OAD
Osservatorio
Attacchi Digitali
in Italia

Rapporto 2019 OAD

a cura di Marco R. A. Bozzetti

Sintesi Direzionale

SPONSOR

advansys

par-tec
beyond the IT domain

QINTESI

Technology Estate

in collaborazione con Polizia Postale e delle Comunicazioni

polizia delle comunicazioni

Indagine effettuata da

aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

malabo
ICT Advisory

Media partner

Reportec

1 L'indagine e il Rapporto 2019 OAD

L'Osservatorio Attacchi Digitali in Italia, OAD, con la presente edizione 2019 arriva all'undicesimo anno di indagini consecutive sugli attacchi digitali in Italia e si avvale, come negli anni precedenti, della preziosa collaborazione con la Polizia Postale e delle Telecomunicazioni. OAD costituisce l'unica indagine indipendente on line via web in Italia sugli attacchi digitali intenzionali ai sistemi informatici delle aziende e degli enti pubblici operanti in Italia.
L'indagine OAD non prevede un predefinito insieme di rispondenti, ma consente ai potenziali interessati un pieno e libero accesso al questionario in Internet via web, in maniera totalmente anonima; grazie al numero di risposte raccolte e alla loro bilanciata distribuzione tra aziende ed enti pubblici di varie dimensioni e appartenenti a vari settori merceologici, esso fornisce precise e contestuali indicazioni sul fenomeno degli attacchi digitali in Italia.

2 Il bacino emerso dei rispondenti per OAD 2019

Secondo gli ultimi dati ISTAT[1], il numero di aziende in Italia è di 4.397.623: il 99,91% sono PMI, Piccole Medie Imprese, sotto i 250 dipendenti, e di queste il 95% sono sotto i dieci dipendenti. Per le pubbliche amministrazioni, poche sono le grandi strutture, la stragrande maggioranza sono sotto i 250 dipendenti. A fronte di questo contesto italiano, di fatto basato su piccole e piccolissime organizzazioni, il bacino di rispondenti emerso nel 2019 risulta costituito, in termini di numero di dipendenti, per il 62,6% da strutture sotto i 250, e di queste il 37,4% sotto i 50. Per le grandi organizzazioni, il 9% dei rispondenti ha più di 5000 dipendenti. Rispetto ai settori merceologici, i rispondenti al 18% appartengono a pubbliche amministrazioni, istruzione statale inclusa, il resto al settore privato: di questo, la maggior parte di aziende appartiene al settore ICT (25,7%) e a quello manifatturiero e delle costruzioni (16,4%), cui seguono con percentuali inferiori organizzazioni appartenenti a tutti gli altri settori merceologici, classificati secondo il codice ATECO[2]. Il campione emerso risulta quindi abbastanza ben bilanciato tra piccole strutture e quelle medio grandi; per i vari settori merceologici il campione è invece prevalente formato da aziende di servizi ICT e del manifatturiero.
I compilatori del questionario 2019 sono per il 18,3% i responsabili dei sistemi informatici (CIO), per il 17% il personale di terze parti cui è terziarizzata, in tutto o in parte, la gestione del sistema informatico e della sua sicurezza, e con una identica percentuale il personale di vertice dell'azienda/ente. Seguono con percentuali a scalare altri ruoli, incluso con il 7,2% quello di responsabile della sicurezza digitale (CISO).

3 Gli attacchi digitali ad aziende ed enti emerse nel 2019 dall'indagine

In termini di attacchi digitali, per la prima volta negli undici anni di indagini dell'Osservatorio, la percentuale di rispondenti che ha subito-rilevato attacchi, il 55,7%, è superiore a chi non li ha subiti: importante indicatore della crescente diffusione degli attacchi digitali.
Le cinque tipologie di attacco più diffuse tra i sistemi informatici dei rispondenti sono state, in ordine di diffusione tra i rispondenti:

- gli attacchi ai sistemi IAA per il controllo degli accessi, con un 54,21%;
- gli attacchi all'intero sistema ICT target, con un 41%;
- gli attacchi alle reti di comunicazione, con un 34,65%;
- il furto di dispositivi mobili d'utente, con un 33,62;
- saturazione sistemi e risorse ICT (DoS, DDoS), con un 30,93%.

[1] ISTAT, Istituto nazionale di statistica.
[2] Codice ATECO: combinazione alfanumerica che identifica una ATtività ECOnomica.

