OAD
Osservatorio
Attacchi Digitali
in Italia

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

Dedica
Il presente Rapporto 2020 OAD è dedicato alla memoria del dott. Giuseppe Saccardi, Presidente e Co-Fondatore di Reportec Srl, venuto a mancare nel corso della sua pubblicazione.

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

OAD
Osservatorio
Attacchi Digitali
in Italia

Sommario

1. Sintesi direzionale

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 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, considerando anche piccole e piccolissime organizzazioni che normalmente le altre indagini nazionali ed internazionali non considerano.
L'indagine OAD 2020 si è svolta nel corso della pandemia Covid-19, che ha reso ancor più difficile degli anni precedenti motivare i potenziali rispondenti al questionario online: nonostante che il questionario prevedesse un alleggerimento delle domande più tecniche per la fotografia di massima, e sempre anonima, dei Sistemi Informatici, oltre ad una macro-valutazione qualitativa del loro livello di sicurezza digitale in funzione delle risposte fornite. Si è comunque riusciti a raggiungere un numero sufficiente di risposte, superando anche il numero di quelle avute negli anni precedenti.
Il bacino di rispondenti emerso 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.

L'indagine OAD 2020 fa 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 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.
Per il 2019 gli 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%**.
Il tipo di attacco, ossia che cosa si attacca, più diffuso in entrambi i periodi considerati è stato quello indirizzato 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. 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.
Come tecniche di attacco, ossia come si attacca, tutte le sette famiglie considerate nel questionario sono state 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, 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.

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.

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, ed i dati emersi evidenziano un netto miglioramento sia delle misure tecniche sia di quelle organizzative.
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.
L'elevato numero di attacchi rilevati nel 2018, e gli obblighi in termini di protezione dei dati personali del GDPR per la privacy 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 dai relativamente pochi rispondenti dei settori merceologici che sono i più diretti interessati a questi sistemi: dal manifatturiero, alla logistica, ai centri di ricerca e sviluppo, alle Pubbliche Amministrazioni Locali per il controllo del territorio, e così via. I dati emersi dall'indagine su queste tematiche sono considerati, e da considerarsi, solo come specifici casi che contribuiscono ai valori generali sugli attacchi.

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

- nell'ambito della protezione delle Infrastrutture Critiche, nel 2019, i 1.181 attacchi rilevati sono più che raddoppiati rispetto a quelli dell'anno precedente, così come le 155 indagini avviate, e le persone arrestate sono state 3; nel 1° quadrimestre 2020 sono stati rilevati 282 attacchi, sono state avviate 34 indagini, e non ci sono stati arresti;
- 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 al più diffuso uso di questi servizi online a causa dei blocchi dovuti alla pandemia Covid-19;
- 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.

Per concludere, l'indagine OAD 2020 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.
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' alta densità 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.

2. Executive Summary

The Digital Attacks Observatory in Italy, OAD, with this 2020 edition reaches the twelfth year of consecutive surveys on cyberattacks in Italy, and, as in the previous years, with the precious collaboration of the Italian Postal and Telecommunications Police.
OAD is the only independent online survey in Italy on intentional digital attacks on IT systems of companies and public bodies operating in Italy. The OAD survey does not provide for a predefined set of respondents, but allows potential interested parties full and free access to the online questionnaire, in a totally anonymous manner. Thanks to the number of responses collected and their balanced distribution between companies and public bodies of various sizes and belonging to various product sectors, the OAD survey provides an accurate picture of the cyberattacks in Italy.
The OAD 2020 survey took place during the Covid-19 pandemic, which made it even more difficult than in previous years to reach the respondents' minimum number necessary to obtain a consistent and credible survey. In order to better motivate the potential respondents, the 2020 questionnaire provided a reduction of the more technical questions, and a qualitative macro evaluation of the level of the cybersecurity of each Informatics System object of the answers provided. By means of these innovations and of the large promotion for the questionnaire compilation, it was possible to reach a sufficient number of answers, even exceeding the number of those received in the previous OAD editions.
The emerged respondents' pool covers all the product sectors, including Public Administrations, even if the majority of the respondents' companies belong to the ICT sector (30.8%). The 2020 pool is well balanced for the size of the organizations, in terms of number of employees, between those below 250 and the largest ones. It must be taken into account that in Italy 99.91% of enterprises are SMEs, Small Medium Enterprises, under 250 employees, and of these 95% are under ten employees. The OAD 2020 survey is therefore able to investigate on small and very small organizations, which are not normally considered in other cybersecurity surveys: 57.5% of respondents belong to structures with less than 250 employees, and of these 22.1 % under 10.

The OAD 2020 survey refers to **the entire year 2019** and to **the 1st quarter of 2020**, when the Covid-19 pandemic exploded. This pandemic has been the trigger for a wide range of cyberattacks, mainly caused by the sudden - and in part unprepared - passage of many to agile working from home and to a strong use of every type of IT service on Internet, mainly derived by the mobility lockdowns imposed by the Italian Authorities.

For 2019, cyberattacks on Informatics Systems of the respondents' basin amounted to **46.6%** of the total, and for the first quarter of 2020 to **44.8%**.
The type of attack (what is attacked) most widespread in both the considered periods is the one aimed at **access control systems** (IAA, Identification Authentication Authorization), **with 34%** in 2019 and **28.2%** in the 1st quarter of 2020. As diffusion among the respondents, the other 14 types of attacks follow, decreasing by a few percentage points among them, whose characteristics and impacts are detailed in the related paragraphs of the OAD 2020 report. Referring to the attack techniques (how to attack), all the seven attacks families considered in the 2020 questionnaire are widely used in the various types of attacks, even simultaneously.
The most widespread one, as an average on the various attacks detected by the respondents' pool, is the **use of toolkits** (rootkits, meta-exploits, etc.) for the identification and exploitation of vulnerabilities on the target system of the attack, with a **38.8 %**, followed by the well-known malicious and unauthorized **collection of information** (social engineering, phishing, etc.) with **34.6%** and the use of **malicious code** and scripts with **34.3%**. The other considered techniques decrease with a few percentage points of difference between them.
The impacts of the most critical attacks are analyzed for each attack type, as well as their possible motivations and the recovery times required by the most critical ones.

In the 2020 OAD survey, all these attacks' characteristics vary for each type of attack, and the emerged results are described in the specific paragraphs dedicated to each attack type. At overall it emerges that:

- the impacts declared by the respondents are balanced between those irrelevant and / or easily resolvable with recovery in short time and at limited costs, and those very critical, which require expensive and long recovery actions, and that, in some cases, can cause business and customer loses; these two very different impact cases depend mainly on the security measures in place;
- the motivations of the cyber-attacks are mainly of an economic nature, therefore done for fraud and blackmail: the widespread diffusion of ransomware in Italy is a clear confirmation of these motivations.

The Informatics Systems considered in the 2020 survey and their cybersecurity are in the medium-high range and the emerged information show a relevant improvement in both technical and organizational measures, in comparison to the previous surveys. Few of the considered Italian Informatics Systems are based on Data Centers in Italy, most of the respondents' companies have medium-small Informatic Systems partly on premise and partly outsourced, with an increasing use of cloud services.
The high number of attacks detected in 2018, and the privacy obligations (GDPR) have certainly contributed to strengthening cyber security measures, and a further improvement comes from the growing use of cloud services, where usually there are high standard security measures.
Organizational measures for cybersecurity, historically lacking and neglected in Italy, have improved in terms of defining roles and separation of duties, of organizational policies and procedures, and of incidents management. These measures often are lacking in small organizations, and in general the cybersecurity awareness and competence are low, and mainly at the top level of the public and private organizations
In Italy, there is still a long way to go in terms of cybersecurity continual training and awareness. A formal and bureaucratic approach for the organizational procedures is still prevalent, which once defined, often do not find a possible concrete applicability, periodic updates and operational tests: an emblematic example is represented by the Disaster Recovery plans for which, several times, the required alternative ICT resources to be used are not forecasted and allocated and there also not provided periodic exercises and simulations of the possible disasters.
Cybersecurity management tools still have limited diffusion among the 2020 OAD respondents, in particular the most advanced ones based on artificial intelligence techniques.
The use of IoT, of industrial automation and of robotics systems, and also of systems based on blockchain techniques find a low number of respondents involved, which also derives from the limited percentage of their product sectors that should be the more interested in these systems: the manufacturing sectors, the logistics, the research and development centers and labs, the Local Public Administrations for territorial control, and so on. For these topics, the data that emerged from the survey are considered only as specific cases that contribute to the general values on the cyberattacks, but which cannot be still considered of reference at the Italian level.

The data provided by the Postal and Communications Police confirm the growing criticality of the cyberattacks and, above all, the difficulties in combating and suppressing cybercrime:

- in the protection of Critical Infrastructures, in 2019, the 1181 attacks detected more than doubled compared to those of the previous year, as well as the 155 investigations launched, and the only 3 people arrested; in the first quarter of 2020, 282 attacks were detected, 34 investigations were launched, but there were no arrests;
- in the fight against "financial cybercrime", fraudulent transactions in 2019 were blocked for a total value of € 21.3 million and € 18 million were recovered; in the 1st quarter of 2020 fraudulent transactions for a good € 20.2 million were blocked, practically reaching in 4 months what was blocked in the 12 months of the previous year, and € 8 million recovered; an indicator of the growth in attacks on financial transactions and services due to the very

large use of these online services caused by the mobility blocks imposed by the Covid-19 pandemic;

- in the fight against cyber terrorism in 2019, 36,000 websites were checked and 250 contents deleted; in the 1st quarter of 2020, 11,962 websites were checked.

To conclude, the OAD 2020 survey highlights a situation of cyberattacks of various types but all technically of ian high complexity and sophistication, with a slightly increasing spread in Italy compared to the trend that emerged in the twelve years of OAD surveys, but lower than the peak of 2018. Despite the proliferation of cyberattacks to varying degrees related to the Covid-19 pandemic, in the first four months of 2020 the general spread of attacks is at similar values to those of 2019: to be verified with the next OAD 2021 if there will be changes to this trend.

The Italian reality, made up of a very large number of small and very small organizations, does not make our country one of the most attractive for cybercriminals, but cyber warfare and massive attacks represent a growing and serious risk, as has already happened in part with the widespread of ransomware on computer systems whit a lack of or with low cybersecurity basic measures.
OAD 2020 notes a clear improvement and strengthening of digital security measures, both technical and organizational, even if the most modern prevention, protection and management systems that use artificial intelligence techniques are still embryonic in the respondents' basin.

The defense measures and techniques in use chase the increasingly sophisticated and smart evolution of attacks, but almost always late. The high density of vulnerabilities requires different approaches and new logics, with the aim of making all ICT systems interconnectable to the Internet intrinsically safe, by default and by design. But we are still a long way from this goal, and in order to decisively improve the concrete fight against continuous attacks and cybercrime, it is currently necessary to increase cybersecurity' awareness and skills at all levels, an effective collaboration between the police at world level, and primarily a real and large usage of the professional ethics both of those involved (supply side) and both of those who decide (demand side) on cybersecurity.

3. Introduzione al Rapporto 2020 OAD

OAD, Osservatorio Attacchi Digitali in Italia, costituisce l'unica indagine indipendente on line via web in Italia sugli **attacchi digitali intenzionali** ai sistemi informatici di aziende ed enti operanti in Italia, incluse le Pubbliche Amministrazioni Centrali e Locali.
Obiettivo primario di OAD è analizzare il fenomeno degli attacchi digitali intenzionali nella realtà italiana, e poter così essere un riferimento, autorevole e indipendente, per l'analisi e la gestione dei rischi informatici. Ulteriore e non meno importante obiettivo è quello di contribuire alla corretta conoscenza della sicurezza digitale e dei suoi impatti e conseguenze, in particolare verso i decisori "non tecnici", tipicamente figure di vertice dell'organizzazione, che decidono e stabiliscono i budget ed i progetti per la sicurezza digitale.

Il presente Rapporto 2020 fa riferimento agli attacchi digitali intenzionali rilevati nel corso dell'intero 2019 ed al 1° quadrimestre 2020**,** congiungendosi ai precedenti Rapporti che coprono un arco temporale di tredici anni consecutivi, dal 2007 al 2020 (per il 1° quadrimestre). Fino al 2015 l'indagine era chiamata OAI, Osservatorio Attacchi Informatici in Italia, dal 2016 è stata chiamata OAD per evidenziare l'integrazione tra informatica e telecomunicazioni - reti (come anche indicato dall'acronimo ICT[1] usato in Europa) e gli attacchi che possono colpire sia la parte di rete sia la parte informatica o entrambe.
Tutti rapporti annuali pubblicati sono scaricabili gratuitamente, insieme alla documentazione prodotta e/o raccolta di articoli e presentazioni ad essi correlati, dallo specifico sito web www.oadweb.it, che costituisce l'archivio documentale completo di tutte le iniziative negli anni sull'Osservatorio.
Il Rapporto 2020 OAD è realizzato dall'autore Marco R. A. Bozzetti con la sua società Malabo Srl, sotto l'egida di e in collaborazione con l'associazione AIPSI, Capitolo italiano di ISSA, con l'editore Reportec Srl e con la Polizia Postale e delle Telecomunicazioni, che ha fornito i dati trattati nel Capitolo 11.
Per coprire almeno una parte dei costi, OAD 2020 è stata sponsorizzata dalle aziende dell'offerta ICT Cloudflare, Sophos, Qintesi, Darktrace e Technology Estate, le cui schede di presentazione, con l'approfondimento delle loro attività, sono in ordine alfabetico nell'Allegato C.
Come per le edizioni precedenti OAD 2020 annovera il patrocinio di numerose associazioni, il cui elenco, con una breve descrizione delle loro attività, è nell'Allegato D. Per OAD il ruolo attivo dei Patrocinatori è significativo per poter allargare e stimolare il bacino dei compilatori del questionario via web, tipicamente tramite i loro soci e simpatizzanti, oltre che per far conoscere e divulgare il rapporto annuale, contribuendo in tal modo anche alla diffusione della cultura sulla sicurezza ICT.

Il Rapporto OAD 2020 si basa sull'elaborazione e l'analisi delle risposte avute dal questionario online reso liberamente disponibile su Internet da maggio a novembre 2020. Essendo libero l'accesso al questionario in Internet, il campione emerso non ha stretta valenza statistica ma, dato il numero di risposte e la buona distribuzione per dimensioni e per settore merceologico delle aziende/enti dei rispondenti, esso fornisce precise e contestuali indicazioni sul fenomeno degli attacchi digitali in Italia. L'indagine rileva anche quali sono gli strumenti di prevenzione, protezione e ripristino in uso nei sistemi informatici dei rispondenti per contrastare e limitare tali attacchi, e come le Aziende/Enti reagiscono in caso di attacco.
Dalle elaborazioni ed analisi delle 310 risposte al questionario OAD 2020, costituito da 117 domande con risposte predefinite tra le quali scegliere, è stato prodotto il presente rapporto finale, costituito da186 pagine A4 e da148 figure tra grafici e tabelle.

1 ICT, Information and Communication Technology.

Per la comprensione del presente rapporto si richiede una conoscenza di base di informatica e di sicurezza digitale, dato l'uso di termini tecnici. Per facilitarne la lettura, è disponibile nell'Allegato B un glossario degli acronimi e dei termini tecnici specialistici usati.

3.1 Le motivazioni dell'Osservatorio sugli Attacchi Digitali in Italia

Le tecnologie informatiche e di comunicazione, indicate nel seguito come "digitali" o con l'acronimo ICT, sono sempre più diffuse e pervasive in ogni attività lavorativa. I sistemi ICT sono divenuti il nucleo fondamentale e insostituibile per il supporto e l'automazione dei processi e il trattamento delle informazioni delle organizzazioni: il loro non funzionamento porta, nella maggior parte dei casi, al blocco o al cattivo funzionamento dell'attività e/o del processo supportato. Gli attacchi ai sistemi informatici minano la continuità operativa e debbono essere il più possibile prevenuti e contrastati con idonee misure di sicurezza, sia tecniche sia organizzative, misure che debbono, o dovrebbero, essere valutate, progettate e implementate a seguito di sistematiche analisi dei rischi. In tale ottica diviene fondamentale poter disporre di informazioni sugli attacchi che più sovente affliggono i sistemi informativi italiani, aggiornate e contestualizzate alla realtà nazionale.
Numerosi sono gli studi e i rapporti a livello internazionale, condotti da Enti specializzati, quali ad esempio il First (Forum for Incident Response and Security Team) o quelli provenienti dai principali Fornitori di sicurezza informatica a livello mondiale, ma difficilmente essi forniscono dati specifici e di dettaglio sulla realtà italiana, e soprattutto quelli riguardanti le piccole e le piccolissime strutture organizzative, che costituiscono la stragrande maggioranza delle imprese e degli enti pubblici italiani.

La disponibilità di dati nazionali sugli attacchi rilevati e sulla tipologia e sull'ampiezza del fenomeno è fondamentale per:

- comprendere il fenomeno degli attacchi e del crimine informatico in Italia;
- effettuare concrete analisi dei rischi e attivare le idonee misure di prevenzione, protezione e ripristino;
- "sensibilizzare" sul tema della sicurezza informatica tutti i livelli del personale, dai decisori di vertice agli utenti finali.

Di qui la decisione di realizzare sotto l'egida di e in collaborazione con AIPSI un osservatorio nazionale annuale, le cui caratteristiche metodologiche sono riportate nell'Allegato A, riprendendo anche l'esperienza passata avuta dall'autore nella creazione e realizzazione dell'iniziativa OCI, Osservatorio Criminalità Informatica, in ambito FTI-Sicurforum[2], nel periodo 1997- 2004. L'approccio è simile: la raccolta dei dati avviene elaborando le risposte via web dei vari rispondenti, il rapporto è elaborato in maniera omogenea dall'autore, in collaborazione con alcune persone di AIPSI, Malabo, Reportec ed utilizzando anche i dati forniti dalla Polizia Postale e delle Telecomunicazioni, si veda Cap. 11.

[2] L'associazione FTI, Forum delle Tecnologie dell'Informazione non esiste più. Per i Rapporti OCI del 1997, 2000 e 2004, pubblicati da Franco Angeli, si veda https://www.francoangeli.it/ricerca/Ricerca_Collana.aspx?CollanaID=571

4. Il quadro generale degli attacchi digitali intenzionali e delle contromisure

Gli attacchi digitali sono un fenomeno, a livello mondiale, 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[3] 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.

La fig. 4-1 dal Global Risk Report[4] del World Economic Forum, WEF, del 2020 evidenzia come i rischi digitali siano ai primi posti tra i rischi "globali" a livello mondiale.
La fig. 4-2, dallo stesso rapporto WEF, mostra le correlazioni tra i vari rischi considerati, e mostra come i rischi digitali (cyber risk nella figura) siano correlati, oltre che con gli altri rischi "tecnologici", anche con numerosi altri "grandi rischi", dai crolli finanziari a quelli delle grandi infrastrutture, dalla disoccupazione alla instabilità sociale, dalle bolle speculative al fallimento della governabilità globale e agli attacchi terroristici.

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 §5.

[3] https://www.hermeneut.eu/
[4] http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

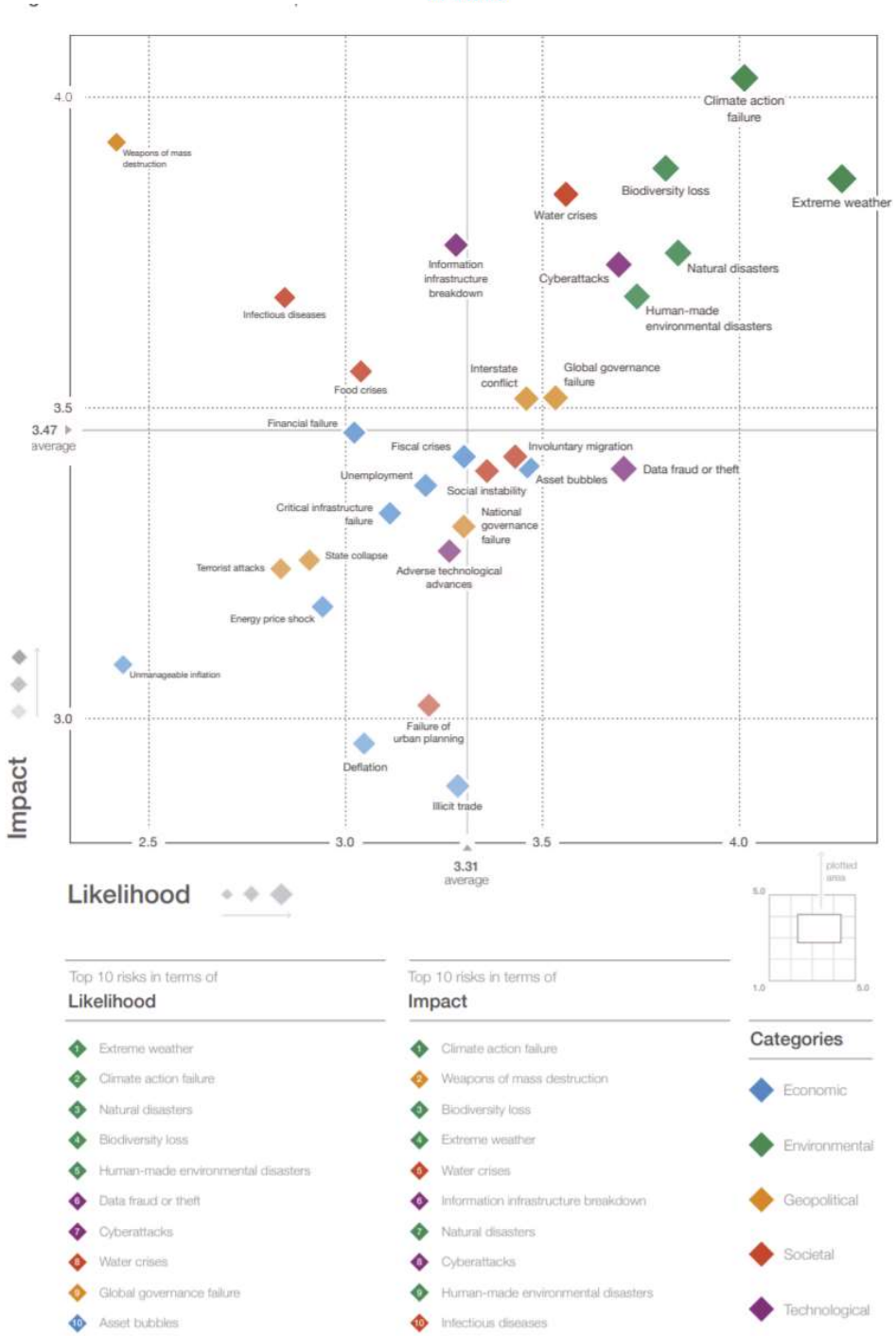


Fig. 4-1 (Fonte World Economic Forum)

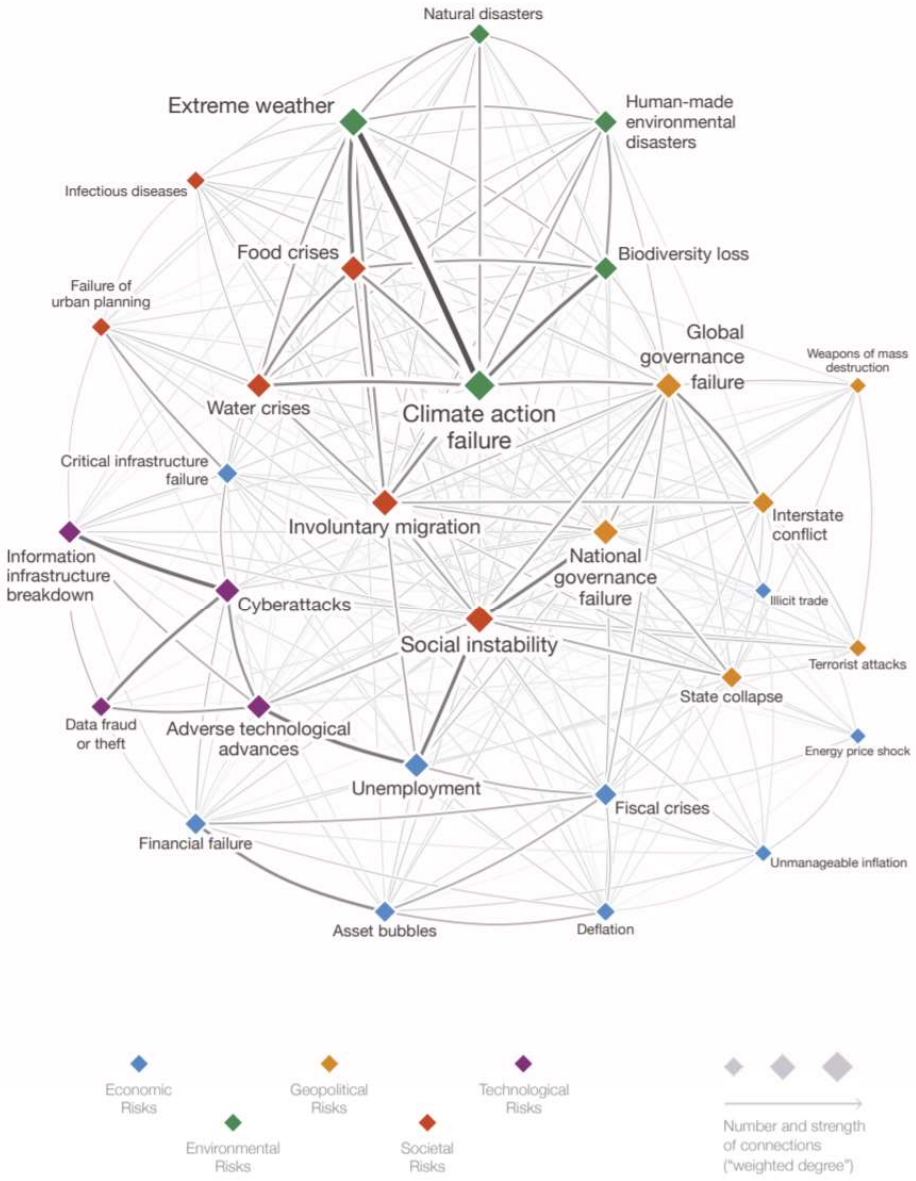


Fig. 4-2 (Fonte World Economic Forum)

4.1 La pandemia Covid-19

A livello mondiale il 2020 sarà ricordato per l'esplosione a livello mondiale della pandemia del Covid-19, esplosa 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: agile o smart working che ha enormemente ampliato l'area di vulnerabilità:

- 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

Non solo i governi e le pubbliche amministrazioni, ma anche gran parte delle aziende si sono fatte trovare dal Covid-19 impreparate a gestire una pandemia: questo a livello mondiale, ma in Italia la percentuale è stata maggiore, causa anche del gran numero di piccole organizzazioni.

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 worker. 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.

Un esempio significativo di un attacco digitale associato ad una truffa nel nome del Covid-19 è iniziata negli US a partire dal 15/7/2020 hackerando Twitter. Una serie di profili Twitter di società operanti con le cripto valute, tra le quali Huobi, Kucoin, Kraken, Gemini, Binance, Coinbase & Trezor, informavano della loro decisone di erogare 5.000,00 $ US di aiuti per la pandemia, con riferimento a CryptoforHealth ed invitavano ad effettuare donazioni per questa iniziativa su uno specifico conto Bitcoin indicato nel sito, dal quale avrebbero ricevuto il doppio di quanto versavano sui loro conti in cripto valuta. Il tutto ovviamente falso, e Twitter Inch bloccò il sito malevolo. Gli attaccanti a questo punto hanno preso il controllo dei profili Twitter di personalità famose, quali ad esempio Elon Musk, Jeff Bezos, Bill Gates, Warren Buffett, e di grandi aziende, da Uber ad Apple, ed hanno twittato da questi profili reali che avrebbero versato il doppio, in bitcoin, di quanto elargito dal donatore, sempre nell'ottica di aiuti alla pandemia. Ovviamente frodi di questo tipo non hanno molto senso e, nonostante i milioni di persone che seguono questi profili, sono state rilevate poche donazioni, attorno a 400. La gravità di questo attacco massivo (si veda §4.2) è data dal fatto che gli attaccanti hanno preso il controllo di questi famosi profili pur avendo questi ultimi autenticazioni forti a due fattori. L'aspetto positivo è che solo pochissimi creduloni, nella massa, hanno abboccato alla truffa, razionalmente senza senso: ma qualcuno che ci casca si trova sempre. Twitter Inch ha poi dichiarato che, in seguito alle indagini effettuate, i profili famosi coinvolti erano circa 130 e che gli attaccanti, probabilmente con tecniche di social engineering, hanno coinvolto utenti privilegiati interni.

In questi ultimi mesi si sono diffusi seri allarmi e si sono verificati i primi attacchi con il furto di informazioni sui vaccini (facilmente prevedibili, visti gli enormi valori economici in gioco), e per la supply chain della loro distribuzione, in particolare per la catena del freddo. Attacchi sofisticati, nella maggior parte basati su un entry point con spear phishing, che probabilmente sconfinano in guerre informatiche tra stati (cyber warfare).

A livello mondiale, ed in parte anche in Italia, i settori più colpiti da attacchi in qualche modo correlati alla pandemia sono quelli finanziari, della sanità e della pubblica amministrazione.

4.2 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 d 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[5] 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. Tali attacchi in taluni casi, 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, ad esempio, 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, i primi tipi sono dei 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, quali ad esempio il Power Shell ed i suoi script nel mondo Windows, dopo aver acquisito, tipicamente da remoto, i diritti di accesso di utente privilegiato, ad esempio sfruttando 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 alla 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

[5] 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.

esempio è dato da attacchi di tipo *crowdturfing*[6]*, 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, ed il più colpito in Europa.
Crescente sovrapposizione e difficoltà a distinguere tra attacchi digitali e *cyber warfare*, vere e proprie guerre informatiche.

4.3 Le contromisure in atto e la loro evoluzione

Così come si sono e si stando evolvendo le tecniche di attacco digitali, allo stesso modo si stanno evolvendo le tecniche per la difesa dei sistemi digitali.
Le logiche evolutive e le tecniche usate si basano principalmente su:

- Il passaggio dalla tradizionale logica "statica" di misure e strumenti di difesa in funzione delle vulnerabilità e rischi individuati, ad una logica "dinamica", indipendente dai rischi ipotizzati, e basata sull'analisi comportamentale effettuata tramite sistemi di machine learning;
- Adozione di logiche, approcci ed architetture "Zero Trust";
- Crescente utilizzo di tecniche di AI e di machine learning in tutte le soluzioni di sicurezza digitale, in particolare nella correlazione dei log e delle segnalazioni di sistema e nella threat intelligence;
- Crescente integrazione, interoperabilità ed automazione dei diversi strumenti di sicurezza digitale: si veda il fiorire di soluzioni e piattaforme quali SIEM, SOAR, SESA, etc.;
- Adozione di tecniche di autenticazione "forte" degli utenti "passwordless";
- Realizzazione e crescente adozione di misure di sicurezza digitale "as a service";
- Crescente terziarizzazione della sicurezza digitale, in particolare a livello della gestione operativa;
- Tendenza alla realizzazione di soluzioni di sicurezza digitale intrinseche (embedded) nei vari sistemi digitali, in modo che tale sicurezza sia di default ed impostata fin dal progetto del sistema stesso (by design). Con l'attuale alta densità di vulnerabilità tecniche, in molti casi si fa ricadere la responsabilità dell'occorrenza di un attacco all'incapacità e agli errori dell'utente. Questa tendenza è un obiettivo a lungo termine, che dovrebbe portare alla realizzazione di sistemi ICT intrinsecamente sicuri, indipendentemente dal buono o cattivo uso da parte dell'utente: sistemi senza vulnerabilità tecniche intrinseche e così facili da usare da ridurre, se non eliminare, le possibili vulnerabilità personali ed organizzative.

La sicurezza digitale assoluta non esiste, ma nel mondo ormai dominato dall'ICT in Internet, la sicurezza digitale è e deve essere un obbligo delle Aziende/Enti, non solo di quelle più "critiche. In attesa dei sistemi ICT intrinsecamente sicuri di cui all'ultimo punto dell'elenco precedente, ora occorre:

- attivare e gestire al meglio tutte le attuali misure;
- far crescere la consapevolezza e le competenze a tutti i livelli sulla sicurezza digitale, sia lato domanda che offerta di sistemi ICT;
- bloccare e reprimere l'hackeraggio/cybercrime, riducendo gli alti guadagni illegali con pochissimi rischi (si veda §11);
- una maggiore collaborazione internazionale per la repressione del crimine informatico, sia a livello legislativo sia a livello forze di Polizia;
- far crescere l'etica professionale di chi si occupa di sicurezza digitale sia lato domanda che lato offerta. Lato domanda non si dovrebbe scendere sotto certi valori come pagamento giornaliero di riferimento, anche in caso di gare, e lato offerta non si dovrebbero vendere

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

soluzioni e sistemi ICT obsoleti o non utili al cliente, approfittando della sua non competenza in merito.

Facendo riferimento all'indagine 2020 OAD, i paragrafi del successivo capitolo 9 forniscono una fotografia delle misure in essere, tecniche ed organizzative, dei Sistemi Informatici delle Aziende/Enti di chi ha liberamente e anonimamente scelto di rispondere al questionario OAD.
Come negli anni precedenti, anche nell'edizione 2020 il bacino emerso di aziende/enti rispondenti si colloca in una fascia medio-alta per il livello complessivo di sicurezza digitale: il solo fatto che le aziende/enti rispondenti abbiano compilato un questionario online, che richiedeva 30-40 minuti per compilarlo, è un chiaro indicatore del loro interesse al tema sicurezza digitale, e della conseguente attenzione nell'adozione di opportune misure tecniche ed organizzative.

In generale, e verrà volutamente ripetuto in varie parti di questo rapporto, le misure di sicurezza adottate nella maggior parte dei casi si basano su approcci tradizionali ormai datati, e che non sono più in grado di reggere le nuove frontiere degli attacchi a sistemi informatici a loro volta più complessi, sofisticati, eterogenei, con loro parti in cloud, sempre esposti su Internet, e con enormi quantità di dati trattati (big data): quindi sempre più difficili da gestire.
Per quanto indicato all'inizio di questo capitolo 4, tutto (o quasi tutto) è digitale e in tempo reale: ed il tempo, oltre alla massa di software interoperante e di dati, richiede automazione.

4.3.1 La terziarizzazione della sicurezza digitale

Nella maggior parte dei casi, in particolare per le piccole e medie organizzazioni, non si può disporre al proprio interno di qualificate ed aggiornate competenze sulla sicurezza digitale: occorre terziarizzarla, dal progetto alla gestione operativa: ma questo non significa rinunciare alle competenze in merito, occorre sempre controllare ciò che la terza parte fa e come, altrimenti si diverrà preda e si sarà in balia dei fornitori.
Moderne piattaforme e soluzioni quali SIEM, SOAR, SESA, o le stesse tecniche di blockchain, costituiscono sistemi molto complessi e già difficili da gestire per grandi organizzazioni con elevate competenze al proprio interno, figuriamoci per le piccole e piccolissime così diffuse in Italia!.
Ma vulnerabilità e rischi digitali esistono, e della stessa complessità e sofisticazione, sia per grandi che per piccole organizzazioni. Ne consegue la necessità, per la maggior parte delle aziende/enti italiani, di terziarizzare la sicurezza digitale: fenomeno che sta crescendo anche in Italia, così come stanno emergendo società specializzate nella fornitura di servizi di sicurezza gestiti, indicate come MSSP, Managed Security Service Provider, o incominciano ad essere utilizzati i servizi di grandi player. Il loro principale strumento è il SOC, Security Operation Center, il sistema di controllo delle attività di un sistemo informatico, reti incluse, focalizzato sul monitoraggio di eventi legati alla sicurezza e che integra vari strumenti e misure di sicurezza, quali le moderne soluzioni di cui sopra. Grandi strutture hanno e gestiscono un SOC al loro interno, o in soluzioni ibride con uno o più MSSP.

5. 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 e così via.

5.1 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.
La fig. 5.1-1 riporta da CVE/MITRE il grafico di confronto del numero di vulnerabilità tecniche individuate per i 50 prodotti ICT commerciali più diffusi secondo i principali fornitori ICT.

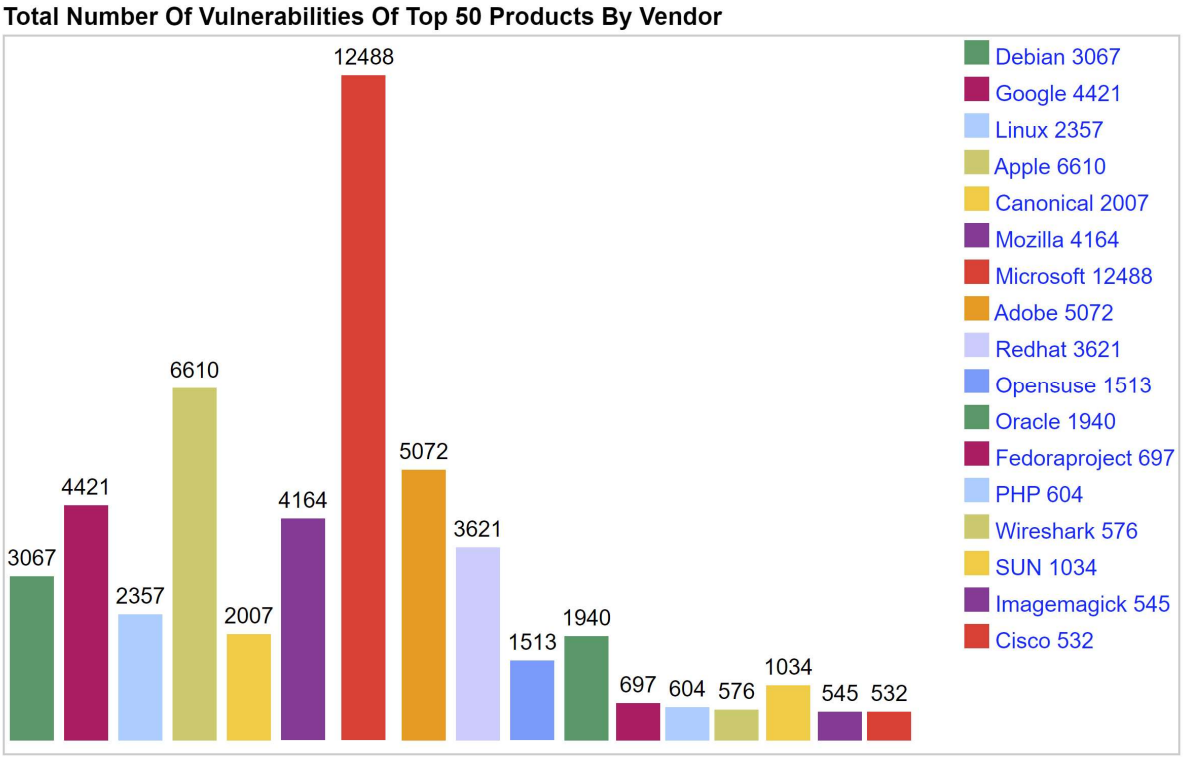


Fig. 5.1-1 (Fonte: CVE-MITRE)

Al primo posto tra le aziende fornitrici si posiziona Microsoft, con 12448 vulnerabilità distinte, date dalla somma di quelle tra i primi 50 suoi numerosi prodotti e relative versioni. Con la stessa logica seguono in questa classifica Apple, Adobe e gli altri fornitori
La fig. 5.1-2 mostra l'elenco dei primi 15 singoli prodotti con più vulnerabilità distinte individuate, sempre da CTE/MITRE. Al primo posto il sistema operativo Debian Linux, cui seguono Android di Google, Linux Kernel, Mac OS X di Apple.

Top 50 Products By Total Number Of "Distinct" Vulnerabilities

Go to year: 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 All Time Leaders

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Debian Linux	Debian	OS	3067
2	Android	Google	OS	2563
3	Linux Kernel	Linux	OS	2357
4	Mac Os X	Apple	OS	2212
5	Ubuntu Linux	Canonical	OS	2007
6	Firefox	Mozilla	Application	1873
7	Chrome	Google	Application	1858
8	Iphone Os	Apple	OS	1655
9	Windows Server 2008	Microsoft	OS	1421
10	Windows 7	Microsoft	OS	1283
11	Acrobat Reader Dc	Adobe	Application	1182
12	Acrobat Dc	Adobe	Application	1182
13	Windows 10	Microsoft	OS	1111
14	Flash Player	Adobe	Application	1078
15	Windows Server 2012	Microsoft	OS	1050

Fig. 5.1-2 (Fonte CVE-MITRE)

L'Allegato E.2 fornisce un elenco, non esaustivo, delle principali fonti internazionali con aggiornati elenchi delle vulnerabilità tecniche ICT.
L'argomento delle vulnerabilità è molto ampio, a livello tecnico estremamente dettagliato, e si rimanda per ulteriori approfondimenti alle fonti citate.
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.

5.2 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.

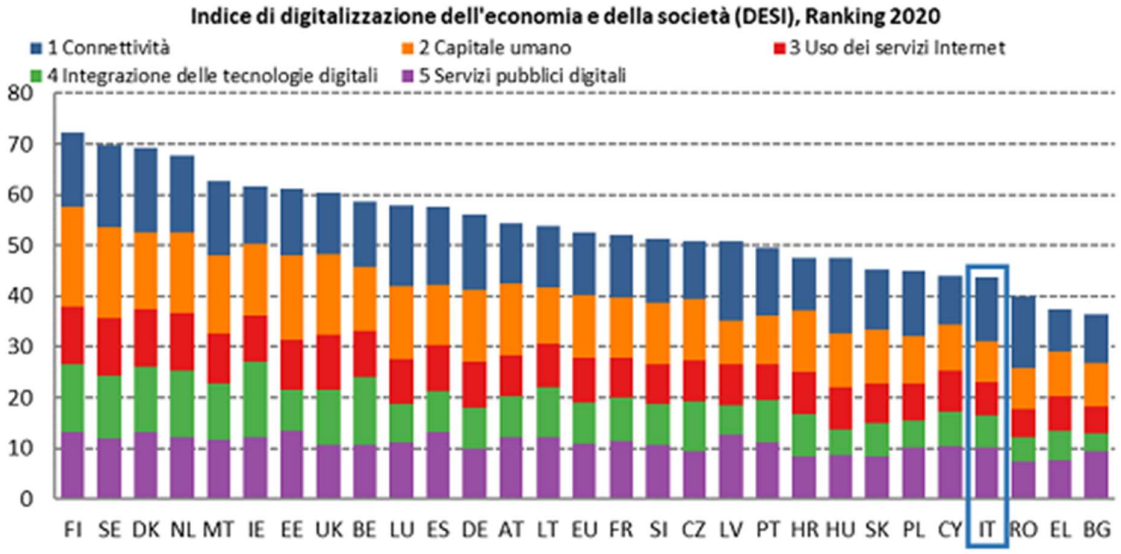


Fig. 5.2-1 (Fonte: DESI)

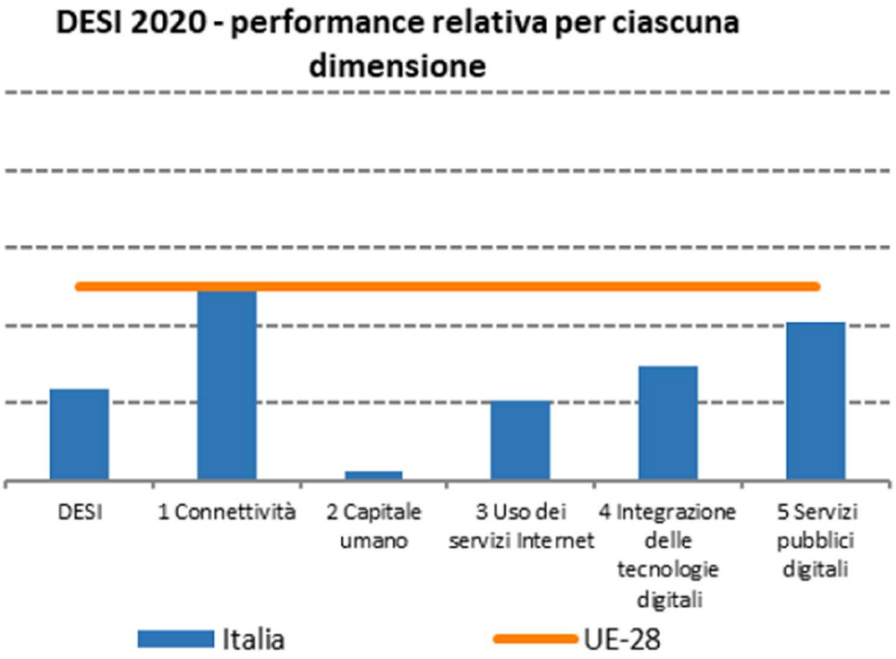


Fig. 5.2-2 (Fonte: DESI)

5.3 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.

6. Gli attacchi digitali rilevati nell'indagine OAD 2020

Nel presente capitolo, ogni tipologia di attacco viene esaminata sulla base delle risposte ricevute da chi ha rilevato, nell'intero arco del 2019 e/o nel primo quadrimestre 2020, la specifica tipologia d'attacco, e che riguardano:

- il numero di attacchi di quel tipo nel 2019, se sopra o sotto la soglia di 10 attacchi rilevati nell'anno; la soglia di 10 per anno è un numero derivato dall'esperienza pluriennale dell'autore;
- le tecniche di attacco (come) che si ritiene siano state usate per portare quel tipo di attacchi, considerando in particolare gli attacchi più gravi per l'Azienda/Ente del rispondente;
- i principali impatti subiti dall'attacco più grave rilevato;
- le possibili motivazioni dell'attacco più grave rilevato;
- il tempo massimo richiesto per il ripristino ex ante nel caso del più grave attacco di quel tipo subito nell'anno 2019 e nel 1° quadrimestre 2020.

La fig. 6-1 mostra, percentualmente, il numero di attacchi rilevati dai rispondenti nel 2019 e nel 1° quadrimestre 2020: essa evidenzia come gli attacchi rilevati complessivamente nel 2019, per un totale di 46,6%, siano diminuiti rispetto al 55,7% del 2018, che ha costituito il picco massimo percentuale tra tutte le indagini OAD dal 2008 e che comportò, per la prima volta, la percentuale di attacchi rilevati maggiore di quelli non rilevati. Come evidenziato nel confronto anno per anno degli attacchi rilevati dai rispondenti evidenziato in fig. 6-3, è tipica l'oscillazione tra un aumento di attacchi in un anno, cui segue tendenzialmente una diminuzione nell'anno successivo, causata ragionevolmente dall'avere rinforzato le misure di sicurezza digitali. Nel 1° quadrimestre 2020, che corrisponde in Italia all'inizio della pandemia Covid-19 e degli attacchi digitali ad essa correlati, come discusso in §4.1, il 44,8% è un valore abbastanza alto, e probabilmente incrementerà ulteriormente considerando l'intero 2020. Si rimanda alla prossima indagine OAD 2021 la verifica di questa possibile tendenza, o se la percentuale per l'intero anno rimarrà attorno ai valori del 1° quadrimestre, dato che l'attenzione sulla sicurezza digitale è aumentata grazie alla diffusione del lavoro agile, con il conseguente rafforzamento delle misure di sicurezza.

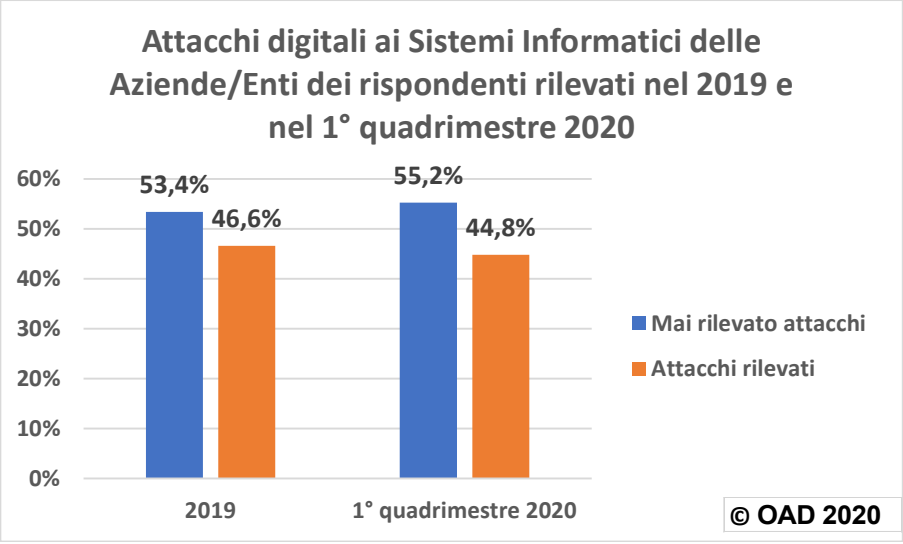


Fig. 6-1

La fig. 6-2 dettaglia la frequenza e la ricorrenza degli attacchi nei periodi considerati, distinguendo tra poche o molte centinaia in un anno. In tale conteggio, come specificato nel questionario, non è considerato il generico spamming, che in taluni periodi può creare centinaia o più messaggi in un solo giorno, mentre viene considerato il phishing. Come si ripete ormai, e ragionevolmente, in ogni indagine OAD, gli attacchi non frequenti sono quelli maggiormente diffusi, e percentualmente risultano tre volte quelli frequenti in entrambi i periodi considerati.

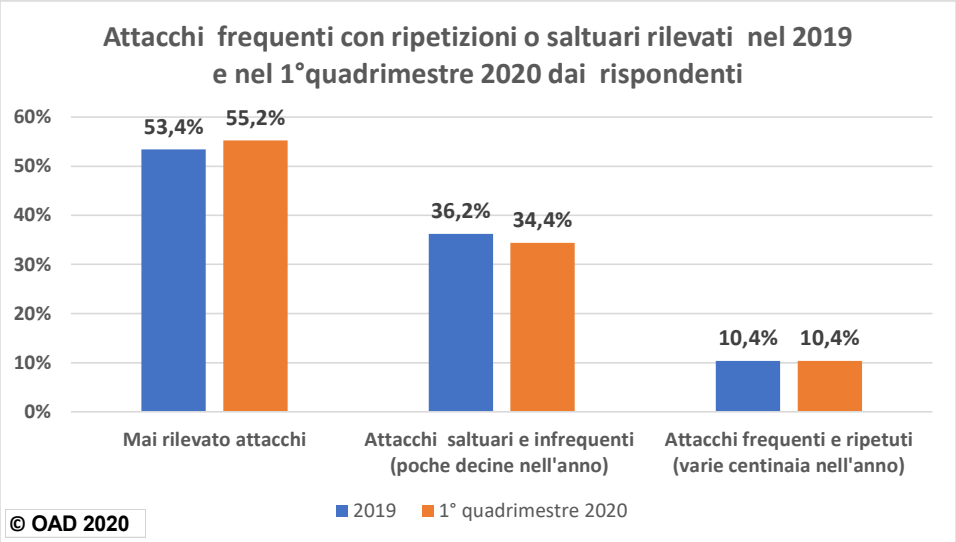


Fig. 6-2

La fig. 6-3 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 mix 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 avuto un sali-scendi 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, e per più di 10 punti, la percentuale di quelli non occorsi/rilevati. Nel 2019 il trend di crescita dei precedenti tre anni si arresta, con una diminuzione al 46,6% e nel 1° quadrimestre 2020 sembra stabilizzarsi: ma come andrà per l'intero 2020? Crescerà rispetto al 2019 con l'inizio di un'altra onda? 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 vedere con la prossima indagine OAD del 2021.
L'onda altalenante 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.

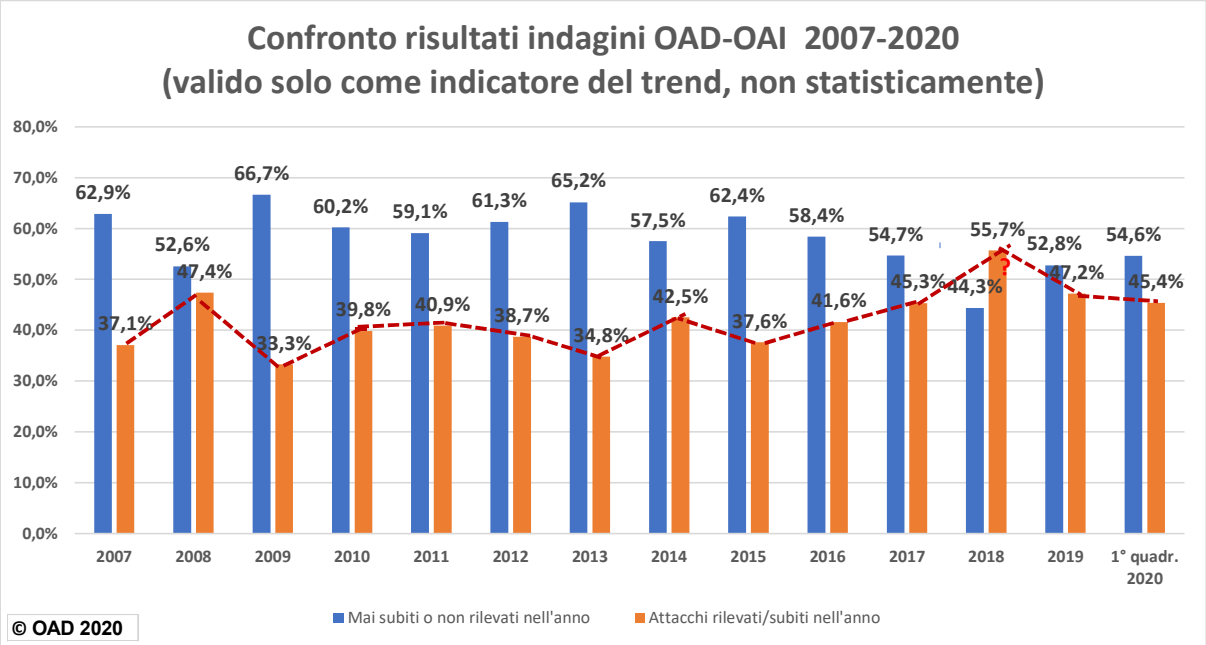


Fig. 6-3

Pur con le varie oscillazioni, il 40% di attacchi rilevati è un valore di trend ed un riferimento stabile negli anni in Italia. Secondo alcuni esperti di indagini di mercato e di sicurezza digitale, questo valore è considerato troppo basso, e viene rimarcato che probabilmente molti attacchi non sono stati rilevati dai rispondenti. Questo è sicuramente possibile, a livello mondiale si stima addirittura che 2/3 degli attacchi lanciati non siano rilevati, anche se vanno a buon fine. Ma a tal proposito l'autore ritiene che il 40% sia ancora una corretta e ragionevole valutazione per la situazione italiana, dato che:

- 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;
- per le Pubbliche Amministrazioni (PA) italiane si calcolano circa 55000 enti, di cui solo poche centinaia hanno grandi dimensioni, come dipendenti; anche per le PA, con una grande prevalenza di piccole strutture, valgono pertanto le stesse considerazioni espresse al punto precedente;
- se l'Azienda/Ente non ha rilevato l'attacco portato, significa che il danno subito non era rilevante, a parte l'eventuale furto di informazioni.

È pertanto evidente che 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 o terroristici (per l'analisi delle possibili motivazioni si rimanda ai successivi paragrafi sulle singole tipologie di attacco, da §6.1 a §6.15).
Questo è confermato analizzando le fig. 6-4 e 6-5 che mostrano la distribuzione percentuale degli attacchi subiti o non nel 2019 e nel 1° quadrimestre 2020 per dimensione delle aziende/enti dei rispondenti[7]. 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

[7] Per le caratteristiche "macro" delle aziende/enti dei rispondenti e dei loro sistemi informatici si veda §10.

saltuari attacchi o al rilevamento di frequenti e ripetuti attacchi.

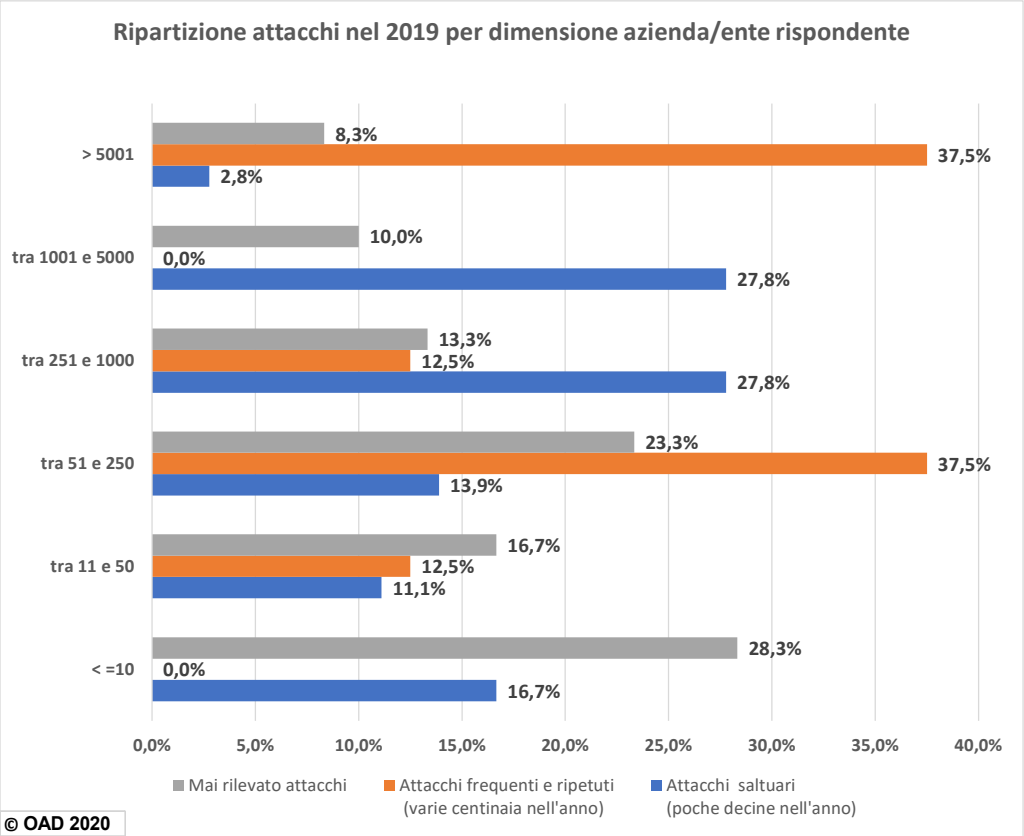


Fig. 6-4

Le strutture con più di 5001 dipendenti, e quelle tra i 51 e 250, sono quelle che percentualmente hanno subito più attacchi, soprattutto quelli più frequenti ed anche ripetuti, sia nel 2019 che nel 2020. Per il 2020 a queste si aggiungono le strutture piccolissime, con <10 dipendenti.
Un'ulteriore conferma viene dalla fig. 6-6 che mostra la ripartizione degli attacchi per il fatturato dell'azienda o per il giro economico per la PA secondo l'ultimo bilancio disponibile (fig. 6-5). La maggior parte degli attacchi rilevati è per le organizzazioni con fatturati /bilanci (per le PA) con più di 5.000,00 €, quindi di organizzazioni "ricche" e potenzialmente appetibili per cyber criminali, e prevalentemente di grandi dimensioni.

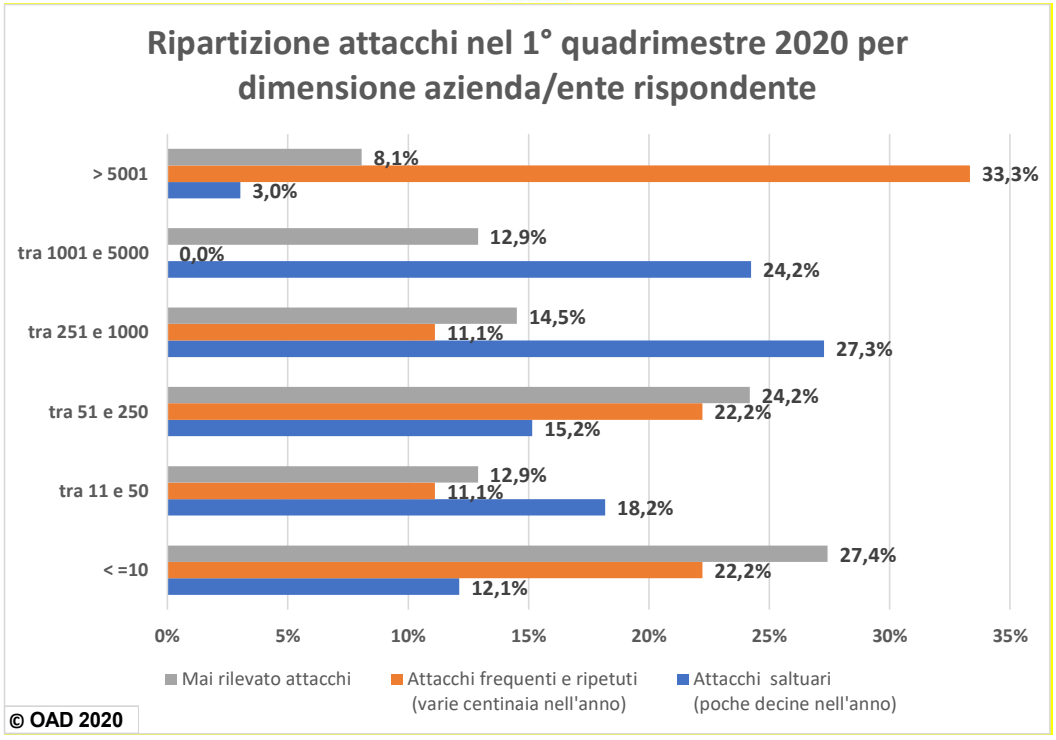

Ripartizione attacchi nel 1° quadrimestre 2020 per dimensione azienda/ente rispondente
> 5001
8,1%
33,3%
3,0%
tra 1001 e 5000
12,9%
0,0%
24,2%
tra 251 e 1000
14,5%
11,1%
27,3%
tra 51 e 250
24,2%
22,2%
15,2%
tra 11 e 50
12,9%
11,1%
18,2%
< =10
27,4%
22,2%
12,1%
0%
5%
10%
15%
20%
25%
30%
35%
Mai rilevato attacchi
Attacchi frequenti e ripetuti (varie centinaia nell'anno)
Attacchi saltuari (poche decine nell'anno)
© OAD 2020

Fig. 6-5

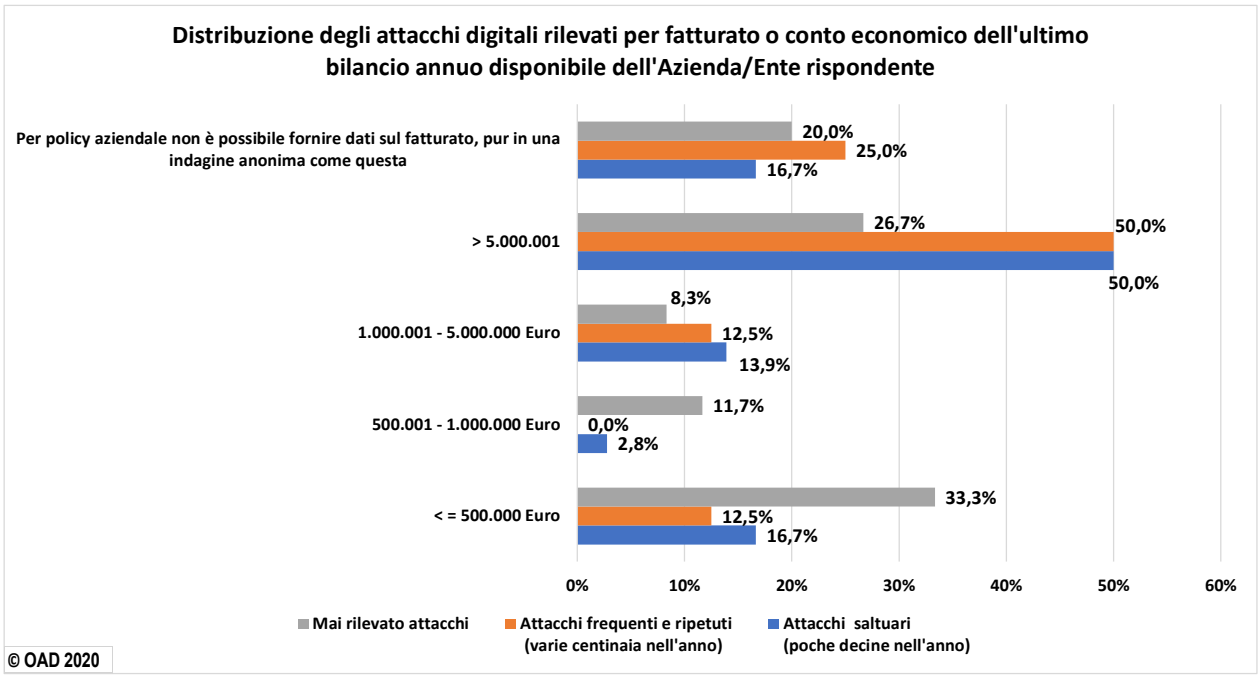

Distribuzione degli attacchi digitali rilevati per fatturato o conto economico dell'ultimo bilancio annuo disponibile dell'Azienda/Ente rispondente
Per policy aziendale non è possibile fornire dati sul fatturato, pur in una indagine anonima come questa
20,0%
25,0%
16,7%
> 5.000.001
26,7%
50,0%
50,0%
1.000.001 - 5.000.000 Euro
8,3%
12,5%
13,9%
500.001 - 1.000.000 Euro
11,7%
0,0%
2,8%
< = 500.000 Euro
33,3%
12,5%
16,7%
0%
10%
20%
30%
40%
50%
60%
Mai rilevato attacchi
Attacchi frequenti e ripetuti (varie centinaia nell'anno)
Attacchi saltuari (poche decine nell'anno)
© OAD 2020

Fig. 6-6

La fig. 6-7 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, in base alle risposte previste nel questionario 2020 OAD ed illustrate nell'Allegato A di questo rapporto, cui si rimanda per gli approfondimenti metodologici. I dettagli forniti dai rispondenti per ogni tipologia di attacco sono descritti e commentati negli specifici paragrafi da §6.1 a §6.15 del presente rapporto.
Si deve inoltre considerare che le tipologie di attacco a sistemi in Cloud, a sistemi IoT, a sistemi di automazione industriale/robotica e a sistemi con tecniche di blockchain, riguardano solo alcuni Sistemi Informatici dei rispondenti, dato che tutte le altre Aziende/Enti non li utilizzano o non sono necessari per le loro attività.
L'ordinamento dall'alto in basso delle tipologie di attacco più diffuse in percentuale rilevate dai rispondenti nella fig. 6-7 fa riferimento, con la barra blu, al 2019. La barra arancione associata fa riferimento a 1° quadrimestre 2020.
Le percentuali indicate nella figura per ogni tipologia d'attacco, e poi commentate negli specifici paragrafi da §6.1 a §6.15, sono calcolate rispetto al totale dei rispondenti al questionario
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.

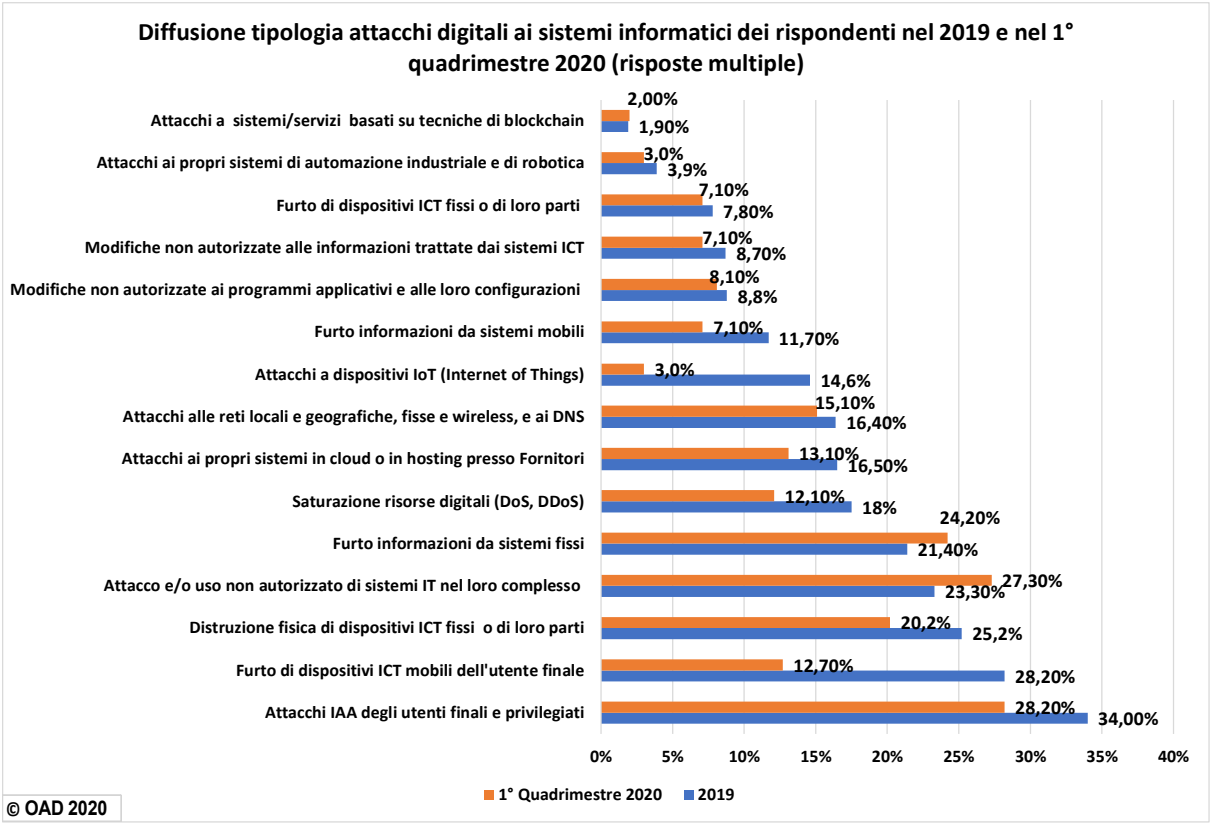


Fig. 6-7

Al secondo posto di questa classifica di diffusione delle tipologie di attacco si posiziona nel 2019 il furto di dispositivi mobili, mentre nel 1° quadrimestre 2020 l'attacco o uso non autorizzato ad un intero sistema ICT, che era al secondo posto anche nel 2018 e che per il 2019 si posiziona al quarto posto.
Il furto di dispositivi mobili è un attacco da tempo diffuso e in certi anni posizionato in cima alle classifiche di OAD, alla luce della semplicità di attuazione, che non richiede competenze tecniche

sull'ICT ma solo destrezza e capacità di furto di un dispositivo. Il furto è dovuto al valore del dispositivo, in particolare per gli smartphone, ed il mercato dell'usato esistente.
Al terzo posto nel 2019 si posiziona la distruzione fisica di dispositivi ICT, tipicamente fissi, o di loro parti. Questo risultato dell'indagine lascia sorpresi, anche se in precedenti indagini OAD era emerso tra i più diffusi tra i sistemi informatici dei rispondenti. Probabilmente molti rispondenti hanno inteso, erroneamente, che questa voce includesse anche rotture non intenzionali di dispositivi hardware, e per questo motivo l'hanno selezionata. Nella prossima edizione del questionario dovrà essere meglio chiarito che questa voce fa riferimento solo a distruzioni fisiche intenzionali, e che come tali dovrebbero essere ben poco frequenti.
Al terzo posto nel 1° quadrimestre 2020 si posiziona il furto di informazioni da sistemi ICT fissi. La preminenza di questa tipologia deriva anche dal secondo posto, in questo periodo, degli accessi non autorizzati ad un sistema ICT. Basta una chiavetta USB, ora con capacità di terabyte, per sottrarre intere banche dati.
Tutte le altre tipologie di attacco decrescono percentualmente. È doveroso evidenziare come le percentuali rilevate da attacchi a sistemi di automazione industriale e a sistemi basate su blockchain sono irrisorie, in quanto sono pochissimi i rispondenti dotati di tali sistemi.
A parte l'elevato numero relativo alla distruzione fisica di dispositivi ICT, dovuto molto probabilmente ad una errata interpretazione della domanda del questionario, la diffusione delle altre tipologie di attacchi rilevate nell'indagine si allinea nella sostanza 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.
Correttezza ulteriormente confermata dall'analisi delle tecniche di attacco usate, o che il rispondente ritiene siano state usate, nel portare le varie tipologie di attacco considerate. Le tecniche di attacco sono raggruppate in sette categorie, illustrate in dettaglio nell'Allegato A.1.1, cui si rimanda per dettagli.
La fig. 6-8 sintetizza percentualmente la diffusione delle tecniche di attacco usate nelle diverse tipologie di attacco rilevati dai rispondenti: diffusione data dalla media dell'occorrenza di una data tecnica in tutte le tipologie di attacchi. Non si distingue tra occorrenza nel 2019 o nel 1° quadrimestre 2020, dato che volutamente la domanda nel questionario chiedeva di selezionare, anche in maniera multipla, le tecniche individuate o presunte negli attacchi più gravi riscontrati, indipendentemente dal periodo in cui sono occorsi.
Al primo posto l'uso di toolkit, nell'edizione scorsa al terzo posto, ed al secondo le varie tecniche di raccolta di informazioni, tipicamente il social engineering, nelle precedenti edizioni quasi sempre al primo posto, ed al terzo, a poca distanza percentuale dal secondo, l'uso di script e malware, nell'indagine del 2018 al secondo posto.
La diffusione dei toolkit è aiutata dai numerosi software gratuiti messi a disposizione su Internet, ed è un chiaro indicatore di come molti degli attacchi siano più sofisticati e partano da una attenta analisi delle vulnerabilità sui sistemi ICT target dell'attacco. La raccolta delle informazioni è la tecnica di base e nella maggior parte degli attacchi costituisce ancora il punto iniziale per attuarlo, il così detto "entry point", basato sulla vulnerabilità dell'essere umano involontariamente coinvolto. L'uso di codici maligni e di script, che includono anche i comandi diretti al sistema operativo e/o alle banche dati, sono un altro diffuso strumento per molti attacchi: ed i ransomware sono molto diffusi in Italia.

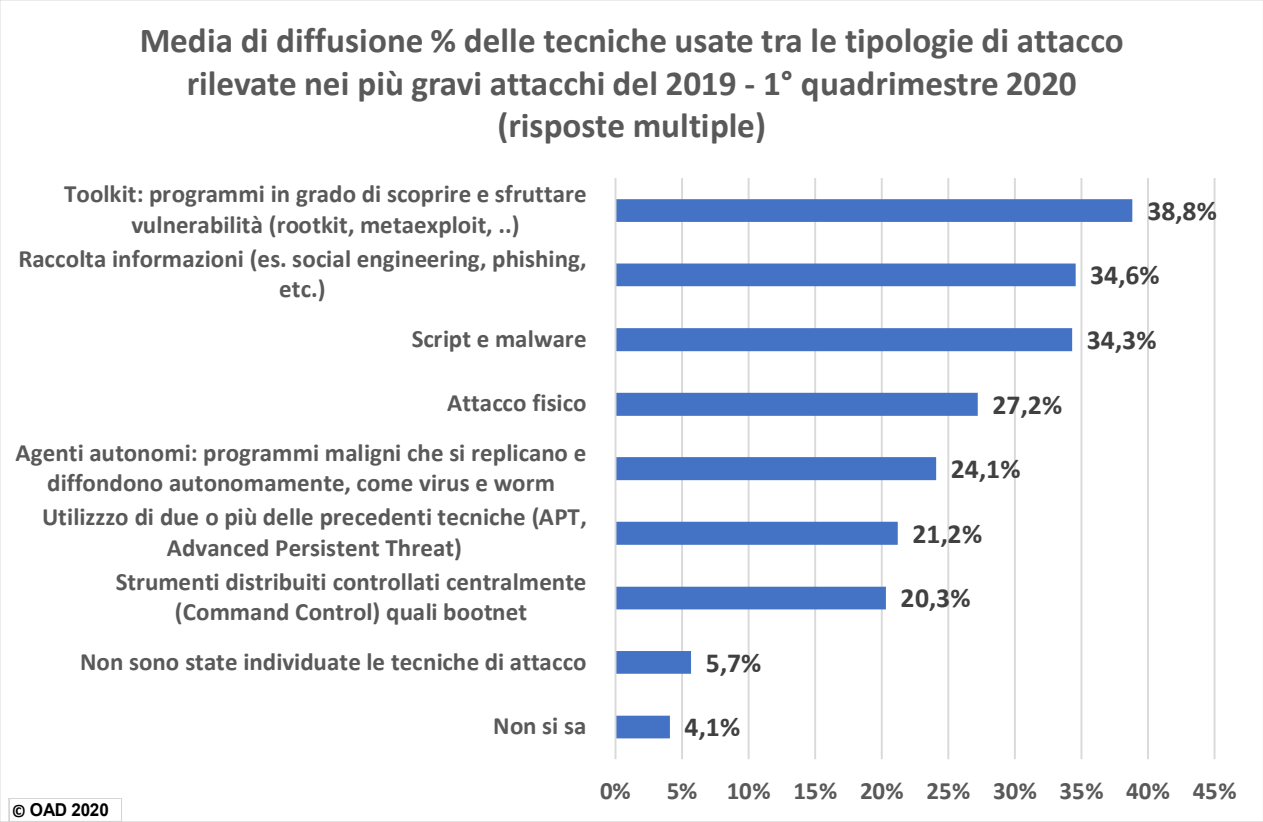


Fig. 6-8

La Tabella in fig. 6-9 dettaglia e mappa, per ciascuna delle tipologie di attacco rilevate dai rispondenti nel 2019 e nel 1° quadrimestre 2020, le tecniche di attacco usate. La tabella evidenzia, per ogni tipologia d'attacco, quali sono le tecniche di attacco che i rispondenti hanno rilevato o che ipotizzano siano state usate. Sia in fig. 6-8 che in fig. 6-9 è riportato che una piccola parte dei rispondenti ha specificato che non sono riusciti ad individuare le possibili tecniche, ed altri che non le conoscono.

