

SEI QUI: [Home](#) » [Featured](#) » Per capire la cybersecurity italiana servono anche i tuoi dati: partecipa a OAD 2026

Per capire la cybersecurity italiana servono anche i tuoi dati: partecipa a OAD 2026

BY REDAZIONE LINEAEDP – 08/09/2026 ⌚ 6 MINS READ

 Facebook

 Twitter

 LinkedIn



Al via la fase conclusiva dell'indagine sugli attacchi digitali alle organizzazioni italiane: più partecipazione significa una fotografia più rappresentativa di rischi, difese e criticità della sicurezza ICT



Foto di Daniel Roberts da Pixabay

[L'indagine OAD 2026](#) entra nella fase conclusiva della compilazione del questionario online. Ogni nuova organizzazione partecipante contribuisce a rendere più rappresentativa la fotografia degli attacchi digitali e delle misure di sicurezza in Italia. E da quest'anno il progetto continua durante tutto l'anno attraverso Comunità OAD e OAD Insight.

Quanti attacchi digitali colpiscono realmente le organizzazioni italiane? Quali sono i più diffusi? Quali riescono ad avere un impatto significativo? E, soprattutto, quali misure di sicurezza sono effettivamente adottate nelle imprese e negli enti del nostro Paese? Non è semplice rispondere. Le statistiche disponibili sulla cybersecurity sono numerose, ma dipendono inevitabilmente dal punto dal quale il fenomeno viene osservato: incidenti denunciati alle autorità, attacchi rilevati dai fornitori di servizi di sicurezza, malware intercettati, vulnerabilità, eventi gestiti dai SOC, sinistri assicurativi oppure casi divenuti pubblici. Tutte informazioni importanti. Ma per comprendere meglio il fenomeno serve anche un altro punto di osservazione: **quello delle organizzazioni che ogni giorno utilizzano e devono proteggere i propri sistemi informativi.**

È da questa esigenza che, ormai diciannove anni fa, è nato **OAD**, Osservatorio Attacchi Digitali in Italia.

Una fotografia costruita direttamente dalle organizzazioni

OAD raccoglie direttamente da aziende ed enti operanti in Italia informazioni sugli attacchi digitali intenzionali rilevati e sulle misure di sicurezza adottate. La compilazione è anonima e aperta a organizzazioni di qualsiasi dimensione e settore, dalle grandi imprese alle PMI e microimprese, fino alle Pubbliche Amministrazioni. È importante sottolineare un aspetto: **non occorre avere subito un attacco per partecipare.** Sapere quante organizzazioni non hanno rilevato incidenti, quali sistemi utilizzano e quali misure di protezione hanno adottato è altrettanto importante per comprendere il fenomeno. È proprio l'insieme delle risposte, provenienti da realtà differenti, che consente di trasformare singole esperienze in una fotografia complessiva. Per questo **la numerosità e, soprattutto, la varietà dei partecipanti costituiscono un elemento fondamentale dell'indagine.**

Settembre 2026: la fase della compilazione del questionario per concludersi

L'edizione OAD 2026 sta entrando nella fase conclusiva della raccolta dei dati dalle compilazioni del questionario online. L'obiettivo ora è ampliare ulteriormente la base delle organizzazioni rappresentate, coinvolgendo aziende ed enti di dimensioni, settori e territori differenti. **Ogni nuova compilazione aumenta il valore dell'indagine.** Questo vale in particolare per le piccole e medie organizzazioni, che costituiscono una componente fondamentale del tessuto economico italiano ma che non sempre trovano adeguata rappresentazione nelle statistiche internazionali sulla cybersecurity. Partecipare significa quindi mettere a disposizione, in maniera anonima, una piccola parte della propria esperienza per contribuire alla costruzione di una conoscenza comune.

Non soltanto fornire dati: un'occasione per interrogarsi sulla propria sicurezza

Il questionario OAD 2026 è stato profondamente riprogettato e semplificato rispetto alle edizioni precedenti. Durante la compilazione vengono considerate le principali tipologie di attacco e tecniche utilizzate, insieme alle diverse famiglie di misure di sicurezza tecniche e organizzative. Questo trasforma il questionario anche in un piccolo esercizio di consapevolezza. Domande apparentemente semplici possono portare a interrogarsi, ad esempio, sull'effettiva copertura della propria autenticazione multifattoriale, sulla gestione delle vulnerabilità, sui backup, sulla protezione delle reti, sulla formazione degli utenti o sui processi organizzativi utilizzati per gestire la sicurezza.

Per chi completa anche le sezioni opzionali sulle misure adottate, il questionario restituisce una **macro-valutazione qualitativa del livello di sicurezza digitale** e un riepilogo delle principali criticità individuate sulla base delle risposte fornite.