Tutte le altre tipologie di attacco, per il bacino di rispondenti, sono a decrescere sotto il 30% come diffusione.
La tecnica di attacco più diffusa e più usata secondo i rispondenti, considerando tutte le tipologie di attacco nel 2018, è stata la raccolta malevole e non autorizzata di informazioni, tipicamente tramite social engineering, cui segue l'uso di codici maligni e script e al terzo posto i toolkit. A ben maggiore distanza percentuale, a decrescere, le altre tecniche considerate.

4 Le misure di sicurezza in atto nei sistemi informatici dei rispondenti di OAD 2019

L'indagine OAD cerca di fotografare, oltre agli attacchi digitali subiti, le misure di sicurezza che i sistemi informatici dei rispondenti hanno in atto, anche per meglio comprendere, pur in linea generale, quanto queste contromisure sono riuscite a prevenire e contrastare gli attacchi.
I sistemi informatici dei rispondenti e le misure di sicurezza che li proteggono, risultano essere, come percentuale di diffusione, nella fascia medio-alta per il livello di sicurezza digitale attuato, pur con qualche elemento di eccellenza e più numerosi elementi di debolezza. In non pochi casi mancano le più elementari e basilari misure sia tecniche sia, soprattutto, organizzative, e questo non solo nelle piccole e piccolissime strutture (anche se la loro prevalenza incide sulle percentuali complessive), ma anche in quelli medio grandi.
Numerose le indicazioni emerse dall'indagine, brevemente nel seguito si indicano solo alcune tra le più interessanti:

- relativamente poche le aziende/enti dei rispondenti che seguono un approccio architetturale basato su standard e best practice per la sicurezza digitale, il 13%, ed il 29,59% dichiara di disporre almeno delle risorse ICT più critiche in alta affidabilità (99,9%); la mancanza di una architettura per la sicurezza digitale porta alla non interazione e coordinamento tra i diversi strumenti;
- assai limitate le misure di sicurezza fisica;
- per la protezione delle reti, il 54,3 usa firewall di rete e DMZ, il 49,8% usa VPN, il 27,6% utilizza sistemi IPS/IDS e di analisi di traffico;
- per il controllo degli accessi, misure per lo più basate sul solo uso di identificatore d'utente e password, per il 60,2% dei rispondenti;
- per la protezione delle applicazioni e dei dati trattati, ancora limitato utilizzo della crittografia sia nella trasmissione dati, 38,9%, sia nella archiviazione di quelli più critici, dati sensibili inclusi, 27,6%.

Le misure e gli strumenti di gestione della sicurezza digitale in uso nei sistemi informatici dei rispondenti sono percentualmente basse, anche per la forte incidenza delle piccole e medie organizzazioni:

- gli strumenti più diffusi sono il monitoraggio ed il controllo centralizzato delle funzionalità e delle prestazioni dei sistemi ICT con un 37,1% dei rispondenti;
- il 42% dei rispondenti terziarizzano in parte o completamente il loro sistema informatico e la gestione della sua sicurezza, ed l'11,8% utilizza SOC e/o SCC.

Le misure organizzative della sicurezza digitale risultano più carenti e meno avanzate rispetto a quelle tecniche:

- circa i ¾ dei rispondenti hanno nella propria organizzazione chi espleta de facto il ruolo di responsabile della sicurezza digitale (CISO), ma solo 1/3 lo ha ufficializzato;
- per il 40% circa sono definite e in uso policy per la sicurezza digitale, percentuali inferiori, a partire da 37,1%, per le relative procedure organizzative;
- scarse attività di sensibilizzazione e formazione sulla sicurezza digitale;
- scarso interesse sulle certificazioni professionali per la sicurezza digitale a livello aziendale e personale, sia all'interno della propria organizzazione sia verso i fornitori.

5 Sui dati della Polizia Postale e delle Comunicazioni

I dati forniti dalla Polizia Postale e delle Comunicazioni confermano le cresciti criticità degli attacchi digitali e soprattutto le difficoltà nel contrastare e reprimere la criminalità informatica:

- nell'ambito della protezione delle Infrastrutture Critiche, gli allarmi diramati nel 2018 sono stati 80.777, più del doppio rispetto al 2017; gli attacchi rilevati sono stati 459, poco meno della metà del 2017, le indagini avviate 74, le persone denunciate 14 e quelle arrestate 1;
- nel contrasto al "financial cybercrime", le transazioni fraudolente nel 2018 sono state bloccate per un valore complessivo di € 38,4 Mln e sono stati recuperati € 9 Mln; non sono stati forniti dati sul numero di denunce e di arresti;
- nel contrasto al cyber terrorismo sono stati controllati 36.000 siti web e cancellati 250 contenuti.

