Webinar presentazione Rapporto OAD 2025
22/10/2025

"Intelligenza Artificiale e Cibersicurezza: cosa emerge dal Rapporto OAD 2025"

1

Marco R. A. Bozzetti
Presidente Onorario AIPSI (m.bozzetti@aipsi.org)
Founder e CEO Malabo srl (www.malaboadvisoring.it)

1

AIPSI, capitolo italiano della mondiale ISSA

- Associazione no-profit di **sole persone fisiche**
- Obiettivo principale: **l'indirizzamento e la crescita professionale dei suoi Soci**
- Tre tipologie di Socio:
  - AIPSI-ISSA (US$ 160,00 /anno)
  - SOLO AIPSI (€ 50,00/anno)
  - AIPSI GIOVANE (fino a 26 anni: primo anno gratuito, poi € 25,00/anno)
  - Si veda: https://www.aipsi.org/associazione/come-associarsi.html
- Socio FIDAInform

- **Servizi riservati a tutti i Soci AIPSI**
  - **supporto alle certificazioni**, in particolare per **eCF Plus** (EN 16234-1:2016) per profili sulla sicurezza digitale con **forti sconti con AICA**
  - **Mentoriship gratuita sull'indirizzamento e sulla crescita professionale**
  - **SIG di approfondimento e discussione**:
    - AI e Cybersec
    - Crescita professionale Soci
  - ***Network Soci a livello nazionale***

2

- **Servizi riservati ai Soci AIPSI-ISSA**
  - **ISSA Journal**
  - **ESG ISSA Survey "The Life and Times of Cyber Security Professionals"**
  - Convegni, workshop, webinar in inglese
  - Corsi online in inglese
  - **SIG, Special Interest Group**
    - Privacy
    - Women in Security
  - **Accordi con sconti per certificazioni individuali**
  - ***Network Soci a livello mondiale***

2

L'indagine OAD/OAI dal 2007 ad oggi

- **18 anni consecutivi di indagini**
  - basate su questionari online anonimi
  - libero accesso al questionario per i referenti di un sistema informativo operante in Italia
- **Per tutti i settori merceologici + Pubbliche Amministrazioni Centrali e Locali**
- **14 Rapporti pubblicati**
- **Specifico sito web** ww.oadweb.it

3

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.

3

Il Rapporto OAD 2025

4

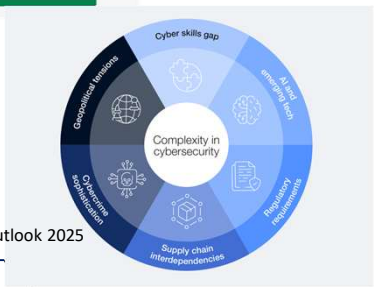
- Il **Rapporto OAD 2025** è di 185 pagine A4, strutturato in 8 Capitoli con l'elaborazione e l'analisi dei dati emersi dall'indagine e in 8 Allegati
- **Prefazioni** di:
  - Massimo Di Virgilio, Presidente FIDAInform
  - Ivano Gabrielli, Direttore del Servizio Polizia Postale e per la Sicurezza Cibernetica
  - Antonio Piva, Presidente AICA
- Nel Capitolo 8 sono riportati i dati forniti dal Servizio Polizia Postale e per la Sicurezza Cibernetica.
- Il Rapporto fornisce nei Capitoli 1 ed 1bis l'Executive Summary in italiano e in inglese.
- Con la collaborazione di: AICA, FidaInform, Malabo Srl, Servizio Polizia Postale e per la Sicurezza Cibernetica

Rapporto OAD 2025 liberamente scaricabile da: https://www.aipsi.org/aree-tematiche/osservatorio-attacchi-digitali/oad-2025/per-scaricare-il-rapporto-oad-2025.html

