L'INDAGINE

Cyber attacco costante alle aziende italiane: i dati OAD

Secondo il Rapporto OAD 2024 di AIPSI, il 72,4% delle aziende italiane ha subito attacchi informatici nel 2023. Le minacce più comuni includono malware, ransomware e attacchi alla supply chain, con impatti significativi sui sistemi informativi

Pubblicato il 25 nov 2024

Marco R. A. Bozzetti

Presidente AIPSI – Associazione Italiana Professionisti Sicurezza Informatica, Founder e CEO Malabo srl

A IPSI[1] ha appena pubblicato il Rapporto OAD[2] 2024 che giunge al diciassettesimo anno di indagini consecutive sugli attacchi digitali e sulle misure di sicurezza dei sistemi informativi in Italia, avvalendosi, come negli anni

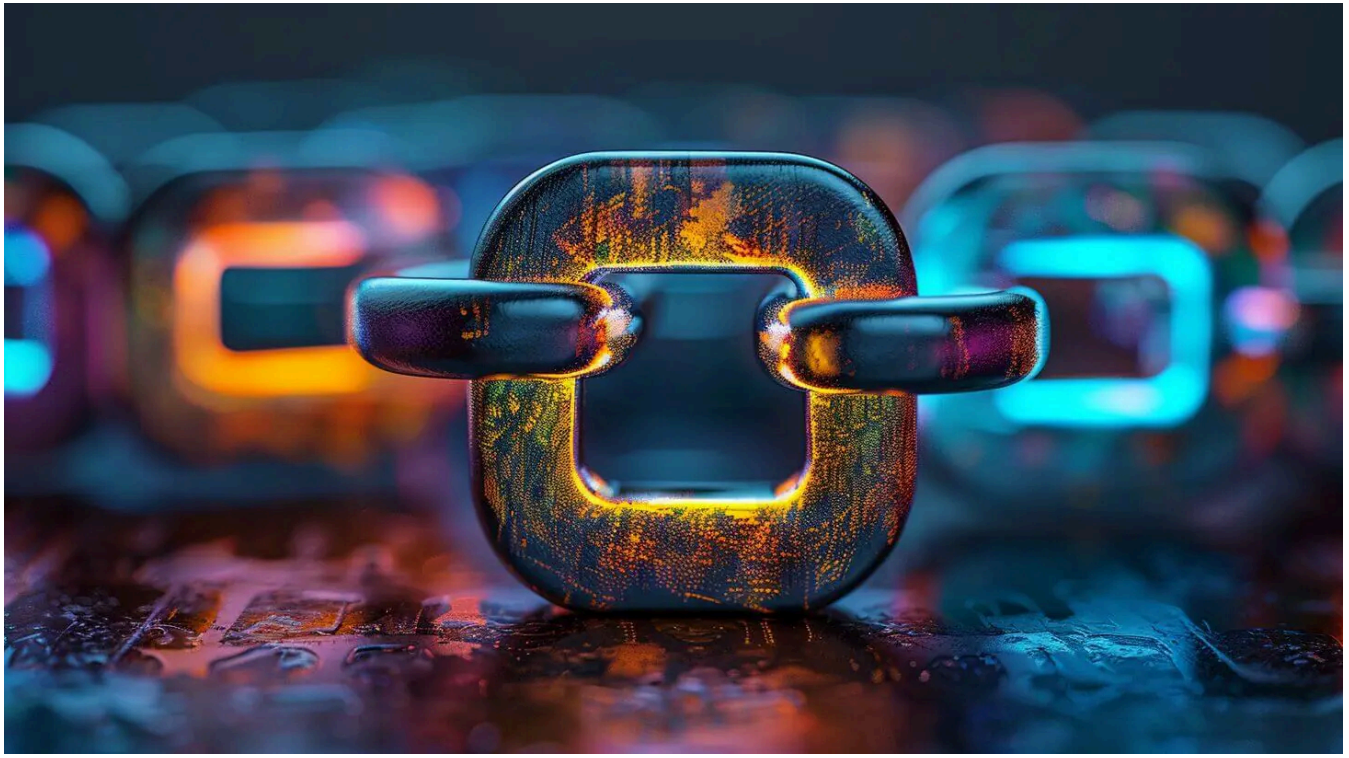
precedenti, della preziosa collaborazione della Polizia Postale, che ha fornito dati e testo del Capitolo 8 del Rapporto, oltre che di FidaInform[3] e di AICA[4].

