COMUNICATO STAMPA

Pubblicato il Rapporto OAD 2026: l'insicurezza digitale è ormai sistemica, la resilienza delle organizzazioni resta una criticità:

- **L'84% delle organizzazioni rispondenti ha rilevato attacchi digitali nel primo quadrimestre 2026.**
- **L'intelligenza artificiale è lo strumento di attacco più temuto.**
- **Nonostante l'ampia diffusione dei backup, solo il 37% dei rispondenti alla relativa sezione ha effettuato prove effettive di ripristino dei sistemi**



Milano, 26 novembre 2026

È stato pubblicato il Rapporto OAD 2026, Osservatorio Attacchi Digitali in Italia, giunto al diciannovesimo anno consecutivo di indagini online sugli attacchi digitali intenzionali e sulle misure tecniche e organizzative adottate da aziende ed enti operanti in Italia per proteggere i propri sistemi informativi.

Il Rapporto, realizzato da Marco R. A. Bozzetti, ideatore e curatore dell'iniziativa OAD, con la collaborazione istituzionale di AICA, FIDAInform e del Servizio Polizia Postale e per la Sicurezza Cibernetica, e con la partnership del Gruppo Qintesi, è liberamente e gratuitamente scaricabile dal sito www.oadweb.it, senza necessità di registrazione.

L'edizione 2026 analizza gli attacchi rilevati **nell'intero 2025** e **nel primo quadrimestre 2026**, inquadrando i risultati dell'indagine OAD nello scenario nazionale, europeo e internazionale, anche attraverso i dati e le analisi del World Economic Forum, dell'ENISA, dell'Agenzia per la Cybersicurezza Nazionale (ACN) e della Polizia Postale.

Una condizione di persistente insicurezza digitale sistemica

Il primo dato significativo che emerge dall'indagine è l'elevata esposizione delle organizzazioni agli attacchi digitali intenzionali.

Il 66,30% delle organizzazioni rispondenti dichiara di aver rilevato attacchi ai propri sistemi informativi nel 2025, mentre tale percentuale raggiunge l'84,02% già nel primo quadrimestre 2026.

Pur riferendosi a periodi di diversa durata, questi dati confermano una condizione di elevata esposizione alle minacce digitali.

L'analisi storica delle indagini OAD evidenzia inoltre come, a partire dal 2020, la percentuale delle organizzazioni che dichiarano di aver rilevato attacchi sia stabilmente superiore a quella delle organizzazioni che non ne hanno rilevati.

Gli attacchi digitali non costituiscono più un fenomeno episodico, ma una minaccia permanente per il funzionamento delle organizzazioni, per la continuità dei servizi e, più in generale, per il sistema economico e sociale.

Attacchi sempre più sofisticati, e cresce il timore per l'intelligenza artificiale

L'evoluzione degli attacchi digitali è caratterizzata dalla crescente complessità delle tecniche utilizzate e dalla difficoltà di individuare tempestivamente le compromissioni.

L'utilizzo combinato di più tecniche di attacco risulta la modalità maggiormente rilevata negli attacchi più gravi: 59,09% nel 2025 e 57,14% nel primo quadrimestre 2026.

L'intelligenza artificiale assume un ruolo sempre più rilevante, sia come strumento di difesa sia come tecnologia in grado di amplificare le capacità degli attaccanti. Il 73,74% dei rispondenti indica l'IA quale strumento di attacco temuto per il prossimo futuro, collocandola al primo posto.

Accanto alle tradizionali motivazioni economiche della criminalità informatica, assumono crescente importanza lo spionaggio, il sabotaggio digitale e l'hacktivism, anche in relazione alle tensioni geopolitiche e ai conflitti internazionali.

Un ulteriore elemento di criticità riguarda le catene di fornitura digitali: il 91,36% dei rispondenti utilizza risorse ICT terziarizzate, con una conseguente necessità di estendere la gestione della sicurezza anche ai fornitori e ai servizi cloud.

Le misure di sicurezza sono diffuse, ma la resilienza resta insufficiente

Uno dei risultati più significativi del Rapporto OAD 2026 riguarda il divario tra l'adozione delle misure di sicurezza e la concreta capacità delle organizzazioni di reagire agli incidenti e ripristinare i propri sistemi informativi.

Tra i partecipanti che hanno risposto alle sezioni opzionali dedicate alle misure di sicurezza emergono dati particolarmente significativi:

- l'89,19% effettua aggiornamenti software periodici;
- l'82,67% utilizza sistemi di autenticazione multifattoriale;
- l'83,56% effettua copie di backup;
- soltanto il 37% ha effettuato negli ultimi dodici mesi prove effettive di ripristino dei sistemi utilizzando le copie di backup;

- appena il 32,88% dispone di un piano di Disaster Recovery che preveda risorse ICT alternative;
- solo il 27,78% effettua attività di formazione periodica e obbligatoria sulla sicurezza digitale.

