OAD
Osservatorio
Attacchi Digitali
in Italia

SINTESI

Rapporto 2020 OAD

a cura di Marco R. A. Bozzetti

GOLD SPONSOR

CLOUDFLARE · DARKTRACE · QINTESI · SOPHOS

SILVER SPONSOR

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

Ringraziamenti
Si ringraziano tutte le persone che hanno compilato il questionario online ed i Patrocinatori che hanno aiutato a promuovere la compilazione del questionario e aiuteranno alla diffusione del presente Rapporto 2020 OAD.
Un grazie particolare agli Sponsor e alle persone che hanno collaborato in vario modo alla realizzazione del questionario on line e del rapporto finale:

- per AIPSI: Massimo Chirivì
- per Malabo Srl: dott. Andrea Bozzetti, Giuseppe Cesa Bianchi, dott. Francesco Zambon
- per Reportec: dott. Gaetano Di Blasio, dott.ssa Paola Saccardi

oltre che alla Polizia Postale e delle Comunicazioni, in particolare al Direttore dott.ssa Nunzia Ciardi.

Dichiarazione di non responsabilità

I grafici ed i testi del presente rapporto sono stati elaborati e redatti con la massima accuratezza e correttezza possibile, partendo dalle risposte al questionario online totalmente anonimo e che pertanto non possono essere verificate. La loro affidabilità, dato il numero delle risposte, è significativa come tendenza, ma non sono in alcun modo di responsabilità da parte dell'autore, Marco R. A. Bozzetti, di Malabo Srl, di Reportec Srl, di AIPSI, né di alcun altro Sponsor e Patrocinatore. Tutte le informazioni pubblicate NON costituiscono in alcun modo un servizio di consulenza, né di offerta ai lettori. Marco R. A. Bozzetti, Malabo Srl, Reportec Srl, AIPSI, gli Sponsor ed i Patrocinatori di OAD 2020 NON sono e NON potranno essere responsabili di qualsivoglia perdita o danno in cui si possa incorrere in seguito all'affidamento sul contenuto delle analisi e delle indicazioni del presente Rapporto 2020 OAD.

Pubblicato il 24 dicembre 2020.
Tutti i marchi depositati e i marchi di fabbrica citati nel presente documento sono dei rispettivi titolari.

AIPSI c/o Malabo srl Via Savona, 26 20144 Milano - tel. 02 39443632 aipsi@aipsi.org
Malabo Srl Via Savona 26 20144 Milano - tel. 02 39443632 info@malaboadvisoring.it
Reportec srl Via Marco Aurelio, 8 20127 Milano - tel.02 36580441 info@reportec.it

Sommario

1. Premessa

Il presente documento rappresenta **una sintesi** del completo **Rapporto 2020 OAD**, Osservatorio Attacchi Digitali in Italia, scaricabile da https://www.oadweb.it/it/oad-2020/per-scaricare-il-rapporto-2020-oad.html, dopo aver fatto il login al sito stesso (per registrarsi basta a inserire pochi dati personali in https://www.oadweb.it/it/component/comprofiler/registers.html).
Obiettivo del presente compendio è di fornire, in maniera semplice e chiara, i risultati dell'indagine OAD 2020, anche per il personale non specializzato nella sicurezza digitale.
Per renderlo più semplice e leggibile, la struttura del presente compendio è diversa da quella del Rapporto finale completo, e non contiene i dettagli e gli allegati del documento originale completo, cui si rimanda per approfondimenti.

2. A che cosa serve il Rapporto 2020 OAD

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 Telecomunicazioni.
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 OAD 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 aziende ed enti pubblici di varie dimensioni e appartenenti a vari settori merceologici, l'indagine OAD fornisce precise e contestuali indicazioni sul fenomeno degli attacchi digitali in Italia, e sulle misure di sicurezza di prevenzione e contrasto a tali attacchi, considerando anche piccole e piccolissime organizzazioni che normalmente le altre indagini nazionali ed internazionali non considerano.

Tale fotografia realmente contestualizzata alla realtà italiana **aiuta i responsabili** delle aziende/enti:

- A prendere coscienza dei rischi e delle problematiche digitali che possono abbattersi sui loro sistemi informatici, che **sono ormai basilari per garantire la continuità operativa delle loro attività e dei loro processi**;
- A **sensibilizzare** sul tema della sicurezza digitale tutti i livelli del personale, dai decisori di vertice agli utenti finali, facendo circolare e leggere questo compendio e, per gli specialisti, il Rapporto completo 2020 OAD
- Ad attuare e redigere, se necessario, **l'analisi delle vulnerabilità e dei rischi digitali**, in particolare per la compliance a normative quali la privacy secondo il GDPR
- A **verificare le misure tecniche, organizzative, di gestione e governo** della sicurezza digitale in atto nell'ambito del proprio sistema informatico, con possibili riscontri sulle soluzioni di miglioramento e potenziamento del loro livello di sicurezza digitale da chiedere ai fornitori.

OAD, con il questionario 2020, ha offerto a chi completava il questionario una macro-valutazione qualitativa del livello di sicurezza digitale nei loro sistemi informatici, in funzione delle risposte selezionate.

In un ambito digitale il problema non è se si verrà attaccati, ma quando e come. Adottare una politica di prevenzione dai cyber-attacchi è diventata una stringente ed ineludibile necessità per ogni organizzazione di qualsiasi dimensione, anche piccolissima, e di qualsiasi settore merceologico. Per l'attuazione di tale politica occorre fare scelte precise, contestualizzate alla propria realtà ed al proprio sistema informatico, oltre che lungimiranti, ossia anche a medio-lungo termine.

I rischi digitali sono dovuti a molteplici fattori, di cui i principali sono le vulnerabilità tecniche, organizzative e degli utenti dei sistemi informatici, sinteticamente considerate nel successivo paragrafo §5.

3. Il quadro generale di vulnerabilità e attacchi digitali

Gli attacchi digitali sono un fenomeno di portata crescente, al pari della crescita del business digitale e della sua complessità, e in grado di portare incredibili guadagni illeciti ai cyber criminali: il progetto europeo di ricerca Hermeneut[1] sulla cybersecurity stima per il 2021 danni a livello mondiale per attacchi digitali pari a 6 trilioni di dollari, una cifra ben superiore ai danni per droga: danni che in gran parte costituiscono il guadagno per i criminali digitali e che si basano prevalentemente sulle vulnerabilità "umane" dell'utente informatico, con attacchi di social engineering quali spear phishing. Quasi ogni attività e/o processo di un'azienda ed ente pubblico è ormai supportata da applicazioni del Sistema Informatico (SI). Sistema sempre più complesso perché eterogeneo, incentrato su Internet, in parte utilizzando servizi in cloud, acceduto da utenti interni ed esterni con sistemi mobili e con sistemi fissi. Il tutto implica integrazioni tra reti fisse e mobili, e l'integrazione funzionale e l'interoperabilità con il SI dei sistemi di automazione industriale e della logistica, e di innumerevoli sistemi di controllo basati su sistemi IoT, Internet of Things: ambienti determinanti ed essenziali per il settore manifatturiero, la logistica, la sanità, l'agro-alimentare, i servizi pubblici ed il controllo del territorio. Nei moderni SI la sicurezza digitale assume un ruolo cruciale non solo per la corretta funzionalità del SI, delle sue applicazioni e dei dati trattati, ma in particolar modo per garantire la continuità operativa (business continuity) dei processi e delle attività dell'intera azienda/ente, o almeno di quelle essenziali e prioritarie. Il SI e la sua sicurezza digitale sono degli elementi fondamentali per il business o per le attività/servizi delle PA: le informazioni trattate sono un vero e proprio bene (asset) e come tali vanno, o dovrebbero essere, protette e gestite. Il loro governo e gestione non sono solo "meri problemi tecnici", ma dell'intera organizzazione per il suo business o per le sue attività/sevizi, e richiede pertanto il diretto coinvolgimento del vertice organizzativo, per aziende/enti di qualsiasi settore e di qualsiasi dimensione**.**

3.1 Le vulnerabilità

Tutte le minacce ICT, intenzionali e non, si basano su vulnerabilità che possono essere categorizzate in tecniche, delle persone, dell'organizzazione.
Le vulnerabilità delle persone sono le più critiche, dato che riguardano il comportamento umano in ambito digitale sia per gli utenti finali sia, in particolar modo, per gli utenti privilegiati: il comportamento umano non è sempre prevedibile ed è difficilmente limitabile/controllabile. La vulnerabilità di una persona per l'ICT è il più delle volte involontaria e causata da fattori quali l'inconsapevolezza, l'imprudenza, l'imperizia, l'ignoranza, dovute e spesso aggravate dalla mancanza di formazione e addestramento, oltre che da carenze ed inefficienze organizzative, quali la mancanza di procedure scritte e divulgate, la mancanza di reali controlli etc.