Indice degli argomenti

L'indagine OAD 2024 di AIPSI

L'indagine **OAD 2024** fa riferimento agli attacchi intenzionali rilevati nell'intero anno 2023**,** ed evidenzia il **permanere di una larga e grave diffusione di attacchi digitali** con forti impatti sui sistemi informativi (SI) delle aziende ed enti rispondenti.

WHITEPAPER



Come evolvono gli attacchi cyber in Italia: le indagini OAD di AIPSI

1 Agosto 2024

di **Marco Rodolfo Alessandro Bozzetti**

Il Rapporto ha due significative prefazioni, quella del Direttore della Polizia Postale, dott. Ivano Gabrielli, e quella del Coordinatore tecnico del Dipartimento per la trasformazione digitale della Presidenza del Consiglio

dei Ministri, ing. Alessandro Musumeci, che testimoniano l'importanza e l'autorevolezza del Rapporto OAD 2024 di AIPSI.

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

- dal sito di AIPSI: **https://www.aipsi.org/aree-tematiche/osservatorio-attacchi-digitali/oad-2024/rapporto-oad-2024-pubblicato-e-scaricabile.html**
- dal sito di OAD: **https://www.oadweb.it/it/**, dal quale si possono scaricare anche i precedenti Rapporti OAD pubblicati
- dal sito di Malabo Srl: **https://www.malaboadvisoring.it/it/**

Il bacino di aziende/enti rispondenti emerso dall'indagine copre tutti i settori merceologici, incluse le Pubbliche Amministrazioni, anche se i più numerosi, in percentuale, sono il settore **Istruzione** con il **23,6%**, il settore **Servizi Professionali e di supporto alle aziende** (avvocati, commercialisti, notai, etc.) con il **12,3%,** il settore **Industria manifatturiera e costruzioni** con l'**11%**.

In termini di dimensioni, come numero di dipendenti, hanno risposto il **69,8%** di piccole e medie organizzazioni, ossia quelle con meno di 250 dipendenti. Significativa, tra queste, il **22,9%** di organizzazioni con meno di 10 dipendenti, che in Italia costituiscono la stragrande maggioranza delle imprese, ma che non sono normalmente considerate nelle analoghe indagini a livello nazionale ed internazionale.

Il ruolo del Sistema Informativo per supportare le attività ed i processi dell'impresa pubblica o privata **è essenziale** per il **70,1%** delle aziende/enti rispondenti e per questo motivo la sua sicurezza digitale deve essere di alto livello, efficace ed

efficiente. Il **10,6 %** dei SI fornisce **servizi essenziali** per l'Italia, soggetti quindi al NIS e nel prossimo futuro alle nuove normative europee NIS2, DORA, etc.

Il questionario on line via web di OAD 2024 ha posto due sole domande sugli attacchi digitali subiti nel 2023 dai Sistemi Informativi delle aziende/enti rispondenti, in modo da poter continuare l'analisi dei trend generali sugli attacchi (che cosa viene attaccato e con quali tecniche) dal 2007 ad oggi[5], ed ha approfondito gli attacchi digitali rilevati nel 2023 **alle applicazioni ed agli ambienti web** ed ai **sistemi OT, Operation Technology**[6].

OAD distingue chiaramente che cosa si attacca, la tipologia d'attacco classificata in 14 diverse macro voci, ed il come si attacca, le tecniche usate per l'attacco e distinte in 7 macro voci (per il dettaglio metodologico si rimanda all'Allegato A, per quanto rilevato dall'indagine al Capitolo 4).

Gli attacchi più diffusi contro le aziende nel 2023

Nel corso dell'intero 2023, il **72,4%** delle aziende/enti rispondenti ha subito attacchi digitali ai propri Sistemi Informativi. Per questi i **tipi di attacchi più diffusi** includono:

- le **modifiche malevoli/non autorizzate ai programmi e alle configurazioni dei sistemi ICT,** con il **31,7%** delle risposte; a questo primo posto sicuramente contribuisce la larghissima diffusione di malware e di ransomware in Italia;
- gli attacchi **DoS/DDoS**, per la saturazione dei sistemi ICT connessi ad Internet, con il **20,7%**; sono stati uno degli attacchi più usati nell'ambito delle cyber warfare, in particolare da parte delle organizzazioni hacker schierate pro Russia;
- l'**uso non autorizzato e malevolo di sistemi ICT del SI**, con il **18,3%**;

