COMUNICATO STAMPA

Pubblicato Rapporto OAD 2024 di AIPSI

AIPSI[1] ha pubblicato il **Rapporto OAD 2024** sull'indagine via web sugli attacchi digitali e sulle misure di sicurezza dei Sistemi Informativi (SI) in Italia, avvalendosi, come negli anni precedenti, della preziosa collaborazione della Polizia Postale e per la Sicurezza Cibernetica, oltre che di FidaInform[2] e di AICA[3]. 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.

OAD, Osservatorio Attacchi Digitali in Italia, costituisce l'unica indagine indipendente online via web in Italia sugli attacchi digitali intenzionali ai Sistemi Informativi (SI) 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). L'attuale edizione 2024 di OAD rappresenta il diciassettesimo anno consecutivo di indagini.

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/

[1] **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/

[2] **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.

[3] **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.

Il **Rapporto OAD 2024** è di 192 pagine A4, con 141 immagini e grafici. E' strutturato in 8 Capitoli (141 pagine A4) con l'elaborazione e l'analisi dei dati emersi dall'indagine e in 8 Allegati (49 pagine A4). Nel Capitolo 8 sono riportati i dati forniti e commentati dalla Polizia Postale e per la Sicurezza Cibernetica. Il Rapporto fornisce nei Capitoli 1 ed 1bis l'Executive Summary in italiano e in inglese.
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.
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.

Analisi degli attacchi

L'indagine, e di conseguenza il Rapporto, si articola in tre parti: la prima fa riferimento a tutti gli attacchi rilevati dalle aziende/enti rispondenti, la seconda approfondisce gli attacchi agli ambienti web, la terza approfondisce gli attacchi ai sistemi OT, Operational Technology[4].
Nel corso dell'intero 2023, il **72,4%** delle aziende/enti rispondenti ha subito attacchi digitali ai propri Sistemi Informativi. Per questi il _tipo di attacco più diffuso tra i rispondenti, con un **31,7%,** le modifiche malevoli/non autorizzate ai programmi e alle configurazioni dei sistemi ICT, grazie anche alla larghissima diffusione di malware e di ransomware in Italia. **L**a 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.

Per quanto riguarda gli attacchi igli ambienti web, 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).
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**.

Per quanto riguarda gli **attacchi agli ambienti OT** 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 sicurezza in essere nei SI 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

[4] **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.

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 tecnica che organizzativa che gestionale**:** 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 SI.

La necessità di gestire l'insicurezza digitale sistemica

Quanto emerge dall'indagine OAD 2024 è **sostanzialmente allineato** con quanto indicato dalle principali indagini: in particolare a livello mondiale dal World Economic Forum, a livello europea da ENISA, l'Agenzia Europea per la cybersicurezza, a livello nazionale da ACN, l'Agenzia per la Cybersicurezza Nazionale, e dal Servizio Polizia Postale e per la Sicurezza Cibernetica (riportati nel Capitolo 8).
Il Capitolo 3 del Rapporto inquadra ed approfondisce il fenomeno degli attacchi digitali, considerando anche le crescenti tensioni geopolitiche ed il forte aumento di attacchi attribuibili alle varie guerre digitali, che anticipano e si affiancano a quelle militari sul territorio.

Gli attacchi digitali sono assai diffusi, indipendentemente dalle dimensioni e dal settore merceologico dell'azienda/ente attaccato, ed hanno forti impatti sull'azienda/ente rispondente in termini sia di gravi disservizi informatici sia di costi, nonostante le misure di sicurezza implementate, e sovente a caro prezzo.
Le misure di sicurezza in essere 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 "sistemica"** 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 "testato".

OAD
Osservatorio
Attacchi Digitali
in Italia