3.2.1 Le vulnerabilità tecniche

A livello tecnico esistono qualificati ed aggiornati siti che elencano, classificandole, le vulnerabilità riscontrate, quali ad esempio CVE/MITRE e la statunitense NVD, National Vulnerability Database.
Per ciascuna vulnerabilità questi siti riportano, se presenti, le modalità per eliminarle.
L'argomento delle vulnerabilità è molto ampio, a livello tecnico estremamente dettagliato, e si rimanda per ulteriori approfondimenti alle fonti citate.

[1] https://www.hermeneut.eu/

Le vulnerabilità tecniche crescono parallelamente alla crescita della complessità dei moderni sistemi informatici, sempre più difficili da gestire anche se di piccole dimensioni e con limitate funzionalità, come sono generalmente quelli usati da piccole e piccolissime organizzazioni, che in Italia rappresentano la stragrande maggioranza.
In termine generali, per le vulnerabilità tecniche:

- non tutte le vulnerabilità esistenti sono state individuate e classificate negli elenchi CVE e NVD: quelle non ancora individuate, ed indicate con il termine "zero-day", sono le più critiche, perché non prevedono ancora alcuna protezione e, se l'attaccante le conosce, può attaccare senza trovare alcun contrasto;
- per alcune vulnerabilità conosciute sono occorsi talvolta mesi prima di avere a disposizione una patch correttiva; pertanto, esistono vulnerabilità note ma senza una correzione disponibile;
- la tendenza negli anni è una leggera crescita delle vulnerabilità tecniche;
- non esiste prodotto ICT, di nessun fornitore, che non abbia delle vulnerabilità note.

Siamo quindi ben lontani, per ora, da sistemi ICT intrinsecamente e totalmente sicuri, come discusso in §4.3.

3.2.2 Le vulnerabilità delle persone

Le vulnerabilità delle persone rappresentano per il mondo digitale rischi ancora più diffusi e gravi rispetto a quelle tecniche: e sono amplificate dalle vulnerabilità organizzative di cui in §5.3
Per le vulnerabilità personali lo strumento di contrasto più importante è la formazione continua e la consapevolezza che, nell'uso dei sistemi informatici, occorre comportarsi sempre in maniera attenta ed etica, seguendo le indicazioni che dovrebbero essere state divulgate dall'Azienda/Ente come policy, linee guida e procedure organizzative. E in Italia tale consapevolezza è molto carente, come indicato dall'indice DESI 2020 mostrato in fig. 5.2-1.
L'indice DESI indica il livello di digitalizzazione dell'economia e della società per tutti i paesi dell'UE, Unione Europea, ed è costituito da 5 indicatori che valutano la connettività, il capitale umano in termini di competenze e di inclusione digitale, l'uso dei servizi Internet, l'integrazione delle tecnologie digitali, la disponibilità di servizi pubblici digitali.
La fig. 5.2-1 mostra che l'Italia ha un forte ritardo nella trasformazione digitale, posizionandosi nel 2020 al quart'ultimo posto. L'aspetto più grave, chiaramente indicato fig. 5.2-2, è che dei 5 parametri considerati, l'Italia ha il valore più basso di tutti sul capitale umano. Il valore 2020 di questo è per l'Italia del 42% contro il 58% della media UE per tutti i paesi della comunità e contro il 70% della Germania.
Una simile carenza di competenze digitali è il fattore principale per la vulnerabilità delle persone, soprattutto a livello business e delle attività digitali delle Pubbliche Amministrazioni (PA). Il problema delle competenze ICT in Italia, anche solo di base, costituisce un grave "minus" nella competitività del nostro paese, non solo in ambito europeo ma mondiale.
Le specifiche competenze per la sicurezza digitale sono ancor più ridotte, essendo un di cui delle più generali dell'ICT, ed incidono profondamente sul livello di sicurezza digitale delle singoli organizzazioni e dell'intero paese. Considerando l'enorme numero di piccole e piccolissime aziende e amministrazioni pubbliche, l'elevata incompetenza sulla sicurezza digitale lascia ampio spazio al millantato credito e a comportamenti scorretti di numerosi attori ed interlocutori dell'offerta, che rasentano sovente la truffa. Come già evidenziato in §4.3.1, questa mancanza è un effetto leva per una forte terziarizzazione della sicurezza digitale, ma al contempo pone evidenti difficoltà nella scelta del fornitore con una soluzione adeguata alla propria realtà.

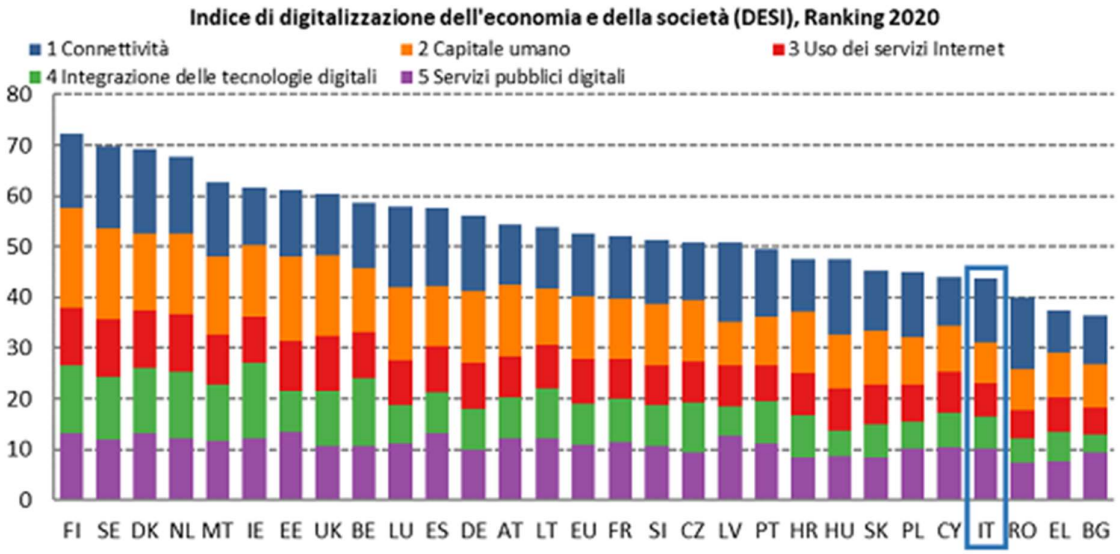

Fig. 3.2.2-1 (Fonte: DESI)

3.2.3 Le vulnerabilità organizzative

Gli aspetti organizzativi sono determinanti per l'attuazione di una reale ed effettiva sicurezza digitale ed impattano sul personale utente del sistema informatico.
Le piccole e medie organizzazioni - ma sovente anche quelle grandi - difficilmente possono disporre al proprio interno delle competenze tecniche ed organizzative aggiornate per la sicurezza digitale: devono terziarizzarle ma, al contempo, devono saperle controllare ed indirizzarle rispetto al loro specifico contesto. In caso contrario dipendono e dipenderanno sempre più dagli outsourcer, che a loro volta potrebbero avere non adeguate competenze nella cybersecurity: e, in tal senso, il cerchio delle incompetenze si chiude con possibili conseguenze molto negative per l'Azienda/Ente, anche al di fuori delle eventuali truffe.
Per quanto concerne il lato domanda ICT, almeno a livello di vertice, occorre acquisire quelle competenze necessarie per saper scegliere fornitori competenti e affidabili, e saperli supervisionare nella gestione della sicurezza digitale; essa non rappresenta solo un problema tecnico, ma anche di business, dato che deve garantire la continuità operativa dell'Azienda/Ente.

3.3 L'evoluzione degli attacchi digitali

Gli attacchi digitali possono essere raggruppati in due grandi categorie:

- Gli **attacchi mirati**, che hanno ciascuno uno specifico obiettivo target che viene attentamente analizzato, ed attaccato con varie sofisticate tecniche, anche contemporaneamente;
- Gli **attacchi massivi**, che si basano sul portare attacchi digitali ad un ampio numero di potenziali vittime: sono indirizzati ad un grande numero di aziende, enti ed anche singole persone.