- **gli attacchi alla supply chain informatizzata,** con il **15%**; questa è la tipologia di attacco aggiunta alla precedente tassonomia di attacchi di OAD, e il dato conferma la diffusione e la criticità di questa tipologia d'attacco, considerata dal World Economic Forum[7] uno dei principali rischi a livello mondiale;
- Il **furto di dispositivi mobili**, con il **13,4%**, prevalentemente per gli smartphone, che da un lato contengono, talvolta senza protezione alcuna, preziose informazioni dell'identità digitale del proprietario, come le password e le modalità di accesso ai servizi informatici utilizzati, dall'altro hanno un alto valore sul mercato dell'usato. Entrambe motivazioni importanti per il loro furto.

Tutte le altre tipologia d'attacco considerate nella tassonomia OAD hanno percentuali al di sotto del 10% e per la prima volta con OAD 2024 i sistemi di controllo degli accessi (IAA, Identificazione-Autenticazione-Autorizzazione) e gli attacchi alle reti geografiche/locali non sono ai primi posti di questa classifica di diffusione delle varie tipologie di attacco, come lo erano invece nelle precedenti edizioni di OAD.

Le tecniche più usate

Le **tecniche di attacco più diffuse** negli attacchi più gravi vedono ai primi posti:

- l'uso di **più tecniche per lo stesso attacco** con il **40,4%;**
- **raccolta illegale di informazioni**, ottenute tipicamente con il **social engineering**, con il **37,6%**;
- i **codici maligni**, alla base degli assai diffusi attacchi di ransomware, con il **25,3%.**

La correlazione dei dati sugli attacchi rilevati con le dimensioni ed il fatturato delle aziende/enti rispondenti mostra anche per il 2023 che il maggior numero di attacchi digitali, ed i più sofisticati, sono rivolti ad organizzazioni di grandi dimensioni e fatturato. Le piccole e piccolissime organizzazioni, sia private che pubbliche, non rappresentano un

obiettivo di interesse specifico per i cyber criminali negli attacchi mirati, mentre esse possono essere coinvolte in attacchi di massa, come quelli basati sul phishing e sul ransomware.

L'indagine verticale sugli attacchi digitali agli ambienti web

L'approfondimento "verticale" sugli **attacchi ai siti, alle applicazioni e agli ambienti web** si è basato, dal punto di vista tecnico, sulla verifica delle cause degli attacchi più gravi subiti in riferimento alle principali vulnerabilità e rischi indicati a livello mondiale da OWASP[8].

Il **58,4%** delle aziende/enti rispondenti **ha rilevato attacchi alle applicazioni ed agli ambienti web**, e di questi il **60,6%** li ha subiti nei propri ambienti web **in cloud** (ambienti in cloud che dovrebbero essere più sicuri di quelli on premise).

Le vulnerabilità causa di tali attacchi sono state, per gli attacchi più gravi, il **92,3%** di tipo **personale,** che in parte dipendono anche dall'organizzazione (ad esempio dalla non formazione degli utenti), per il **82,7%** di tipo **tecnico.** Con riferimento alle 10 principali vulnerabilità per l'ambiente web di OWASP, per gli attacchi **più gravi** rilevati dalle aziende/enti rispondenti, sono al primo posto i **componenti software obsoleti** e vulnerabili, con il **31,7%**, ed al secondo, con il **20,4%**, **l'errata configurazione degli strumenti di sicurezza.**

L'**impatto** dell'attacco più grave agli ambienti web **a livello tecnico** è stato **pesante** per i SI delle aziende/enti rispondenti, con il **85,3%** dei casi che ha riscontrato un disservizio nel SI durato **da 2 giorni in su**. Anche **l'impatto economico** è stato **significativo,** per il **86,5%** con un **aumento dei costi** sul **budget** del SI, e per il **24% il** ripercuotersi dei costi anche **sul bilancio dell'azienda/ente**.

L'indagine verticale sugli attacchi digitali agli ambienti OT

L'approfondimento "verticale" sugli **attacchi agli ambienti OT**[9] (descritto in §4.3) ha coinvolto solo aziende/enti che hanno dichiarato di utilizzare sistemi OT, il **37%** del totale dei rispondenti: di questi, il **48,2**% ha dichiarato di aver **subito attacchi ai propri sistemi OT**.