Disporre di strumenti tecnologici, copie di backup e procedure formalizzate non garantisce, di per sé, la capacità di affrontare un grave incidente digitale e di assicurare la continuità operativa.
La sicurezza digitale richiede pertanto un approccio integrato, che comprenda prevenzione, protezione, rilevazione degli attacchi, gestione degli incidenti e capacità di ripristino, attraverso attività periodiche di verifica e simulazione.
Fondamentale è il coinvolgimento diretto dei vertici delle organizzazioni nelle decisioni relative ai rischi digitali, alle responsabilità e agli investimenti necessari.

Una particolare attenzione alle piccole e medie organizzazioni

Una caratteristica distintiva dell'indagine OAD è il coinvolgimento delle organizzazioni di minori dimensioni, spesso meno considerate nelle grandi indagini nazionali e internazionali sulla cibersicurezza.
Le piccole e medie organizzazioni costituiscono il 63,67% dei rispondenti all'indagine OAD 2026.
La partecipazione all'indagine è volontaria e totalmente anonima. Il bacino dei rispondenti non costituisce quindi un campione statisticamente rappresentativo dell'intero universo delle organizzazioni italiane, ma permette di individuare criticità, fenomeni ricorrenti e tendenze significative, anche attraverso il confronto con le precedenti edizioni e con altre autorevoli fonti nazionali e internazionali.

Il contributo della Polizia Postale e il quadro nazionale

Il Rapporto comprende uno specifico capitolo realizzato con il contributo del Servizio Polizia Postale e per la Sicurezza Cibernetica, contenente dati e analisi sui crimini informatici in Italia, aggiornati al 30 giugno 2026.
Nel corso del 2025 la Polizia Postale ha investigato 52.590 eventi criminosi, mentre il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC) ha gestito oltre 9.000 eventi informatici di rilevante entità e diramato più di 50.000 alert di sicurezza.
Questi dati, insieme alle evidenze dell'ACN e dell'ENISA, contribuiscono a delineare uno scenario nel quale la sicurezza digitale assume una rilevanza strategica per la tutela delle imprese, delle istituzioni e dei cittadini.

OAD evolve: oltre all'indagine annuale ora anche una rubrica online e una comunità permanente sulla sicurezza digitale

L'edizione 2026 segna anche un'importante evoluzione dell'iniziativa OAD.
All'indagine e al Rapporto annuale si affiancano la nuova Comunità OAD, la rubrica periodica OAD Insight, il gruppo OAD su LinkedIn e il rinnovato sito web, con l'obiettivo di creare un ecosistema collaborativo di informazione, sensibilizzazione e confronto sui temi della sicurezza digitale.

L'intento è quello di mantenere alta durante tutto l'anno l'attenzione sui rischi digitali e sulle misure di prevenzione e contrasto, coinvolgendo non soltanto gli specialisti del settore, ma anche i vertici delle organizzazioni e tutti gli utilizzatori delle tecnologie digitali.

Rapporto OAD 2026 e il webinar di presentazione

Il Rapporto si articola in 144 pagine, otto capitoli e otto allegati, con numerosi grafici, approfondimenti e una sintesi direzionale in italiano e in inglese.
È arricchito dalle prefazioni di:

- Massimo Di Virgilio, Presidente FIDAInform;
- Ivano Gabrielli, Direttore del Servizio Polizia Postale e per la Sicurezza Cibernetica;
- Antonio Piva, Presidente AICA.

La presentazione ufficiale del Rapporto OAD 2026 si terrà mercoledì **2 dicembre 2026, dalle ore 17.00 alle 19.00**, nell'ambito del webinar: "Cibersicurezza a 360°: i risultati dal Rapporto OAD 2026 e la Comunità OAD".
All'illustrazione dei principali risultati dell'indagine seguirà una tavola rotonda con rappresentanti del mondo associativo e professionale. La partecipazione è gratuita, previa registrazione.

- Download gratuito del Rapporto OAD 2026: https://www.oadweb.it/it/oad-2026/rapporto-oad-2026-pubblicato-e-scaricabile.html
- Registrazione al webinar del 2 dicembre 2026: https://attendee.gotowebinar.com/register/8557331232870785625

Informazioni e contatti

OAD, Osservatorio Attacchi Digitali in Italia

E-mail: oad@oadweb.it

Sito web: www.oadweb.it