Da qualche anno gli attacchi digitali divengono più sofisticati e pericolosi, con una combinazione ben bilanciata di competenze e capacità tecniche, e il principale elemento di entrata nel sistema informatico target è quasi sempre il phishing o altre modalità di social engineering.
Le caratteristiche tecniche e le logiche più innovative dei moderni attacchi includono:

- Utilizzo delle più avanzate tecniche digitali, quali l'intelligenza artificiale ed il machine learning, per la realizzazione di sistemi di attacco digitale funzionanti prevalentemente in maniera automatica. Le tecnologie digitali sono le stesse usate da chi protegge e da chi

attacca un sistema: ma questi ultimi sono spesso più pronti e determinati ad un loro più efficace utilizzo.

- Malware polimorfici, modulari, con capacità di modificarsi, di replicarsi e di eludere la sua individuazione; taluni sono usati anche come veicoli di altre minacce. Tra gli ultimi diffusi in Italia: Emotet, Qbot e Valak.
- Attacchi tramite ransomware "duplici": da un lato blocco del sistema attaccato criptando gli hard disk, dall'altro furto dei dati e minaccia di pubblicarli se non sarà pagato il riscatto. Attacchi riusciti di questo tipo includono quelli attuati nel 2020 a Campari, Enel, Geox, Luxottica, Optima.
- Uso crescente di chatbot[2] per comportamenti malevoli verso gli utenti e come vettori di attacchi digitali. Tipici esempi di usi malevoli includono spamming, chat malevoli di intimidazione, molestie e bullismo (*harassment*), far collassare servizi e collegamenti di emergenza, fornire informazioni e suggerimenti errati e malevoli, richiedendo informazioni riservate utili per attacchi e frodi digitali, e coì via.
- Forte aumento degli attacchi a sistemi IoT-IIoT, soprattutto per quelli basati su hardware e sistemi operativi obsoleti, e gestiti lacunosamente e separatamente dal sistema informatico. In taluni casi, simili attacchi possono comportare problemi anche seri alla salute e alla sicurezza fisica delle persone coinvolte ed interagenti col sistema ICT attaccato: si pensi, ad esempio, ad attacchi in ambito ospedaliero, o a robot o a sistemi di automazione industriale che, in caso di attacchi, possono ferire gli operatori a loro vicini; tipico è il caso di un braccio di un robot che colpisce l'operatore.
- Crescente diffusione di "fileless malware". Con questo termine si indicano malware che operano solo nelle aree volatili del sistema, quali le memorie RAM, i registri e le aree di servizio del sistema attaccato, senza scrivere dati negli hard disk: di qui il nome di "fileless", senza file. Questo tipo di malware non è nuovo: le prime tipologie sono state riscontrate nei primi anni duemila con, ad esempio, Code Red e SQLSlammer. Gli strumenti usati per inoculare fileless malware sono prevalentemente i legittimi software di supporto ai sistemi operativi dell'unità, fisica o virtuale, attaccata: tipici esempi sono il Power Shell ed i suoi script nel mondo Windows che, dopo aver acquisito tipicamente da remoto i diritti di accesso di utente privilegiato, possono sfruttare la vulnerabilità del sistema. A seconda di dove e come viene inserito il fileless malware, esso può essere persistente o durare finché il sistema non viene chiuso e fatto ripartire (reboot). L'uso crescente di questo tipo di attacco è dovuto alle difficoltà di rilevamento e rimozione.
- Crescita degli attacchi ai beni intangibili, sia indirettamente a causa dell'attacco diretto ad altri obiettivi, sia direttamente tramite un attacco specifico per colpire tali beni immateriali. Un esempio è dato da attacchi di tipo *crowdturfing*[3] e, più in generale, su campagne di disinformazione (fake news) e di manipolazione dell'opinione di un determinato insieme di persone.

Secondo recenti indagini internazionali, l'Italia è uno dei paesi più colpiti al mondo con ransomware, nonché il più colpito in Europa. Attualmente, si è così riscontrata una crescente sovrapposizione e difficoltà a distinguere tra attacchi digitali e *cyber warfare*, vere e proprie guerre informatiche.

4 L'indagine OAD 2020

L'indagine OAD 2020 ha fatto riferimento all'**intero anno 2019** ed al 1**° quadrimestre 2020**, quando è esplosa la pandemia del Covid-19 che ha portato ad un'ampia gamma di attacchi, causata

[2] I chatbot sono programmi software realizzati per interagire con gli umani vai voce e/o scambi di testi. Hanno numerose applicazioni, in primis come assistenti virtuali digitali di supporto agli utenti. Al di là dei loro utili e corretti utilizzi, possono essere usati come vettori di attacchi digitali.

[3] Il termine indica un *attacco basato su recensioni scorrette e false per danneggiare la reputazione di un prodotto o di una azienda/ente*

soprattutto dall'improvviso - ed in parte impreparato - passaggio di molti all'*agile working* da casa e ad un forte utilizzo di ogni tipo di servizio su Internet.

Il **bacino di rispondenti** copre tutti i settori merceologici, incluse le Pubbliche Amministrazioni, anche se la maggior parte di aziende rispondenti appartiene al settore ICT (30,8%). In termini di dimensioni delle Aziende/Enti dei rispondenti, come numero di dipendenti, il bacino emerso è ben bilanciato per le 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. La libera indagine OAD 2020 riesce ad indagare sulle piccole e piccolissime organizzazioni: il 57,5% dei rispondenti appartiene a strutture con un organico inferiore ai 250 dipendenti, e di queste il 22,1% sotto i 10.

4.1 I trend degli attacchi digitali in Italia dalle indagini OAD

La fig. 4.1-1 confronta il numero di attacchi rilevati nei diversi Rapporti OAI dal 2007 al 1° quadrimestre 2020. Tale confronto non ha valenza statistica ed è da considerare come tendenza puramente indicativa, dato che i campioni dei rispondenti nei diversi anni sono diversi come composizione e come numero. Nell'arco temporale considerato, la figura evidenzia come, a parte il 2008 che rappresentò il primo *annus horribilis* per la quantità di attacchi occorsi, dal 2007 al 2015 si è avuta una oscillazione del numero di attacchi rilevati attorno a circa il 40% dei rispondenti, e dal 2015 è iniziata una continua crescita percentuale degli attacchi rilevati fino al 2018 che ha rappresentato non solo il picco più alto in tutti gli anni di indagine OAD, ma anche l'unica volta in cui la percentuale di attacchi rilevati supera la percentuale di quelli non occorsi/rilevati addirittura per più di 10 punti. Dal 2016 il trend medio si è attestato attorno al 45%. Nel 2019 gli attacchi digitali sui Sistemi Informatici del bacino dei rispondenti sono ammontati al 46,6% del totale, mentre nel 1° quadrimestre 2020 si sono attestati al 44,8%. Nel 2019 il trend di crescita dei precedenti tre anni si arresta: ma come andrà per l'intero 2020? Crescerà rispetto al 2019 con l'inizio di un'altra ondata di cresita? Impossibile prevedere la tendenza, dato che i valori nei vari anni dell'indagine non sono statisticamente confrontabili in virtù del diverso bacino di rispondenti di volta in volta emerso. Lo si potrà verificare con la prossima indagine OAD del 2021.
Le ondate altalenanti nei vari anni della percentuale di attacchi rilevati ben rappresenta la continua battaglia tra "guardie e ladri" e l'avvicendarsi di innovazioni sulle modalità d'attacco, cui poi seguono misure di difesa atte a contrastarli, ma con gli ovvi fisiologici ritardi.
Dal 2015 al 2018, il numero di Aziende/Enti che hanno rilevato attacchi è percentualmente sempre cresciuto: **un chiaro indicatore della criticità degli attacchi portati e delle misure di sicurezza di contrasto che non si sono rilevate adeguate**.

I trend emersi dai 12 anni consecutivi di indagini OAD in Italia rappresentano l'effettiva situazione, e sono quindi di reale riferimento per l'utilizzo del Rapporto come indicato nel precedente §2? Secondo l'autore sì, in quanto:

- più dei 2/3 dei rispondenti, specificatamente nell'indagine 2020, ha dichiarato di avere mediamente buone misure di sicurezza digitale, e d'altronde il 30% di rispondenti appartiene al settore ICT;
- come indicato dalle più recenti statistiche ISTAT (http://dati.istat.it/Index.aspx?DataSetCode=DICA_ASIAUE1P), in Italia è elevatissimo il numero di piccole e piccolissime imprese: 99,91% le imprese sotto i 250 dipendenti, le cosiddette PMI, ed il 95% circa è costituito da aziende con meno di 9 dipendenti; come già indicato in precedenza, il 57,5 % dei rispondenti all'indagine 2020 OAD appartiene a PMI o ad enti pubblici di analoga struttura dimensionale. Queste aziende/enti **non sono un target significativo** per **attacchi mirati**, ma al massimo per **attacchi massivi** per cogliere qualche sistema non sufficientemente protetto: si pensi al ransomware, o per motivazioni di hactivism o cyber terrorismo;
- se l'Azienda/Ente non ha rilevato l'attacco portato, come spesso succede, significa che il

danno subito non era rilevante, a parte l'eventuale furto di informazioni.

