo di indagini sugli attacchi digitali intenzionali ai Sistemi Informativi di imprese pubbliche e privati operanti in Italia, e sulle misure di sicurezza, tecniche e organizzative, adottate.

OAD 2025 è stata effettuata da AIPSI con Malabo Srl, e in collaborazione con il Servizio Polizia Postale e per la Sicurezza Cibernetica, AICA e FIDAInform.

Il Rapporto 2025 OAD analizza la situazione degli attacchi digitali in Italia rilevati nell'intero 2024 dai rispondenti al questionario online rigorosamente anonimo. Esso inquadra la situazione emersa dall'indagine OAD nel contesto mondiale, con riferimenti documenti World Economic Forum, nel contesto europeo con riferimenti ai più recenti documenti di ENISA, Agenzia europea per la cibersicurezza, ed in quello nazionale con riferimenti ai dati di ACN, Agenzia italiana per la cibersicurezza, e del Servizio Polizia Postale e per la Sicurezza Cibernetica, che li ha forniti per il Capitolo 8 del Rapporto.

Il **Rapporto OAD 2025** è di 185 pagine A4, con numerosi grafici ed immagini. E' strutturato in 8 Capitoli (141 pagine A4) con l'elaborazione e l'analisi dei dati emersi dall'indagine e in 8 Allegati (44 pagine A4).

Il **Rapporto OAD 2024** è **liberamente scaricabile**, senza alcun login:

- dal sito di AIPSI: https://www.aipsi.org/eventi/eventi-in-programma/992-pubblicato-e-liberamente-scaricabile-il-rapporto-oad-2025-di-aipsi.html
- dal sito di OAD: https://www.oadweb.it/it/oad-2025/per-scaricare-il-rapporto-oad-2025.html, dal quale si possono scaricare anche i precedenti Rapporti OAD pubblicati;
- dal sito di Malabo Srl: https://www.oadweb.it/it/oad-2025/per-scaricare-il-rapporto-oad-2025.html

All'indagine online OAD hanno risposto centinaia di imprese pubbliche e private, e di queste il **63% sono piccole-medio organizzazioni** (fino a 250 dipendenti) , con una forte partecipazione anche di micro imprese. I settori più rappresentati: ICT (21%), manifattura/costruzioni, sanità, servizi professionali. Le figure rispondenti: **manager apicali** (26%), CIO (23%), esperti terziarizzati (20%).
Il **75%** considera il proprio Sistema Informativo (SI) **essenziale**; il **25%** rientra nelle **infrastrutture critiche** (NIS2).

Gli attacchi rilevati nel 2024

Il 71% delle organizzazioni rispondenti **ha subito attacchi digitali** nel 2024.

Le **tipologie di attacco** (che cosa si attacca) **più diffuse,** tra le 16 considerate, includono:

- Modifiche dannose o non autorizzate a programmi/configurazioni ICT (**29 %**);
- Uso malevolo o non autorizzato di interi sistemi ICT (**24%**);

- Attacchi DoS/DDoS (**20%**), spesso collegati a gruppi di attaccanti filo-russi;
- Attacchi alla supply chain (**15%**), un rischio globale significativo secondo il WEF;
- Attacchi ai sistemi basati sull'intelligenza artificiale (**8%**).

Le **tecniche di attacco** (come si attacca) **più diffuse** includono, tra le 8 considerate: attacchi multi-tecnica combinata (**37%**), social engineering (**16%**), malware/ransomware (**10%**).

L'indagine OAD 2025 ha approfondito tre aree di attacco critiche, facendo particolare attenzione agli impatti sui Sistemi Informativi che hanno subito tali attacchi: i siti web, gli ambienti OT, Operational Technology, le applicazioni e i servizi informatici basati su tecniche di Intelligenza Artificiale (IA).

L'analisi verticale degli **attacchi ai sistemi web** ha rivelato:

- Il **94,15%** utilizza sia sistemi web on-premise che esternalizzati;
- Il 58,4% **ha rilevato attacchi** ad applicazioni web, il **60,6%** dei quali ha interessato sistemi in cloud;
- Le vulnerabilità tecniche hanno causato il **93,83%** degli attacchi più gravi;
- Con riferimento alle Top 10 vulnerabilità indicate a livello mondiale da OWASP per i web, il software obsoleto/vulnerabile si è classificato al primo posto (**39,51%**), seguito da errori di configurazione (**30,86%**) e da problemi di autenticazione (**25,93%**);
- Il **64,29%** ha subito interruzioni del servizio per **≥2 giorni**; **l'86,5%** ha sostenuto costi IS più elevati e il **12,36%** ha avuto impatti sul bilancio dell'impresa;
- Sabotaggio (**44,44%**), frode (**40,74%**) ed estorsione (**~30%**) sono stati i motivi principali, mentre l'hacktivismo (**21%**) e la guerra informatica (**16%**) hanno mostrato una crescente influenza geopolitica.