4

Il quadro degli attacchi/rischi digitali a livello mondiale

World Economic Forum Global Risks Perception Survey 2024-2025



World Economic Forum Global Cybersecurity Outlook 2025

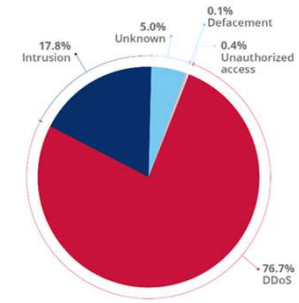
5

www.aipsi.org
www.issa.org

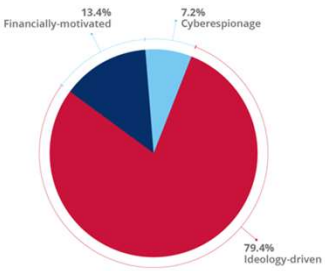
5

Da ENISA

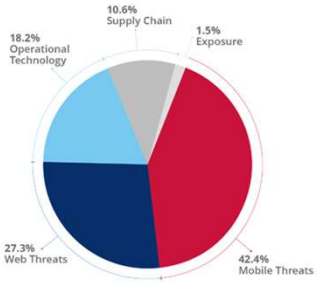
Macro tipologia attacchi in UE



Motivazioni attacchi in UE



In quali ambiti attacchi in UE



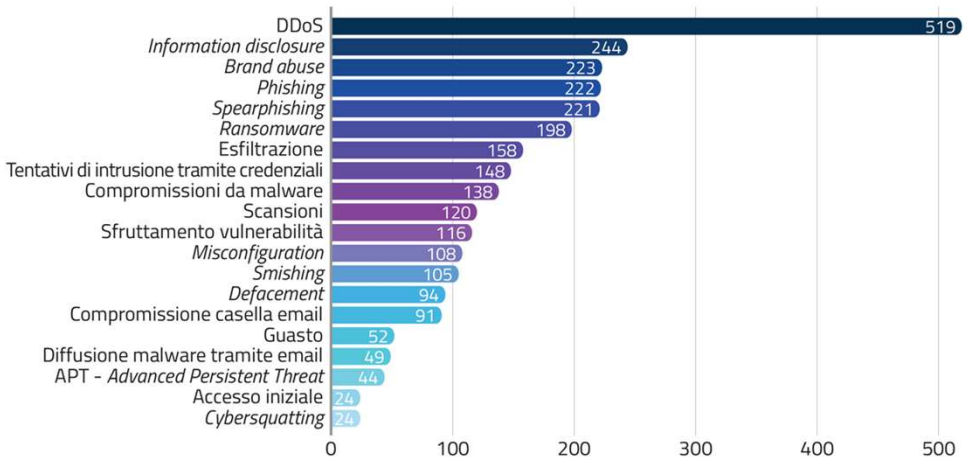
Fonte: ENISA ETL 2025

6

www.aipsi.org
www.issa.org

6

Da ACN: più importanti attacchi rilevati in Italia da CSIRT-ACN nel 2024



7

7

OAD 2025: Computer crime (dati Polizia Postale)

Protezione strutture critiche/essenziali	1 gen - 30 giugno 2025	1 gen - 31 dic 2024	1 gen - 31 dic 2023	1 gen - 31 dic 2022	1 gen - 30 apr 2021	1 gen - 31 dic 2020	1 gen - 31 dic 2019	1 gen – 31 dic 2018	1 gen – 31 dic 2017	1 gen – 31 dic 2016
Attacchi rilevati (*)	4.911 **	12.058 **	12.101 **	13.099	282	509	1181	459	1.032	844
Alert diramati	22.990	59.875	77.012	113.420	24.824	83.416	82.484	80.777	31.524	6.721
Indagini avviate	n.d.	n.d.	96	110	34	103	155	74	72	70
Persone denunciate/indagate (*)	49 **	178 **	224**	334	n.d.	105	117	14	1.316	1.226
Richiesta di cooperazione internazionale in ambito Rete 24/7 High Tech Crime G8 (Convenzione Budapest)	21	63	79	77	17	69	79	108	83	85

* Target: Infrastrutture Critiche (I.C.), Operatori Servizi Essenziali (OSE), Pubbliche Amministrazioni Locali (PAL), Aziende, Privati
** Dati aggregati C.N.A.I.P.I.C. e Centri Operativi per la Sicurezza Cibernetica (C.O.S.C.).