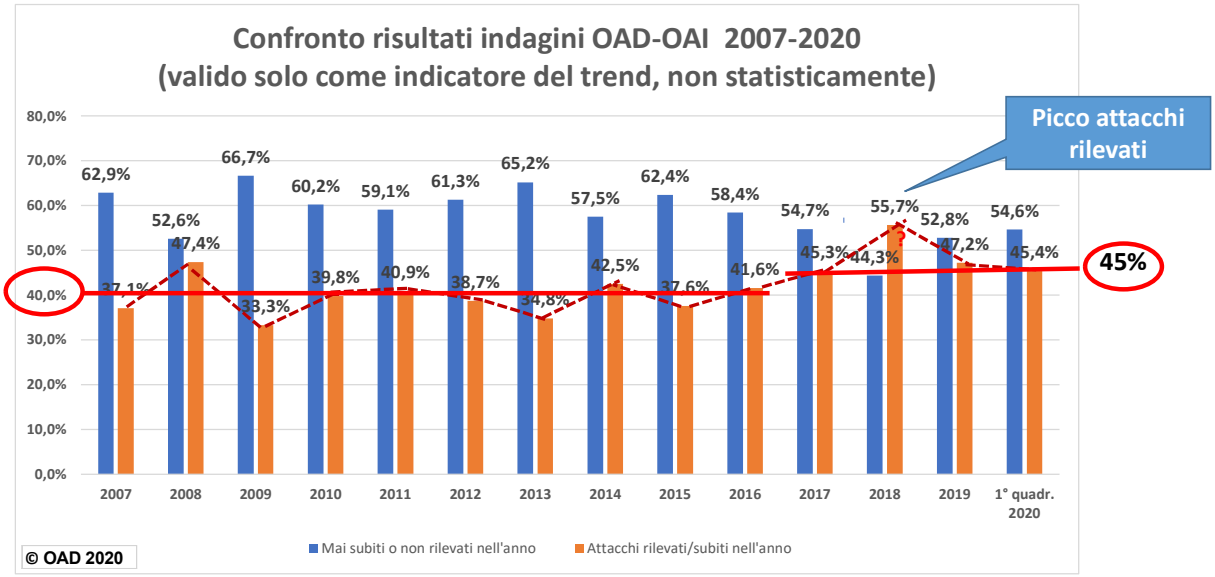

Fig. 4.1-1

4.2 Tipologia di attacchi digitali e meccanismi di attacco rilevati nell'indagine 2020 OAD per il 2019 ed il 1° quadrimestre 2020.

La fig. 4.2-1 ordina, in percentuale, la diffusione nel 2019 e nel 1° quadrimestre 2020 **delle quindici tipologie di attacco** considerate e rilevate dai rispondenti: tipologie di attacco che individuano il "**che cosa**" viene attaccato (per i dettagli metodologici si rimanda all'Allegato A del Rapporto 2020 completo). I dettagli forniti dai rispondenti per ogni tipologia di attacco sono descritti e commentati negli specifici paragrafi del citato Rapporto completo.

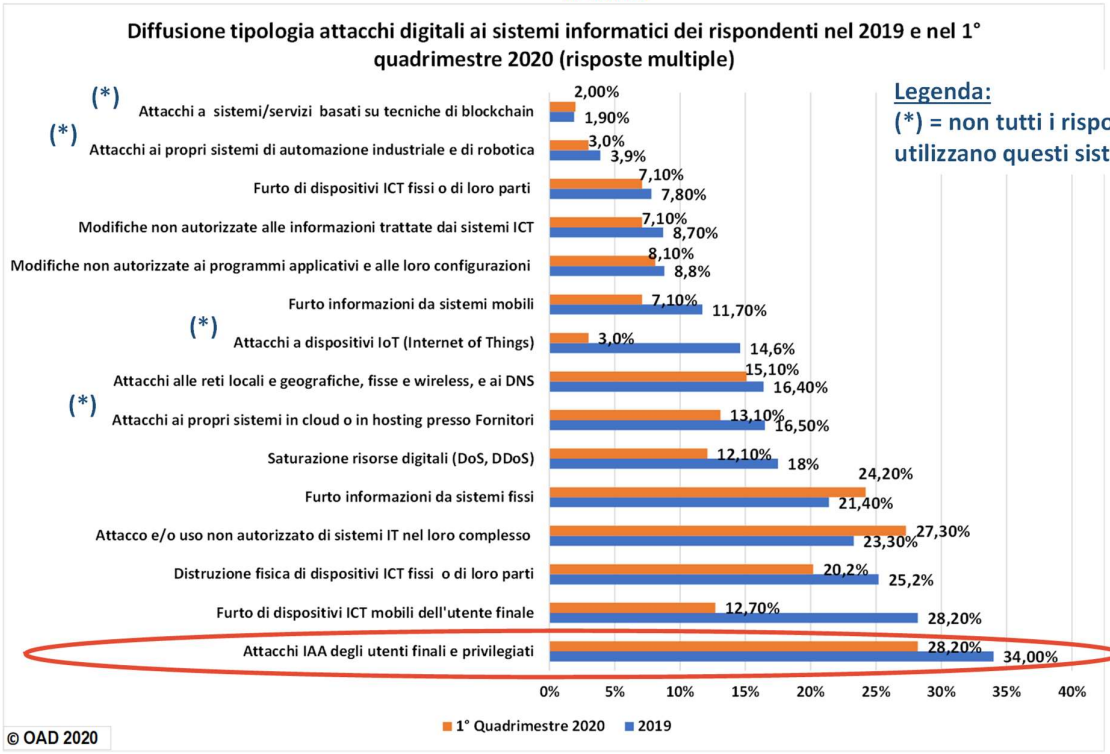

Fig. 4.2-1

Le percentuali indicate nella figura per ogni tipologia d'attacco sono calcolate rispetto al totale dei rispondenti al questionario. Come indicato nella legenda della figura per (*), taluni sistemi quali quelli in Cloud, i sistemi IoT, i sistemi di automazione industriale/robotica ed i sistemi con tecniche di blockchain, sono utilizzati solo in alcuni Sistemi Informatici dei rispondenti.
L'ordinamento dall'alto in basso delle tipologie di attacco più diffuse in percentuale rilevate dai rispondenti nella fig. 4.2-1 fa riferimento, con la barra blu, al 2019. La barra arancione associata fa riferimento a 1° quadrimestre 2020.
Al primo posto sia per il 2019 che per il 1° quadrimestre 2020, si posizionano gli attacchi al controllo degli accessi, come si era rilevato negli anni 2018 e 2017 dei precedenti rapporti OAD, pur con percentuali diverse.
Come diffusione tra i rispondenti seguono, a decrescere di pochi punti percentuali, le altre 14 tipologie d'attacco, le cui caratteristiche ed i cui impatti sono approfonditi nei relativi paragrafi del Rapporto completo.
Come tecniche di attacco, ossia come si attacca, tutte le sette famiglie considerate nel questionario sono state largamente impiegate nei vari tipi d'attacco, talvolta anche contemporaneamente, come mostrato nella fig. 4.2-2. La più diffusa, quale media sui vari attacchi rilevati dal bacino di rispondenti, è **l'uso di toolkit** (rootkit, meta-exploit, 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.

