Marco R. A. Bozzetti (*)

Attacchi digitali e misure di sicurezza: l'indagine OAD di AIPSI in Italia

OAD, Osservatorio Attacchi Digitali in Italia, è l'unica indagine annuale on line sugli attacchi digitali intenzionali ai sistemi informativi (SI) di aziende ed enti operanti in Italia e sulle misure di sicurezza tecniche ed organizzative presenti. Con l'edizione 2024 ora in corso, OAD ha raggiunto i 17 anni consecutivi di indagine, ed è realizzata da AIPSI, capitolo italiano di ISSA. Benché il diverso bacino di rispondenti anno per anno non conferisca al confronto delle informazioni una stretta valenza statistica, l'indagine fornisce significative indicazioni sui trend della sicurezza digitale in Italia, anche per le piccole e piccolissime organizzazioni private e pubbliche (tra il 50 ed il 60 % dei rispondenti), che costituiscono il 95% delle imprese in Italia (ISTAT) e che non sono normalmente considerate nelle altre indagini. Nel seguito sono presentati alcuni dei principali trend emersi dalla analisi correlata dei diversi rapporti OAD pubblicati.

(*) Presidente AIPSI, Associazione Italiana Professionisti Sicurezza Digitale **www.aipsi.org,** capitolo italiano di ISSA **www.issa.org** e Founder-CEO Malabo Srl

La figura 1 mostra l'andamento degli attacchi digitali rilevati dai rispondenti al questionario dal 2007 al 2022 (ogni rapporto pubblicato fa riferimento all'indagine dell'anno precedente). La barra arancione evidenzia la percentuale degli attacchi rilevati anno per anno; la riga rossa mostra come dal 2007 al 2016 gli attacchi si siano attestati sul 40%. Dal 2017 la percentuale di attacchi inizia a crescere, e nel 2018 si verifica la prima svolta: la percentuale di attacchi rilevati supera quella degli attacchi non subiti (o non rilevati). Dal 2020 questa crescita è in continua forte ascesa, e raggiunge il picco nel 2022. Si vedrà dall'indagine in corso se avremo un'ulteriore crescita o un rallentamento.

Perché crescono gli attacchi?

I motivi sono molteplici e in qualche misura correlati tra loro. Da un lato il crescente uso di servizi e sistemi ICT in ogni tipo di attività e di settore merceologico, con conseguente crescita di crimini informatici "tradizionali" (frodi informatiche, furti di informazioni e di identità digitali, ricatti e sabotaggi digitali, etc). Poi ci sono elementi geopolitici.

1) Il Covid-19 da marzo 2020 indusse, in pochi giorni, a lavorare da remoto via Internet, ma le misure di sicurezza erano nella maggior parte dei casi inadeguate e insufficienti. Questo portò ad un forte ampliamento della superficie di vulnerabilità e quindi degli attacchi.

2) Nel 2022 l'invasione dell'Ucraina da parte della Federazione Russa, tutt'ora in corso, è stata preceduta - ed è accompagnata - da attacchi alle infrastrutture critiche ucraine e dei paesi occidentali che si sono affiancati alla causa ucraina. In questi ultimi anni sono inoltre significativi gli attacchi digitali da parte di paesi e di gruppi jihadisti, che si affiancano, e con notevoli capacità tecniche, ai gruppi e paesi antioccidentali. Queste molteplici motivazioni hanno portato al picco dell'85,1% nel 2022 come diffusione di attacchi digitali ai SI dei rispondenti al questionario OAD.

I più colpiti

Correlando la diffusione degli attacchi con le dimensioni ed il fatturato delle imprese che li hanno subiti, emerge che le più colpite sono quelle di maggiori dimensioni e di maggior fatturato, in particolare per gli attacchi targeted: essendo la motivazione di un attacco prevalentemente di tipo economico, non si attaccano aziende/enti piccoli, poco conosciuti e con bassa capacità finanziaria.

L'indagine mostra che, dal 2017 in avanti, ai primi posti - come percentuale di diffusione - si alternano: attacchi ai sistemi di identificazione, autenticazione e autorizzazione (IAA); furto di dispositivi "fisici" mobili o fissi (o di alcune loro parti); attacchi alle reti di comunicazione, soprattutto alle connessioni ad Internet; saturazione delle risorse ICT collegate ad Internet (DoS/DDoS, Denial of Service/Distributed DoS).