Cyber Terrorismo	1 gen -30 giugno 2025	1 gen - 31 dic 2024	1 gen - 31 dic 2023	1 gen - 31 dic 2022	1 gen - 30 apr 2021	1 gen - 31 dic 2020	1 gen - 31 dic 2019	1 gen – 31 dic 2018
Spazi web monitorati	101.683	295.493	182.209	175.572	11.962	37.081	36.377	36.000
Spazi Virtuali con contenuti illeciti rilevati	983	4.642	2.037	1.598				
Spazi oscurati per attiv. infoinvestigative	275	2.369	2.700	338				

8

Frodi informatiche	1 gen -30 giugno 2025	1 gen - 31 dic 2024	1 gen - 31 dic 2023	1 gen - 31 dic 2022
Casi trattati	4.116	8.602	10.755	5.908
Persone indagate	379	923	927	725
Somme sottratte (€)	28.466.633	48.674.917	40.503.616	35.509.160

Truffe online	1 gen -30 giugno 2025	1 gen - 31 dic 2024	1 gen - 31 dic 2023	1 gen - 31 dic 2022
Casi trattati	9.261	18.967	16.637	15.699
Persone indagate	1.950	3.627	3.610	3.570
Somme sottratte (€)	109.235.401	183.377.101	139.536.457	116.454.550

- **truffa online** induce in errore la vittima tramite "artifizi e raggiri" per ottenere un profitto
- **frode informatica** consiste nella manipolazione e alterazione di un sistema informatico o telematico, o nell'intervento non autorizzato su dati e programmi al suo interno, per ottenere un ingiusto profitto.

8

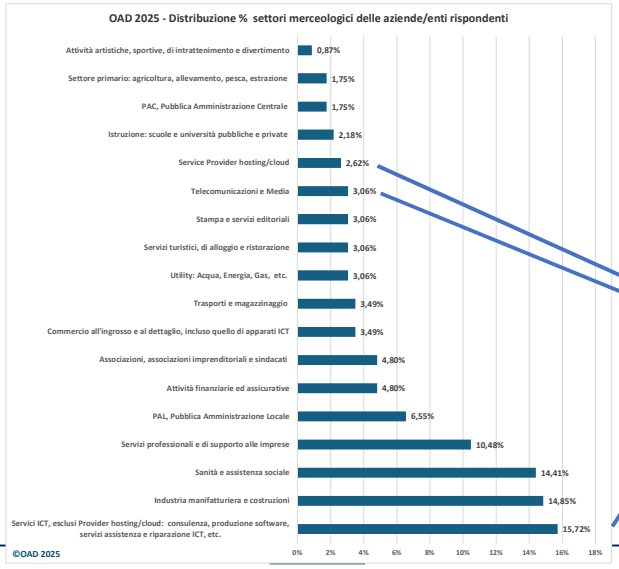
9

Dall'indagine OAD 2025

www.aipsi.org
www.issa.org

9

OAD 2025: Settore merceologico delle aziende/enti rispondenti



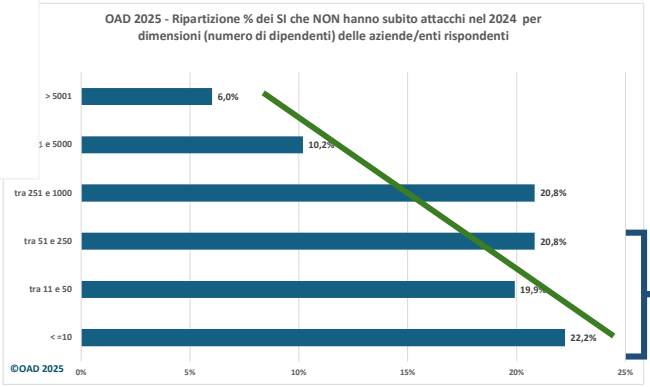
ICT 21,40%

www.issa.org

10

10

OAD 2025: attacchi digitali rilevati e correlati alla dimensione dell'azienda/ente rispondente (# addetti)



Numero addetti	Numero imprese	% aziende/classe addetti
0-9	4.469.118	94,8%
10-49	214.793	4,6%
50-249	27.223	0,6%
da 250 in su	4.619	0,1%
Totale imprese	4.715.753	
Totale PMI	4.711.134	99,9%