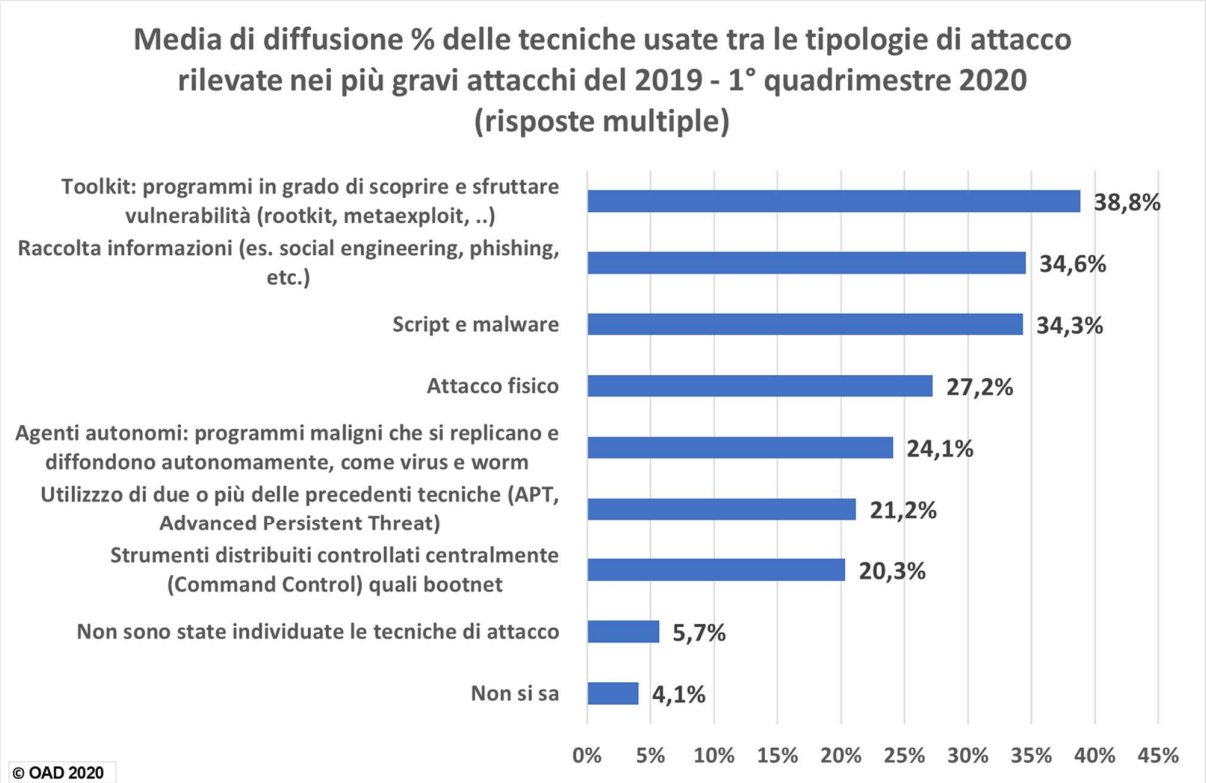

Fig. 4.2-2

In sostanza, la diffusione delle varie tipologie di attacchi rilevate nell'indagine 2020 si con quelle rilevate nei principali rapporti internazionali e nazionali sugli attacchi digitali, valori delle percentuali a parte, e conferma così la correttezza dei valori forniti dall'indagine OAD 2020.

4.3 L'impatto della pandemia Covid-19 sugli attacchi digitali in Italia

Il 2020 sarà ricordato per l'esplosione della pandemia del Covid-19, scoppiata in Italia proprio nel 1° quadrimestre e che ha avuto, ed ancora sta avendo, forti ripercussioni sugli attacchi digitali, sia a livello mondiale che in Italia.
In pochi giorni sempre più persone sono state costrette a ricorrere al lavoro da remoto sia con connessioni fisse o mobili che ha inevitabilmente ampliato l'area di vulnerabilità,tra cui possiamo annoverare:

- Collegamenti non protetti tra i dispositivi d'utente e le applicazioni sui server, fisici o virtualizzati, on premise o terziarizzati/in cloud.
- Aumento crescente dell'utilizzo dei dispositivi ICT di proprietà dell'utente, dal PC al tablet e allo smartphone, sui quali raramente sono stati attivati gli opportuni strumenti di sicurezza

A questi si sono affiancati specifici attacchi basati su informazioni e servizi sulla pandemia, che includono:

- Phishing e spear phishing con informazioni sulla pandemia, talvolta false;
- Creazione di specifici malware e ramsoware;
- Ampia diffusione di siti malevoli inerenti la pandemia ed il Covid-19, sovente linkati alle e-mail di phishing;
- Utilizzo del Remote Desktop Protocol di Windows (RDP) come veicolo di attacco. RDP è un diffuso strumento per i server Windows che consente l'accesso da remoto, quindi agli agile workers. Molti attaccanti hanno provato a sfruttare RDP cercando la password dell'utente

con tecniche automatiche di deep crack (forza bruta) e/o sfruttando le mal configurazioni del RDP sul server.

Il Rapporto 2020 OAD, con l'indagine anche statisticamente valida per il medesimo bacino di rispondenti, fornisce una preziosa indicazione dell'impatto della pandemia nel 2020 rispetto al 2019, evidenziata nella fig. 4.3-1.

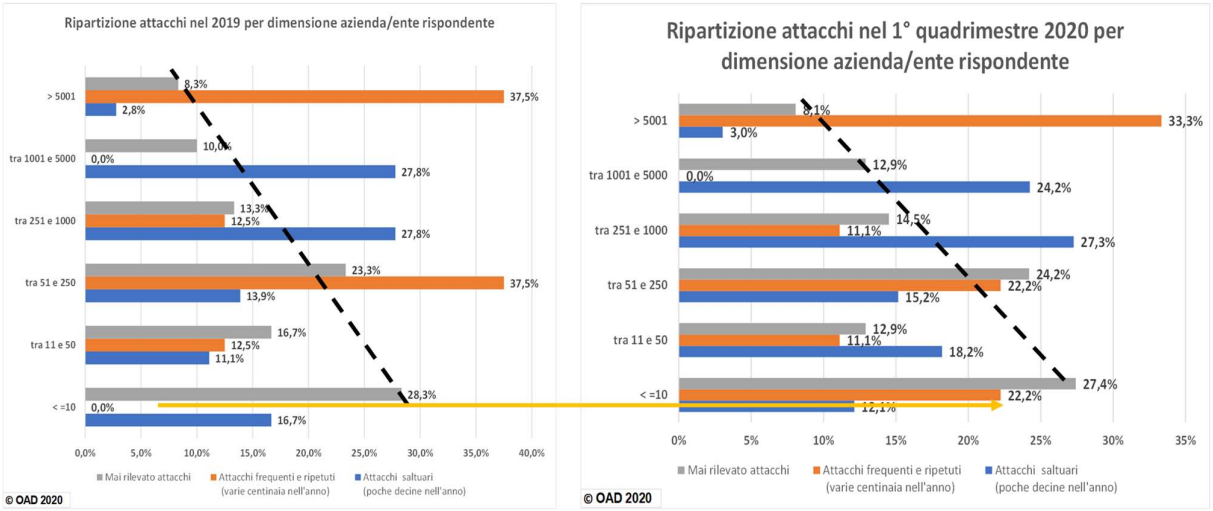

Fig. 4.3-1

Questo è confermato analizzando il confronto in fig. 4.3-1 che mostra la distribuzione percentuale degli attacchi digitali subiti o non nel 2019 e nel 1° quadrimestre 2020 per dimensione delle aziende/enti dei rispondenti. In entrambi i periodi considerati la percentuale di attacchi non rilevati è decrescente dalle piccolissime organizzazioni con meno di dieci dipendenti alle grandissime con più di 5001. Si noti che le percentuali sono calcolate e fanno riferimento, per ciascun periodo, al rilevamento di saltuari attacchi o al rilevamento di frequenti e ripetuti attacchi.

4.3.1 I dati forniti dalla Polizia Postale e delle Comunicazioni

La Polizia Postale e delle Comunicazioni, grazie alla sua responsabile nazionale, il Direttore dott.ssa Nunzia Ciardi, ha fornito significativi dati sulle azioni svolte in Italia nel 2019 e nel 1° quadrimestre 2020 sul fronte del contrasto agli attacchi digitali e ai crimini informatici, facendo in particolare riferimento alle infrastrutture critiche, al crimine digitale finanziario, al cyber terrorismo.