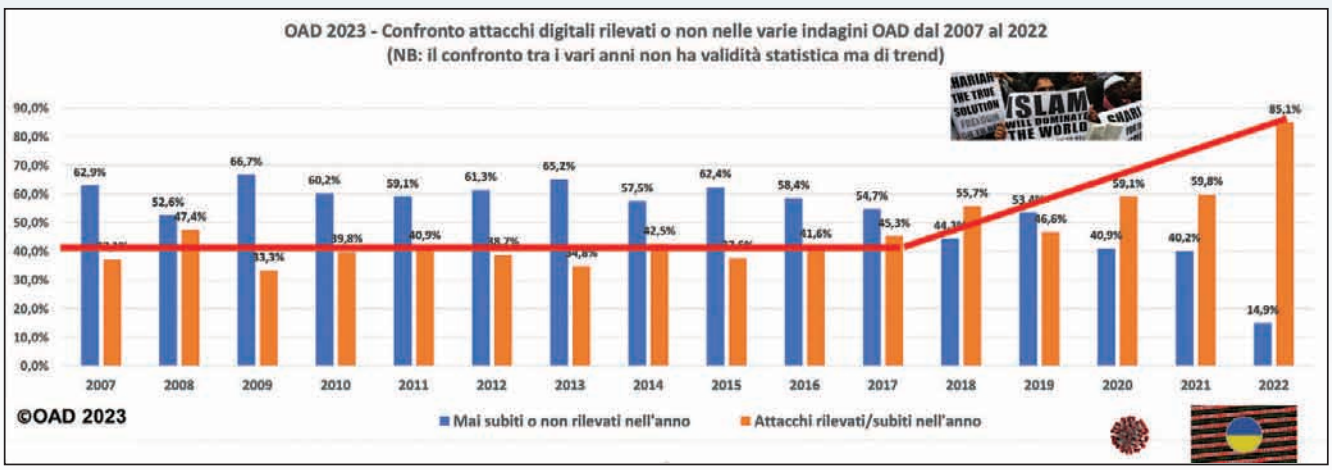

Figura 1.

Gli attacchi più diffusi

L'analisi dei trend negli anni mostra le tre tecniche di attacco più diffuse rilevate dai rispondenti anno per anno, nell'ambito delle sette famiglie di tecniche di attacco considerate dall'Osservatorio:

- la famiglia "script-codici maligni", che include il ransomware;
- la famiglia "raccolta non autorizzata di informazioni", che include il social engineering;
- l'attacco fisico, che include il furto di dispositivi fissi e mobili, ed il furto di informazioni con chiavette USB.

Il questionario OAD 2024 è online, anonimo e sicuro: compilatelo o fatelo compilare da chi gestisce il vostro sistema informativo:

L'indagine OAD è rivolta ad aziende/enti di ogni settore merceologico, incluse le PA Centrali e Locali, e di ogni dimensione (come numero di dipendenti e fatturato/giro d'affari).

Misure di sicurezza

La figura 2 mostra i diversi tipi di misure di sicurezza considerati nei questionari OAD, dal 2017 in avanti. Di seguito i principali trend emersi.

Misure tecniche di sicurezza digitale. Molte delle tematiche indicate in figura 2 presentano percentuali di diffusione relativamente alte fin dai primi anni, come ad esempio il controllo perimetrale e degli accessi fisici alle aree che contengono sistemi ICT in funzione, la ridondanza delle linee di collegamento ad Internet, l'uso di Firewall, il backup (relativamente) sistematico. Queste ed altre voci hanno avuto un incremento negli ultimi anni, a causa della recrudescenza degli attacchi e della conseguente necessità di potenziamento delle misure tecniche per individuare, bloccare o ridurre l'attacco: in particolare l'analisi delle vulnerabilità tecniche dei sistemi ICT, l'autenticazione forte per gli utenti privilegiati e il progetto e l'implementazione sicura del software, la crittografia dei dati personali (e soprattutto sensibili) e di quelli più confidenziali e critici per l'impresa.

Misure organizzative. Molte delle misure indicate in figura 2 presentano percentuali abbastanza alte in tutti gli anni, ma permangono carenze su questo versante soprattutto per le piccole realtà. Gli ultimi due anni considerati hanno una impennata complessiva, ma per le piccole organizzazioni rimangono ancora carenti ed insufficienti. In particolare risultano poco diffuse tra la aziende/enti rispondenti le certificazioni sulla sicurezza digi-