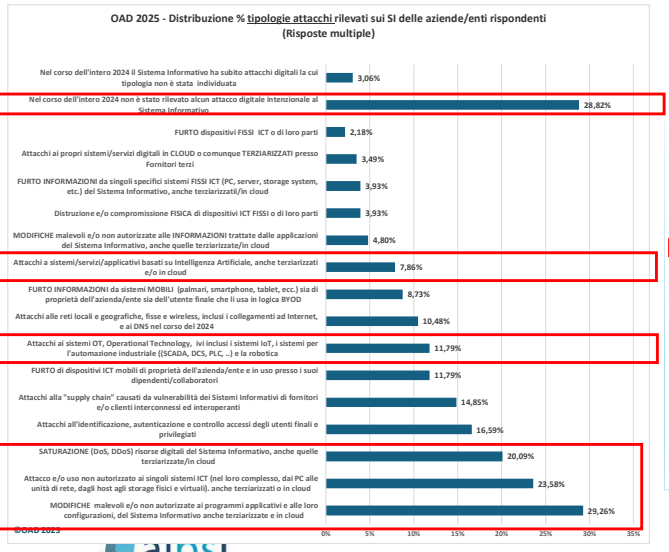
11

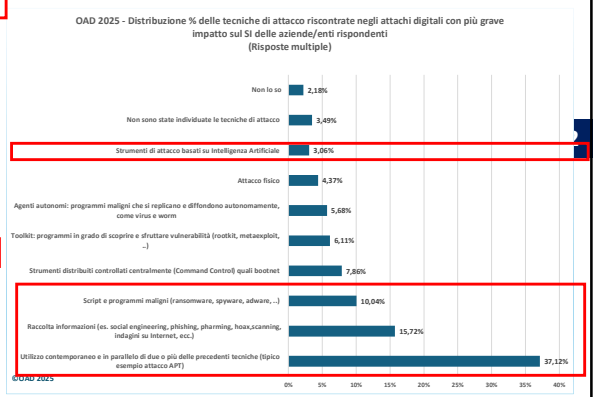
63%

www.aipsi.org
www.issa.org

11

OAD 2025: Tipologie e tecniche di attacco più diffuse tra i rispondenti



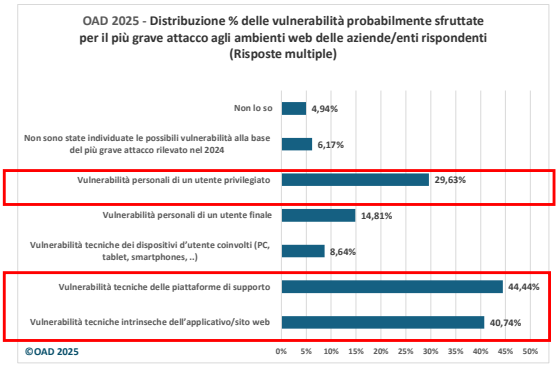


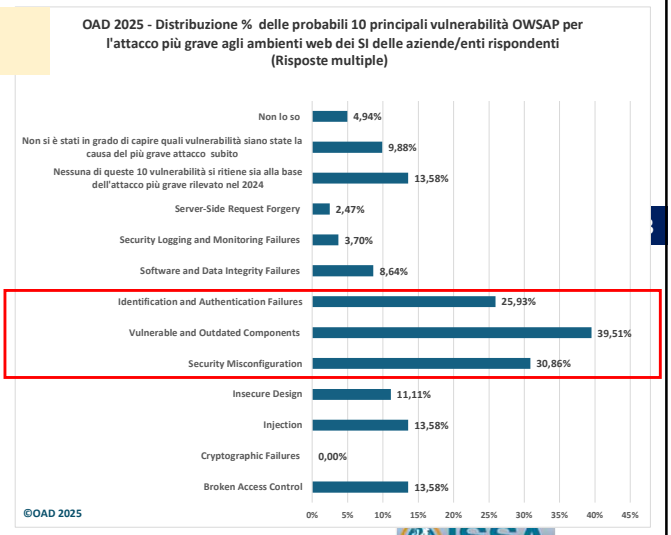
www.aipsi.org
www.issa.org

12

OAD 2025: attacchi agli ambienti web

- **94,15%** usa sistemi web in locale e/o terziarizzati
- **64,29%** ha subito interruzioni del servizio per ≥2 giorni