La tabella di fig. 4.3.1-1 fa riferimento alle infrastrutture critiche monitorate dal Il C.N.A.I.P.I.C., Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (https://www.commissariatodips.it/profilo/cnaipic/index.html): è una struttura della Polizia Postale e delle Comunicazioni incaricata in via esclusiva della prevenzione e della repressione dei crimini informatici di matrice comune, organizzata o terroristica, che hanno come obiettivo le infrastrutture informatizzate di natura critica e di rilevanza nazionale. Queste includono tipicamente le infrastrutture ICT per la produzione e distribuzione di ogni forma di energia (elettricità, gas, etc.), per le reti di telecomunicazione, per le reti idriche, per la sanità, per i trasporti (aereo, navale, ferroviario, stradale), per le banche ed i servizi finanziari, per la protezione e la difesa civile e militare, per il supporto degli organi governativi centrali e territoriali. Il numero delle persone arrestate è risalito da 1 ad appena 3, nonostante il forte aumento delle denunce osservato nel 2019, quasi decuplicato rispetto all'anno precedente.
Il problema di fondo, già evidenziato e commentato nelle scorse indagini OAD, di fatto non cambia: a fronte di centinaia di attacchi rilevati, in concreto il numero totale di arrestati è minimo

Il cyber crime rimane di fatto quasi impunito, nonostante l'Italia abbia adottato da anni una precisa e severa legislazione - anche in ambito penale - relativa al computer crime, e vi sia una forza specifica di Polizia, la Polizia Postale, operante sul territorio e con il supporto di unità specializzate dell'Arma dei Carabinieri e della Finanza. In secondo luogo, le leggi sul computer crime differiscono notevolmente tra i vari paesi, ed anche a livello europeo: risulta pertanto assai difficile, soprattutto al di fuori della UE, poter effettuare delle rogatorie. In terzo luogo, la problematica del computer crime e la sua pericolosità per ogni attività e per ogni business sono ancora sottostimate, soprattutto da parte del management aziendale e delle Pubbliche Amministrazioni. Infine, le problematiche insite nella giustizia italiana, in ambito organizzativo ed afferenti alle tempistiche dei procedimenti, notoriamente lunghe, incidono significativamente sulla impunibilità di fatto dei reati informatici.

Protezione strutture critiche	1 gen - 30 apr 2020	1 gen - 31 dic 2019	1 gen – 31 dic 2018	1 gen – 31 dic 2017	1 gen – 31 dic 2016
Attacchi rilevati	282	1181	459	1.032	644
Alert diramati	24.824,00	82.484,00	80.777	31.524	8.721
Indagini avviate	34	155	74	72	70
Persone arrestate	0	3	1	3	3
Persone denunciate	0	117	14	1.316	1.226
Perquisizioni	n.d.	n.d.	n.d.	73	58
Richiesta di cooperazione internazionale in ambito Rete 24/7 High Tech Crime G8 (Convenzione Budapest)	17	79	108	83	85
Indagini avviate su attacchi rilevati	12,05%	13,12%	16,12%	6,98%	8,29%
Persone arrestate su persone denunciate	0%	2,50%	7,14%	0,23%	0,24%

Fig. 4.3.1-1
(Fonte: Polizia Postale e delle Comunicazioni)

La fig. 4.3.1-2 evidenzia il fenomeno del Financial Cyber Crime ed il notevole impatto della pandemia, almeno nel primo quadrimestre 2020, che risulta essere dello stesso livello di grandezza d'intero 2019, come transazioni bloccate.

Financial Cyber Crime	1 gen - 30 apr 2020	1 gen - 31 dic 2019	1 gen – 31 dic 2018	1 gen – 31 dic 2017	1 gen – 31 dic 2016
Transazioni Fraudolente Bloccate	€ 20.200.000,00	€ 21.333.990,00	€ 38.400.000,00	€ 20.839.576,00	€ 16.050.812,50
Somme Recuperate	€ 8.700.000,00	€ 18.000.000,00	€ 9.000.000,00	€ 862.000,00	nd
Arrestati	nd	nd	nd	25	25
Denunciati	nd	nd	nd	2.851	3.772
Recupero/frode	43,06%	84,37%	23,44%	4,14%	

Fig. 4.3.1-2
(Fonte: Polizia Postale e delle Comunicazioni)

Nel contrasto al cyber terrorismo nel 2019 sono stati controllati 36.000 siti web e cancellati 250 contenuti; nel 1° quadrimestre 2020 sono stati controllati 11.962 siti web.

4.4 Gli impatti subiti dagli attacchi digitali più gravi

Gli impatti a seguito degli attacchi più gravi sono analizzati per ogni tipologia di attacco, così come le possibili motivazioni degli attaccanti ed i tempi di ripristino a seguito degli attacchi più gravi.
Tutti questi approfondimenti variano per ogni tipologia di attacco, cui si rimanda ai vari paragrafi del rapporto, ma in linea generale emerge che:

- gli impatti dichiarati dai rispondenti si bilanciano mediamente tra quelli irrilevanti e/o facilmente risolvibili con ripristini in tempi brevi e a costi limitati, e quelli gravi con serie interruzioni dei servizi digitali, che richiedono costosi e lunghi interventi di ripristino, perdita

di immagine e in taluni casi di business e di clienti; queste due diverse valenze degli impatti dipendono dalle misure di sicurezza in essere;

- 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.

5. Tipologia attacchi digitali e tecniche di attacco più temute per il prossimo futuro

La fig. 5-1, basata sulle risposte multiple dei rispondenti, mostra quali sono le tipologie di attacco ritenute più pericolose dai rispondenti, e quindi più temute nel prossimo futuro, indipendentemente dagli attacchi eventualmente subiti.