Nella tabella di fig. 6-9, per ogni riga relativa ad una tipologia di attacco, è evidenziata in neretto la percentuale più alta tra le tecniche considerate nelle varie risposte date. Analizzando la tabella per colonna, si vede dal numero di valore in neretto, quanto quella tecnica sia diffusa ed utilizzata (almeno presumibilmente) per i diversi tipi di attacco.

Tecniche attacco/tassonomia per i più gravi attacchi digitali nel 2019 e nel 1° quadrimestre 2020 (risposte multiple)	Attacco fisico	Raccolta informazioni (es. social engineering, phishing, etc.)	Agenti autonomi: programmi maligni che si replicano e diffondono autonomamente, come virus e worm	Script e malware	Toolkit: programmi in grado di scoprire e sfruttare vulnerabilità (rootkit, metaexploit, ..)	Strumenti distribuiti controllati centralmente (Command Control) quali bootnet	Utilizzzo di due o più delle precedenti tecniche (APT, Advanced Persistent Threat)	Non sono state individuate le tecniche di attacco	Non si sa
Distruzione fisica di dispositivi ICT fissi o di loro parti	100,0%								
Furto di dispositivi ICT mobili	100,0%								
Furto di dispositivi ICT fissi o di loro parti	100,0%								
Furto informazioni da sistemi fissi (PC, server, storage system, etc.)	13,0%	n.c.	17,4%	**56,5%**	39,1%	17,4%	21,7%	4,3%	8,7%
Furto informazioni da sistemi mobili	20,0%	**90,0%**	n.c.	50,0%	30,0%	10,0%	30,0%	10,0%	0,0%
Attacchi all'identificazione, autenticazione e controllo accessi	0,0%	**81,3%**	31,3%	56,3%	53,1%	25,0%	21,9%	9,4%	9,4%
Attacchi alle reti locali e geografiche, fisse e wireless, e ai DNS	5,9%	64,7%	29,4%	**70,6%**	52,9%	35,3%	17,6%	5,9%	5,9%
Attacco e/o uso non autorizzato di sistemi ICT nel loro complesso	3,8%	65,4%	30,8%	**88,5%**	34,6%	23,1%	23,1%	7,7%	7,7%
Modifiche non autorizzate ai programmi applicativi e alle loro configurazioni	55,6%	11,1%	33,3%	11,1%	77,8%	33,3%	**77,8%**	11,1%	11,1%
Modifiche non autorizzate alle informazioni trattate dai sistemi ICT	0,0%	**75,0%**	50,0%	37,5%	62,5%	25,0%	37,5%	0,0%	0,0%
Saturazione sistemi e risorse ICT (DoS, DDoS)	10,0%	40,0%	10,0%	15,0%	35,0%	**65,0%**	5,0%	5,0%	5,0%
Attacchi ai propri sistemi ICT in cloud e/o in hosting (*)	0,0%	53,3%	46,7%	**66,7%**	60,0%	33,3%	33,3%	6,7%	13,3%
Attacchi a dispositivi IoT (Internet of Thinks) (*)	0,0%	12,5%	12,5%	12,5%	**37,5%**	12,5%	0,0%	0,0%	0,0%
Attacchi ai propri sistemi di automazione industriale (SCADA, DCS, PLC, ..) e di robotica (*)	0,0%	25,0%	**50,0%**	**50,0%**	**50,0%**	25,0%	0,0%	25,0%	0,0%
Attacchi a propri sistemi o a sistemi/servizi di terze parti basati su tecniche di blockchain (*)	0,0%	0,0%	50,0%	0,0%	**50,0%**	0,0%	**50,0%**	0,0%	0,0%
Indice diffusione tecnica di attacco per tutte le tipologie di attacco considerate	**27,2%**	**34,6%**	**24,1%**	**34,3%**	38,8%	**20,3%**	**21,2%**	**5,7%**	**4,1%**
© OAD 2020	n.c. = non considerata nel questionario								

Fig. 6-9

La fig. 6-10 mostra la diffusione percentuale degli attacchi rilevati dalle aziende/enti dei rispondenti nel 2019 ripartita per settore merceologico. La fig. 6-11 mostra l'analoga diffusione per settore merceologico nel 1° quadrimestre 2020. Le aziende dei rispondenti sono classificate da OAD su raggruppamenti basati secondo i codici ATECO[8], cui vengono aggiunte le Pubbliche Amministrazioni Centrali (PAC) e Locali (PAL). In §10.2 è dettagliata la tipologia e la numerosità dei rispondenti per settore merceologico.

I grafici in fig. 6-10 e 6-11 sono ordinati dal valore percentuale più alto e a decrescere per i settori dei rispondenti che non hanno rilevato attacchi nei due periodi considerati. Il settore dei Sevizi ICT è quello nettamente al primo posto in entrambi i periodi, ed è ragionevole, per non dire ovvio, date le specifiche competenze in sicurezza digitale. Ed è anche il primo sia per attacchi saltuari che frequenti nel 1° quadrimestre 2020, affiancato per questi ultimi dai settori PAC e Istruzione. Nel 2019 è il settore PAC dei rispondenti che ha rilevato più attacchi frequenti e ripetuti.

[8] https://www.istat.it/it/files/2011/03/metenorme09_40classificazione_attivita_economiche_2007.pdf

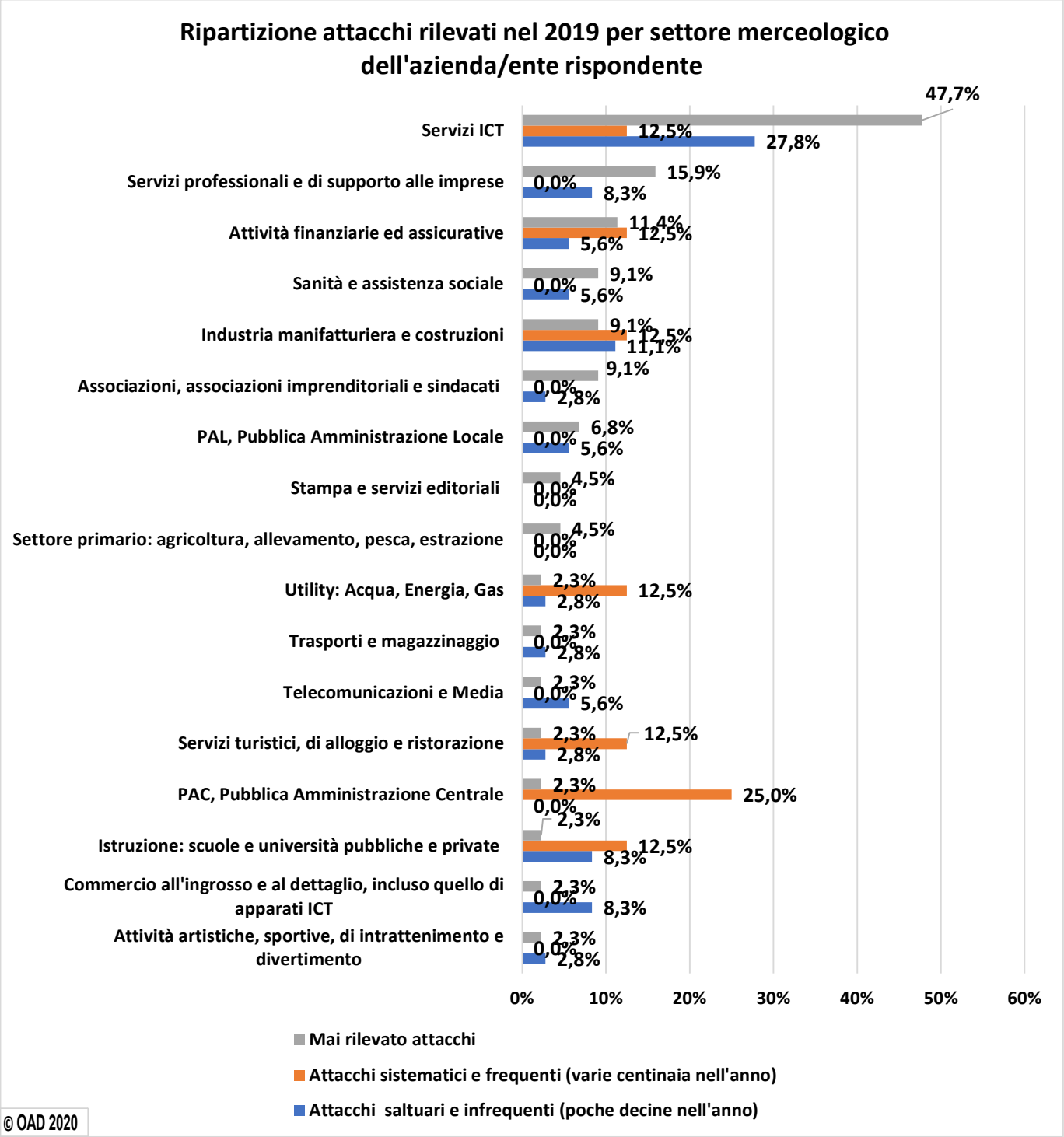

Ripartizione attacchi rilevati nel 2019 per settore merceologico dell'azienda/ente rispondente
Servizi ICT
47,7%
12,5%
27,8%
Servizi professionali e di supporto alle imprese
15,9%
0,0%
8,3%
Attività finanziarie ed assicurative
11,4%
12,5%
5,6%
Sanità e assistenza sociale
9,1%
0,0%
5,6%
Industria manifatturiera e costruzioni
9,1%
12,5%
11,1%
Associazioni, associazioni imprenditoriali e sindacati
9,1%
0,0%
2,8%
PAL, Pubblica Amministrazione Locale
6,8%
0,0%
5,6%
Stampa e servizi editoriali
4,5%
0,0%
0,0%
Settore primario: agricoltura, allevamento, pesca, estrazione
4,5%
0,0%
0,0%
Utility: Acqua, Energia, Gas
2,3%
12,5%
2,8%
Trasporti e magazzinaggio
2,3%
0,0%
2,8%
Telecomunicazioni e Media
2,3%
0,0%
5,6%
Servizi turistici, di alloggio e ristorazione
2,3%
12,5%
2,8%
PAC, Pubblica Amministrazione Centrale
2,3%
25,0%
0,0%
Istruzione: scuole e università pubbliche e private
2,3%
12,5%
8,3%
Commercio all'ingrosso e al dettaglio, incluso quello di apparati ICT
2,3%
0,0%
8,3%
Attività artistiche, sportive, di intrattenimento e divertimento
2,3%
0,0%
2,8%
0%
10%
20%
30%
40%
50%
60%
Mai rilevato attacchi
Attacchi sistematici e frequenti (varie centinaia nell'anno)
Attacchi saltuari e infrequenti (poche decine nell'anno)
© OAD 2020

Fig. 6-10

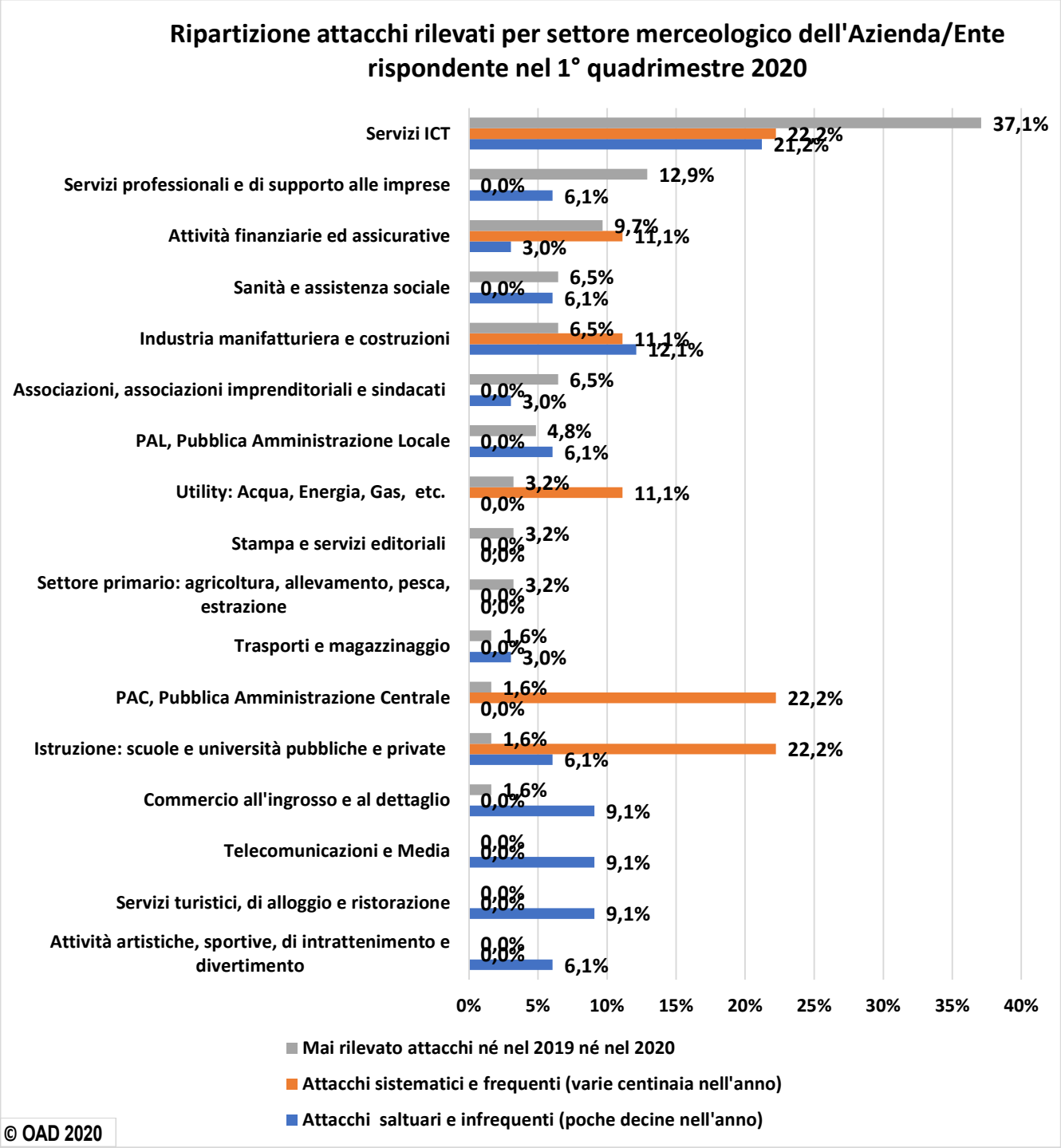


Fig. 6-11

Le due figure evidenziano, così come più chiaramente quelle in §10.2, che la maggior parte dei rispondenti a OAD 2020 appartengono al settore dei sevizi ICT,
Grazie ai ripetuti inviti a compilare il questionario on line, ed anche al voluto protrarsi della chiusura del questionario per poter raggiungere un numero "minimo" di rispondenti, tutti i settori merceologici hanno fornito delle risposte, ma solo i settori sopra indicati hanno fornito un numero sufficiente, seppur ancora basso, di risposte, e le indicazioni percentuali loro relative forniscono indicatori

significativi e credibili. Tutti gli altri contribuiscono numericamente all'inquadramento generale del fenomeno degli attacchi digitali in Italia, sono interessanti, ma sono troppo pochi per poter effettuare specifiche analisi settoriali e considerarli indicatori di riferimento della situazione degli attacchi digitali del loro settore. I referenti di alcune aziende/enti non hanno risposto ad alcune delle domande del questionario, trincerandosi dietro le policy aziendali che impediscono il fornire questo tipo di informazioni classificate come riservate, anche se il questionario è totalmente anonimo. Per questo motivo si ritiene più significativo correlare gli attacchi rilevati, o non, con le dimensioni delle Aziende/Enti in termini di numero di dipendenti e in termini di fatturato annuo, come mostrato nelle fig. 6-5 e 6-6.

L'acquisizione di risposte al questionario OAD 2020 è stata particolarmente difficile, dati i gravi problemi per qualsiasi azienda o ente causati dalla pandemia Covid-19 scatenatasi ad inizio 2020 e tuttora perdurante. Ma l'indagine OAD ha sempre avuto difficoltà, anche negli anni precedenti, a far rispondere al questionario, soprattutto per settori lontani, come specifiche competenze, dall'ambiente digitale. Per questo motivo AIPSI ed OAD hanno deciso di sviluppare nel 2021-22 un progetto, chiamato OAD Extended, per coinvolgere ben più diffusamente e sistematicamente i potenziali rispondenti e fruitori di OAD di ogni settore merceologico, PA incluse, oltre a far evolvere OAD nell'ottica di fornire ad aziende/enti della domanda ICT specifici servizi per aiutarle a realizzare per il loro sistema informatico le idonee misure e strumenti di sicurezza digitale, in modo autore ed indipendente dai fornitori. La scheda del progetto OAD Extented, con maggiori dettagli è disponibile in https://www.oadweb.it/it/l-indagine-oad/oad-extended.html. Il progetto OAD Extended rientra nei progetti dell'iniziativa strategica della Presidenza del Consiglio dei Ministri "Repubblica Digitale": si veda https://repubblicadigitale.innovazione.gov.it/it/

Ogni tipologia di attacco viene analizzata e commentata nel relativo paragrafo del presente Capitolo 6, cui si rimanda, ma complessivamente l'indagine OAD 2020 ben rappresenta, percentualmente, la situazione italiana (si veda fig. 6-4 e §10.2): il 57,5% dei rispondenti è di aziende/enti di medio piccole dimensioni (fino a 250 dipendenti), e di queste il 27,1% sotto i 10.

Al di là della diffusione della tipologia di attacchi e delle tecniche usate per attuarli, l'indicatore più significativo per valutare la gravità di un attacco è l'impatto che può avere sull'Azienda/Ente. Impatti rilevati o stimati dai rispondenti per ogni tipo di attacco, e riportati nei paragrafi seguenti.
Indipendentemente dal tipo di attacco, l'impatto più significativo, in termini generali, è quello economico, cui si possono inoltre parametrare tutti gli altri impatti considerati. In §7.1, cui si rimanda, sono analizzati i dati rilevati dai rispondenti su tali impatti.

6.1 Distruzione fisica di dispositivi ICT o di loro parti

La distruzione fisica intenzionale di dispositivi ICT o di loro parti, e non dovuta quindi a malfunzionamenti e rotture che possono capitare "fisiologicamente" a qualsiasi dispositivo, soprattutto se molto usato o obsoleto, oppure per eventi straordinari quali calamità naturali, crolli o esplosioni accidentali nei locali ove operano, non può che essere attuata tramite un attacco di tipo fisico, svolto da persone che entrano, con o senza permessi, nei locali ove sono situati questi sistemi, e volutamente li danneggiano a livello fisico: forti colpi per scassare la loro struttura, rottura delle connessioni e delle parti elettroniche, rottura delle ventole di raffreddamento e della parte di alimentazione, etc.
Nel Questionario OAD 2020, essendo la possibile tecnica di attacco solo di tipo fisico, non sono state riportate le sotto-domande sulle possibili tecniche di attacco usate.

La fig. 6.1-1 evidenzia quanti rispondenti hanno subito tale attacco nei periodi considerati: la percentuale emersa porta questa tipologia d'attacco al terzo posto come diffusione nel 2019, si veda fig. 6-4. A parere dell'autore le percentuali emerse sono alte, anche si simili a quelle rilevate per il 2018 (24,17%): come già sottolineato in §6, è probabile che taluni rispondenti abbiano selezionato questo attacco anche in caso di normali rotture del dispositivo fisico.

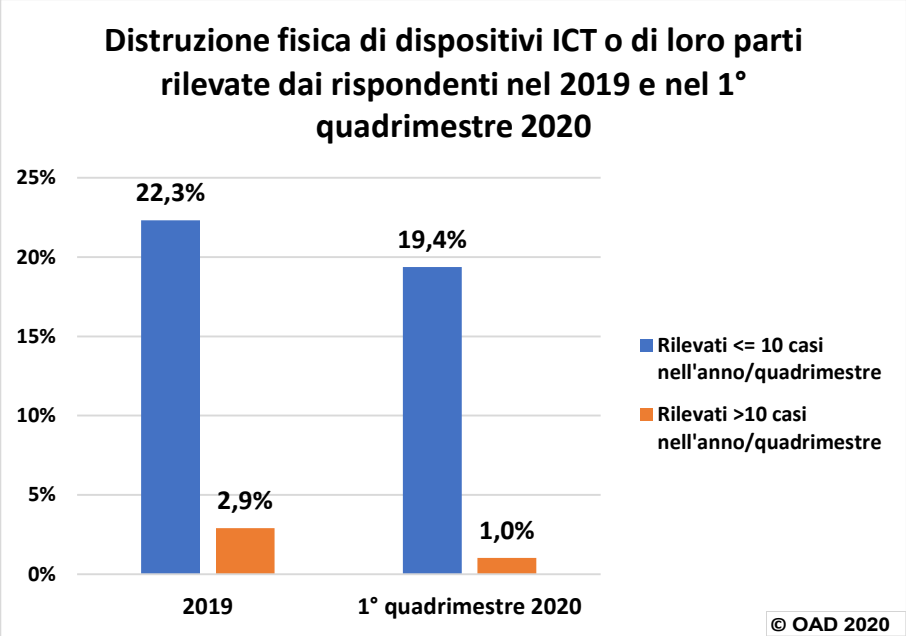


Fig. 6.1-1

La fig. 6.1-2 evidenzia, con risposte multiple, che per la maggioranza dei rispondenti gli impatti, pur nei casi più gravi, sono stati irrilevanti. Un quarto e più ha subito una parziale interruzione, ma con un ripristino in tempi brevi. Impatti più gravi hanno percentuali più basse, a parte nel 1° quadrimestre la perdita di immagine per un quarto dei rispondenti, impatto che non trova, stranamente, riscontro nel 2019.
La fig. 6.1-3, con risposte multiple, elenca le principali motivazioni dell'attacco: al primo posto la ritorsione e/o il ricatto. Interessante notare che quasi un terzo dei rispondenti che hanno rilevato questa tipologia d'attacco dichiara di non conoscere la possibile motivazione: una così alta percentuale conferma il sospetto dell'autore che probabilmente molti hanno selezionato la distruzione fisica volontaria di un dispositivo, quando questo si è rotto o guastato per suoi problemi interni. Da notare l'alta percentuale, 26,9%, che indica il sabotaggio.
La fig. 6.1-4 mostra il tempo di ripristino della situazione *ex ante* nel caso del peggior attacco subito. Tutti riescono a ripristinare entro una settimana, ed il 60% entro il primo giorno. Questo significa che i rispondenti hanno dispositivi di scorta e/o contratti di manutenzione che consentono una veloce sostituzione dei sistemi e dispositivi ICT rovinati.

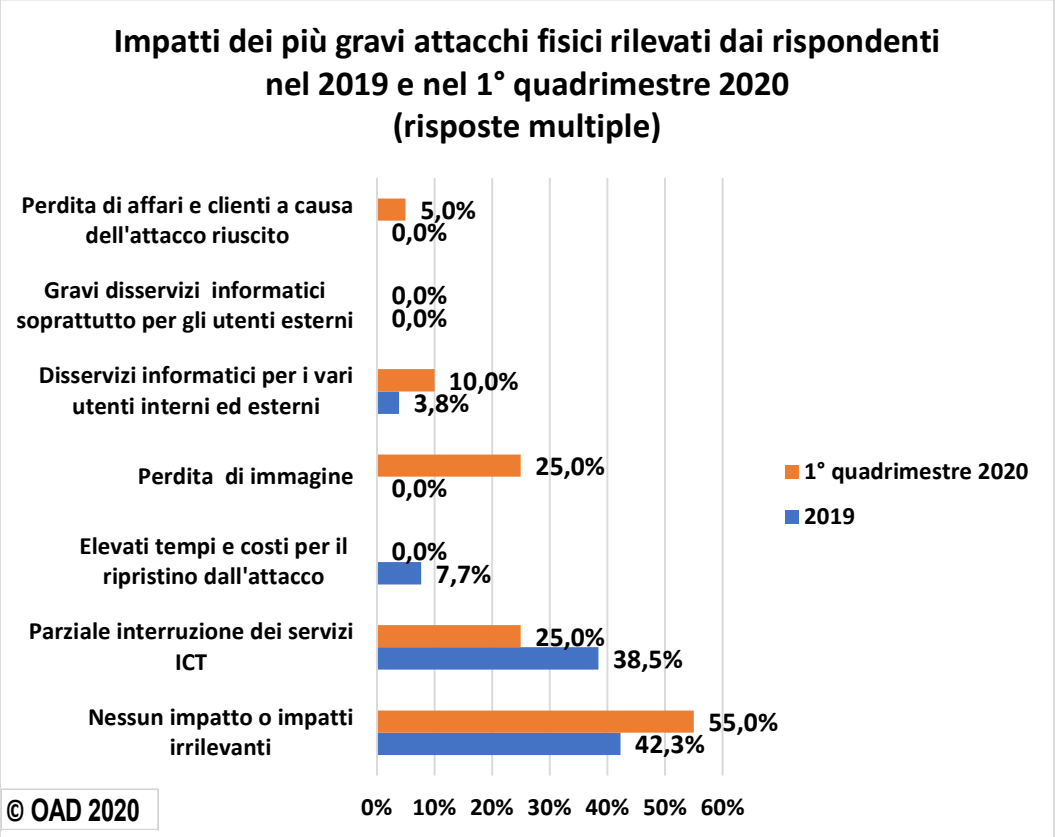


Fig. 6.1-2

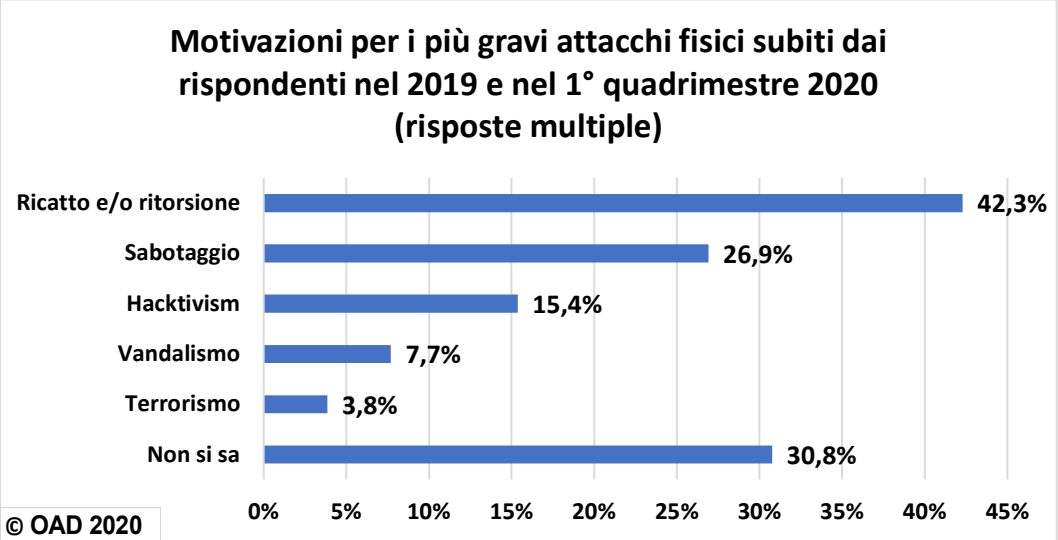


Fig. 6.1-3

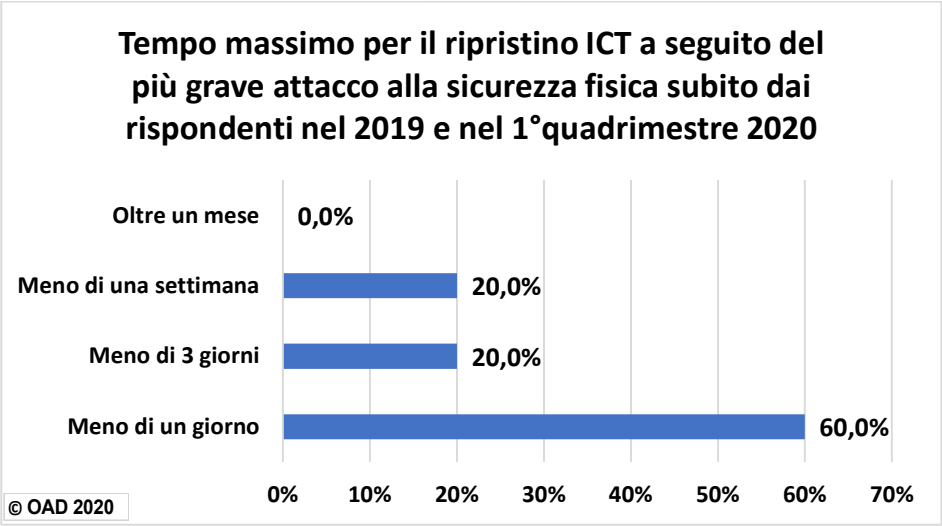


Fig. 6.1-4

6.2 Furto di dispositivi ICT mobili

Il furto di dispositivi mobili di proprietà dell'Azienda/Ente, costituiti soprattutto da laptop (PC mobili), smartphone e tablet, è relativamente semplice e facile, date le loro piccole dimensioni, e il prezzo non indifferente di tali dispositivi alimenta un ampio mercato "nero" per la loro rivendita. La maggior parte dei furti di questi dispositivi includono smartphone e tablet, ed è dovuta al loro valore - e in misura inferiore per utilizzare i dati conservati, spesso molto riservati: questo è confermato dai dati in §6.5 sul furto delle informazioni dai dispositivi mobili.
Si deve tener presente che i dispositivi mobili includono anche le chiavette USB e gli hard disk removibili e/o con interfaccia USB. Il furto di tali dispositivi è probabilmente più dovuto alla acquisizione delle informazioni in essi contenuti, che per il valore del dispositivo.

La fig. 6.2-1 mostra che il 28,2% ed il 17,2% dei rispondenti che hanno rilevato attacchi nei due periodi considerati hanno subito questo tipo di furto. poco più di 1/3 dei rispondenti, 33,6%, ha subito un furto di dispositivi ICT mobili nel 2018: una percentuale alta, che indica come ancora gli utenti non pongano la dovuta attenzione alla protezione, anche solo fisica, di questi dispositivi, che invece sono tecnicamente sempre più potenti e che di fatto sono sempre più utilizzati in sostituzione dei PC, anche di tipo laptop.
La tecnica d'attacco per rubare dispositivi mobili può essere solo l'attacco fisico: per tale motivo nel questionario OAD 2019, per questa tipologia di attacco non sono state riportate le sotto-domande sulle possibili tecniche di attacco usate.
La fig. 6.2-2, con risposte multiple, mostra gli impatti subiti a seguito del furto di dispostivi ICT mobili: per la stragrande maggioranza gli impatti sono stati irrilevanti, e più della metà dichiara che ha risolto l'interruzione del servizio in tempi brevi e con costi limitati. Qualcuno ha invece avuto problemi più seri, forse perché il dispositivo conteneva dati riservati non duplicati su altro strumento, o perché i dati contenuti sono stati poi usati per specifici attacchi (si veda §6.5).
La fig. 6.2-3, con risposte multiple, elenca le principali motivazioni, individuate o stimate, dell'attacco: il 66.7% dei rispondenti ritiene che il motivo sia il valore della risorsa ICT rubata da rivendere, e il 33,3% per il furto del contenuto informativo dell'oggetto rubato.

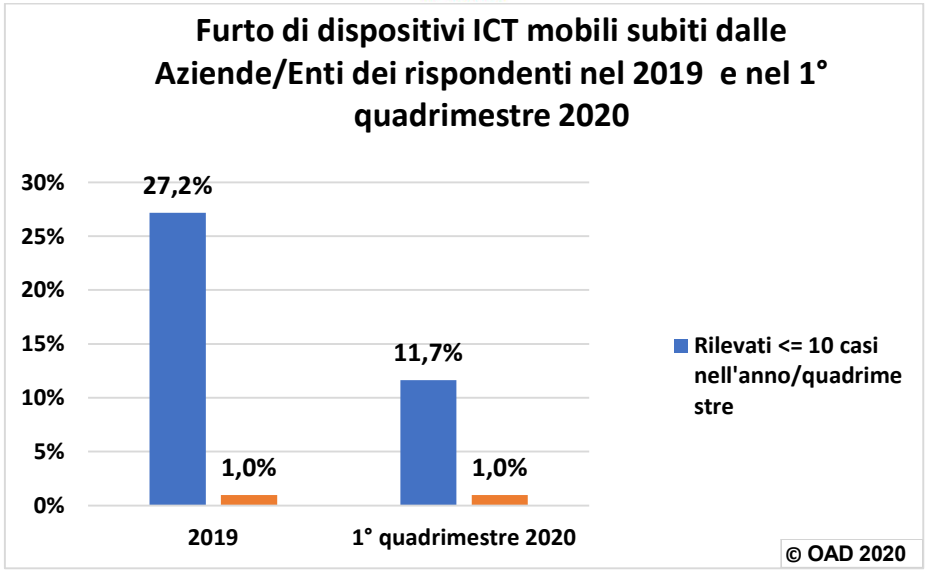


Fig. 6.2-1

La fig. 6.2-4 mostra il tempo di ripristino nel caso del peggior caso di furto di un dispositivo mobile nell'intero periodo considerato. Data la semplicità del ripristino, il 96% dei casi peggiori sono stati risolti entro una settimana, ed il 39% in un solo giorno.

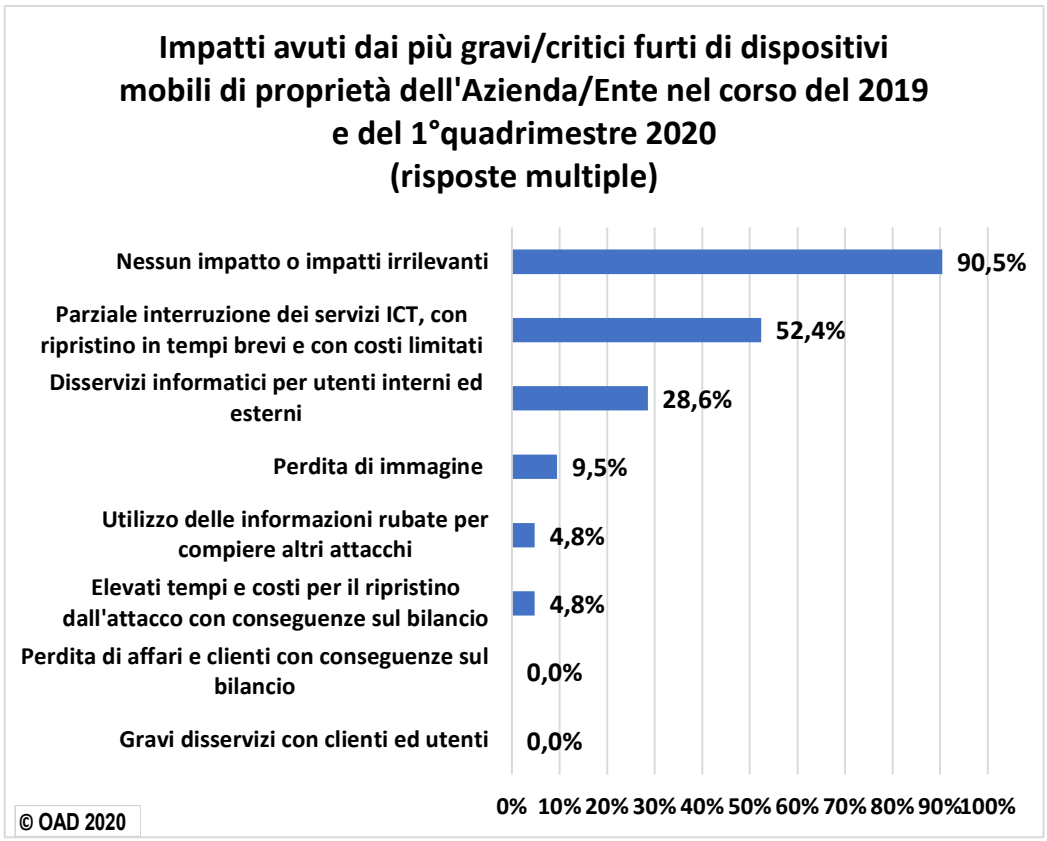


Fig. 6.2-2

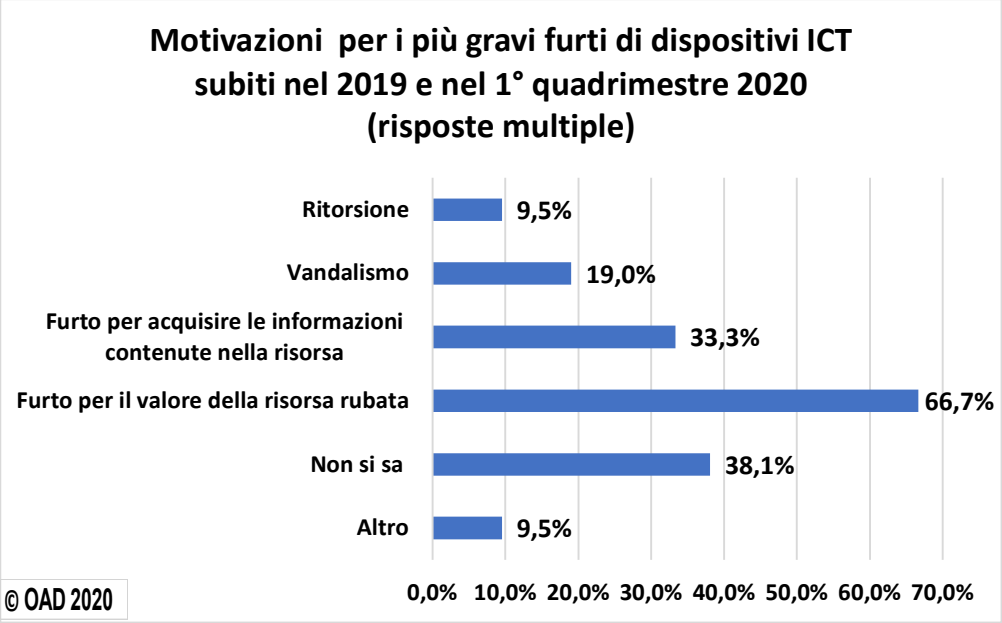


Fig. 6.2-3

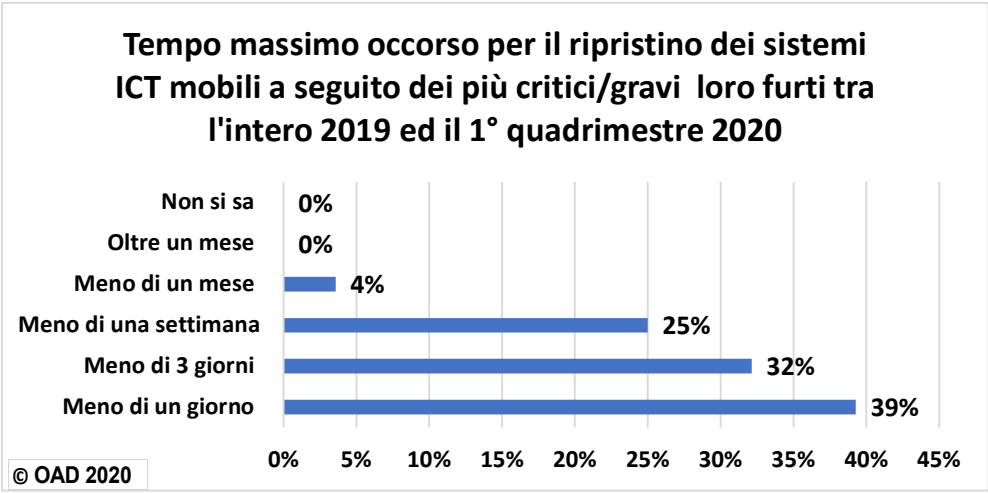


Fig. 6.2-4

6.3 Furto di dispositivi ICT fissi o di loro parti

I dispositivi ICT includono server, sistemi di storage, unità di rete, dispositivi d'utente fissi quali PC e workstation; le loro parti includono i vari componenti dalla scheda madre ai connettori, dai singoli chip alle periferiche quali ad esempio l'hard disk (non quello removibile o le chiavette USB), il mouse e/o il video. La tecnica d'attacco può essere solo quella dell'attacco fisico: per tale motivo nel questionario OAD 2020, per questa tipologia di attacco non sono state riportate le sotto-domande sulle possibili tecniche di attacco usate.

La fig. 6.3-1 evidenzia come la diffusione, in percentuale, di questa tipologia d'attacco è inferiore, soprattutto nel 2019, rispetto al ben più facile e semplice furto di dispositivi mobili. Ma questo tipo di furti esiste ancora, soprattutto nelle piccole realtà con i sistemi ICT disposti negli stessi uffici dell'Azienda/Ente o in computer room fisicamente poco protette.

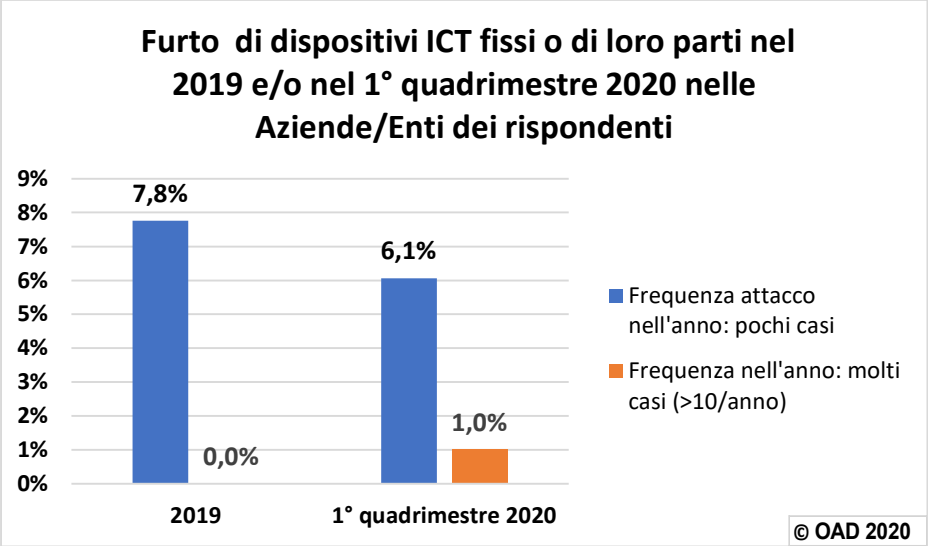


Fig. 6.3-1

La fig. 6.3-2 mostra gli impatti subiti a seguito del furto di dispostivi ICT fissi o di loro parti: tre quarti dei rispondenti ha dichiarato di aver avuto disservizi, ma risolti in tempi relativamente brevi ed a costi limitati. Solo il 37,5% non ha avuto impatti o sono stati irrilevanti e di facile risoluzione. Percentuali minori, ma sopra il 10%, per gli impatti più gravi, tra i quali la perdita di immagine.

La fig. 6.3-3 elenca le principali possibili motivazioni dell'attacco, molti simile a quelle indicate per i sistemi mobili. Alla pari al 50% le motivazioni principali: il valore della risorsa ICT fissa rubata e per il furto del contenuto informativo.

La fig.6.3-4 conferma che la maggior parte degli impatti sono stati o trascurabili o comunque rimediabili in relativamente poco tempo: nel 44,5% dei casi è stata risolta in giornata, nel 94,4% entro una settimana.

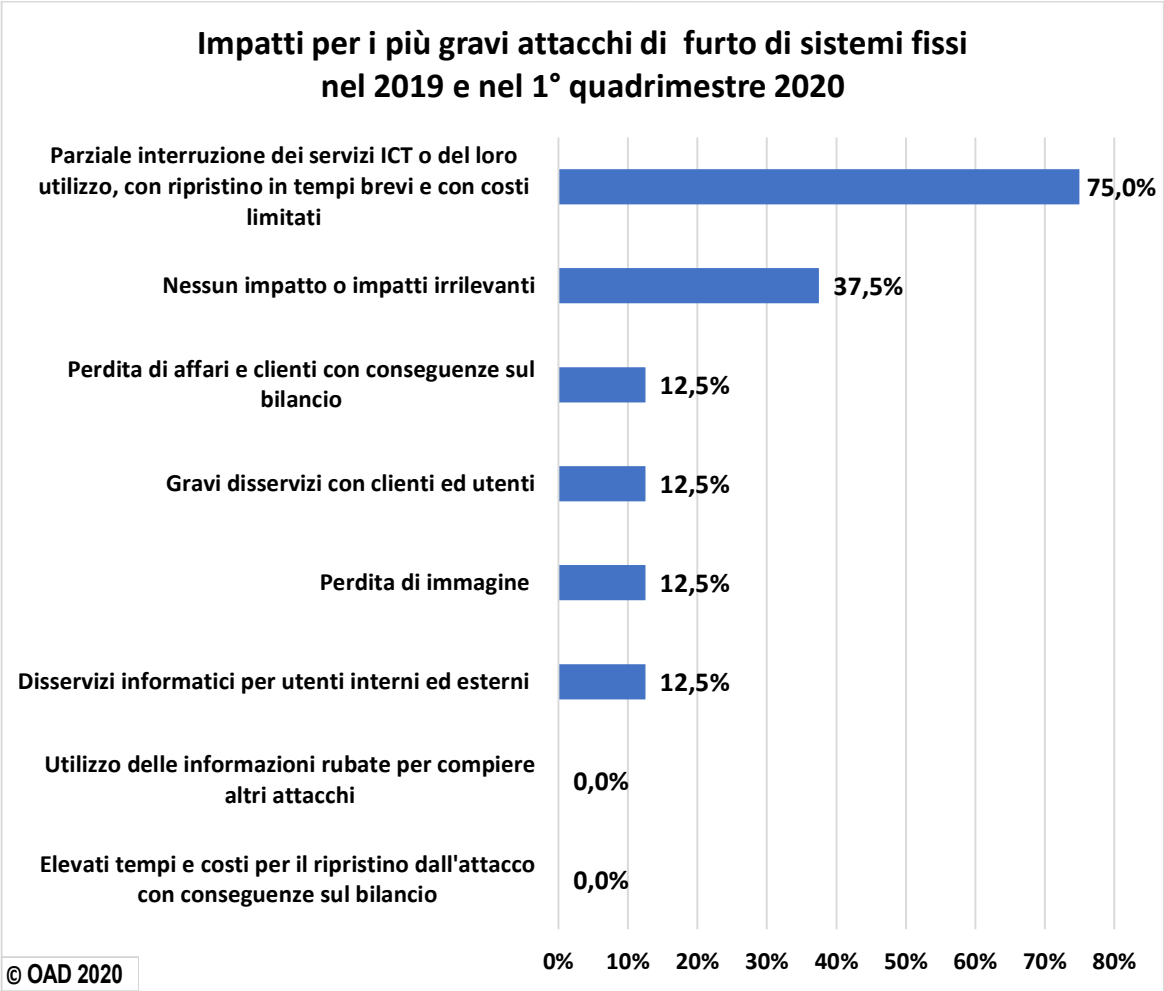

Impatti per i più gravi attacchi di furto di sistemi fissi nel 2019 e nel 1° quadrimestre 2020
Parziale interruzione dei servizi ICT o del loro utilizzo, con ripristino in tempi brevi e con costi limitati
75,0%
Nessun impatto o impatti irrilevanti
37,5%
Perdita di affari e clienti con conseguenze sul bilancio
12,5%
Gravi disservizi con clienti ed utenti
12,5%
Perdita di immagine
12,5%
Disservizi informatici per utenti interni ed esterni
12,5%
Utilizzo delle informazioni rubate per compiere altri attacchi
0,0%
Elevati tempi e costi per il ripristino dall'attacco con conseguenze sul bilancio
0,0%
0%
10%
20%
30%
40%
50%
60%
70%
80%
© OAD 2020

Fig. 6.3-2

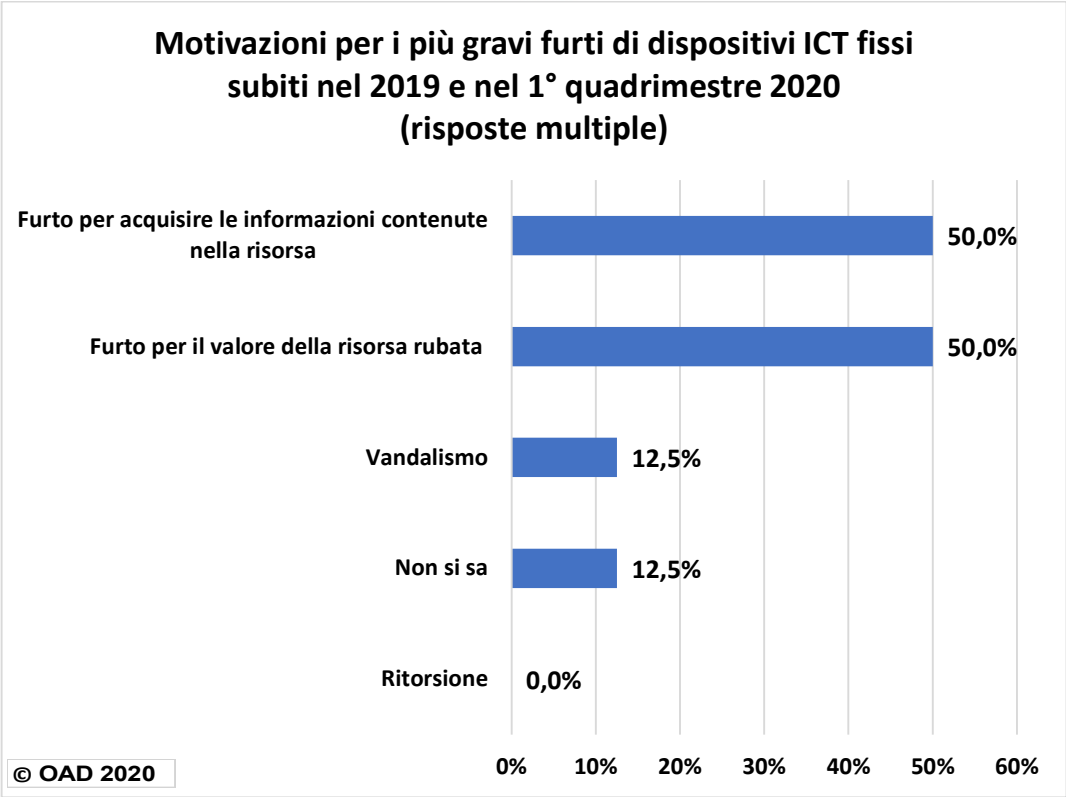


Fig. 6.3-3

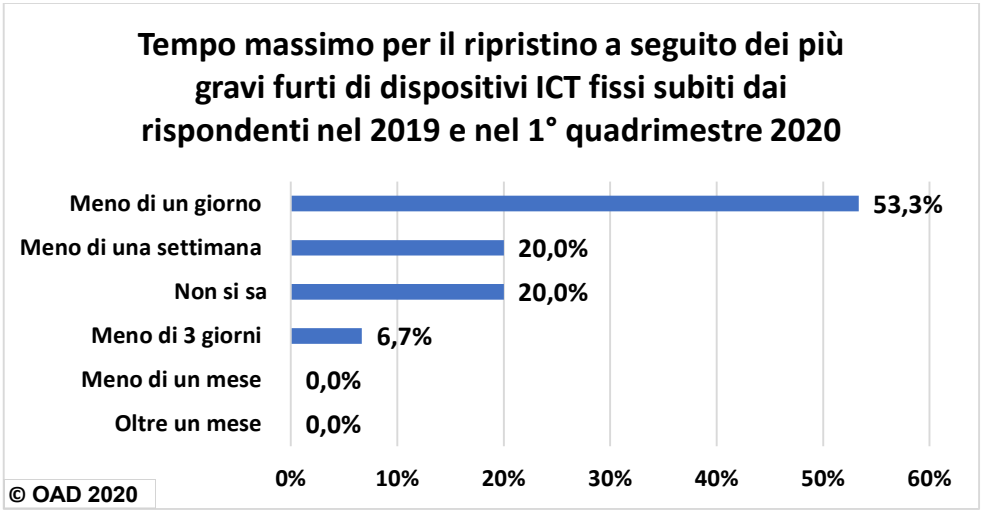


Fig. 6.3-4

6.4 Furto informazioni da sistemi ICT fissi

Il furto di informazioni da sistemi fissi implica che l'attaccante sia stato in grado di accedere, senza averne i diritti, al sistema ICT ed una volta entrato di acquisire le informazioni, tipicamente archiviate in file o su banche dati, e di copiarle: il contesto tipico è il PC e la workstation fissi, dato che rubare informazioni da sistemi ICT quali un server o uno storage è (o dovrebbe essere) ben più difficile, anche se concettualmente analogo. Ma da questi sistemi fissi, se dotati di porte USB, è facile estrarre "fisicamente" grandi quantità di dati grazie alle moderne potenti chiavette USB , che hanno ormai capacità di vari Terabyte: e che sono facilmente occultabili in una tasca o in una borsa.
È difficile individuare il furto di un'informazione, dato che, al contrario di un bene materiale, con il suo furto non viene a mancare l'informazione originale (a meno che non sia cancellata dopo la copia): scoprire il furto non è quindi semplice e lo si fa prevalentemente in maniera indiretta, verificando i log degli accessi, scoprendo se l'informazione è presente in altri sistemi esterni, se è stata pubblicata, etc.
L'unico modo per proteggere un'informazione dal suo furto (o anche da una sua lettura non autorizzata) è di crittografarla, come il GDPR[9] indica: si veda anche §9.2 sulle misure tecniche di contrasto in atto da parte dei rispondenti.

La fig. 6.4-1 mostra quanti rispondenti hanno subito tale tipo di attacco nel 2019 e nel 1° quadrimestre 2020, evidenziando che nell'ultimo periodo considerato si è rilevato un aumento di circa il 3% rispetto al 2019. I dati emersi simili a quanto rilevato nel 2018 e nel 2017 delle precedenti edizioni di OAD, ben superiori al solo 1,54% del 2016. Questi forti aumenti, e l'ulteriore incremento del 2020 indicano come dal 2017 gli attacchi digitali anche nella realtà italiana siano cresciuti significativamente per numero e gravità. Le percentuali emerse del 20,4% e del 23,2% sono nettamente superiori a quelle relative ai furti di informazioni dai dispositivi d'utente mobili, 11,7% e 7,1% (si veda §6.5). Sembrerebbe più facile il furto fisico di un dispositivo mobile, e da questo avere accesso ai file e ai dati ivi contenuti. Ma essendo ben nota tale vulnerabilità, chi ha dati critici sui sistemi mobili tende a proteggerli adeguatamente, anche crittandoli, e non passa il proprio dispositivo a colleghi, amici, conoscenti. Le possibilità d'attacco per il furto di dati da sistemi fissi sono molto più ampie, dato che vanno dai dispositivi d'utente fissi ai server, dalle unità di rete ai servizi terziarizzati e in cloud. Il posto di lavoro fisso, essendo molto diffuso, è anche più vulnerabile e può contenere dati critici, soprattutto con gli applicativi di informatica individuale, e può essere talvolta usato da più utenti diversi; ed i dati contenuti non sono il più delle volte crittati.

[9] GDPR, General Data Protection Regulation, EU Regulation 2016/679 (119 pagine A4), è il nuovo regolamento europeo sulla privacy**,** che sostituisce la precedente norma europea sulla privacy, la Direttiva 95/46/EC alla base delle precedenti leggi italiane sulla privacy, la 675/1996 e la 196/2003.
Per scaricare il GDPR in italiano: http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32016R0679

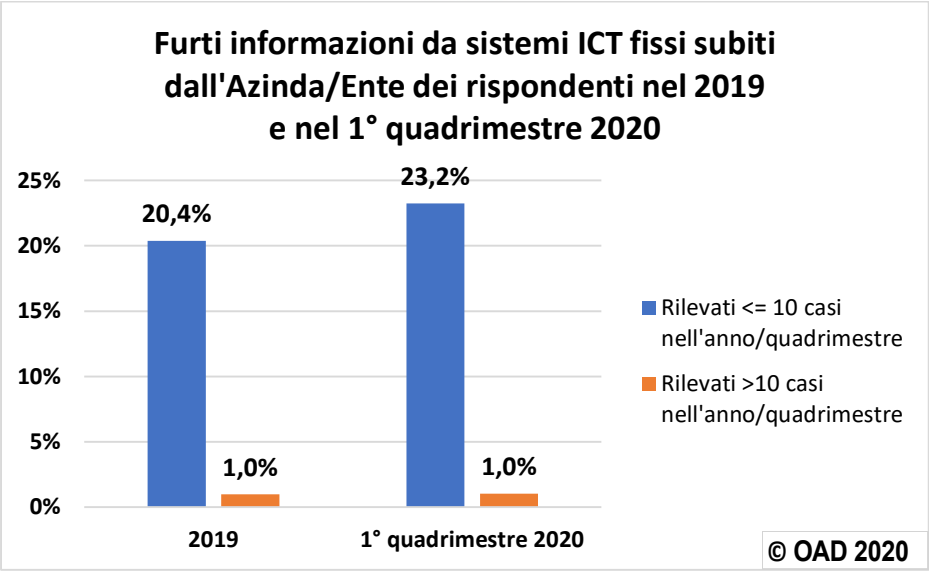


Fig. 6.4-1

La fig. 6.4-2 dettaglia le tecniche d'attacco per il furto di informazioni da sistemi ICT fissi, con risposte multiple. Al primo posto, con un elevato 73,9%, le tecniche di raccolta informazioni, quali il social engineering, cui seguono, a scalare, le altre tecniche, ma sempre con valori abbastanza elevati (risposte multiple): un chiaro indicatore della sofisticazione e della complessità degli attacchi odierni. Elemento che viene confermato nella fig. 6.4-3, con risposte multiple, sugli impatti rilevati. Poco più della metà dei rispondenti, il 52,2% non ha avuto impatti, o sono stati irrilevanti, ma il 4,8%, poco meno della metà, ha subito gravi disservizi anche con i clienti. Seguono a scalare, ma con percentuali molto inferiori, gli altri impatti considerati. Le motivazioni stimate dai rispondenti per questa tipologia d'attacco sono riportate nella fig. 6.4-4, con risposte multiple: la motivazione più diffusa, con il 60,9%, è il furto per utilizzare in proprio o per rivendere le informazioni. Segue per più della metà, l'uso di tali informazioni per effettuare ulteriori specifici attacchi digitali. Una percentuale non trascurabile, quasi il 40%, riguarda ritorsioni e ricatti.

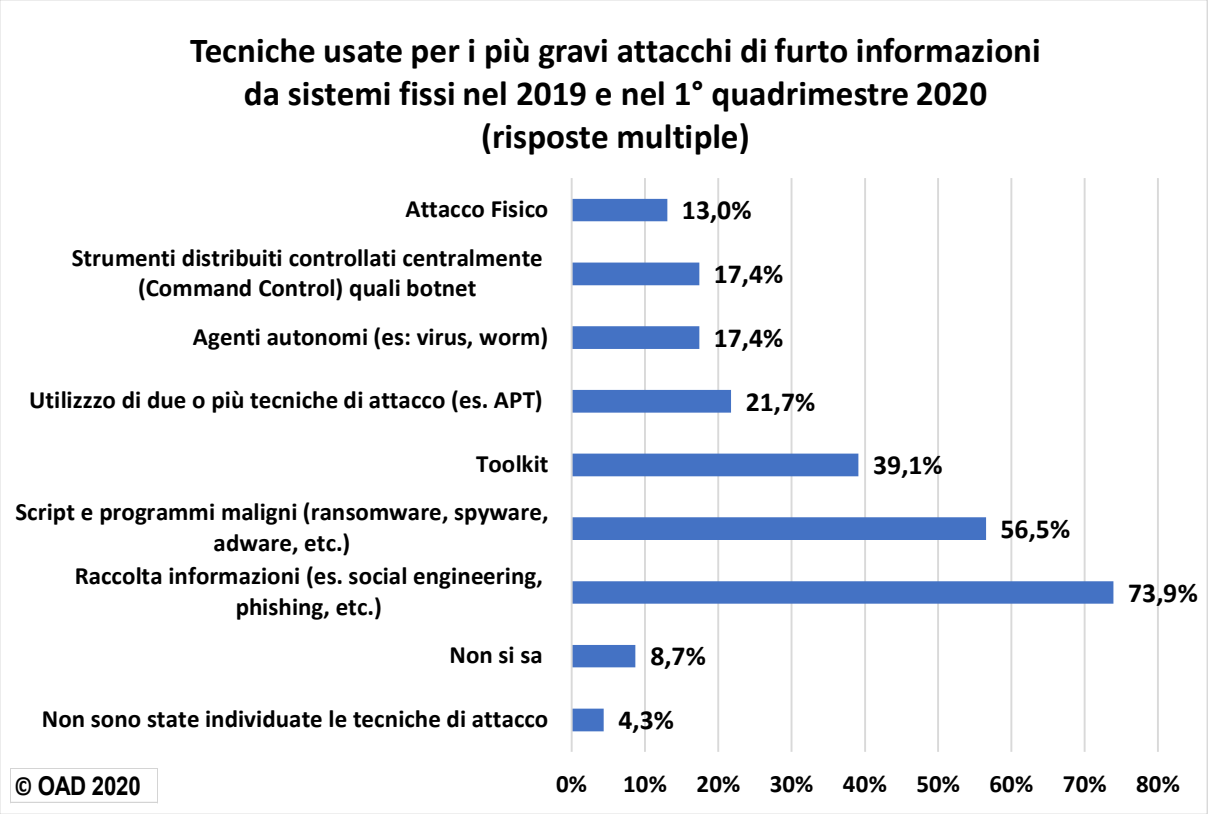


Fig. 6.4-2

La fig. 6.4-5 mostra che, a seguito del più grave furto di informazione da sistemi fissi, sono occorsi per il ripristino della situazione ex ante 3 giorni per l'87,5% dei rispondenti, di cui il 29,2% ripristina nella stessa giornata. Nessuno ha avuto bisogno di più di un mese per il ripristino, ma un elevato 8,3% dei rispondenti ammette di non sapere quanto tempo sia stato necessario per il ripristino

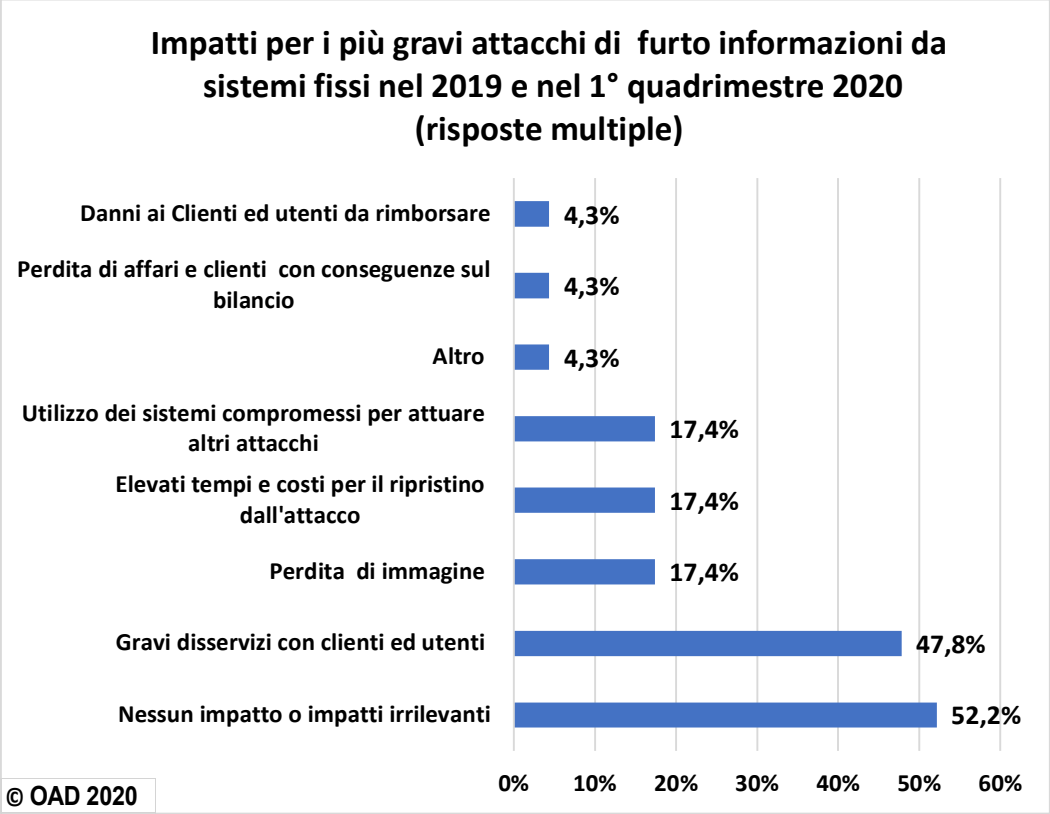


Fig. 6.4-3

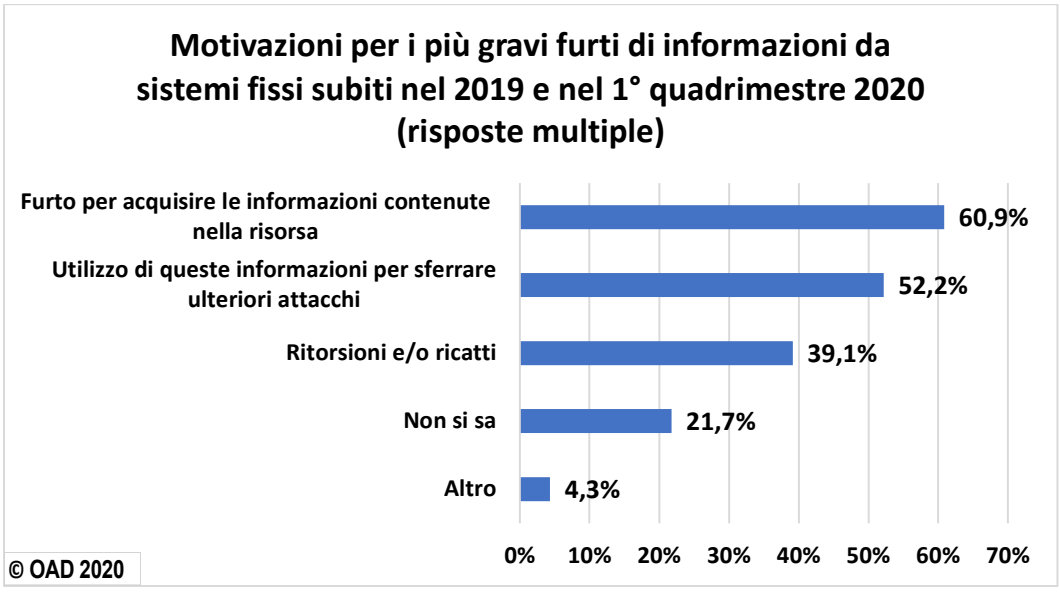


Fig. 6.4-4

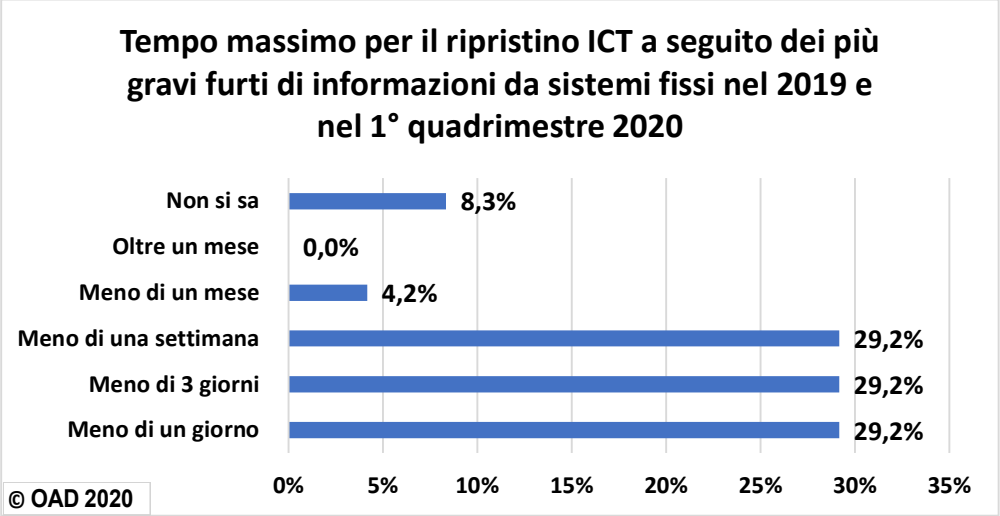


Fig. 6.4-5

6.5 Furto informazioni da sistemi ICT mobili

Come già indicato in §6.2, con il termine di "sistemi ICT mobili" si intendono i vari dispositivi d'utente mobili, che includono tipicamente smartphone, tablet e laptop, le chiavette e gli hard disk removibili con interfaccia USB, che hanno raggiunto e stanno superando i 2 Terabyte a prezzi ragionevoli, con dimensioni tascabili e senza alimentazione separata a supporto. Chiavette e hard disk removibili così potenti sono usati sovente come supporti ai back-up, e come tali possono essere rubati per ottenere grandi quantità, o anche la totalità, di dati dell'Azienda/Ente target dell'attacco. Questi dispositivi con simile capacità di memoria e con dimensioni fisiche tali da poter essere occultati facilmente in una tasca, possono inoltre essere utilizzati per copiare interi file system da server, da unità di storage, oltre che da singoli PC e workstation, ma questo fa riferimento al precedente §6.4 sul furto di informazioni da sistemi ICT fissi, ed esula da questo paragrafo.

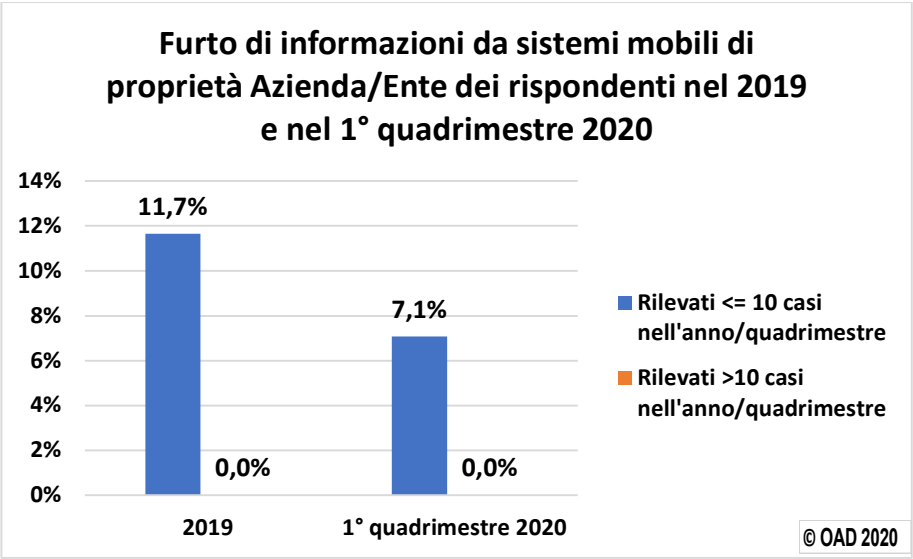


Fig. 6.5-1

Come mostrato nella fig. 6.5-1, nel 2019 il furto dei dati da appariti mobili è circa la metà, in percentuale, del furto "fisico" dell'apparato stesso, pari a 27,2% come da fig. 6.2-1. Nel 1° quadrimestre 2020 il 7,1% è un di cui rispetto all'11,7% del furto fisco del dispositivo. dei rispondenti ha rilevato attacchi di questo tipo. Si deve considerare che il furto delle informazioni dai sistemi ICT mobili può avvenire sostanzialmente in due modi: o rubando il dispositivo, per poi cercare di carpire le informazioni contenute, oppure accedono al dispositivo ma senza sottrarlo.
Il primo caso implica il furto dell'intero dispositivo mobile, considerato in §6.2: ed i dati emersi tra furto di dispositivi mobili e furto delle informazioni in essi contenuti sono congruenti.
La fig. 6.5-2, con risposte multiple, evidenzia che la tecnica più diffusa, almeno nel caso dell'attacco più grave, è la raccolta di informazioni, tipicamente il social engineering, con il 90%. Seguono a distanza, ma con percentuali significative, l'uso di script/programmi maligni con un 50%, cui segue l'uso di toolkit. L'attacco fisico, ossia il furto fisico del dispositivo mobile (18,2% dei rispondenti) è solo al quarto posto. Questo significa che gli attacchi, anche sui dispostivi mobili, sono in prevalenza logici ed effettuati con opportuni strumenti informatici. Infatti, se sui dispositivi mobili ci sono informazioni appetibili, essi sono protetti, con i dati anche crittati: così il semplice furto non consente di accedere alle informazioni che vi sono contenute; con opportuni script o malware, magari attivati via phishing, è ben più probabile raggiungere le informazioni contenute.