L'**impatto** dell'attacco più grave ad un sistema OT è stato molto alto, in termini di blocco del sistema: per **circa 1/3** dei rispondenti il **blocco è durato tra i 2 e 3 giorni**, ma **per quasi la metà è durato più di 3 giorni.** Dato che la maggior parte dei sistemi OT interagisce oggi con applicazioni del SI, il blocco si è propagato anche ad alcune applicazioni del SI, causando **significativi disservizi anche sul SI**: il **40,7%** ha avuto un **blocco tra i 2 e 3 giorni di applicazioni del SI** causate da questo propagarsi.

Le misure di cybersicurezza nei sistemi informativi delle aziende/enti rispondenti

Nel questionario OAD 2024, le domande sulle **misure tecniche, organizzative e di gestione della sicurezza digitale** presenti nei Sistemi Informativi e nelle aziende/enti rispondenti **erano opzionali**: ad esse ha risposto il **35,4%** del totale di rispondenti. Nel capitolo 7 del Rapporto sono riportati i dati emersi sulle misure di sicurezza tecniche ed organizzative, cui si rimanda per i dettagli. Nel complesso la **maggior parte dei rispondenti risulta avere buoni livelli di sicurezza sia fisica che organizzativa che gestionale**. Questo dato positivo è probabilmente dato anche dal fatto che aziende/enti con bassi livelli di sicurezza non hanno compilato la parte opzionale sulle misure di sicurezza,

Alcune carenze sono più diffuse, come è logico, nelle organizzazioni più piccole, soprattutto per gli aspetti organizzativi; anche le piccole organizzazioni utilizzano servizi terziarizzati per la gestione della sicurezza digitale.

A conferma che le aziende/enti rispondenti gestiscono il loro Sistemi Informativi con un buon/elevato livello di sicurezza, vengono elencate alcune percentuali significative emerse :

- per le **misure organizzative** di sicurezza digitale
- l'**81,3%** ha definito ed usa policy e procedure organizzative per la sicurezza digitale;
- il **73,1%** ha policy e procedure per la gestione degli incidenti informatici
- il **50%,** delle aziende/enti rispondenti dichiara di avere un ERT, Emergency Response Team, con definite e in uso le relative procedure organizzative
- il **73,4%** effettua l'analisi dei rischi digitali;
- il **60,9%** effettua auditing per la sicurezza digitale
- il **45,3%** ha certificazioni sulla sicurezza digitale
- per le **misure tecniche** di sicurezza digitale
- Il **60%** dispone di un Data Center in Italia con un elevato livello di affidabilità;
- nell'**80%** dei casi sono previste misure per il controllo dell'**accesso fisico di persone** nei locali con sistemi ICT, a parte l'eventuale Data Center per il quale è dato per scontato che abbia tali misure di controllo;
- l' **86,8%**, dispone di UPS nei locali/computer room, a parte l'eventuale Data Center;
- il **54,3%** gestisce **centralmente le password**;
- **71,6%,** dei SI **controlla centralmente** funzionalità, prestazioni e livelli di sicurezza delle reti;
- il **33,3%** dei software applicativi sviluppati ad hoc hanno seguito procedure e metodiche di **sviluppo sicuro;**
- **l'80%** dei SI usa **FWA**, **Firewall Applicativi;**
- l'**84,7%** gestisce la **manutenzione correttiva** degli applicativi;
- il **63,1%** dichiara di **aver classificato i dati** trattati dalle applicazioni del SI;
- il **44,6%** dei SI effettua il **backup** "a regola d'arte";
- il **75,4%** ha e utilizza **procedure per il ripristino dei sistemi ICT dai dati di backup;**
- per le **misure di gestione e controllo** della sicurezza digitale

- il **l'80%** utilizza sistemi di gestione e di controllo in modalità diverse, e tra questi **16,8%** li ha terziarizzati;
- **78,5%** delle aziende/enti rispondenti effettua l'analisi delle vulnerabilità
- Il **77,9%** archivia i log degli utenti, ed il **50%** li gestisce;
- Il **75%** ha previsto un **Piano di Disaster Recovery** (DR)
  - l'**83,3%** di queste ha previsto o allocato risorse ICT alternative per poterlo realmente attuare.