Si crea quindi un piccolo circolo virtuoso: **fornire informazioni all'Osservatorio, confrontarsi con le misure di sicurezza considerate e ricevere una prima indicazione sul proprio livello di protezione.**

Ma OAD 2026 non termina con il questionario

Una delle principali novità dell'edizione 2026 è proprio questa. OAD non vuole più essere soltanto un'indagine che raccoglie dati e pubblica un rapporto annuale. Sta diventando un **ecosistema collaborativo permanente sulla sicurezza digitale**, articolato intorno all'indagine, al Rapporto OAD, alla Comunità OAD, al Gruppo OAD su LinkedIn e alla nuova rubrica **OAD Insight**. L'obiettivo è mantenere vivo durante l'intero anno quel processo di condivisione della conoscenza che l'indagine contribuisce ad alimentare.

La Comunità OAD è aperta a professionisti, aziende, enti, associazioni e più in generale a chiunque sia interessato ai temi della sicurezza digitale. Non ha finalità commerciali e consente di ricevere aggiornamenti selezionati sulle iniziative OAD, sui temi di maggiore attualità e, progressivamente, sulle evidenze che emergono dall'Osservatorio.

Dai numeri agli insegnamenti: OAD Insight

La conoscenza della sicurezza digitale non deriva soltanto dalle statistiche. Deriva anche dalla capacità di analizzare gli incidenti e capire quali insegnamenti possano essere applicati alla propria organizzazione. È la funzione di **OAD Insight**, la nuova rubrica che propone periodicamente brevi approfondimenti dedicati alternativamente alle tecniche di sicurezza e all'analisi di attacchi realmente avvenuti. Gli ultimi contributi, ad esempio, hanno affrontato due problemi estremamente attuali.

Il primo riguarda l'**outsourcing della cybersecurity**: affidarsi a operatori specializzati può consentire anche alle organizzazioni più piccole di accedere a competenze e capacità difficilmente sostenibili internamente, ma non deve trasformarsi in una delega della responsabilità sulla sicurezza.

Il secondo parte dal caso **Arup**, nel quale una sofisticata frode basata su deepfake ha utilizzato una falsa videoconferenza per convincere un dipendente a disporre trasferimenti milionari. Un episodio che dimostra come, nell'era dell'intelligenza artificiale generativa, non sia più sufficiente domandarsi se un volto o una voce sembrano autentici: devono essere i processi organizzativi a garantire la sicurezza della transazione.

Sono esempi diversi, ma accomunati dalla stessa logica: **conoscere ciò che accade agli altri per migliorare la propria capacità di prevenzione.**

Più partecipazione, più conoscenza

È questo il filo che unisce oggi le diverse iniziative OAD. Le organizzazioni partecipano all'indagine e contribuiscono a costruire una base informativa indipendente. I dati vengono analizzati e restituiti attraverso il Rapporto OAD. La Comunità mantiene aperto il confronto. Gli OAD Insight trasformano tecniche, incidenti e casi concreti in occasioni di approfondimento.

Perché tutto questo produca valore, però, **il primo ingrediente continua ad essere la partecipazione.**

Per questo, mentre **OAD 2026 si avvicina alla conclusione della fase di compilazione del questionario online, assolutamente anonimo**, l'invito rivolto a CIO, CISO, responsabili ICT, professionisti e organizzazioni è semplice: **compilate il questionario OAD 2026 e diffondetelo presso colleghi, clienti, fornitori e interlocutori che possano contribuire all'indagine.**

Non serve essere vittime di un attacco. Serve conoscere sufficientemente la propria realtà informatica ed essere disponibili a contribuire, anonimamente, alla costruzione di una fotografia più ampia della sicurezza digitale italiana. E per continuare a
ecipare anche dopo il questionario è possibile **entrare nella Comunità OAD e**

seguire gli OAD Insight. Perché più esperienze riusciamo a mettere in comune, **più accurata sarà la fotografia. E più utile sarà la conoscenza che potremo restituire.**

Per partecipare a OAD 2026

- **Compila il questionario OAD 2026:** <https://www.oadweb.it/LimeS2026/index.php/173435?lang=it>
- **Entra nella Comunità OAD:** <https://www.oadweb.it/it/comunita-oad.html>
- **Segui OAD Insight:** <https://www.oadweb.it/it/comunita-oad/oad-insight.html>
- **Partecipa al Gruppo OAD su LinkedIn:** <https://www.linkedin.com/groups/3862308/>
- **Condividi l'iniziativa con chi può contribuire all'indagine.**

A cura di Marco R. A. Bozzetti – Ideatore e coordinatore OAD

cybersecurity OAD 2026



REDAZIONE LINEAEDP



LineaEDP è parte di BitMAT Edizioni, una casa editrice che ha sede a Milano con copertura a 360° per quanto riguarda la comunicazione rivolta agli specialisti dell'Information & Communication Technology.

CORRELATI