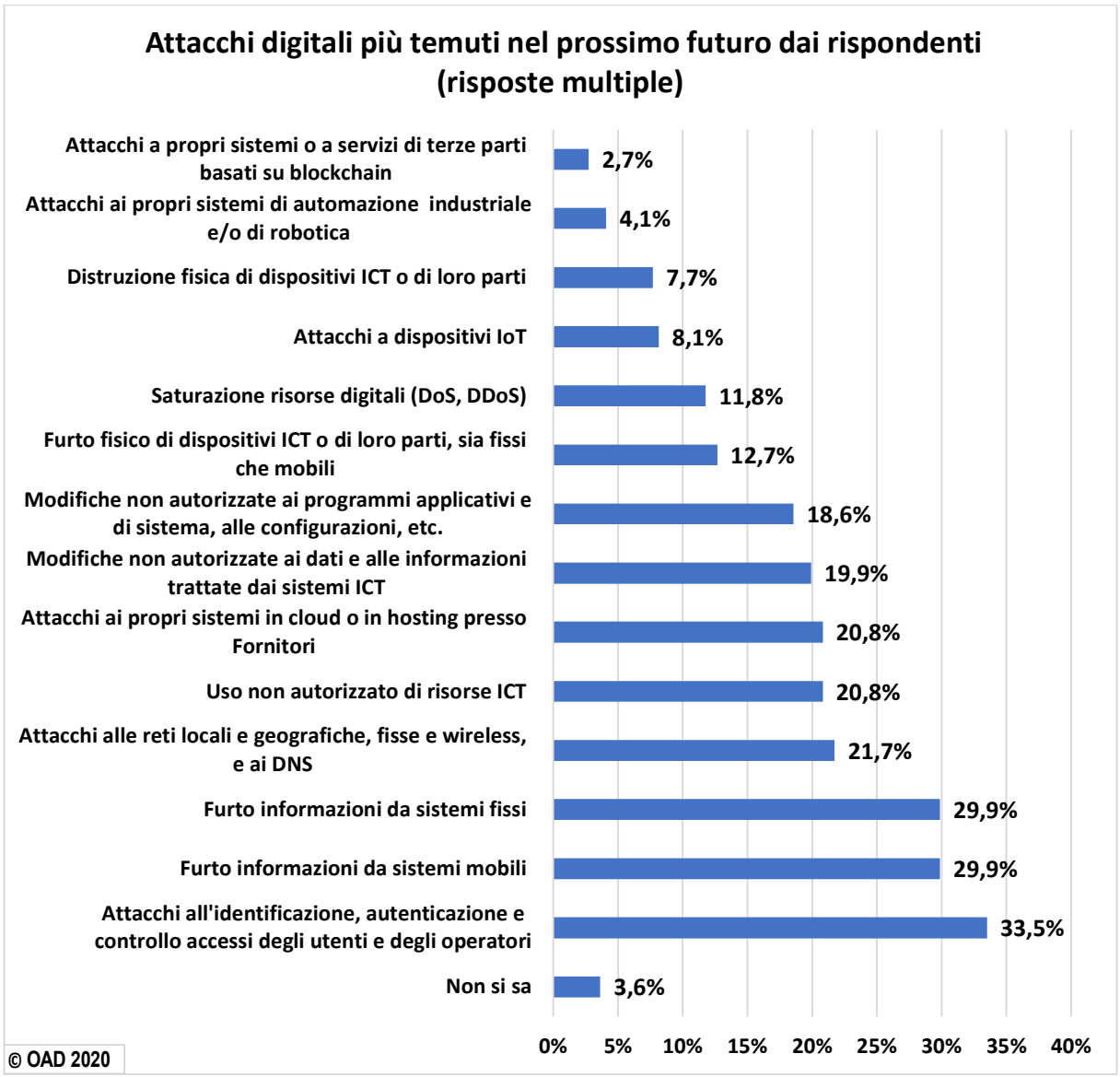

Fig. 5-1

Come è ragionevole aspettarsi e come si è verificato anche nelle precedenti indagini di OAD/OAI, per il futuro rimangono forti timori in relazione ad alcuni degli attacchi più diffusi rilevati negli anni precedenti, e in particolare nel 2019 e nel 1° quadrimestre 2020 (si veda fig. 4.2-1 e 2).
L'attacco più temuto da poco più di 1/3 dei rispondenti risulta quello all'IAA, seguito con pochi punti percentuali e alla pari dal furto delle informazioni da dispositivi fissi e da quelli mobili. Seguono poi con un 21,7% gli attacchi alle reti e con un punto percentuale di differenza l'uso non autorizzato di sistemi ICT e alla pari gli attacchi ai sistemi terziarizzati e in cloud. Scendono a scalare i timori per gli altri tipi di attacco, ma sempre con piccole differenze percentuali.
La fig. 5-2, con risposte multiple, mostra le tecniche di attacco più temute nel prossimo futuro dai rispondenti: tutti hanno selezionato malware e script, considerando probabilmente anche la sempre crescente diffusione di malware e ransomware in Italia. Seguono a scalare tutte le altre tecniche considerate, con differenze percentuali dell'ordine di 10-20 punti.

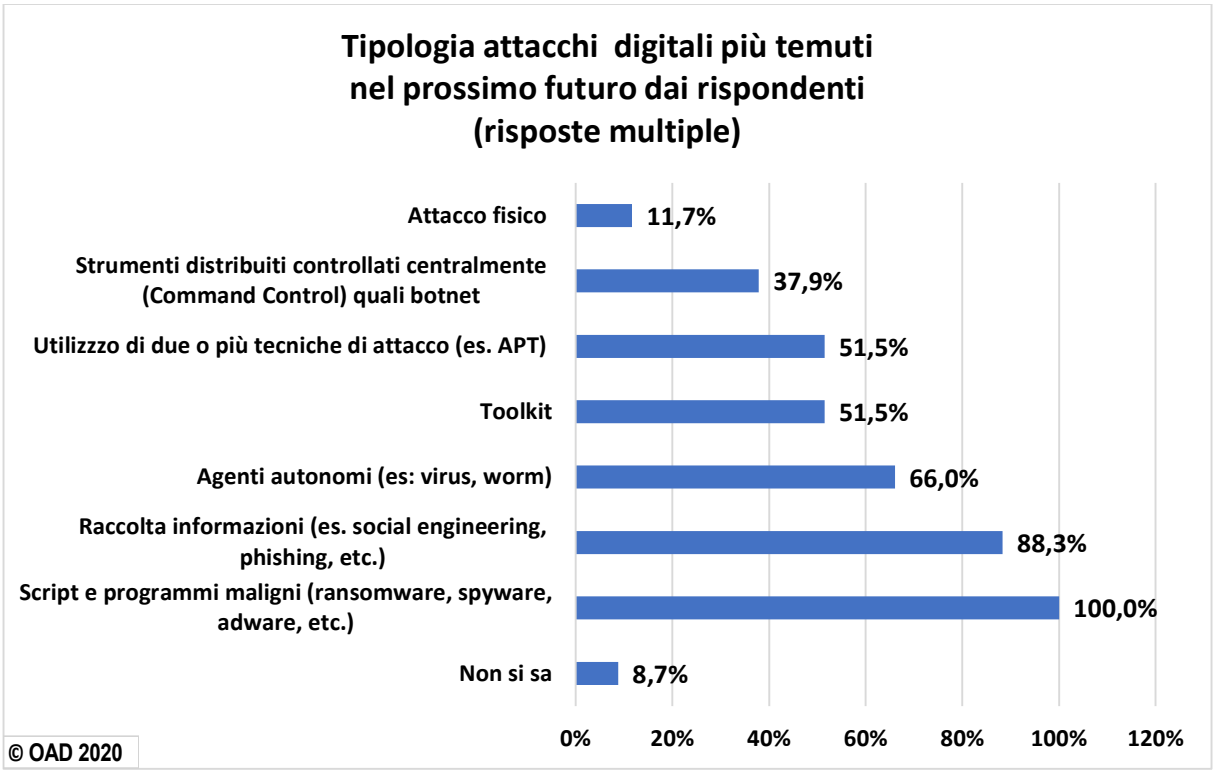

Fig. 5-2

6. Misure e strumenti di sicurezza digitale adottate nelle Aziende/Enti dei rispondenti dell'indagine 2020

Circa la metà del Questionario OAD è orientato a rilevare e a commentare le misure e gli strumenti di sicurezza in uso nei sistemi informatici delle Aziende/Enti dei rispondenti. Gli strumenti e le misure per la sicurezza digitale sono raggruppati in tre sezioni:

- misure organizzative, che includono:
  - Struttura organizzativa, ruoli, competenze, certificazioni
  - Policy e procedure organizzative

  - Contratti e clausole sicurezza digitale con le Terze Parti
  - Sensibilizzazione, consapevolezza (awareness), formazione e addestramento in ambito sicurezza digitale a tutti i livelli
  - Auditing ICT e della sua sicurezza
- misure tecniche, che includono:
  - Architettura complessiva delle misure di sicurezza digitale, integrata con l'intera architettura del sistema informatico
  - 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 per la gestione operativa ed il controllo della sicurezza digitale, che includono:
  - Sistemi di controllo, monitoraggio e gestione della sicurezza digitale
  - Piano di Disaster Recovery (DR)

Le misure di gestione sono un mix di misure organizzative e di strumenti tecnici: l'attribuzione din questa sezione è stata effettuata dall'autore nell'ottica di una maggior chiarezza concettuale e sulla base della sua diretta esperienza in merito.

Per i dettagli delle misure in essere da parte dei rispondenti si rimanda al Rapporto completo.
Nel seguente paragrafo si sintetizzano brevemente i risultati emersi da questa parte dell'indagine 2020 OAD.
Come già anticipato, nel complesso le misure in atto sono nettamente migliorate rispetto a quelle rilevate nelle precedenti indagini OAD, ma:

- Le **misure organizzative** devono essere potenziate soprattutto per le piccole strutture, tipicamente le PMI. Il regolamento europeo per la privacy, il GDPR, richiede l'attuazione di gran parte delle misure organizzative necessarie e l'obbligatorietà della conformità ad esso, in vigore dal 25/5/2018 per tutte le Aziende/Enti dell'Unione Europea, con significative pene pecuniarie in caso di inadempienza, dovrebbe favorire una maggior attenzione su questi aspetti: ma di fatto, soprattutto per le piccole e piccolissime organizzazioni, si è ancora assai lontani da quanto dovrebbe essere effettuato per ottemperare realmente alla normativa. E la crisi economica derivata dalla pandemia ha e sta ulteriormente ritardando l'adozione delle misure necessarie.
  - Il ruolo del responsabile della sicurezza digitale nella struttura organizzativa, il CISO, Chief Information Security Officer, è formalizzato[4] e attuato dal 44% delle organizzazioni dei rispondenti, soprattutto in quelle di grandi dimensioni
  - il CISO ed il suo personale possono operare nell'ambito dell'UOSI, Unità Organizzativa Sistemi Informatici, diretta dal CIO, Chief Information Officer, oppure in un'altra struttura organizzativa dell'Aziende/Ente, ma non nell'ambito UOSI. Da sempre il posizionamento del CISO in ambito UOSI, e quindi sotto il CIO, è considerato ledere il principio della separazione delle responsabilità (la ben nota "*separation of duties*" nella letteratura manageriale): infatti il controllato, ossia il CIO, controlla il controllore, ossia il CISO.
  - Per la maggior parte dei rispondenti è già attuato, o in corso di definizione e realizzazione, **l'ERT, Emergency Response Team**, per poter fronteggiare seri problemi o disastri ed attuare, quando necessario, il Disaster Recovery In questo ambito le procedure organizzative di particolare importanza sono quelle per la **gestione degli incidenti** e la **gestione delle emergenze**, Come evidenziato nel §7

[4] Per formalizzazione di un ruolo all'interno di una struttura organizzativa si intende la pubblicazione della lettera di incarico/ordine di servizio, che definisca attività e responsabilità del ruolo e sua posizione nell'organigramma della struttura

delle conclusioni, la tendenza in atto, soprattutto per le organizzazioni più piccole dimensioni, è di terziarizzare queste importanti gestioni a società specializzate.