Questi dati evidenziano che i Sistemi Informativi delle aziende/enti rispondenti si posizionano in gran parte **nella fascia alta** per le misure tecniche ed organizzative di sicurezza digitale implementate: ma nonostante questo hanno subito molti attacchi digitali, che hanno avuto forti impatti in termini di disservizi e di costi per l'intera azienda/ente rispondente e per il suo Sistema Informativo.

Prime conclusioni dai dati emersi dall'indagine

Quanto emerge dall'indagine OAD 2024 è **sostanzialmente allineato** con quanto indicato dal World Economic Forum, da ENISA, l'Agenzia Europea per la cybersicurezza, da ACN, l'Agenzia per la Cybersicurezza Nazionale, e dal Servizio Polizia Postale e per la Sicurezza Cibernetica, che ha fornito ad OAD i dati sul crimine informatico rilevati nel 2023 e nel 1 semestre del 2024, riportati nel Capitolo 8 del Rapporto, cui si rimanda per i dettagli. Inoltre il Capitolo 3 approfondisce la situazione globale degli attacchi digitali con riferimento ai rapporti forniti dagli enti sopracitati.

In estrema sintesi, **nel 2023 permane complessivamente l'ampia diffusione di gravi attacchi digitali e di un forte rischio cibernetico a livello mondiale, europeo e in Italia: e tale situazione sembra essere destinata a continuare anche nel 2024.**

L'anno **2023** ha visto un peggioramento della situazione geopolitica a livello mondiale, con guerre digitali in pieno corso quali l'invasione della Federazione Russa in Ucraina a febbraio 2022 e la difesa di quest'ultima, e la "guerra" tra lo Stato di Israele e Hamas, chiamata anche la guerra di Gaza, causata dall'attacco terroristico del 7 ottobre 2023 ad Israele da parte di Hamas. A fianco di questi due eventi, che sono sola la punta del critico e pericoloso iceberg geopolitico, e che hanno portato innumerevoli attacchi digitali, è fortemente cresciuta la disinformazione e la mala informazione, inizialmente assai preoccupante in Europa soprattutto per le elezioni 2024, e le tecniche di Intelligenza Artificiale (IA) usate in vari strumenti di attacco. Insieme al "tradizionale" crimine informatico, tutto questo ha portato il 2023 ad avere ancora una altissima diffusione di attacchi digitali intenzionali, con gravi impatti sia sul budget del SI sia, in certi casi, sul conto economico dell'azienda/ente rispondente.

La fig. 1 mette a confronto gli attacchi rilevati dalle aziende/enti che hanno risposto negli anni all'indagine OAD. Dal 2016 gli attacchi rilevati dai rispondenti aumentano, e dal 2020 la percentuale delle aziende/enti attaccati supera quella dei non attaccati. Il confronto in figura non ha validità statistica, ma fornisce un chiaro andamento nel tempo del fenomeno attacchi digitali in Italia.