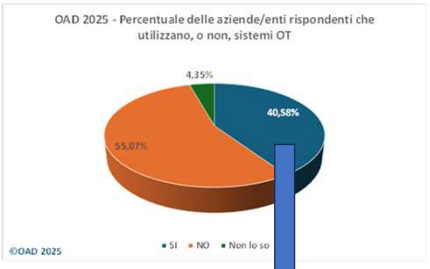


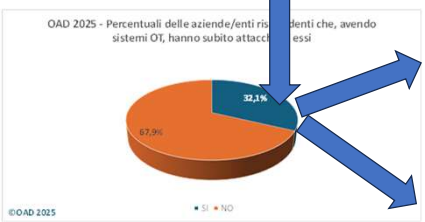


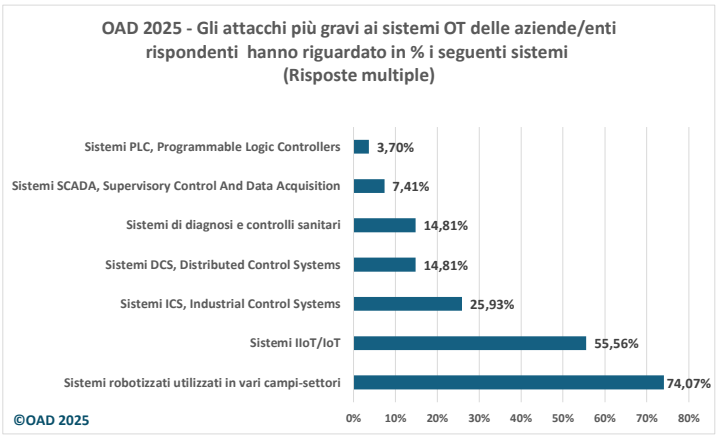
www.aipsi.org
www.issa.org

13

OAD 2025: attacchi agli ambienti OT, Operational Technology







- **Blocco** sistema è durato **più di 2 giorni** per **> 85%**
- **Impatto sul SI → blocco 2-3 g** per **30%**

www.aipsi.org
www.issa.org

14

L’era dell’Intelligenza Artificiale

15

15

IA Generativa e LLM

IA Generativa

crea contenuti come immagini, video, musica, audio e testo basandosi su **modelli di deep learning** addestrati su grandi set di dati.

- Il deep learning è una tecnica di **machine learning** per l'analisi e l'interpretazione di grandi volumi di dati basata su **reti neurali**
- Il **trasformatore** è un tipo di rete neurale in grado di elaborare il linguaggio più rapidamente, ed è usato per LLM
- I principali scenari di utilizzo dell'IA generativa sono chatbot, creazione ed editing di immagini, assistenza alla stesura di codice software, supporto alle decisioni e alla ricerca scientifica.

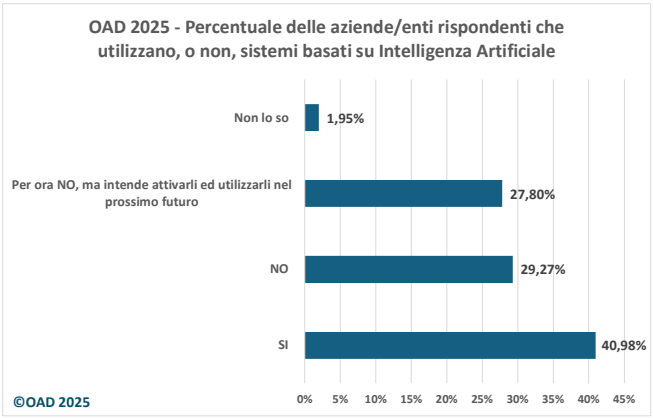
LLM, Large Language Model

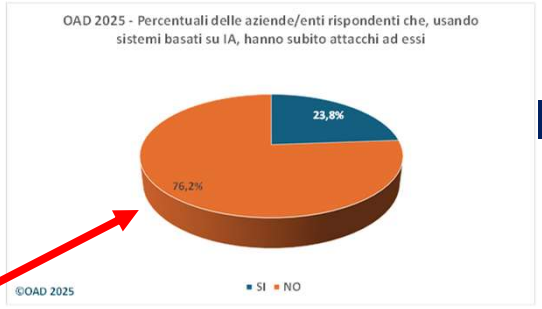
- Modello di intelligenza artificiale (IA) che comprende e genera testo in grado di:
  - Riconoscere e interpretare il linguaggio umano
  - Tradurre, riassumere, e generare testo
  - Rispondere a domande
  - Analizzare il sentiment
  - Riconoscere la voce
- Gli LLM sono formati analizzando grandi quantità di dati testuali e utilizzano reti neurali profonde.
- Sono usati in molti settori, come il digital marketing, la finanza, le assicurazioni, la sanità, e le risorse umane.