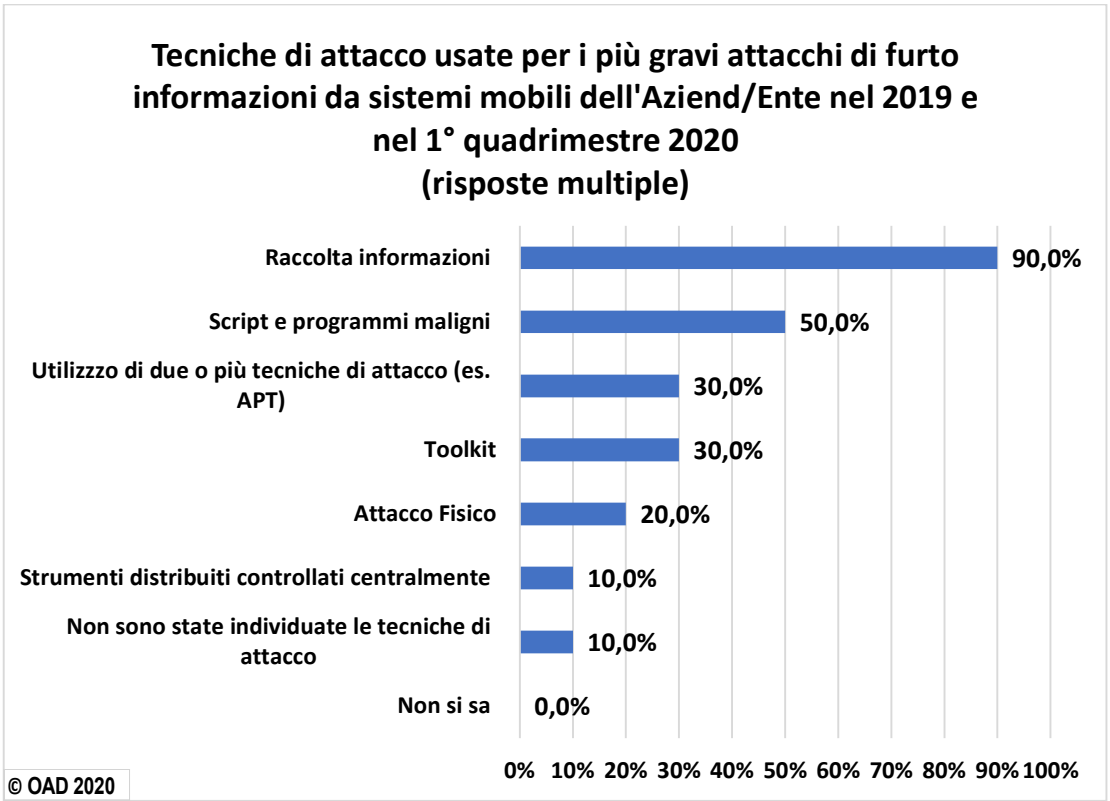


Fig. 6.5-2

La fig. 6.5-3, con risposte multiple, evidenza come l'80% dei rispondenti che hanno subito questo tipo di attacco, anche nei casi più gravi non ha riscontrato impatti, o solo impatti irrilevanti. Ma in molti hanno riscontrato impatti significativi anche sul business: il 30% gravi disservizi, il 20% perdita di immagine con un 20%.
Dalle possibili motivazioni in fig. 6.5-4, con risposte multiple, emerge al primo posto l'utilizzo delle informazioni rubate per sferrare ulteriori attacchi digitali, con un significativo 40%, mentre l'attuazione di ritorsioni/ricatti, che era al primo posto (con un 40,9%) nella scorsa indagine, si posiziona ora al

terzo posto con un 20%. In posizione intermedia l'uso di queste informazioni rubate per rivenderle o per usarle, probabilmente per altri attacchi.
La fig. 6.5-5 relativa al tempo massimo per il ripristino (nel caso più grave) conferma che la maggior parte di questi attacchi non ha avuto significativi impatti: il 92,3% dei rispondenti è riuscito a ripristinare il caso peggiore entro una settimana, e più della metà ha ripristinato nella stessa giornata.

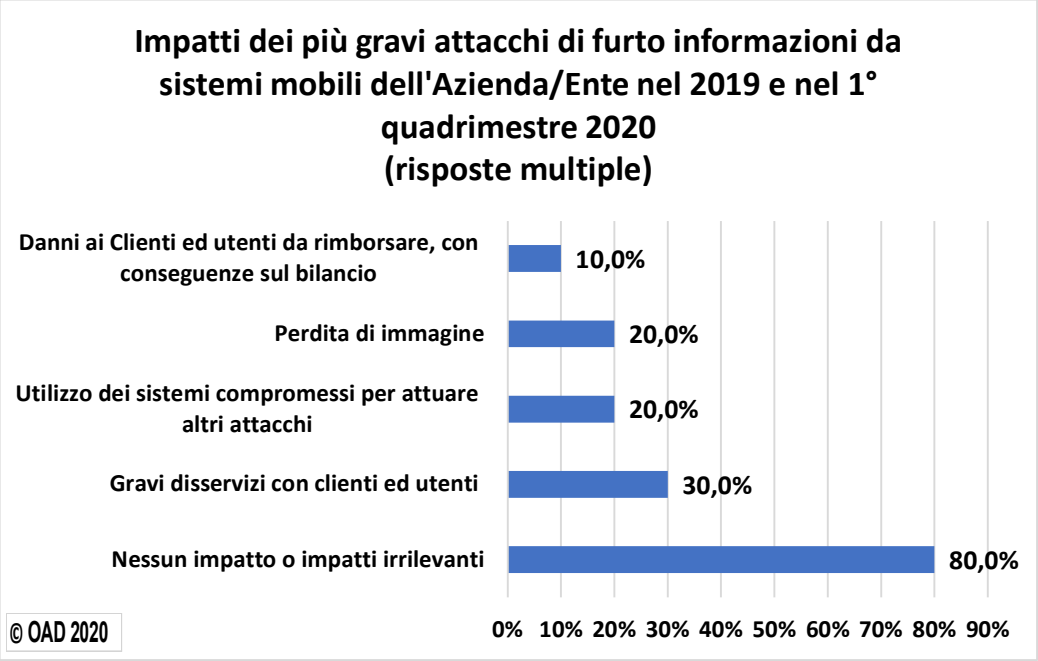


Fig. 6.5-3

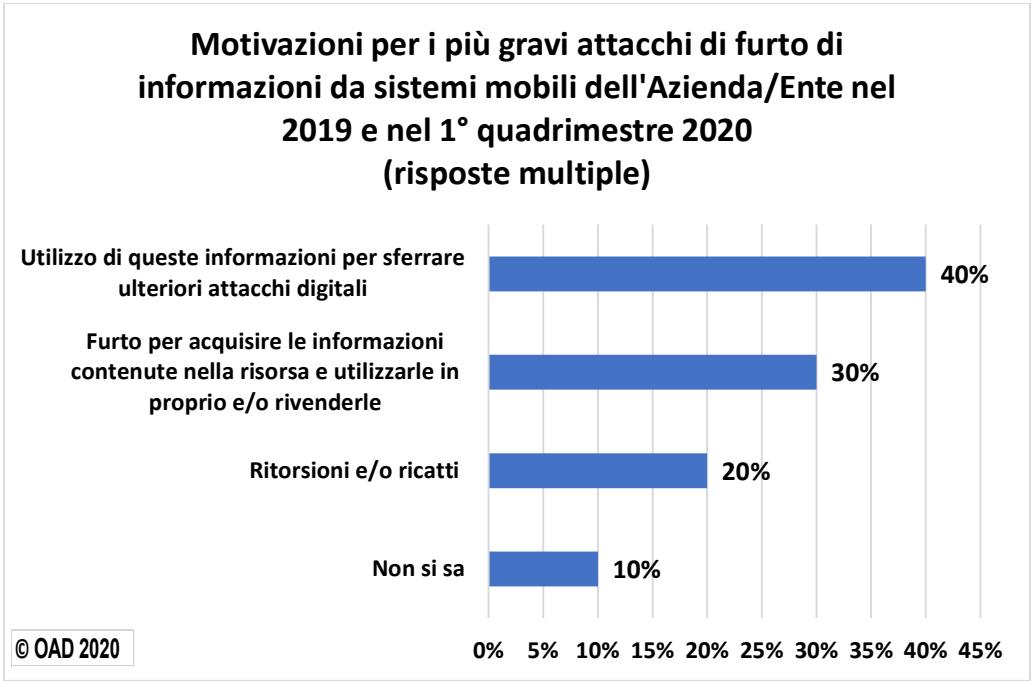


Fig. 6.5-4

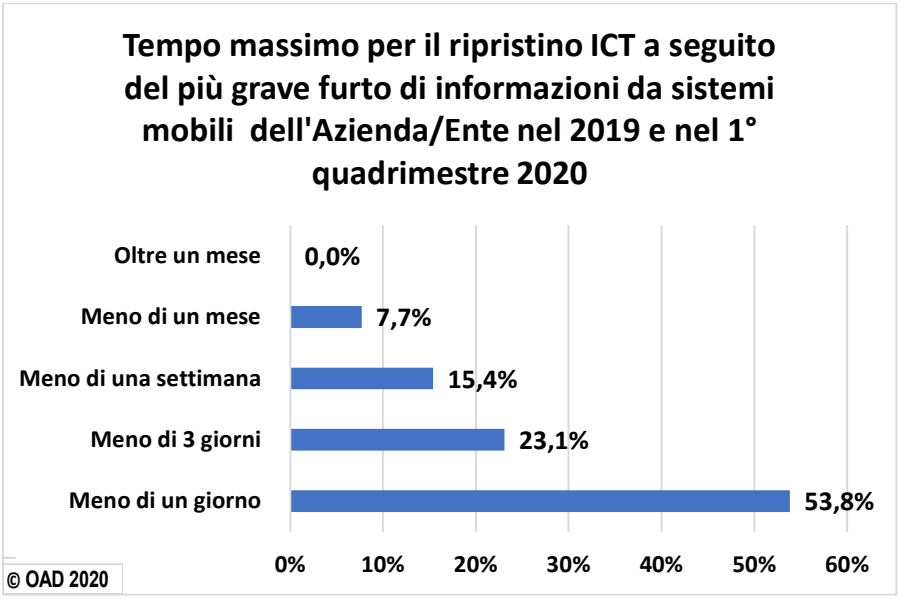


Fig. 6.5-5

6.6 Attacchi all'identificazione, autenticazione e autorizzazioni degli utenti finali e privilegiati

Questa tipologia di attacco è risultata essere la più diffusa tra i rispondenti nel 2019 e nel 1° quadrimestre 2020, come già evidenziato in fig. 6-7. Questa tipologia di attacchi è alla base del furto dell'identità digitale sia a livello di utenti finali sia a livello degli utenti privilegiati, che includono i vari livelli di amministratori e tecnici dei sistemi informatici interni all'organizzazione o di terze parti, quali consulenti, fornitori, sviluppatori software, manutentori, etc.

Riuscendo ad acquisire i diritti per accedere ad un sistema ICT, a seconda del livello di tali diritti, si possono poi compiere specifiche azioni malevoli, dall'inserimento di malware e/o di bot all'uso non autorizzato di applicazioni, acquisendo informazioni e/o manipolandole o eliminandole.

Rubare l'identità digitale di una persona significa acquisire, in maniera illegale, uno o più dei suoi account per poi spacciarsi sui sistemi informatici dell'azienda/ente e su Internet per tale individuo e in tal modo, ad esempio, effettuare transazioni dai suoi conti correnti, usare le sue carte di credito, entrare con le sue credenziali nei sistemi aziendali e delle pubbliche amministrazioni, e così via. L'acquisizione degli account degli utenti privilegiati consente di alterare, anche in maniera diffusa e grave, le configurazioni e le funzionalità dei sistemi informatici dell'azienda/Ente e le informazioni da questi trattate. In taluni casi questo mascherarsi digitalmente per un'altra persona non richiede elevate capacità tecniche, sovente basta un semplice - ma abile - social engineering. I dati per accedere all'account possono essere forniti dallo stesso utente, ad esempio quando richiede che un suo collega, di cui (erroneamente) si fida, lo aiuti o lo sostituisca, anche per un breve periodo, in qualche sua attività informatica. È un atteggiamento abbastanza diffuso in molti uffici e studi professionali, ma è rischioso e dovrebbe essere quanto più possibile evitato e disincentivato.

Nell'ambito generale del controllo degli accessi ai sistemi informatici, si fa riferimento ai tre livelli gerarchici di identificazione, autenticazione e autorizzazione, indicati nel seguito con la sigla IAA.

Sia nel 2019 che nel 1° quadrimestre 2020 gli attacchi IAA tra le Aziende/Enti dei rispondenti hanno la più alta diffusione rispetto alle altre tipologie d'attacco, con 30,9% e 24,2% rispettivamente, come

già evidenziato in fig. 6-7 e dettagliato nella fig. 6.6-1, che evidenza la ripartizione tra attacchi più o meno frequenti e ripetuti.

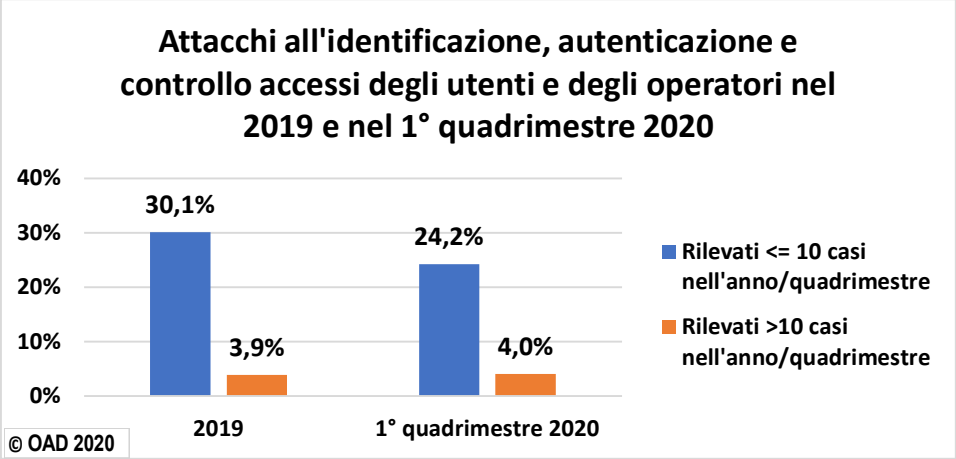


Fig. 6.6-1

Un primato nella diffusione degli attacchi a IAA analogo a quello riscontrato nelle passate indagini OAD: nel 2018 con un 34,2% e nel 2017 con un 39,39%. Pur non essendo confrontabili i dati tra le varie indagini OAD a livello statistico, come trend esse indicano come questi attacchi all'IAA siano fortemente cresciuti rispetto al 2016, dove l'indagine OAD registrò "solo" un 6,67%. Questo fenomeno, secondo l'autore, è dovuto anche, ma non solo, alla forte diffusione ed uso di servizi online finanziari e delle Pubbliche Amministrazioni via Internet. Il furto di identità digitali ed il superamento dei controlli degli accessi permetteva di ottenere facili, illegali ma significativi ritorni economici. All'esplosione di questi attacchi, le misure di sicurezza in ambito IAA, oltre che in altri ambiti, sono state rafforzate e questi attacchi si sono parzialmente ridotti: è la tipica onda *up and down* degli attacchi digitali, già discussa in §6. Si pensi, ad esempio, in questi ultimi anni alla crescente diffusione, soprattutto per l'accesso ad ambiti bancari e delle pubbliche amministrazioni, dell'autenticazione a due o più fattori, spesso con OTP (One Time Password) via cellulare. o con certificati digitali: in Italia la diffusione dello Spid[10] ne è un'ulteriore conferma. I trend tecnologici già indicano ulteriori rafforzamenti della sicurezza in IAA con tecniche di autenticazione passwordless e con identificazioni biometriche.
In §9.2 sono riportate le misure e le tecniche di sicurezza per IAA usate dai rispondenti, cui si rimanda per alcune specifiche considerazioni.
Se circa 1/3 dei sistemi informatici ha ancora rilevato attacchi digitali sull'IAA, significa che le misure in atto non sono sufficienti: numerose ricerche a livello internazionale, ma anche l'esperienza professionale sul campo dell'autore, evidenziano come le misure di base per IAA sono troppo spesso non o malamente attuate. Si pensi, solo per citare i più diffusi problemi nella realtà italiana, gli

[10] Spid, Sistema Pubblico di Identità Digitale, obbligatorio per accedere ai servizi on line delle Pubbliche Amministrazioni italiane, viene fornito da varie società IdP, Indentity Provider, in grado di erogare servizi certificati di IdaaS, Identity as a Service. Spid Fornisce tre livelli crescenti di identificazione ed autenticazione:

1) Identità SPID di primo livello:
   - autenticazione tramite identificativo d'utente e password stabilite dall'utente
2) Identità SPID di secondo livello
   - autenticazione tramite password + generazione di una One Time Password (OTP) inviata all'utente tramite e-mail o SMS oppure tramite App OTP dell'IdP.
3) Identità SPID di terzo livello
   - autenticazione tramite password + certificati digitali PKI, Public Key Infrastructure
   - può trattarsi della chiave segreta usata per la firma digitale

account non personali, le password troppo semplici, troppo corte e/o raramente cambiate, l'uso della stessa password per accedere a diversi sistemi informatici, il lasciare per gli identificativi d'utente degli amministratori di sistema quelli di default, e così via

Inoltre, la fig. 6.6-1 mostra quanto siano relativamente bassi gli attacchi ripetuti nell'anno per più di 10 volte, anche se la tendenza per il 2020 appare in crescita. L'IAA è di fatto considerato dagli attaccanti come uno dei primi sistemi di protezione da abbattere per poter effettuare successivamente le azioni illegali poste come target: ma se l'IAA è ben protetto, l'attaccante preferisce tentare su altri sistemi ICT, e non continuare a provare sul medesimo sistema.

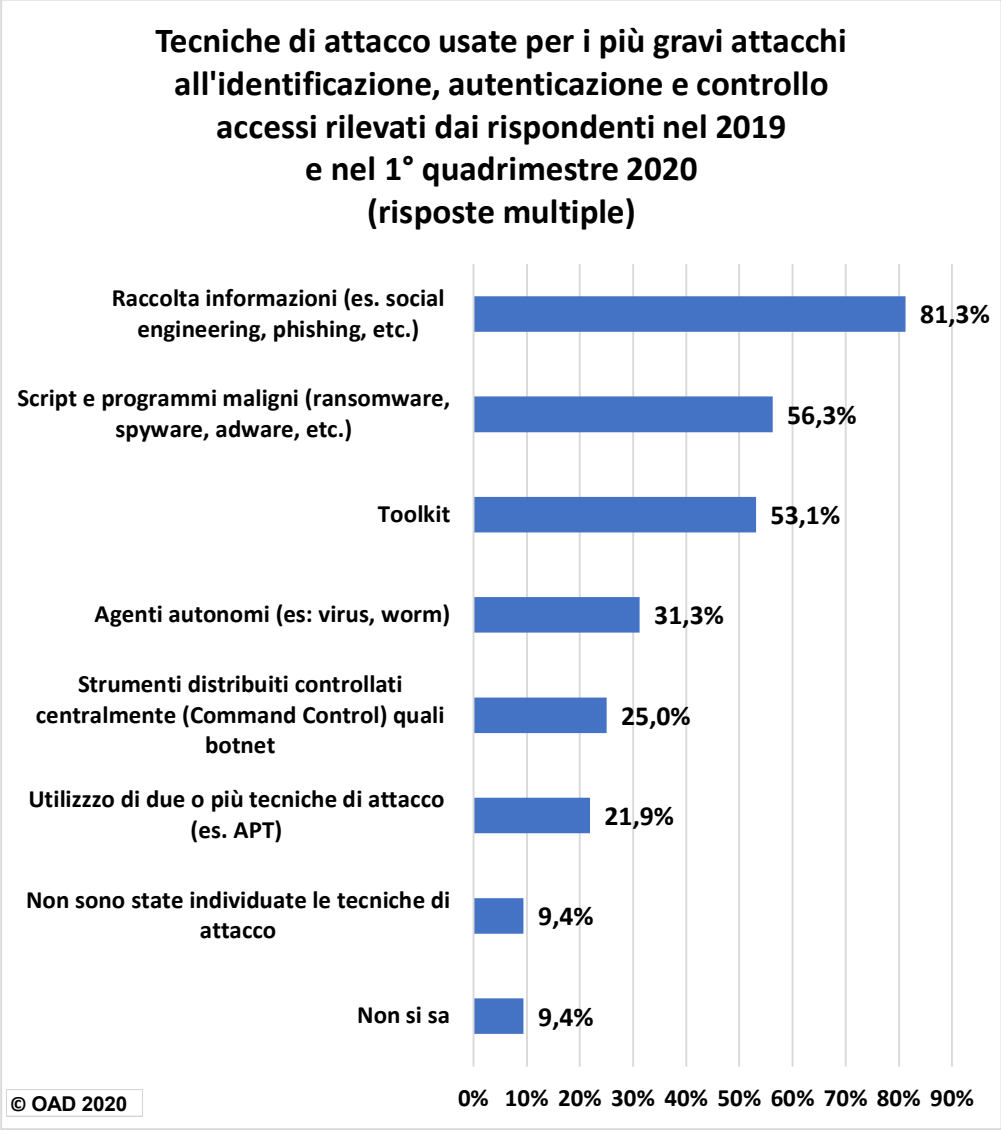


Fig. 6.6-2

La fig. 6.6-2, con risposte multiple, mostra come la tecnica di attacco più diffusa tra i rispondenti sia la raccolta di informazioni, con phishing ed altre tecniche di social engineering per più dell'80 % dei rispondenti, cui segue l'uso di script e di codici maligni, con un 56,3%, e l'uso di toolkit con 31,3%. Seguono Command Control e tecniche multiple, sofisticate e persistenti come APT, con percentuali che si attestano tra il 21,9% e il 25%. Alto, ma comprensibile, il quasi 20% di rispondenti che

ignorano, o che non sono stati in grado di individuare o di ipotizzare le tecniche usate nell'attacco IAA rilevato.
La fig. 6.6-3, con risposte multiple, mostra che nella maggior parte dei casi gli impatti riscontrati sono stati irrilevanti o comunque risolti in breve tempo ed a costi limitati. A questa segue la parziale interruzione di servizi ICT erogati, per il 37,5%. Tutti gli altri impatti sono gravi, ma pur con percentuali inferiori ai due precedenti, nel complesso sono assai significativi: ¼ dei rispondenti ha rilevato gravi disservizi, con costi elevati per il ripristino, anche se nessuno dichiara di aver perso affari e clienti a seguito di attacchi all'IAA.

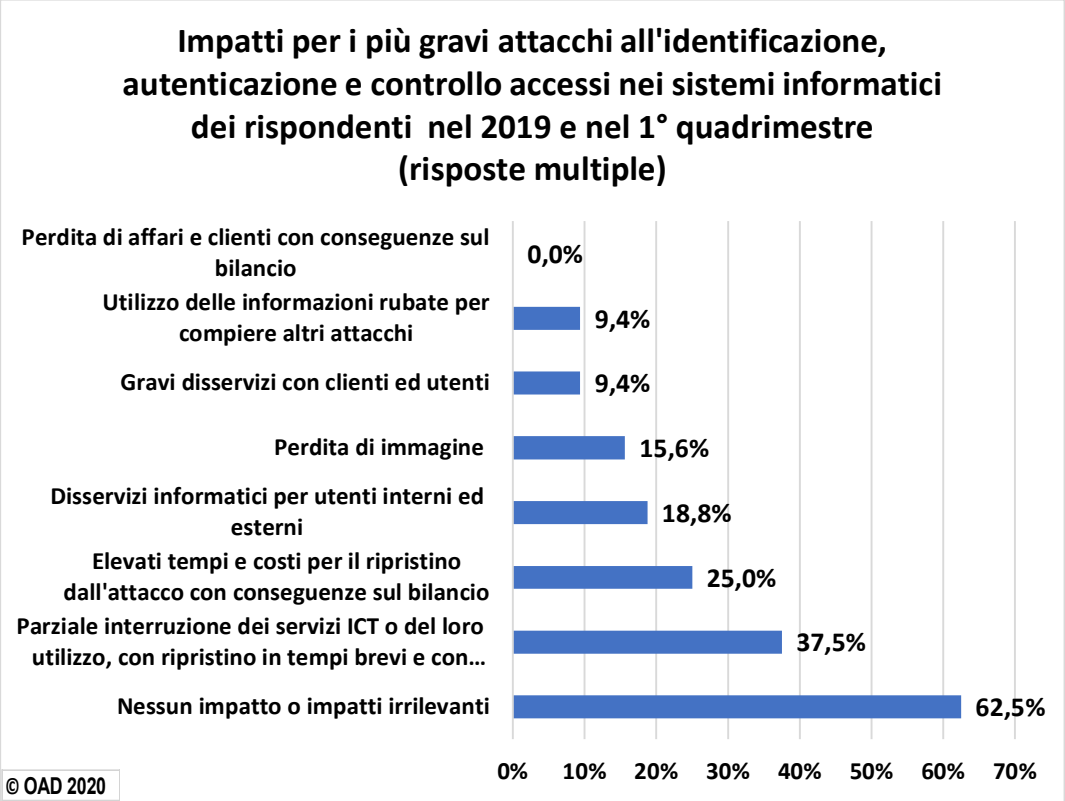


Fig. 6.6-3

Le principali possibili motivazioni indicate dai rispondenti che hanno subito questa tipologia d'attacco, con risposte multiple, sono mostrate in fig. 6.6-4, che evidenzia al primo posto la frode, seguita dalla ritorsione/ricatto con un alto 59,4% e dal sabotaggio, con un altrettanto alto 37,5%. Questo significa che ben più di 1/3 dei rispondenti ha prove o ragionevolmente stima che l'attacco ai sistemi di IAA, cui probabilmente segue un ulteriore attacco digitale ancor più in profondità (31,3%), sia dovuto a tentativi di sabotaggio: un dato veramente preoccupante.
I dati della fig. 6.6-5 sui tempi di ripristino nel caso peggiore rilevato confermano quanto emerge dalla fig. 6.6-3 sugli impatti riscontrati a seguito dell'attacco. Il 90% dei rispondenti indica che la ripartenza è avvenuta in meno di 3 giorni, ma "solo" il 38,5% in un solo giorno. Ed il 7,7% indica che ha ripristinato in 4-7 giorni, mentre nessun attacco ha richiesto più di un mese. Si conferma quindi quanto emerso dal confronto tra impatti e tempi di ripristino, nei casi peggiori occorsi: molti attacchi a IAA sono stati senza o con scarsi impatti, e quindi risolvibili in brevissimo tempo, ma tanti altri attacchi, con impatti più gravi, hanno richiesto tempi più lunghi - ma non oltre il mese - per ripristinare i sistemi attaccati.

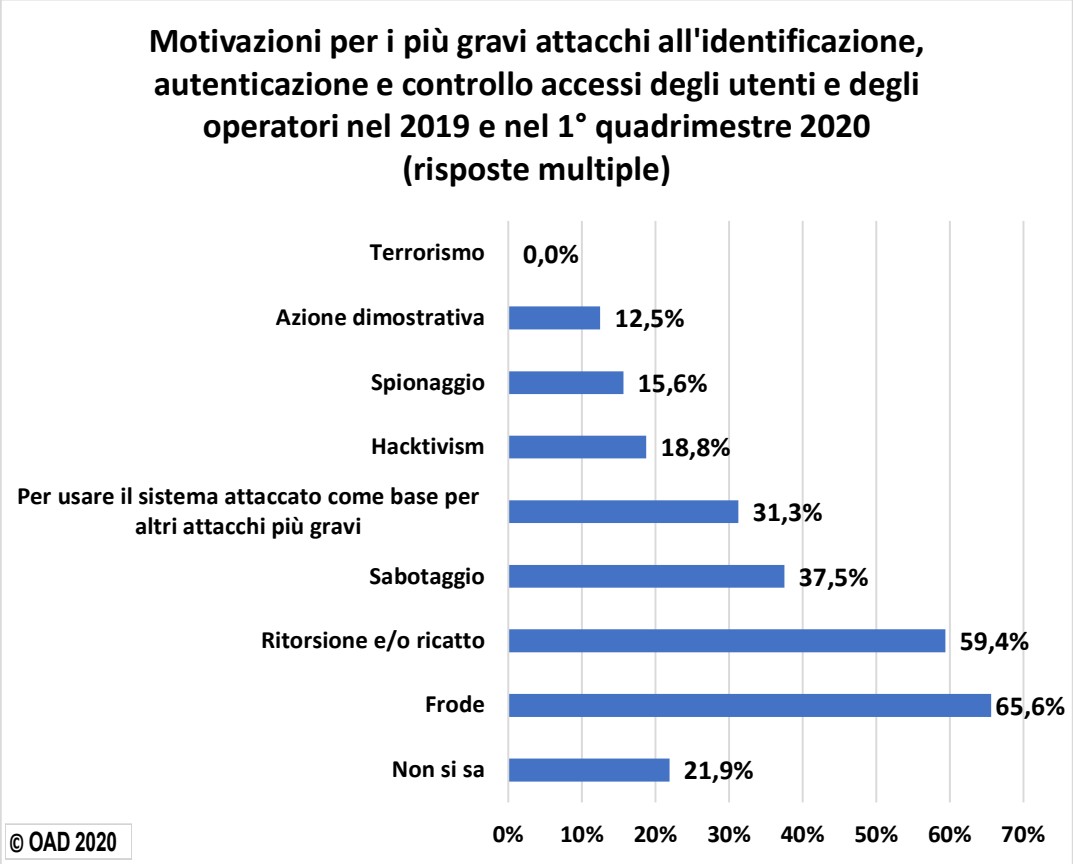


Fig. 6.6-4

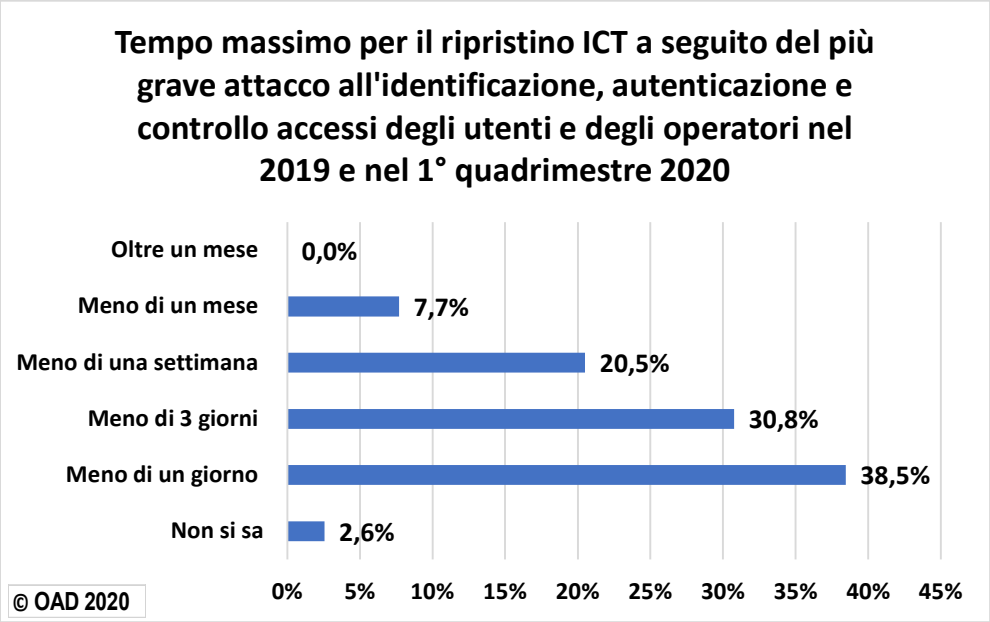


Fig. 6.6-5

6.7 *Attacchi alle reti, locali e geografiche, fisse e wireless, e ai DNS*

In questa tipologia, gli attacchi si differenziano significativamente, sia come obiettivo che come modalità d'attacco, in funzione del tipo di rete e dei protocolli usati: reti geografiche e reti locali, reti fisse e senza fili (wireless). Queste ultime, sia locali (WLAN, WiFi) che geografiche per la telefonia mobile[11], sono quelle che consentono la mobilità sia del lavoro che degli usi personali/domestici e di intrattenimento. Sono quelle più cresciute negli ultimi anni, e che hanno portato a nuovi tipi di vulnerabilità, rischi e possibili attacchi. Data la complessità tecnica del moderno mondo delle telecomunicazioni e delle reti, volutamente il questionario 2020 OAD ha raggruppato in un'unica tipologia l'ampia e diversificata famiglia dei possibili attacchi alle reti, che costituiscono uno dei punti di ingresso al sistema informatico sia per specifici attacchi alle reti, sia, soprattutto, per ulteriori e più mirati attacchi digitali ai sistemi ICT connessi a tali reti, e tramite questi alle loro applicazioni ed informazioni. Tali attacchi includono modifiche al routing per l'instradamento del traffico, le modifiche ai DNS che cambiano il nome della risorsa ICT associata all'indirizzo IP, l'attacco al DHCP, lo sniffing del traffico, la saturazione della rete con un attacco DoS/DDoS per rendere non più agibili le applicazioni, tipicamente web, disponibili su Internet (si veda §6.11), e così via.
Come hanno rilevato diversi rapporti internazionali, negli ultimi anni gli attacchi ai DNS, Domain Name System, sono aumentati significativamente e si sono differenziati non solo per reindirizzare il traffico destinato ai server - ad esempio dirottandolo su un server dell'attaccante - ma anche per sferrare attacchi DoS/DDoS.

La fig. 6.7-1 mostra che le percentuali dei rispondenti che hanno rilevato attacchi alle reti dei loro sistemi informatici nel 2019, 17,5%, e nel 1° quadrimestre 2020, 15,2%. Pur con queste percentuali relativamente basse[12], questa tipologia d'attacco si posiziona nella presente edizione al terzo posto come diffusione (si veda fig. 6-7). Il motivo della relativa riduzione di diffusione degli attacchi alle reti e dovuto dal fatto che quasi tutte le reti geografiche, fisse e mobili, sono gestite da fornitori specializzati che, offrendole sul mercato, devono assicurare adeguate misure di sicurezza digitali; proprio per questo risulta più difficile effettuare attacchi digitali che vadano a buon fine, per cui occorrono tecniche sofisticate come indicato nella successiva fig. 6.7-2.

[11] La telefonia mobile include due settori, quello della telefonia cellulare e quello della telefonia satellitare. La telefonia cellulare, la più diffusa ed estesa a livello mondiale, ha visto il susseguirsi nel tempo di diverse tecnologie e protocolli di rete, che vengono individuate come generazioni (G) e sotto generazioni: il G0 analogico di metà anni '80; il G1 ancora analogico basato su standard TACS, Total Access Communication System, e ETACS, Extended TACS; il G2 basato su standard GSM, Global System for Mobile communications; il G2.5 basato su standard GPRS, General Packet Radio Service; il G2.75 basuto su standard EDGE, Enhanced Data rates for GSM Evolution; il G3 basato su standard UMTS, Universal Mobile Telephone System il G3.5 basato su standard HSDPA, High Speed Downlink Packet Access, e HSPA; G4 basato su standard VSF-Spread OFDM, Variable-Spreading-Factor Spread Orthogonal Frequency Division Multiplexing e su LTE, Long Term Evolution; il G5, già in corso di installazione ed erogazione, anche se limitata, in Italia. Attualmente in Italia le reti cellulari supportano dal G2 in avanti, e prevalentemente sono G3-G4. La telefonia satellitare si basa sulle reti satellitari ed ha un uso assai ridotto visti i suoi costi, le dimensioni dei telefoni satellitari e l'impossibilità del loro utilizzo in luoghi chiusi. Tramite reti satellitari, che includono ad esempio Iridium, Globalstar, Teledesic, Hot Bird, alcune società offrono servizi di telefonia satellitare.

[12] se si fa riferimento a precedenti indagini OAD, come quella del 2018 con un 34,7% e quella del 2016, in cui gli attacchi alle reti risultavano al primo posto tra tutti gli attacchi rilevati dai rispondenti di allora. Si rammenta sempre che le cifre emerse dai rapporti OAD di anni diversi non possono essere statisticamente confrontate, ma posso solo fornire delle indicazioni di trend dei fenomeni cui fanno riferimento.

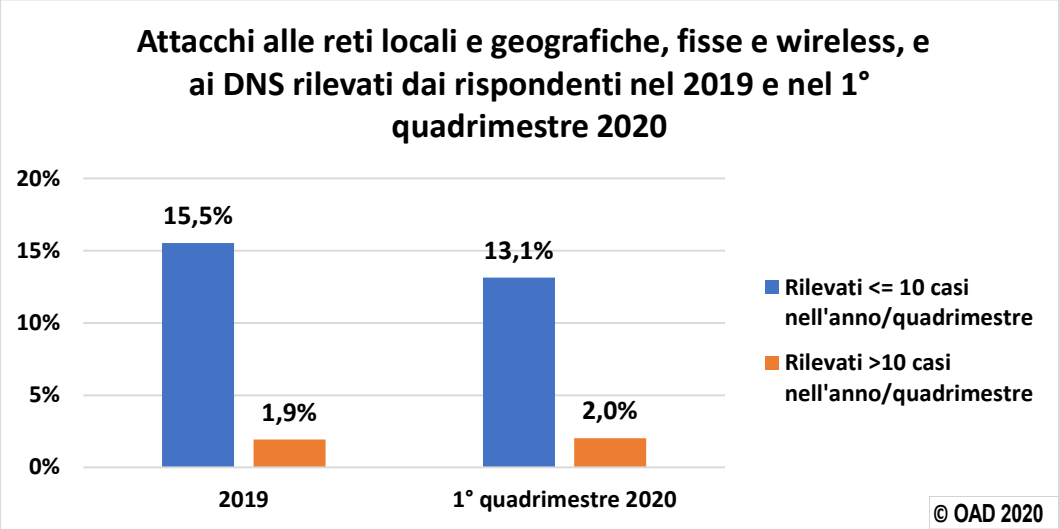


Fig. 6.7-1

La fig. 6.7-2 evidenzia, con risposte multiple, che la tecnica di attacco più usata per questa tipologia di attacco è stata l'uso di malware e script, con un 70,6%, seguita dalla raccolta di informazioni con un 64,7% e dall'uso di toolkit con un 52,9%. Altre tecniche seguono, ma con percentuali decisamente minori.
La fig. 6.7-3 mostra, con risposte multiple, gli impatti causati alle Aziende/Enti dei rispondenti dai più gravi attacchi alle reti rilevati nel periodo considerato. Gli impatti causati sono stati abbastanza seri: al primo posto, per quasi la metà dei rispondenti, il 47,1%, disservizi per utenti interni ed esterni, ed al secondo posto la perdita di immagine per il 35,3%, più di 1/3. La stessa percentuale per la parziale interruzione dei servizi ICT, con ripristino in tempi brevi e con costi limitati. Ma ben il 29,4% lamenta elevati tempi e costi per il ripristino dall'attacco con conseguenze sul bilancio. Nessuno dei rispondenti che ha subito attacchi alle reti ha avuto per questa causa una perdita di affari e di clienti, e solo il 5,9% ha subito gravi disservizi con clienti ed utenti. Un 29,4% indica che gli impatti sono stati irrilevanti. È importante ricordare che il questionario OAD da sempre lascia alla sensibilità, competenza e conoscenza del rispondente la valutazione qualitativa della gravità dell'impatto.

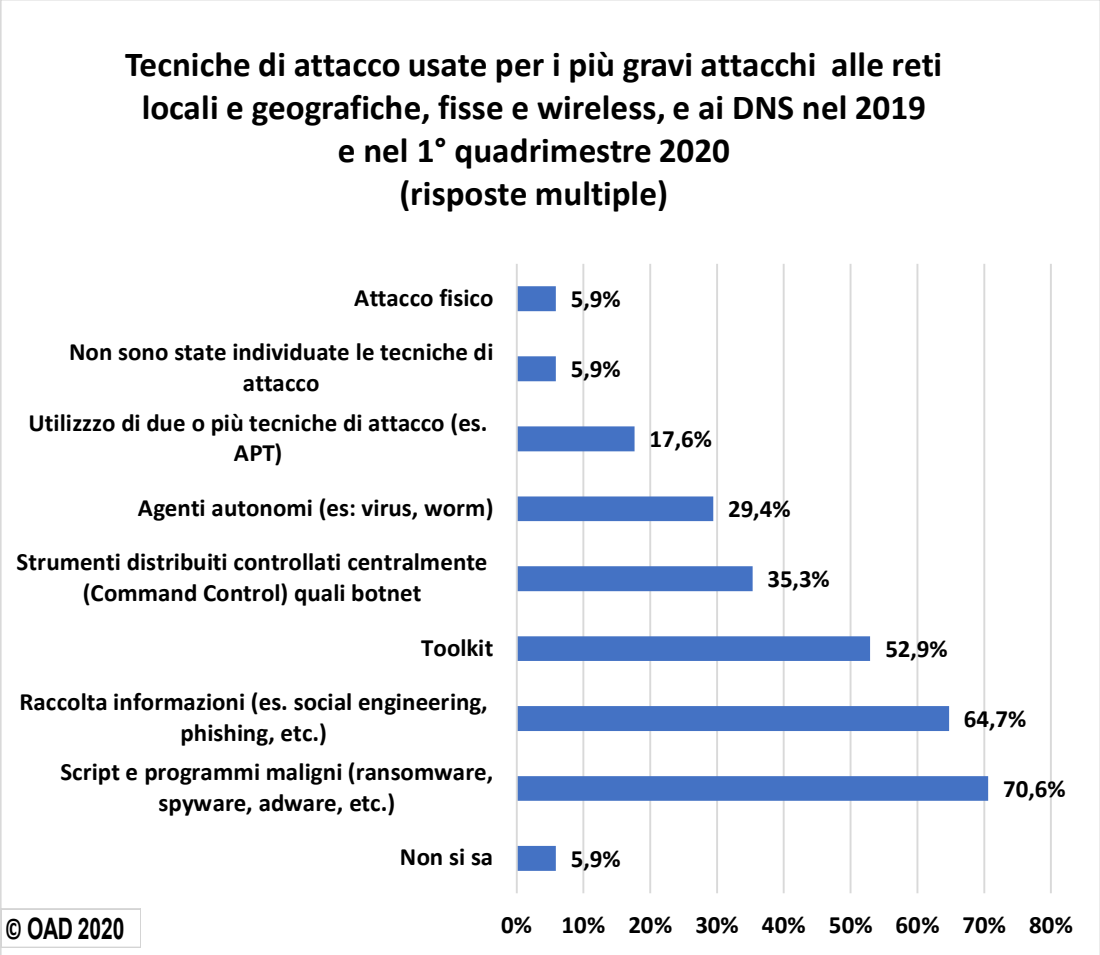


Fig. 6.7-2

La fig. 6.7-4 mostra, con risposte multiple, le possibili motivazioni, individuate o stimate dai rispondenti, per i più gravi attacchi alle reti dei loro sistemi informatici: la frode risulta percentualmente in testa a tutte le altre, praticamente per più della metà di chi ha subito questo tipo di attacco. Seguono a scalare le altre motivazioni previste nel questionario, che per quelle nella fascia del 40-50% si discostano tra loro di circa 5-6 punti. E queste sono tutte motivazioni per attacchi dagli effetti preoccupanti.
A conferma di quanto evidenziato all'inizio del presente paragrafo che sovente l'attacco alle reti, analogamente a quello all'IAA, sono propedeutici e punti di ingresso per ulteriori, spesso più gravi attacchi alle applicazioni e ai loro dati, al secondo posto si trova proprio questa motivazione, con un 47,1% di rilievo, ma ragionevole e confermata dai fatti: quasi il 50% degli attacchi più gravi aveva anche questa motivazione.
L'hacktivism ha una percentuale bassa ma non insignificante, indicata da rispondenti di grandi organizzazioni (si ricorda che il questionario è rigorosamente anonimo, ma nell'elaborazione dei dati si possono correlare le risposte inserite nel questionario con il tipo di Aziende/Ente e le sue caratteristiche, quali dimensioni, fatturato, etc.). Si veda in merito anche §10.2 e §10.3.

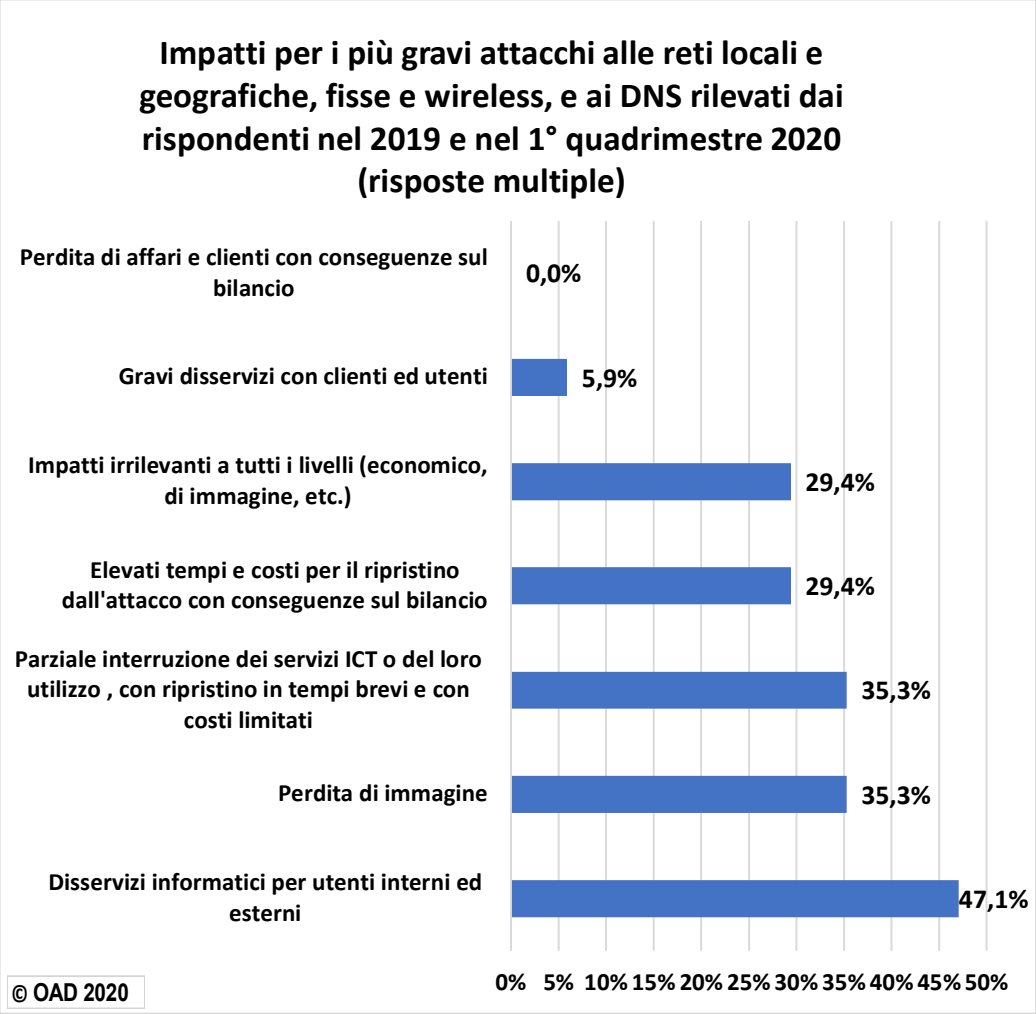


Fig. 6.7-3

Nessuno ha individuato o stimato motivazioni di terrorismo cibernetico. Con "Altro" alcuni rispondenti hanno precisato che l'attacco alle loro reti faceva parte di un attacco su larga scala che aveva come target vari sistemi informatici di diverse organizzazioni, o che era inserito in "attacchi automatici" non meglio specificati.

La fig. 6.7-5 mostra i tempi di ripristino che sono stati necessari a seguito dei più gravi attacchi alle reti nel periodo 2019 – 1° quadrimestre 2020. I dati emersi confermano la gravità e la criticità degli attacchi portati. Anche se in nessun caso il tempo massimo di ripristino della rete, geografica o locale, fissa o mobile, abbia richiesto più di un mese, il 31,6% dei rispondenti coinvolti indica che il ripristino ha richiesto tra 4 e 7 giorni, e il 15,8% addirittura tra gli 8 ed i 30 giorni. Tempi veramente troppo elevati per un servizio fondamentale come quello delle reti per garantire la connettività ed i collegamenti, e che normalmente non potrebbe attendere più di qualche ora.

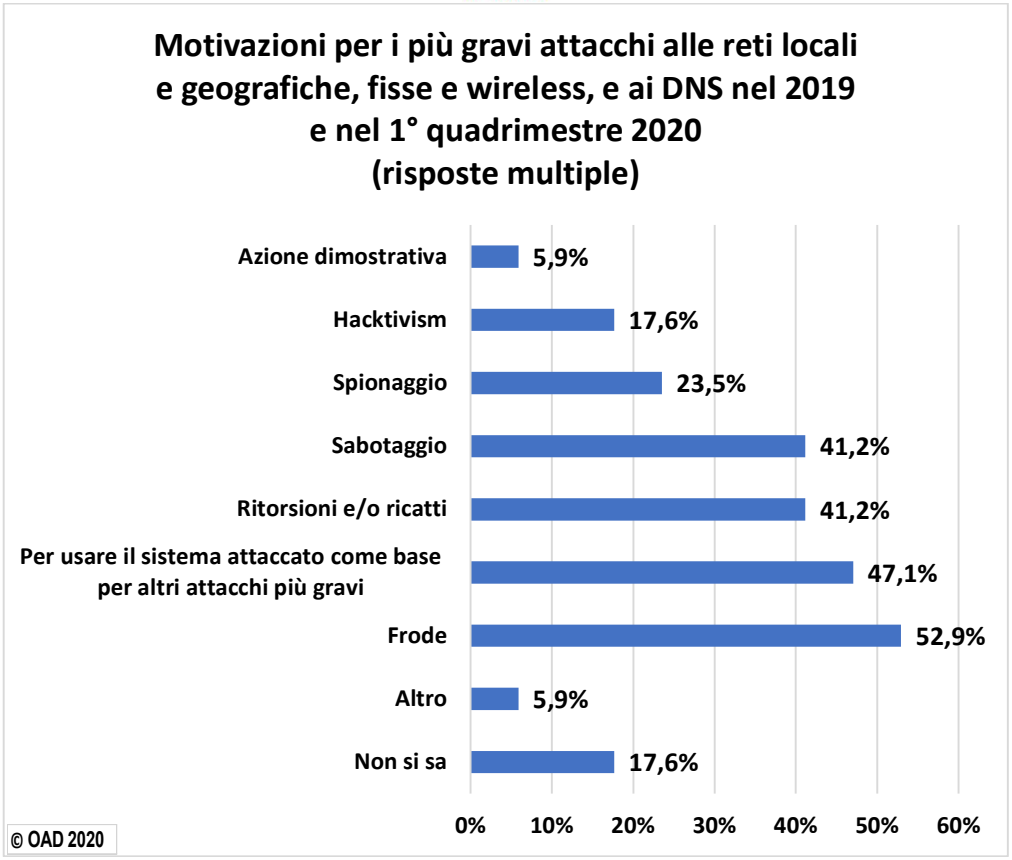


Fig. 6.7-4

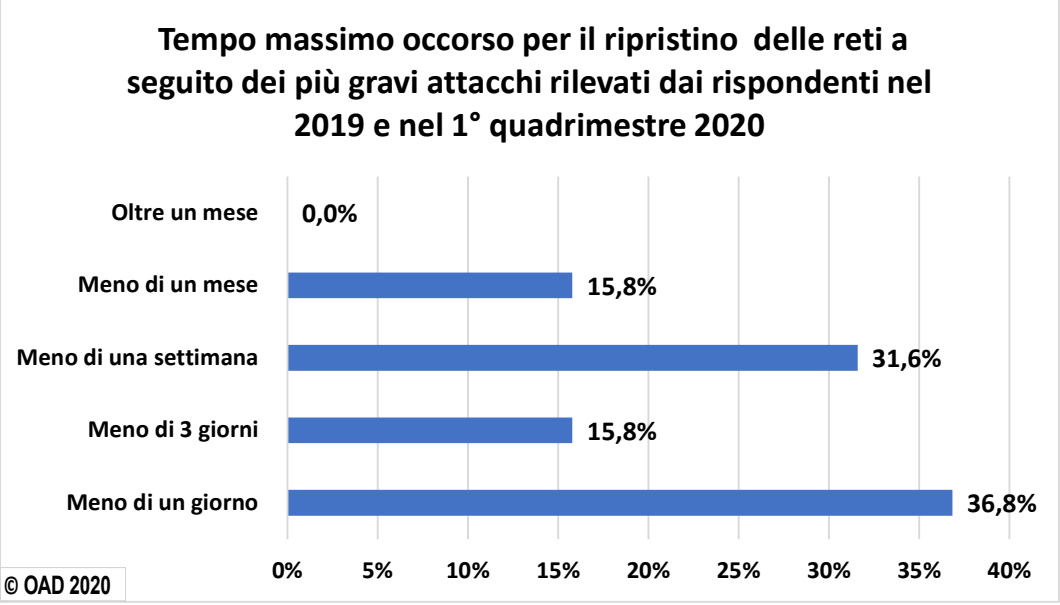


Fig. 6.7-5

6.8 *Uso non autorizzato sistemi ICT nel loro complesso*

L'uso non autorizzato di risorse ICT nel loro complesso, dai PC ai dispositivi mobili d'utente, dalle unità di rete ai server, fisici e virtuali, gestite internamente (on premise) e/o terziarizzate (hosting, housing, cloud), nel 2019 si è posizionato al quarto posto (23,3%) come diffusione tra i rispondenti che hanno subito attacchi, ma nel 1° quadrimestre 2020 è balzato per diffusione al secondo posto (27,3%), con meno di 1 punto percentuale dal primo in classifica, la tipologia di attacchi su IAA, e a 4 punti percentuali rispetto all'anno precedente, il 2019, come già evidenziato nella fig. 6-7.
Questa tipologia d'attacco all'intero sistema ICT, fisico o virtuale, è il più delle volte alla base di attacchi ai sistemi operativi e al software di base, agli applicativi, alle informazioni da loro trattate, ai sistemi di storage. L'incremento percentuale tra 2019 e 2020 è dovuto anche all'esplosione di attacchi digitali nel corso della pandemia Covid-19, così come discusso in §6.
La fig. 6.8-1 dettaglia che in entrambi i periodi questa tipologia d'attacco tra i rispondenti ha avuto pochissime ripetizioni, e quasi sempre è stata oggetto di un singolo o di pochi attacchi nel periodo considerati.

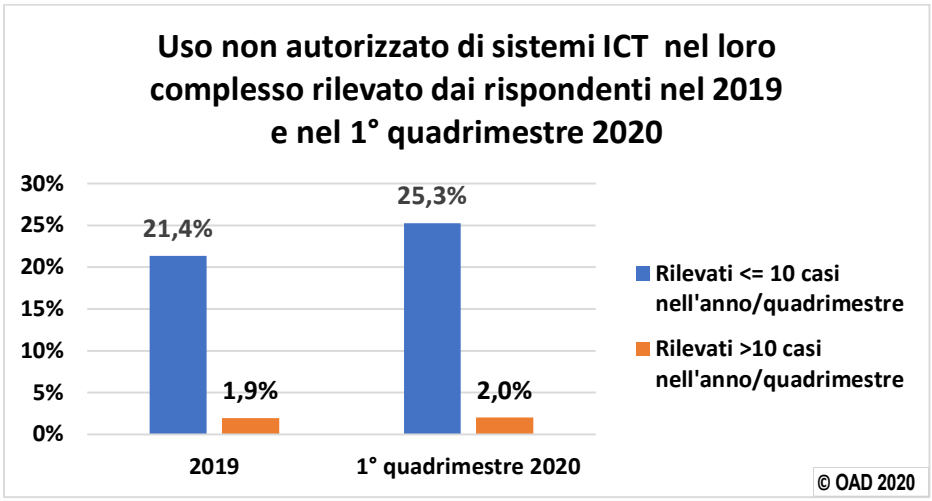


Fig. 6.8-1

La fig. 6.8-2, con risposte multiple, elenca le tecniche di attacco usate negli attacchi di questo tipo portati ai sistemi informatici dei rispondenti. La famiglia di tecniche più diffuse, con un elevato 88,5% (rispetto al 53,7% del 2018) è risultata quella basata su script e malware, seguita dalla raccolta illecita di informazioni, con un 65,4% (rispetto al 48,8% del 2018), dall'uso di toolkit 34,6% e da agenti autonomi, quali i virus, con un 30,8%. Le altre famiglie di tecniche sono state usate, ma nella fascia di diffusione del 20%. Più del 15% dei rispondenti coinvolti in questo tipo di attacco non è riuscito ad individuare, o non conosce, le tecniche di attacco usate. Nel loro complesso, tutte queste informazioni confermano l'elevato livello tecnico, di competenze e di sofisticazione di questa tipologia di attacco nel periodo considerato
La fig. 6.8-3 evidenzia, con risposte multiple, che questa tipologia d'attacco ha causato in percentuale più danni che non danni o danni irrilevanti. Il 36,6% dei rispondenti lamenta come conseguenza la perdita di affari, cui si aggiunge la perdita d'immagine per il 24,4%, lunghi e costosi tempi di ripristino per il 22%, danni ai clienti per 4,9%. Non danni o danni irrilevanti per il 31,7%, e ripristini in brevi tempi e bassi costi per il 7,3%.

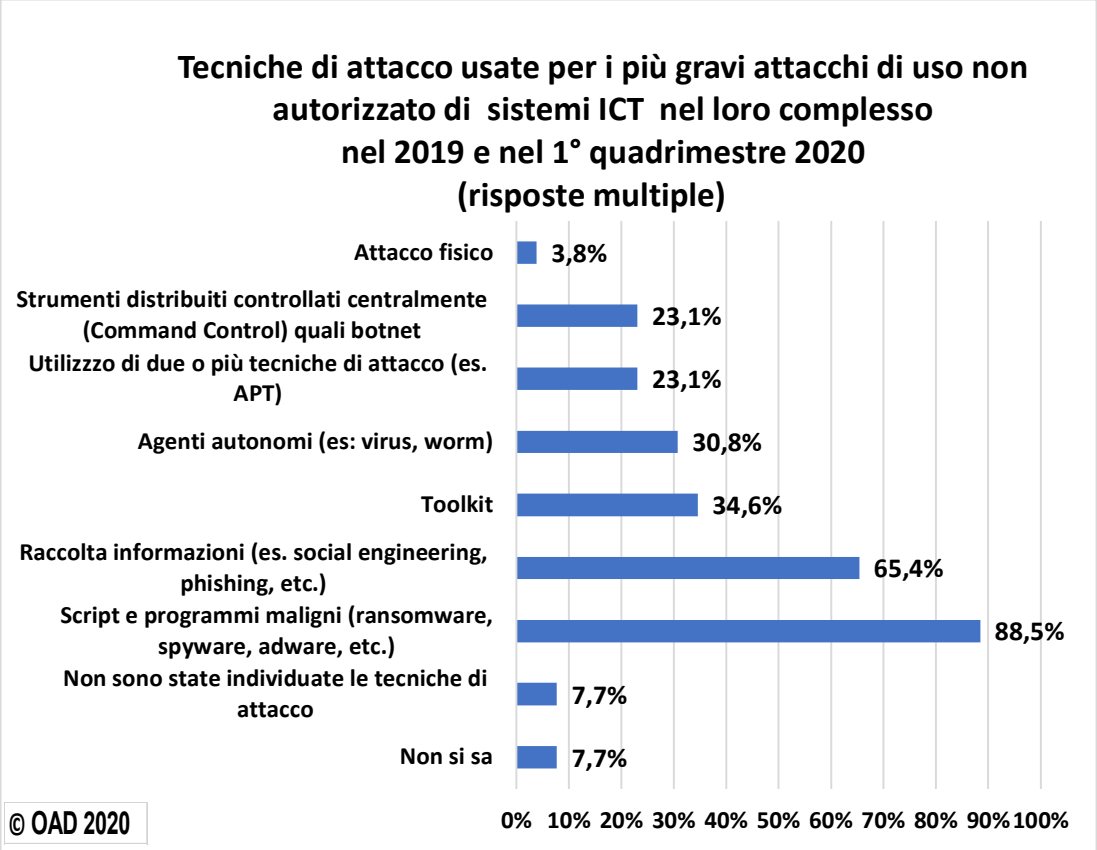


Fig. 6.8-2

La fig. 6.8-4, con risposte multiple, mostra le probabili motivazioni degli attaccanti fornite dai rispondenti coinvolti in questo tipo di attacco, che confermano la gravità della situazione creatasi nel periodo considerato. Ai primi tre posti, a scalare tra loro con molti punti percentuali, il "trittico" delle tipiche motivazioni "gravi" per l'Italia: ritorsioni con un 73,1%, strettamente correlato con l'ampia diffusione di malware, che include anche i ransomware, di cui alla fig. 6.8-2, il sabotaggio, con un 52,7%, e le frodi, con un 30,8%. Le altre motivazioni vanno fortemente a scalare in percentuale, ed i rispondenti coinvolti in questa tipologia di attacco non hanno individuato alcun attacco per terrorismo informatico.

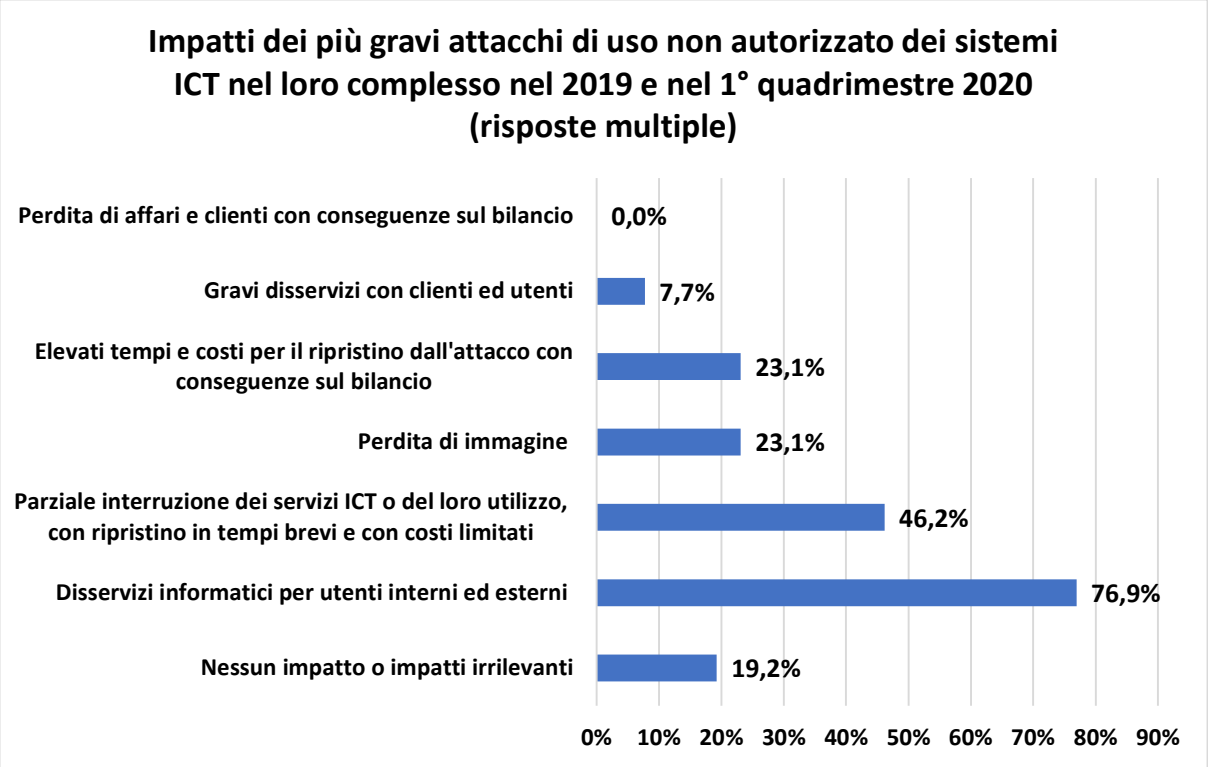


Fig. 6.8-3

La gravità per questo tipo di attacco da parte dei rispondenti è confermata dai tempi massimi di ripristino relativamente alti per il più grave di questi attacchi subiti. La fig. 6.8-5 mostra che quasi il 72% riesce a ripristinare la situazione *ex ante* entro una settimana, ma solo il 15,6% riesce entro il primo giorno. Un non trascurabile 28,1% necessita da 4 a 30 giorni, anche se nessuno ha indicato che è stato necessario più di un mese.

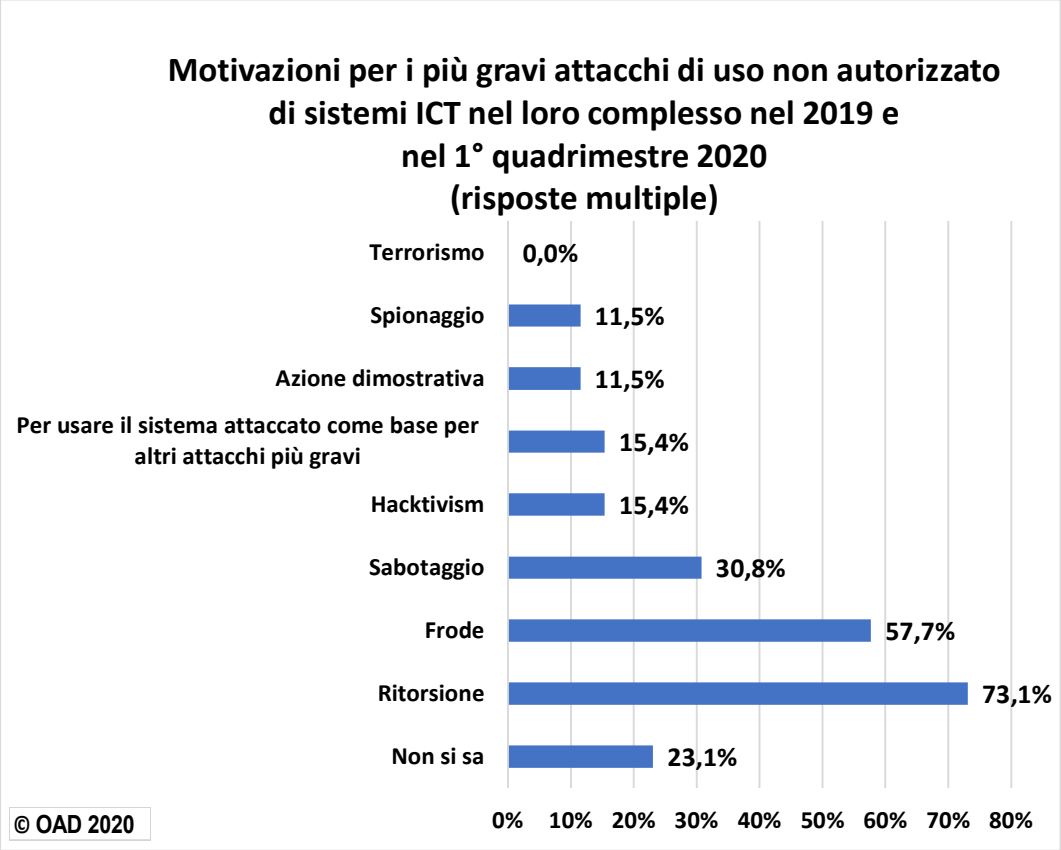


Fig. 6.8-4

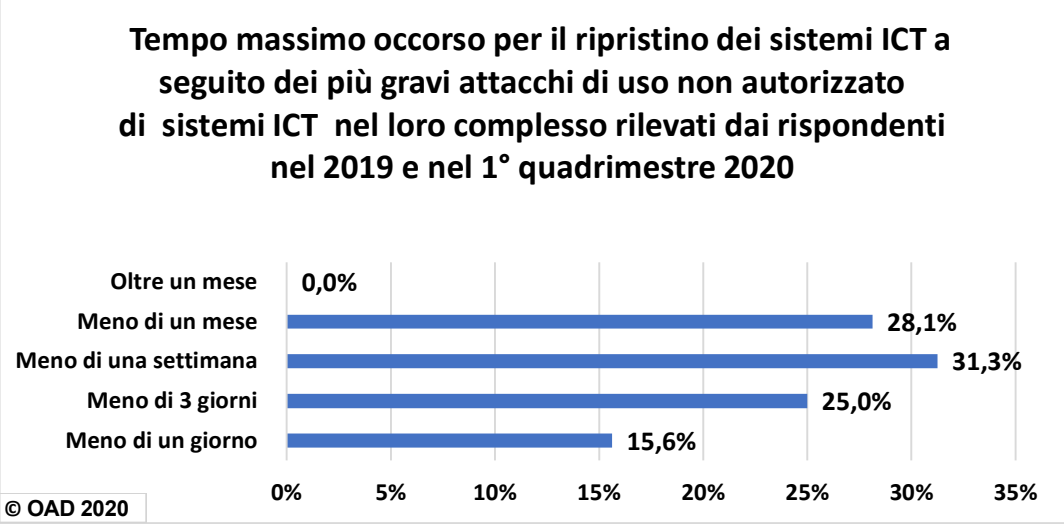


Fig. 6.8-5

6.9 *Modifiche non autorizzate ai programmi applicativi e alle loro configurazioni*

Questa tipologia di attacchi rientra nella fascia di quelli complessi e sofisticati, e andando a buon fine un attacco di questo tipo può causare seri danni al sistema informatico attaccato, anche perché non sempre di facile e diretta individuazione.
La diffusione di questo attacco tra i rispondenti che hanno subito attacchi nel 2019 e nel 1° quadrimestre 2020 non è pertanto molto alta, del 8,7% e del 8,1% rispettivamente, come mostrato nella fig. 6-7.
La fig. 6.9.1 evidenzia come questi attacchi non siano ripetuti frequentemente, data la loro complessità.

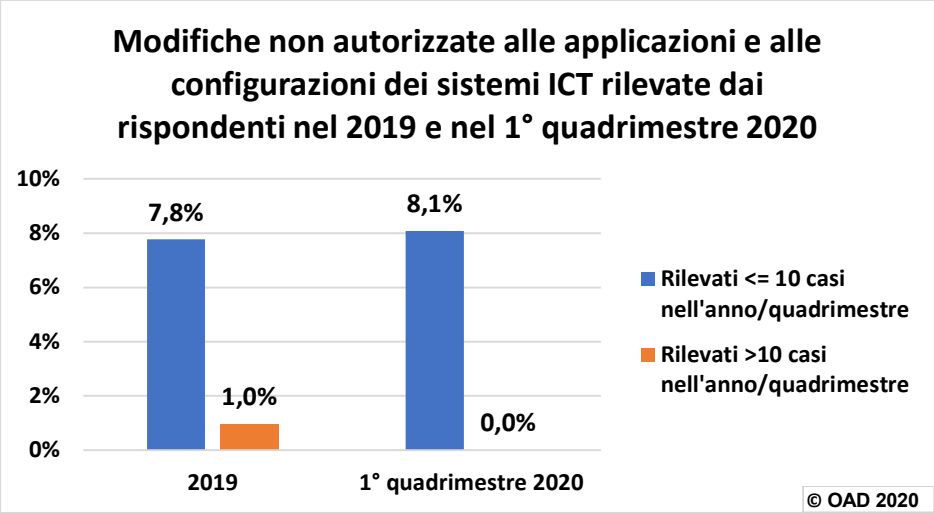


Fig. 6.9-1

La controprova della complessità tecnica di questo attacco è fornita dalla diffusione delle tecniche più usate per condurre questi attacchi, secondo i rispondenti che li hanno subiti, riportate nella fig. 6.9-2 con risposte multiple. Al primo posto, alla pari e con un elevato 77,8% (rispetto al 62,5% riscontrato nel 2018), malware e la raccolta illegittima di informazioni. Seguono, con più di 20 punti di differenza percentuale, l'uso di toolkit per individuare e sfruttare le vulnerabilità software e, sempre con un simile range di differenza, agenti autonomi come i virus e sistemi di controllo di agent da distanza. Per attacchi di questa sofisticazione non può mancare l'uso contemporaneo di più tecniche, che ha in questa indagine una percentuale di diffusione relativamente bassa, in confronto a quelle delle altre tipologie. Una ancor più piccola percentuale di rispondenti indica anche l'uso di attacchi fisici, effettuati con l'inserimento di chiavette USB e di hard disk removibili.

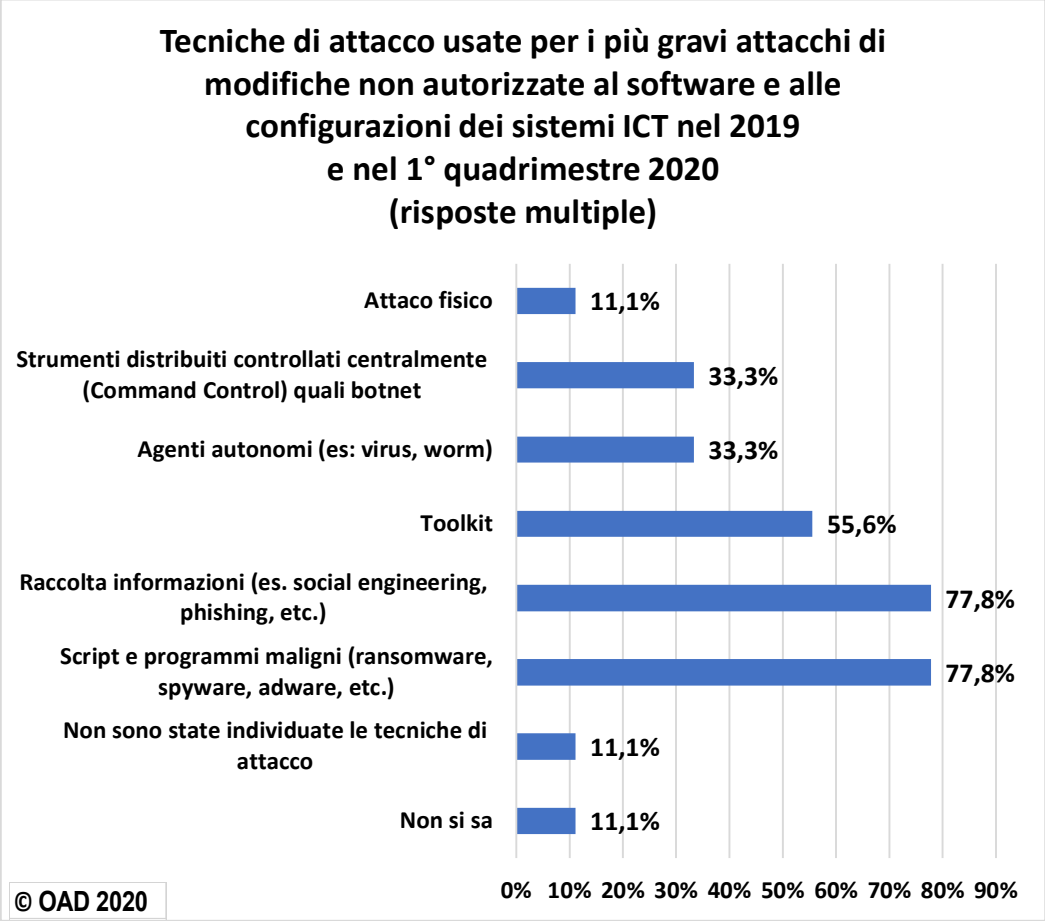


Fig. 6.9-2

La rischiosità di questa tipologia di attacchi è confermata dagli impatti avuti dai rispondenti che hanno subito tali tipi di attacchi. Come dettagliato con risposte multiple nella. fig. 6.9-3, più della metà dei rispondenti evidenzia la perdita di immagine e gravi disservizi per gli utenti del sistema informatico: nonostante ciò, non si sono avuti costi di rimborso per danni subiti dai clienti, o loro dismissioni e fughe alla concorrenza per questo motivo.
D'altro canto, un 1/3 dei rispondenti dichiara di non aver avuto impatti, ed il 44,4% di aver riscontrato disservizi risolvibili in breve tempo e a costi ridotti. Questi dati non sono contradditori, come potrebbe sembrare ad un loro semplice confronto. Ogni attacco, di qualsiasi tipologia, può causare più o meno danni, in funzione delle misure tecniche di sicurezza in essere, e soprattutto di quelle organizzative. Un ulteriore aspetto che può condizionare gli impatti è la cultura e l'abitudine dell'Azienda/Ente ad usare efficacemente gli strumenti informatici nelle sue attività e processi.
La fig. 6.9-4, con risposte multiple, mostra le probabili motivazioni degli attaccanti per gli attacchi di questo tipo rilevati dai rispondenti. Al primo posto troviamo la ritorsione/ricatto con un elevato 66,7%, chiaro indice della prevalenza di ransomware tra le tecniche usate, come evidenziato nella fig. 6.9-2. È bene evidenziare come questa congruenza delle risposte avute evidenzi la correttezza di coloro che hanno compilato il questionario, e quindi della consistenza e veridicità dei dati dell'indagine OAD.
Segue la frode, con più di 20 punti percentuali di distacco, e a scalare le altre motivazioni. Non trascurabile, ma comprensibile e ragionevole, che più di un quinto dei rispondenti (il 22,2%) non sia stato in grado di individuare delle motivazioni per gli attacchi di questo tipo subiti.