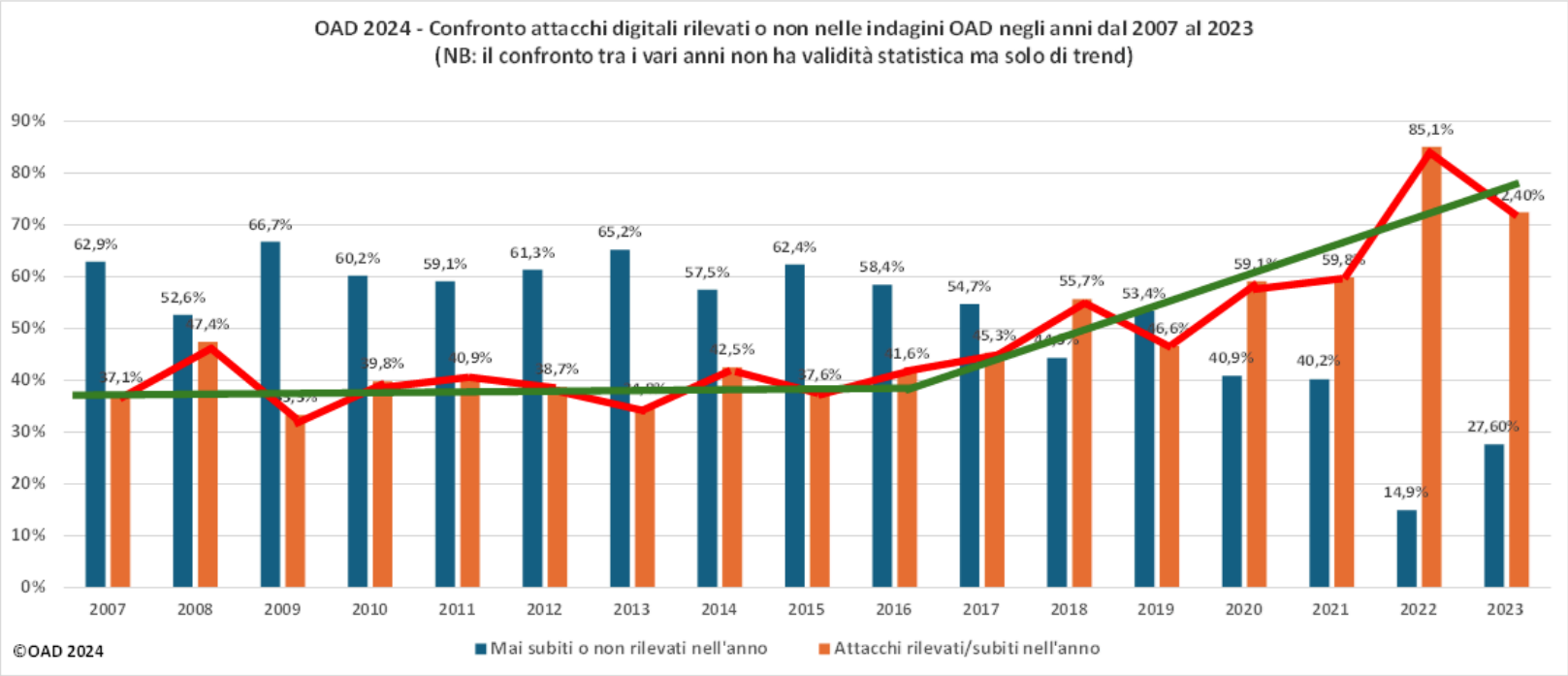


Fig. 1

Come mostra la figura, anche per l'Italia dal 2020 si è entrati nell'**era della insicurezza digitale sistemica** Nonostante le misure di sicurezza implementate, e sovente a caro prezzo, queste non sono state e non sono ancora capaci di bloccare gli attacchi digitali.

Con le misure attualmente a disposizione, che vanno potenziate e non certo dismesse, occorre imparare a gestire questa insicurezza grazie a **politiche di resilienza dell'intera impresa e del suo SI**. Resilienza che lato business può

essere garantita dalla “**business continuity**”, la continuità operativa almeno dei processi fondamentali per il funzionamento dell’impresa; e lato informatico da un piano di **Disaster Recovery** effettivo, attuabile e “provato”.

Note

OT, Operational Technology, definisce un ampio insieme di sistemi ICT per controllare, monitorare ed automatizzare processi fisici ed i dispositivi e le infrastrutture che effettuano e/o supportano tali processi fisici. Tipici esempi di tali processi sono quelli manifatturieri, quelli chimici, quelli nucleari, quelli del controllo del territorio, delle reti di distribuzione dell’energia, e così via. Il concetto di OT è molto ampio ed include i sistemi ICS, Industrial Control System, i robot industriali e di ricerca, i sistemi di diagnostica medica, i sistemi IoT, Internet of Thinks e IIoT, Industrial IoT. ↑

AIPSI, Associazione Italiana Professionisti Sicurezza Informatica, è una associazione di persone fisiche, apolitica e senza fini di lucro, Capitolo Italiano di ISSA, Information Systems Security Association, (**www.issa.org**), la più grande associazione no-profit di professionisti della sicurezza cibernetica nel mondo. Obiettivo principale di AIPSI è aiutare i Soci nella loro crescita professionale e di competenze, tramite un insieme di servizi e di opportunità forniti da AIPSI a livello nazionale e da ISSA a livello internazionale. AIPSI è inoltre impegnata a diffondere la cultura interdisciplinare della sicurezza digitale in Italia e a fornire contributi ai vari tavoli istituzionali in materia. Per i vari servizi offerti e le iniziative organizzate da AIPSI si veda il sito **https://www.aipsi.org/** ↑