16

16

OAD 2025: utilizzo di e attacchi ai sistemi basati su IA



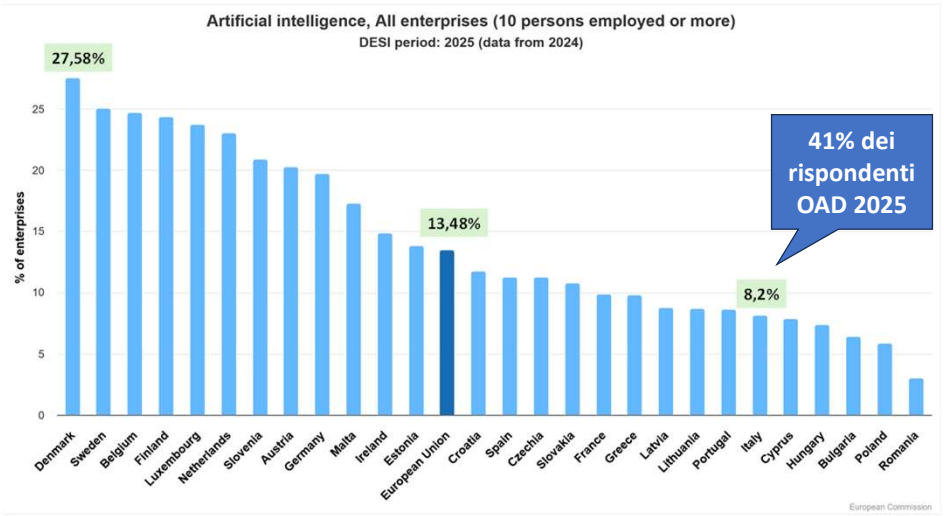


17

www.aipsi.org
www.issa.org

17

Utilizzo IA nelle imprese italiane

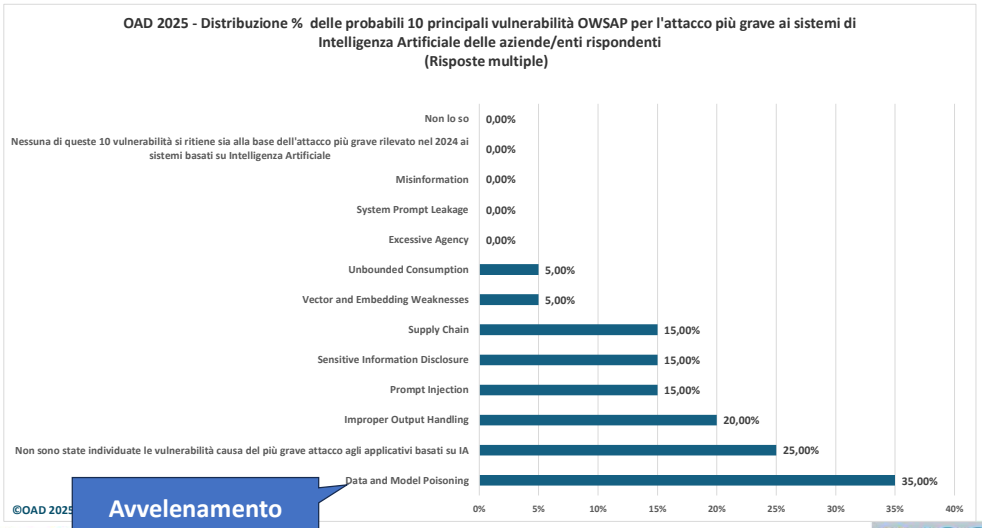


18

www.aipsi.org
www.issa.org

18

OAD 2025: attacchi ai sistemi IA – le vulnerabilità più sfruttate dai rispondenti (top ten OWSAP AI)



www.aipsi.org
www.issa.org

19

19

Misure di sicurezza digitale basate su tecniche IA

Misure tecniche

- Automazione monitoraggio sistemi ICT e loro sicurezza
- Analisi in tempo reale delle possibili minacce anche «zero day»
- Risposta in tempo reale ad incidenti e ad attacchi
- Integrazione tra i sistemi di monitoraggio e controllo sistemi ICT (SI) e quelli per la sicurezza digitale
- Facilita l'interazione macchina-persona utente con il linguaggio naturale