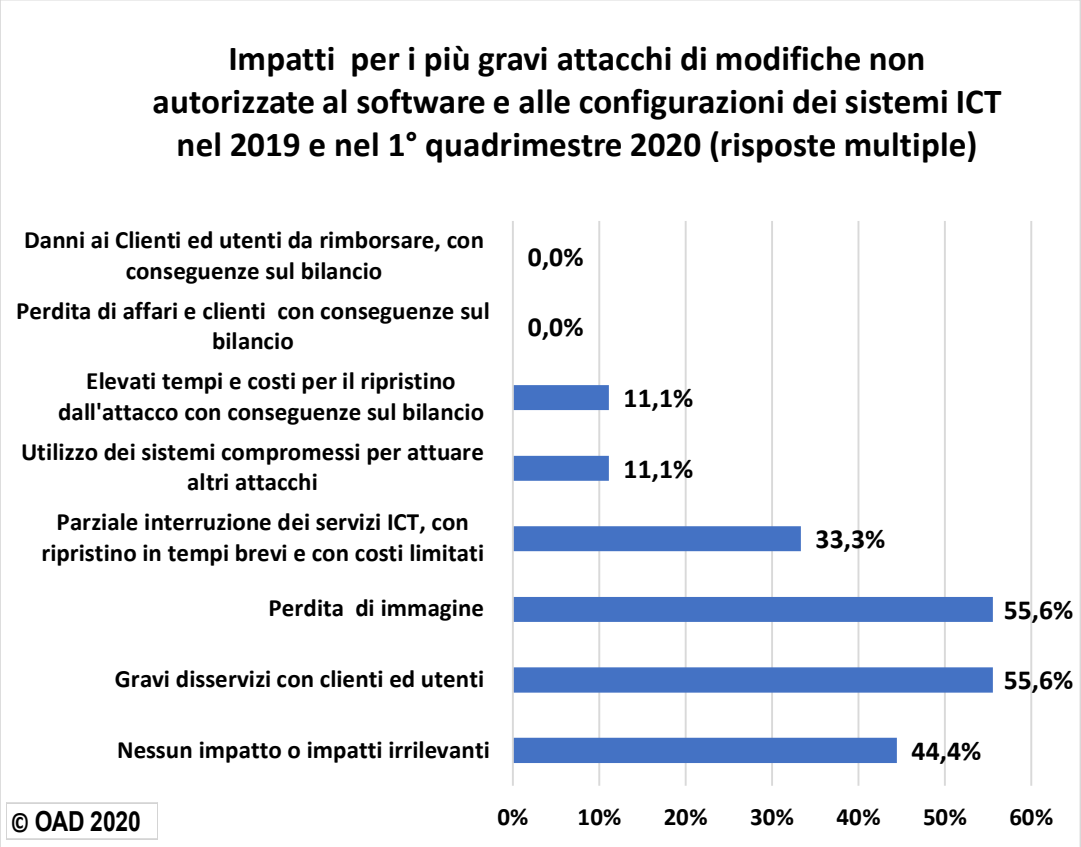


Fig. 6.9-3

La gravità di questo tipo di attacco, per i rispondenti che l'hanno subito, è confermata dai tempi massimi di ripristino nel caso peggiore di questo tipo d'attacco, come mostrato in fig. 6.9-5.
Circa il 91% dei rispondenti ha effettuato il ripristino entro una settimana, ma in giornata solo il 18,2%. Dato preoccupante è che per il 9,1% dei rispondenti il ripristino abbia richiesto un arco temporale davvero lungo, tra gli 8 ed i 30 giorni. Nessun caso ha richiesto più di un mese.

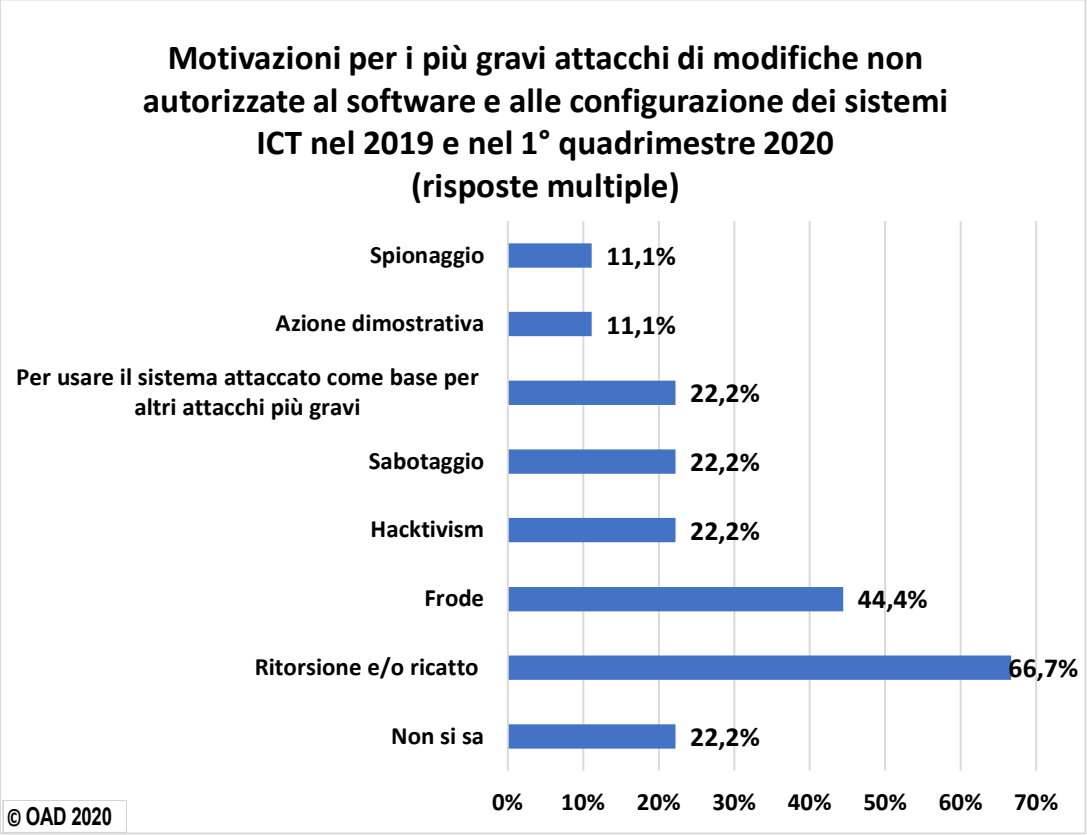


Fig. 6.9-4

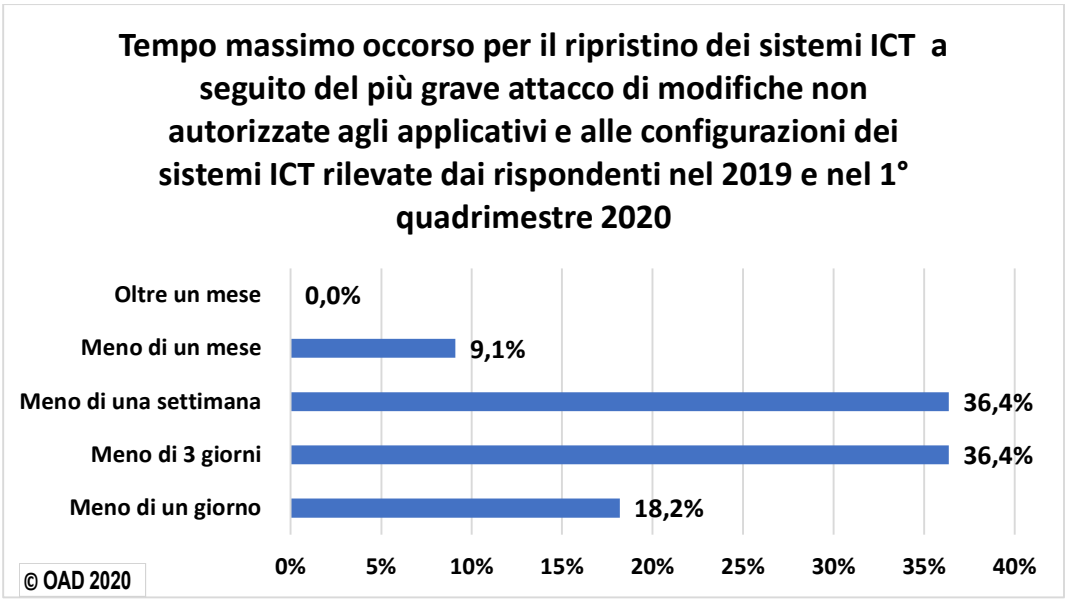


Fig. 6.9-5

9.10 Modifiche non autorizzate alle informazioni trattate dai sistemi ICT

Le modifiche non autorizzate alle informazioni trattate da un sistema informatico sono tra gli attacchi più subdoli e critici, in quanto minano l'integrità e la consistenza stessa dell'informazione, che è uno dei principali asset (beni) dell'azienda/ente, ed in molti casi è difficile individuare, soprattutto in breve tempo, una alterazione non autorizzata dei dati.
La diffusione di questa tipologia di attacco tra i rispondenti che li hanno subiti nel 2019 e nel 1° quadrimestre 2020 non è pertanto molto alta, del 8,8% e del 8,1% rispettivamente, come mostrato nella fig. 6-7.
La fig. 6.10-1 evidenzia come questi attacchi non siano quasi mai ripetuti frequentemente, data la loro complessità.

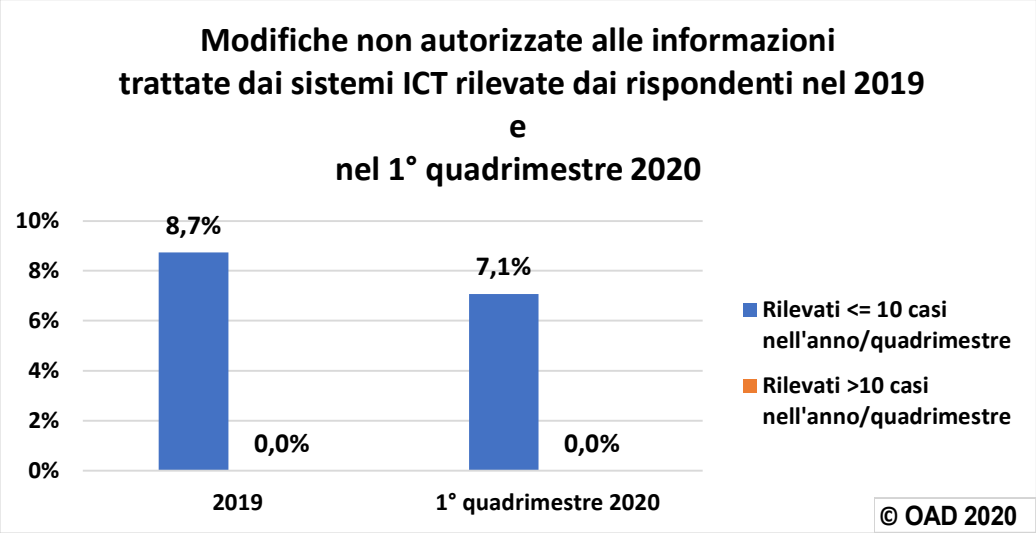


Fig. 6.10-1

In fig. 6.10-2 sono riportate, con risposte multiple, le tecniche più diffuse per effettuare tali attacchi, nei casi rilevati dai rispondenti. Per i 2/3 degli attacchi più critici, la tecnica più diffusa è la raccolta di informazioni, tipicamente il social engineering: per poter manipolare i dati in una banca dati o trattati da un'applicazione occorre disporre di molte informazioni sia tecniche sia funzionali. Un attaccante esterno deve pertanto poterne disporre, più facilmente grazie al coinvolgimento, volontario o non, di personale interno che disponga di tali informazioni: ed il social engineering può essere un'arma efficace per carpire tali informazioni, ben più velocemente che tramite approfondite analisi con strumenti tipo toolkit. Ed infatti quest'ultimo tipo di strumento d'attacco si posiziona subito dopo, con una elevate percentuale del 62,5%. Al terzo posto, con circa 12 punti percentuali di distacco dai toolkit, le tecniche basate su agenti autonomi, ad esempio i virus. Questa tipologia di attacco deve essere sofisticata per poter colpire, e sfrutta sovente più tecniche contemporaneamente, e talvolta in maniera persistente: di qui la ragione di un 37,5% rilevato dai rispondenti, che con una identica percentuale indicano anche l'uso di malware/script. All'ultimo posto, ma ancora con una non bassa percentuale, l'uso di tecniche di command control da remoto.

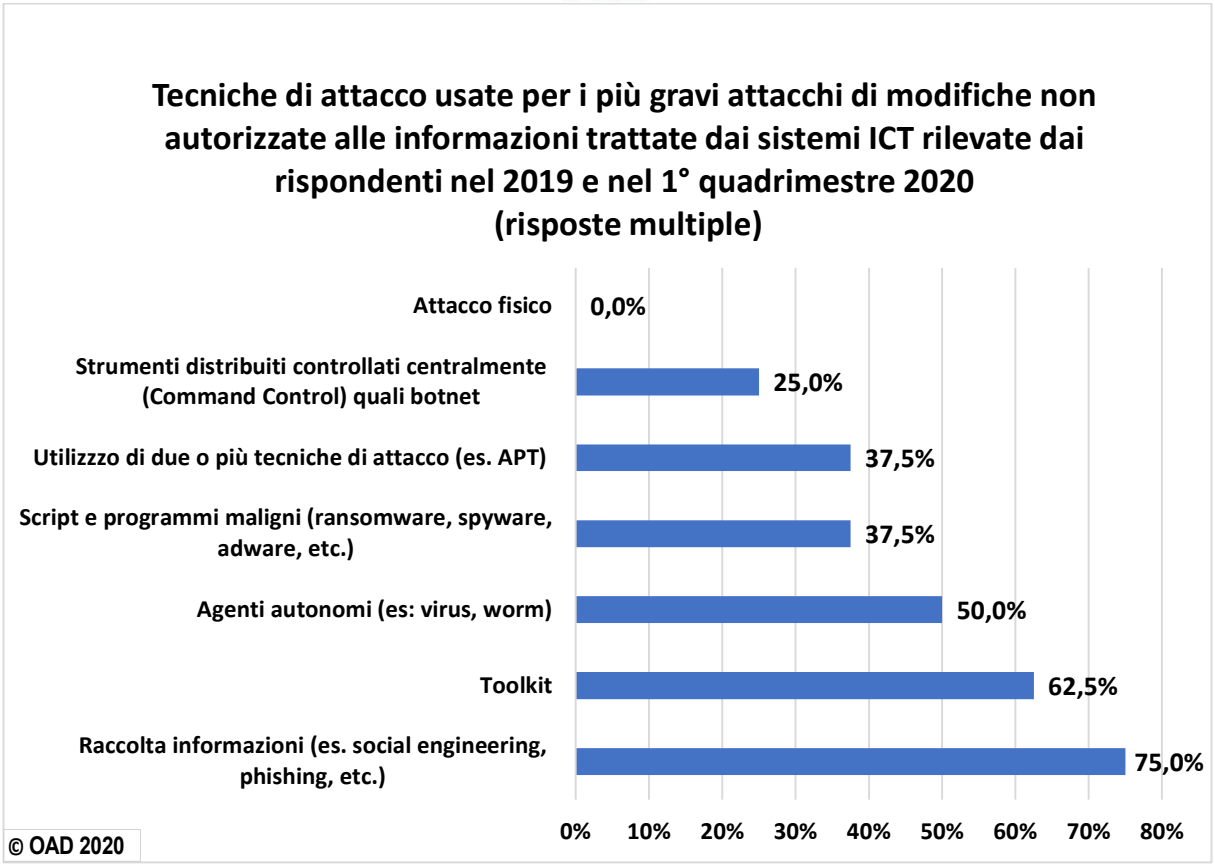


Fig. 6.10-2

La fig. 6.10-3, con risposte multiple, riporta gli impatti causati ai rispondenti dagli attacchi più gravi di questo tipo subiti. Emerge una situazione analoga a quella descritta per i precedenti attacchi: una parte dei rispondenti ha subito gravi impatti, un'altra impatti irrilevanti o risolti in tempi brevi e con costi limitati. Per quanto concerne la parte che ha subito gravi impatti: la metà dei rispondenti ha riscontrato gravi disservizi ed il 25% la perdita di immagine, e con uguale percentuale danni tali da richiedere costi elevati e lunghi tempi per il ripristino (si veda anche fig. 6.10-5); infine il 12,5% ha riscontrato gravi disservizi per clienti ed utenti. Nessuno ha dovuto rimborsare danni ai clienti e nessuno li ha persi o ha perso affari per questi attacchi. Per la parte con impatti poco gravi: il 37,5% non ha subito impatti o li ha subiti irrilevanti, mentre solo il 12,5% ha avuto parziali disservizi ma risolvibili in tempi brevi e con poco costo. Nessuno ha rilevato che l'attacco sia servito per portare ulteriori attacchi.

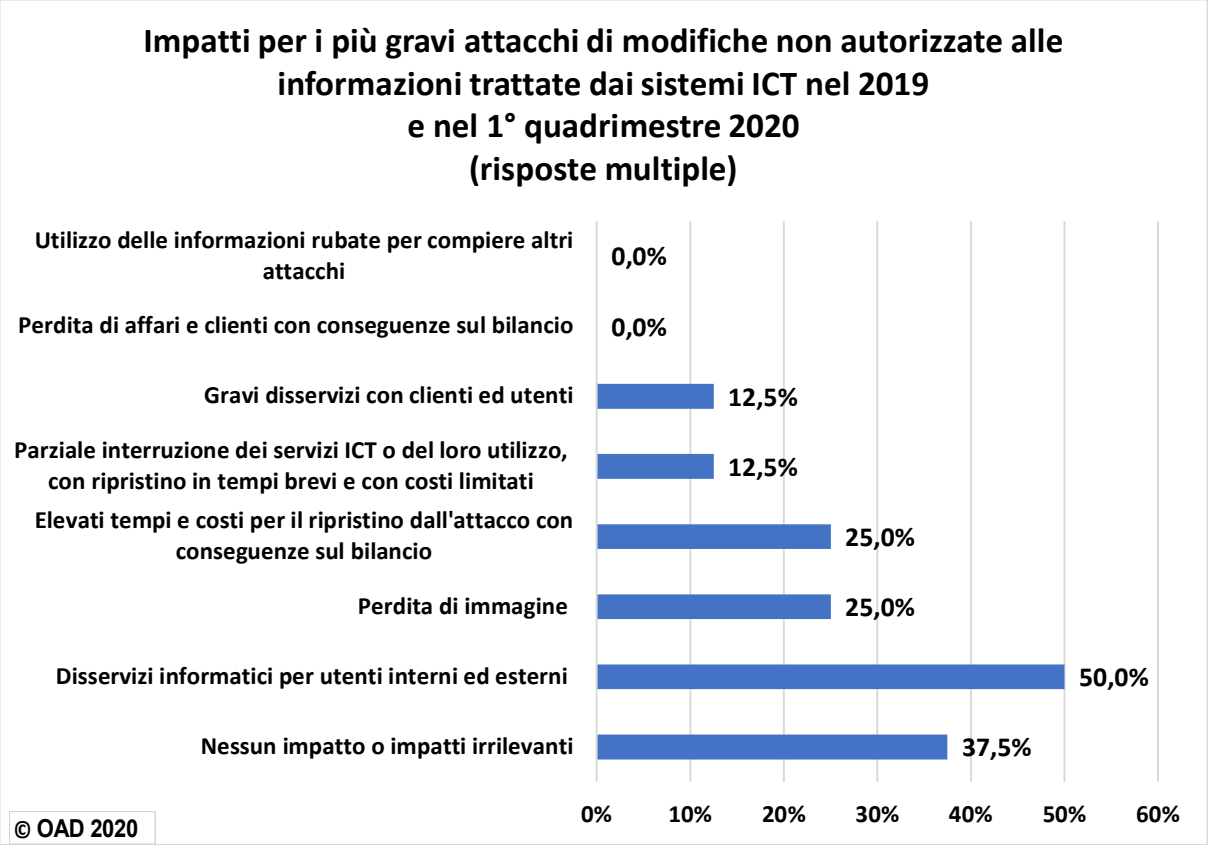


Fig. 6.10-3

La fig. 6.10-4, con risposte multiple, fornisce le possibili motivazioni per questi attacchi secondo i rispondenti che li hanno subiti. Al primo posto, come motivazione più diffusa, risulta la ritorsione/ricatto per i ¾ dei rispondenti coinvolti, cui segue il sabotaggio, con un elevato 62,5%: la modifica malevola di dati può portare realmente alla rovina una Azienda/Ente che l'ha subita, e costituisce di fatto un vero e proprio sabotaggio. Al terzo posto la frode per la metà dei rispondenti coinvolti.

I tempi di ripristino rappresentano un ulteriore indicatore della gravità dell'attacco. La fig. 6.10-5 mostra che il 75% dei rispondenti coinvolti in questo tipo d'attacco sono riusciti a ripristinare entro tre giorni, e di questi il 50% entro un solo giorno. Ma per un 12,5% il ripristino ha richiesto da 4 ad 7 giorni, e per una latro 12,5% addirittura da 8 a 30 giorni. Nessun caso ha richiesto interventi per più di un mese.

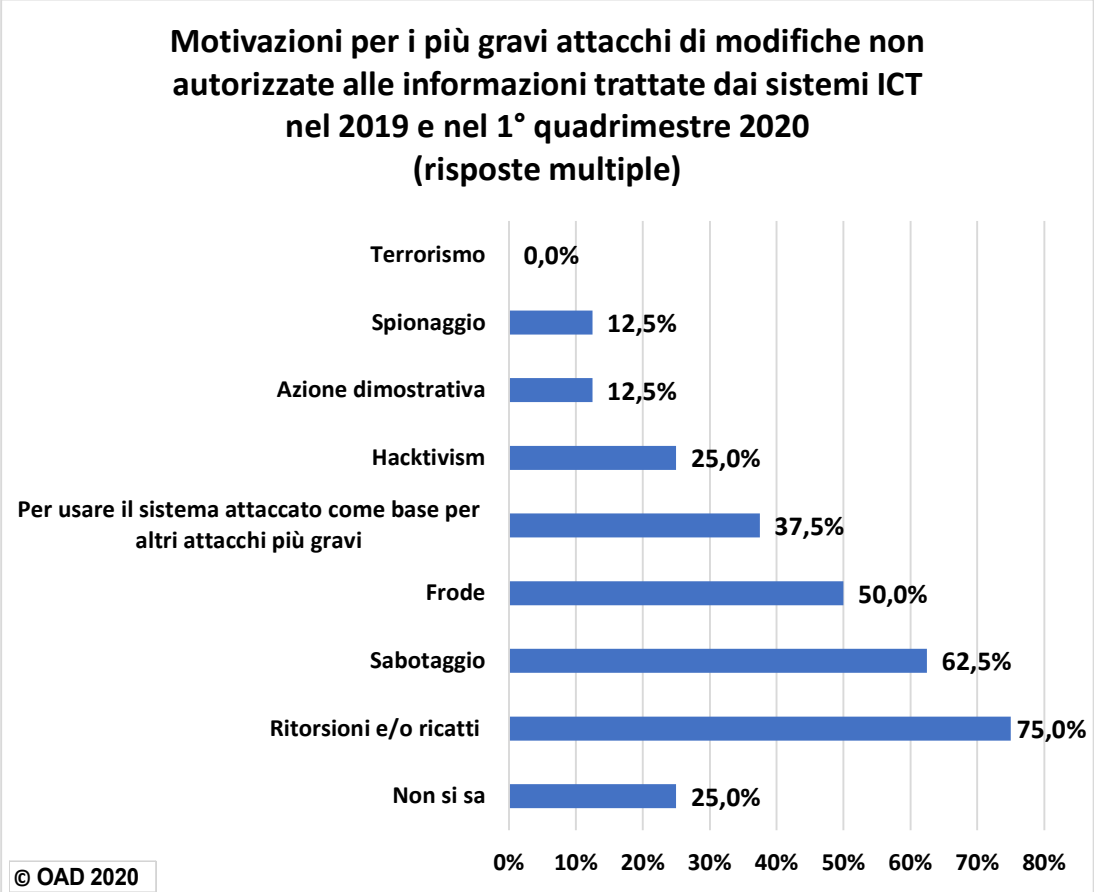


Fig. 6.10-4

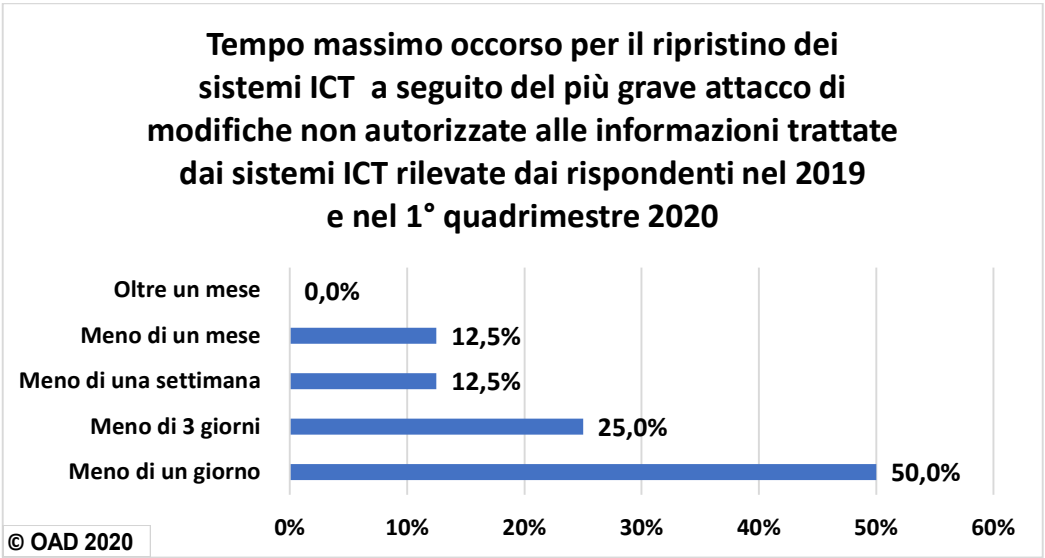


Fig. 6.10-5

6.11 Saturazione risorse digitali (DoS, DDoS)

La saturazione delle risorse ICT, indicata sovente anche in Italia con l'acronimo inglese DoS/DDoS, Denial of Service/Distributed DoS, è una tipologia di attacco consolidata, fino a poco tempo fa abbastanza critica per prevenirla-contrastarla, dato che richiedeva un accordo con i forniti di servizi di telecomunicazione perché, in caso di attacco, questi ultimo potessero individuarlo in tempo quasi reale, e creare percorsi alternativi per dirottare il traffico di saturazione. Negli ultimi tempi sono attivi anche in Italia fornitori di servizi, tipicamente in cloud, che consentono di prevenire o bloccare questa insidiosa tipologia d'attacco con soluzioni semplici e trasparenti per l'utente. L'adozione di efficaci misure di contrasto, come rilevato dalle indagini OAD, hanno ridotto la diffusione di questa tipologia di attacco: come trend di evoluzione, e non come confronto strettamente statistico, si è passati dal circa 30% dei rispondenti che avevano subito questo attacco nel 2017 e 2018, al 17,5% nel 2019 e al 12,1% nel 1° quadrimestre 2020, come evidenziato nella fig. 6-7.
La fig. 6.11-1 dettaglia come nel 2019 si siano rilevati pochi attacchi ad alta ripetizione e frequenza, e nessuno nel 1° quadrimestre 2020. Per questa tipologia di attacchi, infatti, è difficile mantenere per tempi abbastanza lunghi tutti i bot attivi e nascosti nei vari sistemi ICT infettati (possono essere migliaia a livello mondiale) per poi scatenare l'attacco. Inoltre, come per ogni altra tipologia d'attacco, quando si riscontra che il sistema target ha le idonee misure di contrasto, e inutile ripetere l'attacco di quel tipo, non potrà avere successo.

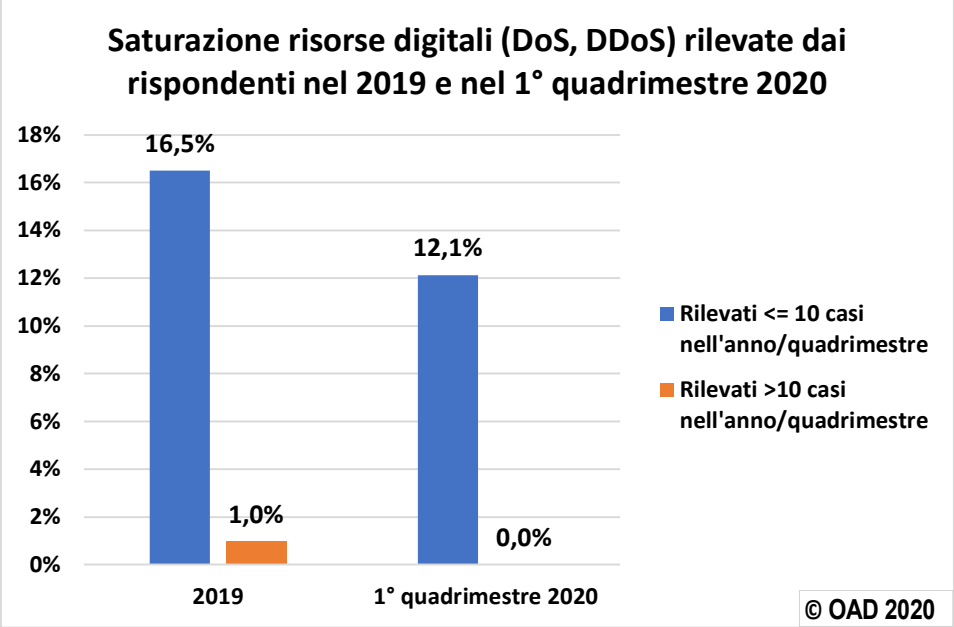


Fig. 6.11-1

La fig. 6.11-2 riporta, con risposte multiple, le tecniche rilevate dai rispondenti che hanno subito Dos/DDoS: al primo posto, giustamente con un'altissima percentuale, l'uso di botnet e Command Control da remoto, le tipiche tecniche usate per portare questa tipologia di attacchi. Al secondo posto la raccolta di informazioni, con un 53,3%, indispensabile per avere le informazioni necessarie sugli applicativi target da saturare. Al terzo posto i toolkit, con un considerevole 46,7%. A scalare, con percentuali assai più basse, le altre tecniche di attacco.

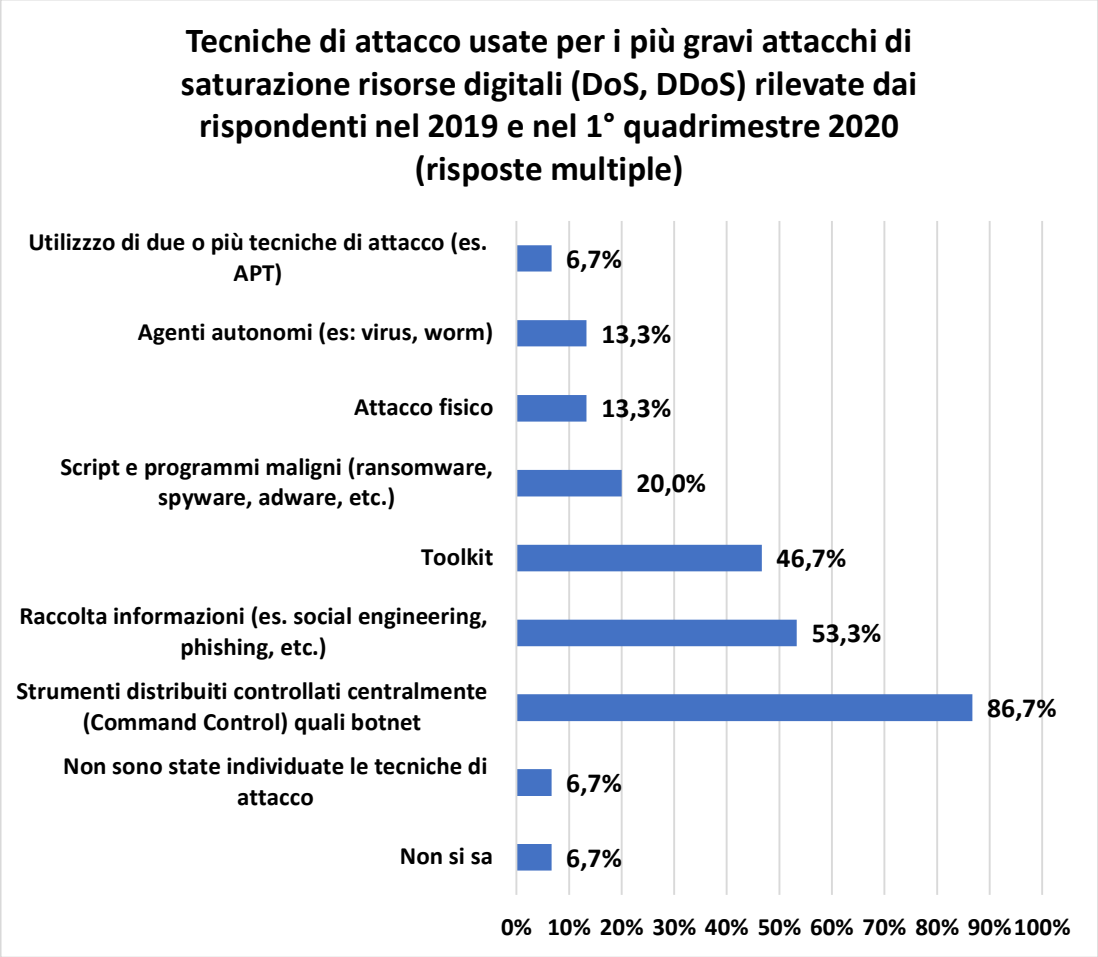


Fig. 6.11-2

Le implicazioni ed i danni causati da un DoS/DDoS, se riuscito, sono sempre gravi, in quanto bloccano per un certo arco di tempo i sistemi informatici che l'hanno subito. La fig. 6.11-3, con risposte multiple, evidenzia che, nei casi più gravi, quasi i ¾ dei rispondenti hanno subito gravi disservizi, con perdita di immagine per più del 26,7% dei rispondenti, ma solo per il 6,7% ricadono le conseguenze più gravi: elevati tempi e costi per ritornare alla normale operatività, perdita di affari e di clienti, danni da risarcire. Il 40% dei rispondenti non ha avuto invece alcun impatto, ed 1/3 ha avuto disservizi di breve durata, con un ritorno alla normalità in tempi brevi ed a costi ridotti. Questi casi di "pochi" e "non gravi" impatti riguardano Aziende/Enti che già disponevano di soluzioni anti Dod/DDoS o accordi coi loro fornitori di TLC e di networking.
Chi non li aveva, in certi casi ha avuto seri problemi, con tempi e costi elevati come anche rilevato nella fig. 6.11-5.
La fig. 6.11-4 mostra, con risposte multiple, le percentuali delle motivazioni per l'attacco DoS/DDoS subito, a giudizio dei rispondenti. Al primo posto, con un elevatissimo 80% si posiziona il sabotaggio: un attacco che mette fuori servizio il sistema informatico, o una sua parte, è un effettivo sabotaggio all'intera Aziende/Ente o a una sua parte. Un 40% reputa l'attacco un'azione dimostrativa, che si collega logicamente alla ritorsione-ricatto, anch'essa con un 40%. L'attaccante blocca in saturazione i collegamenti con il sistema informatico, e poi ricatta l'Azienda/Ente, normalmente con una elevata cifra economica, per smettere il DoS/DDos. Da sottolineare che, anche per questa tipologia di attacco, una delle motivazioni considerate dai rispondenti sia il terrorismo cibernetico.

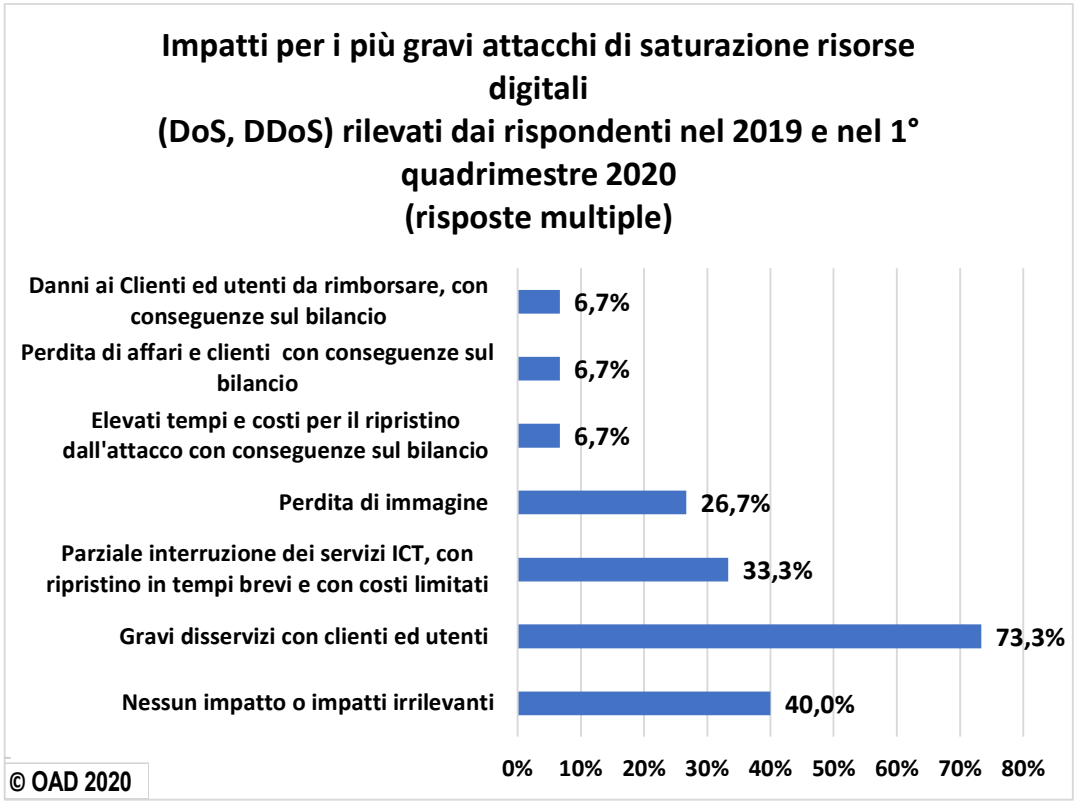


Fig. 6.11-3

La fig. 3.11-5 mostra i tempi di ripristino rilevati dai rispondenti per gli attacchi più gravi subiti di DoS/DDoS. Il 22,7% dei casi ha richiesto dai 4 ai 7 giorni, ed il 16,7% dagli 8 ai 30 giorni. Queste due ultime percentuali, molto alte per tempi di ripristino così prolungati, sono dovute alla mancanza di accordi coi fornitori di TLC o di utilizzo di servizi anti-saturazione ICT come quello fornito a livello mondiale da Cloudflare. La metà dei rispondenti, che ha probabilmente già attivato questo tipo di servizi ed accordi, riesce a ripristinare la situazione *ex ante* in un solo giorno.

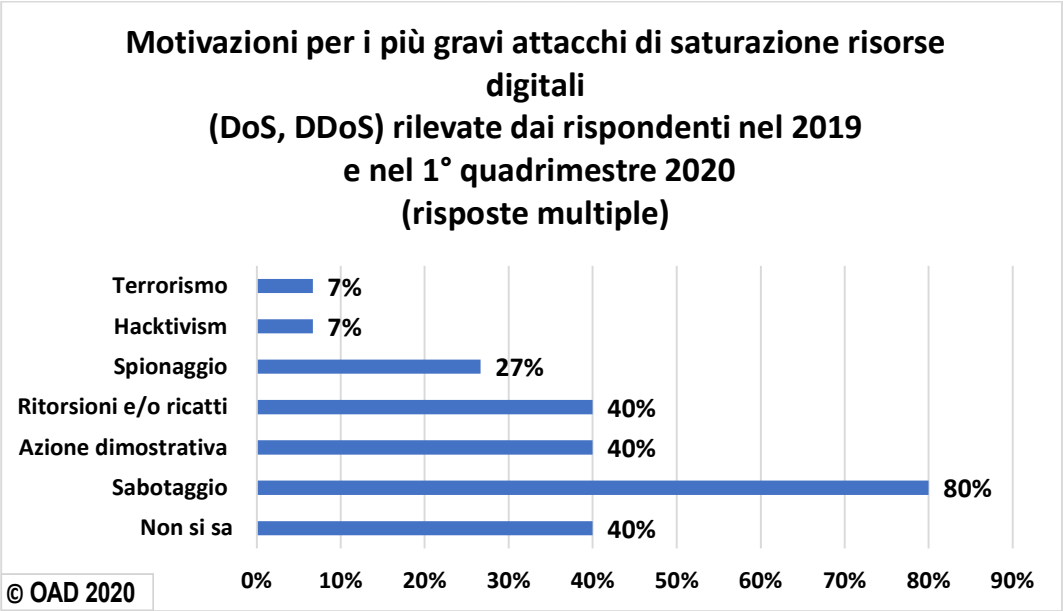


Fig. 6.11-4

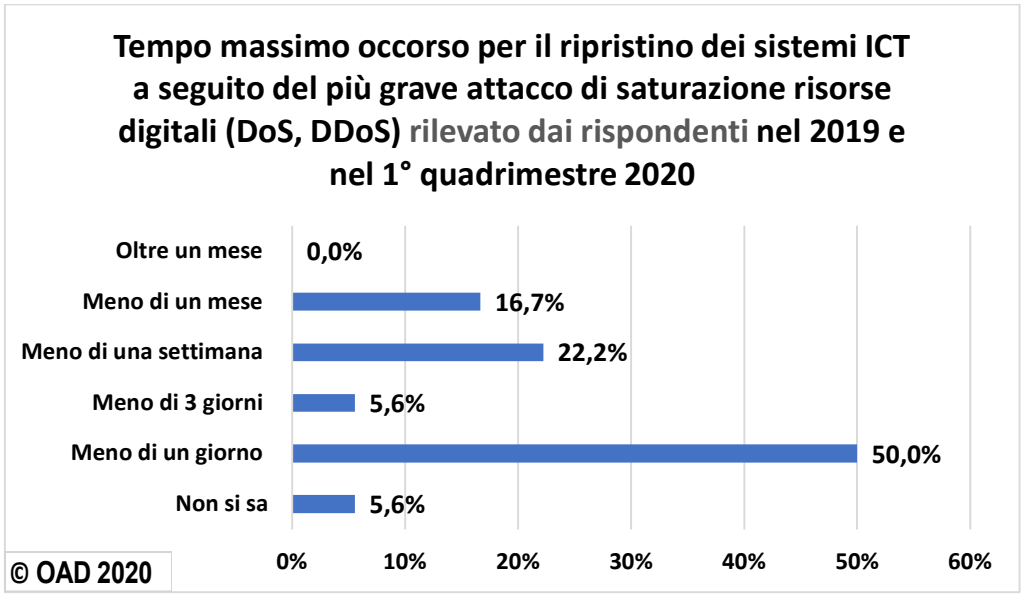


Fig. 6.11-5

6.12 Attacchi ai propri sistemi in cloud o in housing/hosting presso fornitori terzi

Le Aziende/Enti italiani fanno un crescente uso della terziarizzazione di servizi ICT e di servizi in cloud: parte del, e in certi casi l'intero sistema informatico è presso terzi, a livello di software o anche di hardware (housing), così come la sua gestione operativa: un attacco digitale ai sistemi di questi fornitori di terziarizzazione ICT, che include anche il cloud, chiamati per brevità outsourcer, diviene

anche un attacco al sistema informatico dell'Azienda/Ente cliente. Gli outsourcer sono medie e grandi imprese, anche a livello internazionale, conosciuti sul mercato e per questo loro stessi un interessante target di attacco.
Nella maggior parte dei casi questi fornitori hanno serie e sofisticate contromisure di sicurezza, molto più potenti ed efficaci di quelle che potrebbero mettere in atto, nella media, i loro clienti. Ma per attaccanti con competenze e risorse, colpire e perforare un outsourcer significa conoscere e attaccare nello stesso tempo almeno una parte dei clienti operanti con quell'outsourcer, clienti che possono essere ben più significativi per l'attaccante dell'outsourcer stesso.
Volutamente nell'elenco delle tipologie di attacchi declinate sul "che cosa attacco" si è inserita questa generica voce di attacco ai cloud ed alle risorse ICT terziarizzate, senza dettagliare le possibili differenti tipologie di attacco considerate nella tassonomia di attacchi di OAD: non sono state pertanto richieste nel questionario diverse possibili modalità di attacco ai sistemi di hosting e di cloud, da quello fisico alle reti, dall'IAA agli applicativi e ai dati trattati, per non rendere troppo lunga e difficoltosa la sua compilazione.
Nell'indagine 2020 di OAD, i rispondenti che utilizzano per il loro sistema informatico, in tutto o in parte, soluzioni terziarizzate sono circa il 69% nel 2019, e cresciuti a 70, 5% nel 1° quadrimestre 2020, come indicato in §10.3. Questi rispondenti hanno rilevati attacchi ai loro sistemi terziarizzati/in cloud il 16,5% nel 2019, ed il 13,1% nel 1°quadrimestre 2020, come indicato nella fig. 6-7.
La fig. 6.12-1 mostra come in entrambi i periodi si siano verificati frequenti e ripetuti attacchi anche se con basse percentuali: nel 1° quadrimestre si è riscontrata una lieve crescita degli attacchi molto frequenti e ripetuti, rispetto al 2019, forse dovuta anche all'effetto Covid-19 (§6).

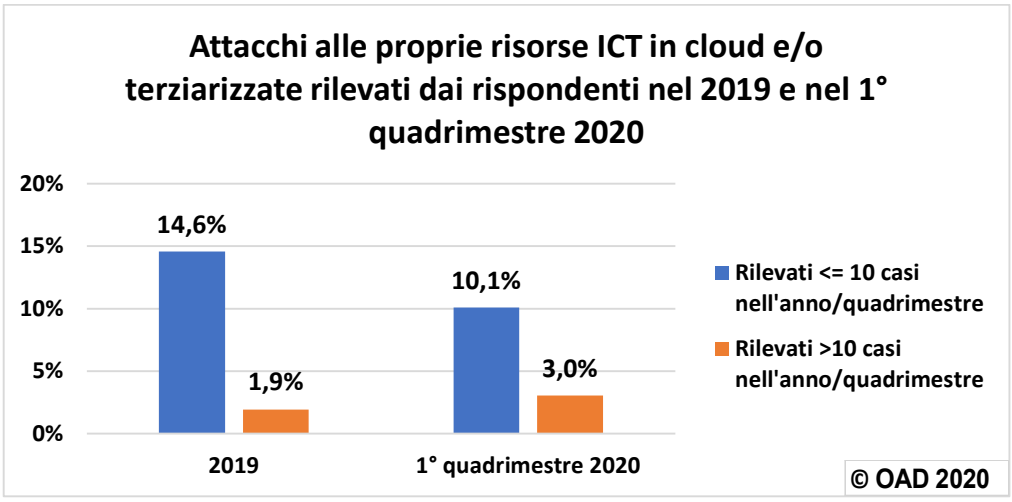


Fig. 6.12-1

La fig. 6.12-2 mostra, con risposte multiple, le tecniche di attacco usate secondo i rispondenti che hanno subito questo tipo di attacco. Al primo posto con un elevato 66,7% malware e script, indice che la forte diffusione di malware in Italia ha colpito anche alcuni outsourcer, nonostante le loro misure di sicurezza. Al secondo posto, con un 60% a poca distanza percentuale da malware/script, i toolkit, necessari per esaminare possibili punti di ingresso e vulnerabilità dell'outsourcer, cui segue a breve distanza la raccolta di informazioni: social engineering, phishing, etc. Con percentuali decrescenti, ma sempre alte, le altre tecniche di attacco: a conferma della sofisticazione degli attacchi portati agli outsourcer, che usano in pratica un ampio spettro di tecniche d'attacco, anche contemporaneamente e in maniera persistente. L'unica tecnica non utilizzata è, ovviamente, l'attacco fisico.

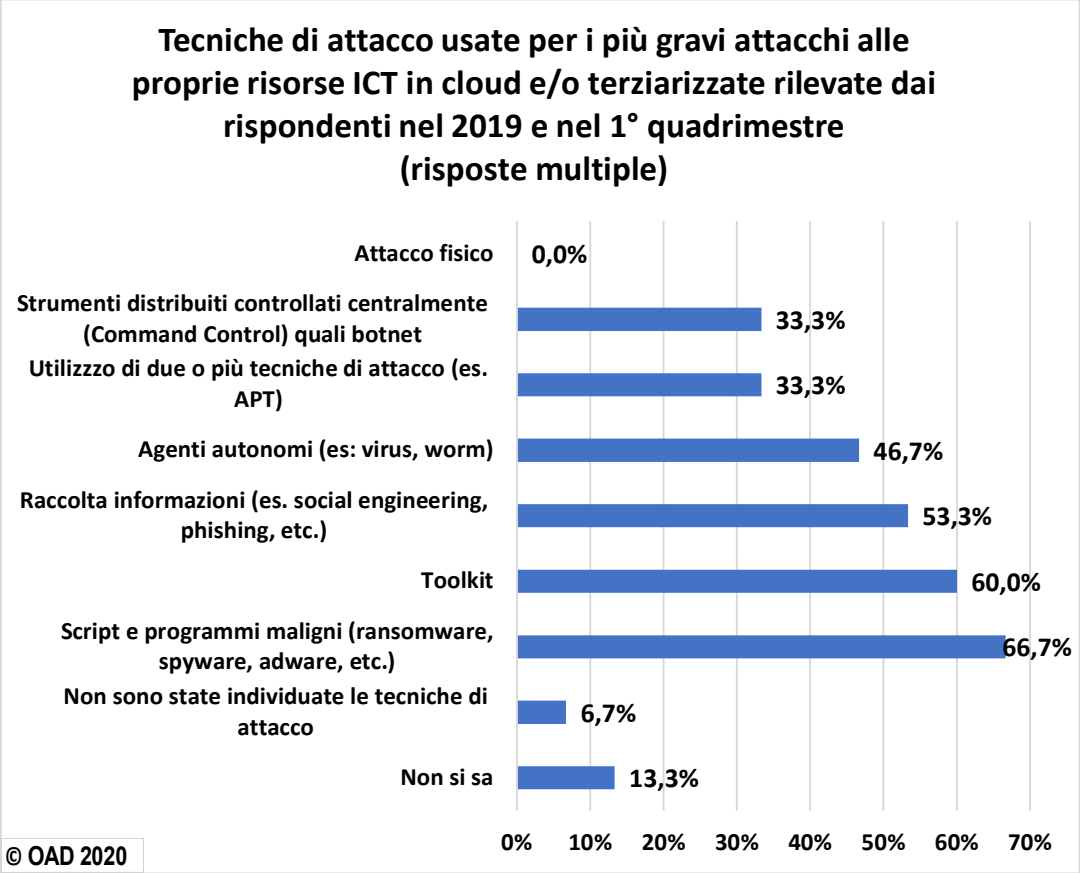


Fig. 6.12-2

La fig.6.12-3 illustra, con risposte multiple, gli impatti riscontrati dai rispondenti a seguito dell'attacco ai propri sistemi ICT terziarizzati. I dati emersi evidenziano, alla stregua di altre tipologie d'attacco, una situazione duplice e abbastanza bilanciata: circa metà dei rispondenti ha riscontrato pochi o nulli impatti, mentre l'altra metà ha subito gravi impatti e relative conseguenze anche economiche.
L'indagine OAD è assolutamente anonima, e non richiede informazioni specifiche sui prodotti e servizi usati dai rispondenti: non si conosce quindi chi sia l'outsourcer ed i livelli di sicurezza digitale da questi forniti al sistema informatico oggetto delle risposte del questionario. Non tutti gli outsourcer hanno o forniscono livelli di sicurezza digitali al top, dipende anche dalle clausole contrattuali stabilite, e dai relativi prezzi pagati. Il 60% dei rispondenti non ha rilevato impatti, se non irrisori, ed il 26,7% ha subito dei disservizi, ma risolti in poco tempo ed a basso costo. Un altro 60% ha invece subito gravi disservizi, il 40% perdita di immagine sul mercato, il 6,7% elevati tempi e costi per la ripresa, ed un altro 6,7% perdita di clienti ed affari. Una piccola percentuale di rispondenti segnala che l'attacco ai sistemi terziarizzati/in cloud è servito come base per portare altri attacchi: ormai casi rari, date le misure di sicurezza digitale che gli outsourcer attivano, ma usati per sviluppare malware, per installare agent e bot, per simulare attacchi, e così via.
Si tenga inoltre conto che molti rispondenti utilizzano diversi servizi in cloud, offerti da diversi fornitori, così come possono utilizzare più outsourcer per i loro housing e hosting.

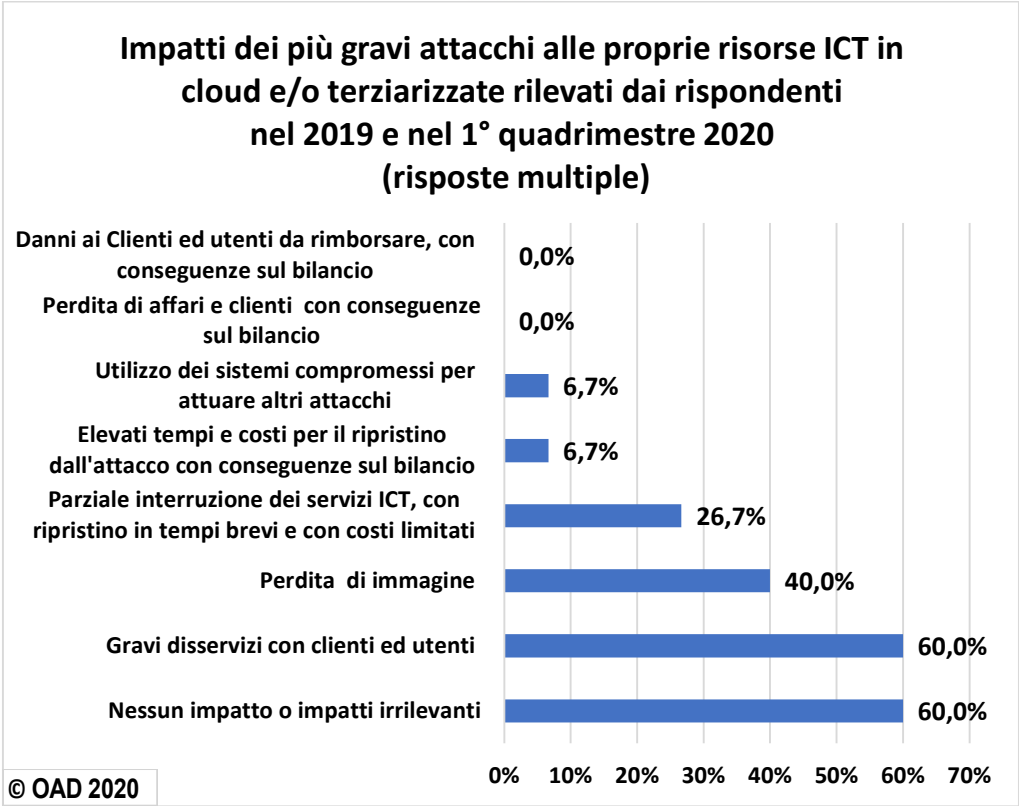


Fig. 6.12-3

Le possibili motivazioni per l'attacco più grave (fig. 6.12-4, con risposte multiple) portano al primo posto la frode, con un ampio 60% dei rispondenti che l'hanno subita. Seguono, con percentuali a scalare, ma non troppo distanziate tra loro. 1/5 dei rispondenti non è stato in grado di indicare le motivazioni per il più grave attacco ai sistemi in terziarizzati/in cloud.

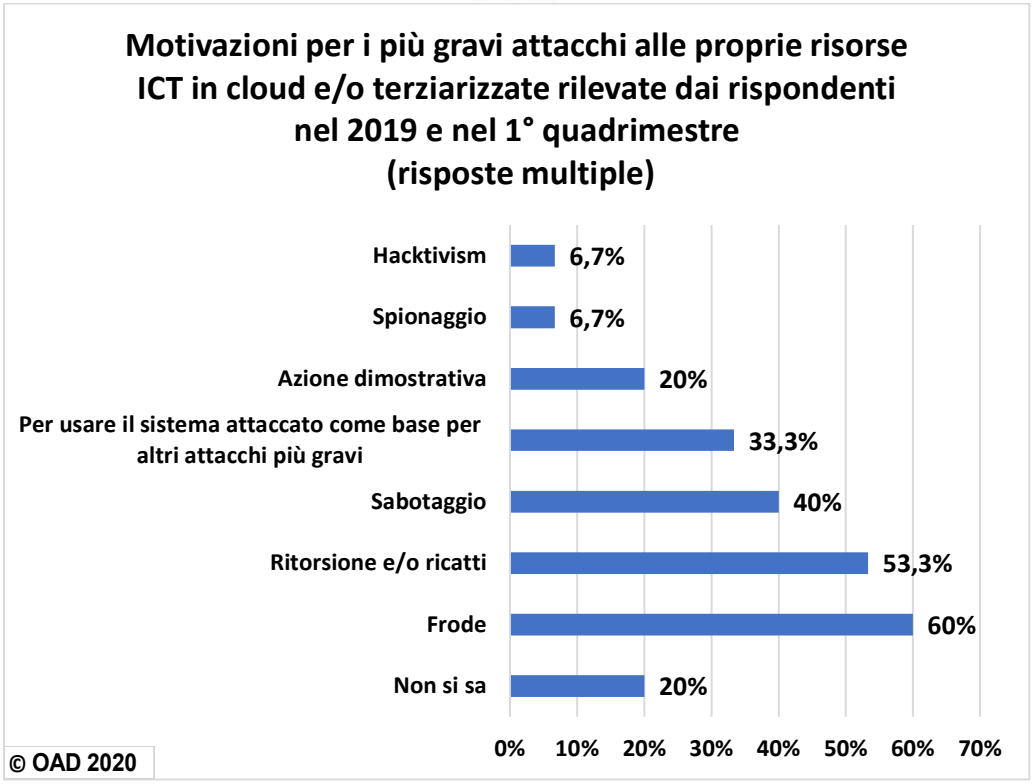


Fig. 6.12-4

La già citata fig. 6.12-5 conferma il doppio scenario emerso per questa tipologia di attacco per i rispondenti che lo hanno subito. Il 61,7% dei sistemi/servizi terziarizzati/in cloud sono stati ripristinati entro un solo giorno. Il 5,6% in due-tre giorni. Ma il 17,7 % ha avuto bisogno di 4-7 giorni, la medesima percentuale ha richiesto tra 8 e i 30 giorni.

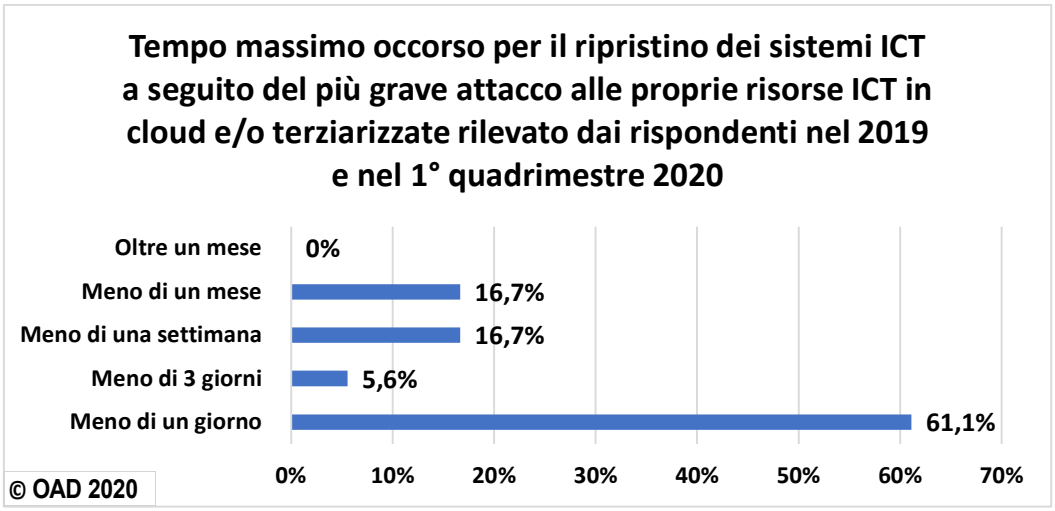


Fig. 6.12-5

6.13 Attacchi a dispositivi IoT (Internet of Things) in uso

Come già anticipato nei precedenti Capitoli 4 e 5, la pervasività di Internet e l'inserimento di capacità elaborativa e di comunicazione in un numero crescente di oggetti anche di uso comune ha allargato ampiamente l'area di interoperabilità tra oggetti con capacità elaborativa digitale, e quindi l'area di possibili attacchi digitali. Tutti questi sistemi, spesso chiamati "smart" per le capacità di "intelligenza" elaborativa al loro interno, comunicano via Internet seguendo i suoi protocolli, ed interoperano tra di loro.

In tale ambito negli ultimi anni è esploso il fenomeno degli IoT, Internet of Things. Al di là dell'inserimento di un piccolo sistema ICT con capacità elaborativa e di trasmissione, i cosiddetti sistemi "*embedded*", qualsiasi oggetto "comune" come un abito, un paio di scarpe, un giocattolo, un piatto e così via può divenire riconoscibile ed un poco "smart" grazie ad etichette di identificazione quali tag RFID[13] o codici QR[14], in grado di comunicare in rete e di essere riconosciuti da ed interagire con dispositivi mobili quali smartphone e tablet dotati delle opportune applicazioni. Queste etichette sono usate ed usabili anche per gli animali e per il tracciamento del cibo, dal produttore al distributore finale.

Pertanto, IoT indica una rete di oggetti (o di loro parti) che, grazie alle loro capacità elaborative e di connettività, sono in grado di interoperare tra loro e con i sistemi informatici, abilitando nuove soluzioni e nuove integrazioni in moltissimi settori. Il singolo dispositivo IoT è un "oggetto smart", caratterizzabile da capacità funzionali quali l'identificazione, la connessione, la localizzazione, l'elaborazione di dati e la comunicazione a livello locale e/o geografico. Il mondo degli IoT sta esplodendo in innumerevoli settori, specializzando tecnicamente e funzionalmente i singoli sistemi. I diversi settori di applicazione includono (elenco non esaustivo) domotica, robotica, controlli industriali e del territorio, trasporti (dalle auto alle moto, dai pullman agli autocarri, dai muletti nei magazzini agli ascensori, dai treni alle navi), avionica, elettrodomestici, biomedicale, agricoltura e zootecnia, smartgrid, smartcity, telemetria, misurazioni da remoto (la cosiddetta "*smart metering*" usata per i contatori intelligenti di gas ed energia elettrica), etc.

Si devono poi tenere conto della convergenza in corso tra il mondo IoT e quello OT, Operational Technology, che include tutti i sistemi di automazione industriale (considerati nel prossimo paragrafo §6.14), con i sistemi IoT che, se funzionali a tale automazione, sono ora indicati come IIoT, Industrial IoT.

In termini di sicurezza digitale gli IoT sono balzati al centro dell'attenzione per la concomitanza di alcuni fattori: in primo luogo per la loro connessione ad Internet, poi per la loro numerosità e, infine, perché gran parte dei primi IoT, molti dei quali ancora in uso, non furono progettati tenendo conto dei problemi della sicurezza digitale ed il loro software, compreso il sistema operativo, non è stato mai aggiornato. Molti dei "vecchi" IoT, pur funzionanti e in produzione, sono tecnicamente obsoleti e presentano gravi vulnerabilità, eliminabili con opportune patch o nuove versioni del software, ma che il più delle volte non è possibile attuare per vincoli tecnici, quali limiti di memoria, capacità CPU, etc., o per la difficoltà a raggiungerli fisicamente per manutenzioni, data la loro posizione: in cima a pali o tralicci, in posti critici per interventi di personale, etc. Se la rete di IoT è in qualche misura interoperante, se non integrata, con il sistema informatico, le vulnerabilità degli IoT costituiscono gravi rischi per l'intero sistema informatico. Si deve poi tenere conto della numerosità di questi dispositivi, a livello mondiale ma anche italiani. Dal 2007, a livello mondiale, il numero di oggetti connessi ad Internet ha superato il numero delle persone connesse, ma le previsioni di crescita di pochi anni fa di arrivare a 50 miliardi di dispositivi sono state considerevolmente ridotte: autorevoli ricerche di mercato parlano dai 5,6 ai 9 miliardi.

L'indagine OAD fa riferimento ai soli attacchi intenzionali ai sistemi informatici di Aziende/Enti, non considera attacchi ai sistemi ICT di persone, domestici e dei loro oggetti smart; questo riduce fortemente il numero di IoT da considerare per le indagini OAD, quella 2020 inclusa.

[13] Tag RFID

[14] Un codice QR, Quick Response, è un codice a barre bidimensionale, ossia a matrice, composto da moduli neri disposti all'interno di uno schema bianco di forma quadrata. Genericamente il formato matriciale è di 29x29 quadratini e contiene 48 alfanumerici. Viene impiegato per memorizzare informazioni generalmente destinate a essere lette tramite uno smartphone.

Inoltre, il campione di rispondenti liberamente emerso coi rispondenti all'indagine OAD 2020, le cui caratteristiche principali sono illustrate in §10.2 e §10.3, copre nel suo piccolo tutti i settori merceologici, cui si aggiungono le PAC e le PAL: il numero di rispondenti che dispone al proprio interno di sistemi IoT/IIoT è limitato nell'ordine di circa il 10% rispetto a tutte le Aziende/Enti che hanno risposto al questionario.
Le indicazioni sulle caratteristiche di maggior dettaglio evidenziate dalla fig. 6.13-2 alla fig. 6.13-5 sono quindi da considerarsi solo come specifici casi reali di attacchi a IoT/IIoT forniti dai rispondenti: non essendo sufficientemente numerosi, non possono essere considerate di riferimento statistico per l'intero ambito di uso di IoT/IIoT in Italia.
L'uso di IoT di fatto continua a crescere anche in ambito business, non solo per la domotica o per usi personali/ludici. Tenendo presente questo contesto, l'ambito IoT dei rispondenti ha rilevato attacchi nel 2019 per il 14,6% e nel 1° quadrimestre 2020 per il 3,0%, come evidenziato nella fig. 6-7.
La fig. 6.13-1 dettaglia come solo nel 2019 si sono verificati alcuni frequenti e ripetuti attacchi ai sistemi dei rispondenti, ma con una bassa percentuale del 2,9%, e nessun attacco ripetuto e frequente nel 1° quadrimestre 2020.

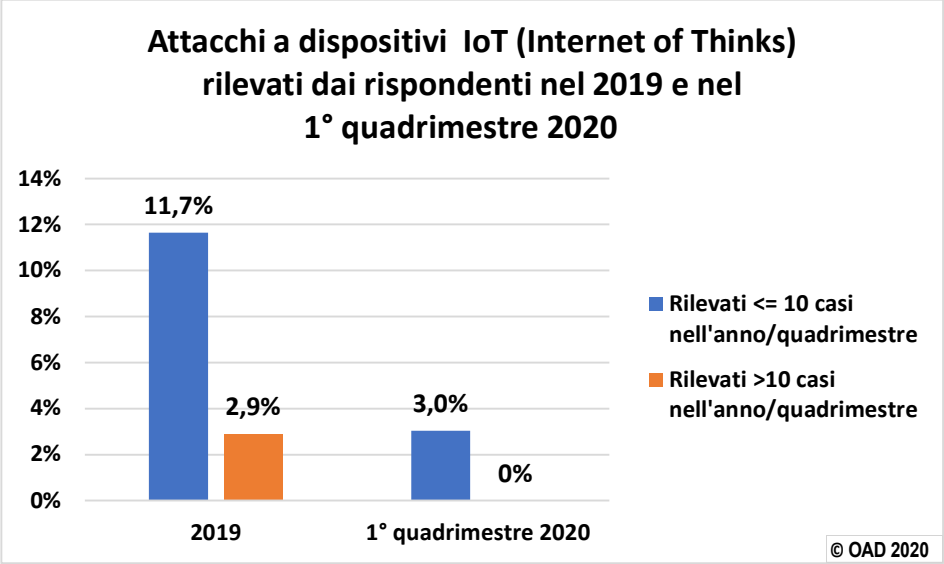


Fig. 6.13-1

Analizzando e correlando le risposte al questionario OAD 20120, risulta che le Aziende/Enti che hanno subiti attacchi ai loro ambienti IoT appartengono ai seguenti settori merceologici (si veda §10.2):

- Servizi ICT: consulenza, produzione software, service provider ICT, gestione Data Center, servizi assistenza e riparazione ICT, etc. (Codici Ateco J62, J63, S95.1)
- Trasporti e magazzinaggio (Codici Ateco H)
- Utility: Acqua, Energia, Gas, etc. (Codici Ateco D ed E).

Le tecniche di attacco indicate dai rispondenti che hanno subito e rilevato attacchi ai loro sistemi IoT sono elencate in percentuale nella fig. 6.13-2, con risposte multiple. Al primo posto, per 1/3 dei rispondenti, i toolkit usati per verificare i possibili punti deboli e le vulnerabilità da sfruttare per effettuare l'attacco. Seguono con lo stesso 11,1% la raccolta di informazioni, l'uso di codici maligni e di script, l'uso di agenti autonomi, l'uso di botnet. Nei casi rilevati dai rispondenti non sono state usate semplici tecniche "fisiche" e sofisticati utilizzi contemporanei di più tecniche di attacco.

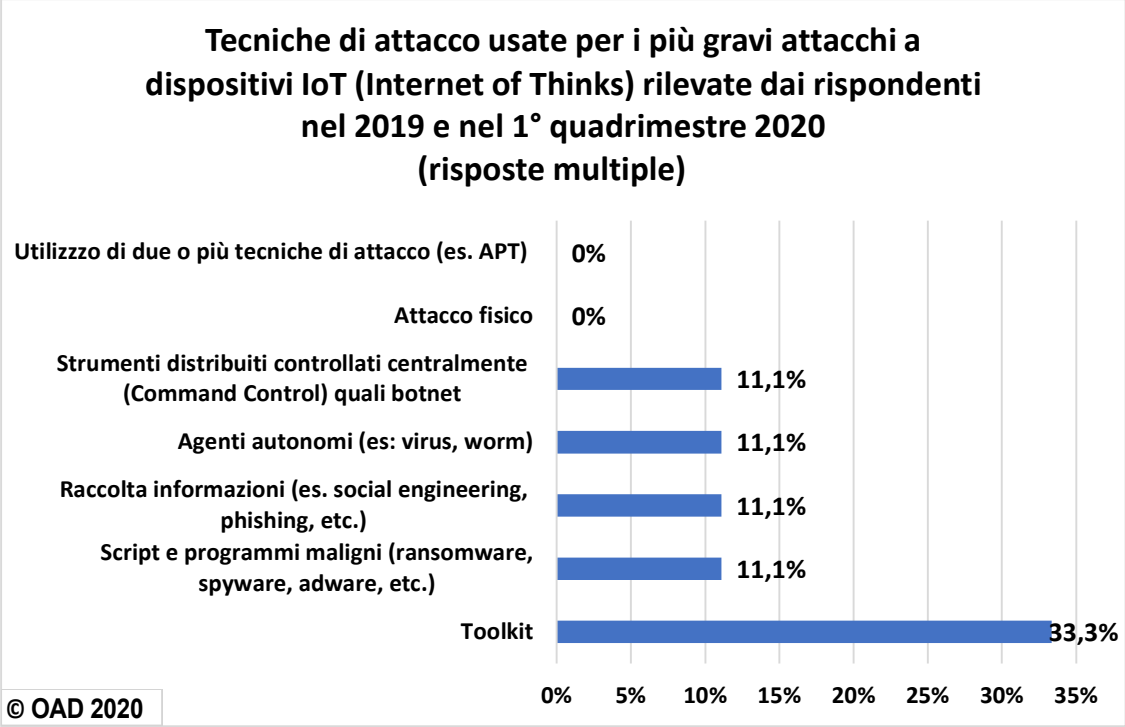


Fig. 6.13-2

Come mostrato in fig. 6.13-3, con risposte multiple, gli impatti causati dagli attacchi più gravi subiti sui sistemi IoT sono stati severi e critici per questi rispondenti: poco meno di 1/3 ha riscontrato disservizi informatici, più di 1/5 perdita di immagine e poco più di 1/10 la perdita di affari e clienti. Solo l'11% dichiara disservizi informatici limitati e con ripartenze in tempi brevi e con costi limitati.

La fig. 6.13-4 mostra, con risposte multiple, le probabili motivazioni degli attaccanti per gli attacchi più gravi indicate dai rispondenti che le hanno subite. Il 22% indica, sempre con la stessa percentuale, la frode, le ritorsioni/ricatti e l'azione dimostrativa, probabilmente propedeutica al ricatto. Non sono considerate altre motivazioni.

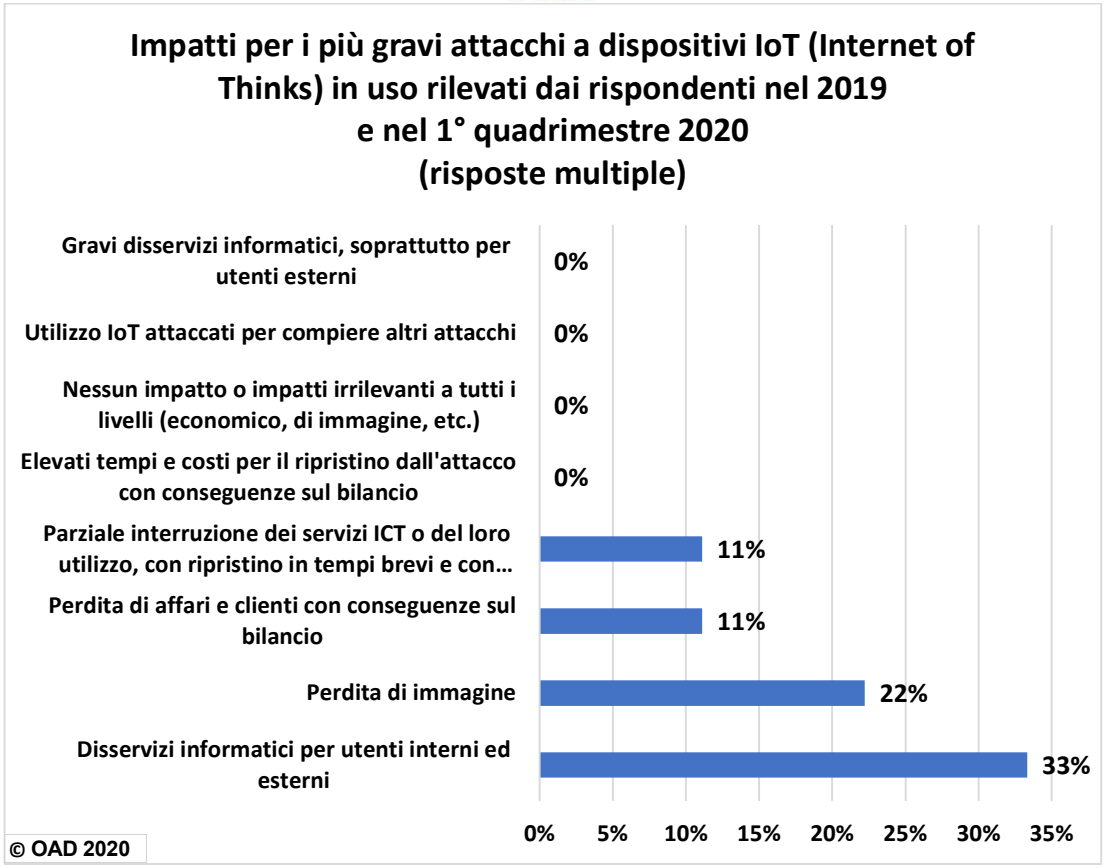


Fig. 6.13-3

La fig.6.13-5 mostra, con risposte multiple, i tempi massimi per il ripristino dopo gli attacchi più gravi rilevati agli IoT. Interessante evidenziare come tali tempi non siano stati brevi, anche se in nessun caso il ripristino richiese più di una settimana: solo il 25% in una sola giornata, ma nella maggior parte dei casi, il 50%, entro 3 giorni ed il 25% tra 4 e 7 giorni.
Questi tempi massimi riscontrati dai rispondenti per il ripristino dopo un attacco ai loro IoT, pur senza alcuna pretesa di fornire statistiche generali sul fenomeno, indicano un leggero miglioramento rispetto ai dati emersi dalle precedenti indagini OAD, e risultano ragionevoli, tenendo conto che, da un lato i dispositivi IoT non sempre sono monitorati e controllati centralmente in maniera continua e sistematica, dall'altro che alcuni dispositivi sono dislocati in punti non facilmente raggiungibili dalle persone che devono manutenerli e che possono aggiustarli. Infine, è probabile che i precedenti sistemi IoT siano stati sostituiti da quelli di nuova generazione, più affidabili e sicuri.