OAD costituisce l’unica indagine indipendente online VIA WEB in Italia 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. Dato il numero di risposte raccolte e la loro distribuzione tra aziende ed enti pubblici di varie dimensioni e appartenenti a diversi settori merceologici, l'indagine OAD fornisce preziose indicazioni sul fenomeno degli attacchi digitali intenzionali in Italia e delle misure di sicurezza in essere nei sistemi informativi delle imprese rispondenti. OAD riesce a coinvolgere nell'indagine anche le piccole e piccolissime realtà, che costituiscono in Italia la stragrande maggioranza e che le altre indagini nazionali ed internazionali difficilmente considerano ed analizzano. L'indagine OAD è ideata e realizzata per conto di AIPSI da Malabo Srl, la società di consulenza direzionale sull'ICT dell'autore (**https://www.malaboadvisoring.it**). ↑

Fidainform, Federazione Nazionale delle Associazioni Professionali di Information Management, è la federazione di varie associazioni italiane no profit e di sole persone che si occupano della tecnologia dell'informazione, molte delle quali operanti a livello regionale. Si propone come "nodo" attivo del Sistema-Paese per lo sviluppo del settore ICT. ↑

AICA, Associazione Italiana per l'Informatica e il Calcolo Automatico, è l'associazione italiana senza scopo di lucro di cultori e professionisti ICT per lo sviluppo e la diffusione delle conoscenze digitali. Tra le varie sue iniziative, ha realizzato a livello europeo l' ICDL e l'eCF (UNI EN 16234-1:2016): per quest'ultimo è accreditata come ente certificatore. ↑

Per un confronto ed una analisi dei trend emersi dalla varie indagini OAD, fino a quelle del 2023, si veda l'articolo: **https://www.agendadigitale.eu/sicurezza/evoluzione-degli-attacchi-digitali-in-italia-lanalisi-delle-indagini-oad-di-aipsi/** ↑

OT, Operational Technology, definisce un ampio insieme di sistemi ICT per controllare, monitorare ed automatizzare processi fisici ed i dispositivi e le infrastrutture che effettuano e/o supportano tali processi fisici. Tipici esempi di tali processi sono quelli manifatturieri, quelli chimici, quelli nucleari, quelli del controllo del territorio, delle reti di

distribuzione dell'energia, e così via. Il concetto di OT è molto ampio ed include i sistemi ICS, Industrial Control System, i robot industriali e di ricerca, i sistemi di diagnostica medica, i sistemi IoT, Internet of Thinks e IIoT, Industrial IoT. ↑

https://www.weforum.org/reports/global-risks-report-2023/ ↑

OWASP, Open Web Application Security Project, iniziativa che formula a livello mondiale linee guida, strumenti e metodologie per migliorare la sicurezza delle applicazioni in ambito web. ↑

Valuta la qualità di questo articolo

B

Marco R. A. Bozzetti

Presidente AIPSI – Associazione Italiana Professionisti Sicurezza Informatica, Founder e CEO Malabo srl