Misure tecniche	Architettura complessiva delle misure della sicurezza digitale, integrata con l'intera architettura del sistema informatico, che può includere Zero Trust, SASE, SOAR, etc.
	Analisi vulnerabilità
	Contromisure fisiche
	Misure di Identificazione, Autenticazione, Autorizzazione (IAA)
	Contromisure tecniche sicurezza digitale a livello di reti locali e geografiche
	Contromisure tecniche per la protezione logica dei singoli sistemi ICT
	Contromisure tecniche per la protezione degli applicativi
	Contromisure per la protezione dei dati
Misure organizzative	Struttura organizzativa, ruoli, competenze, certificazioni
	Analisi rischi ed impatti
	Policy e procedure organizzative
	Contratti e clausole sicurezza digitale con le Terze Parti
	Consapevolezza della sicurezza digitale a tutti i livelli della struttura organizzativa
	Auditing
Misure di gestione e di governo	Sistemi di controllo e monitoraggio (gestione operativa della sicurezza digitale)
	Governo (strategico) della sicurezza digitale
	Disaster Recovery (piano, allocazione risorse alternative, etc.).

Figura 2.

tale, tipo ISO 20000 e ISO 27001, e sono poche le richieste di questo tipo di certificazioni aziendali, o di quelle individuali, per i diversi fornitori ed il loro personale. Altrettanto poche le richieste di certificazioni a livello individuale per il personale interno che si occupa di sicurezza digitale. Ancora limitati corsi ed altre forme di comunicazione, sensibilizzazione e formazione sulla sicurezza digitale. La diffusione dell'analisi dei rischi ICT (e dei loro impatti) è però cresciuta tra i rispondenti, in particolare dal 2017 in avanti. Le strutture organizzative interne per la sicurezza digitale sono prevalentemente presenti nelle grandi strutture, e si va diffondendo la terziarizzazione della sua gestione a consulenti e ad aziende specializzate.

Gestione della sicurezza digitale e del Disaster Recovery (DR). I sistemi centralizzati di gestione della sicurezza digitale, sia on premise che terziarizzati o in mix, sono appannaggio prevalente delle grandi strutture, così come l'auditing e la gestione dei log di sistema e dell'utenza; e questo vale per tutto l'arco temporale considerato. Lenta l'evoluzione verso la terziarizzazione della gestione della sicurezza digitale grazie a MSS, Managed Security Services, e alla Security as a Service, anche se molte piccole organizzazioni demandano la progettazione e poi la gestione della cybersecurity a consulenze esterne. Cresce la diffusione dei Piani di DR, ma ben più lentamente la necessaria disponibilità di sistemi ICT alternativi in caso di DR e la predisposizione di strutture e procedure organizzative per la gestione del DR e del suo ripristino. Il Piano di DR è quindi più una "formalità burocratica" necessaria per certificazioni e conformità a normative, che una reale necessità ben organizzata. Pur con valori fortemente altalenanti, un "minimo" di DR è comunque presente in più di 1/3 dei rispondenti in tutti gli anni considerati.

Prime conclusioni

Il trend che emerge dalle indagini OAI-OAD negli anni è in linea con le principali indagini europee e mondiali, e conferma la validità dell'indagine AIPSI. In termini di misure in atto, si riscontrano significative differenze tra medio-grandi SI (con almeno un Data Center) e quelli piccoli (senza Data Center). Quasi tutti i rispondenti, di ogni settore merceologico e di ogni dimensione, hanno soluzioni ibride del SI con sistemi/applicazioni-servizi in cloud. Il bacino di aziende/enti rispondenti si posiziona fin dall'inizio dell'iniziativa nella fascia medio-alta in termini di livello di sicurezza posto in essere (probabilmente questo è uno dei motivi di compilazione del questionario).

Gli attacchi digitali crescono come diffusione e soprattutto come gravità di impatto quando vanno a buon fine, pur con misure di sicurezza tecniche ed organizzative non irrisorie e costose: quindi le misure poste in essere non sono sufficienti. Nel breve termine occorre usare gli strumenti che si hanno a disposizione, da un lato aggiornandoli e potenziandoli e dall'altro coinvolgendo tutto il personale, interno e della filiera della logistica (clienti e fornitori che interagiscono con il SI e che se non sono sicuri ampliano i rischi e consentono gli attacchi tipici della supply chain), e soprattutto i vertici decisionali. La formazione e la sensibilizzazione di tutti sulla sicurezza digitale è un "must be", così come il coinvolgimento del vertice nella sua governance. La sicurezza digitale non è solo un problema tecnico, ma di business: se è carente, non può garantire la continuità operativa dell'azienda/ente.

OAD, Osservatorio Attacchi Digitali in Italia. Il sito https://www.oadweb.it/ è una repository. liberamente consultabile. dei rapporti finali pubblicati e della documentazione degli eventi in cui si sono presentati e discussi i dati emersi nei 17 anni di attività.