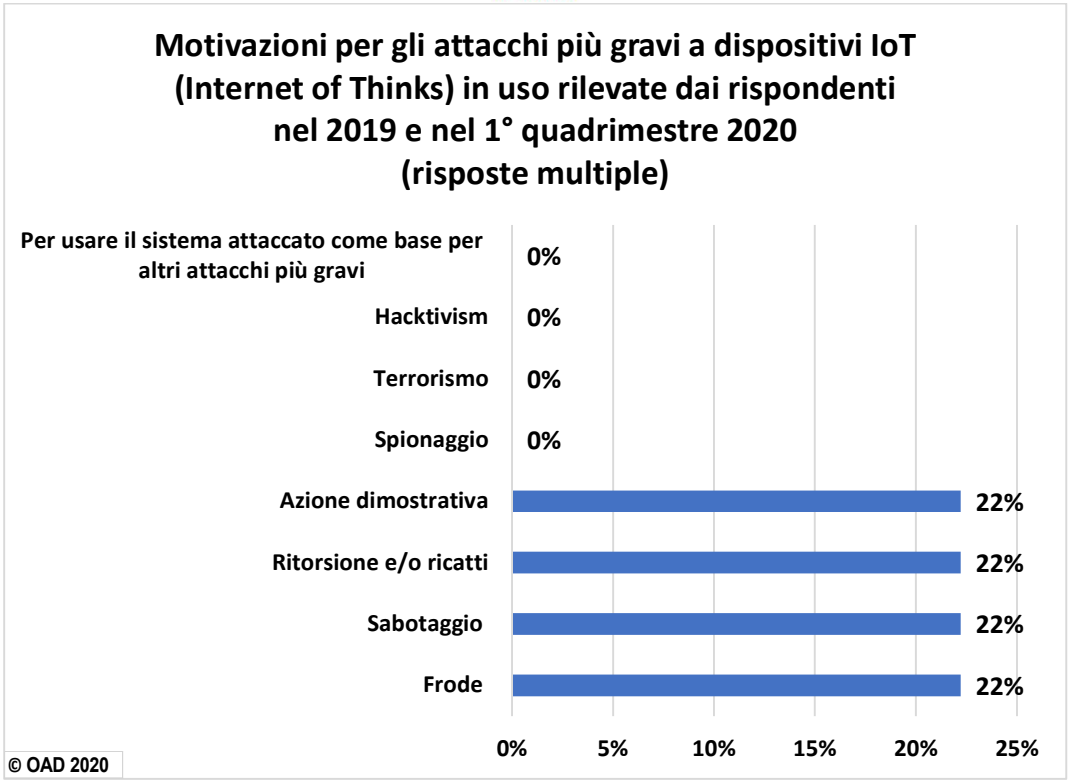


Fig. 6.13-4

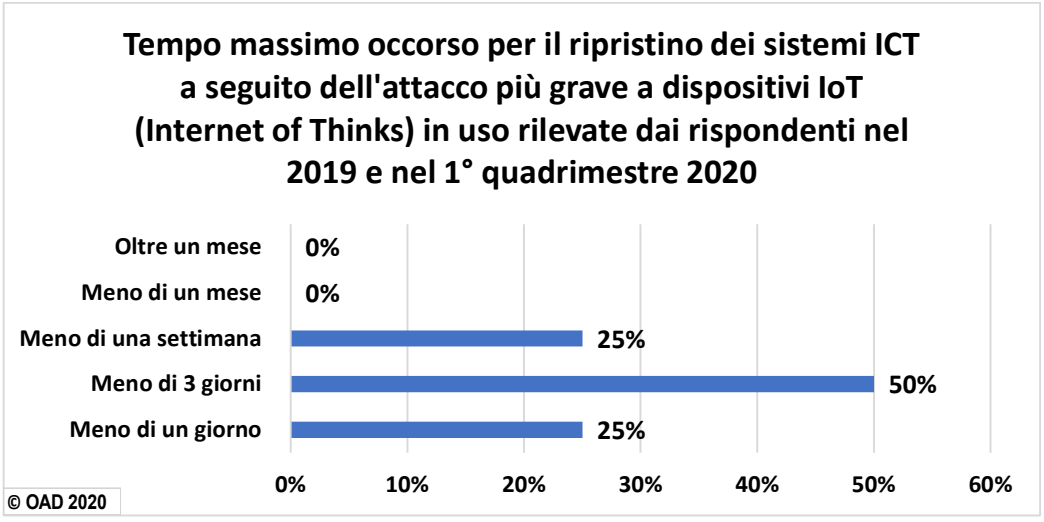


Fig. 6.13.5

6.14 Attacchi ai propri sistemi di automazione industriale e di robotica

I sistemi di automazione industriale e di robotica si vanno estendendo dal tradizionale e consolidato settore manifatturiero per l'automazione della produzione ad altri, quali l'automazione dei magazzini per la logistica, l'automazione delle facility di un Data Center, l'ambito ospedaliero - soprattutto per sale operatorie robotizzate ed i sistemi di diagnostica computerizzata - la ricerca e sviluppo in vari settori, e così via.
Per coprire con un unico termine questo ampio e complesso contesto, è emersa la sigla OT, Operational Technology, che nell'uso comune include anche i sistemi IoT/IIoT, trattati separatamente, data la loro maggior numerosità e il loro elevato tasso di crescita, nel precedente §6.13.
I sistemi per l'automazione della produzione e della robotica, che inizialmente operavano in modo autonomo e sovente non erano nemmeno considerati risorse del sistema informatico, ora sono quasi tutte collegate al sistema informatico per interoperare con le applicazioni centralizzate tipo ERP, oltre che direttamente ad Internet, per poter essere accedute da remoto per controlli e manutenzione.
La connessione ai Data Center e soprattutto ad Internet sono elementi che hanno aumentato la vulnerabilità di questi ambienti.
IIoT, sistemi di automazione della produzione e sistemi di robotica vanno sempre più integrandosi e ad interoperare via Internet, e gli apparati, ormai tutti smart e capacci di comunicare, si differenziano per le loro funzionalità ed i loro utilizzi.
Come per l'IoT, dato il numero relativamente esiguo di rispondenti – rispetto al totale - che dispongono di sistemi OT e che vi hanno rilevato attacchi digitali, i dati che seguono devono essere considerati come esempi di casi specifici, e non essere presi come riferimento della situazione in Italia degli attacchi agli ambienti OT. Il numero di rispondenti che dispone e utilizza sistemi OT è limitato nell'ordine di circa il 7-9% rispetto a tutte le Aziende/Enti che hanno risposto al questionario. Tenendo presente questo contesto, l'ambito OT dei rispondenti ha rilevato attacchi nel 2019 per il 3,9% e nel 1° quadrimestre 2020 per il 3,0%, come evidenziato nella fig. 6-7.

Correlando e analizzando i dati acquisiti dai rispondenti, emerge che sistemi OT sono in uso presso i seguenti settori merceologici:

- Industria manifatturiera e costruzioni: meccani, sui quali a, chimica, farmaceutica, elettronica, alimentare, edilizia, ecc. (Codici Ateco C e F)
- Istruzione: scuole e università pubbliche e private (Codici Ateco P)
- Servizi ICT: consulenza, produzione software, service provider ICT, gestione Data Center, servizi assistenza e riparazione ICT, ecc. (Codici Ateco J62, J63, S95.1)
- Servizi professionali e di supporto alle imprese: attività immobiliari, notai, avvocati, commercialisti, consulenza imprenditoriale, ricerca scientifica, noleggio, call center, etc. (Codici Ateco L, M, N77, N78, N80, N81, N82)
- Servizi turistici, di alloggio e ristorazione: agenzie di viaggio, tour operator, hotel, villaggi turistici, campeggi, ristoranti, bar, etc. (Codici Ateco I e N79)
- Telecomunicazioni e Media: produzione musicale, televisiva e cinematografica, trasmissioni radio e televisive, telecomunicazioni fisse e mobili (Codici Ateco J59, J60, J61)
- Trasporti e magazzinaggio (Codici Ateco H)
- Utility: Acqua, Energia, Gas, etc. (Codici Ateco D ed E).

Nell'ambito della indagine 2020 di OAD, Il numero di settori merceologici che usa questi sistemi digitali è più ampio di quello relativo ai sistemi IoT/IIoT, considerati in §6.13, e che volutamente, come già sottolineato in precedenza, non sono stati inclusi nel più ampio ambito OT. Si noti inoltre che nessuno dei rispondenti del settore sanitario ed ospedaliero ha indicato di utilizzare sistemi OT: strano, secondo l'autore, ma può essere, dato anche il loro numero limitato nella presente indagine.

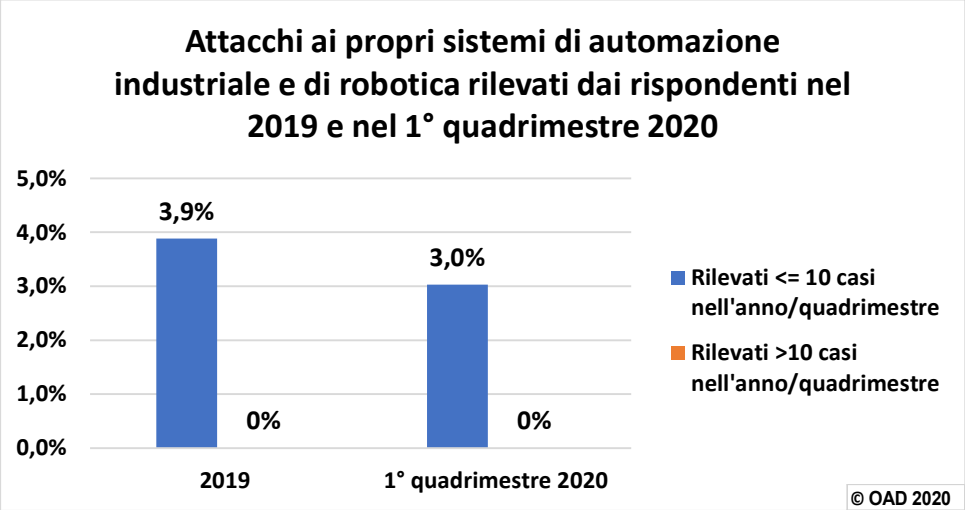


Fig. 6.14-1

La fig. 6.14-1 dettaglia come non si siano rilevati, in entrambi i periodi considerati, frequenti e ripetuti attacchi (oltre a 10) ai sistemi OT dei rispondenti. Questo tipo di attacco deve essere specifico per il sistema OT target, e di una certa complessità, come risulta evidente anche dai dati nelle figure di questo paragrafo: ben difficile che lo stesso tipo di attacco OT possa essere ripetuto molte volte se non ha avuto successo, visto anche il rischio che, a ripeterlo frequentemente, l'attaccante possa essere più facilmente individuato.
La fig. 6.14-2, con risposte multiple, mostra che le tecniche di attacco rilevate e più usate includono, con il medesimo 50%, i toolkit, gli agenti autonomi ed i malware/script. Seguono con un 25% ciascuno, i sistemi distribuiti con controllo centrale e la raccolta di informazioni. Non sono state rilevate tecniche fisiche di attacco e quelle multiple e persistenti. Per l'autore risulta insolita quest'ultima mancanza, dato che le tecniche tipo APT sono proprio specifiche per attaccare sistemi OT.
La fig. 6.14-3 (con risposte multiple) conferma una certa gravità degli impatti di questi attacchi subiti dal seppur limitato numero di rispondenti con sistemi OT. Nessuno ha avuto impatti irrilevanti, ma nemmeno molto gravi e con conseguente perdita di clienti. L'impatto nettamente più diffuso, per il ¾ dei rispondenti, è stata la perdita di immagine. Si bilanciano, ciascuno con un 50%, i disservizi limitati e facilmente recuperabili, con disservizi informatici più consistenti (ma non gravissimi) per utenti e clienti, che hanno comportato significativi tempi e costi per il ripristino.
La fig. 6.14-4 mostra, con risposte multiple, le possibili motivazioni degli attacchi più gravi, così come stimate dai rispondenti attaccati: il sabotaggio è al primo posto, considerato da tutti con un significativo 100%, seguito da ritorsioni/ricatti con un 66,6%. Spionaggio e hacktivism hanno il medesimo 33,3%.
La relativa gravità degli attacchi ai sistemi OT subiti e rilevati dai rispondenti è ulteriormente confermata dai tempi massimi che sono stati necessari per il ripristino della situazione *ex ante* l'attacco. La fig. 6.14-5 mostra infatti che il 25% dei rispondenti riuscì a ripristinare tra una settimana ed il mese, un lasso di tempo veramente lungo, mentre il 50% riuscì entro un singolo giorno, ed il 25% entro tre giorni.

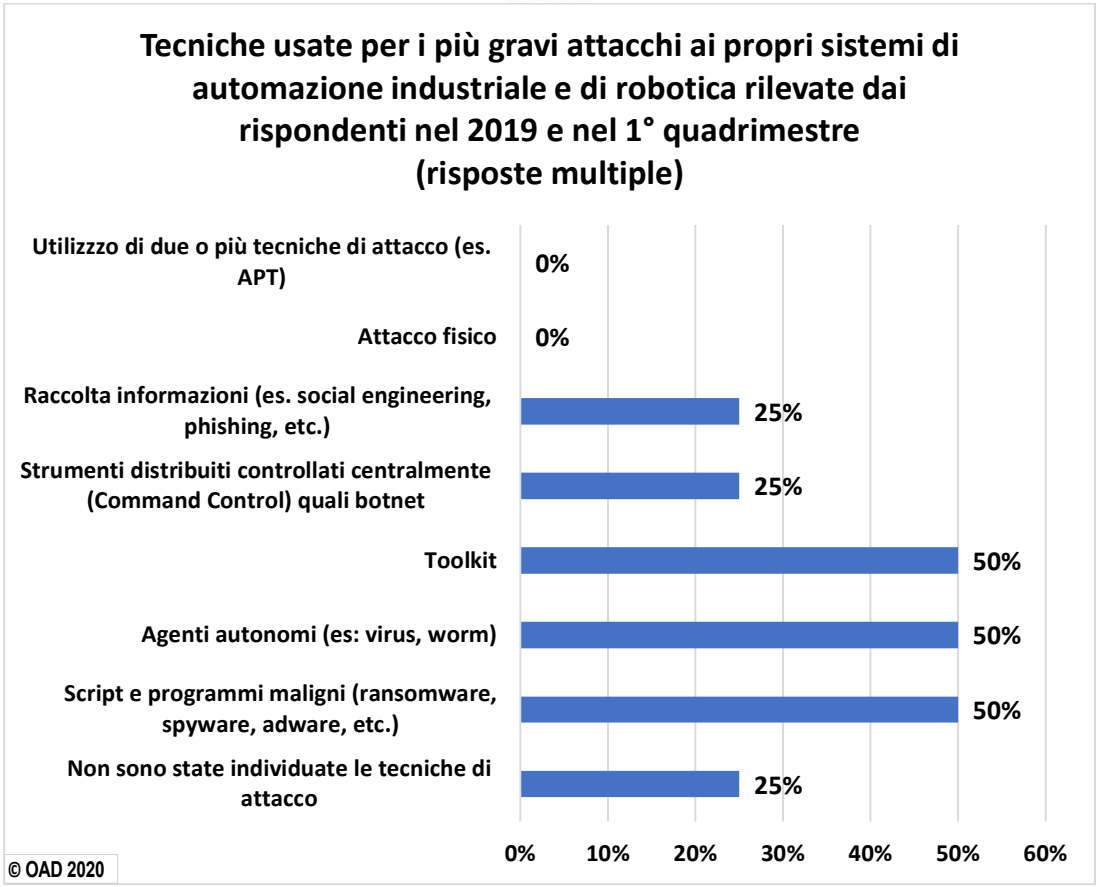

Tecniche usate per i più gravi attacchi ai propri sistemi di automazione industriale e di robotica rilevate dai rispondenti nel 2019 e nel 1° quadrimestre (risposte multiple)
Utilizzzo di due o più tecniche di attacco (es. APT)
0%
Attacco fisico
0%
Raccolta informazioni (es. social engineering, phishing, etc.)
25%
Strumenti distribuiti controllati centralmente (Command Control) quali botnet
25%
Toolkit
50%
Agenti autonomi (es: virus, worm)
50%
Script e programmi maligni (ransomware, spyware, adware, etc.)
50%
Non sono state individuate le tecniche di attacco
25%
0%
10%
20%
30%
40%
50%
60%
© OAD 2020

Fig. 6.14-2

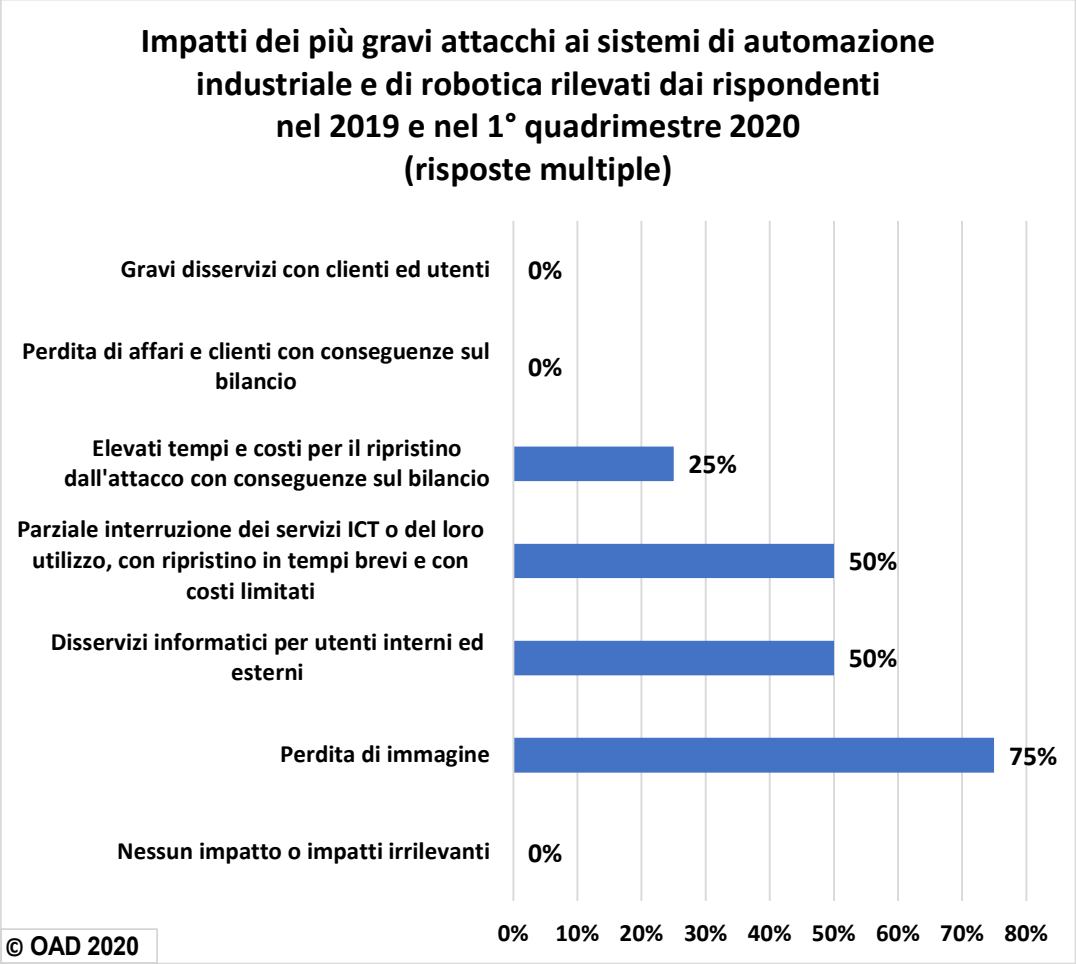


Fig. 6.14-3

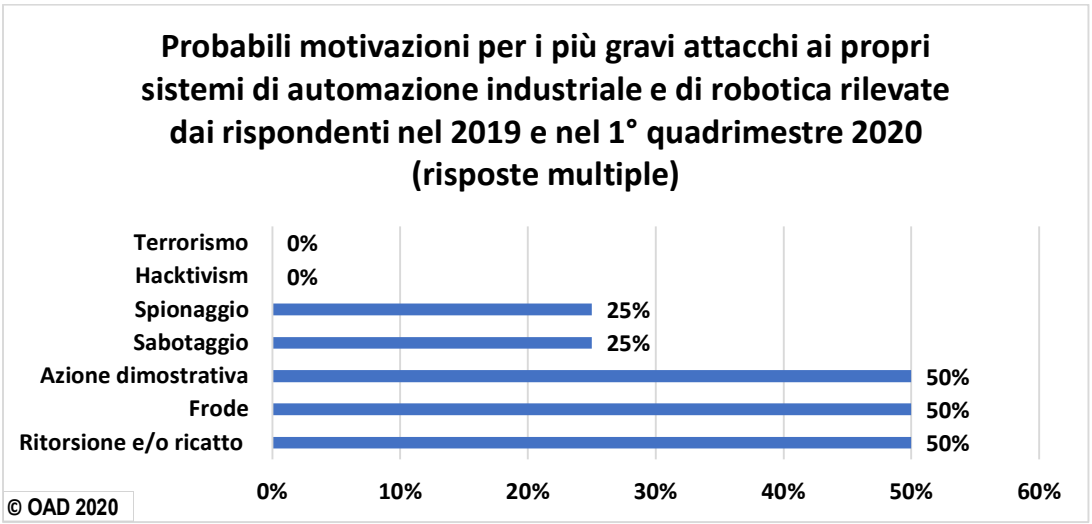


Fig. 6.14-4

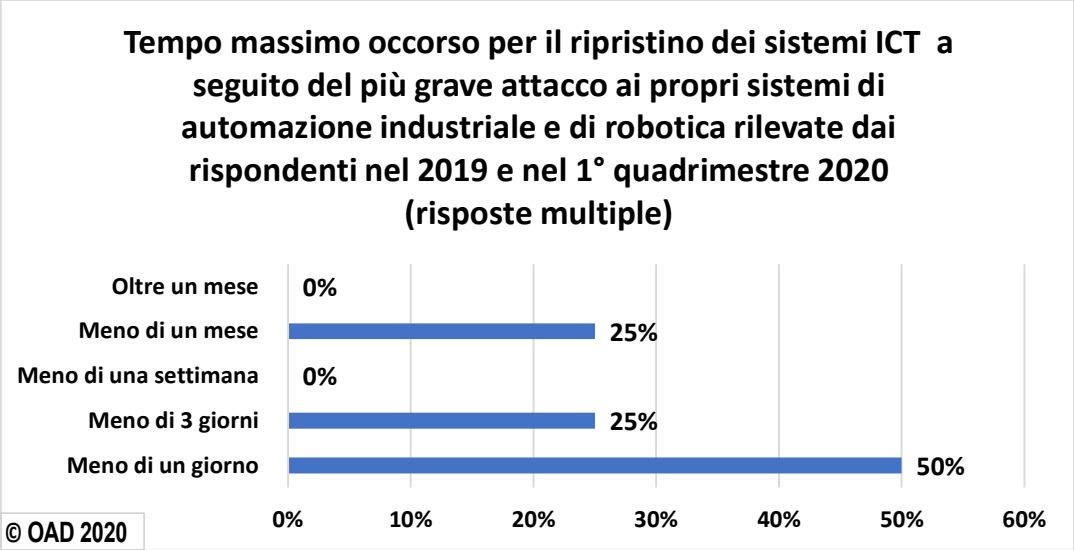


Fig. 6.14-5

6.15 Attacchi a sistemi e/o servizi basati su blockchain

La Blockchain è una tecnica introdotta nel 2008 per convalidare le transazioni e la generazione della cripto-valuta bitcoin, con l'obiettivo della libera circolazione della cripto-valuta tra gli utenti, senza o con bassi costi sulle operazioni e soprattutto senza il controllo di un organo centrale regolatore.
Questa tecnica, teoricamente sicura "*by design*", si basa sull'elaborazione distribuita ad alta affidabilità (*fault tolerance*) su consolidate tecniche di moderna crittografia (KPI) e con il consenso decentralizzato. È stata ed è tuttora utilizzata, personalizzandola, per diversi compiti in numerosi settori quali, ad esempio, la registrazione di eventi, dei record medicali, della gestione dell'identità, delle transazioni, della tracciabilità (in particolare del cibo), dell'IoT.
Blockchain usa diverse tecniche crittografiche e si basa sostanzialmente sull'assenza di 'intermediari', di un controllo centrale e sulla gestione della fiducia: la catena dei blocchi, questo il nome in italiano di blockchain, è un insieme di record (chiamati appunto blocchi), crescente (banca data distribuita), collegati tra loro e crittati.
Esistono sistemi di blockchain aperti, dove tutti possono partecipare scaricando l'opportuno programma (tipico esempio le cripto valute), e chiusi, dove solo determinati interlocutori possono partecipare. Questi ultimi sono quelli presi prevalentemente utilizzati da grandi imprese ed istituzioni per implementare loro specifiche soluzioni, alcune delle quali ancora in fase dimessa a punto.
Le tecniche di blockchain non sono a priori sicure, utilizzano i certificati di una PKI, Public Key Infrastructure, e parte della loro sicurezza digitale dipende da aspetti organizzativi, che possono cambiare nelle diverse realizzazioni specifiche. Per questo motivo OAD fin dall'edizione del 2018 ha incluso la blockchain tra le tipologie di attacco. Essa infatti è già stata più volte attaccata, e varie sue vulnerabilità tecniche sono già state identificate e classificate, ad esempio nella banca dati CVE della Mitre (si veda §).
Come per l'IoT e l'OT, dato il numero relativamente esiguo di rispondenti che hanno subito questo tipo di attacco (rispetto al totale dei compilatori del questionario 2020), i dati sulla blockchain che seguono, presentati nelle figure da 6.15-2 a 6.15-5, devono essere considerati come esempi di casi specifici, e non essere presi come riferimento della situazione in Italia sull'uso e sugli attacchi digitali a sistemi ICT che fanno uso di blockchain. Il numero di rispondenti 2020 che dispone di questi sistemi è limitato nell'ordine di circa il 5% rispetto a tutte le Aziende/Enti che hanno risposto al questionario.

Correlando e analizzando i dati acquisiti dai rispondenti, emerge che sistemi ed i servizi basati sulla blockchain sono in uso presso i seguenti settori merceologici:

- Attività finanziarie ed assicurative: assicurazioni, banche, istituti finanziari, broker, intermediazione finanziaria, etc. (Codici Ateco M)
- Servizi ICT: consulenza, produzione software, service provider ICT, gestione Data Center, servizi assistenza e riparazione ICT, ecc. (Codici Ateco J62, J63, S95.1)
- Servizi professionali e di supporto alle imprese: attività immobiliari, notai, avvocati, commercialisti, consulenza imprenditoriale, ricerca scientifica, noleggio, call center, etc. (Codici Ateco L, M, N77, N78, N80, N81, N82)
- Utility: Acqua, Energia, Gas, etc. (Codici Ateco D ed E).

È interessante notare che in questa indagine 2020 le (poche) PA che hanno risposto al questionario non utilizzano sistemi/servizi con tecniche di blockchain, mentre nella passata indagine solo le PA che allora avevano risposto, costituivano l'unico settore ad aver rilevato attacchi ai loro sistemi informatici basati su tali tecniche. Le PA rispondenti ai due questionari del 2019 e del 2020 sono sicuramente diverse, ma dato l'assoluto anonimato OAD non può sapere quali PA risposero.
Tenendo presente questo contesto, l'ambito dei sistemi basati sulla blockchain dei rispondenti ha rilevato attacchi nel 2019 per l'1,9% e nel 1° quadrimestre 2020 per il 2,0%, come evidenziato nella fig. 6-7.
La fig. 6.15-1 dettaglia come non si siano rilevati, in entrambi i periodi considerati, frequenti e ripetuti attacchi (oltre a 10) ai sistemi dei rispondenti con blockchain, per le stesse ragioni espresse dall'autore commentando la fig. 6.14-1 per i sistemi OT.

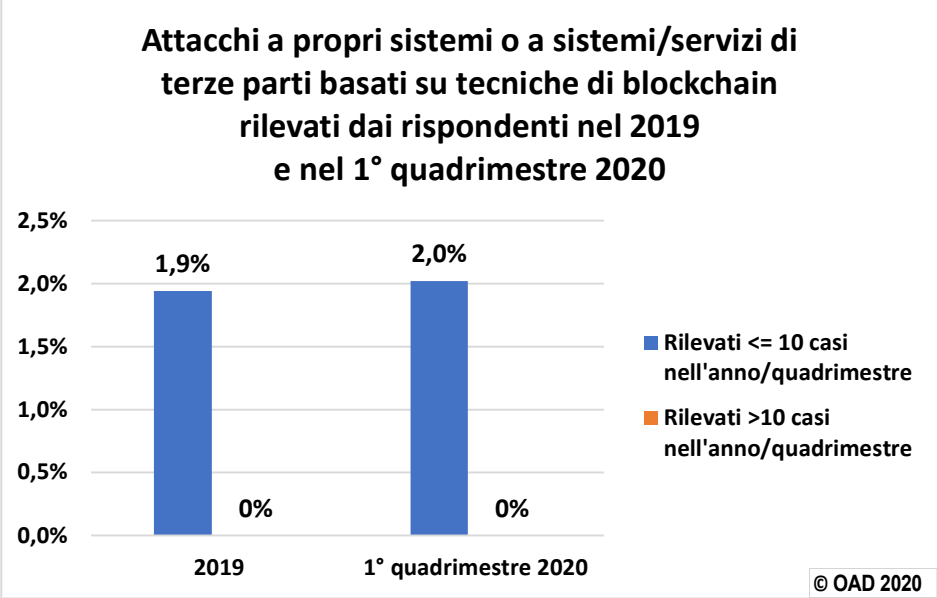


Fig. 6.15-1

Nella fig. 6.15-2, con risposte multiple, le tecniche di attacco probabilmente usate secondo i rispondenti che hanno subito questo tipo di attacco. Tre sole quelle rilevate, tutte e tre con il medesimo 50%: tecniche tipo APT, agenti autonomi, toolkit. Questo significa che gli attacchi si sono basati su tecniche sofisticate e non banali.
Gli impatti avuti dagli attacchi più gravi (fig. 6.15-3, con risposte multiple) riguardano solamente, e con lo stesso 50%, la perdita di immagine (il che significa che questi sistemi erano in produzione, non in ambito sperimentale, e conosciuti/usati da loro clienti), disservizi seri ma non gravissimi, impatti irrilevanti o gestibili in breve tempo ed a costi bassi. Come per altre tipologie di attacco

discusse nei paragrafi precedenti, alcuni rispondenti hanno avuto impatti leggeri, altri abbastanza pesanti ma non gravissimi. Ciò è altresì confermato dalle motivazioni e dai tempi massimi di ripristino per questi attacchi a blockchain.
La fig. 6.15-4 indica infatti solo due motivazioni: l'azione dimostrativa e l'hacktivism, entrambe con un 50%.
La fig. 6,15-5 evidenzia come i tempi massimi di ripristino sia avvenuti, dopo tutti gli attacchi subiti, entro 3 giorni, e per un 50% entro un solo giorno. Questo indica che i (pochi) sistemi basati su blockchain in uso presso le Aziende/Enti dei rispondenti sono molto ben monitorati e controllati, forse perché da poco passati in produzione, o ancora in una fase di sperimentazione prototipale.

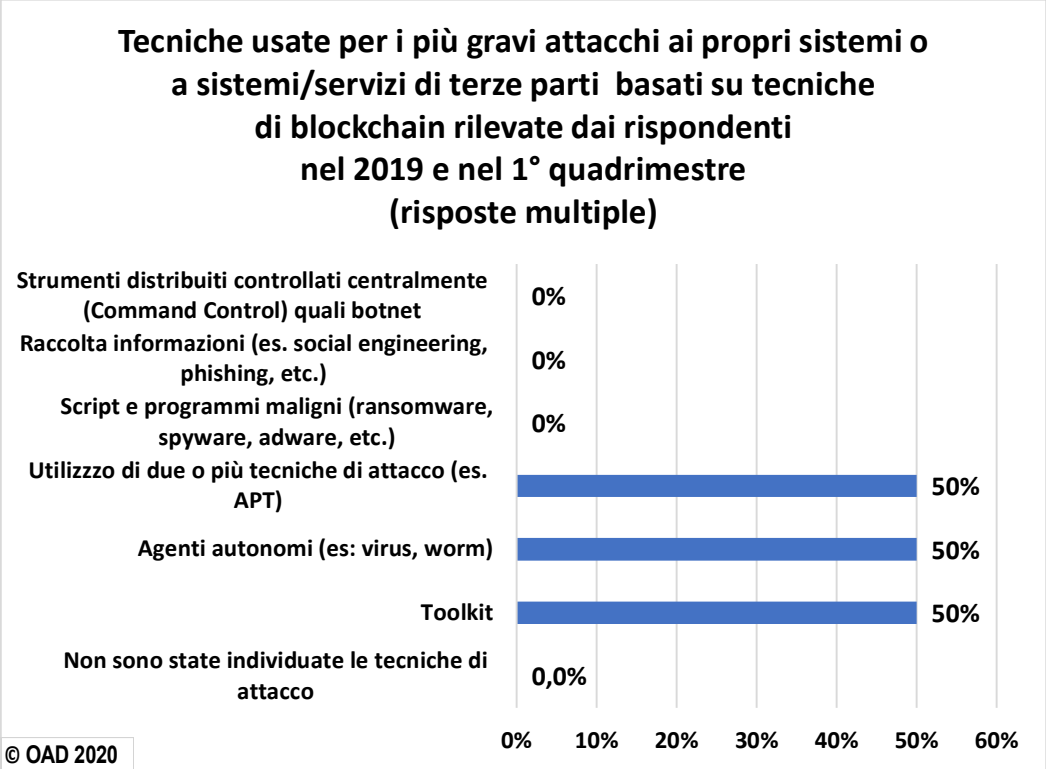


Fig. 6.15-2

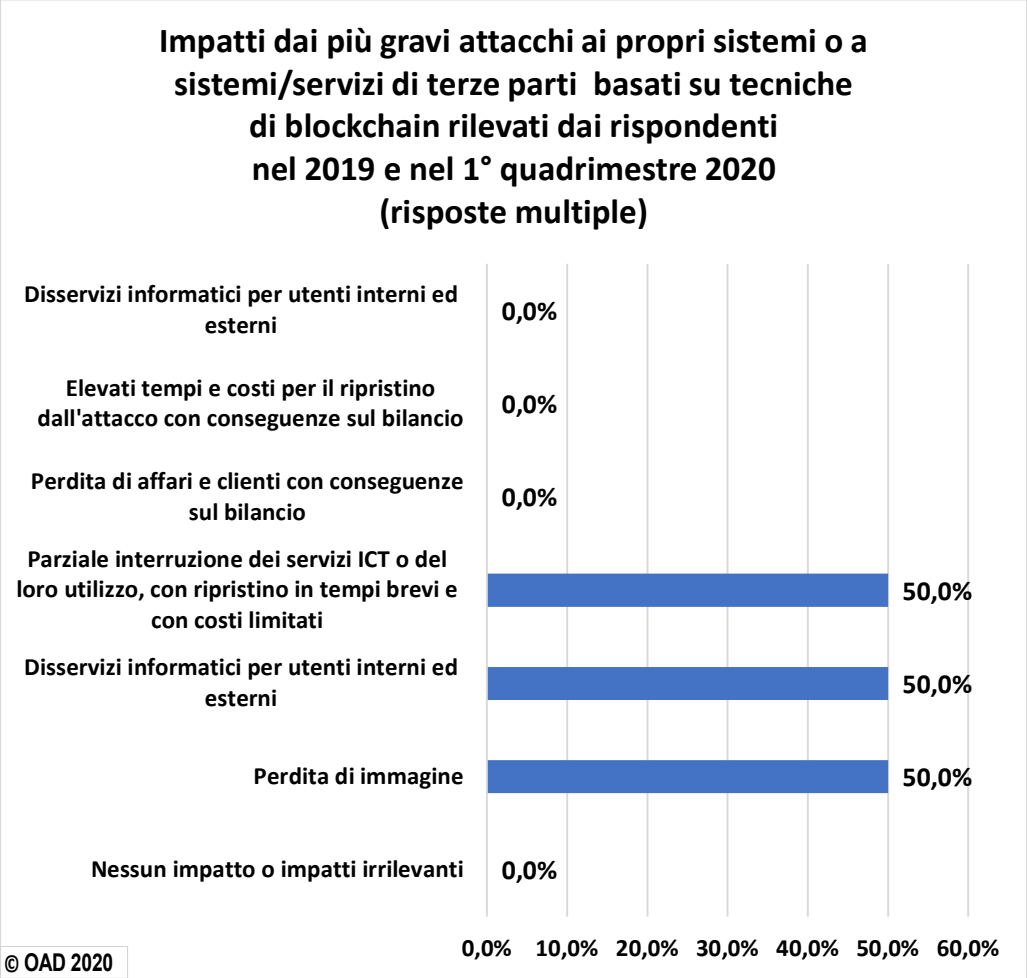


Fig. 6.15-3

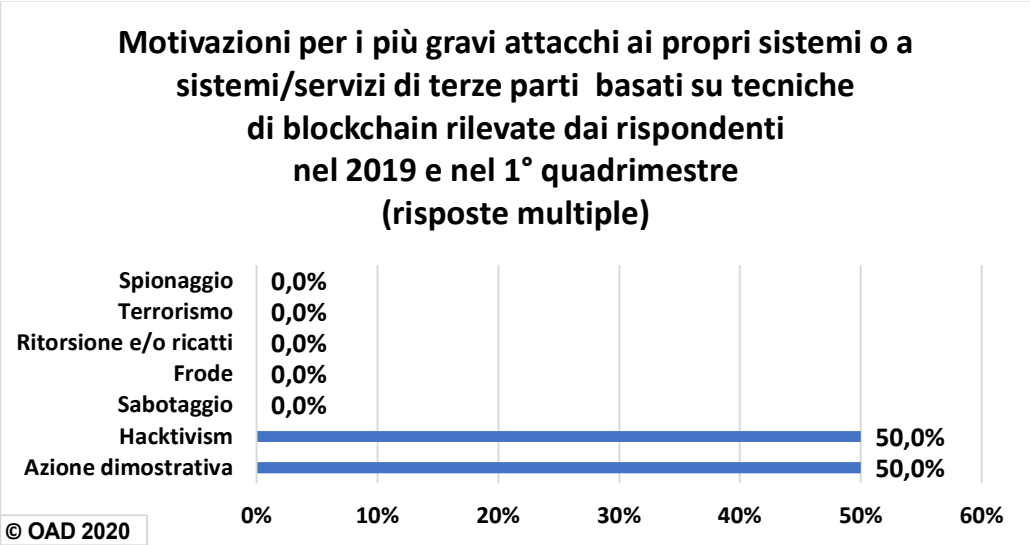


Fig. 6.15-4

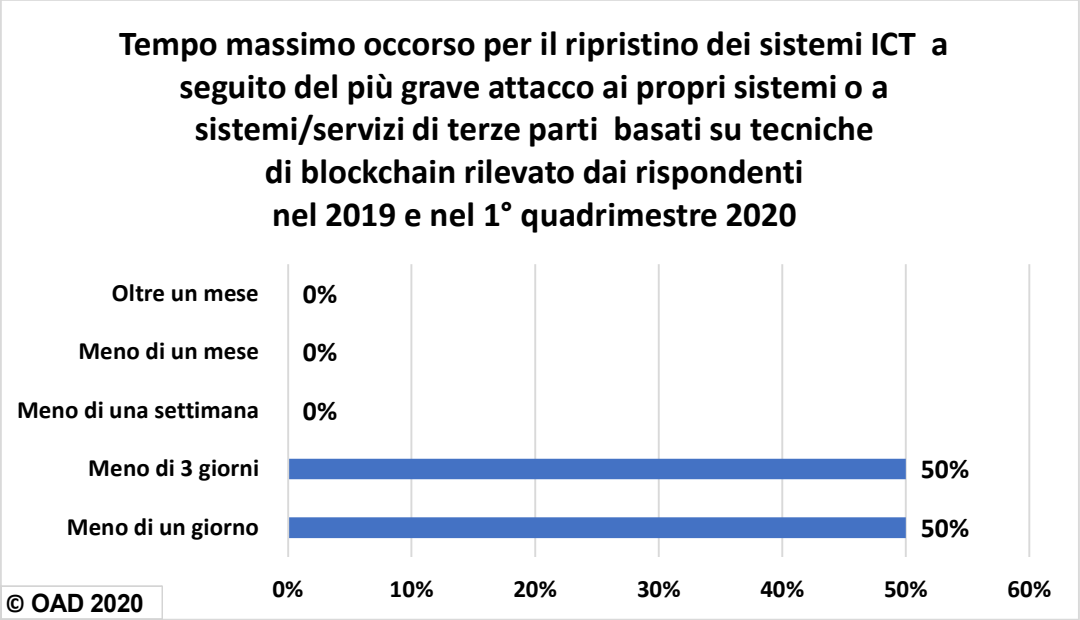

Tempo massimo occorso per il ripristino dei sistemi ICT a seguito del più grave attacco ai propri sistemi o a sistemi/servizi di terze parti basati su tecniche di blockchain rilevato dai rispondenti nel 2019 e nel 1° quadrimestre 2020
Oltre un mese
Meno di un mese
Meno di una settimana
Meno di 3 giorni
Meno di un giorno
0%
0%
0%
50%
50%
0%
10%
20%
30%
40%
50%
60%
© OAD 2020

Fig. 6.15-5

7. La rilevazione e la gestione degli attacchi, ed il loro impatto economico

Un insieme delle domande del questionario 2020 era rivolta a comprendere come e da chi vengono rilevati gli attacchi digitali e come sono gestiti.
La fig. 7-1, con risposte multiple, mostra la provenienza delle segnalazioni di un attacco che è sostanzialmente simile a quelle rilevate nelle edizioni OAD del 2019 e del 2018, confronto sempre non statistico.
Per il campione dei rispondenti, il 33,7% delle segnalazioni arriva dagli utenti privilegiati interni (amministratori di sistema, operatori ICT, etc.) ed il 30,8% dagli utenti finali interni. Positivamente il 16,3% arriva dai sistemi di monitoraggio e controllo del sistema informatico e l'11,5% dalle segnalazioni degli operatori ICT esterni, il che significa che il sistema informatico e la sua sicurezza sono in toto o in parte terziarizzate. Il 10,6% arriva dalla constatazione diretta del danno subito, ad esempio blocco dei sistemi ICT, ed il 5,8% dall'analisi dei dati raccolti (ad esempio dal monitoraggio del sistema informatico e dai log degli utenti e dei sistemi). La segnalazione dell'attacco da parte di utenti esterni è all'ultimo posto, con un 2,9%. Per comprendere ed interpretare correttamente i dati sulla segnalazione di un attacco, si ricorda che il più delle volte tali segnalazioni arrivano contemporaneamente da più fonti diverse.

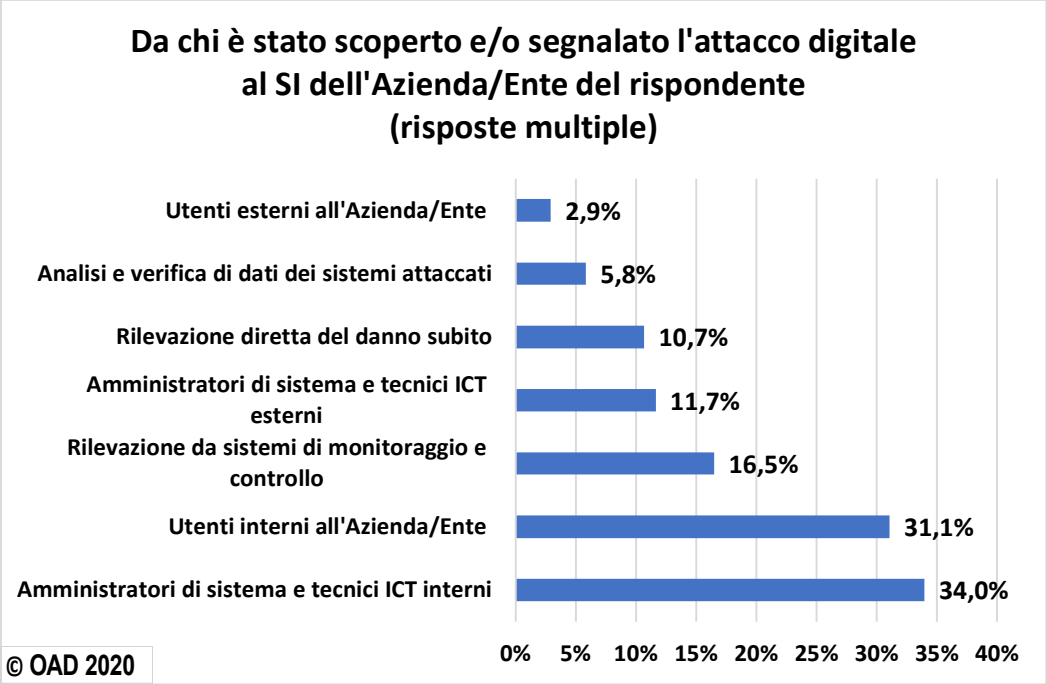


Fig. 7-1

L'eventuale comunicazione all'esterno dell'Azienda/Ente dell'avvenuto e rilevato attacco, con risposte multiple, è indicata nella fig. 7-2. Il 23,3% dei rispondenti che hanno subito attacchi digitali non comunica nemmeno i più gravi all'esterno per i motivi elencati in fig. 7-3. Il 21,4% lo comunica ai propri fornitori e consulenti, così che gli esperti/addetti ai lavori possano intervenire per ripristinare la situazione *ex ante*, e comunque capire le ragioni e l'origine dell'attacco, quali contromisure non sono state sufficienti e come migliorare il livello di sicurezza digitale. Solo il 17,5% lo comunica alle autorità competenti, tipicamente alla Polizia Postale: una percentuale quasi identica è stata rilevata

in OAD 2019. Il 3,9% dichiara di comunicarlo all'Autorità Garante, in quanto l'attacco ha riguardato (anche) dati personali, così come richiesto dal regolamento europeo sulla privacy, il GDPR, in caso di "*data breach*". Il 3,9% informa dell'attacco centri specializzati tipo Cert (si veda Allegato E2) e solo il 1,9% lo comunica alla propria assicurazione, chiaro indicatore del limitato numero di Aziende/Enti che in Italia assicura il rischio digitale.

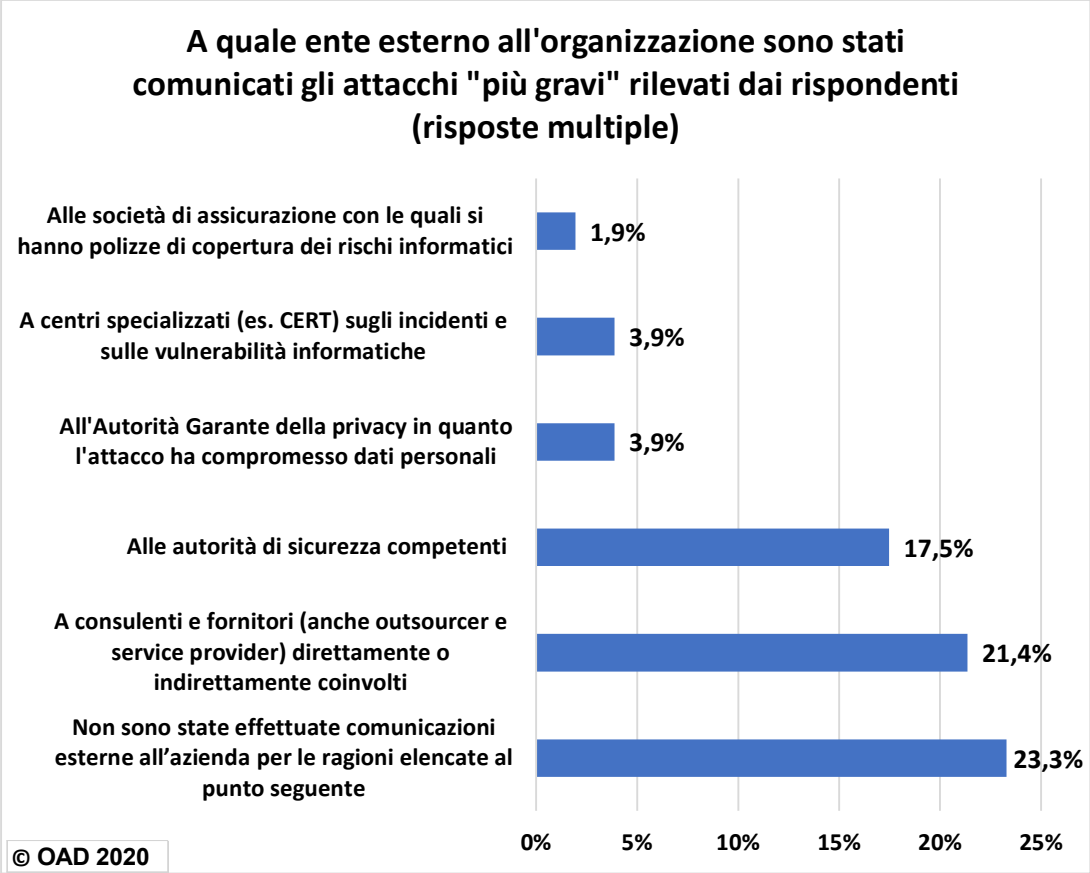


Fig. 7-2

Come indicato nella fig. 7-3, con risposte multiple, il motivo principale della mancata comunicazione dell'attacco all'esterno: per la stragrande maggioranza dei rispondenti che non l'hanno comunicato, il 96,2%, il motivo è che l'attacco non era abbastanza significativo. Al secondo posto si collocano una serie di specifiche motivazioni che i rispondenti hanno inserito sotto la voce di "Altro": nella fattispecie, comunicazione dell'attacco solo alla holding, l'attacco non ha coinvolto dati di utenti e clienti, attacco solo a propri ambienti di sviluppo/test. Un 11,5% non ha fornito comunicazioni all'esterno, in quanto non previsto e/o impedito dalle policy dell'Azienda/Ente: a giudizio dell'autore, policy assai discutibili che con il GDPR, e soprattutto con il buon senso, dovrebbero essere velocemente e profondamente modificate. Agli ultimi posti, con percentuali del 7,7%, la tutela dell'immagine e la volontà di non fornire informazioni sulle vulnerabilità e sulle misure di sicurezza digitali in atto.

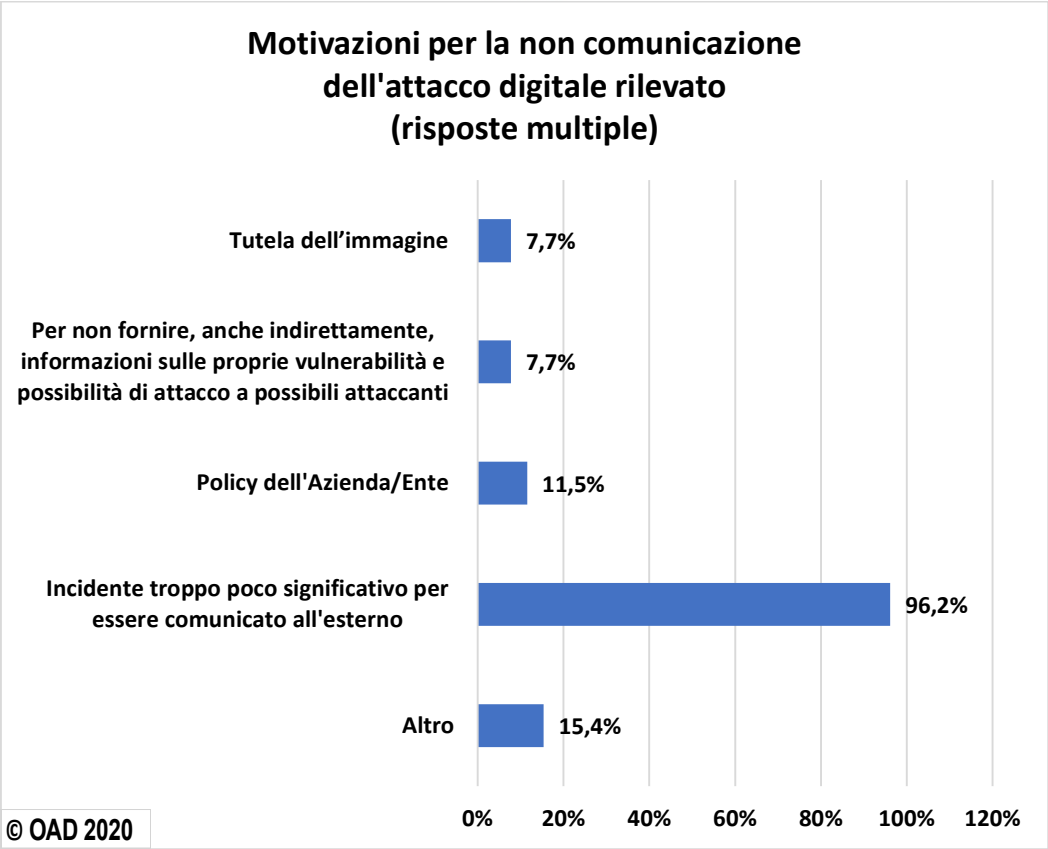


Fig. 7-3

Le azioni intraprese dalle Aziende/Enti rispondenti dopo aver subito un attacco, a parte l'eventuale comunicazione ad enti esterni sopra trattata, sono mostrate nella fig. 7-4, con risposte multiple. Tali azioni sono tra le principali per una efficace ed efficiente gestione del "dopo attacco". I tre interventi con le più alte percentuali sono l'attivazione di indagini interne con il 34%, l'attivazione di nuovi strumenti di sicurezza digitale con il 28,2% e la sostituzione degli strumenti trovati vulnerabili.
A scalare seguono gli altri interventi attuati. Da evidenziare come l'attivazione di legali, interni o esterni, e di investigatori siano agli ultimi posti, così come l'attivazione di contratti assicurativi contro il rischio e gli attacchi digitali. Con la voce "Altro" alcuni rispondenti hanno specificato di non aver intrapreso alcuna azione (lascia perplessi questa passività) ed altri rispondenti di aver pagato il riscatto richiesto dal ransomware.
Con percentuali sempre più basse gli altri interventi considerati nel questionario, con risposte multiple. Nella voce "altro" è stato specificato da alcuni rispondenti il rimpiazzo dei dispositivi ICT rubati e le modifiche di configurazione del software di base ed applicativo, per renderlo più sicuro.

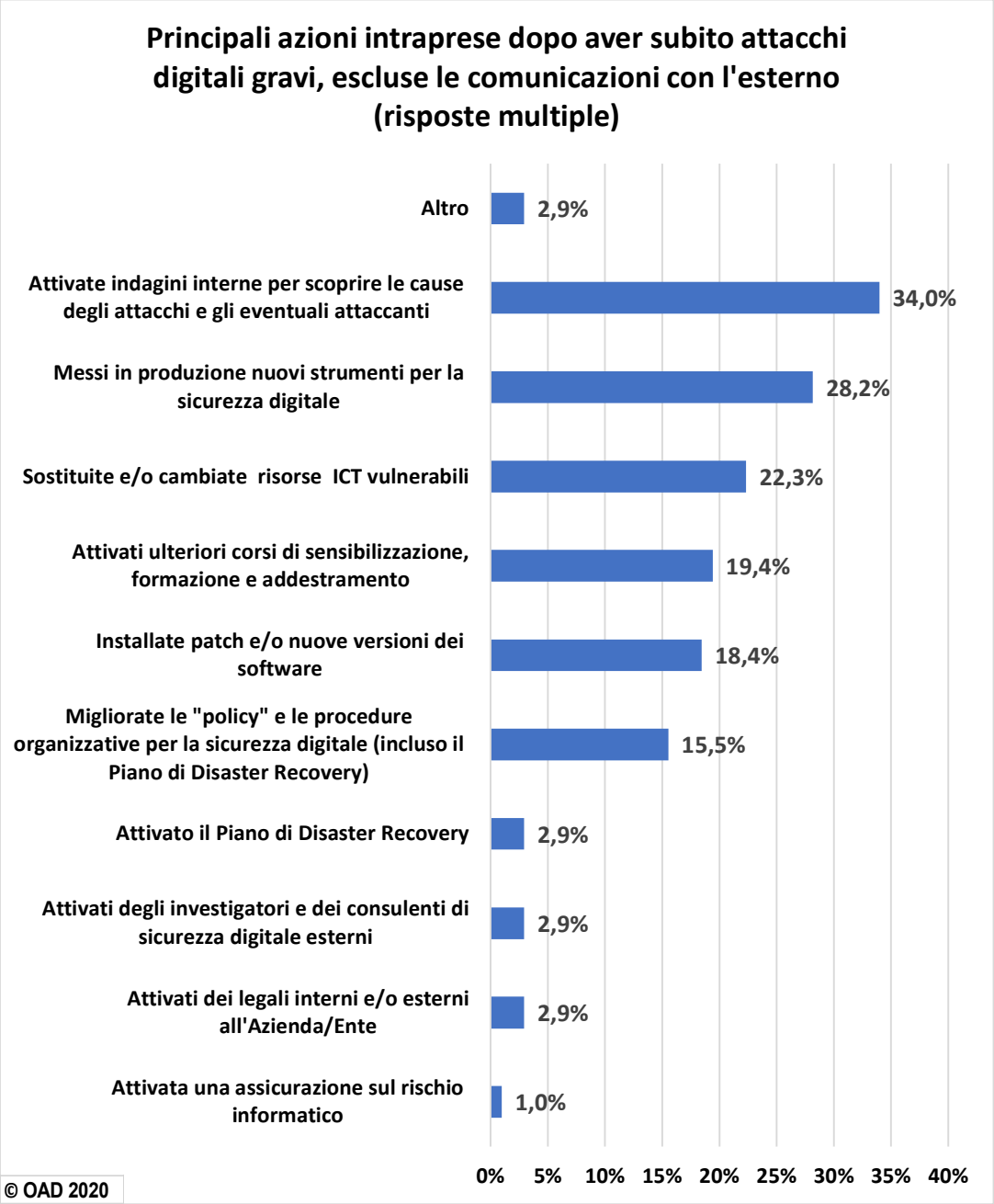

Principali azioni intraprese dopo aver subito attacchi digitali gravi, escluse le comunicazioni con l'esterno (risposte multiple)
Altro
2,9%
Attivate indagini interne per scoprire le cause degli attacchi e gli eventuali attaccanti
34,0%
Messi in produzione nuovi strumenti per la sicurezza digitale
28,2%
Sostituite e/o cambiate risorse ICT vulnerabili
22,3%
Attivati ulteriori corsi di sensibilizzazione, formazione e addestramento
19,4%
Installate patch e/o nuove versioni dei software
18,4%
Migliorate le "policy" e le procedure organizzative per la sicurezza digitale (incluso il Piano di Disaster Recovery)
15,5%
Attivato il Piano di Disaster Recovery
2,9%
Attivati degli investigatori e dei consulenti di sicurezza digitale esterni
2,9%
Attivati dei legali interni e/o esterni all'Azienda/Ente
2,9%
Attivata una assicurazione sul rischio informatico
1,0%
0% 5% 10% 15% 20% 25% 30% 35% 40%
© OAD 2020

Fig. 7-4

7.1 *L'impatto economico degli attacchi subiti*

In termini di impatto, il danno economico causato da un attacco digitale è l'elemento determinante: ogni tipo di danno può essere valorizzato in termini economici, da quello del disservizio a quello di immagine, dal tempo uomo speso per ripristinare ai nuovi eventuali strumenti da utilizzare. Come per l'impatto richiesto per ogni tipologia di attacco, anche per il danno economico è stata lasciata libertà al rispondente di considerarlo e stimarlo secondo le sue abitudini e prassi.

Nei paragrafi del Capitolo 6 sono stati riportati, per ogni tipologia d'attacco, gli impatti causati al sistema informatico e/o all'intera organizzazione dall'attacco più grave. Volutamente, per ogni tipologia d'attacco, non si è chiesto il danno economico per il più grave attacco subito di quel tipo, per non rendere troppo lunga, e difficile, la compilazione del questionario. Si è preferito chiedere in questa sezione, e senza rendere obbligatoria la risposta, la stima del costo complessivo degli attacchi per l'intero anno e/o il costo economico dell'attacco più grave, indipendentemente dalla sua tipologia.

Come nelle edizioni precedenti, in pochi hanno risposto e quelli che l'hanno fatto hanno indicato valori molti differenti, anche per le diverse dimensioni, fatturati e settori merceologici; e magari anche per la non esatta conoscenza o valutazione del danno economico effettivamente subito. Essendo il questionario assolutamente anonimo, non ci sono possibilità di verifica dell'attendibilità di dati che risultano fortemente anomali rispetto a quelli abbastanza consolidati per l'Italia e a quelli forniti da altri rispondenti.

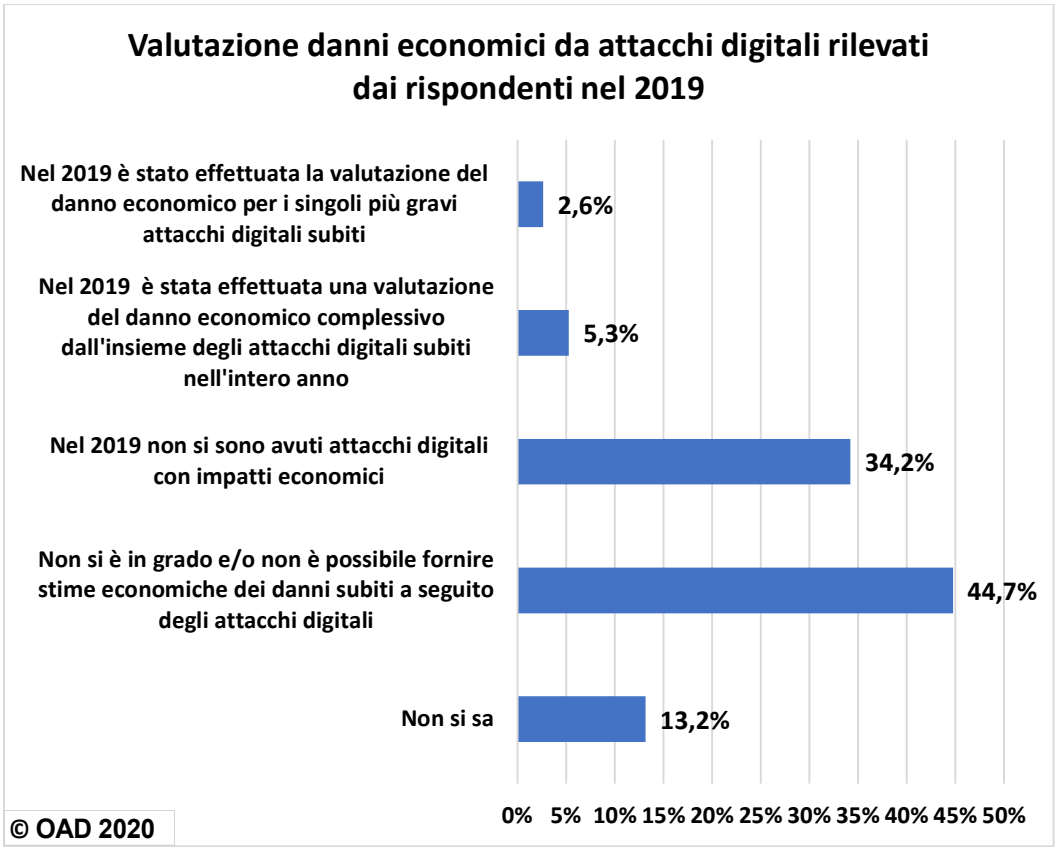


Fig. 7.1-1

Alcuni rapporti internazionali forniscono indicazioni sui costi complessivi degli attacchi digitali / data breach subiti, evidenziando la difficoltà, per le Aziende/Enti, di considerare tutti i costi diretti, indiretti e consequenziali: ma le loro analisi, con valutazioni di alcuni milioni di dollari per attacco, fanno riferimento a grandi realtà, sia pubbliche che private, ma non hanno senso per le piccole e piccolissime organizzazioni che costituisco la stragrande maggioranza delle aziende private e delle Pubbliche Amministrazioni. Dai milioni di dollari si deve passare a qualche migliaio di Euro.

La fig. 7.1-1 mostra le risposte sulla valutazione dell'impatto economico degli attacchi subiti. Il 44,7% dei rispondenti dichiara che non si è in grado o non è possibile, per policy aziendale, fornire dati economici. Il 13,2% dei rispondenti ammette esplicitamente di non conoscere la valutazione economica degli attacchi ed il 34,2% dichiara che gli attacchi digitali rilevati non avevano impatto economico: quindi attacchi digitali che sono stati gestiti nell'ordinaria amministrazione del sistema informatico e dei suoi possibili incidenti. Solo il 7,9% dei rispondenti ha effettuato valutazioni sui costi degli attacchi subiti.
Questo dato è molto significativo, ed è un indicatore della poca attenzione che ancora Aziende/Enti prestano agli attacchi digitali.

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

La fig. 8-1, 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.

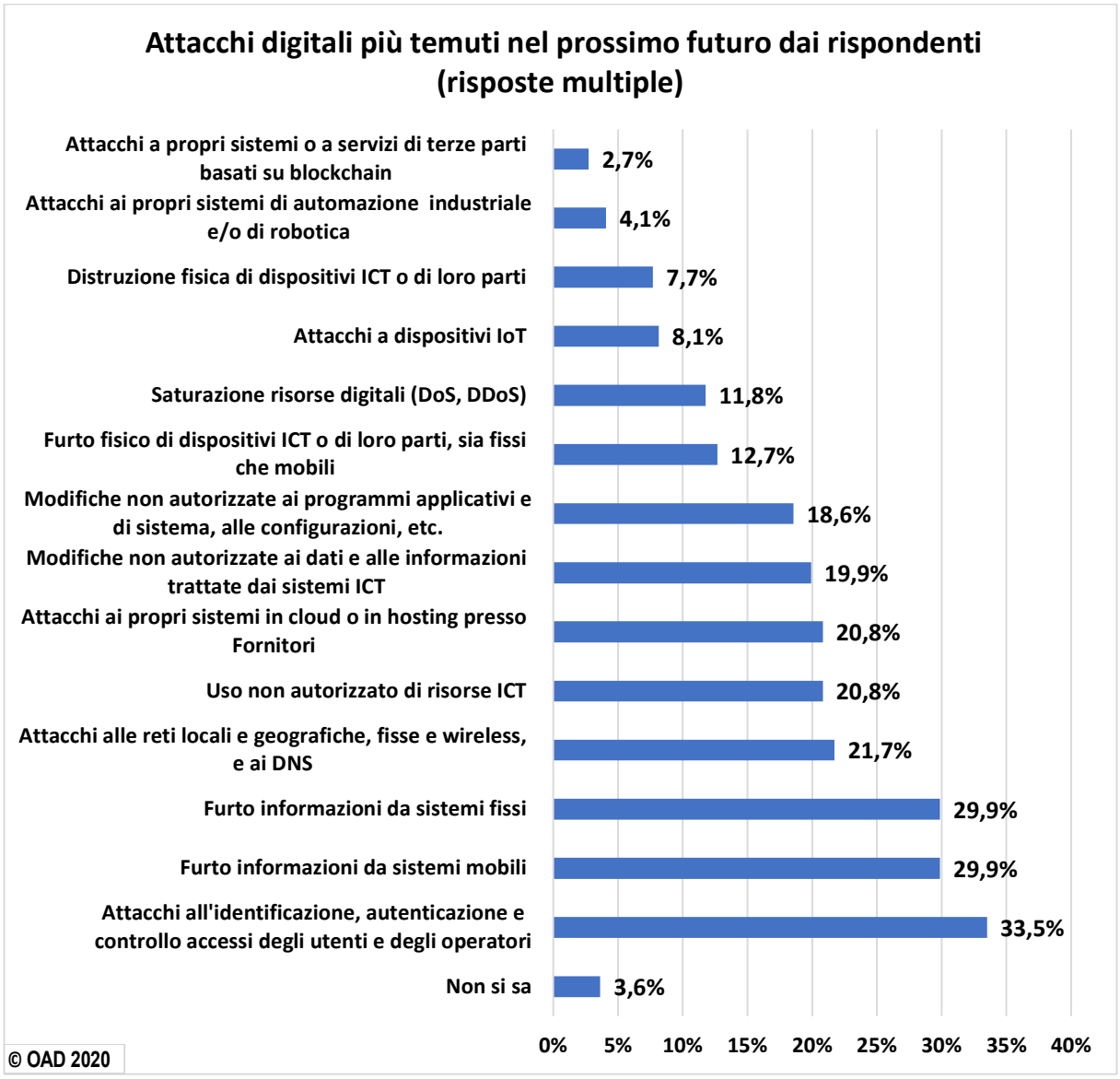


Fig. 8-1

Anche in questo caso, come per le domande sugli impatti in ogni tipologia d'attacco del Cap. 6, non si è volutamente specificato quali siano i criteri per considerare un attacco più pericoloso e critico, lasciando libertà al rispondente (sempre strettamente anonimo) di rispondere secondo il suo giudizio e la sua esperienza.

Come è ragionevole aspettarsi e come si è verificato anche nelle precedenti indagini di OAD/OAI, rimangono per il futuro forti timori per alcuni degli attacchi più diffusi rilevati negli anni precedenti, e in particolare nel 2019 e nel 1° quadrimestre 2020 (si veda fig. 6-7).
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.
L'andamento scalare con piccole differenze tra le diverse tipologie di attacco della fig. 8-1 è simile a quella dell'edizione precedente, ed è un interessante indicatore di come non ci sia una singola tipologia fortemente e chiaramente temuta più delle altre: al di là degli attacchi in aree specifiche come OT, IoT e blockchain, tutti gli altri rientrano in una fascia tra il 10 ed il 33%. Unica eccezione è quella della distruzione fisica di sistemi ICT o di loro parti: è temuta solo dal 7,7% dei rispondenti, anche se nel 2019 lo stesso bacino di rispondenti ha rilevato questo attacco al 25,2%, posizionandolo al terzo posto tra quelli più diffusi. Questa non è una contraddizione: un attacco può verificarsi per vari motivi, ma questa tipologia in particolare è relativamente facile da proteggere, con misure di sicurezza fisica e limitando gli accessi fisici al personale, ed è anche relativamente facile da ripristinare con copie di scorta ed acquisti specifici. Non rappresenta quindi un forte timore, come altre tipologie invece fanno.

La fig. 8-2, 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.

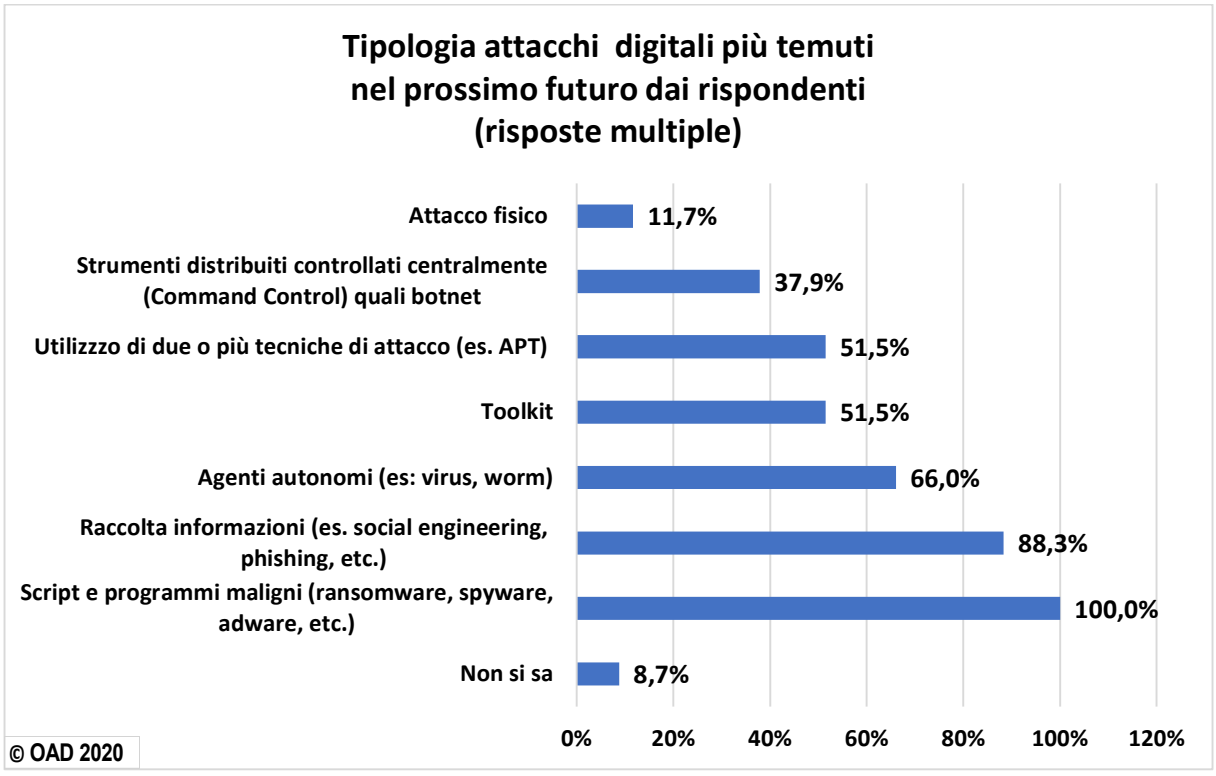


Fig. 8-2

Come evidenziato nel commento alla figura precedente, anche questa concentrazione percentuale relativamente forte tra le sette famiglie tecniche di attacco indica che per attacchi futuri più critici e più temuti, i rispondenti ritengono che quasi tutte queste tecniche d'attacco potranno essere utilizzate, ed anche in maniera contemporanea e persistente. Anche tra le tecniche d'attacco, quella fisica è la meno temuta, per le ragioni già evidenziate commentando la figura precedente.
La fig. 8-3, con risposte multiple, mostra le principali motivazioni ipotizzate per i futuri attacchi: la frode è di gran lunga la motivazione più votata, con una percentuale quasi doppia rispetto alla seconda, la ritorsione/ricatto. Seguono, decrescendo con pochi punti di stacco le altre possibili motivazioni, posizionandosi all'ultimo il terrorismo.

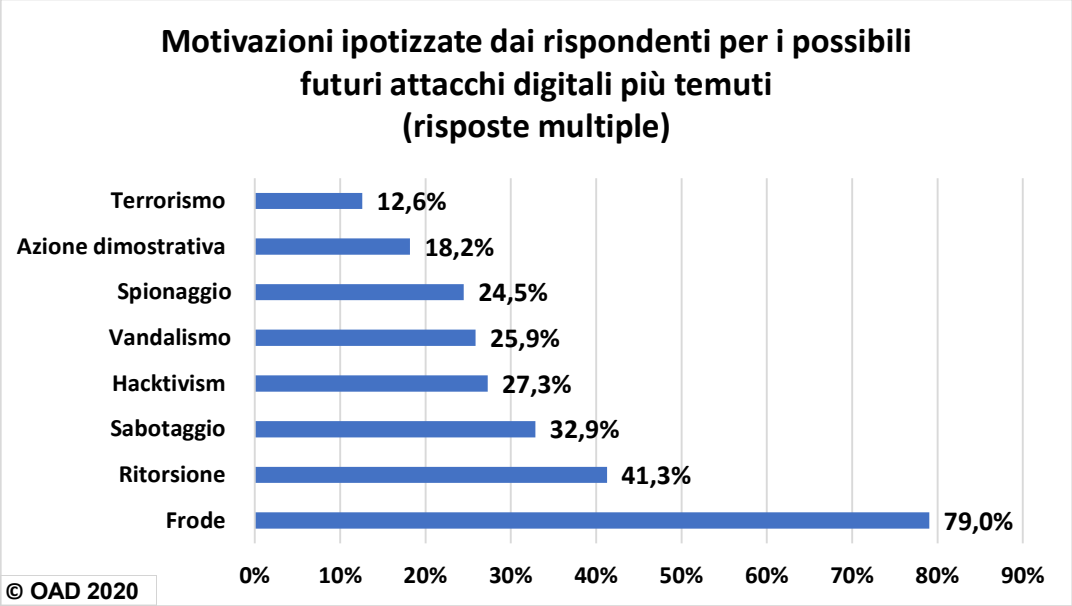


Fig. 8-3

9. Strumenti e misure di sicurezza digitale adottate nelle Aziende/Enti dei rispondenti

Il seguente capitolo descrive gli strumenti di sicurezza in uso nei sistemi informatici delle Aziende/Enti dei rispondenti, le cui macro-caratteristiche sono descritte in §10.3, così da poter meglio comprendere in quali ambiti e con quali livelli di sicurezza di contrasto sono stati attuati gli attacchi rilevati e riportati nel Capitolo 6. Gli strumenti e le misure per la sicurezza digitale sono raggruppati in tre sezioni: misure organizzative, misure tecniche, misure per la gestione operativa ("management") della sicurezza digitale.
Le misure di gestione sono un mix di misure organizzative e di strumenti tecnici: l'attribuzione di alcune misure in quale sezione, sempre discutibile, è stata effettuata dall'autore nell'ottica di una maggior chiarezza concettuale e sulla base della sua esperienza.
Il questionario 2020 OAD ha semplificato e modificato, rispetto agli anni precedenti, le domande e le risposte preimpostate delle sezioni sul Sistema Informatico (SI), sulle sue misure di sicurezza digitale in essere e sull'Azienda/Ente del rispondente per poter valutare il livello di sicurezza digitale, con le modalità descritte nell'Allegato A.
È bene infine ricordare che il presente rapporto non è un testo esplicativo della sicurezza digitale, ma la presentazione commentata dei principali dati emersi dall'indagine OAD 2020. Molti concetti sulla sicurezza di base, in particolare quelli di base, sono pertanto dati per conosciuti al lettore del presente rapporto.