Misure organizzative

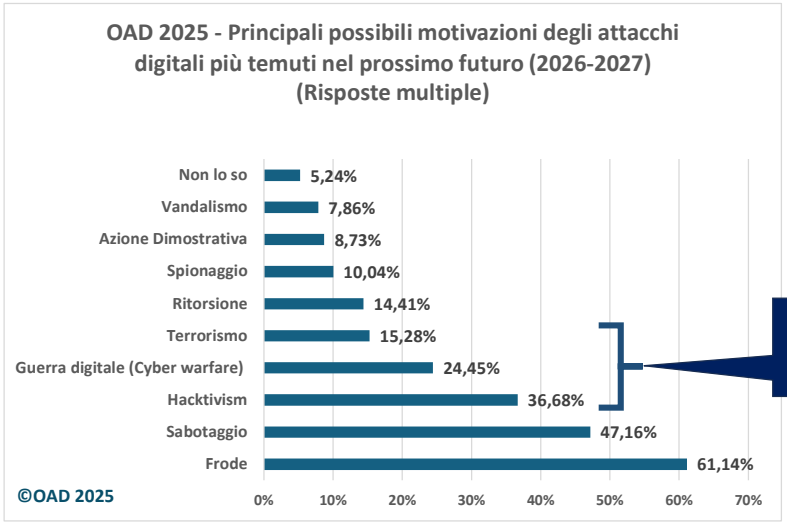
- Automazione procedure organizzative con risposte in tempo reale
- Analisi rischi predittiva
  - Analisi comportamentale dei sistemi ICT e degli utenti
  - Intelligence su possibili attaccanti
- Miglioramento continuo informativa e supporto all'utenza sugli strumenti di sicurezza
- Miglioramento continuo nella presa di decisioni sulla sicurezza basata su dati (data driven)
- Produzione di rapporti più puntuali e chiari

www.aipsi.org
www.issa.org

20

20

OAD 2025 : le principali motivazioni degli attaccanti nel prossimo futuro



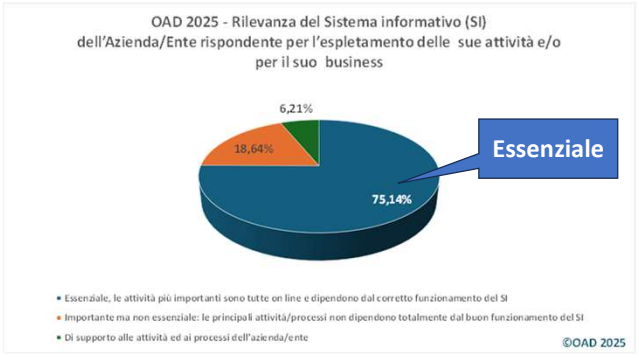
Motivazioni ideologiche 76,41%

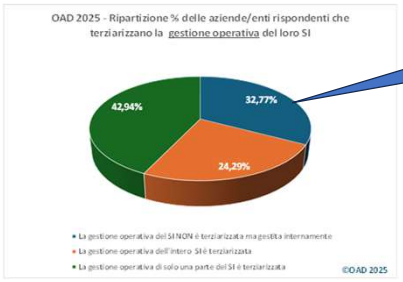
21

www.aipsi.org
www.issa.org

21

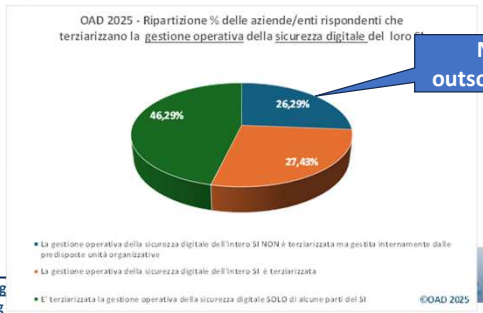
OAD 2025: importanza del SI ed uso di terziarizzazioni per la gestione del SI e della sua sicurezza digitale





