OAD
Osservatorio
Attacchi Digitali
in Italia

COMUNICATO STAMPA

Milano, 30 dicembre 2020

Pubblicato il Rapporto 2020 OAD: la metà circa delle aziende e degli enti italiani hanno subito attacchi informatici nonostante il potenziamento delle loro misure di cybersecurity.

L'Osservatorio Attacchi Digitali in Italia, OAD, con la presente edizione 2020, giunge al dodicesimo anno di indagini consecutive sugli attacchi digitali in Italia, avvalendosi, come negli anni precedenti, della preziosa collaborazione della **Polizia Postale e delle Comunicazioni**. L'indagine 2020 è sponsorizzata da aziende leader a livello mondiale nella cybersecurity come **Cloudflare**, **Darktrace** e **Sophos**, e da autorevoli system integrator italiani quali **Qintesi** e **Technology Estate**.

OAD costituisce l'unica indagine indipendente online in Italia sugli attacchi digitali intenzionali ai sistemi informatici delle aziende e degli enti pubblici operanti in Italia. L'indagine non prevede un predefinito insieme di rispondenti, ma consente ai potenziali interessati un pieno e libero accesso al questionario online, in maniera totalmente anonima; grazie al numero di risposte raccolte e alla loro bilanciata distribuzione tra organizzazioni di varie dimensioni e appartenenti a vari settori merceologici, l'indagine OAD fornisce un preciso quadro sul fenomeno degli attacchi digitali intenzionali in Italia.

L'indagine OAD 2020 fa riferimento all'intero anno 2019 ed al 1° quadrimestre 2020, quando è esplosa la pandemia del Covid che con i blocchi alla mobilità ha portato ad un'ampia gamma di attacchi, causata soprattutto dall'improvviso, e per lo più impreparato, passaggio di molti all'*agile working* da casa e ad un forte utilizzo di ogni tipo di servizio su Internet.

Per il 2019 la diffusione di attacchi digitali sui Sistemi Informatici del bacino dei rispondenti sono ammontati al **46,6%** del totale, e per il 1° quadrimestre 2020 al **44,8%**.

I principali dati emersi dal Rapporto 2020 OAD includono:

- **Il contesto: tipologia delle aziende ed enti dei rispondenti.** Il bacino di rispondenti emerso copre tutti i settori merceologici, incluse le Pubbliche Amministrazioni, anche se la maggior parte di aziende appartiene al settore ICT (30,8%). Il bacino emerso è ben bilanciato tra organizzazioni per

aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA
malabo
ICT Advisory
Reportec

numero di dipendenti, tra quelle al di sotto dei 250 e quelle più grandi. Si deve tener conto che in Italia il 99,91% delle imprese sono PMI, Piccole Medie Imprese, sotto i 250 dipendenti, e di queste il 95% sono sotto i dieci dipendenti. L'indagine OAD riesce pertanto ad indagare anche sulle piccole e piccolissime organizzazioni, che normalmente non sono considerate nelle altre indagini sulla cybersecurity: il 57,5% dei rispondenti appartiene a strutture con un organico inferiore ai 250 dipendenti, e di queste il 22,1% sotto i 10.