9.1 Misure organizzative per la sicurezza digitale

Gli aspetti organizzativi sono determinanti per l'attuazione e la gestione di una effettiva ed efficace sicurezza digitale, dato che le maggiori vulnerabilità, e le più difficili da eliminare o ridurre, sono proprio quelle delle persone e delle organizzazioni nelle quali operano.
Gli aspetti organizzativi sono talvolta trascurati, soprattutto dalle piccole strutture, perché considerati prevalentemente come oneri burocratici e spese di consulenza non necessarie: di interesse, di fatto, solo per le grandi organizzazioni. Sono invece misure essenziali per l'effettivo funzionamento della sicurezza digitale, e necessarie per qualsiasi tipo di organizzazione, indipendentemente dalle sue dimensioni: devono però essere commisurate e calate nelle specifiche realtà di ogni Azienda/Ente.
Le misure organizzative considerate nel questionario OAD includono la struttura organizzativa per la sicurezza digitale interna all'azienda/ente, il suo posizionamento nell'organigramma complessivo, l'esistenza di policy e di procedure organizzative, i ruoli, le competenze e le certificazioni richieste all'interno della struttura ed ai fornitori ICT, le best practice e gli standard seguiti, la sensibilizzazione, formazione e addestramento sia degli utenti finali sia degli utenti privilegiati interni ed esterni (operatori ed amministratori di sistema, sviluppatori software, manutentori sistemi ICT, system integrator, etc.), attività di audit interno e/o esterno.
Il regolamento europeo per la privacy, il GDPR, richiede l'attuazione di gran parte delle misure organizzative considerate, e l'obbligatorietà della conformità ad esso, in vigore dal 25/5/2018 per tutte le Aziende/Enti della Comunità Europea, con significative pene pecuniarie in caso di inadempienza[15], dovrebbe favorire una maggior attenzione su questi aspetti: ma come si vedrà nel seguito, soprattutto per le piccole e piccolissime organizzazioni si è ancora assai lontani da quanto dovrebbe essere effettuato per ottemperare realmente alla normativa.
Quanto emerge dall'indagine OAD 2020, così come dalle precedenti, conferma che le Aziende/Enti del campione, pur diversificato, presentano un livello di sicurezza digitale di medio-alto livello all'interno del contesto italiano, soprattutto per le Aziende/Enti di più grandi dimensioni.

[15] 1) una multa fino a 10 milioni di euro, o fino al 2% del volume d'affari globale registrato nell'anno precedente nei casi previsti dall'Articolo 83, Paragrafo 4 del GDPR (violazione obblighi dei titolari e dei responsabili)
2) una multa fino a 20 milioni di euro o fino al 4% del volume d'affari nei casi previsti dai Paragrafi 5 e 6 dello stesso articolo del GDPR (violazione principi base, diritti interessati, trasferimenti, ordini del Garante)

Le attività pluriennali di sensibilizzazione e di trasferimento di conoscenza grazie a riviste, convegni, associazioni di categoria e specifiche di settore, come AIPSI, hanno contribuito, e tuttora stanno contribuendo, in tal senso, ma ancora troppo lentamente. Come già evidenziato nei capitoli iniziali, la pandemia del Covid-19 ha fatto esplodere l'agile working, ma prevalentemente con processi, procedure, logiche e modalità identiche a quelle applicate in ufficio anche per il lavoro da casa/da remoto: perdendo così l'opportunità, almeno per il momento, di ripensare e ri-progettare le modalità di lavoro nei contesti e con il forte supporto di risorse digitali. In tal senso, si sono rese sempre più evidenti le carenze tecniche su molti aspetti del digitale in Italia, a partire dalla sua sicurezza.

9.1.1 La struttura organizzativa per la sicurezza digitale

La prima misura organizzativa per la sicurezza digitale è data dalla definizione del ruolo e delle responsabilità di chi ne è, o dovrebbe essere a capo: il responsabile della sicurezza digitale, indicato anche nel seguito con l'acronimo inglese di CISO, Chief Information Security Officer.
La fig. 9.1.1-1 mostra che il ruolo del CISO è formalizzato[16] e attuato dal 44% delle organizzazioni dei rispondenti, soprattutto dalle organizzazioni di grandi dimensioni, per il 60,9%, come indicato in fig. 9.1.1-2. Interessante notare come tale ruolo, le sue funzioni e responsabilità siano definite ed attuate anche nelle piccole e piccolissime strutture: del loro complessivo 39,1%, un 10,9% è per strutture organizzative con <10 dipendenti. Questo dato riflette ancora una volta come le Aziende/Enti dei rispondenti a OAD 2020 siano nella fascia medio-alta in termini di livelli di sicurezza
La fig. 9.1.1-3 mostra in quali strutture organizzative sono svolte le funzioni e le attività del CISO, indipendentemente che il suo ruolo sia definito e formalizzato oppure no. Nel primo caso, con ruolo definito e attuato all'interno dell'organizzazione, il CISO ed il suo personale possono operare nell'ambito dell'UOSI[17], Unità Organizzativa Sistemi Informatici, diretta dal CIO, Chief Information Officer, per il 29,4% dei rispondenti oppure in un'altra struttura organizzativa dell'Aziende/Ente, ma non nell'ambito UOSI, per il 14,7%.

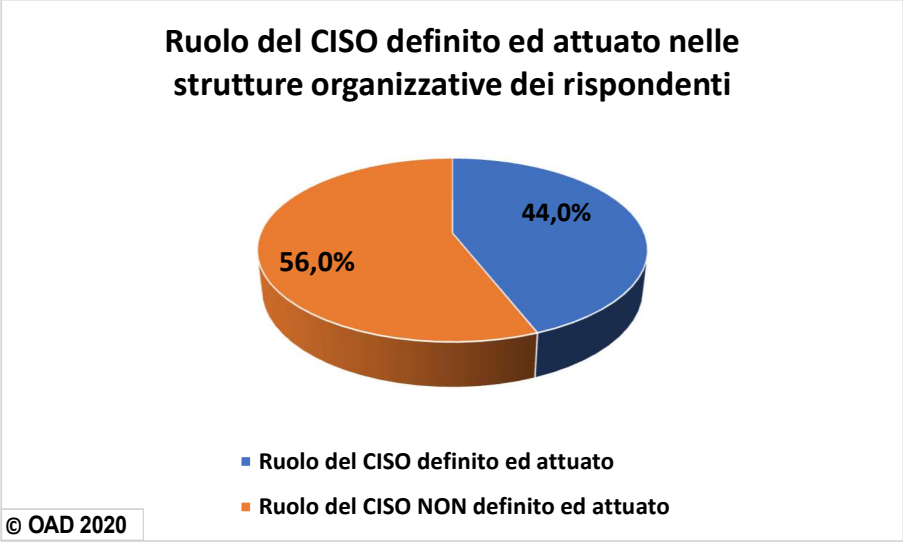


Fig. 9.1.1-1

[16] 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
[17] Si è preferito usare nell'intero rapporto il generico termine di UOSI per rendere tale struttura organizzativa indipendente dal suo posizionamento nell'organigramma. In Italia è ancora raro, e solo presso grandi organizzazioni, che il CIO sia un responsabile di primo livello e che la sua struttura sia quindi una Direzione.

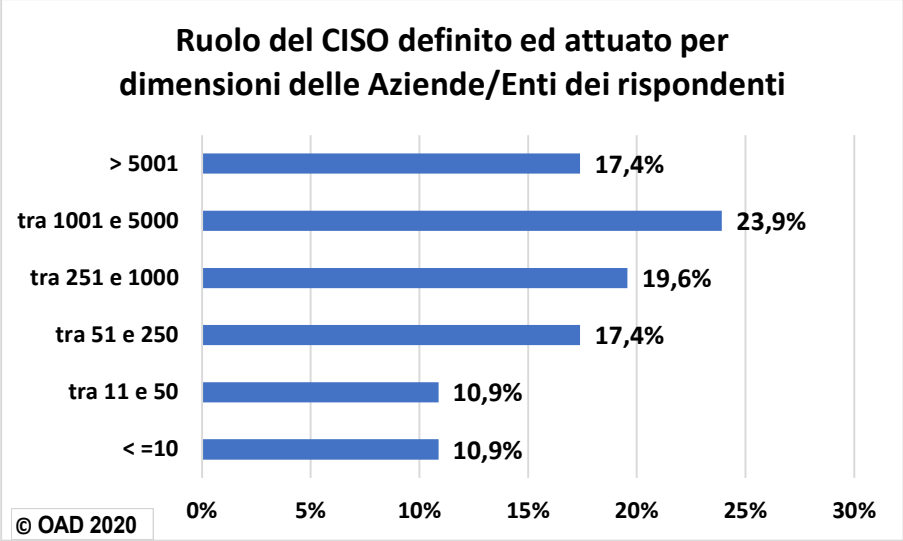


Fig. 9.1.1-2

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.
In alcune grandi organizzazioni, soprattutto in ambito finanziario, il CISO è allocato con le persone che con lui operano in altre strutture interne, ad esempio nell'ambito della struttura del CSO oppure in staff alla Direzione Generale, oppure nelle Direzione Personale e Organizzazione. Per le aziende facenti parti di holding questo ruolo è svolto, nella maggior parte dei casi, nell'ambito della struttura organizzativa della holding stessa. Si deve però tener conto che le più recenti best practice e framework, quali COBIT e ITIL, hanno in parte superato il principio della separazione delle responsabilità per favorire la velocità delle decisioni e dei conseguenti interventi: tipico, in questo senso, l'integrazione dello sviluppo di un software con la sua messa in produzione nella logica Devops[18].

[18] Con il termine DevOps si intende un approccio che combina (tendenzialmente fino ad integrare) lo sviluppo del software (dev) con la gestione operativa dei sistemi informatici (ops), con l'obiettivo di ridurre il ciclo di vita dello sviluppo e realizzazione di sistemi ICT, e di fornire un miglioramento continuo dello sviluppo e dell'operation con elevati livelli di qualità.

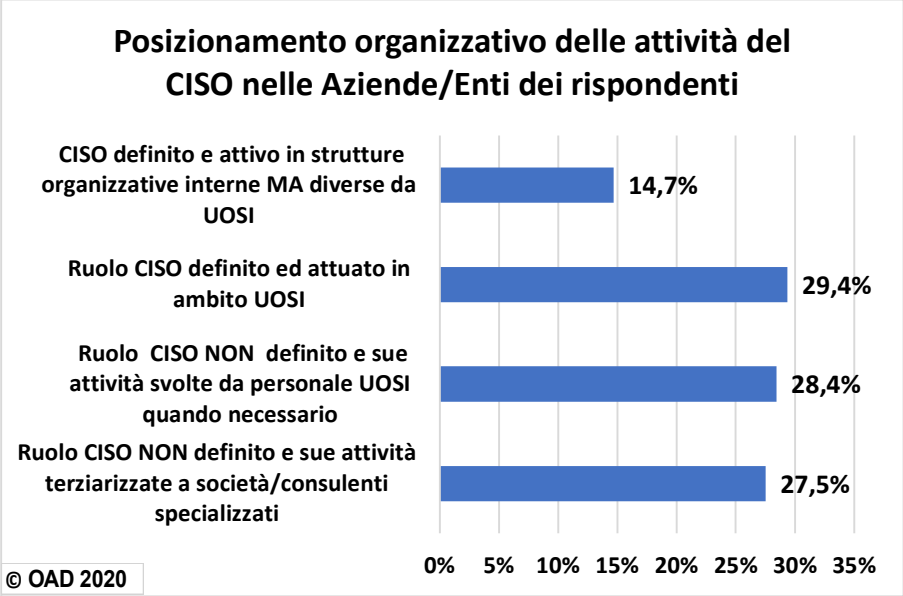


Fig. 9.1.1-3

Per le Aziende/Enti dei rispondenti che non hanno previsto formalmente nelle loro organizzazioni interne un CISO, e sono la maggioranza, due sono le soluzioni di fatto in atto, più o meno con la stessa percentuale: o la terziarizzazione della funzione del CISO e del suo mansionario a consulenti o a società specializzate esterne, oppure far svolgere, quando necessario, gli interventi sulla sicurezza digitale da personali interno all'UOSI. In quest'ultimo caso, de facto il ruolo del CISO è svolto direttamente dal CIO.
Di terziarizzazione della sicurezza digitale si è già parlato in §4: è e sarà un fenomeno crescente soprattutto in Italia, dato il numero di PMI e di analoghe piccole-medie strutture nelle PA, soprattutto nelle PAL. Ma il dato rilevato nell'attuale indagine OAD, 27,5%, è ancora limitato, e dello stesso ordine di grandezza di quello emerso, 23,3%, in OAD 2019, e comunque percentualmente più alto di quelli emersi nelle indagini precedenti, dal 2018 in giù. Questo significa che il trend di crescita della terziarizzazione è in atto, ma con tempi finora lunghi che forse si ridurranno a causa della pandemia ancora in corso.
Occorre poi distinguere tra terziarizzazione del ruolo del CISO, tipicamente ad un consulente, e terziarizzare la sicurezza digitale, soprattutto nella sua parte di gestione operativa. Gli aspetti strategici, e le conseguenti decisioni, possono essere aiutate e facilitate da consulenti anche direzionali, ma devono, o dovrebbero, essere sempre in carico al vertice dell'Azienda/Ente.

9.1.2 Policy e procedure organizzative per la sicurezza digitale

Una policy su un determinato tema, nel contesto della sicurezza digitale, definisce le linee guida e gli indirizzi, il più delle volte con valenza pluriennale e strategica, ed è rilasciata, o comunque sottoscritta e validata, dal vertice dell'Azienda/Ente. Si usa di preferenza il termine inglese "policy", in quanto l'equivalente termine "politica" in italiano o è ben dettagliato o può creare confusione.
Le procedure organizzative, da non confondere con le policy, forniscono dettagliate istruzioni sia organizzative sia tecniche su come comportarsi per svolgere specifiche attività e per far fronte a determinate situazioni, e sono rivolte sia alle persone che svolgono determinati ruoli, sia alle strutture organizzative che debbono espletare e/o controllare talune attività, funzioni e processi: ad esempio, dalla effettuazione dei back up ai ripristini, dalla creazione e gestione degli account alla gestione delle emergenze e dei problemi.
Le policy e le procedure organizzative fanno spesso riferimento a normative che occorre rispettare per legge o per avere specifiche certificazioni, ad esempio per la sicurezza digitale o per la

governance del sistema informatico con standard della famiglia ISO e best practice quali i già citati ITIL e COBIT.
Policy e procedure organizzative scritte, fatte conoscere ed aggiornate periodicamente, non sono da considerare un' inutile e costosa burocrazia, e nemmeno attività solo per Aziende/Enti di grandi dimensioni: sono necessarie ed utili per formalizzare e divulgare documentazione su come usare e gestire le risorse ICT e la loro sicurezza ad utenti finali e privilegiati, e fornire specifiche indicazioni alle terze parti che possono essere coinvolte nella gestione e/o nel governo del sistema informatico. Sono inoltre essenziali per dimostrare l'accountability[19], così come richiesto ad esempio dal GDPR, e più in generale da varie leggi e normative, e non solo per l'ICT.

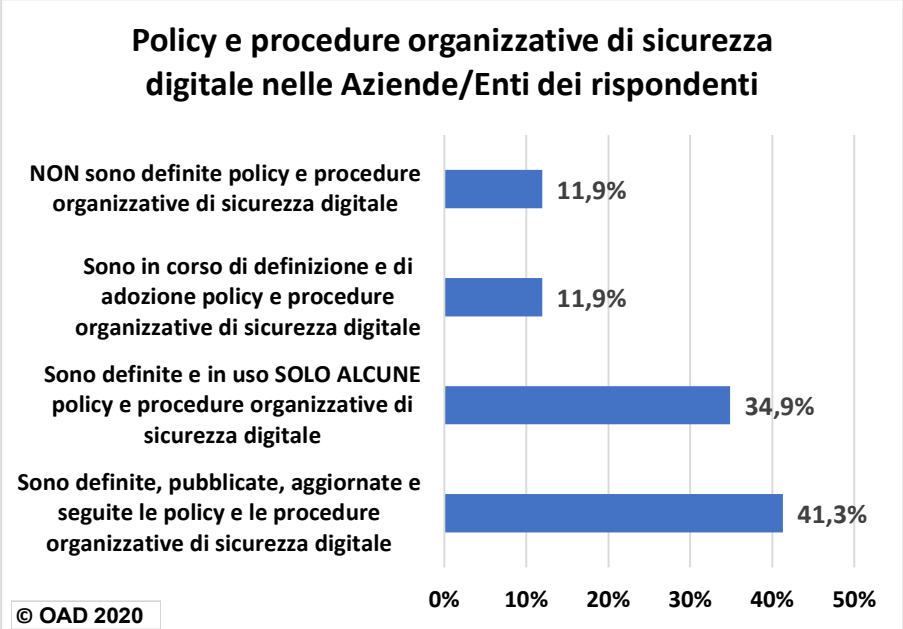


Fig. 9.1.2-1

La fig. 9.1.2-1 mostra che la maggior parte delle Aziende/Enti, il 76,1%, ha definito ed usa policy e procedure organizzative sulla sicurezza digitale. L'11,9% le sta definendo, sicuramente sotto la spinta delle varie normative, in primis il GDPR per la privacy, mentre un altro 11,9% non le ha ancora definite. Situazione insperatamente positiva, che deriva dalla fascia medio-alta del bacino dei rispondenti in quanto ad adozione di misure di sicurezza digitale.

La fig. 9.1.2-2, con risposte multiple, presenta la situazione tra i rispondenti sulle procedure organizzative inerenti l'ICT e soprattutto la sua sicurezza. Percentualmente l'uso di procedure organizzative risulta di poco inferiore rispetto a quelle delle policy della figura precedente: questo dato conferma la tendenza purtroppo assai diffusa in ogni tipo di Azienda/Ente in Italia a definire, magari in maniera molto generica, succinte policy così da poter dimostrare il formale adempimento a obblighi di leggi e normative, ad esempio del GDPR, ma a non definire procedure operative - assai più utili e necessarie per l'operatività sui sistemi informatici, ma che richiedono ben maggior impegno sia nella stesura che nell'aggiornamento. Le procedure più diffuse tra i rispondenti sono quelle per gli utenti finali con il 37,1%, mentre quelle per gli utenti privilegiati, nella pratica assai più importanti, scendono al quinto posto con il 21,7%. Con la medesima percentuale le procedure organizzative sono in fase di stesura, e il 12,7% ammette che non esistono. Interessante evidenziare come al

[19] Il termine "accountability" significa responsabilizzazione nei vari ruoli che sono tenuti a dimostrare che le loro azioni ed attività sono coerenti con quanto richiesto dalla normativa, che hanno piani ed iniziative per mettere in atto le idonee misure tecniche e organizzative, che possono comprovarne l'adeguatezza anche tramite adeguati strumenti.

secondo posto, con il 25,8%, siano le procedure per il Disaster Recovery, DR, probabilmente all'interno di un più generale piano di continuità operativa (business continuity): in merito si veda anche §9.3.

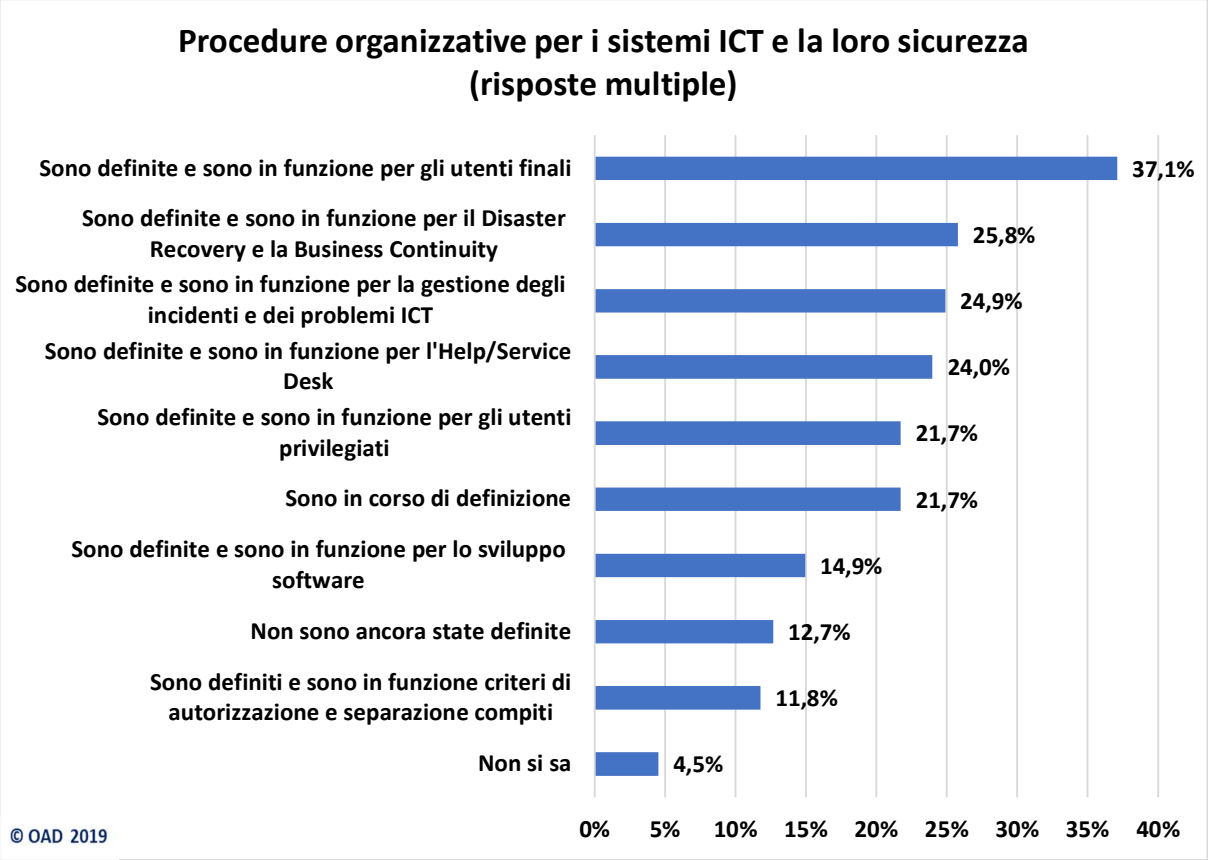


Fig. 9.1.2-2

Due procedure organizzative in particolare sono essenziali per la sicurezza digitale: la gestione degli incidenti e la gestione delle emergenze, e tra queste ultimi un eventuale "disastro".

La fig. 9.1.2-3 mostra la situazione delle procedure organizzative per la gestione degli incidenti. Il 62,2% dispone di queste procedure ed ha a disposizione un Help Desk, al proprio interno o terziarizzato, cui gli utenti possono fare riferimento via telefono, via posta elettronica o un'applicazione ad hoc, chiamata "Trouble Ticketing", che consente di emettere una segnalazione, il ticket, che viene inoltrato a chi può risolvere il problema posto e che a sua volta segnala tramite l'applicazione l'avvenuta risoluzione o che cosa si sta facendo. Questa applicazione permette di registrare e misurare i tempi di risposta e di risoluzione dei problemi posti.
Il 20,7%, pur avendo procedure organizzative in merito, non dispone di Help Desk e tanto meno di un'applicazione di Trouble Ticketing, e gli utenti, quando hanno un problema, chiamano una persona dell'UOSI, Unità Organizzativa Sistemi Informatici, che ritengono in grado di risolvere il loro problema, o una Terza Parte, Società o singola persona, che collabora tecnicamente sui sistemi informatici: tipicamente è il personale di assistenza di sistemi e di applicazioni acquisite dall'Azienda/Ente.

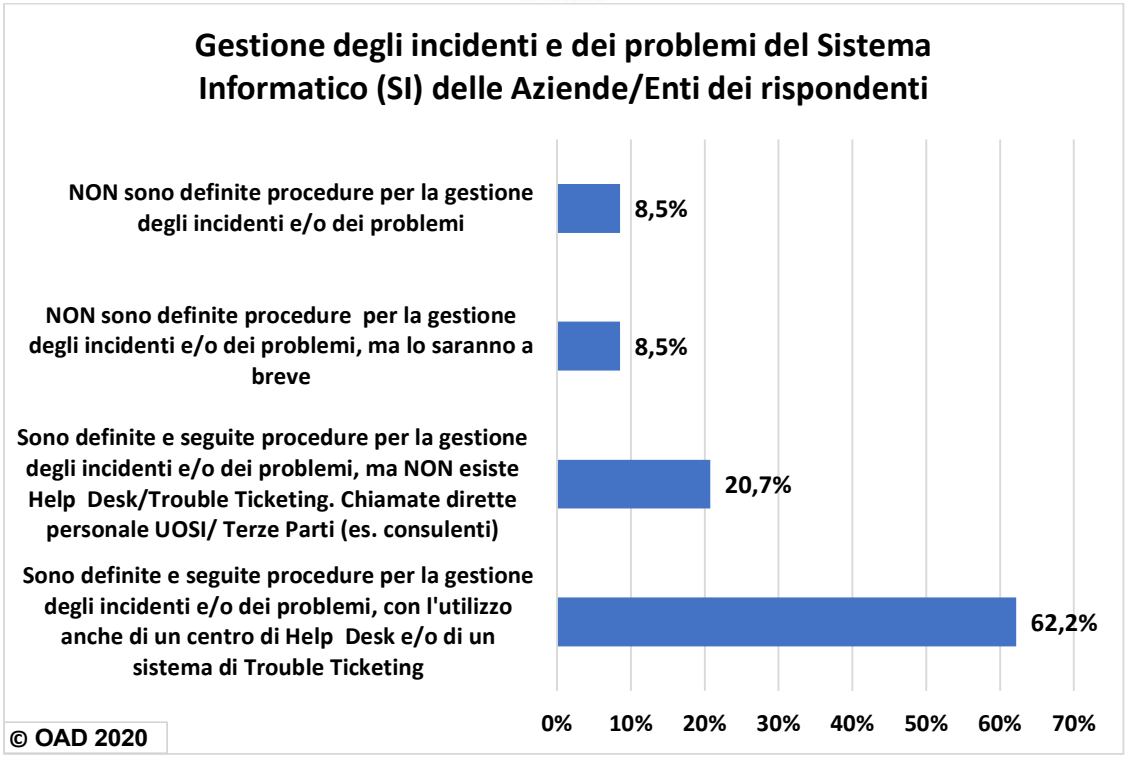


Fig. 9.1.2-3

La fig. 9.1.2-4 mostra la situazione dell'esistenza di un ERT, Emergency Response Team, e del suo utilizzo.
Circa un ¼ ha attivato un team delle emergenze che periodicamente effettua prove e simulazioni di emergenza, mentre un 40% l'ha definito ma non prova la sua effettiva funzionalità. Di nuovo un approccio formale e burocratico.

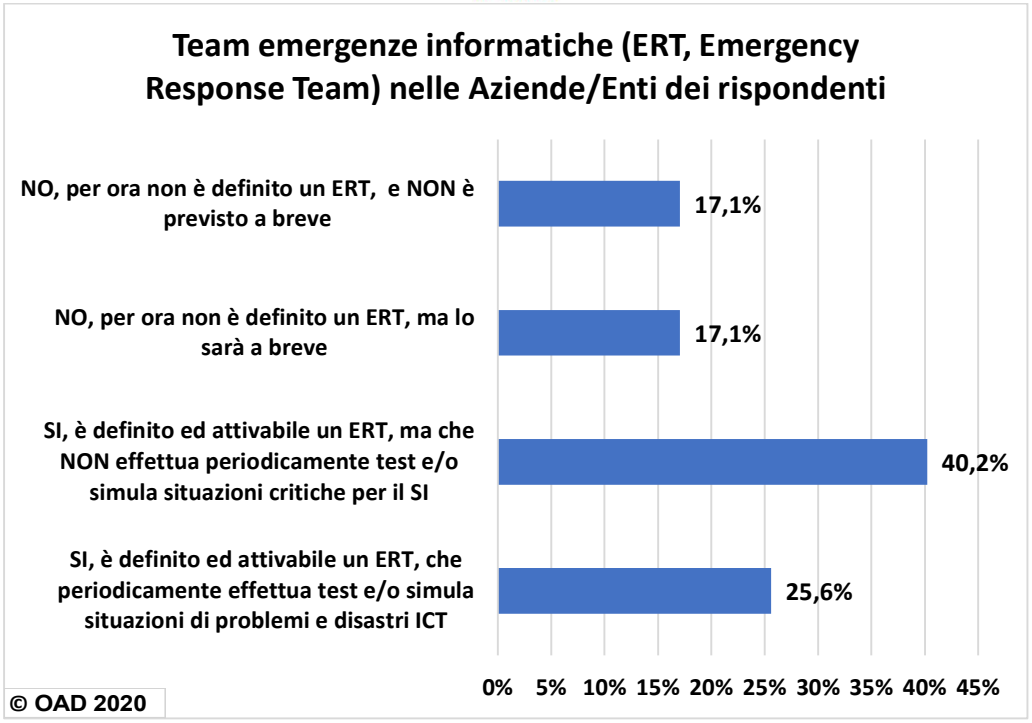


Fig. 9.1.2-4

9.1.3 Sensibilizzazione, formazione ed addestramento sulla sicurezza digitale

La crescente diffusione ed efficacia degli attacchi digitali è dovuta anche - e forse principalmente - alla scarsa consapevolezza della sua realtà e, in termini pragmatici, dei considerevoli danni che possono causare alle attività e al business, in pratica alla continuità operativa dell'intera Azienda/Ente. Scarsa consapevolezza sia al vertice dell'azienda/ente, sia a livello di tutti gli utenti, finali e privilegiati, che operano sui sistemi informatici e/o li utilizzano.
Questo dipende, a giudizio dell'autore, da due fatti principali: lato utenti, dal costo della formazione e dell'addestramento del personale. Lato vertice, dalla scarsa cultura ed interesse per l'ICT, di fatto considerato ancora come un "male necessario" e/o come una pura commodity, tipo presa corrente per l'energia elettrica: e sicuramente questo è dovuto anche alla enorme prevalenza in Italia di piccolissime e nano Aziende/Enti. Ma è proprio a livello di vertice che dovrebbe esserci una chiara consapevolezza dei possibili impatti degli attacchi digitali, e di quali misure di sicurezza, almeno a livello generale, la loro specifica realtà operativa avrebbe bisogno: consapevolezza necessaria per le decisioni da prendere in merito, dal budget da allocare agli interventi tecnici ed organizzativi da (far) effettuare con le opportune priorità.

Come dalla fig. 9.1.3-1, con risposte multiple, il 28,1% dei rispondenti indica che il personale interessato alla sicurezza digitale partecipa a corsi e seminari, ma che il 19,9%, in pratica 1/5, delle Aziende/Enti rispondenti non effettua alcun tipo di formazione.

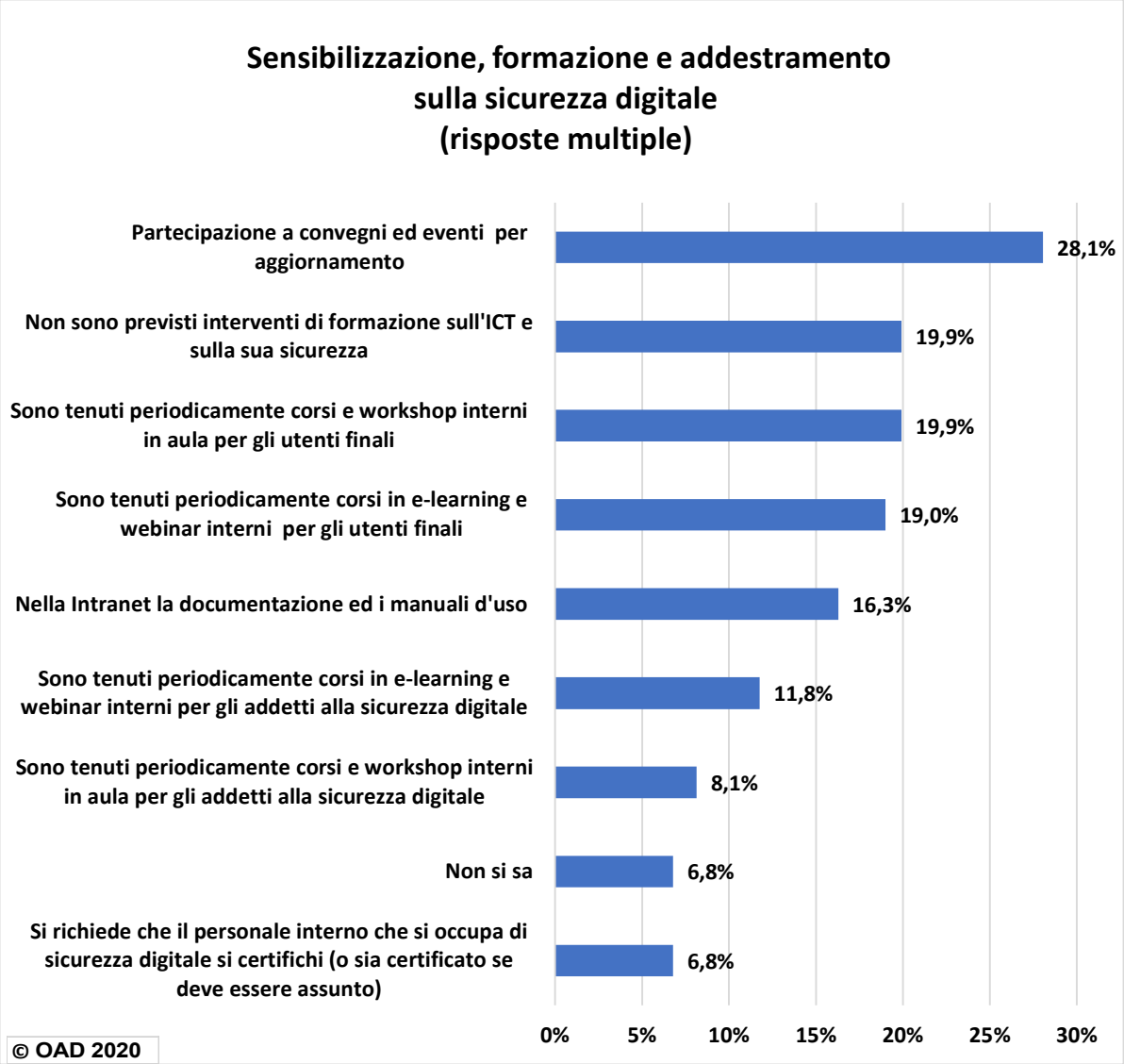


Fig. 9.1.3-1

La figura mostra che sono più diffusi i corsi per gli utenti finali sia in aula che in e-learning.
Il 16,3% dispone della documentazione condivisibile agli interessati nella Intranet, dato che la Intranet è tipicamente realizzata in strutture medio-grandi.

9.1.4 Certificazioni sulla sicurezza digitale

L'uso delle certificazioni è basilare non solo per qualificare la persona e l'Azienda/Ente che ne dispone, ma anche come primo strumento per verificare e scegliere consulenti e fornitori che si offrono come competenti ed esperti del settore.
Questo tipo di certificazioni sono da tempo assai diffuse per Aziende e professionisti dell'offerta di sicurezza digitale: ora stanno crescendo per Aziende e professionisti lato domanda, come richiesto da varie normative e qualificazioni, per poter dimostrare un livello di competenza ed esperienza qualificato e comprovato.

In ambito sicurezza digitale esistono numerosi i tipi di certificazioni indipendenti ed internazionali, quali ad esempio eCF (l'unica con validità legale in Europa), Eucip, CISSP, SSCP, CISA, CSSLP.
Esistono poi innumerevoli certificazioni "proprietarie" da parte di fornitori e costruttori ICT, prevalentemente focalizzate a validare la buona conoscenza tecnica e sistemistica dei loro prodotti, soluzioni e servizi ICT.
Si ricorda poi che in Italia sono in vigore due leggi, quella n. 4/2013 sulle "professioni non regolamentate" ed il D. Lgs. n. 13/2013 sulla "certificazione delle competenze" che hanno definito le certificazioni personali con valore legale per le figure professionali non regolamentate da Ordini. La prima normativa di riferimento indicata da queste norme è EN 16234-1:2016 (UNI 11506), che riprende la certificazione europea eCF sulle competenze e sui profili professionali dell'ICT. Nell'ambito della sicurezza digitale eCF prevede due figure: il Security Manager ed il Security Specialist.

La fig. 9.1.4-1 riporta la situazione delle certificazioni sulla sicurezza digitale a livello Azienda/Ente e del suo personale, per quanto riportato dai rispondenti. Il 37, 5% (era il 41,2 % nella precedente edizione, e circa il 40% in quella del 2018) delle Aziende/Enti non sono certificate e non richiedono certificazioni specifiche al loro personale. Solo il 18,3% sono certificate e richiedono certificazioni specifiche al loro personale. Una percentuale piuttosto alta di rispondenti, 12,5%, dichiara di non sapere sulla situazione delle certificazioni: questo è dovuto prevalentemente ai rispondenti di piccole e piccolissime organizzazioni.

In più punti del presente Rapporto si fa riferimento alla terziarizzazione della sicurezza digitale, e all'importanza, soprattutto per le piccole organizzazioni, di scegliere un fornitore competente e che fornisca il corretto servizio al richiedente. Un difficile compito per il decisore che non ha, e non può avere normalmente specifiche competenze in materia. Per non cadere facile preda di millantatori e di Terze Parti di scarsa etica professionale, uno dei criteri necessari (ma talvolta non sufficienti) è la verifica che la Terza Parte abbia certificazioni, così come il suo personale che interagisce con il cliente. In questa ottica il questionario 2020 OAD ha chiesto se vengono richieste alle Terze Parti e al loro personale specifiche certificazioni sulla sicurezza digitale. Il risultato è riportato nella fig. 9.1.4-2.

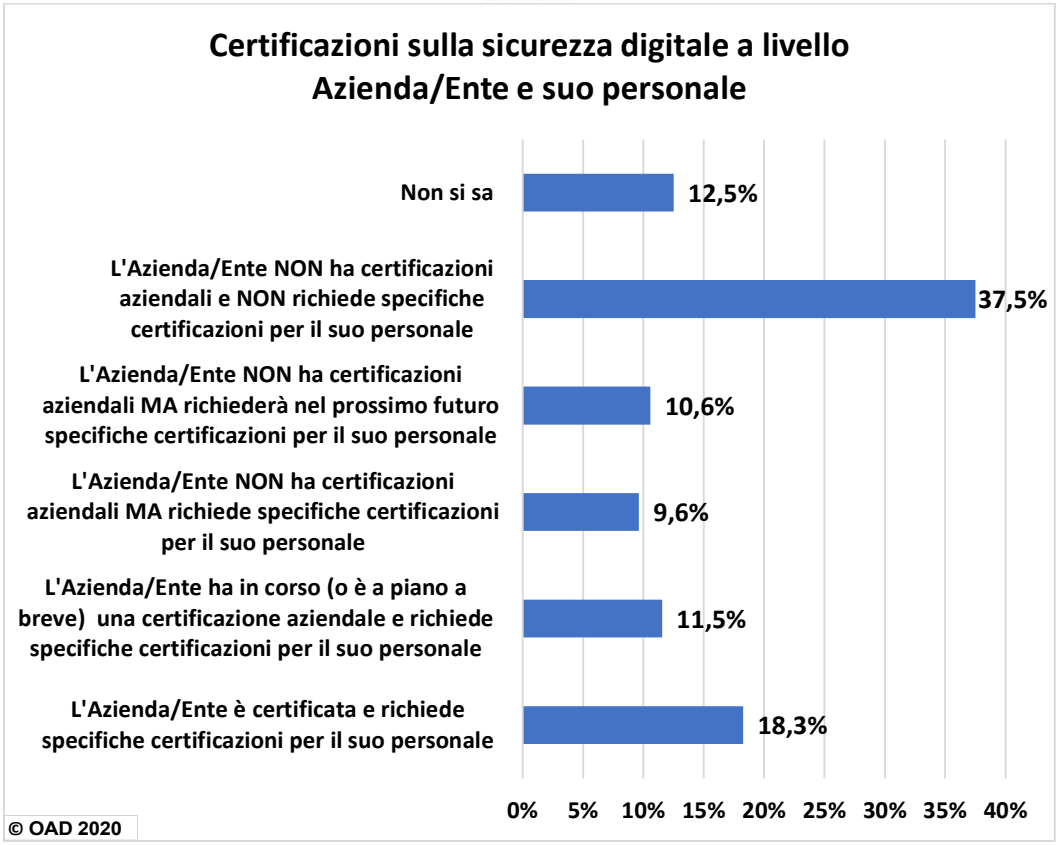


Fig. 9.1.4-1

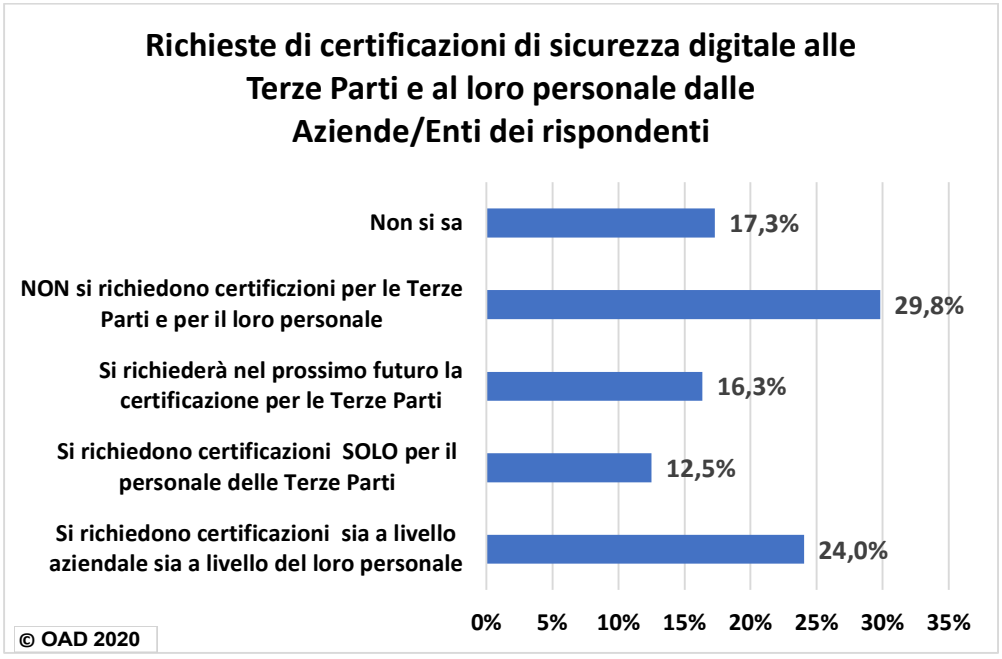


Fig. 9.1.4-2

Il 24% delle Aziende/Enti dei rispondenti richiede alla Terze Parti certificazioni sulla sicurezza digitale sia a livello aziendale che del loro personale che interagisce con il cliente. Quasi il 30% invece non le richiede, ed il 12,5 le richiede solo per il personale della Terza Parte che interagisce con il suo personale. Un 16,3% richiede certificazioni nel prossimo futuro, ed un elevato 17,3% dichiara di non sapere nulla di questo tema. Si noti che questa percentuale è di circa 5 punti superiore a quella riscontrata nella fig. 9.1.4-2, e fa riferimento allo stesso bacino di rispondenti. Difficile dare una spiegazione a questo fatto, numericamente troppo alto per essere attribuito solo ad errori nella scelta delle risposte al questionario. Al di là delle motivazioni indicate in precedenza, ossia che queste risposte sono prevalentemente fornite da rispondenti di piccole e piccolissime organizzazioni, un ulteriore motivo è che alcuni rispondenti di grandi organizzazioni, dal ruolo tecnico e specialistico, possono non avere conoscenza delle richieste e delle clausole per i fornitori.

9.1.5 Analisi e assicurazione dei rischi digitali

L'**a**nalisi dei rischi ICT è basilare per la progettazione delle misure di sicurezza contestualizzate sulla specifica realtà dell'Azienda/Ente. L'analisi dei rischi è inoltre richiesta per la conformità a varie norme e leggi, a partire dal GDPR. Sono ormai consolidate da anni varie metodiche, best practice e framework per effettuare tali analisi, pur con differenti livelli di dettaglio e di granularità: dallo standard ISO 27005 a NIST, CRAMM, Mehari, Octave-Allegro, e così via.
I rischi digitali dipendono dalle vulnerabilità tecniche, organizzative e delle persone che usano e gestiscono i sistemi informatici e più in generale ogni dispositivo ICT. Per una corretta individuazione dei rischi digitali occorre prima effettuare un'analisi delle vulnerabilità digitali, trattate in §5 cui si rimanda.
Per semplificare le domande nel questionario 2020, si è volutamente accorpata in una sola domanda l'analisi dei rischi e delle vulnerabilità. Quanto emerso dal bacino dei rispondenti è riportato in fig. 9.1.5-1 risulta veramente positivo: il 77,1% (era il 54,5% nella precedente indagine) delle Aziende/Enti dei rispondenti effettua nel complesso l'analisi dei rischi, ma di questi il 34,5% la effettua solo se richiesto e/o in maniera sporadica, ad esempio dopo aver subito un grave attacco digitale, ed il 10,5% senza effettuare l'analisi di vulnerabilità. Il 6,7% ha in piano di effettuare analisi di vulnerabilità e dei rischi digitali nel prossimo futuro.
Solo il 16,2% dei rispondenti dichiara che nella sua Azienda/Ente non viene effettuata l'analisi dei rischi, tantomeno quella di vulnerabilità. Queste percentuali non solo confermano il livello medio-alto del bacino dei rispondenti, che pure includono in maggioranza PMI (si veda §10.) in termini di misure di sicurezza digitali, ma anche la crescita a partire dal 2017 di chi effettua l'analisi dei rischi e delle vulnerabilità digitali: un aumento sicuramente favorito dall'obbligo di conformità alle normative sulla privacy, in ultimo il GDPR, e ad altre normative nazionali ed internazionali, alle certificazioni e più in generale alla lenta crescita e diffusione di cultura digitale.

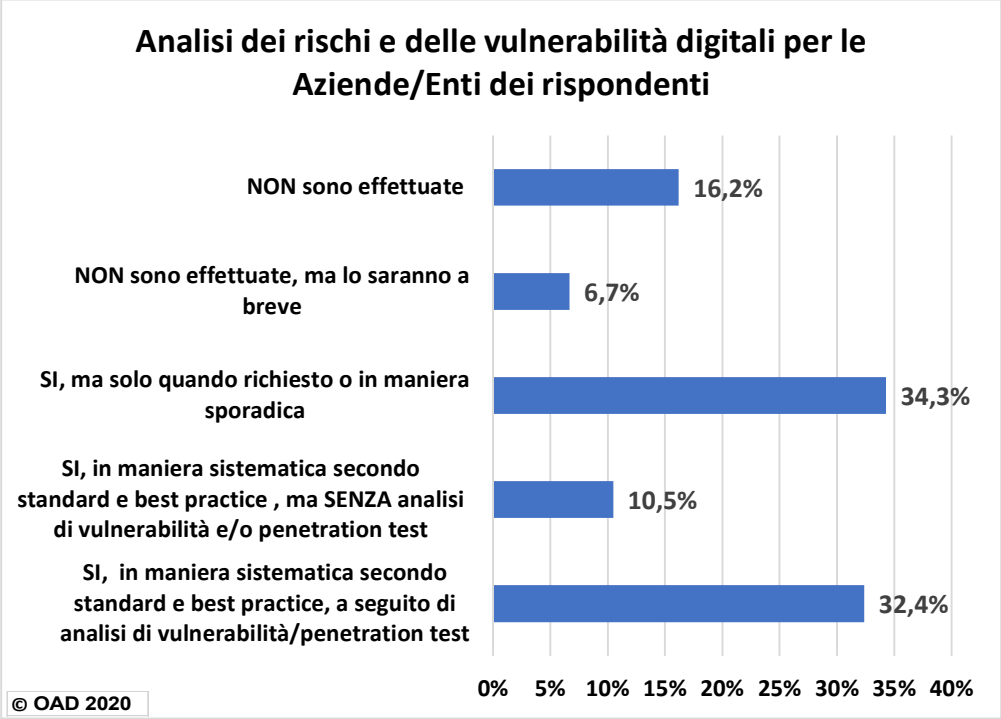


Fig. 9.1.5-1

La sicurezza digitale assoluta non esiste e non può esistere, un rischio residuo rimane sempre pur avendo adottato tutte le misure allo stato dell'arte. La dove il sistema informatico riveste un ruolo essenziale, è opportuno quindi assicurare questo rischio residuo tramite società di assicurazioni. E per l'assicurazione il livello delle misure di sicurezza poste in atto e il livello di accuratezza dell'analisi dei rischi sono determinanti, per non incorrere in prezzi troppo alti del premio assicurativo. I tecnici delle assicurazioni ben valutano i livelli di sicurezza digitale in essere, sia a livello tecnico che organizzativo, per stabilire il prezzo dell'assicurazione.

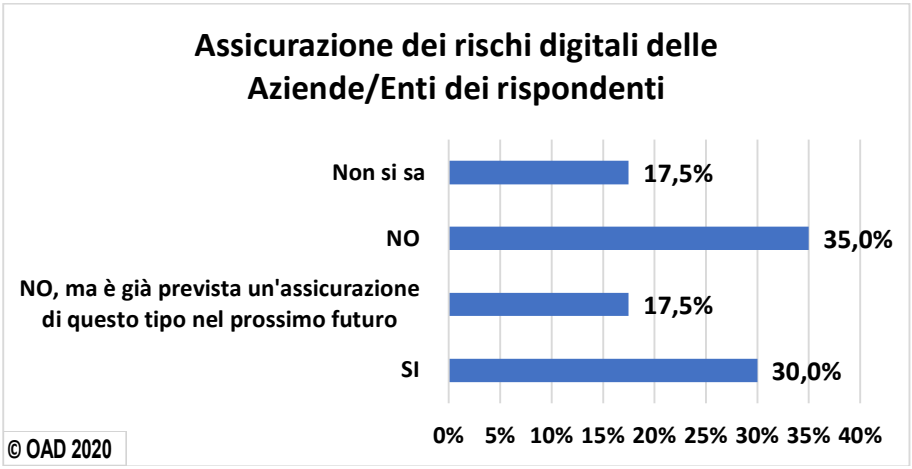


Fig. 9.1.5-2

La fig. 9.1.5-2 mostra che il 30% dei rispondenti ha già stipulato nel 2019 una specifica assicurazione per i rischi ICT, mentre il 17,5% ha in programma di sottoscriverne una. Come tendenza, e senza valore statistico per la diversità dei bacini dei rispondenti, la percentuale di chi ha già nel 2019 una assicurazione sui rischi digitali è maggiore rispetto al 23,2% del 2018, che a sua volta è quasi raddoppiata rispetto a quella del 2017: anche questo un indice del crescente interesse, seppur lento, nell'assicurare il sistema informatico.

9.1.6 Auditing sicurezza digitale

Con il termine di "auditing" si intende il processo di valutazione della sicurezza digitale, e della sua gestione, di una Azienda/Ente. Con il termine di "audit" si intende il risultato di tale valutazione, rappresentato tipicamente di un rapporto all'alta direzione. Sovente, anche tra gli addetti ai lavori, i due termini vengono usati, erroneamente, come sinonimi. L'auditing può essere inoltre effettuato con personale interno o con esperti e società esterne, ed alcuni grandi organizzazioni lo effettuano sia internamente che esternamente.

La fig. 9.1.6-1 indica che più della metà rispondenti, il 51,9%, già effettua auditing per la sicurezza del proprio sistema informatico, ed il 7,7% lo ha a piano a breve. Valori percentuali alti, superiori come tendenza a quanto rilevato dalle indagini OAI/OAD negli anni precedenti, ed indice anche questo, come l'analisi dei rischi del precedente paragrafo, del buon livello medio di sicurezza digitale per i rispondenti di OAD 2020. Un 28,8% non lo effettua, ed è il caso delle piccole e piccolissime organizzazioni.

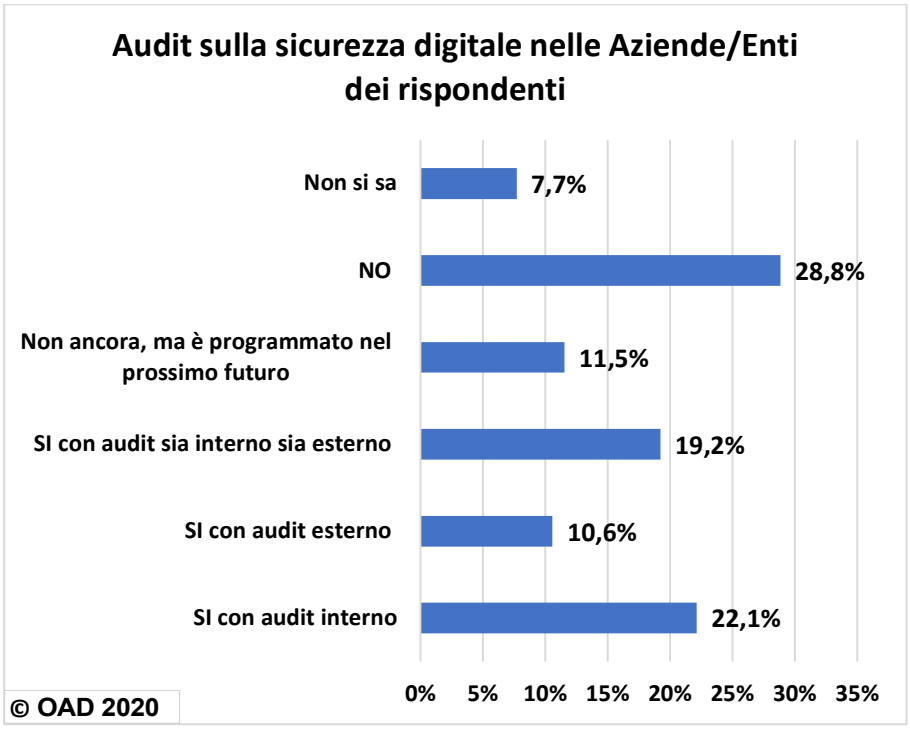


Fig. 9.1.6-1

9.2 Misure tecniche per la sicurezza digitale

Facendo riferimento alle macro-caratteristiche dei sistemi informatici e delle Aziende/Enti dei rispondenti illustrate in §10, nel seguito vengono descritti gli strumenti di sicurezza digitale in uso in questi sistemi informatici, a livello sia tecnico sia organizzativo: è così possibile comprendere meglio in quali contesti e con quali livelli di sicurezza digitale siano potuti occorrere gli attacchi rilevati (§6).
Nel questionario OAD 2020 le misure tecniche sono state raggruppate in:

- Architettura complessiva delle misure della 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 (non fisica) dei singoli sistemi ICT anche terziarizzati/in cloud
- Contromisure tecniche per la protezione del software e degli applicativi dei sistemi ICT anche terziarizzati/in cloud
- Contromisure per la protezione dei dati
- Sistemi di controllo, monitoraggio e gestione della sicurezza digitale
- Piano di Disaster Recovery (DR) con l'allocazione, o non, dei relativi ambiti alternativi.

La prima domanda sulle misure tecniche riguarda l'architettura della sicurezza digitale posta in esercizio, e che dovrebbe essere integrata nell'architettura dell'intero Sistema Informatico. La domanda serve per inquadrare l'approccio tecnico che l'Azienda/Ente sta, o non, seguendo nella realizzazione della sicurezza digitale per i suoi sistemi ICT, tenendo conto che anche per l'architettura tecnica della sicurezza digitale esistono standard e best practice di riferimento, quali ad esempio gli standard ISO, quelli NIST SP 800, quelli SOA/OASIS, l'OSA, Open Security Architecture, e che da anni gli esperti di sicurezza digitale sottolineano l'importanza di una "security by design", richiesta anche dal GDPR per implementare una privacy by design e by default.

La fig. 9.2-1 dettaglia le risposte fornite dai rispondenti sull'implementazione di un'architettura di sicurezza digitale per il Sistema Informatico della loro Azienda/Ente. La situazione emersa è molto positiva, riconfermando il livello medio-alto di sicurezza digitale del campione emerso nel 2020: nel complesso, pur con modalità diverse dettagliate nella figura, quasi il 70% ha implementato una sua architettura di sicurezza digitale ed il 3,9% la sta adottando o la farà breve. E ben il 38,8% ha implementato questa architettura seguendo i principali standard e best practice, ed includendo anche le risorse ICT terziarizzate.
La fig. 9.2-2 approfondisce il livello di alta affidabilità che l'implementazione dell'architettura della sicurezza digitale fornisce al Sistema Informatico dell'Azienda/Ente dei rispondenti. Confermando quanto emerso nella figura precedente, il 25,8% afferma di avere un sistema ad altissima affidabilità, che garantisce il 99,9% di funzionamento senza interruzioni non prestabilite, tipicamente nell'arco temporale di un anno. Il 21,7% dei rispondenti indica che l'alta affidabilità è riservata solo alle risorse più critiche per il buon funzionamento del Sistema Informatico. Un decimo dei rispondenti segnala che l'architettura per la sicurezza digitale, pur definita ed implementata, non prevede soluzioni ad alta affidabilità.
.
Le misure di sicurezza fisica e perimetrali per i Sistema Informatici (SI) considerati nell'indagine differiscono in maniera significativa se questi sono di medie-grandi dimensioni con Data Center centralizzati e risorse ICT locali concentrate in apposite "Computer Room", o se sono invece piccoli, senza un effettivo Datacenter, con le risorse ICT nei locali ove operano i dipendenti delle Aziende/Enti rispondenti, e che sono dotati delle misure fisiche di protezione che gli stessi locali hanno.

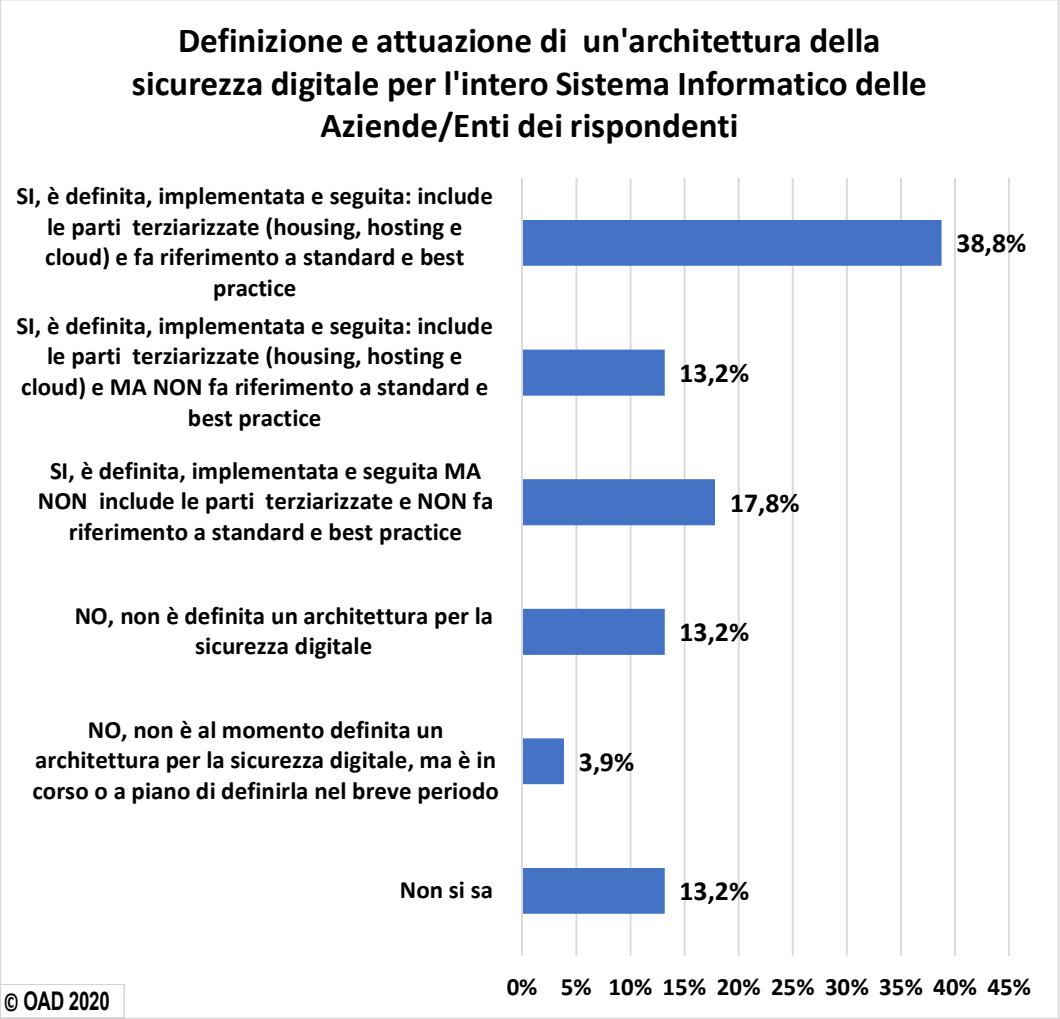


Fig. 9.2-1

Gli strumenti di sicurezza fisica includono i sistemi per garantire la continuità elettrica (dagli UPS ai gruppi di continuità), i sistemi di climatizzazione nei locali ove sono concentrate le risorse ICT, i vari sistemi rilevatori di fumo, gas, e umidità, le protezioni perimetrali passive e attive, recinzioni anti-scavalcamento, inferiate alle finestre e alle porte, sistemi di allarme antintrusione a radar o a micro onde, la videosorveglianza. Includono anche i sistemi di controllo degli accessi delle persone fisiche ai Data Center e alle Computer Room, quali la guardiania, le bussole d'ingresso, i lettori di badge ed i sistemi di riconoscimento biometrico, etc.
Nelle realtà più piccole le misure di sicurezza fisica coincidono con quelle di protezione di queste aree, ossia le porte chiudibili a chiave, le inferriate alle finestre. Le parti del Sistema Informatico terziarizzate, ossia in housing/hosting/cloud godono delle misure di sicurezza dei Data Center del fornitore, che nella maggior parte dei casi sono di alto livello.

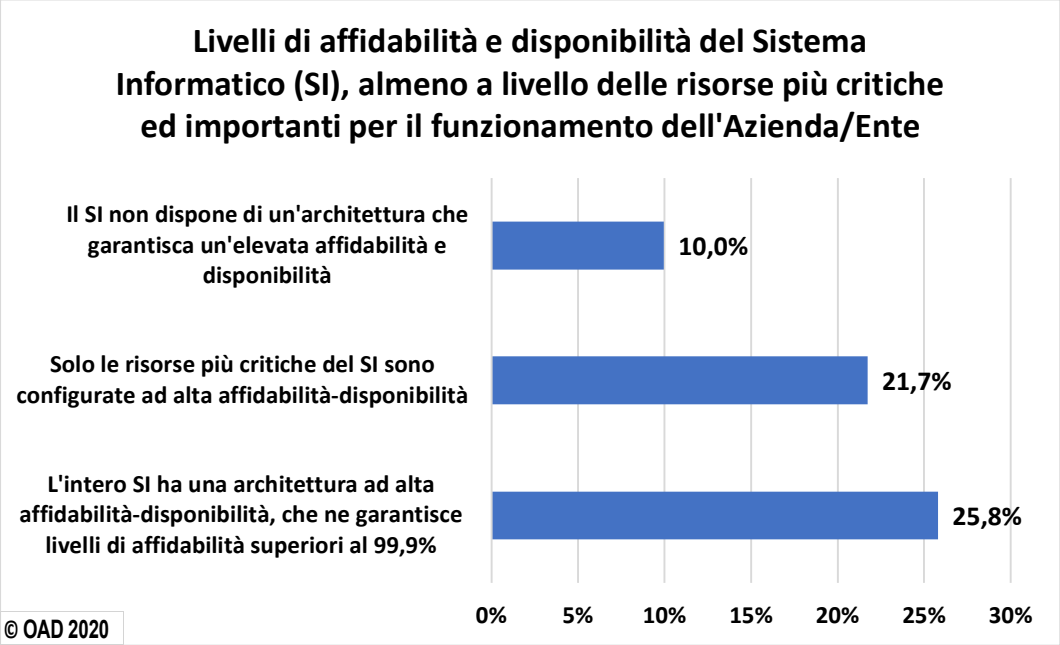


Fig. 9.2-2

La fig. 9.2-3 mostra la situazione delle misure di sicurezza fisica e perimetrali dei SI oggetto delle risposte di chi ha compilato il questionario.

Il 55,8% dei rispondenti dispone delle idonee misure di sicurezza fisica in tutte i Data Center e le Computer Room, ed il 24% solo presso i Data Center: in pratica un buon livello per più dei ¾ dei rispondenti.

Gli strumenti di identificazione, autenticazione e autorizzazione (IAA) per gli utenti finali e per quelli privilegiati (questi ultimi sono gli amministratori-operatori ICT, i manutentori, gli sviluppatori software, che hanno tutti dei particolari privilegi di accesso) sono fondamentali per l'effettiva protezione di un Sistema Informatico, ed ancor più critici dato che nel 2019, così come nel 2018 e 2017, il più diffuso insieme di attacchi è stato proprio all'ambiente IAA.

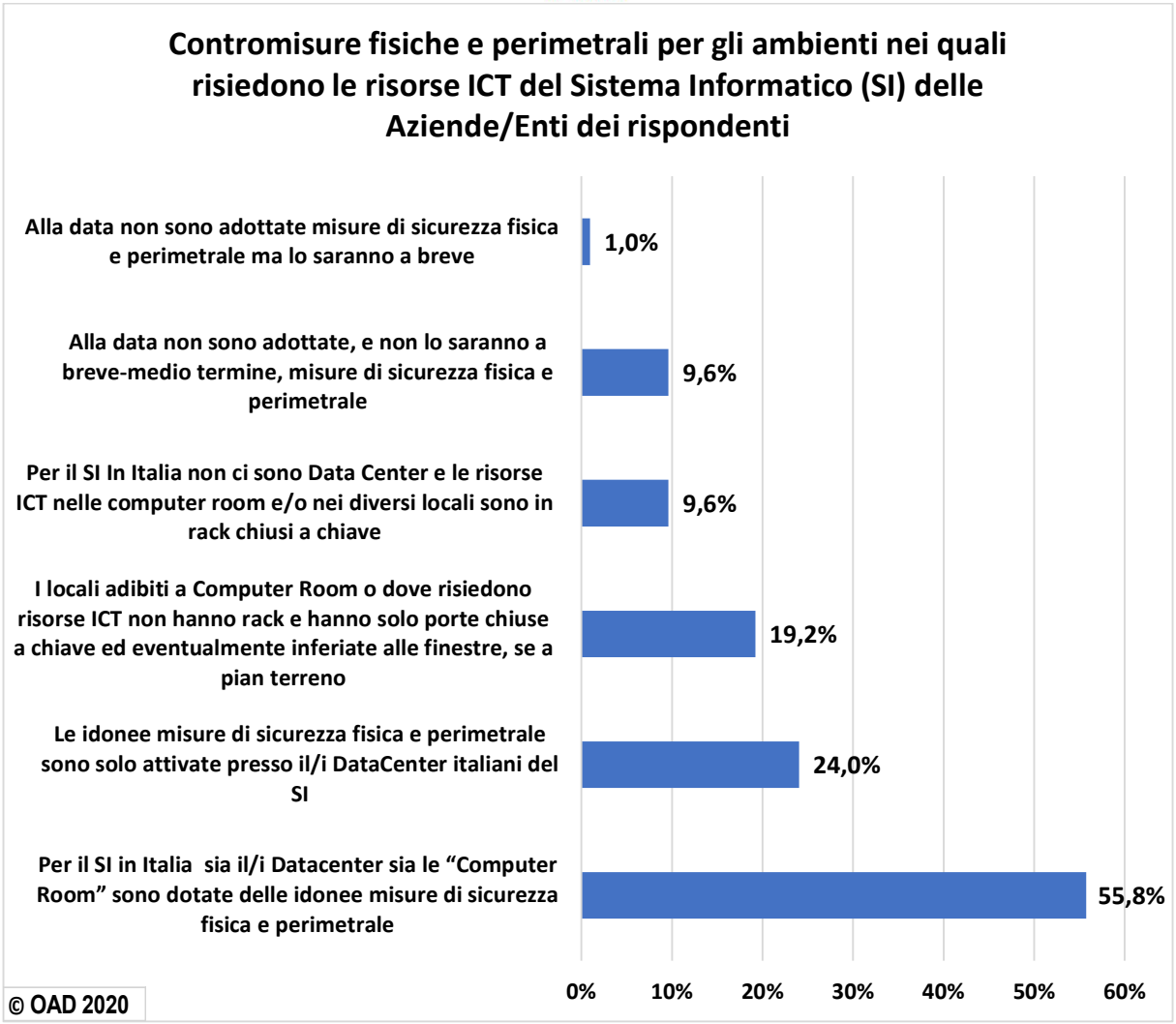

Contromisure fisiche e perimetrali per gli ambienti nei quali risiedono le risorse ICT del Sistema Informatico (SI) delle Aziende/Enti dei rispondenti
Alla data non sono adottate misure di sicurezza fisica e perimetrale ma lo saranno a breve
1,0%
Alla data non sono adottate, e non lo saranno a breve-medio termine, misure di sicurezza fisica e perimetrale
9,6%
Per il SI In Italia non ci sono Data Center e le risorse ICT nelle computer room e/o nei diversi locali sono in rack chiusi a chiave
9,6%
I locali adibiti a Computer Room o dove risiedono risorse ICT non hanno rack e hanno solo porte chiuse a chiave ed eventualmente inferiate alle finestre, se a pian terreno
19,2%
Le idonee misure di sicurezza fisica e perimetrale sono solo attivate presso il/i DataCenter italiani del SI
24,0%
Per il SI in Italia sia il/i Datacenter sia le "Computer Room" sono dotate delle idonee misure di sicurezza fisica e perimetrale
55,8%
0%
10%
20%
30%
40%
50%
60%
© OAD 2020

Fig. 9.2-3

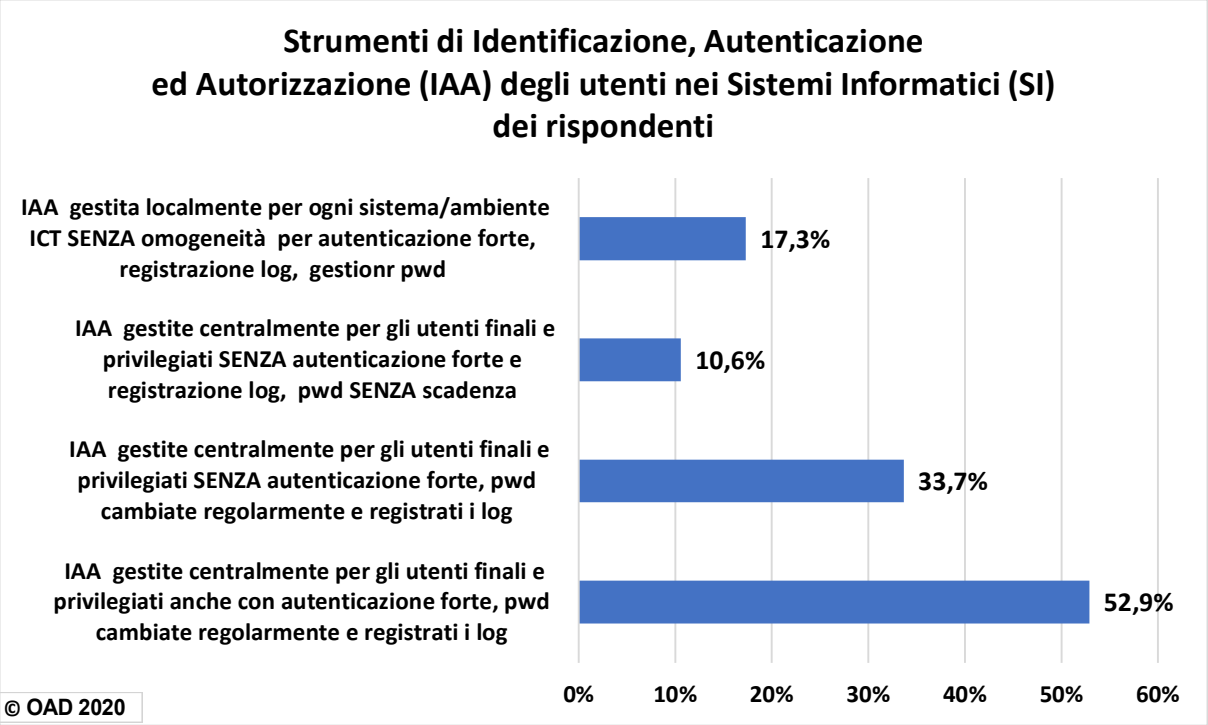


Fig. 9.2-4

Nell'indagine 2020 OAD, il questionario non ha posto domande specifiche sulle tecniche di IAA, come c'erano per le precedenti edizioni, ma ha preferito porre domande meno tecniche, anche per facilitarne la compilazione. 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[20], 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.
La fig. 9.2-4 riporta le misure di IAA in uso nei SI dei rispondenti, che risulta nettamente migliorata rispetto a quelle emerse negli anni precedenti.
Circa il 53% ha sistemi IAA allo stato dell'arte, centralizzati, con tecniche di autenticazione forte, registrazione e gestione dei log, gestione delle dimensioni, complessità e scadenze delle password. Un ulteriore 33,7% usa IAA centralizzate, ma non ha attivato e non gestisce l'autenticazione forte, i log, le password. Il rimanente 17,3% gestisce l'IAA localmente su ogni singolo sistema
Anche nell'ambito delle contromisure per le reti, il questionario 2020 non ha posto domande specifiche sulle tecniche in uso, per rendere più facile e corretta la compilazione da parte dei

[20] 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

rispondenti. Numerose le tecniche disponibili, alcune referenziate nelle domande, che includono connessioni multiple in ridondanza per garantire alta affidabilità e disponibilità, dispositivi firewall di rete e DMZ, DeMilitarized Zone (in italiano zona demilitarizzata), crittografia nelle comunicazioni (HTTPS, FTPS.) e VPN, Virtual Private Network, IDS/IPS, Intrusion Detection/Prevention System, filtraggio traffico ed indirizzi, analisi comportamentali delle unità di rete intelligenti.
La fig. 9.2-5 evidenzia che solo l'8,2% dei rispondenti è dotata di misure tecniche di sicurezza digitale per le reti. Tutti gli altri rispondenti dichiarano di utilizzare le principali misure indicate: il 50,8%, la maggioranza sul totale, dispone di soluzioni ad alta affidabilità con duplicazione delle risorse più critiche.