6 Prime conclusioni

L'indagine OAD 2019 evidenzia l'incremento di attacchi digitali, talvolta con impatti e conseguenza serie, ma nella maggior parte dei casi le misure di contrasto in essere, pur avendo lacune, riescono a tamponarli.

La realtà italiana, costituita da un grandissimo numero di piccole e piccolissime imprese, non fa rientrare il nostro paese tra quelli più appetibili per i criminali digitali, ma cyber warfare e gli attacchi massivi costituiscono un rischio crescente e grave, come in parte è già successo con la larga diffusione di ransomware su sistemi informatici cui mancano, o sono mal gestite, le misure di base.

Ancora forte la sottovalutazione della sicurezza digitale, con la conseguente non implementazione delle idonee misure di difesa, soprattutto nelle pubbliche amministrazioni. Misure di difesa che rincorrono l'evoluzione, sempre più sofisticata e smart, degli attacchi, ma quasi sempre in ritardo.

L'attuale alta densità di vulnerabilità richiede nuovi approcci e nuove logiche, con l'obiettivo di rendere intrinsecamente sicuri, by default e by design, tutti i sistemi ICT interconnettibili ad Internet.

Ma alla data siamo ancora lontani da tale obiettivo, e per migliorare decisamente il concreto contrasto al cybercrime occorre ora accrescere la consapevolezza e le competenze sulla sicurezza digitale a tutti i livelli, la fattiva collaborazione tra le polizie a livello mondiale, l'etica professionale di chi si occupa (lato offerta) e di chi decide (lato domanda) sulla sicurezza digitale.

7 Indice del Rapporto 2019 OAD

1 Sommario

8 AIPSI, Capitolo italiano della mondiale ISSA

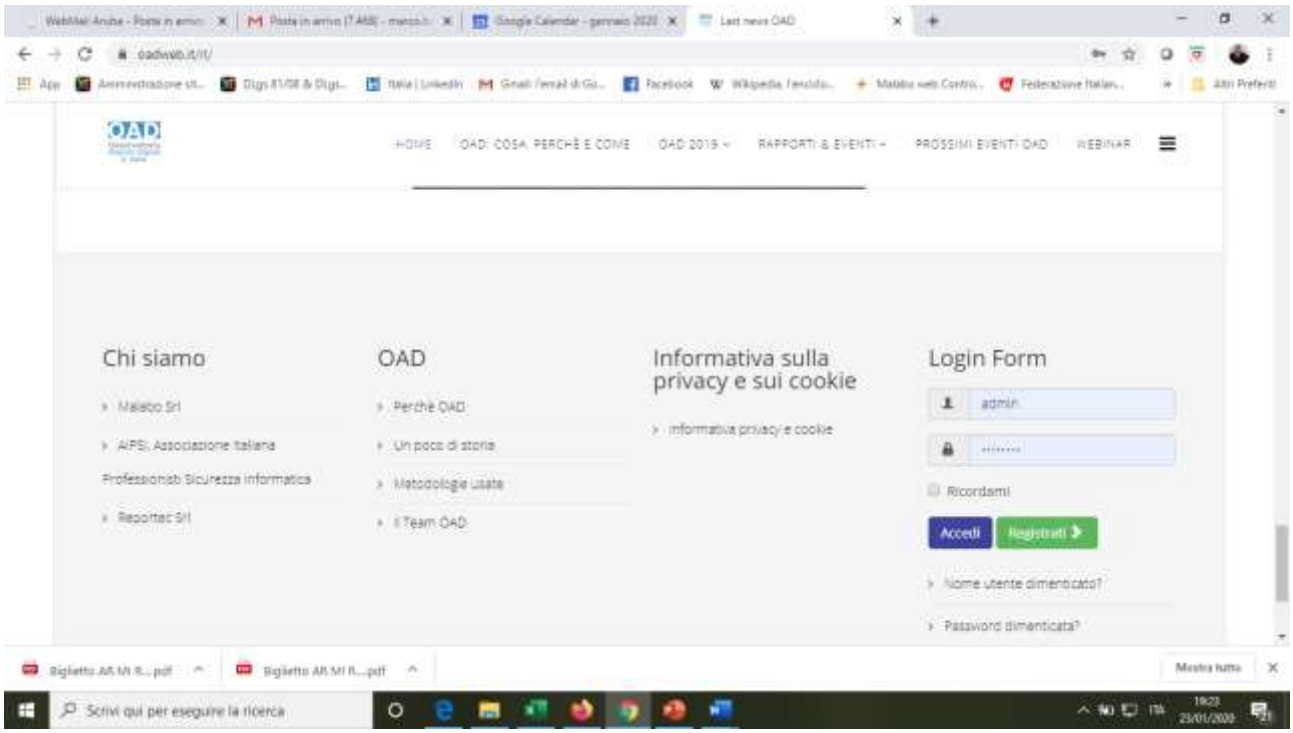
AIPSI, Associazione Italiana Professionisti Sicurezza Informatica, è il capitolo italiano di ISSA, l'organizzazione internazionale no-profit di professionisti ed esperti praticanti, e fa così parte della più grande e qualificata associazione sulla sicurezza digitale con oltre 12000 aderenti in più di 100 capitoli a livello mondiale. AIPSI, come ISSA, è una associazione di sole persone che si occupano a qualsiasi livello e ruolo di sicurezza digitale. Il suo obiettivo primario è aiutare i Soci nella crescita professionale e nel loro aggiornamento continuo sui temi tecnici, organizzativi, legislativi della sicurezza digitale. L'organizzazione di eventi e di webinar di approfondimento e di trasferimento di conoscenze, la redazione di documenti e pubblicazioni, il supporto per le certificazioni europee eCF (EN 16234-1:2016) per i ruoli di security manager e security specialist, oltre all'interazione fra i vari Soci, contribuiscono concretamente ad incrementare le competenze e la crescita professionale dei Soci, oltre che a promuovere più in generale la cultura della sicurezza ICT in Italia. L'appartenenza al contesto internazionale ISSA, permette ai Soci AIPSI, che lo sono anche di ISSA, di interagire con gli altri capitoli europei, americani e del resto del mondo. ISSA ed AIPSI sono focalizzate nel mantenere la posizione di "Global voice of Information Security": in tale ottica AIPSI collabora attivamente con numerose altre associazioni italiane per effettuare congiuntamente varie iniziative, la più importante delle quali è la realizzazione di OAD, Osservatorio Attacchi Digitali in Italia, e la pubblicazione del relativo Rapporto annuale.
Di recente AIPSI ha creato un "gruppo speciale di interesse" sul ruolo professionale delle donne nella sicurezza digitale in Italia.
I principali benefici per i Soci AIPSI-ISSA includono:

- Ricezione dell'ISSA Journal, l'autorevole rivista mensile di ISSA, cui un Socio AIPSI può proporre un proprio articolo in inglese sul tema della sicurezza digitale.
- Ricezione delle newsletter di AIPSI.
- Partecipazione ai frequenti webinar internazionali di ISSA, in inglese, ed a quelli in italiano di AIPSI.
- Partecipazione a Gruppi di Lavoro, a convegni e workshop organizzati da AIPSI e/o dai/con i suoi Partner per la formazione e l'aggiornamento continuo sulla sicurezza digitale.
- Supporto alle certificazioni professionali per le competenze sulla sicurezza digitale, in particolare per eCF, con coaching ed e-learning, oltre che in certi casi con significativi sconti sui prezzi di certificazione.
- Networking con altri professionisti del settore.
- Possibilità di costituire gruppi di lavoro per ricerche e condivisione informazioni su tematiche d'interesse comune.
- Possibilità di redigere articoli per conto di AIPSI/ISSA e loro pubblicazione nel sito web AIPSI.
- Pubblicazione e ricerca di curricula per agevolare la domanda/offerta di competenze e di professionalità.
- Accesso al materiale riservato ai soci sul sito web di ISSA e di AIPSI.
- Visibilità nazionale ed internazionale grazie al riconoscimento di ISSA nel mondo.
- Possibilità di partecipare come oratore a seminari e conferenze per conto di AIPSI/ISSA.

Per maggiori informazioni: https://www.aipsi.org e www.issa.org

9 Per scaricare l'intero Rapporto 2019 OAD

1. Per prima cosa occorre registrarsi al sito oadweb.it, se non si ha già un account; so lo si ha effettuare il login (al fondo della home page di https://www.oadweb.it/it/)



2. Accedere alla pagina https://www.oadweb.it/it/oad2019/per-scaricare-il-rapporto-2019-oad.html
   a. *Chi non è registrato non vede l'icona del file da scaricare*
   b. I registrati che hanno fatto il login vedono l'icona, cliccando sopra "download ottengono il Rapporto