Per i **sistemi OT (Operational Technology)**:

- **utilizzati dal 40,58%** dei rispondenti; **32,1% attaccati**
- I sistemi robotici sono stati i più colpiti (**70%**), seguiti da IoT/IIoT (**55,56%**);
- **L'85%** ha segnalato tempi di inattività **superiori a 2 giorni**, spesso estesi alle applicazioni del Sistema Informativo (il **30% per 2-3 giorni**);
- Il **37%** ha segnalato aumenti significativi dei costi per il Sistema Informativo, con un impatto per il **30%** sul bilancio dell'impresa;
- Il sabotaggio è stato il fenomeno dominante (**93%**), seguito da vandalismo (**37%**) ed estorsione (**22%**).

Per i **sistemi basati su IA**:

- Il **41%** utilizza già applicazioni di IA; il **23,8%** ha subito attacchi digitali a questi sistemi di IA;
- Con riferimento alle vulnerabilità Top 10 OWASP per l'IA (LLM e GenAI), le principali usate nell'attacco più grave sono state "Data and Model Poisoning" (**35%**) e "Improper Output Handling" (**20%**);
- La maggior parte delle vulnerabilità dell'IA sono legate agli input immediati e all'avvelenamento dei metodi di addestramento dei modelli.

Misure di sicurezza adottate

Il **40%** ha compilato le sezioni opzionali del questionario OAD 2025 sulle **misure di sicurezza adottate**, ed ha fornito i seguenti principali dati:

- **Misure tecniche** di sicurezza digitale
  - il **60%** gestisce centralmente le password;

- il **55%** dei Sistemi Informativi controlla centralmente funzionalità, prestazioni e livelli di sicurezza delle reti;
- il **20%** dei software applicativi sviluppati ad hoc hanno seguito procedure e metodiche di sviluppo sicuro**;**
- **l'80%** dei Sistemi Informativi usa FWA, Firewall Applicativi**;**
- l'**85%** gestisce la manutenzione correttiva del software;
- l'**84%** delle aziende/enti rispondenti effettua l'analisi delle vulnerabilità;
- il **44,6%** dei Sistemi Informativi effettua il backup "a regola d'arte".

- **Misure organizzative** di sicurezza digitale
  - l'**80%** ha definito ed usa policy e procedure organizzative per la sicurezza digitale;
  - il **81%** effettua l'analisi dei rischi digitali;
  - il **52%** effettua auditing per la sicurezza digitale;
  - Certificazioni: **27%** richieste al proprio interno, **30%** richieste ai Fornitori.
- **Misure di gestione e controllo della sicurezza digitale**
  - **l'80%** utilizza sistemi di gestione e di controllo seppure in modalità diverse;
  - Il **81%** archivia i log degli utenti, ed il **48%** li gestisce;
  - **79%** effettua controlli sulla sicurezza delle supply chain**;**
  - Il **70%** ha previsto un Piano di Disaster Recovery;
    - Il **70%** di questi ha previsto o allocato risorse ICT alternative per poterlo realmente attuare.

Conclusioni e raccomandazioni

OAD 2025 conferma il preoccupante quadro di **diffusione, gravità e impatto crescente degli attacchi digitali intenzionali** già riscontrato nella precedente edizione OAD 2024.
A questa situazione ha contribuito da un lato la criminalità informatica, dall'altro il quadro geopolitico instabile, con guerre ibride in corso (Ucraina, Medio Oriente), che hanno visto un'escalation di **cyber warfare, disinformazione e attacchi digitali mirati** contro infrastrutture pubbliche e private. L'uso dell'**Intelligenza Artificiale** ha avuto un ruolo crescente, sia come vettore d'attacco sia come bersaglio.

Nel 2024 permane il periodo di insicurezza digitale sistemica.

Serve un cambio di paradigma: dalla protezione alla resilienza.

La resilienza può e deve essere assicurata dalla **business continuity**, ossia la **continuità operativa dei processi essenziali**; mentre, sul versante ICT, da un piano di **Disaster Recovery** efficace, attuabile e testato.

Le **necessità prioritarie** includono:

- Investire in **formazione, automazione della gestione operativa della sicurezza digitale**, e nella **gestione del rischio ICT**.
- Monitorare e adattarsi costantemente **all'evoluzione delle minacce**, con particolare attenzione a **OT, IA e supply chain**.
- **IA utile per l'automazione** della gestione della sicurezza digitale, per la sistematica analisi e correlazione dei dati monitorati, per l'analisi del rischio ICT predittiva, per **l'analisi comportamentale** di utenti e sistemi ICT.



OAD è l'unica indagine online in Italia (completamente indipendente e "terza" rispetto ai vari attori in gioco) sugli attacchi digitali intenzionali ai sistemi informativi delle aziende e degli enti pubblici operanti in Italia, e sulle misure tecniche ed organizzative che questi hanno in esercizio. OAD non predefinisce uno specifico bacino di rispondenti, il medesimo negli anni, ma consente a chiunque, interessato e coinvolto nella gestione di un sistema informativo di una azienda/ente, un pieno e libero accesso al questionario online, in maniera totalmente anonima.