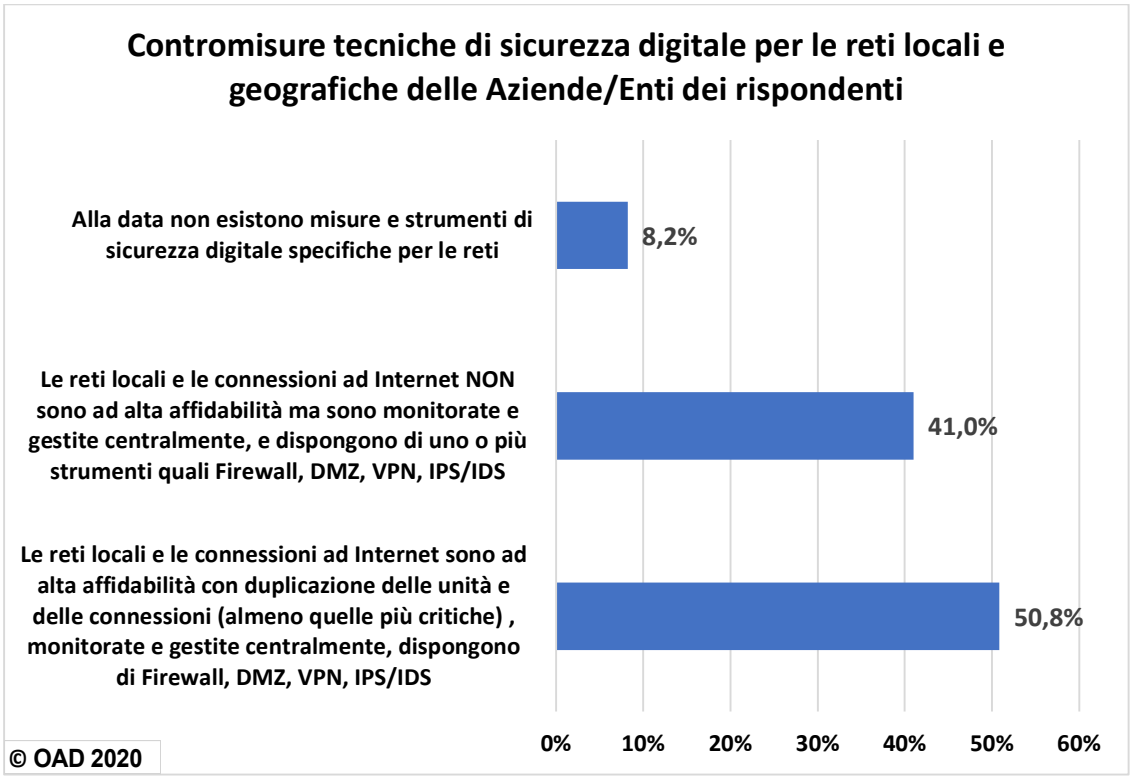


Fig. 9.2-5

La fig. 9.2-6 mostra in maniera esplicativa le misure di sicurezza digitale (non fisica) in essere sui singoli sistemi ICT, tipicamente server e storage, fisici e virtuali, posti di lavoro (PC), unità di rete, etc. Le misure considerate a livello dei singoli sistemi ICT includono le configurazioni ad alta affidabilità, i sistemi anti-malware, la virtualizzazione dei sistemi, la gestione delle versioni e delle patch per il software, la raccolta e la gestione dei log di sistema, e così via
Anche in questo caso le risposte al questionario fanno emergere una situazione molto buona nei Sistemi Informatici delle Aziende/Enti dei rispondenti: il 60,7% dichiara che le misure in essere, incluso il monitoraggio e controllo centrale, sono allo stato dell'arte, e solo l'8,2% dei sistemi ICT sono gestiti in loco con misure di sicurezza digitali non omogenee.

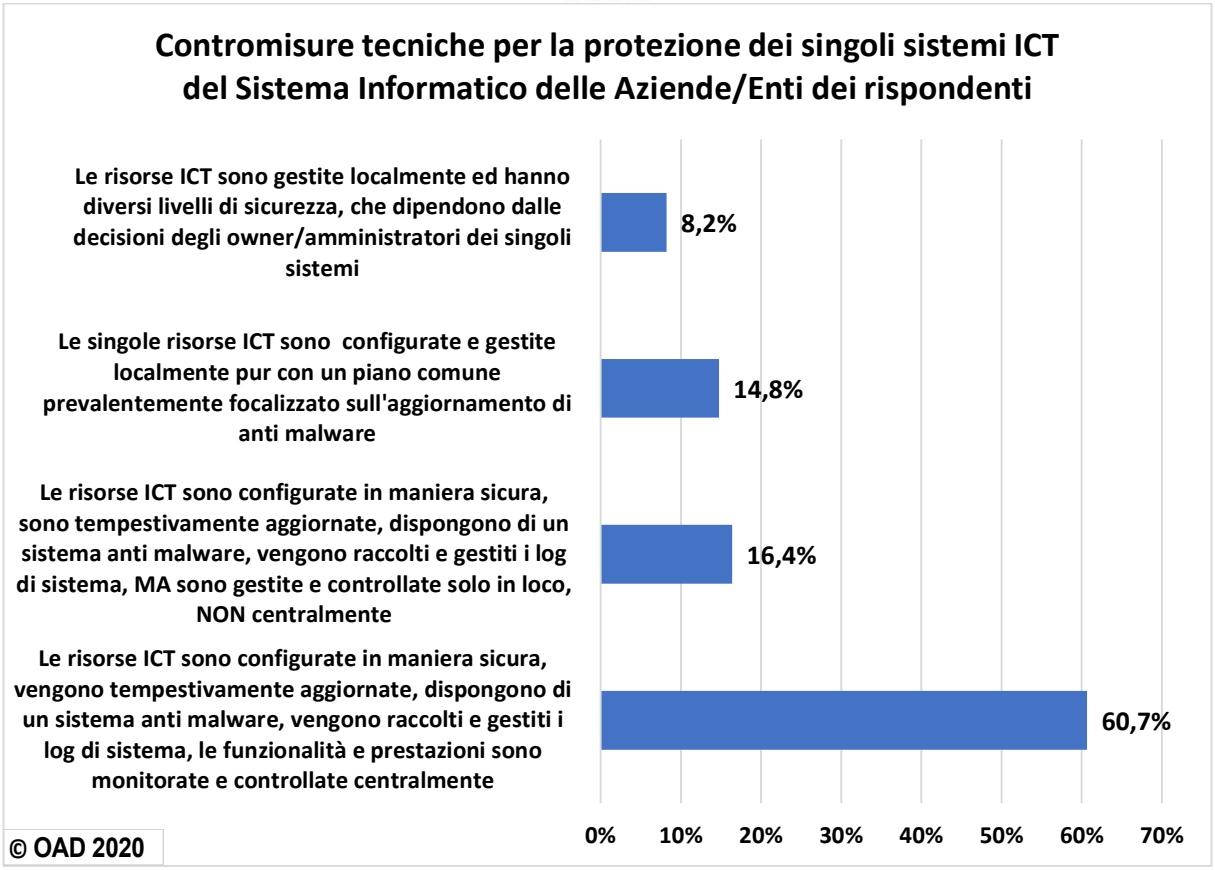


Fig. 9.2-6

Le contromisure a livello applicativo includono una serie di tecniche e di misure specifiche, dallo sviluppo sicuro del software al controllo della sicurezza intrinseca del codice (ad esempio con reverse engineering, con l'analisi di vulnerabilità del codice e con penetration test) dai firewall applicativi (FWA) all'isolamento (da Internet) di applicativi critici, dall'aggiornamento sistematico del codice alle clausole contrattuali coi fornitori, dalla sistematica profilatura dei diritti d'accesso degli utenti, sia finali che privilegiati, alla configurazione sicura e all'interoperabilità sicura con altri applicativi, e così via. La sicurezza del software di un applicativo deve, o dovrebbe, essere in primo luogo "intrinseca" e, data la grande diffusione di applicazioni commerciali, soprattutto per le PMI, questa dovrebbe essere garantita dal fornitore. Ma può poi essere corrotta da errate installazioni e configurazioni, da aggiunte per l'integrazione e l'interoperabilità con altre applicazioni. Per i software commerciali, poi, in tempi di crisi economica come l'attuale, non vengono talvolta rinnovati i contratti per la loro manutenzione correttiva ed evolutiva, lasciando così in produzione software vulnerabili facile preda degli attaccanti.
Per non entrare in troppi tecnicismi, anche per queste misure il questionario 2020 OAD ha posto domande orientate ad inquadrare per ampie classi le misure di sicurezza digitale per gli applicativi, classi con misure a decrescere descritte nei seguenti punti dal livello più alto a quello più basso:

- Applicativi del Sistema Informatico allo stato dell'arte della sicurezza, sia con sviluppi ad hoc sia con software commerciali: codice software sviluppato secondo le più recenti prassi e standard per la sua sicurezza "intrinseca", diritti d'accesso profilati per chi lo deve realmente usare o manutenere e sistematicamente controllati, uso di firewall applicativi, aggiornamenti sistematici e tempestivi, manutenzione correttiva ed evolutiva effettuata secondo specifiche best practice (coi fornitori specifiche clausole sono nel contratto), funzionalità e prestazioni dell'applicazione monitorate e controllate sistematicamente e centralmente.

- Software applicativo del Sistema Informatico prevalentemente o solo commerciale, con sistematici aggiornamenti seguendo le indicazioni del fornitore, con funzionalità e prestazioni monitorate e controllate sistematicamente e centralmente; essendo software commerciali, il controllo della loro sicurezza intrinseca è limitato all'analisi, ogni tanto, delle loro vulnerabilità.
- Software applicativo del Sistema Informatico prevalentemente o solo commerciale, aggiornato SOLO quando indispensabile e non in maniera sistematica, funzionalità e prestazioni dell'applicazione monitorate e controllate centralmente.
- Il software applicativo NON monitorato centralmente ed aggiornato SOLO per indispensabili necessità e cambi funzionali.

La fig. 9.2-7, basandosi sulle quattro classi sopra descritte, sintetizza a grandi linee le misure tecniche di sicurezza digitali in prevalente uso per gli applicativi dei Sistemi Informatici oggetto delle risposte al questionario.

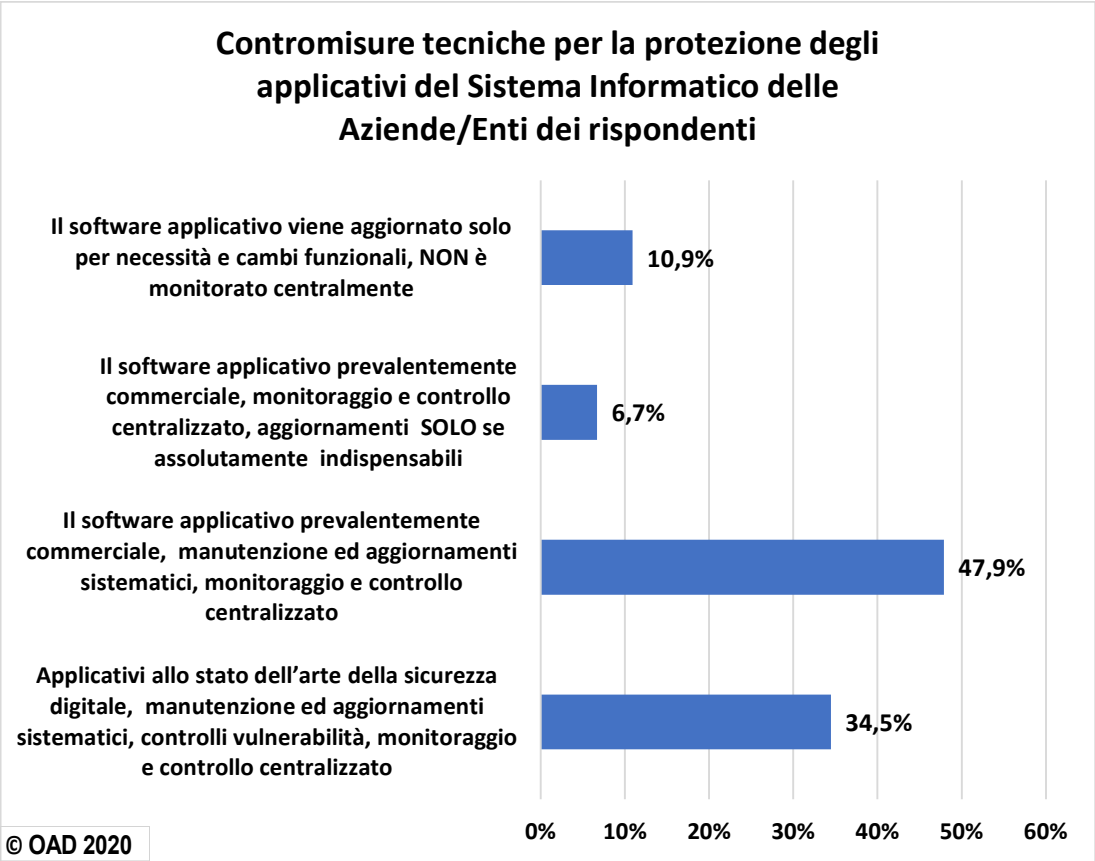


Fig. 9.2-7

Più di 1/3 dei rispondenti ha applicativi con misure di sicurezza allo stato dell'arte, sia per software utilizzati ad hoc che per quelli commerciali. Il 47,9% usa prevalentemente software commerciali, controllati centralmente ed aggiornati sistematicamente. Il 10,9% degli applicativi non è monitorato e controllato centralmente, ed i suoi aggiornamenti non sono sistematici.

Numerose le misure tecniche per la protezione dei dati, che costituiscono il reale e più importante "asset ICT" dell'Azienda/Ente. Esse partono dalla classificazione dei dati trattati in merito alle loro necessità di protezione, classificazione, da sempre necessaria per la privacy per l'individuazione dei

dati personali e "sensibili", ed includono la crittografia dei dati più critici, inclusi quelli personali e sensibili per la privacy, ed i back up e la loro gestione per il ripristino.
La fig. 9.2-8, auto-esplicativa, inquadra a grandi linee le misure per la protezione dei dati in essere nei Sistemi Informatici delle Aziende/Enti dei rispondenti, ma non entra nel dettaglio dei backup e dei ripristini, che sono considerati nella figura successiva. Infatti, data l'importanza delle misure di back e di ripristino, il questionario ha previsto una specifica domanda in merito, tenendo conto che nelle piccole e medie organizzazioni, sovente i backup ed i ripristini sono gestiti in maniera non sistematica e/o solo parziale, con talvolta l'impossibilità di ripristini completi (uno dei motivi della efficace proliferazione in Italia dei malware e ransomware).

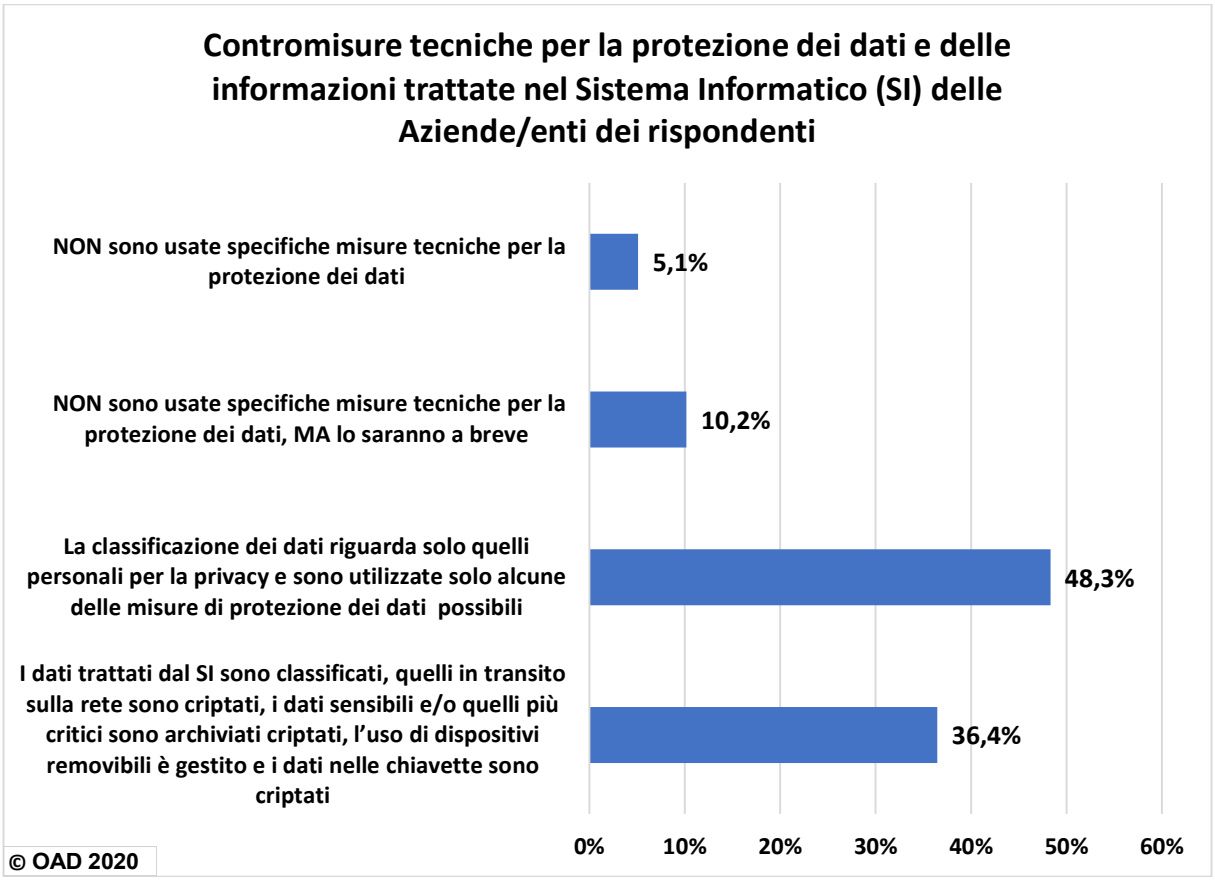


Fig. 9.2-8

La fig. 9.2-8 mostra che gran parte dei SI dei rispondenti, l'84,7%, classifica i dati trattati ed utilizza strumenti di protezione almeno per quelli più critici, anche nell'ottica del GDPR per la privacy.

La fig. 9.2-9 mostra la situazione per le essenziali misure di backup e ripristino, sintetizzata in base alle seguenti classi che costituivano le risposte tra le quali scegliere e che sono elencate al decrescere del livello complessivo di sicurezza digitale:

- Tutti i dati del SI sono regolarmente backuppati in maniera automatica, con copie dei backup criptate su media removibili (es: hard disk removibile e offline) e allocate in sedi geograficamente diverse da quelle dei Data Center/Computer room. Sono inoltre definite le procedure di ripristino dai backup e periodicamente verificate.

- Tutti i dati del SI sono regolarmente backuppati in maniera automatica, con copie dei backup criptate su media removibili (es: hard disk removibile e offline) e allocate in sedi geograficamente diverse da quelle dei Data Center/Computer room, ma le procedure di ripristino dai backup o non esistono o sono molto generiche, e non sono verificate.
- Tutti i dati del SI sono regolarmente backuppati in maniera automatica, ma le copie di backup non sono criptate ed i media di archiviazione non allocati in sedi geograficamente diverse da quelle dei data center/computer room. Inoltre, le procedure di ripristino dai backup o non esistono o sono molto generiche, e non sono verificate.

La fig. 9.2-9 mostra come la maggioranza dei rispondenti, il 52,2%, effettua backup e ripristini secondo lo stato dell'arte. Il resto dei rispondenti evidenzia soprattutto la mancanza di procedure di ripristino, e le copie dei backup lasciate nelle stesse sedi dove si trovano i sistemi ICT backuppati, con gravi rischi in caso di incidenti fisici e naturali in queste sedi, quali ad esempio incendi, attacchi fisici, crolli di muri e soffitti, etc.

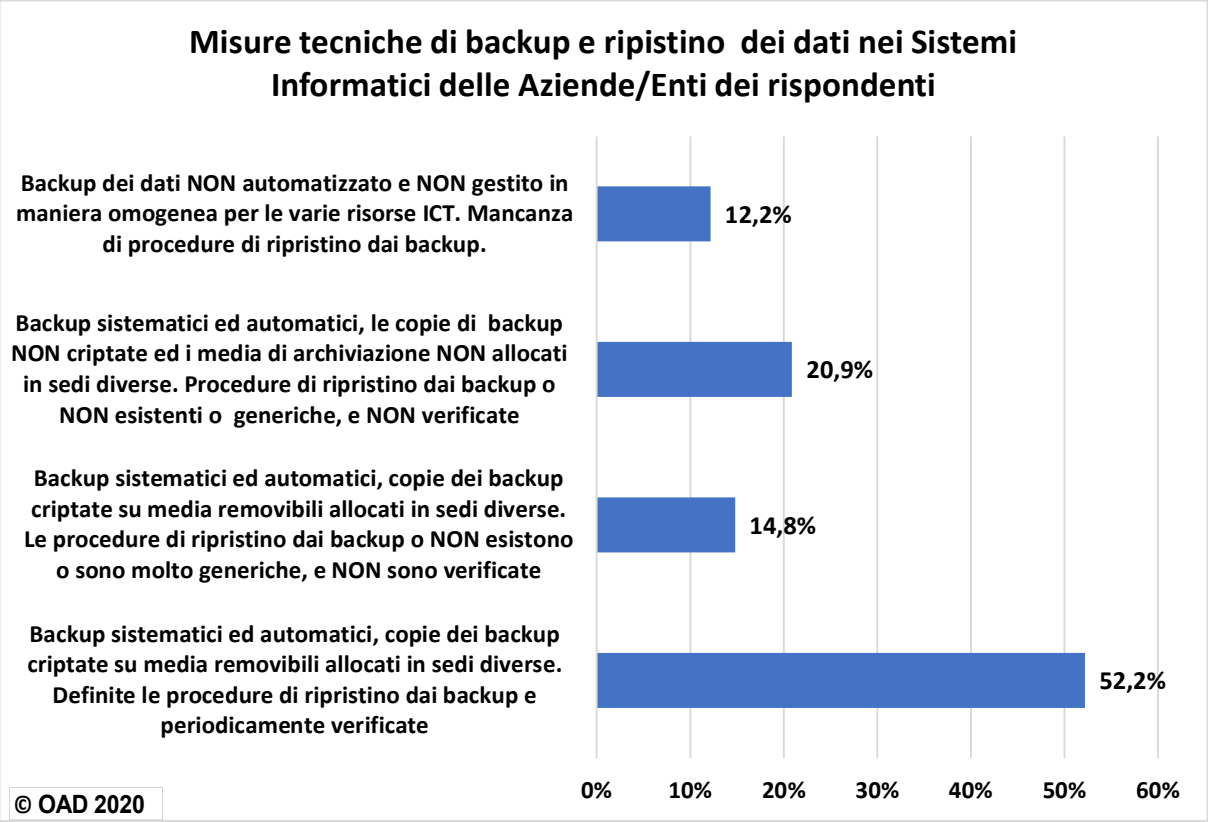


Fig. 9.2-9

9.3 Misure per la gestione della sicurezza digitale

Vari strumenti per la gestione della sicurezza digitale nel suo complesso sono un mix di strumenti tecnici ed organizzativi, ed alcuni strumenti possono essere considerati anche nelle misure di contrasto specifiche per area. L'autore ha voluto evidenziare in un capitolo a sé stante taluni strumenti per la gestione operativa della sicurezza digitale, che sovente sono integrati ed in parte coincidono con quelli per la gestione del sistema informatico e dei suoi componenti.

Le misure e gli strumenti che sono stati fatti rientrare nell'ambito del governo della sicurezza digitale, e che sono 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. Oltre a queste misure e strumenti, che per lo più operano in maniera continua e in tempo reale o quasi, sono considerati alcuni strumenti e logiche già trattate e considerate nei paragrafi precedenti, che includono strumenti di analisi e di gestione dei rischi, i sistemi per la gestione dei log degli utenti, il Disaster Recovery (DR). Questa ripetizione è voluta, da un lato tenendo conto che molti considerando questi come strumenti di gestione più che come strumenti di prevenzione e contrasto, dall'altro per verificare, almeno a grandi linee, la correttezza delle risposte fornite dai rispondenti[21].
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.

La fig. 9.3-1 mostra la situazione per l'inventario hardware delle risorse ICT del Sistema Informatico dell'Azienda/Ente dei rispondenti.

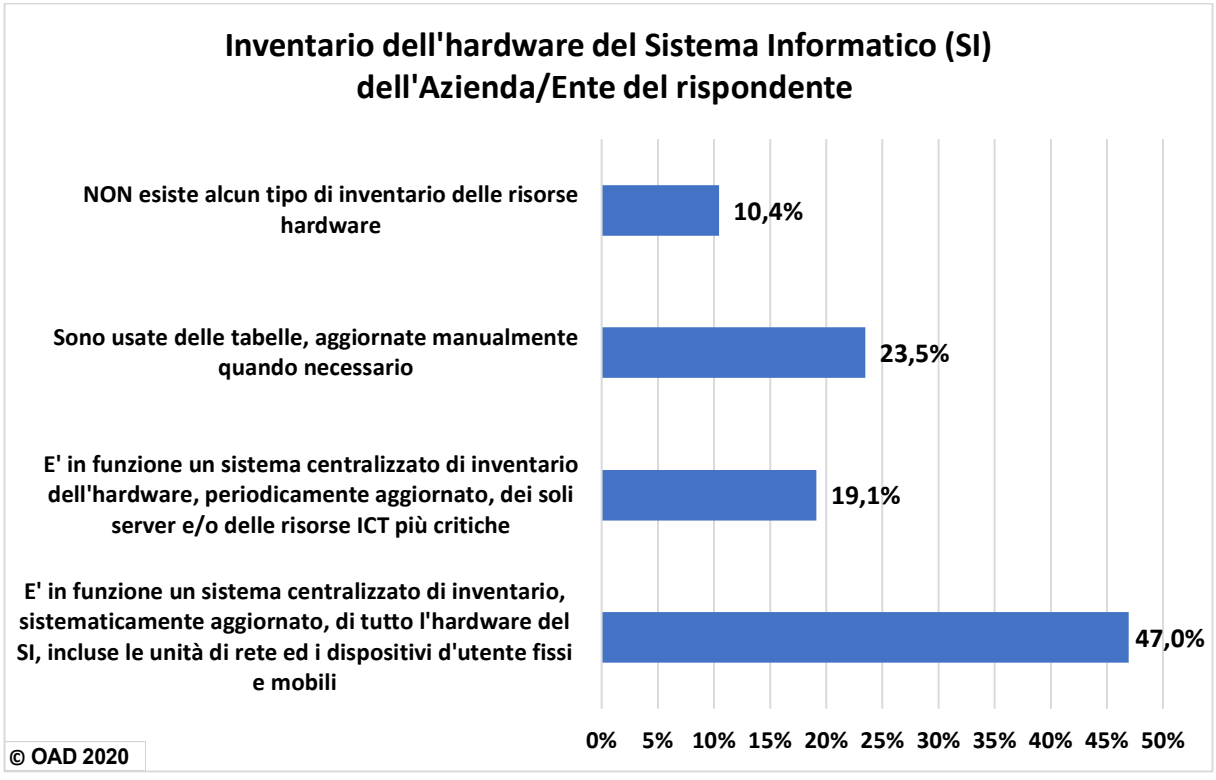


Fig. 9.3-1

[21] Risposte fortemente differenti sullo stesso tema fornite da un rispondente sono scartate nell'ambito della elaborazione dei dati raccolti dalle risposte on line al questionario.

Quasi i 2/3 dei rispondenti dispongono di sistemi centralizzati per l'inventario, e di questi il 19,1% solo per le risorse ICT più critiche. Il 23,5%, tipicamente per le piccole organizzazioni, utilizza dei fogli elettronici.
La fig. 9.3-2 mostra la situazione per l'inventario del software, ed in questo sono inclusi i servizi e gli ambienti terziarizzati in hosting e in cloud. La percentuale di chi ha l'inventario centralizzato del software, complessivamente il 60,9%, è inferiore rispetto a quella relativa all'hardware, 66,1% di cui sopra: è infatti più facile considerare l'hardware rispetto al software.

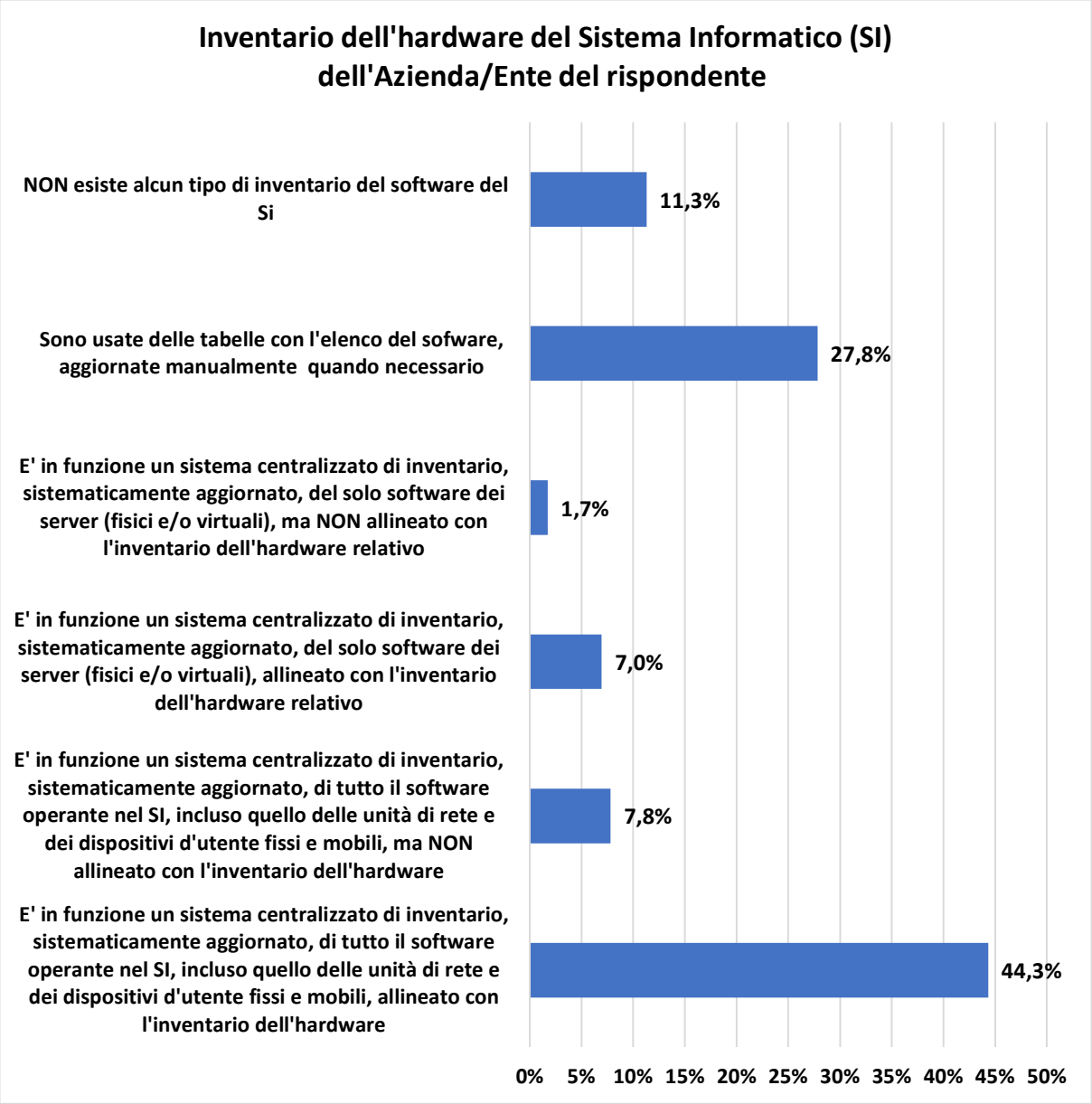


Fig. 9.3-2

Il 27,8% usa tabelle manuali, tipicamente fogli elettronici, e la percentuale è più alta rispetto all'analoga per l'hardware.
Anche per gli strumenti informatici e servizi per la gestione ed il controllo della sicurezza digitale del Sistema Informatico (SI), data la quantità e la complessità delle possibili soluzioni, per poter pesare le risposte previste e semplificare al contempo la compilazione del questionario, sono state previste le seguenti risposte tra cui scegliere, senza dettagli tecnici e riferimento a gruppi generali di soluzioni, con livelli di sicurezza a decrescere:

- Utilizzo di un SOC[22] (interno, terziarizzato, in mix interno-esterno), monitoraggio centralizzato, utilizzo di IDS/IPS, SIEM e gestione dei log, periodiche analisi di vulnerabilità e penetration test, strumenti di analisi comportamentale e/o di correlazione tra i vari dati, uso di tecniche di intelligenza artificiale e/o di autoapprendimento (learning machine).
- Utilizzo di un SOC (interno, terziarizzato, in mix interno-esterno), monitoraggio centralizzato, utilizzo IDS/IPS, SIEM e gestione log, periodiche analisi di vulnerabilità e penetration test ma non utilizzo di strumenti di intelligenza artificiale e/o di autoapprendimento (learning machine).
- Utilizzo del solo monitoraggio centralizzato, ma sistematico.
- Non si dispone alla data di strumenti di gestione della sicurezza digitale, ma è in corso o è a piano una loro implementazione nel breve-medio termine.
- Non si dispone alla data di strumenti specifici per la gestione ed il controllo sistematico della sicurezza digitale. Eventuali interventi sono effettuati di volta in volta in locale a seguito di segnalazioni.

La fig. 9.3-3 mostra la diffusione dei gruppi di strumenti di gestione della sicurezza sopra elencati nei Sistemi Informatici delle Aziende/Enti dei rispondenti: una situazione nettamente migliorativa rispetto a quanto rilevato nelle indagini degli anni scorsi, dato che il 42,8% dichiara l'utilizzo di sistemi avanzati, con o senza l'uso delle più moderne tecniche di intelligenza artificiale. Questo dato è sicuramente dovuto alla crescente diffusione in Italia di soluzioni SOC avanzate in cloud, e di soluzione basate su logiche SASE e SOAR sempre offerte "*as a service*" ed a prezzi molto interessanti.
Poco più di ¼ dei rispondenti evidenzia che viene effettuato solo il monitoraggio centralizzato del Sistema Informatico, e questo probabilmente è ritenuto sufficiente anche per l'individuazione di problemi sulla sicurezza digitale. Il 18,8% asserisce che idonei sistemi di gestione della sicurezza sono a piano nel breve tempo, ed il 12,5 ammette di non aver alcun sistema di gestione della sicurezza, e che i problemi relativi vengono di volta in volta individuati dagli utenti e risolti in loco, sul sistema ICT causa del problema.

Le varie tecniche di intelligenza artificiale costituiscono uno dei fronti più innovativi nell'ambito della sicurezza digitale, soprattutto per correlare grandi numeri di informazioni e di log, e per individuare comportamenti di persone e/o di sistemi ICT considerati anomali rispetto ai loro abituali funzionamenti, e cercare così di prevenire deterioramenti funzionali ed attacchi.
La complessità dei moderni sistemi informatici e la produzione di una miriade di segnalazioni non consentono, per essere realmente gestiti e in tempi quasi reali, una gestione non automatizzata. La gestione manuale non ha ormai più senso, nemmeno nelle realtà di medio-piccole dimensioni.

[22] SoC, Security Operation Center: è un centro interno all'Azienda/Ente o esterno, ossia terziarizzato in toto o in parte a società specializzate, che attua la gestione operativa della sicurezza digitale, monitorando i sistemi ICT, gli utenti, le vulnerabilità ed i rischi digitali. Effettua quando necessario gli opportuni interventi di prevenzione, protezione e di ripristino.

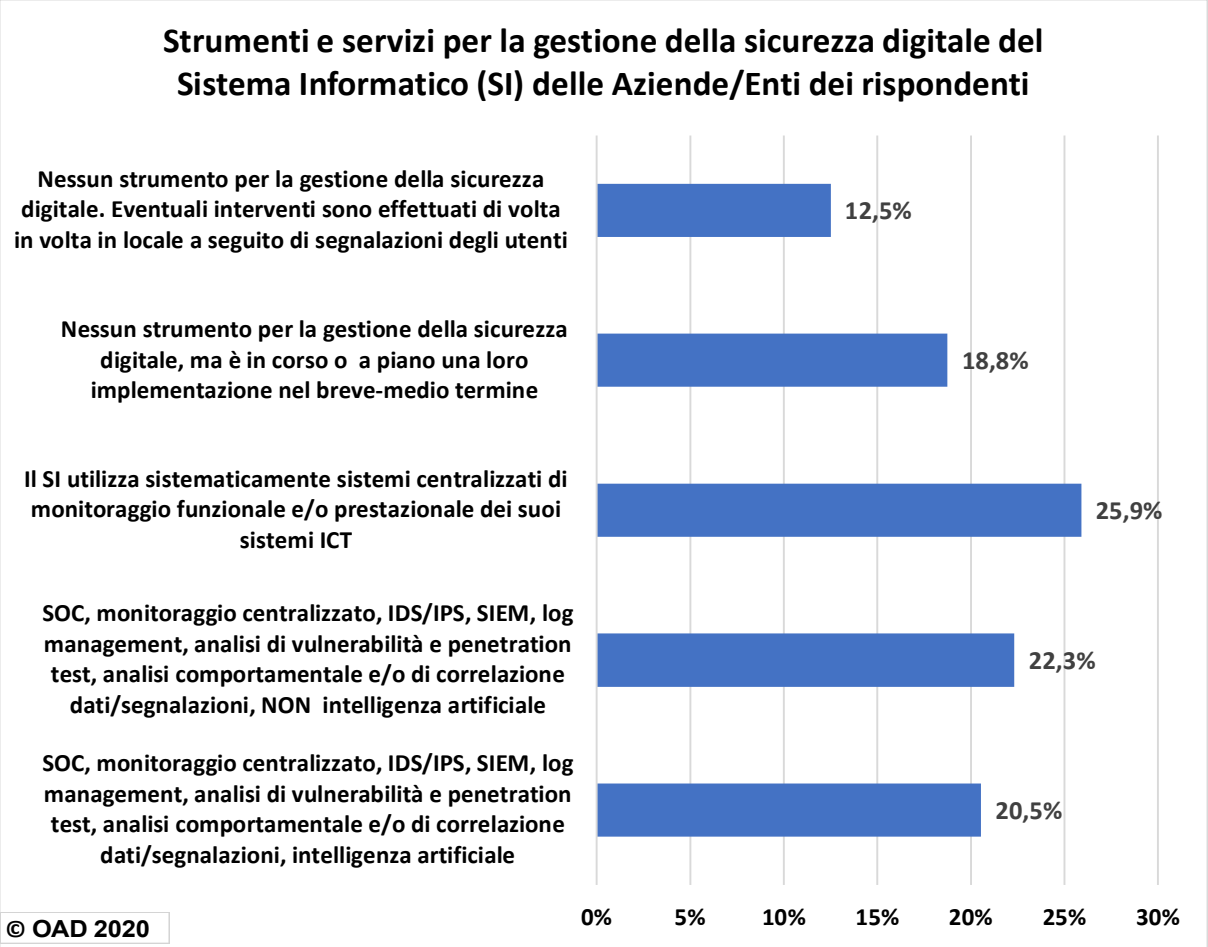


Fig. 9.3-3

Nell'ambito della gestione della sicurezza digitale un aspetto importante è la definizione di un Piano di Disaster Recovery (DR) del Sistema Informatico, che consenta all'Azienda/Ente, in caso di "disastro", di poter disporre di almeno le principali risorse ICT per poter garantire la continuità operativa dei processi e delle attività che non possono e che non dovrebbero fermarsi nemmeno in caso di disastro. Per questo motivo il Piano DR fa sovente parte del più generale Piano di Continuità Operativa (Business Continuity Plan) per l'intera Azienda/Ente. I frequenti terremoti ed altri disastri naturali in Italia, oltre alla pandemia Covid-19, costituiscono un ambito tale da richiedere effettivi piani di DR e di BC anche per medie e piccole organizzazioni, non solo per quelle grandi e grandissime. È necessario inoltre evidenziare la differenza tra avere un piano di DR e disporre delle risorse ICT per poterlo attuare: il piano di DR è un documento, più o meno dettagliato, che specifica come e quando attuare un DR con quali misure tecniche ed organizzative. La disponibilità delle risorse ICT per attivare il DR in siti remoti ed alternativi significa aver attivato, e quindi pagare, la disponibilità di tali risorse ICT alternative a quelle del sistema informatico.
Molte Aziende/Enti hanno un piano di DR, ma non hanno in parallelo già "riservato" le risorse ICT alternative, anche virtuali, necessarie per poter riattivare almeno le parti essenziali del sistema informatico su queste risorse alternative. In aggiunta, occorre provare periodicamente le procedure relative al DR con tutto il personale predefinito da coinvolgere (si veda in particolare l'ERT in fig. 9.1.2-4 e in §9.1.4)

Sulla base di queste considerazioni il questionario 2020 OAD ha predisposto le possibili risposte alla domanda sul DR.
La fig. 9.3-4 mostra la situazione emersa dai rispondenti, che come tutte le precedenti evidenzia un netto miglioramento rispetto alle precedenti indagini OAD. Il 38,3% afferma di disporre del Piano di DR e delle risorse ICT alternative da utilizzare in caso di disastro, e di effettuare periodicamente delle esercitazioni (tipicamente a tavolino, chiamate DTE, Desk Top Exercise). È la situazione tecnico-organizzativa allo stato dell'arte. Un altro 42% ha il Piano di DR, ma senza risorse alternative o senza DTE.
Quindi in totale 80,2% dei rispondenti ha un Piano di DR definito, ma più della metà non saprebbe come usarlo: purtroppo un tipico esempio "all'italiana" dove i vari piani, ammesso che siano aggiornati, esistono solo per aspetti burocratici ma nella pratica poi non sono (il più delle volte) attuabili.

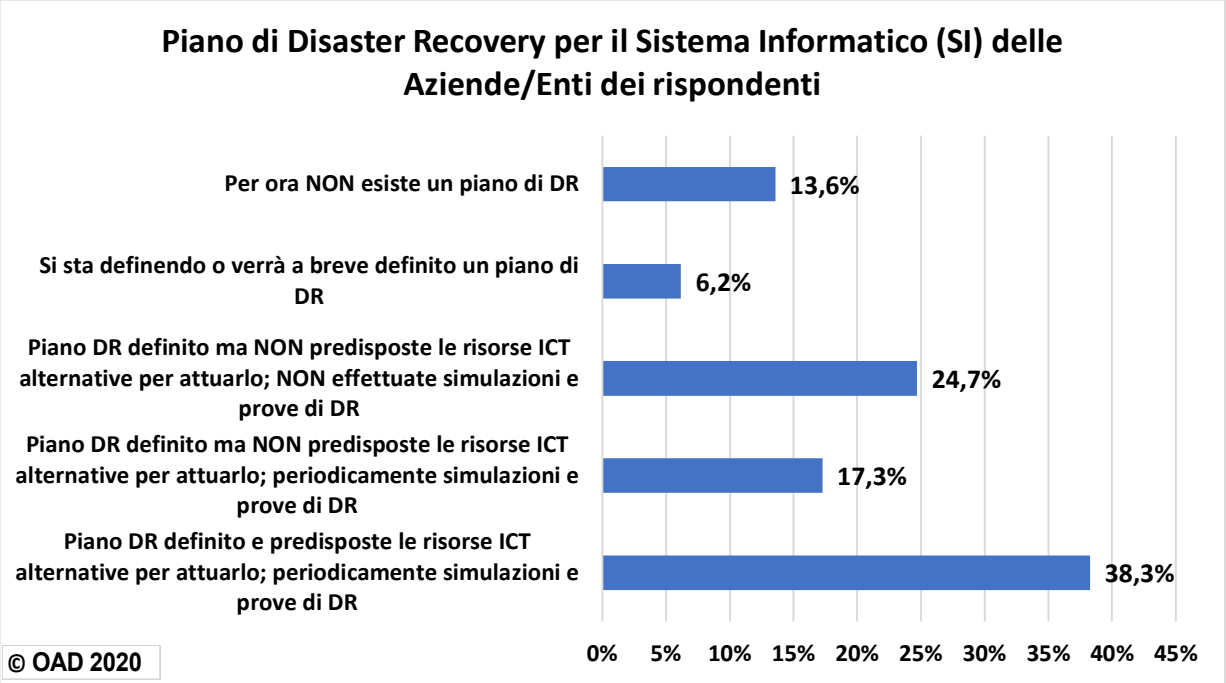


Fig. 9.3-4

10. Il campione di rispondenti e delle loro Aziende/Enti emerso dall'indagine

Le risposte avute al questionario OAD 2020 sono state 310, rispetto alle 296 di OAD 2019 e alle 269 di OAD 2018. La cosa positiva è che il numero di risposte complete, ossia di tutte le 127 domande articolate in 7 sezioni del questionario 2020, è stato superiore a quelle dell'anno precedente.
I potenziali rispondenti sono stati contatti prevalentemente via posta elettronica, tramite le segnalazioni sui siti web e sui social network da AIPSI, Malabo e Reportec, oltre che dalle Associazioni patrocinanti.
Le risposte ricevute sono in numero sufficiente e significativo per poter fornire delle concrete indicazioni sugli attacchi ai sistemi informatici in Italia e su quali sono le principali misure di contrasto messe in atto.

10.1 Ruolo del rispondente nell'azienda/ente

Il bacino di rispondenti, assolutamente anonimi è costituito prevalentemente da CIO e da figure operanti nella struttura dei sistemi informatici, la UOSI, Unità Organizzativa Sintemi Informatici, dai fornitori ICT e dai consulenti che gestiscono per l'Azienda/Ente la sicurezza digitale (interamente o sue parti), fino ai responsabili di massimo livello delle aziende piccole e piccolissime che conoscono e decidono per i loro sistemi informatici e la relativa sicurezza. I CISO, Chief Information Security Officer, i responsabili della sicurezza digitale, che dovrebbero essere i rispondenti più diffusi, sono al quarto posto con un 10,3% sul totale dei rispondenti. Il motivo è semplice: in Italia questo ruolo esiste prevalentemente solo nelle grandi organizzazioni e l'Italia, come già evidenziato in più occasioni all'interno del presente rapporto, è il paese delle piccole e piccolissime organizzazioni.

La fig. 10.1-1 mostra la ripartizione dei compilatori per ruolo: per la prima volta nel corso dei 12 anni di indagini di OAD, al primo posto tra i rispondenti, con il 27,8% il personale di strutture organizzative dell'Azienda/Ente che non appartengono all'UOSI, l'Unità Organizzativa Sistemi Informatici: tipici probabili esempi, soprattutto nelle medie grandi organizzazioni, personale in staff alla direzione generale, personale dell'organizzazione o delle pubbliche relazioni. Al secondo posto, con un 21,6%, il vertice dell'Azienda/Ente, quale ad esempio il Proprietario, il Partner, il Presidente, l'Amministratore Unico o Delegato, il CEO Chief Executive Officer/Direttore Generale. Per le piccole e piccolissime organizzazioni è il vertice che decide sul sistema informatico e che di fatto coordina e supervisiona i fornitori ed i consulenti che vi operano: e per queste strutture è questo vertice che ha risposto al questionario (si veda anche fig. 10.2-4). Il CIO, Chief Information Officer, il responsabile del sistema informatico, si posiziona al terzo posto con un 18,6% sul totale dei rispondenti. Seguono con percentuali decrescenti altri ruoli tra i quali il CSO, Chief Security Officer, responsabile della sicurezza dell'intera Azienda/Ente ed il CTO, Chief Technology Officer, che si posiziona all'ultimo posto.

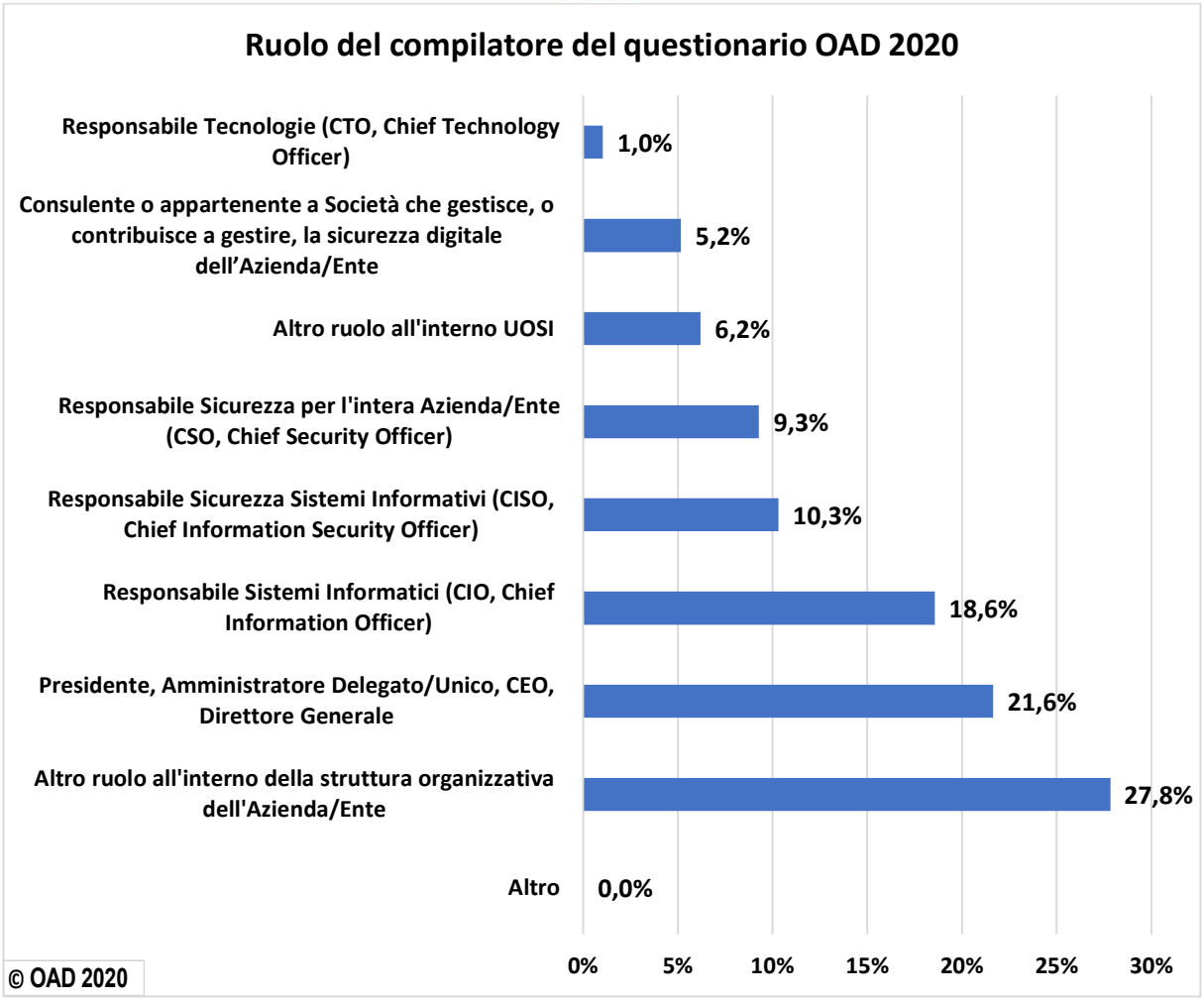


Fig. 10.1-1

10.2 L'Azienda/Ente del rispondente

La fig. 10.2-1 riporta la tabella con la tassonomia della classificazione di OAD dei settori merceologici: essa fa riferimento alla classificazione ATECO, sulla cui base si sono raggruppati alcune classi e alla quale si sono aggiunte le Pubbliche Amministrazioni Centrali e Locali.
Questa classificazione abbastanza dettagliata, pur con vari raggruppamenti, è stata ritenuta utile per ridurre possibili errori di posizionamento della loro azienda da parte dei rispondenti. Problema che era emerso nei primi anni dell'indagine OAI/OAD.
La fig. 10.2-2 mostra la ripartizione merceologica delle Aziende/Enti dei rispondenti secondo la Tabella di cui sopra. Da un lato, essa evidenzia che il bacino dei rispondenti emerso con l'indagine del 2020 copre tutti i settori merceologici elencati ma, dall'altro, che i rispondenti appartengono per la quota maggiore al settore ICT, con un 30,7%, cui seguono i raggruppamenti di settore considerati, ma tutti con una percentuale decrescente nella fascia del 10%.
A parte il settore dell'ICT, tutti gli altri settori merceologici hanno avuto dei rispondenti, ma con percentuali troppo basse di rispondenti perché possano essere elaborate rappresentative tendenze settoriali. Per questo motivo nel presente rapporto non sono state elaborate analisi e correlazioni per settori, ma solo per dimensione delle Aziende/Enti come numero di dipendenti.

1. Settore primario: agricoltura, allevamento, pesca, estrazione (Codici Ateco A e B)
2. Industria manifatturiera e costruzioni: meccanica, chimica, farmaceutica, elettronica, alimentare, edilizia, ecc. (Codici Ateco C e F)
3. Utility: Acqua, Energia, Gas ecc. (Codici Ateco D ed E)
4. Commercio all'ingrosso e al dettaglio, incluso quello di apparati ICT (Codici Ateco G)
5. Trasporti e magazzinaggio (Codice Ateco H)
6. Attività finanziarie ed assicurative: assicurazioni, banche, istituti finanziari, broker, intermediazione finanziaria, ecc. (Codice Ateco M)
7. Servizi turistici, di alloggio e ristorazione: agenzie di viaggio, tour operator, hotel, villaggi turistici, campeggi, ristoranti, bar, etc. (Codice Ateco I e N79)
8. Attività artistiche, sportive, di intrattenimento e divertimento: teatri, biblioteche, archivi, musei, lotterie, case da gioco, stadi, piscine, parchi, discoteche, etc. (Codice Ateco R)
9. Stampa e servizi editoriali (Codice Ateco J58)
10. Servizi professionali e di supporto alle imprese: attività immobiliari, notai, avvocati, commercialisti, consulenza imprenditoriale, ricerca scientifica, noleggio, call center, etc. (Codici Ateco L, M, N77, N78, N80, N81, N82)
11. Servizi ICT: consulenza, produzione software, service provider ICT, gestione Data Center, servizi assistenza e riparazione ICT, etc. (Codici Ateco J62, J63, S95.1)
12. Telecomunicazioni e Media: produzione musicale, televisiva e cinematografica, trasmissioni radio e televisive, telecomunicazioni fisse e mobili (Codici Ateco J59, J60, J61)
13. Sanità e assistenza sociale: ospedali pubblici o privati, studi medici, laboratori di analisi, etc. (Codice Ateco Q)
14. Istruzione: scuole e università pubbliche e private (Codice Ateco P)
15. Associazioni, associazioni imprenditoriali e sindacati (Codice Ateco S94)
16. PAC, Pubblica Amministrazione Centrale
17. PAL, Pubblica Amministrazione Locale

Fig. 10.2-1 Tabella dei raggruppamenti in settori merceologici considerati

La fig. 10.2-3 mostra la ripartizione percentuale delle aziende/enti dei rispondenti per dimensioni, in termini di numero di dipendenti, distinguendo in quattro classi quelle fino a 250 dipendenti, che raggruppano 57,7% dei rispondenti (erano il 62,6% nella precedente edizione); altre 3 classi per le grandi e grandissime, che complessivamente coprono il rimanente con un 42,3% (erano il 37,4% nella precedente edizione. Nella presente indagine sono quindi aumentati, e non di poco, i rispondenti di grandi organizzazioni: questo è uno dei motivi per il quale al primo posto dei rispondenti, come ruolo, si sono posizionate figure che non appartengono direttamente al mondo ICT ed UOSI, come indicato nella fig. 10.1-1.

La distribuzione per dimensione delle aziende/enti del campione emerso risulta abbastanza ben bilanciato e rappresentativo delle varie classi considerate in OAD, ed anche in riferimento alle già citate e più recenti statistiche ISTAT sulle imprese attive (§6 e fig. 6-4), pur con una percentuale ben più alta per le organizzazioni oltre i 250 dipendenti. La Tabella di fig. 10.2-4 confronta, a livello percentuale, la ripartizione ISTAT con quella emersa dal bacino dei rispondenti al questionario 2019 OAD.
Per le Pubbliche Amministrazioni, centrali e locali, non si hanno dati precisi: le stime più autorevoli indicano circa 55.000 enti, *con autonomia funzionale e finanziaria*, incluse scuole, ASL ed ospedali.

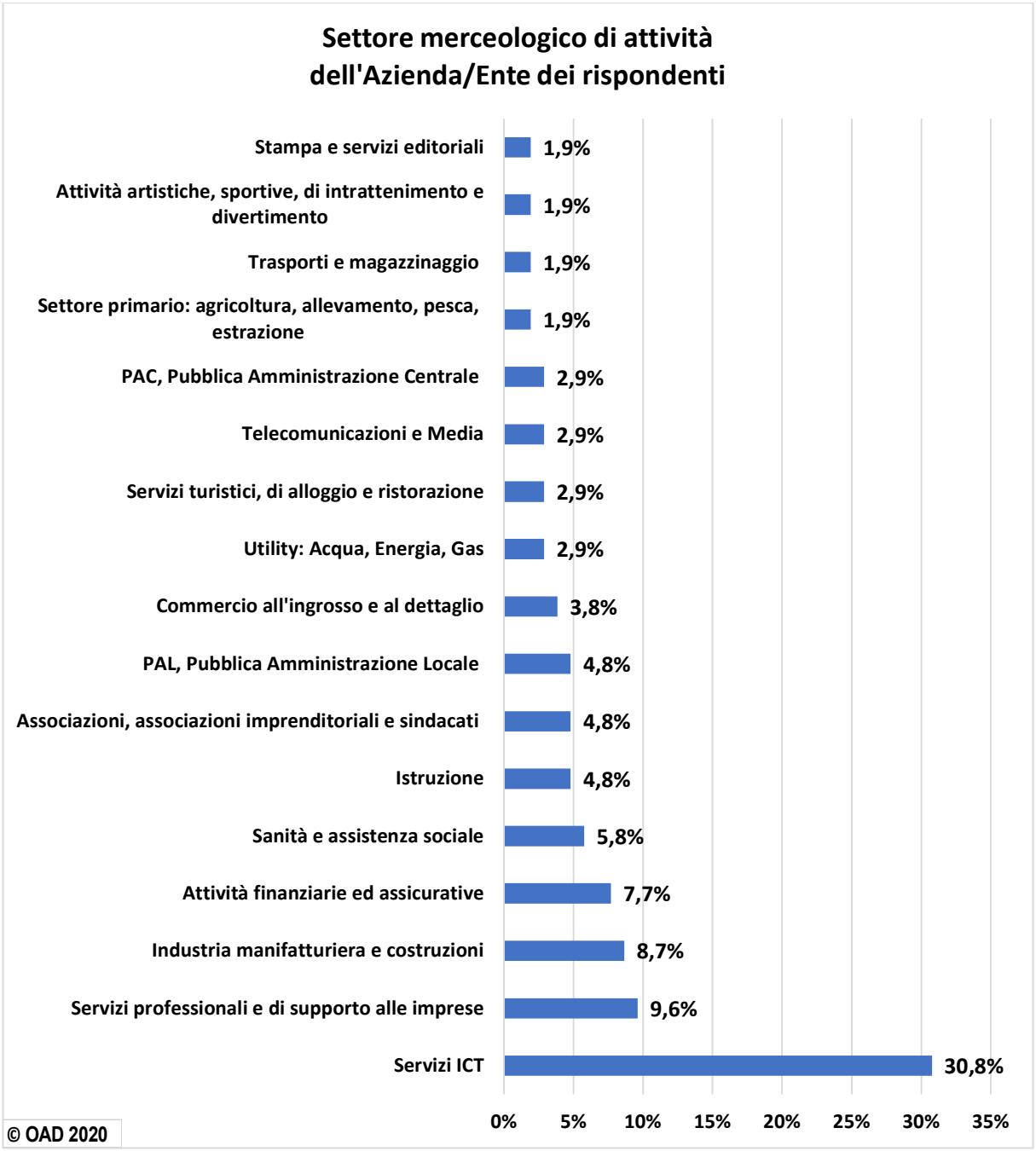

Settore merceologico di attività dell'Azienda/Ente dei rispondenti
Stampa e servizi editoriali 1,9%
Attività artistiche, sportive, di intrattenimento e divertimento 1,9%
Trasporti e magazzinaggio 1,9%
Settore primario: agricoltura, allevamento, pesca, estrazione 1,9%
PAC, Pubblica Amministrazione Centrale 2,9%
Telecomunicazioni e Media 2,9%
Servizi turistici, di alloggio e ristorazione 2,9%
Utility: Acqua, Energia, Gas 2,9%
Commercio all'ingrosso e al dettaglio 3,8%
PAL, Pubblica Amministrazione Locale 4,8%
Associazioni, associazioni imprenditoriali e sindacati 4,8%
Istruzione 4,8%
Sanità e assistenza sociale 5,8%
Attività finanziarie ed assicurative 7,7%
Industria manifatturiera e costruzioni 8,7%
Servizi professionali e di supporto alle imprese 9,6%
Servizi ICT 30,8%
0% 5% 10% 15% 20% 25% 30% 35%
© OAD 2020

Fig. 10.2-2

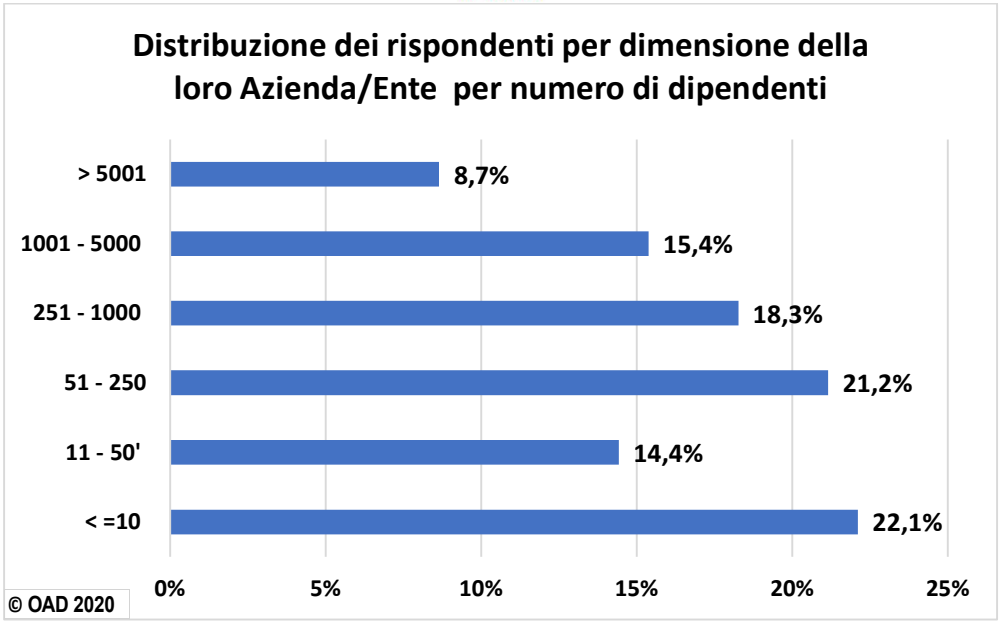


Fig. 10.2-3

ISTAT: Imprese private per numero dipendenti	ISTAT 2020 Numero Imprese	% sul totale ISTAT 2020	% rispondenti OAD 2020
< 10	4.180.761	94,92%	22,10%
11-49	196.076	4,45%	14,40%
50-249	23.647	0,54%	21,20%
>250	4.017	0,09%	42,30%
Totale imprese ISTAT /rispondenti OAD 2020	4.404.501		310
PMI 1-249	4.400.484	99,91%	57,70%

Fig. 10.2-4

La fig. 10.2-5 mostra la ripartizione percentuale delle aziende/enti dei rispondenti per il fatturato annuo nell'ultimo anno disponibile, fatturato suddiviso nelle quattro classi indicate nel questionario e riportate in figura.
Il questionario 2019 prevedeva: fino a € 500.000, da € 500.000 a 1 Milione, da 1 a 5 Milioni €, oltre i 5 Milioni di €.

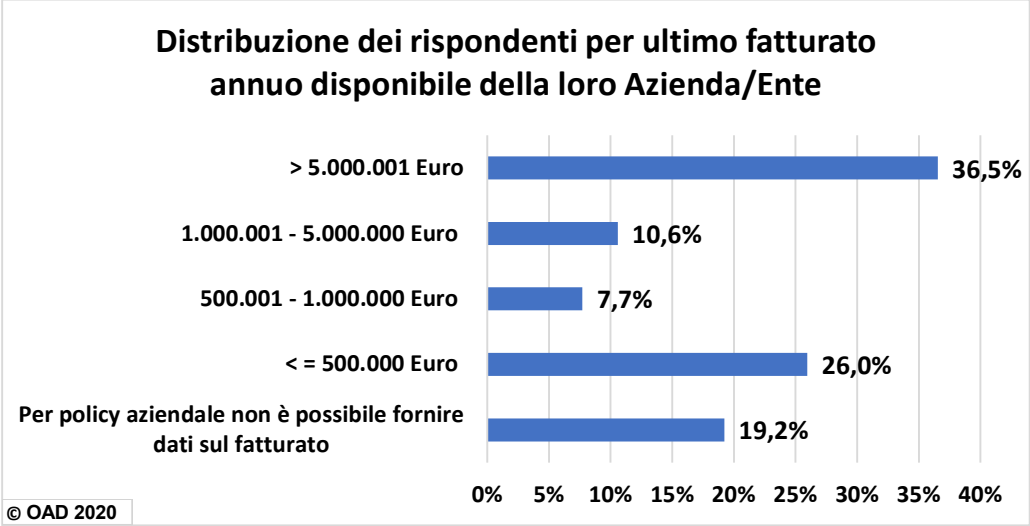


Fig. 10.2-5

Il bacino di rispondenti emerso dall'indagine è abbastanza ben bilanciato rispetto alla distribuzione di fatturato annuo, considerando il numero ben maggiore di strutture piccole rispetto alle grandi, e quindi di fatturati piccoli rispetto a quelli grandi. La maggior parte dei rispondenti, 36,5% dichiara che la sua Azienda/Ente fattura più di 5 milioni nell'ultimo anno di bilancio. Da sottolineare che quasi 1/5 dei rispondenti non ha potuto/voluto fornire la classe di fatturato nella quale rientra, affermando che le policies di riservatezza gli impedivano di indicare una classe di fatturato, pur in una indagine completamente anonima.

La fig. 10.2-6 mostra la distribuzione dell'Azienda/Ente del dipendente per area geografica di copertura delle attività svolte: la stragrande maggioranza opera in Italia, il 77,9% e di questi il 43,3% nel solo nord Italia, mentre il 21,2% opera a livello internazionale con l'Europa ed il resto del mondo.

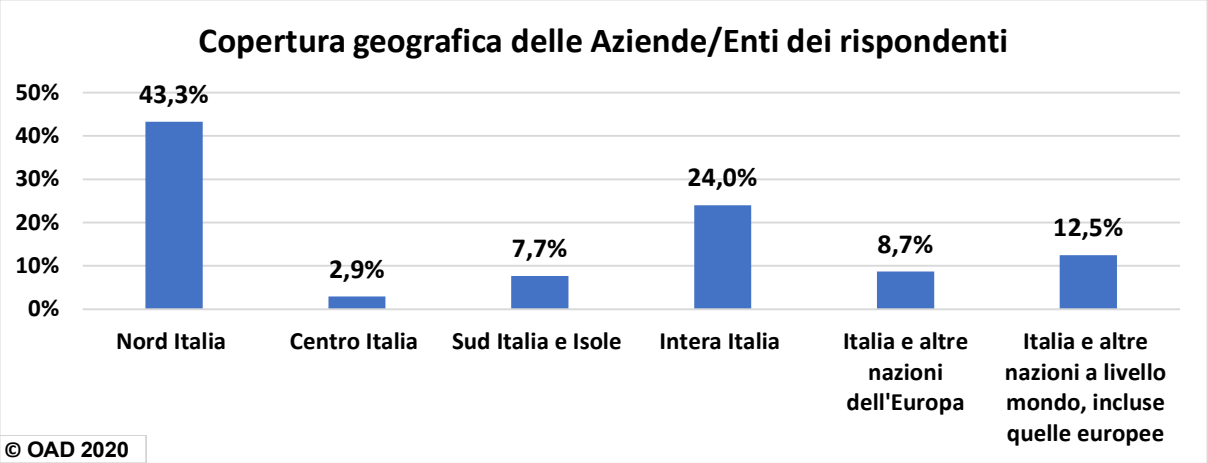


Fig. 10.2-6

10.3 Macro-caratteristiche dei sistemi informatici delle aziende/enti dei rispondenti

Come per tutte le precedenti edizioni di OAI-OAD, anche nell'edizione 2020 il questionario OAD poneva alcune domande per inquadrare tecnicamente il tipo di Sistema Informatico (SI) dell'Azienda/Ente del rispondente, iniziando dalle sue macro-caratteristiche.
La fig. 10.3-1 mostra, con risposte multiple, che per il 43,9% dei rispondenti il SI opera ed è gestito e controllato in Italia, e per il 29,9% utilizza soluzioni in cloud o terziarizzate con specifici fornitori.
Il 18,1% dei SI dei rispondenti ha uno o più Data Center in Italia, e per il 9% il SI in Italia è solo una parte di un più grande SI operante a livello internazionale ed il cui controllo non è in Italia: solo il 4,5% ha il controllo del SI mondiale in Italia.

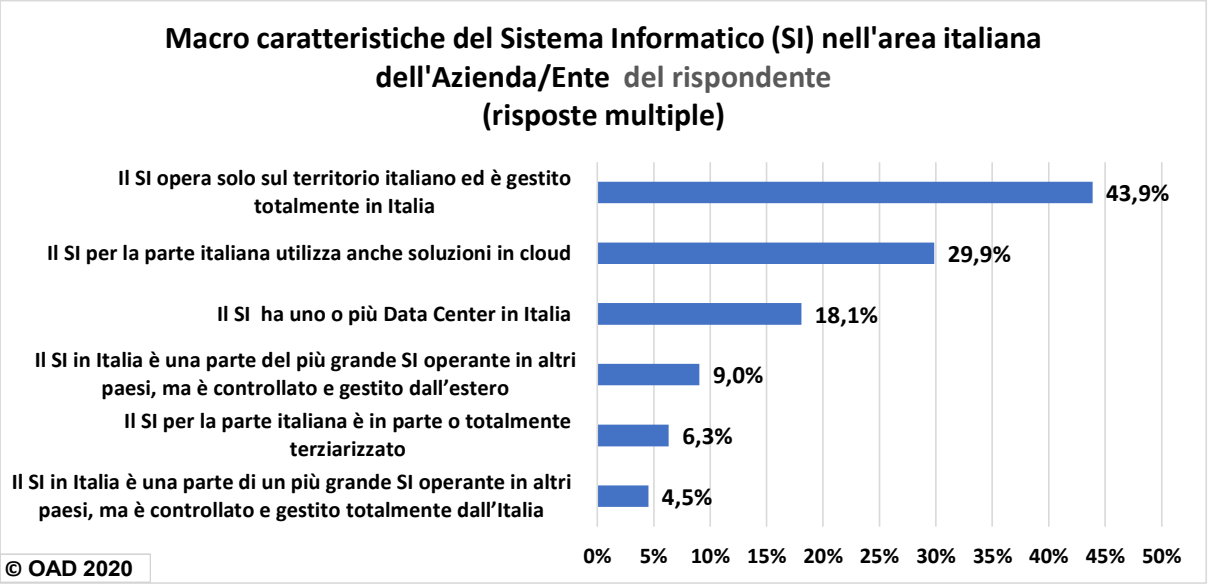


Fig. 10.3-1

La fig. 10.3-2 fornisce le dimensioni del Sistema Informatico del rispondente come numero di utenti configurati, ossia di utenti potenziali nel dimensionamento del SI stesso: i dati confermano che la maggior parte dei SI sono di piccole dimensioni.

Per comprendere il fabbisogno di sicurezza digitale per il Sistema Informatico oggetto delle risposte al questionario, è importante conoscere, almeno a livello qualitativo, qual è la sua strategicità per il business e per le attività dell'Azienda/Ente del rispondente. La fig. 10.3-3 evidenzia che per quasi i ¾ dei rispondenti il SI è essenziale per il funzionamento delle attività e dei processi, e quindi per il business.

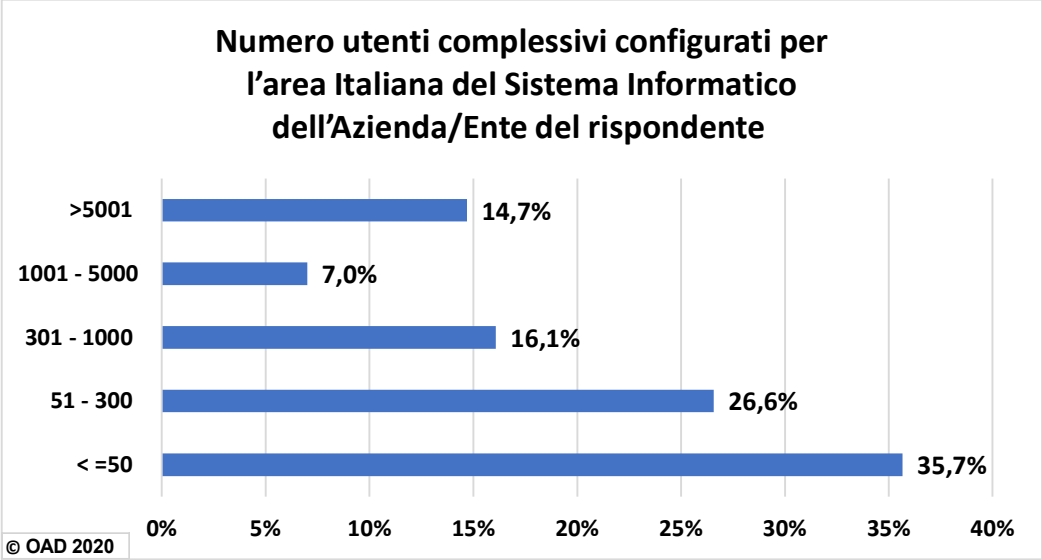


Fig. 10.3-2

Sempre per comprendere il fabbisogno di sicurezza digitale, la fig. 10.3-4 riporta la percentuale dei SI dell'Azienda/Ente che hanno applicazioni per il trattamento di dati personali e sensibili, e che quindi devono soddisfare le normative sulla privacy, in particolare il GDPR e le raccomandazioni emanate dall'Autorità Garante italiana: la quasi totalità li tratta, ed in particolare il 51,8% tratta dati sensibili[23] della privacy e quindi deve obbligatoriamente proteggere tali dati come sancito dal GDPR. Si ricorda che, per evitare gli obblighi di comunicazione a tutti gli interessati e alle autorità in caso di data breach, è necessario che questi dati siano crittografati.

[23] Nel regolamento GDPR il termine "dati sensibili" non è più definito come lo era nei precedenti codici, ma data la sua consolidata diffusione, viene riutilizzato nel rapporto per facilmente indicare i dati relativi alla salute, i dati genetici e biometrici.