- **Diffusione degli attacchi digitali nel bacino dei rispondenti**
    - per gli attacchi mirati (targeted), le micro e le nano imprese sicuramente non rappresentano un obiettivo di interesse specifico per i cyber criminali. Esse possono essere coinvolte in attacchi di massa, come quelli basati sul phishing e sul ransomware, così come avviene tipicamente o per cogliere qualcuno nella massa, o per motivi ideologici (hactivism) o terroristici. Infatti in entrambi i periodi considerati la percentuale di non attacchi rilevati è decrescente dalle piccolissime organizzazioni con meno di dieci dipendenti alle grandissime con più di 5000. Questo è confermato considerando i fatturati o il conto economico delle aziende/enti attaccate: il 50% è di quelle con più di € 5 Mlni.
    - Il tipo di attacco, ossia che cosa si attacca, più diffuso in entrambi i periodi considerati è stato quello ai sistemi di controllo degli accessi, l'IAA, Identificazione Autenticazione Autorizzazione, con un 34% nel 2019 e con un 28,2% nel 1° quadrimestre 2020. Al secondo posto come diffusione nel 2019 si posiziona il furto di dispositivi mobili, con un 28,2%, mentre nel 1° quadrimestre 2020 si posiziona l'accesso non autorizzato all'intero sistema ICT target, con un 27,3%. Come diffusione tra i rispondenti seguono, a decrescere di pochi punti percentuali, le altre tipologie d'attacco, le cui caratteristiche ed i cui impatti sono approfonditi nei relativi paragrafi del Rapporto.
    - Come tecniche di attacco, ossia come si attacca, le sette famiglie considerate nel questionario sono largamente impiegate nei vari tipi d'attacco, anche contemporaneamente. La più diffusa, quale media sui vari attacchi rilevati dal bacino di rispondenti, è l'uso di toolkit (rootkit, metaexploit, etc.) per l'individuazione e lo sfruttamento delle vulnerabilità sul sistema target dell'attacco, con un 38,8%, seguita dalla ben nota raccolta malevole e non autorizzata di informazioni (social engineering, phishing, etc.) con un 34, 6% e dall'uso di codici maligni e script con un 34,3%. Seguono le altre tecniche considerate a decrescere con pochi punti percentuali di differenza tra loro.
- **Le motivazioni degli attacchi digitali** sono nella stragrande maggioranza dei casi di tipo economico, quindi per frode e ricatto: l'ampia diffusione in Italia dei ransomware ne è una chiara conferma.
- **I Sistemi Informatici, e loro misure di sicurezza digitale, delle aziende ed enti rispondenti** risultano essere, come percentuale di diffusione, nella fascia medio-alta per il livello di sicurezza digitale attuato, ed i dati emersi evidenziano un netto miglioramento sia delle misure tecniche sia di quelle organizzative, rispetto agli anni precedenti (come trend, non a livello statistico).
    - Pochi i Sistemi Informatici con Data Center in Italia, la maggior parte dei rispondenti ha Sistemi Informatici di medio-piccole dimensioni in parte on premise e in parte terziarizzati, con uso di servizi in cloud.
- **I dati forniti dalla Polizia Postale e delle Comunicazioni** confermano le crescenti criticità degli attacchi digitali e, soprattutto, le difficoltà crescenti nel contrastare e reprimere la criminalità informatica.
    - Nell'ambito della protezione delle Infrastrutture Critiche, nel 2019, i 1181 attacchi rilevati sono più che raddoppiati rispetto a quelli dell'anno precedente, così come le 155 indagini avviate; nel 1° quadrimestre 2020 sono stati rilevati 282 attacchi, sono state avviate 34 indagini;
    - Nel contrasto al "*financial cybercrime*", le transazioni fraudolente nel 2019 sono state

bloccate per un valore complessivo di € 21,3 Mln e sono stati recuperati € 18 Mln; nel 1° quadrimestre 2020 sono state bloccate transazioni fraudolente per ben € 20,2 Mln, raggiungendo in pratica in 4 mesi quanto bloccato nei 12 mesi dell'anno precedente, e recuperati € 8 Mln; un indicatore della crescita degli attacchi alle transazioni ed ai servizi finanziari dovuta all'enorme uso di questi servizi online causati dai blocchi della pandemia Covid 19.

Il Rapporto 2020 OAD, costituito da 186 pagine formato A4 e da 148 figure, è gratuitamente scaricabile da: https://www.oadweb.it/it/oad-2020/per-scaricare-il-rapporto-2020-oad.html

OAD 2020 è un'iniziativa di:

- **AIPSI**, Associazione Italiana Professionisti Sicurezza Informatica, è il Capitolo italiano della internazionale ISSA (www.issa.org)
- **Malabo Srl** (www.malaboadvisoring.it) è la società dell'autore che ha ideato e realizzato l'indagine OAD ed il Rapporto
- **Reportec Srl** (www.reportec.it) è il media partner di AIPSI.

Per qualsiasi maggior informazione contattare: aipsi@aipsi.org