No outsourcing

22



No outsourcing

www.aipsi.org
www.issa.org

22

OAD 2025: buon livello delle misure di sicurezza digitale in essere dichiarate (40% rispondenti)

Le domande sulle misure di sicurezze adottate erano opzionali nel questionario.
Ha risposto il 40% del totale dei rispondenti

- **Misure di gestione e controllo**
  - **l'80%** utilizza sistemi di gestione e di controllo in modalità diverse
  - Il **81%** archivia i log degli utenti, ed il **48%** li gestisce
  - **79%** effettua un controllo sulla **sicurezza delle supply chain**
  - Il **70%** ha previsto un **Piano di Disaster Recovery** (DR) ed
    - **Il 70%** di queste ha previsto o allocato risorse ICT alternative per poterlo realmente attuare.

- **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%** al proprio interno, **30%** ai Fornitori

- **Misure tecniche** di sicurezza digitale
  - il **60%** gestisce **centralmente le password**;
  - **55%** dei SI **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 SI usa **FWA**, **Firewall Applicativi;**
  - l'**85%** gestisce la **manutenzione correttiva** degli applicativi;
  - Il **84%** delle aziende/enti rispondenti effettua l'analisi delle vulnerabilità
  - il **44,6%** dei SI effettua il **backup** "a regola d'arte";

23

www.aipsi.org
www.issa.org

23

I mega trend emersi dalle indagini OAD

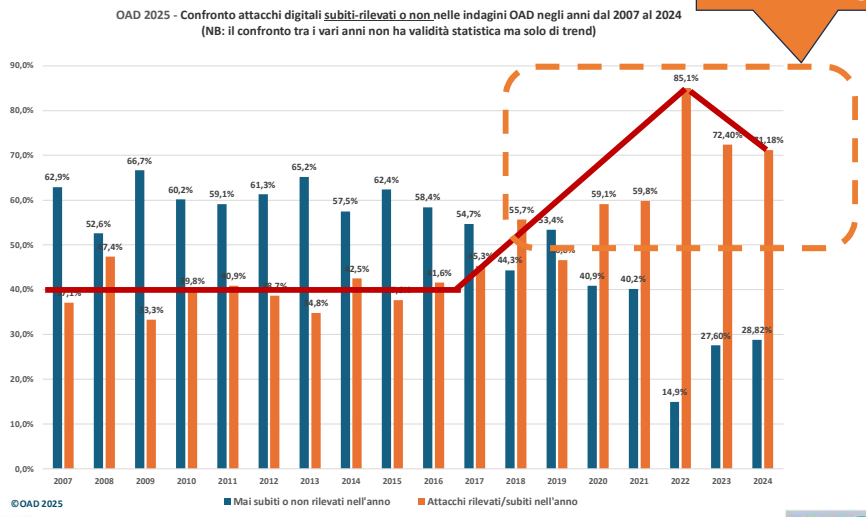
24

www.aipsi.org
www.issa.org

24

OAD 2025: il trend degli attacchi digitali dal 2007 al 2024

Insicurezza digitale sistemica



25

www.aipsi.org
www.issa.org

25

OAD 2025: prime conclusioni

- **I dati emersi da OAD 2025 trovano sostanziale conferma nelle indagini e nei rapporti degli Enti istituzionali a livello nazionale ed internazionale**
- **Il 2024 conferma il permanere di un 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.

Raccomandazioni

- 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.

26

www.aipsi.org
www.issa.org

26

GRAZIE PER L'ATTENZIONE e …

Questa presentazione sarà scaricabile in pdf dal sito web di AIPSI

Se volete essere sistematicamente aggiornati e **crescere professionalmente** nel campo della sicurezza digitale:

- **Seguite le iniziative AIPSI**
- **Diventate Soci di AIPSI**
  - **https://www.aipsi.org/associazione/come-associarsi.html**

https://www.aipsi.org/ 27

https://www.issa.org/