- Le **misure tecniche** sono migliorate, rispetto alle indagini degli anni precedenti, anche grazie alla crescente adozione di soluzioni in cloud, ma per le piccolissime strutture sono da potenziare e rendere sistematiche soprattutto **le misure di base**, dal controllo degli accessi, IAA, degli utenti ai backup e agli aggiornamenti del software;
    - Basilari, anche per l'ampia diffusione degli attacchi all'identità digitale, come evidenziato nella fig. 4.2-1. Le tecniche di IAA includono il consueto "account", costituito dalla coppia identificatore utente e password, l'autenticazione forte a due o più fattori, ad esempio con token e con controlli via cellulare e con i certificati (in Italia forte la spinta di SPID[5], obbligatorio per le pubbliche amministrazioni), l'identificazione biometrica e la grafometria, gli strumenti di gestione e controllo degli accessi quali i diffusi Active Directory e l'LDAP, l'uso delle ACL, Access Control List, per la verifica dei privilegi degli utenti abilitati all'accesso alle applicazioni. Numerose le innovazioni tecnologiche che si stanno diffondendo per migliorare la sicurezza dell'IAA, che rappresenta un'area fondamentale per la sicurezza complessiva dell'intero Sistema Informatico e per rendere queste misure più semplici per l'utente finale e più facilmente gestibili per gli operatori. Tra le principali innovazioni che iniziano ad essere usate o che già hanno acquisto interessanti quote di mercato le autenticazioni "*passwordless*" basate su riconoscimento biometrico (si veda ad esempio il Progetto FIDO2), ed i sistemi SASE, Secure Access Service Edge, orientati al cloud che combinano prestazioni e sicurezza tra rete e controllo/gestione degli accessi.
- **Le misure di gestione e di controllo**: sono tendenzialmente migliorate ma ancora embrionali e soventi carenti, soprattutto nelle piccole realtà. Il mercato offre soluzioni sofisticate e avanzate, sempre più basate su logiche di intelligenza artificiale e di "machine learning", ma a parte grandi realtà che già le hanno o le stanno adottando, una loro effettiva adozione è ancora agli inizi, data anche la loro complessità ed in taluni casi i costi di adozione. Le misure e gli strumenti che sono stati fatti rientrare nell'ambito del controllo e della gestione della sicurezza digitale, e che sono di norma un di cui della più generale gestione dell'intero sistema informatico, includono i sistemi di directory di tutte le risorse digitali e delle loro configurazioni e licenze (ICT Asset Management), i sistemi di monitoraggio e controllo delle funzionalità e delle prestazioni dei sistemi ICT, i sistemi di raccolta, correlazione e gestione di tutti gli eventi (SIEM) rilevati dai sistemi ICT, i sistemi SOAR (Security Orchestration, Automation and Response), che consentono di automatizzare e di velocizzare la gestione della sicurezza digitale, i sistemi SASE (SASE, Secure Access Service Edge), i sistemi di analisi comportamentali di utenti e risorse ICT, i sistemi di individuazione e prevenzione di attacchi e data breach. Tra gli strumenti che ormai sono basilari per una efficace ed efficiente gestione della sicurezza digitale, e più in generale dell'intero Sistema Informatico, l'Intelligenza Artificiale, i sistemi esperti e le machine learning. Lo strumento basilare per poter gestire la sicurezza è avere, aggiornato, l'inventario di tutte le risorse hardware, software e terziarizzate.
    - Il **piano di Disaster Recovery**, DR, è fondamentale, indipendentemente dalle dimensioni e dalle attività dell'azienda/ente, per poter effettivamente garantire la sua business continuity. Ma quanto emerge dall'indagine 2020 OAD è che il DR è più formale che sostanziale: viene specificato il piano, ma non sono attuate le risorse informatiche alternative per attuarlo, ad esempio in cloud, e raramente vengono fatti esercizi di prova e di test per la sua attuazione. Il DR rimane quindi più un documento "burocratico" e formale che un sostanziale piano di intervento fattibile ed attuabile in caso di disastro.

[5] SPID, Sistema Pubblico di Identità Digitale, è erogato da diversi fornitori qualificati da AgID, e fornisce tre livelli di sicurezza: il livello 1, basato sul semplice uso di un identificativo d'utente e di una password; il livello 2 che aggiunge al livello 1 una OTP, One Time Password; il livello 3 che fornisce una autenticazione forte utilizzando certificati digitali con token quali smartcard

7. Per concludere

L'indagine 2020 OAD fotografa una situazione di attacchi digitali di vario tipo ma tutti tecnicamente di crescente complessità e sofisticazione, con una diffusione leggermente crescente rispetto al trend emerso nei dodici anni di indagini, ma inferiore rispetto al picco del 2018. Nonostante il proliferare di attacchi digitali in varia misura relativi alla pandemia Covid-19, nel primo quadrimestre 2020 la diffusione generale di attacchi si attesta su valori simili a quelli del 2019: da verificare con il prossimo OAD 2021 se, nel resto dell'anno, si avranno modifiche a questa tendenza.
L'elevato numero di attacchi rilevati nel 2018, e gli obblighi in termini di protezione dei dati personali imposti dal GDPR hanno sicuramente contribuito a rafforzare le misure di sicurezza digitale, ed un ulteriore miglioramento deriva dal crescente uso di servizi in cloud, dove le misure di sicurezza sono normalmente di alto livello e allo stato dell'arte.
Le misure organizzative per la sicurezza digitale, storicamente carenti e trascurate, sono migliorate soprattutto nella definizione dei ruoli e nella separazione delle responsabilità, nelle policy e nelle procedure organizzative, nella gestione degli incidenti: risultano comunque carenti per le piccole organizzazioni, mancando ancora, in generale, una effettiva consapevolezza e la cultura della sicurezza digitale, nella fattispecie ai vertici delle organizzazioni

Vi è ancora molta strada da fare in termini di formazione e di sensibilizzazione continua. Risulta poi ancora prevalente l'approccio formale e burocratico delle procedure organizzative, che una volta definite non trovano concreta applicazione, periodiche verifiche e test operativi: emblematico esempio è costituito dai piani di Disaster Recovery per i quali, sovente, non solo predefinite e allocate le risorse ICT alternative, e tanto meno le periodiche simulazioni a tavolino di un possibile disastro.
Gli strumenti di gestione della sicurezza digitale hanno ancora una diffusione limitata tra i rispondenti, in particolare quelle che utilizzano tecniche di intelligenza artificiale.
L'uso di IoT, di sistemi di automazione industriale e di robotica, e di sistemi basati su tecniche di blockchain trovano un numero basso di rispondenti coinvolti. Questo è causato anche dal numero relativamente esiguo di rispondenti appartenenti ai settori merceologici che sono più direttamente interessati a questi sistemi: dal manifatturiero, alla logistica, ai centri di ricerca e sviluppo, alle Pubbliche Amministrazioni Locali per il controllo del territorio, etc. I dati emersi dall'indagine su queste tematiche sono considerati, e da considerarsi, solo come specifici casi che contribuiscono ai valori generali sugli attacchi.

La realtà italiana, costituita da un grandissimo numero di piccole e piccolissime organizzazioni, 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 sicurezza digitale di base.

OAD 2020 rileva un netto miglioramento e rafforzamento delle misure di sicurezza digitali, sia tecniche che organizzative, anche se i più moderni sistemi di prevenzione, protezione e gestione che utilizzano tecniche di intelligenza artificiale sono ancora embrionali come uso nel bacino dei rispondenti.
Le misure e le tecniche di difesa prevalentemente in uso rincorrono l'evoluzione, sempre più sofisticata e smart, degli attacchi, ma quasi sempre in ritardo. L'attuale alta concentrazione di vulnerabilità richiede approcci diversi e nuove logiche, con l'obiettivo di rendere intrinsecamente sicuri, by default e by design, tutti i sistemi ICT interconnettibili ad Internet. Ma si è ancora lontani da tale obiettivo, e per migliorare decisamente il concreto contrasto ai continui attacchi e al cybercrime occorre al momento 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.

OAD
Osservatorio
Attacchi Digitali
in Italia

I Patrocinatori di OAD 2020