Seguimi su

11 Nov 2024

Argomenti

R ransomware T trasformazione digitale Tutto su Cyber Security

Canali

S Sicurezza digitale

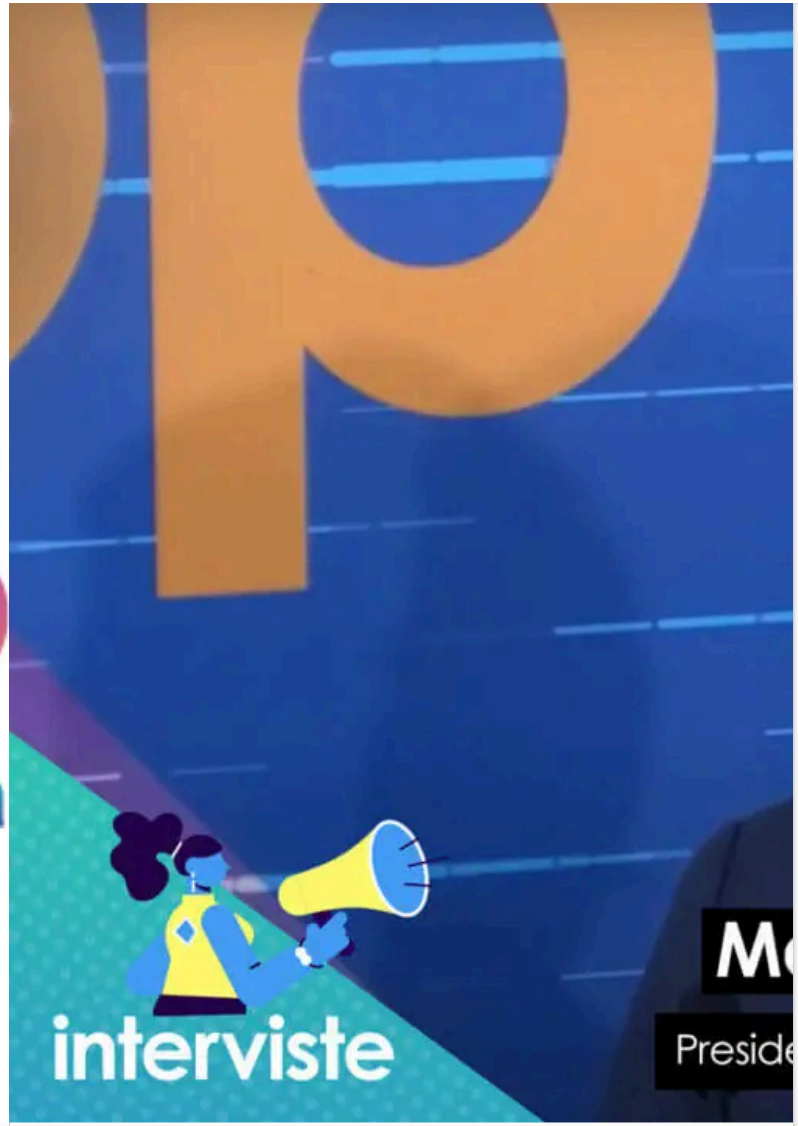
EU Stories - La coesione innova l'Italia

EU STORIES
La coesione innova l'Italia

Filtra per topic

TORIES

La coesione innova l'Italia



IS

INTERVISTE

Marco De Giorgi (PCM): "Come comunicare

Articoli correlati

INTELLIGENZA ARTIFICIALE

La "voce" dell'AI è femmina? Ma è sessismo

01 Ago 2024

di **Marco Ongaro**

Condividi

GESTIONE DELLA QUALITÀ

ISO 9001:2015/Amd 1:2024: guida pratica alle modifiche per la gestione del cambiamento climatico

25 Giu 2024

di **Monica Perego**

Condividi

L'ANALISI DI BERTELÈ

Trimestrali Meta, Microsoft e Google: che ci dicono sul prossimo futuro

26 Apr 2024

di **Umberto Bertelè**

Condividi

INTELLIGENZA ARTIFICIALE

La “voce” dell’AI è femmina? Ma è sessismo

Al casello dell’autostrada, una voce femminile guida gli utenti, simbolo di un trend globale che vede assistenti vocali sempre più femminilizzati. Da Emma, doppiatrice italiana, a Sky, chatbot di OpenAI, l'articolo esplora come la robotica sfrutti la femminilità, sollevando questioni di stereotipi e integrazione uomo-macchina

Pubblicato il 1 ago 2024

CONTINUA A LEGGERE

22 Mag 2024

GESTIONE DELLA QUALITÀ

ISO 9001:2015/Amd 1:2024: guida pratica alle modifiche per la gestione del cambiamento climatico

L'emendamento ISO 9001:2015/Amd 1:2024 introduce modifiche per affrontare il cambiamento climatico nei sistemi di gestione della qualità. Le applicazioni delle nuove disposizioni, le implicazioni sui requisiti di contesto e parti interessate, e come le aziende possono integrare queste misure per migliorare l'efficienza e ridurre i costi

Pubblicato il 25 giu 2024

16 Set 2024

11 Nov 2024

Trimestrali Meta, Microsoft e Google: che ci dicono sul prossimo futuro

I colossi della tecnologia Meta, Microsoft e Alphabet-Google hanno presentato i risultati finanziari del loro ultimo trimestre fiscale, mostrando una crescita impressionante. Nonostante questo, le reazioni di Wall Street sono state diverse, influenzate da prospettive future e investimenti in intelligenza artificiale

Pubblicato il 26 apr 2024

CONTINUA A LEGGERE

INFOGRAFICA

Il modello delle competenze AI Marketing DNA

17 Set 2024

08 Ott 2024