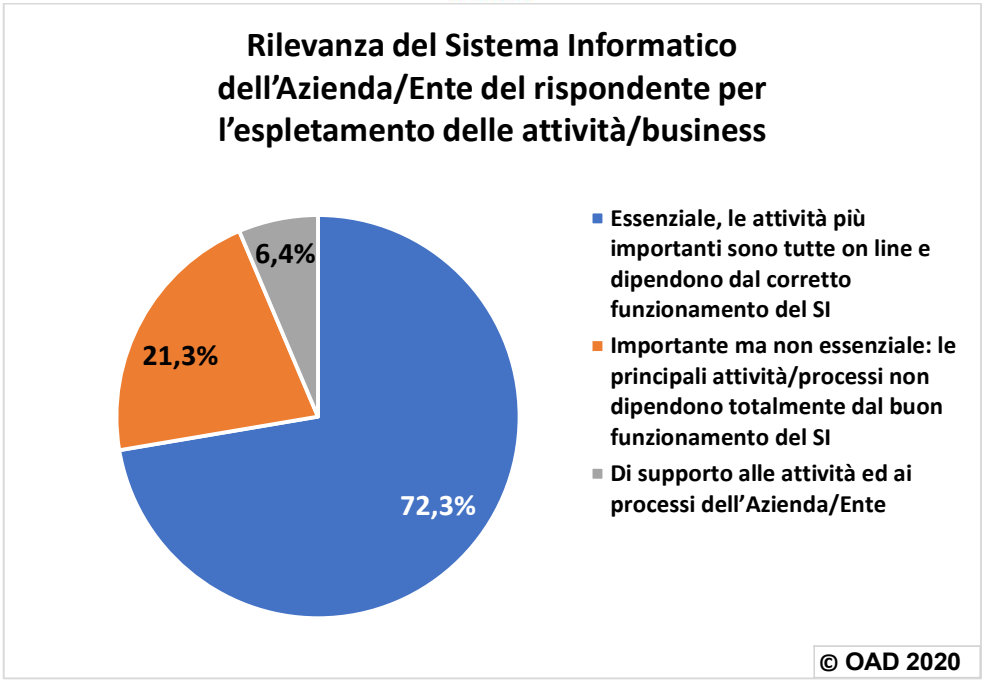


Fig. 10.3-3

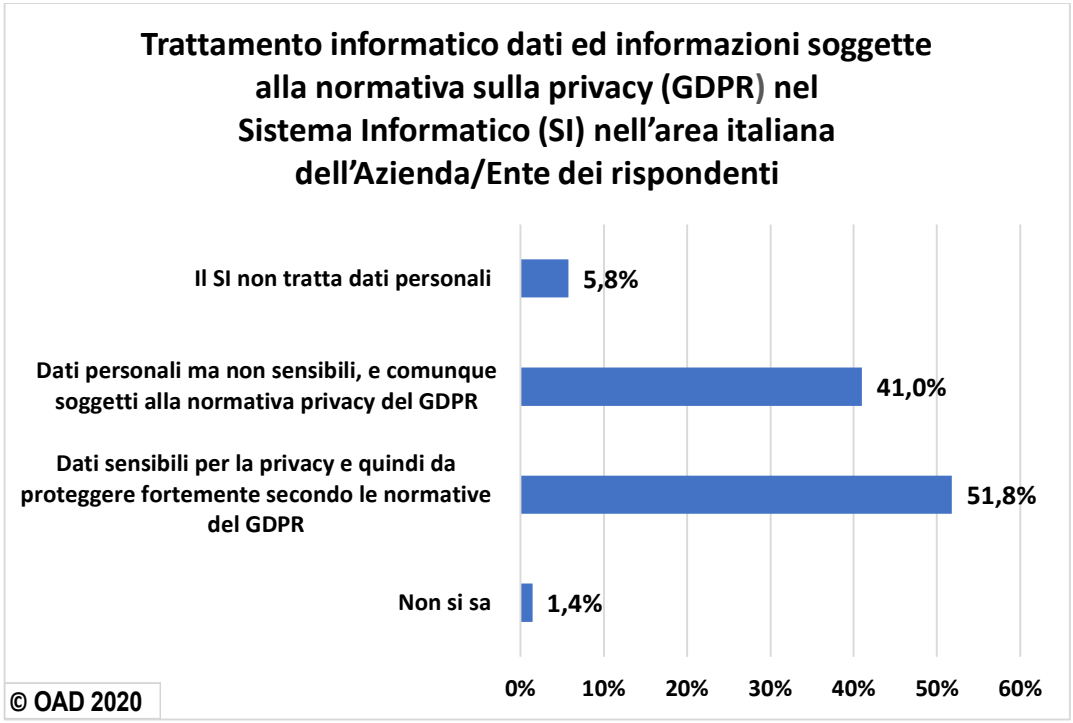


Fig. 10.3-4

I dati personali non sono le uniche informazioni critiche trattate dalle applicazioni del SI: si pensi ad esempio ai piani di sviluppo, ai segreti industriali, all'elenco dei clienti e dei fornitori con le condizioni

di vendita ed acquisto, e così via. La fig. 10.3-5 mostra quali SI dei rispondenti trattano informazioni critiche e riservate, indipendentemente da quelle personali soggette alla normativa sulla privacy, e che come tali richiedono un elevato livello di protezione digitale. Il 73,8% tratta informazioni critiche riservate, e di queste il 26,1% sono molto critiche e molto riservate.

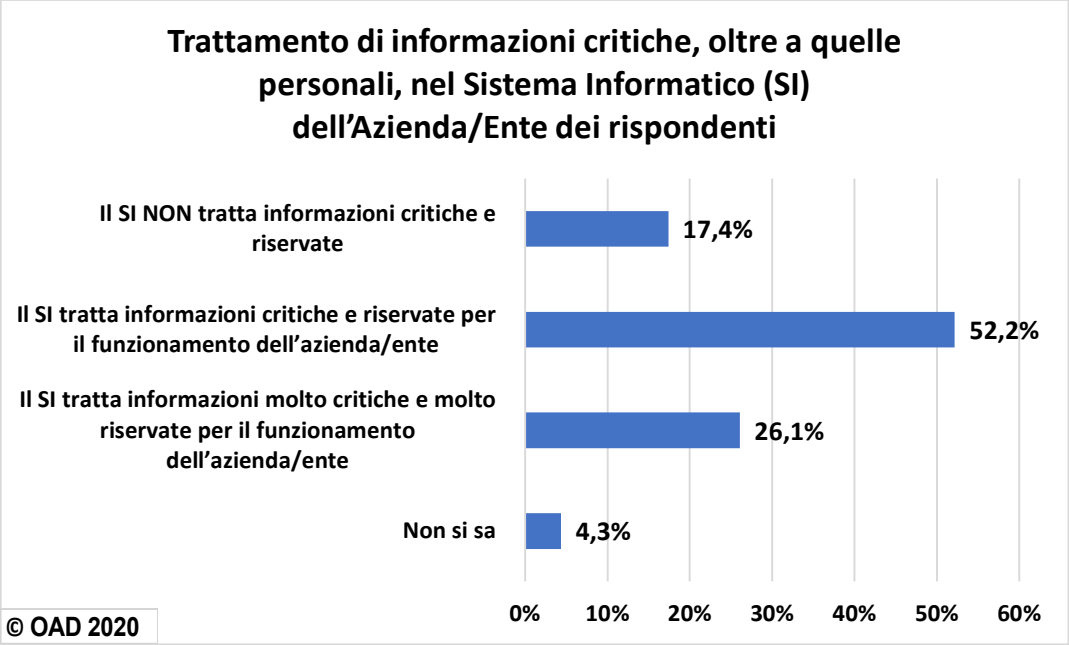


Fig. 10.3-5

11. 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 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.
Il contrasto ai crimini informatici si basa principalmente sulla prevenzione, sul far conoscere e far comprendere a tutti gli utenti - dalle aziende ai singoli cittadini - quali siano i pericoli di Internet e come fare per strutturare l'attività del commercio elettronico in maniera sicura, corretta ed efficiente.
La Polizia Postale e delle Comunicazioni opera da anni in questa direzione, con azioni di formazione e di sensibilizzazione a vari livelli, sia a livello regionale per organizzazioni imprenditoriali ed enti, sia a livello nazionale.

11.1 Infrastrutture critiche (C.N.A.I.P.I.C.) e computer crime

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.
Le Infrastrutture Critiche 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.
Per le Infrastrutture Critiche a livello europeo è stata emanata la Direttiva 2008/114/CE[24], per individuare e designare le infrastrutture critiche europee, nonché un approccio per migliorarne la protezione. Essa, pur se focalizzata solo sui settori dell'energia e dei trasporti, ben definisce come infrastruttura critica "*"un elemento, un sistema o parte di questo ubicato negli Stati membri che è essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale dei cittadini ed il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in uno Stato membro a causa dell'impossibilità di mantenere tali funzioni".*
Tale direttiva è stata recepita in Italia con il D.Lgs n. 61 dell'11 aprile 2011[25].

Protezione strutture critiche	1 gen - 31 dic 2019	1 gen – 31 dic 2018	1 gen – 31 dic 2017	1 gen – 31 dic 2016
Attacchi rilevati	**1181**	**459**	**1.032**	**844**
Alert diramati	**82484**	**80.777**	**31.524**	**6.721**
Indagini avviate	**155**	**74**	**72**	**70**
Persone arrestate	**3**	**1**	**3**	**3**
Persone denunciate	**117**	**14**	**1.316**	**1.226**
Perquisizioni	**n.d.**	**n.d.**	**73**	**58**
Richiesta di cooperazione internazionale in ambito Rete 24/7 High Tech Crime G8 (Convenzione Budapest)	**79**	**108**	**83**	**85**

Fig. 11.1-1 Attività per la protezione delle Infrastrutture Critiche dal 2016 al 2019 (Fonte: Polizia Postale e delle Comunicazioni)

[24] https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32008L0114
[25]http://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2011-05-04&atto.codiceRedazionale=011G0101&elenco30giorni=false

La tabella in fig. 11.1-1 confronta i dati forniti dalla Polizia Postale e delle Comunicazioni inerenti alle attività svolte dal C.N.A.I.P.I.C. nel quadriennio 2016-2019 sulle infrastrutture critiche italiane.
Numerose le considerazioni e gli spunti che si possono trarre dall'analisi di questi dati.
Il primo dato che emerge è il forte incremento di attacchi rilevati, nel 2019 quasi triplicato rispetto al 2018, tornando a livelli poco superiori del 2017. Ne è derivato un aumento delle indagini avviate nel 2019, raddoppiate rispetto al 2018, registrando ben 155 procedimenti investigativi contro gli appena 74 dell'anno precedente.
Un altro aspetto interessante è fornito dal leggero, seppur costante, aumento degli alert diramati, superiore di 2000 unità rispetto al 2018, anno in cui è stata registrata un'impennata delle segnalazioni da parte della Polizia Postale (più di 80,000 a fronte di appena 31,524 del 2017): pertanto, rimane un indicatore incontrovertibile della crescita dei rischi ICT, causato anche dalla più volte citata estensione dell'area potenziale di attacco dovuta anche dall'interoperabilità con ambienti OT ed in particolare IoT/IIoT.
Il numero delle persone denunciate è tornato ad aumentare con 117 denunce effettuate a seguito del drastico calo registrato nel 2018 – con appena 14 unità – mantenendosi comunque lontano dai dati registrati nel 2017 e nel 2016 che superavano il migliaio di unità.
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, alla fine gli arrestati si contano su una mano: 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.
Varie le cause concomitanti che provocano una simile "distorsione" nella persecuzione dei crimini digitali: in primis, la difficoltà nell'avviare un procedimento nei confronti del presunto attaccante, anche se si è riusciti ad individuarlo, in particolare se è di nazionalità straniera, presentando prove incontrovertibili della sua colpevolezza. La prima precauzione di un attaccante è quella di svolgere ogni sua azione con modalità il più possibile anonime, attaccando con agent inseriti su sistemi ICT di ignari possessori su scala mondiale, e cambiando molto velocemente, nell'ordine dei minuti, i sistemi da cui controlla e guida gli attacchi: anche questi ultimi risultano essere anonimizzati ed operanti da diverse nazioni.
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.
Per combattere realmente ed efficacemente il crimine digitale è fondamentale la collaborazione tra le varie forze di polizia ed i governi centrali, iniziando da quelli europei: in tale collaborazione internazionale, la Polizia Postale italiana è attiva e propositiva da anni, promuovendo e partecipando a vari gruppi di lavoro. Ad esempio, in ambito C.N.A.I.P.I.C. è attivo il Punto di Contatto Italiano per le emergenze tecnico-operative connesse al verificarsi di episodi di criminalità ICT transnazionale, secondo quando stabilito dalla Convenzione sul Cybercrime di Budapest del 2001[26]. L'ultima riga della tabella in fig. 11.1-1 mostra le richieste di collaborazione nell'ambito di questa Convenzione nei vari anni.
La fig. 11.1-2 mostra gli analoghi dati per il 1° quadrimestre 2020, che confermano quanto sopra discusso.

[26] Con Convenzione di Budapest si intende la Convenzione del Consiglio dell'Europa sulla criminalità informatica, stipulata a Budapest il 23 novembre 2001 (http://www.conventions.coe.int/Treaty/en/Treaties/Html/185.htm). l'Italia l'ha ratificata con la Legge 18 marzo 2008 n. 48 (http://www.camera.it/parlam/leggi/08048l.htm)

	1 gen –30 aprile 2020
Attacchi rilevati	282
Alert diramati	24.824
Indagini avviate	34
Persone arrestate	0
Persone denunciate	8
Richiesta di cooperazione internazionale in ambito Rete 24/7 High Tech Crime G8 (Convenzione Budapest)	17

Fig. 11.1-2 Attività per la protezione delle Infrastrutture Critiche nel 1° quadrimestre 2020 (Fonte: Polizia Postale e delle Comunicazioni)

11.2 Financial Cyber Crime

Gli attacchi digitali agli ambienti e alle transazioni finanziarie sono prevalentemente finalizzati ad ottenere un illecito guadagno economico, per cui ogni transazione economica rappresenta un potenziale target. La Polizia Postale è da sempre attiva per contrastare questo tipo di crimine informatico, che include anche attacchi indirizzati alle piattaforme di E-Commerce, ivi inclusi i relativi pagamenti on line.
La tabella in fig. 11.2-1 sintetizza i risultati dell'attività della Polizia Postale e delle Comunicazioni su questo fronte negli anni dal 2017 al 201 . Per quanto riguarda il blocco delle transazioni fraudolente, il 2019 ha visto una forte diminuzione rispetto all'anno precedente, registrando un -79,99% rispetto al 2018 e riallineandosi alle cifre riportate nel 2017.
Tuttavia, è significativo il totale delle somme recuperate, che non solo raddoppia in termini assoluti rispetto al 2018, ma rappresenta l'84% delle transazioni fraudolente bloccate in totale: infatti, dei 21, 3 milioni di € sono stati recuperati ben 18 milioni, dimostrando un netto miglioramento nell'efficienza dell'attività di recupero delle somme sottratte (nel 2018 le somme recuperate si attestavano a 9 milioni di € a fronte di ben 38,4 milioni di €). Inoltre, se si rapportano i dati registrati nel 2019 a quelli del 2017, si evince un forte aumento nel recupero delle somme sottratte a parità di transazioni bloccate (18 milioni di € contro 862,000 €).

Financial Cyber Crime	1 gen - 31 dic 2019	1 gen – 31 dic 2018	1 gen – 31 dic 2017
Transazioni Fraudolente Bloccate	**€ 21.333.990,00**	**€ 38.400.000,00**	**€ 20.839.576,00**
Somme Recuperate	**€ 18.000.000,00**	**€ 9.000.000,00**	**€ 862.000,00**

Fig. 11.2-1 Attività di contrasto al cyber crime finanziario dal 2017 al 2019 (Fonte: Polizia Postale e delle Comunicazioni)

La tabella in fig. 11.2-2 mostra gli analoghi dati di contrasto al cyber ciano rime finanziario nel 1° quadrimestre 2020, ed evidenzia come in questi soli primi quattro mesi si siano rilevate transazioni finanziarie dello stesso ordine di quelle nell'intero anno 2019. Questo forte incremento e sicuramente causato, a giudizio dell'autore, dall'aumento delle transazioni finanziarie on line e dell'uso dei servizi finanziari on line a causa della pandemia del Covid-19.

Financial Cyber Crime	1 gen –30 aprile 2020
Transazioni Fraudolente in €	20.200.000,00
Somme Recuperate	8.700.000,00

Fig. 11.2-2 Attività di contrasto al cyber crime finanziario nel 1° quadrimestre 2020 (Fonte: Polizia Postale e delle Comunicazioni)

11.3 Cyber Terrorismo

Siti web, social network ed Internet contribuiscono fortemente al proselitismo, alla preparazione e al coordinamento di attacchi terroristici. Attacchi solo cibernetici con intento terroristico possono colpire con attacchi specifici infrastrutture critiche e con attacchi di massa anche medio-piccole organizzazioni, magari di specifici settori merceologici, così da paralizzare per un certo lasso di tempo l'intera economia dei settori oggetto dell'attacco. Il confine tra cyber terrorismo e cyber warfare, la guerra digitale, può essere in taluni casi di difficile individuazione.
La tabella in fig. 11.3-1 fornisce pochi dati ma interessanti: sono stati monitorati dalla Polizia Postale nel 2019 migliaia di siti web, incrementando lievemente il numero di siti web sottoposti ad indagine rispetto al 2018, con un aumento di 377 siti. Il numero di spazi web monitorati 1° quadrimestre 2020 è congruente con quelli per gli interi anni 2018 e 2019, e sta per ora ad indicare una certa stabilità, almeno nel periodo considerato, delle attività di cyber terrorismo via Internet.
Non sono stati forniti dati sulla quantità di contenuti rimossi nel 2019 e nel 1° quadrimestre 2020.

Cyber Terrorismo	1 gen - 30 apr 2020	1 gen - 31 dic 2019	1 gen – 31 dic 2018
Spazi web monitorati	**11.962**	**36.377**	**36.000**
Contenuti rimossi			**250**

Fig. 11.3-1 Attività di contrasto al cyber terrorismo nel 2018, nel 2019 e nel 1°quadrimestre 2020 (Fonte: Polizia Postale e delle Comunicazioni)

ALLEGATI

Allegato A Aspetti metodologici dell'indagine OAD

L'indagine annuale OAD, come le precedenti con il marchio OAI, è indirizzata all'analisi totalmente anonima delle azioni deliberate e intenzionali rivolte contro i sistemi informatici in Italia, e non ai rischi cui i sistemi sono sottoposti per il loro cattivo funzionamento, per un maldestro uso da parte degli utenti e degli operatori, o per fenomeni accidentali esterni; tale analisi include anche, sempre in maniera anonima, la macro-rilevazione delle principali caratteristiche dei sistemi informatici dei rispondenti, e delle loro misure di sicurezza in atto o a piano nel breve tempo.
Devono essere considerati solo gli attacchi che sono stati effettivamente rilevati, e non è necessario che essi abbiano creato danni ed impatti negativi al sistema informatico attaccato, ovvero che l'attacco non ha avuto il successo sperato dall'attaccante.
L'attacco contro un sistema informatico è tale quando si intende violato, con una attività non autorizzata, almeno uno dei requisiti della sicurezza ICT, intesa come la "protezione dei requisiti di integrità, disponibilità e confidenzialità" delle informazioni trattate, ossia acquisite, comunicate, archiviate e processate.
L'indagine si basa sulle risposte, assolutamente e totalmente anonime, ad un questionario con risposte predefinite da selezionare, posto on line su un sito web accessibile via Internet.
Il questionario è totalmente anonimo: non viene richiesta alcuna informazione personale e/o identificativa del compilatore e della sua azienda/ente, non viene rilevato e tanto meno registrato il suo indirizzo IP, sulla banca dati delle risposte non viene nemmeno specificata la data di compilazione. Tutti i dati forniti vengono usati solo a fini di analisi complessiva e comunque il livello di dettaglio sulle caratteristiche tecniche dei sistemi ICT non consente in alcun modo di poter risalire alla azienda/ente rispondente. Per garantire un ulteriore livello di protezione ed evitare l'inoltro di più questionari compilati dalla stessa persona, il questionario, una volta completato e salvato, non può più essere modificato, e dallo stesso posto di lavoro non è più possibile compilare una seconda volta il questionario. L'autore, AIPSI, Malabo e Reportec garantiscono inoltre la totale riservatezza sulle risposte raccolte, utilizzate solo per la presente indagine, la produzione del presente Rapporto e l'eventuale presentazione dei risultati in eventi.
OAD è un'indagine via web, anonima, cui possono rispondere gli utenti interessati che partecipano su base volontaria tramite un browser ed una connessione ad Internet, senza alcun controllo preventivo da parte del sistema sul web. Il bacino di rispondenti all'indagine non è pertanto predefinito e bilanciato statisticamente. L'indagine OAD non ha pertanto valore strettamente statistico, ma dato il numero e l'eterogeneità delle aziende/enti dei rispondenti, sia per settore merceologico sia per dimensione, è comunque significativa e sufficiente per fornire attendibili indicazioni sul fenomeno degli attacchi digitali in Italia e sulle loro tendenze.
Per acquisire il maggior numero possibile di rispondenti, AIPSI, il suo Media Partner Reportec, Malabo Srl, ed i Patrocinatori coinvolti, invitano a compilare il questionario i potenziali rispondenti, tramite posta elettronica, social network e con specifiche pagine o messaggi sui loro siti web. Ulteriori inviti alla compilazione del questionario sono inoltre effettuati nell'ambito di eventi sull'ICT e sulla sicurezza digitale.
Quando termina il periodo previsto per la compilazione del questionario, Malabo elabora ed analizza i dati raccolti tramite fogli elettronici, e sulla base di tali elaborazioni viene redatto il Rapporto finale dell'anno, poi pubblicato su vari siti, in primis quello di OAD, per poter essere scaricato gratuitamente da tutti gli interessati.
L'elaborazione dai dati raccolti inizia con l'eliminazione di quelli palesemente errati o che non hanno senso.
Il calcolo statistico per la creazione dei grafici da pubblicare nel Rapporto finale differisce a seconda che le risposte possano essere multiple oppure no, e se la domanda, con relative risposte, è un dettaglio rispetto ad una precedente risposta
Per le risposte multiple ad una data domanda, il denominatore nel calcolo della percentuale è dato dal numero di rispondenti complessivo per quella domanda o insieme di domande, non per la sommatoria delle risposte avute: la somma finale delle percentuali di ogni singola risposta può essere pertanto superiore o inferiore al 100%

Per le risposte singole ad una data domanda, il denominatore nel calcolo della percentuale è dato dalla somma dei rispondenti: la somma finale delle percentuali di ogni singola risposta è e deve essere 100%.
In molti casi delle domande fanno riferimento ad una specifica risposta di una domanda precedente: ad esempio se si è rilevata una certa tipologia di attacco, quali sono le tecniche con le quali, probabilmente, è stata attuata. Per queste "sotto domande" il valore al denominatore per il calcolo della percentuale è dato dal numero dei rispondenti che hanno selezionato la specifica risposta cui fa poi riferimento la successiva sotto domanda. Nell'esempio di chi ha subito un certo di tipo di attacco, il calcolo delle percentuali sulle tecniche di attacco ha come riferimento il numero di chi ha rilevato quella tipologia (quindi come denominatore nel calcolo della percentuale).
La correlazione tra i dati forniti da domande diverse dal questionario è effettuata tramite pivot del foglio elettronico contenente tutte i record delle risposte, e da questi fogli pivot vengono rielaborati i dati estratti ed eventualmente creati i relativi grafici
Il questionario OAD 2020, rispetto alle precedenti edizioni, è stato modificato, come descritto nel seguente paragrafo §A1, per semplificare le domande e le relative risposte sulle misure di sicurezza digitale in esere o a piano in breve tempo, e poterle opportunamente "pesare" per fornire a chi termina il questionario di avere una macro valutazione qualitativa del livello di sicurezza digitale del sistema informatico oggetto delle risposte.
Il questionario OAD 2020 è stato implementato da Malabo Srl basandosi sul software open source Lime Survey nel dominio del sito OAD, https://www.oadweb.it/, realizzato e gestito da Malabo.
Il questionario è rimasto accessibile on line via web da fine maggio ai primi di dicembre 2020, con una lunga proroga sulla sua chiusura, dovuta alla cronica difficoltà di far rispondere, e completamente, al questionario stesso. Nel complesso il numero delle persone contattate è intorno alle quattromila, appartenenti ad un ampio insieme di aziende, enti e studi professionali di ogni dimensione e settore merceologico, inclusi enti pubblici centrali e locali.
Il questionario 2020 era composto da un totale di 116 domande, molte delle quali, le sotto-domande specifiche per ogni tipo di attacco, venivano automaticamente saltate se il rispondente indicava di non aver rilevato quel tipo di attacco. Questa logica implementativa del questionario online ha permesso di ridurre significativamente i tempi per completare l'intero questionario.

A.1 La tassonomia degli attacchi digitali per OAD 2020

L'edizione 2020 ha ripreso la logica della precedente edizione del 2020, migliorando alcune definizioni e mantenendo a 15 le tipologie di attacco considerate.
La classificazione degli attacchi distingue il che cosa si attacca dal come. Spesso infatti, anche nei più autorevoli rapporti internazionali, la distinzione tra che cosa viene attaccato e quali tecniche si usano per effettuare tale attacco non sempre è chiara, anche perché talvolta il nome usato per individuare l'attacco rappresenta anche la tecnica di attacco. Si è cercato di distinguere il più chiaramente possibile il target dell'attacco, ossia che cosa si attacca, dalle tecniche usate (sovente una loro combinazione), queste ultime raggruppate in 7 voci, approfondite nel paragrafo successivo §A.1.1.
Le 15 tipologie di attacco considerate (il che cosa attacco):

1. Distruzione fisica di dispositivi ICT o di loro parti
2. Furto di dispositivi ICT mobili
3. Furto di dispositivi ICT fissi o di loro parti
4. Furto informazioni da sistemi fissi (PC, server, storage system, etc.)
5. Furto informazioni da sistemi mobili (palmari, smartphone, tablet, etc.)
6. Attacchi all'identificazione, autenticazione e autorizzazioni degli utenti finali e privilegiati
7. Attacchi alle reti, locali e geografiche, fisse e wireless, e ai DNS
8. Uso non autorizzato sistemi ICT nel loro complesso (dai dispositivi d'utente ai server-storage e ai servizi in cloud)
9. Modifiche non autorizzate ai programmi applicativi e alle loro configurazioni
10. Modifiche non autorizzate alle informazioni trattate dai sistemi ICT
11. Saturazione risorse digitali (DoS, DDoS)

12. Attacchi ai propri sistemi in cloud o in housing/hosting presso fornitori terzi
13. Attacchi a dispositivi IoT (Internet of Things) in uso
14. Attacchi ai propri sistemi di automazione industriale e di robotica (OT, Operational Technology)
15. Attacchi a sistemi e/o servizi usati e basati su blockchain

Nel testo del presente Rapporto 2020 OAD la tassonomia del che cosa viene attaccato è prevalentemente indicata come "tipologia attacchi"; le principali modalità di attacco, ossia il come, come "tecniche di attacco".
L'indagine 220 di OAD fa riferimento agli attacchi intenzionali rilevati nel 2019 e nel primo quadrimestre 2020. Per ogni tipo di attacco (il che cosa) è stata creata una sezione specifica, con gruppi di sotto domande che includono, se l'attacco è stato rilevato (in caso contrario questa parte viene automaticamente saltata):

- la frequenza di attacchi: meno di o uguale a 10, più di 10
- le "macro" tecniche di attacco, se individuate o ipotizzate, per l'attacco di quel tipo più grave secondo chi risponde, con risposte multiple
- I principali impatti subiti dall'attacco più grave, con risposte multiple
- le possibili motivazioni dell'attacco più grave secondo la stima del compilatore, con risposte multiple
- il tempo massimo richiesto per il ripristino ex ante dei sistemi ICT, nel caso del più grave attacco subito nell'anno.

A.1.1 Le classi di tecniche di attacco considerate (come si attacca)

Facendo riferimento principalmente alle tassonomie sviluppate da CERT[27] e da Sandia[28], si sono categorizzate le tecniche di attacco sotto riportate per poter descrivere e richiedere nel Questionario 2020 OAD in modo sistematico quali sono (o quali si pensa possano essere state) le tecniche usate dall'attaccante per portare l'attacco rilevato.

E' opportuno sottolineare e ricordare che la fantasia degli attaccanti rende l'argomento piuttosto fluido e soggetto a rapida evoluzione e, a causa di ciò, variabile e dinamico anche nella nomenclatura. Il presente rapporto non può illustrare e spiegare l'ampio argomento interdisciplinare della sicurezza digitale, e per chi volesse approfondire tale argomento si rimanda alle numerose pubblicazioni disponibili.

A.1.1.1 Attacco fisico

Nell'ambito degli attacchi intenzionali che OAD tratta, quelli di tipo fisico ai sistemi ICT richiedono la presenza fisica di uno o più attaccanti che:

- Rompono e/o sconnettono i sistemi ICT ed i servizi a loro supporto (alimentazione elettrica, condizionamento aria, allarmi antintrusione, allarmi antincendio, etc.): l'attacco può essere distruttivo se uno o più dispositivi, o loro parti, vengo fracassate. Può essere non distruttivo se non viene rotto nulla ma vengono sconnessi e/o riconnessi in maniera sbagliata i vari dispositivi: ad esempio sconnessione e/o scambio delle porte degli switch di rete, sconnessioni o taglio dei cavi di connessione, etc.

- Rubano dispostivi ICT o loro parti, dagli smartphone ai laptop, dagli hard disk alle chiavette

[27] Per CERT/CC si veda https://www.sei.cmu.edu/about/divisions/cert/index.cfm, per il sito italiano: https://www.certnazionale.it/
[28] https://www.sandia.gov/

USB, sia per il loro valore sul mercato sia per i dati contenuti.

L'attacco fisico è considerato sia come tipologia d'attacco, in quanto vengono attaccati indispostivi ICT o loro parti (il che cosa viene attaccato), sia come tecnica d'attacco, perché scassare o rubare i dispositivi ICT è una tecnica per manomettere, anche gravemente, il funzionamento dell'intero sistema informatico o di sue parti, oltre che sottrarre e/o distruggere le informazioni contenute in tali dispositivi.

A.1.1.2 Raccolta/diffusione malevola e non autorizzata di informazioni

Per attaccare un sistema ICT sono utili, in taluni casi indispensabili, informazioni sia dirette sulla sua posizione, sul suo funzionamento, sulla sua configurazione, sulle misure di sicurezza di cui dispone, sugli account degli utenti sia indirette, come i nomi dei suoi utenti e dei suoi gestori, indirizzi fisici e digitali, numeri di telefono, contatti anche via rete con dipendenti potenzialmente infedeli o ingenui ecc. Innumerevoli le tecniche per carpire, direttamente o indirettamente, le informazioni che servono per attuare poi un attacco digitale. Alcune sono "manuali" e consentono di interagire con le persone che trattano con il sistema informatico e con il loro ambiente di lavoro: ad esempio recuperare informazioni dai cestini dei rifiuti o richiedere in maniera subdola informazioni sia de visu sia per telefono (anche questo è social engineering). Altre tecniche per raccogliere informazioni sono informatiche ed includono social engineering, phishing, pharming, hoax, scam, data entry in server trappola, scannerizzazioni e ricerche in Internet, ecc.
Si sta inoltre assistendo in maniera crescente alla diffusione, soprattutto via Internet, di informazioni false (le così dette fake news) o addirittura malevoli atte a far compiere all'ignaro utente operazioni di ausilio all'attuazione dell'attacco e/o che costituiscono un danno economico a lui stesso. I canali principali per la diffusione malevola di informazioni sono prevalentemente i social network, seguite da spamming e spear phishing oltre che da siti malevoli il più delle volte linkati ai precedenti canali.

A.1.1.3 Script e programmi maligni

Gli script sono semplici programmi software scritti in un linguaggio interpretato facile da utilizzare, senza interfaccia grafica, che svolgono funzioni molto specifiche ed accessorie, ed in grado di interfacciarsi con altri programmi più complessi per svolgere operazioni più sofisticate. Gli script sono sovente usati per personalizzare la configurazione automatica del sistema, per rendere più dinamica una pagina web, per fornire comandi al sistema operativo (tipico dei così detti "script shell") ed al data base, pe personalizzare e rendere "smart" documenti Microsoft Office o simili (es. Libre Office). Esempi di linguaggi di scripting includono Bash, AppleScript, JavaScript, Perl, Python, PHP, VBScript.
Programmi in script sono usati per attacchi digitali, e quelli più semplici richiedono un intervento umano per farli giungere sul sistema bersaglio (ad esempio l'apertura di un allegato in posta elettronica o lo sfruttamento di un buffer overflow presente in una applicazione); quelli più sofisticati sono in grado di attaccare senza bisogno di interventi della vittima.
Con linguaggi più complessi e sofisticati, come C, C++, C#, Java, si possono realizzare programmi d'attacco più complessi e sofisticati, chiamati genericamente malware o codici maligni. Essi sono caratterizzati da un qualche meccanismo con il quale riescono a raggiungere il bersaglio, ed in base sono classificati con specifici nomi, e da un "payload", una parte che esegue l'azione di attacco.
La classificazione per funzioni e capacità dei malware include troian horse, ransonware, spyware, adware (si veda il Glossario in Allegato B per una sintetica spiegazione di questi termini). Occorre sottolineare che la sofisticazione oggi raggiunta da molti codici maligni rende difficile una esatta classificazione, dato che essi sono in grado di svolgere diverse funzioni anche alternative tra loro, il così detto polimorfismo.
Nella categoria "script e programmi maligni" è stata inclusa anche quella così detta di "command", ossia di comandi al sistema operativo o al DBMS che quando vengono eseguiti hanno conseguenze dannose per il sistema. Si tratta tipicamente di comandi malformati che controlli inadeguati

consentono di mandare in esecuzione. La tipica conseguenza è l'esecuzione di un comando che altrimenti non sarebbe stato autorizzato. Il comando può modificare i diritti di accesso al sistema, consentire di interrogare, modificare, distruggere informazioni. L'attaccante in questi casi ha solo attivato una sessione Telnet con il bersaglio o, nel caso di "SQL injection" scritto solo pochi caratteri in un form web. Un esempio di comando al DB è il XSS (Cross Site Scripting).

A.1.1.4 Agenti autonomi

Sono programmi maligni capaci di replicarsi e diffondersi in rete su altri sistemi autonomamente, come i virus ed i worm.

A.1.1.5 Toolkit

Come dice il nome, sono una "cassetta degli attrezzi" di strumenti informatici che aiutano a compiere l'attacco col trovare le informazioni necessarie e le vulnerabilità presenti nel sistema target, e aiutando a sviluppare codici maligni. Alcuni toolkit sono specifici per determinati linguaggi, altri più generali.
Sono da evidenziare due categorie di toolkit: i rootkit ed i meta exploit tool. I primi derivano il nome dal termine "root", radice, che nei sistemi Unix è il livello a cui si ottengono i massimi livelli amministrativi: i rootkit sono quindi strumenti per acquisire i diritti di "root". Con il tempo e nei sistemi Windows è prevalso questo secondo significato: uno strumento che nasconde la presenza di malware. Tipicamente il rootkit guadagna i diritti di amministratore usando vulnerabilità note o social engineering, e poi modifica il sistema operativo in modo da nascondere la sua presenza e quella di altro malware che ad esempio può installare backdoor, keylogger o strumenti che sconfiggono i meccanismi di controllo delle licenze o di protezione delle copie.
Gli exploit sono attacchi ad una risorsa ICT basandosi sulle sue vulnerabilità ed il termine "meta exploit" indica strumenti software che facilitano la loro realizzazione e la loro verifica, comprendendo anche basi di conoscenza contenenti centinaia di exploit.
Questi strumenti non solo sono usati per effettuare attacchi, ma anche per eseguire "penetration test" in sistemi applicativi, middleware e prodotti informatici.

A.1.1.6 Botnet e simili

Strumenti distribuiti controllati centralmente (da un Command & Control, C&C, il più delle volte anonimo e che continua a spostarsi da un server all'altro per non farsi identificare). Gli agenti distribuiti sono codici maligni, talvolta virus, e sono chiamati bot, droni, zombi. Dopo essere stati installati all'insaputa dell'utente e/o del gestore del sistema ICT involontariamente ospite, restano dormienti fino a quando il C&C ordina loro di attivarsi.

A.1.1.7 Utilizzo di due o più tecniche di attacco (es. APT)

I moderni e più temibili attacchi digitali utilizzano più di una tecnica di attacco, anche contemporaneamente: ad esempio sono in grado di analizzare le vulnerabilità di un sistema ICT, e di attaccarlo con la tecnica più idonea, e in parallelo attivare virus, inondare di agent gli altri sistemi, e mantenere il controllo di tutto questo trame un C&C di cui al precedente paragrafo.
Attacchi di questo tipo possono richiedere tempi lunghi, ed i vari agent e codici maligni rimanere per lungo tempo annidati nei sistemi ICT target. Questo tipo di attacco multiplo viene sovente indicato con l'acronimo APT, Advanced Persistent Threat. Come dice il nome, questa tecnica, o insieme di tecniche, realizza un attacco persistente, ovvero che può durare nel tempo, soprattutto nella fase preparatoria e di individuazione delle vulnerabilità da sfruttare (persistent), e che utilizza innovazioni tecnologiche (advanced). Attacchi ATP sono realizzati ed usati prevalentemente da organizzazioni con grandi capacità e risorse, in taluni casi anche da stati.

A2 La macro valutazione qualitativa del livello di sicurezza digitale del sistema informatico oggetto delle risposte al questionario

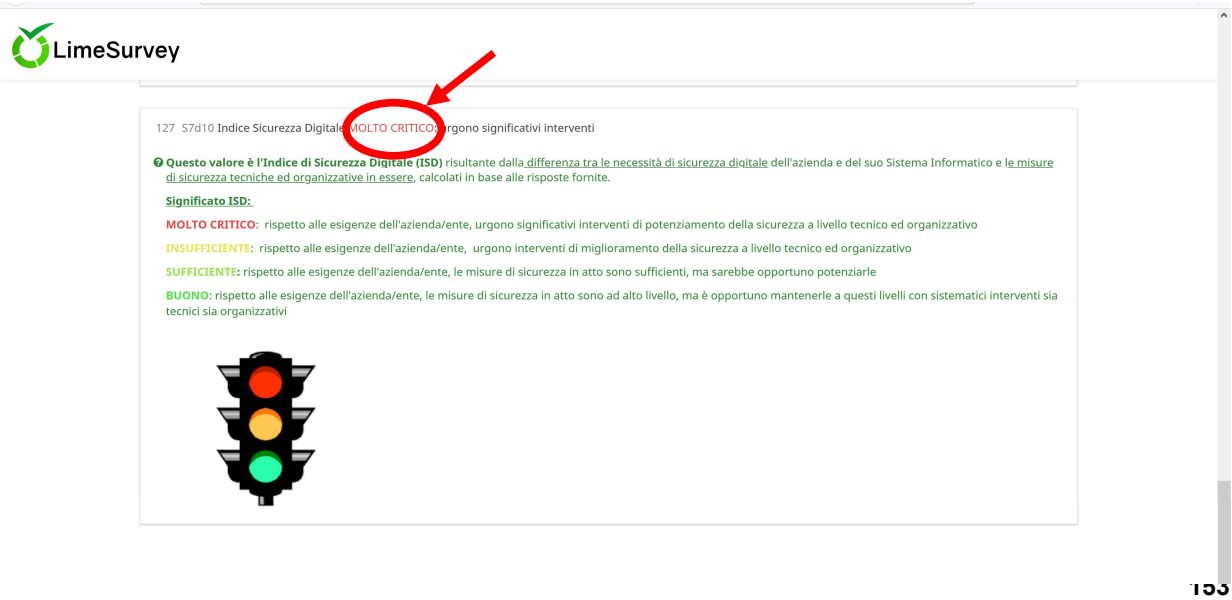
La più importante innovazione introdotta nel Questionario 2020 OAD, con l'obiettivo di meglio e più fortemente motivare un potenziale rispondente a compilare il questionario, è stata il fornire al rispondente, in tempo reale al completamento della compilazione, una macro valutazione qualitativa del livello di sicurezza digitale del sistema informatico oggetto delle sue risposte, rispetto alle esigenze di sicurezza dell'azienda/ente.
La macro valutazione è stata realizzata assegnando degli opportuni "pesi" numerici a tutte le opzioni di risposta previste nel questionario rispetto alle domande relative:

- alle generali caratteristiche del sistema informatico (**A**)
- all'importanza e alla necessità del sistema informatico, e della sua sicurezza, per le attività ed il business dell'Azienda/Ente del rispondente (**B**)
- alle misure di sicurezza digitale, tecniche ed organizzative, in essere nel sistema informatico e selezionate dal rispondente scegliendo le varie opzioni di risposta predefinite presenti in questo settore (**S**).

Nel procedere nella compilazione del questionario, il sistema LImeSurvey, opportunamente configurato e predisposto, somma i pesi delle risposte relative alle domande inerenti A, B ed S.
Calcola poi un Indice di Sicurezza Digitale numerico (IDS) dato dalla formula seguente:

$$\textbf{Indice Sicurezza Digitale} = (\sum Ai + \sum Bi) - \sum Si$$

Il numero IDS calcolato viene posizionato in un range di valori numerici che caratterizzano le seguenti valutazioni qualitative del livello di sicurezza digitale: buono, sufficiente, insufficiente, molto critico. Ed è una di queste la valutazione qualitativa fornita al compilatore, in funzione delle varie risposte fornite.
La fig. 2 sottostante mostra un esempio tipo della risposta che viene fornita alla/al rispondente al termine della compilazione. Nel cerchio in rosso evidenziato da una freccia nella figura appare la valutazione finale. Nelle righe sottostanti viene brevemente spiegato il significato delle diverse possibili valutazioni.



Allegato B Glossario OAD 2020

Glossario dei principali termini ed acronimi relativi prevalentemente alla sicurezza e agli attacchi digitali

- Account: insieme di informazioni di identificazione ed autenticazione di un utente di un sistema informativo. Tipicamente è costituito da un identificativo d'utente e da una password, ma può estendersi a certificati digitali, riconoscimenti biometrici e richiedere l'uso di token quali smart card, chiavette USB, ecc.
- ACL, Access Control List: elenco di regole per il controllo degli accessi a risorse ICT.
- Active Directory: sistema di directory della Microsoft, integrato nei sistemi operativi Windows dal 2000 in avanti. Utilizza SSO, LDAP, Kerberos, DNS, DHCP, ecc.
- Active X Control: file che contengono controlli e funzioni in Active X che “estendono” (eXtension) ed espletano specifiche funzionalità; facilitano lo sviluppo di software di un modulo software dell’ambiente Windows in maniera distribuita su Internet.
- Address spoofing: generazione di traffico (pacchetti IP) contenenti l’indicazione di un falso mittente (indirizzo sorgente IP).
- Adware: codice maligno che si installa automaticamente nel computer, come un virus o lo spyware, ma in genere si limita a visualizzare una serie di pubblicità mentre si è connessi a Internet. L'adware può rallentare sensibilmente il computer e nonostante costringa l'utente a chiudere tutte le finestre pop-up visualizzate, non rappresenta una vera minaccia per i dati, a meno che non nasconda un codice maligno.
- AET, Advanced Elusion Techniques: tecniche avanzate di elusione degli strumenti di sicurezza in uso.
- App: neologismo ed abbreviazione di "application" (applicazione) per indicare, anche in italiano, le applicazioni operanti localmente sui sistemi mobili, tipicamente su smartphone.
- ATP, Advanced Persistent Threat: attacco persistente e sofisticato, basato su diverse tecniche operanti contemporaneamente e capaci di scoprire e sfruttare diverse vulnerabilità. Usato da organizzazioni con grandi capacità e risorse.
- Alert: viene spesso usato il termine inglese di “allarme” per indicare segnalazione di eventi e problemi inerenti la sicurezza informatica; la segnalazione può essere generata sia da dispositivi di monitoraggio e controllo sia dalle persone addette.
- Attacco mirato, indicato sovente con il termine inglese targeted attack: attacco portato ad uno specifico sistema obiettivo, o a un gruppo similare di obiettivi, con tecniche sofisticate e specifiche per il sistema target. Viene incluso sovente tra gli ATP.
- Attacco massivo, o di massa: attacco rivolto ad una grande massa di obiettivi simili, anche dell’ordine di milioni: può essere semplice e non sofisticato, ma nella massa qualche attacco va quasi sempre a buon fine. Tipici esempi i phishing ed i ransomware.
- Backdoor: interfaccia e/o meccanismo nascosto che permette di accedere ad un programma superando le normali procedure e barriere d’accesso.
- Blade server: "lama", ossia scheda omnicomprensiva di elaborazione di un sistema ad alta affidabilità costituito da più lame interconnesse ed interoperanti.
- Blended Threats: attacco portato con l’uso contemporaneo di più strumenti, tipo virus, worm e trojan horse.
- Bluetooth: protocollo, standard de facto, di collegamento senza fili a brevi distanze. Opera in radio frequenza in campi attorno ai 2,45 GHz.
- Bots: sono programmi, chiamati anche Drones o Zombies, usati originariamente per automatizzare talune funzioni nei programmi ICR, ma che ora sono usati per attacchi distribuiti.
- Botnet: per la sicurezza ICT questo termine indica un insieme di computer, chiamati “zombi”, che a loro insaputa hanno agenti (programmi) malevoli dai quali partono attacchi distribuiti, tipicamente DDOS.

- Buffer overflow: consiste nel sovra-scrivere in un buffer o in uno stack del programma dati o istruzioni con i quali il programma stesso può comportarsi in maniera diversa dal previsto, fornire dati errati, bloccare il sistema operativo, ecc.
- BYOD, Bring Your Own Device: policy aziendale che consente l'utilizzo di dispositivi mobili di proprietà dell'utente anche nell'ambito dei sistemi dell'azienda/ente. Il fenomeno è chiamato anche consumerizzazione.
- Captcha, Completely Automated PublicTuring test to tell Computers and Humans Apart: l'acronimo indica una famiglia di test costituita da una o più domande e risposte per assicurarsi che l'utente sia un essere umano e non un programma software.
- CASB, Cloud Access Security Brokers.
- C&C, Command&Control: Sistema centrale di commando e controllo di una botnet.
- CED, Centro Elaborazione Dati: centro di calcolo ove risiedono tutti i sistemi centralizzati di elaborazione, archiviazione e trasmissione dei dati.
- CERT, Computer Emergency Response Team.
- Chatbot: programma software realizzato per interagire con gli umani via voce e/o scambi di testi. Hanno numerose applicazioni, tipicamente l'assistente virtuale digitale, ma possono essere programmati per agire in maniera malevola e costituire un componente di un attacco digitale.
- Churn rate: tasso di abbandono a favore della concorrenza, tipicamente dopo un attacco.
- CIO, Chief Information Officer: il responsabile dell'intero sistema informatico.
- CISA, ISACA Certified Information Systems Auditor di ISACA.
- CISO, Chief Information Security Officer: il responsabile della sicurezza digitale dell'intero sistema informatico.
- CISSP, Certified Information Systems Security Professional.
- Cyberwarfare: guerra cibernetica.
- Cluster: insieme di computer e/o di schede (es lame di un sistema blade) cooperanti per aumentare l'affidabilità complessiva del sistema; il termine è anche usato per identificare un insieme contiguo di settori in un disco rigido.
- Cnaipic, Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche.
- Consumerizzazione: vedi BYOD.
- Container: istanza di un ambito virtualizzato di applicazioni, che isola le risorse hardware e software in uso da ognuna di esse, pur sempre all'interno di un solo e unico sistema operativo.
- CSIRT, Computer Security Incident Response Team: in Italia sostituisce CERT-PA e Cert Nazionale In ottemperanza alla Direttiva NIS (Decreto legislativo 18 maggio 2018 n. 65).
- Crowdturfing*:* termine derivato dalla combinazione di "crowdsourcing" e "astroturfing", indica un attacco basato su recensioni scorrette e false per danneggiare la reputazione di un prodotto o di una azienda/ente.
- CSO, Chief Security Officer; responsabile della sicurezza dell'intera azienda/ente, prevalentemente per la sicurezza fisica di edifici e del personale. In alcune organizzazioni il CISO riporta a questa figura.
- CSSLP, Certified Secure Software Lifecycle Professional.
- CTO, Chief Technology Officer: è il direttore tecnico di più alto livello, tipicamente per aziende che producono prodotti e servizi. In talune organizzazioni il CIO riporta a questa figura.
- DAC, Discretionary Access Control.
- Darknet: sistema usato in Internet per monitorare la rete e possibili attaccanti, con funzionalità simili a quelle di un honeypot.
- Dark web: siti web che si raggiungono via Internet ma attraverso specifici software, configurazioni e accessi autorizzativi, e non sono indicizzati, e quindi ritrovabili, dai motori di ricerca. Molti dark web contengono informazioni criminali, dalla pedopornografia a strumenti informatici di attacco e da account e identità digitali rubate.
- Data Breach: letteralmente "violazione dei dati", spesso è usato come sinonimo di furto di identità digitale. Tecnicamente è usato per indicare l'accesso a banche dati o a file system contenenti identità digitali o informazioni a quest'ultime correlate.

- Data Center, Centro Dati: si veda CED.
- DB, Data Base: banca dati.
- DBMS, Data Base Management System.
- DCS, Distributed Control System.
- Deadlock: un caso particolare di “race condition”, consiste nella condizione in cui due o più processi non sono più in grado di proseguire perché ciascuno aspetta il risultato di una operazione che dovrebbe essere eseguita dall'altro.
- Deamon: software di base operante in back-ground in un ambiente multi-tasking.
- Defacing o defacement: in inglese significa deturpare, e nel gergo della sicurezza informatica indica un attacco ad un sito web per modificarlo o distruggerlo; spesso con tale attacco viene modificata solo la home-page a scopo dimostrativo.
- Denial of service (DOS) e Distributed Denial of service (DDOS): attacco per saturare sistemi e servizi ed impedire la loro disponibilità.
- Dialer: programma software che connette il sistema ad Internet, ad una rete o ad un computer remoto tramite linea telefonica (PSTN o ISDN); può essere utilizzato per attacchi e frodi.
- DKIM, Domain Keys Identified Mail: in ambito DMARC, chiavi di crittografia asimmetrica per l’autenticazione di ogni messaggio di posta elettronica. Il messaggio viene firmato dal server e il destinatario controlla i messaggi con la chiave pubblica DKIM, che viene fornita nel DNS del dominio.
- DMARC, Domain-based Message Authentication, Reporting, and Conformance: sistema standard di autenticazione dei messaggi di posta elettronica, che aiuta gli amministratori della posta a impedire che hacker e altri malintenzionati eseguano lo spoofing dell'organizzazione e del dominio.
- Docker: software per la creazione di container.
- DLP, Data Loss Prevention: sistemi e tecniche per prevenire la perdita e/o il furto di dati nel corso del loro trattamento, archiviazione inclusa.
- DMZ, DeMilitarized Zone: isola del sistema informatico costituita da sottoreti locali, fisiche o virtuali, ove sono allocati i server esposti ad Internet.
- DNS, Domain Name System: sistema gerarchico di nomi (naming) di host su Internet che vengono associati al loro indirizzo IP di identificazione nella rete.
- Drive-by Downloads: attacchi causati dallo scaricare (anche inconsapevolmente) codici maligni o programmi malevoli.
- Drones, Droni: si veda bots.
- ECDL, European Computer Driving Licence: ideata, realizzata e gestita da AICA, ora al 20° anno di vita, è il patentino europeo di conoscenza di vari aspetti dell’ICT soprattutto nell’ottica dell’utente finale.
- eCF, European Competence Framework: quadro europeo standardizzato sulle competenze digitali e sui ruoli ICT che espletano professionalmente tali competenze.
- EDGE, Enhanced Data rates for GSM Evolution.
- ENISA, European Union Agency for Cybersecurity.
- ETACS, Extended TACS.
- FTP, File Transfer Protocol: protocollo per il trasferimento di file.
- FTPs, FTP sicuro con la criptazione dei dati durante la trasmissione.
- Exploit: attacco ad una risorsa ICT utilizzando sue vulnerabilità.
- Extranet: Intranet accessibile anche da utenti esterni all’azienda/ente.
- Ethical hacking: attività di provare attacchi ai fini di scoprire bachi e vulnerabilità dei programmi, e porvi rimedio con opportune patch/fix.
- Eucip, European Certification of Informatics Professionals: è ora sostituito da eCF.
- Fix: correzione di un programma software, usato spesso come sinonimo di patch.
- Flash threats: tipi di virus in grado di diffondersi molto velocemente.
- Form: in informatica indica il campo generato da una applicazione visibile su una schermata, nel quale l’utente deve inserire dei caratteri per interagire con l’applicazione stessa; è l’elemento base per l’interfaccia tra utente e applicazione per l’inserimento dei dati (data entry).

- FTPS, File Transfer Protocol Secure: per il trasferimento di file crittati.
- FW, FireWall generico, normalmente di rete.
- FWA, FireWall Applicativo.
- GPRS, General Packet Radio Service.
- GSM, Global System for Mobile communications.
- Hactivism: termine derivato dalla combinazione di hack e di activism, indica un uso sovversivo dell'ICT per promuovere un'ideologia politica/religiosa e la sua agenda o un cambiamento sociale.
- Hijacking: tipico attacco in rete "dell'uomo in mezzo" tra due interlocutori, che si maschera per uno dei due e prende il controllo della comunicazione. In ambito web, questo termine è usato per indicare un attacco ove: le richieste di pagine a un web vengo dirottate su un web falso (via DNS), sono intercettati validi account di e-mail e poi attaccati questi ultimi (flooding).
- Hoax: in italiana bufala o burla, indica la segnalazione di falsi virus; rientra tra le tecniche di social engineering.
- Honeynet: è una rete di honeypot.
- Honeypot: sistema "trappola" su Internet per farvi accedere con opportune esche possibili attaccanti e poterli individuare.
- Hosting: servizio che "ospita" risorse logiche ICT del Cliente su hardware del fornitore del servizio.
- Housing: concessione in locazione di uno spazio fisico, normalmente in un Data Center già attrezzato, ove riporre, funzionanti, le risorse ICT di proprietà del Cliente.
- HSDPA, High Speed Downlink Packet Access.
- HTTPS, HyperText Transfer Protocol Secure: protocollo sicuro per le transazioni crittate tra browser e sito web, e viceversa.
- Hypervisor: elemento di base di un sistema virtualizzato, che crea e gestisce sistemi virtuali.
- IAA, Identificazione - Autenticazione – Autorizzazione: per il controllo degli accessi ai sistemi ICT.
- IaaS, Infrastructure as a Service.
- IAM, Identity & Access Management.
- Information Leakage: diffusione-dispersione non autorizzata di informazioni.
- Intranet: rete e server operanti in http/https ed accessibili solo ad utenti interni ad una data azienda/ente.
- IoT, Internet of Things (Internet delle Cose): componenti/sistemi intelligenti ed interoperanti su Internet.
- IIoT, Industrial IoT.
- ISACA, Information Systems Audit and Control Association.
- Key Logger: sistema di tracciamento dei tasti premuti sulla tastiera per poter carpire informazioni quali codici, chiavi, password.
- Kerberos: metodo sicuro per autenticare la richiesta di un servizio, basato su crittografia simmetrica. Utilizzato da Active Directory.
- Kubernets: sistemi per la gestione di carichi di lavoro e servizi containerizzati, in grado di facilitare sia la configurazione dichiarativa che l'automazione.
- LDAP, Lightweight Directory Access Protocol: protocollo standard per la gestione e l'interrogazione dei servizi di directory che organizzano e regolano in maniera gerarchica le risorse ICT ed il loro utilizzo da parte degli utenti. Il termine LDAP indica anche il sistema di directory nel suo complesso.
- Log bashing : operazioni tramite le quali un attaccante cancella le tracce del proprio passaggio e attività sul sistema attaccato. Vengono ricercate e distrutte le voci di registri, log, contrassegni e file temporanei, ecc. Possono operare sia a livello di sistema operativo (es. deamon sui server Unix/Linux), sui registri dei browser, ecc. Esistono innumerevoli programmi per gestire le registrazioni, ma sono tecnicamente complessi.
- LTE, Long Term Evolution.
- MAC, Mandatory Access Control.

- MAC: codice indirizzo assegnato in modo univoco ad ogni scheda di rete.
- MAC flooding: tecnica di attacco ad uno switch per bloccarne il corretto funzionamento.
- MAC Media Access Control: sub strato del livello datalink del modello ISO/OSI.
- Malicious insider : attaccante interno all'organizzazione cui viene portato l'attacco.
- Malvertising, contrazione di "malicious advertisements": pubblicità malevola, con pagine web che nascondono un codice maligno o altre tecniche di attacco, come il dirottamento su siti web mascherati e fraudolenti.
- Malware: termine generico che indica qualsiasi tipo di programma di attacco.
- Microservizi: approccio allo sviluppo ed all'organizzazione dell'architettura dei software, evoluzione dell'architettura SOA e dell'object orientation. I microservizi sono moduli software autonomi, specializzati, indipendenti di piccole dimensioni che comunicano tra loro tramite API ben definite. Le architetture dei microservizi permettono di scalare e sviluppare le applicazioni in modo rapido e semplice.
- Mirroring: termine inglese per indicare la replica e la sincronizzazione di dati su due o più dischi.
- MSSP, Managed Security Service Provider: fornitore di servizi per la sicurezza digitale
- NAC, Network Access Control: termine usato con più significati, che complessivamente indica un approccio architetturale ed un insieme di soluzioni per unificare e potenziare le misure di sicurezza a livello del punto di accesso dell'utente al sistema informativo.
- NIS, Network and Information Security: normativa europea per armonizzare la sicurezza digitale dei vari paesi.
- OASIS: Consorzio di aziende ICT no profit che fornisce norme implementative per alcuni standard, tra i quali la SOA e la sua sicurezza (SALM SPML, XACML).
- OSA, Open Security Architecture.
- OT, Operational Technology.
- OTP, One Time Password: dispositivo che genera password da usarsi una sola volta per sessione/transazione.
- Outsourcer: fornitore dei servizi di terziarizzazione.
- PaaS, Platform as a Service.
- PAC, Pubblica Amministrazione Centrale.
- PAL, Pubblica Amministrazione Locale.
- Payload: è il "carico utile" di informazioni all'interno di un programma, di un protocollo, ecc.; tipicamente è il codice maligno da attivare sul sistema attaccato dopo esservi penetrati.
- PEC, Posta Elettronica Certificata.
- Pharming: attacco per carpire informazioni riservate di un utente basato sulla manipolazione dei server DNS o dei registri del sistema operativo del PC dell'utente.
- Phishing: attacco di social engineering per carpire informazioni riservate di un utente, basato sull'invio di un falso messaggio in posta elettronica che fa riferimento ad un ente primario, che richiede di collegarsi ad un server (trappola) per controllo ed aggiornamento dei dati.
- Ping of death: invio di pacchetti di ping di grandi dimensioni (ICMP echo request), che blocca la pila di protocolli TCP/IP: è un tipo di attacco DoS/DDoS.
- PLC, Programmable Logic Controller.
- PMI, Piccole e Medie Imprese: sotto i 250 dipendenti.
- Port scanner: programma che esplora una fascia di indirizzi IP sulla rete per verificare quali porte, a livello superiore, sono accessibili e quali vulnerabilità eventualmente presentano. È uno strumento di controllo della sicurezza, ma è anche uno strumento propedeutico ad un attacco.
- PUP, Potentially Unwanted Programs: programma che l'utente consente di installare sui suoi sistemi ma che, a sua insaputa, contengono codici maligni o modificano il livello di sicurezza del sistema. Tipici esempi: adware, dialer, sniffer, port scanner.
- QR, Quick Response: è un codice a barre bidimensionale, ossia a matrice, che è impiegato per memorizzare informazioni generalmente destinate a essere lette tramite uno smartphone.

- Race condition: indica le situazioni derivanti da condivisione di una risorsa comune, ad esempio un file o un dato, ed in cui il risultato viene a dipendere dall'ordine in cui vengono effettuate le operazioni.
- Ransomware: codice maligno che restringe e/o blocca i diritti d'accesso e tramite il quale viene chiesto un riscatto (ransom) per far funzionare correttamente il sistema.
- RBAC, Request Based Access Control.
- RBAC, Role Based Access Control.
- RFID, Radio-Frequency Identification: tecnologia per l'identificazione e/o memorizzazione automatica di informazioni inerenti oggetti, animali o persone, basata su un tag intelligente identificativo dell'entità oggetto dell'identificazione ed un dispositivo in grado di riconoscere l'entità se in sua prossimità, scambiando in radio frequenza delle informazioni.
- Ricatto: significa che l'attacco perpetrato viene poi usato per ricattare l'attaccato perché paghi per non subirne di altri, magari più perniciosi. Il malware ransomware ha come tipica motivazione il ricatto, che è un tipo della più generale frode informatica.
- Ritorsione: significa che l'attacco è stato portato come "vendetta" verso torti subiti, o come tali ritenuti: tipico il caso di un dipendente cui è stata negata una sua richiesta, o di ex dipendente licenziato. L'attaccante intende "colpire" con un attacco digitale l'Azienda/Ente che ritiene "colpevole" dei (presunti) torti subiti.
- Rogueware: falso antivirus. E' a sua volta un codice maligno che infetta il sistema.
- Rootkit: Programma software di attacco che consente di prendere il completo controllo di un sistema, alla radice come indica il termine.
- SaaS, Software as a Service.
- SALM, Security Assertion Markup Language.
- SASE, Secure Access Service Edge.
- SCADA, Supervisory Control And Data Acquisition: sistema informatico distribuito per il controllo ed il monitoraggio di processi, ed in parte per la loro automazione.
- Scam: tentativo di truffa via posta elettronica. A fronte di un millantato forte guadagno o forte vincita ad una lotteria, occorre versare un anticipo o pagare una tassa.
- Scammer: chi effettua uno scam.
- SCAP, Security Content Automation Protocol.
- SCC, Security Command Centre.
- Scareware: software d'attacco che finge di prevenire falsi allarmi, e diffonde notizie su falsi malware o attacchi.
- Scraping: letteralmente "raschiando", è il termine in informatica usato per l'attività di ricerca e raccolta, in maniera automatica, di determinate informazioni dai sistemi connessi in Internet.
- SD-WAN, Software Defined WAN (Wide Area Network).
- SGSI, Sistema Gestione Sicurezza Informatica.
- SIEM, Security Information and Event Management: sistemi e servizi per la gestione in tempo reale di informazioni ed allarmi generati dalle risorse ICT di un sistema informativo, inclusi i log.
- Sinkhole: metodo per reindirizzare specifico traffico Internet per motive di sicurezza, tipicamente per analizzarlo, per individuare attività anomale o per sventare attacchi. Può essere realizzato tramite darknet o honeynet.
- Sistema Informatico: insieme dei sistemi e dei servizi ICT, dalle reti ai server ed agli applicativi, anche terziarizzati e in cloud, organizzato in una specifica architettura e che una azienda/ente usa a supporto delle proprie attività. Il sistema informatico può includere anche i dispositivi d'utente fissi e mobili (PC, smartphone, tablet, etc.), i sistemi di automazione e controllo industriale (DCS, PLC, robot, ecc.) ed i dispositivi IoT.
- SOA, Service Oriented Architecture.
- SOC, Security Operation Centre.
- Social Engineering (ingegneria sociale): con questo termine vengono considerate tutte le modalità di carpire informazioni, quali l'user-id e la password, per accedere illegalmente ad

una risorsa informatica. In generale si intende lo studio del comportamento individuale di una persona al fine di carpire informazioni.

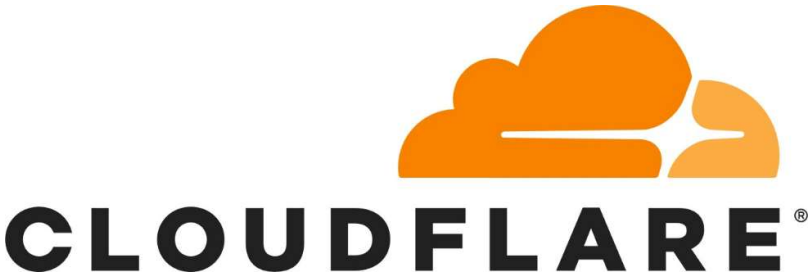
- Sniffing-snooping: tecniche mirate a leggere il contenuto (pay load) dei pacchetti in rete, sia LAN che WAN.
- Smart city: città "intelligente" largamente dotata di infrastrutture e soluzioni ICT sia per i suoi abitanti e per interagire con loro, sia per migliorare il controllo del territorio, della sua sicurezza, dell'ambiente, della viabilità, etc.
- Smart grid: grid è la rete elettrica di distribuzione di energia, che affiancata da una rete informatica che la gestisce diviene smart.
- Smurf: tipo di attacco per la saturazione di una risorsa, avendo una banda trasmissiva limitata. Si usano tipicamente pacchetti ICMP Echo Request in broadcast, che fanno generare a loro volta ICMP Echo Replay.
- SOA, Service Oriented Architetture.
- SOAR, Security Orchestration, Automation and Response.
- Spamming: invio di posta elettronica "indesiderata" all'utente.
- SPF, Sender Policy Framework: in DMARC, un record di testo DNS nel dominio considerato, che indica ai servizi di posta e ai ricevitori di ricevere l'e-mail dall'IP del server fornito nel record SPF.
- SPID, Sistema Pubblico di Identità Digitale: è attualmente obbligatorio per accedere on line ai servizi digitali delle Pubbliche Amministrazioni.
- SPML, Service Provisioning Markup Language.
- Spoofing: tipo di attacco digitale che falsifica l'indirizzo nell'intestazione Da: di un messaggio email. Un messaggio contraffatto mediante lo spoofing sembra provenire dall'organizzazione o dal dominio la cui identità è stata rubata.
- Spyware: codice maligno che raccoglie informazioni riguardanti l'attività online di un utente (siti visitati, acquisti eseguiti in rete, etc.) senza il suo consenso, utilizzandole poi per trarne profitto, solitamente attraverso l'invio di pubblicità mirata.
- SQL, Structured Query Language: linguaggio per interazione con un DB relazionale.
- SQL injection: tecnica di inserimento di codice in un programma che sfrutta delle vulnerabilità sul database con interfaccia SQL che viene usata dall'applicazione.
- SSCP, Systems Security Certified Practitioner.
- SSO, Single Sign On: autenticazione unica per avere accesso a diversi sistemi e programmi.
- Stealth: registrazione invisibile.
- Stuxnet: uno dei primi e più noti attacchi ATP, portato ai sistemi di controllo delle centrifughe delle centrali nucleari iraniane.
- SYN Flooding: invio di un gran numero di pacchetti SYN a un sistema per intasarlo.
- TA, Targeted Attacks: attacchi mirati, talvolta persistenti, effettuati con più strumenti anche contemporaneamente; rientrano in questa categoria APT e Watering Hole.
- TACS, Total Access Communication System.
- TLC, Telecomunicazioni.
- Trojan Horse (cavallo di Troia): codice maligno che realizza azioni indesiderate o non note all'utente. I virus fanno parte di questa categoria.
- TOR, The Onion Router: sistema di comunicazione anonima in Internet basato sul protocollo onion router e su tecniche di crittografia.
- Trouble ticketing: processo e sistema informatico di supporto per la gestione delle richieste e delle segnalazioni da parte degli utenti; tipicamente in uso per help-desk e contact center.
- UOSI, Unità Organizzativa Sistemi Informatici.
- UMTS, Universal Mobile Telephone System.
- URL, Uniform Resource Locator: sequenza di carattere che identifica in maniera nome univoca una risorsa ICT in rete; esempio: www.oadweb.it.
- Utente finale: utente di un sistema d'utente e/o di una o più applicazioni con i diritti di accesso relativi al suo ruolo, ma non di tipo privilegiato.
- Utente privilegiato: operatori, manutentori ed amministratori di sistema di un sistema informatico, che hanno i più elevati diritti per poter accedere e gestire le risorse ICT del

sistema informatico sulle quali debbono operare. Rientrano in questa categoria anche gli sviluppatori di software. Gli attuali trend di forte terziarizzazione di queste funzioni portano a personale esterno dei fornitori dell'azienda/ente cliente tali diritti, con la necessità di maggiori controlli su di loro per assicurarsi l'adeguate livello di sicurezza digitale.

- VoIP, Voice over IP.
- VPN,Virtual Private Network: rete virtuale creata tramite Internet per realizzare una rete "privata" e sicura per i soli utenti abilitati.
- XACML, eXstensible Access Control Markup Language.
- XSS, Cross - site scripting: una vulnerabilità di un sito web che consente di inserire a livello "client" dei codici maligni via "script", ad esempio JavaScript, ed HTML per modificare le pagine web che l'utente vede.
- Watering Hole: famiglia di attacchi che rientrano nella categoria dei Targeted Attack. Il termine, traducibile in" attacco alla pozza d'acqua", fa riferimento agli agguati di animali carnivori alle prede che si dissetano in una pozza d'acqua. La metafora è usata per attacchi mirati a siti web specialistici, ad esempio di finanza, di politica, di strategie, ecc., cui una persona o un'azienda target accede periodicamente.
- Worm: un tipo di virus che non necessita di un file eseguibile per attivarsi e diffondersi, dato che modifica il sistema operativo del sistema attaccato in modo da essere eseguito automaticamente e tentare di replicarsi sfruttando per lo più Internet.
- Zero-day attack: attacchi basati su vulnerabilità a cui non è ancora stato trovato rimedio.
- Zero Trust: approccio progettuale ed architetturale alla sicurezza digitale che si basa sul "non fidarsi" della sicurezza dei vari dispositivi e servizi ICT usati.
- Zombies, zombi: si veda bots.

Allegato C1 Profili GOLD SPONSOR

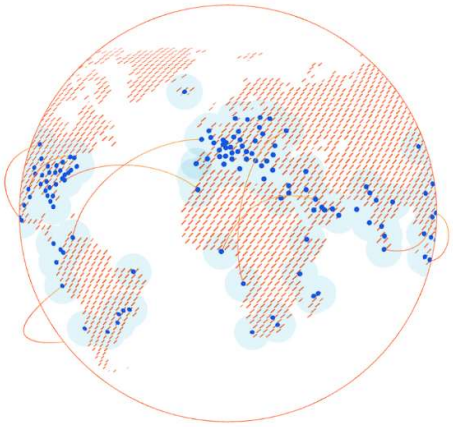
Cloudflare



www.cloudflare.com/it

Cloudflare è un'azienda leader nel campo della sicurezza, delle prestazioni e dell'affidabilità, con l'obiettivo di aiutare a costruire un Internet migliore. Attualmente Cloudflare gestisce uno dei più grandi network al mondo, con circa 28 milioni di internet properties e oltre il 16% delle aziende Fortune 1000 utilizza almeno un prodotto targato Cloudflare.

La nostra piattaforma è in grado di proteggere e accelerare qualsiasi applicazione Internet, senza alcun bisogno di aggiungere piattaforme hardware, installare nuovi programmi o modificare una sola riga di codice. L'intero traffico delle proprietà Internet che si affidano a noi viene distribuito sulla nostra rete globale intelligente, che diventa sempre più efficace richiesta dopo richiesta. Il risultato finale è un miglioramento significativo delle prestazioni e una diminuzione del traffico spam e di altri tipi di attacchi.



Cloudflare si posiziona in modo unico nell'ambito del modello SASE, *Secure Access Service Edge*, per l'ampiezza e flessibilità del portfolio e l'integrazione delle soluzioni su obiettivi di security e performance.

Aiutiamo circa 3,2 Milioni di clienti, da piccole e medie imprese a organizzazioni multinazionali a superare le sfide di performance su Internet e proteggere i propri user, applicazioni e reti da attacchi malware, in uno scenario sempre piú complesso.

Oltre 28 milioni di Internet Properties si affidano alle Soluzioni Cloudflare.
Leggi alcuni dei nostri Case Study per saperne di più! https://www.cloudflare.com/it-it/case-studies/

Soluzioni Cloudflare

Protezione DDoS
La protezione DDoS Cloudflare protegge siti web, applicazioni e intere reti, garantendo nel contempo che le prestazioni del traffico legittimo non vengano compromesse.
La rete da 51 Tbps di Cloudflare blocca in media 72 miliardi di minacce al giorno, tra cui alcuni dei più grandi attacchi DDoS della storia.

Protezione degli utenti che accedono a Internet
Cloudflare for Teams offre un accesso rapido, sicuro e ininterrotto a Internet e a tutte le applicazioni da qualsiasi dispositivo e luogo.

Dipendenti, collaboratori e clienti hanno bisogno di una rete sicura, veloce e affidabile per lavorare. Cloudflare for Teams sostituisce i perimetri di sicurezza legacy con il nostro edge globale, rendendo Internet più veloce e sicuro per i team dislocati in tutto il mondo.

Gestione dei bot

I bot dannosi non rilevati possono danneggiare il marchio, sottrarre informazioni sensibili, impossessarsi di account e avere un impatto negativo sui ricavi.
Ora è possibile gestire i bot benigni e maligni in tempo reale con velocità e precisione grazie al database (bot threat score) di dati provenienti dall'analisi di tutte le richieste IP che attraversano la rete Cloudflare.
Tutto questo con un'implementazione facile e veloce.

Accelerare le apps su Internet per incrementare i tassi di conversione

La crescente complessità delle pagine Web e la dispersione sempre maggiore degli utenti a livello globale pregiudica inevitabilmente l'esperienza utente. Memorizzando nella cache della propria rete i contenuti statici delle pagine Web, Cloudflare riesce ad avvicinare i contenuti ai tuoi utenti. I file grafici possono essere ottimizzati per migliorare in modo significativo i tempi di caricamento e i contenuti dinamici possono essere compressi e indirizzati lungo il percorso più veloce e meno congestionato verso l'utente finale. Questo permette alle aziende di offrire esperienze utente ottimali per applicazioni Internet che aumentano il coinvolgimento degli utenti e le conversioni, riducendo anche i costi.

Queste sono solo alcune delle soluzioni offerte da Cloudflare, per scoprire di più, visiti il nostro Sito Web, oppure contatti il Dipartimento Vendite:
https://www.cloudflare.com/it-it/plans/enterprise/contact/?utm

Darktrace

www.darktrace.com/it/

DARKTRACE

Darktrace

In sintesi

- Fondata nel 2013 da matematici
- Headquarters a San Francisco e Cambridge, UK
- "Europe's fastest-growing cyber security company" (Financial Times, 2020)
- Leader mondiale nell'Intelligenza Artificiale per la cyber defense
- Creatori delle tecnologie Cyber AI e Autonomous Response
- Piattaforma Cloud-native

Darktrace è la principale azienda di cyber IA al mondo e ideatrice della tecnologia di risposta autonoma.

La sua IA auto-apprendente è modellata sul sistema immunitario umano e utilizzata da oltre 4.000 organizzazioni per proteggere dalle minacce al cloud, e-mail, IoT, network e sistemi industriali. Ciò include insider threat, spionaggio industriale, IoT compromessi, malware zero-day, perdita di dati, rischio della supply chain e vulnerabilità infrastrutturali a lungo termine.

Darktrace applica la sua tecnologia alla sfida di rilevare attività digitali minacciose all'interno delle reti aziendali, con l'obiettivo di combattere nuovi attacchi informatici che aggirano gli strumenti di sicurezza basati su regole.

L'azienda ha oltre 1.300 dipendenti, 44 uffici e sede a San Francisco e Cambridge, UK, con uffici a Milano e Roma. Ogni 3 secondi, l'IA di Darktrace combatte contro una minaccia cyber, impedendole di causare danni.

DARKTRACE

SCHEDA DI PRESENTAZIONE

La sicurezza come priorità

Darktrace è l'inventore dei sistemi di intelligenza artificiale ad autoapprendimento per la difesa informatica. In termini di capitalizzazione di mercato e numero di clienti Darktrace è il leader indiscusso nel campo. Abbiamo il set di prodotti più ampio per supportare la configurazione completa delle aziende, con un braccio di sviluppo del prodotto in rapido movimento e fortemente investito. Recenti scoperte come AI Analyst, a soli sei mesi dal rilascio di Antigena Email, mostrano che il nostro appetito e la nostra capacità di risolvere i problemi dei clienti del mondo reale sono enormi.

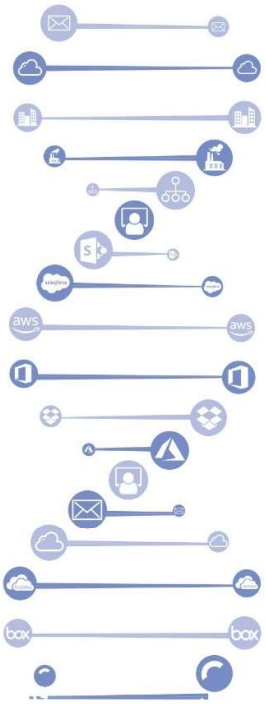
Siamo orgogliosi di essere una delle aziende tecnologiche leader a livello mondiale che opera su scala globale. Gli esperti del settore e gli analisti concordano sul fatto che mentre altre tecnologie stanno iniziando ad adottare il nostro approccio, nessuna è stata in grado di sviluppare la capacità, l'implementazione e l'usabilità per cui siamo leader di fama mondiale. Con oltre 4.000 clienti in ogni settore verticale, la nostra piattaforma sta trasformando il modo in cui le aziende proteggono la propria infrastruttura digitale.

La nostra tecnologia:

- ✔ Piattaforma di Cyber AI
- ✔ Risposta Autonoma
- ✔ Cyber AI Analyst
- ✔ Visualizzazione delle Minacce
- ✔ Sicurezza del Cloud
- ✔ Sicurezza delle E-mail

Darktrace e' l'unica piattaforma che:

- ✔ Impara le norme "sul lavoro" per rilevare nuovi attacchi e minacce interne
- ✔ Fornisce protezione unificata e personalizzata su e-mail, cloud, IoT e rete
- ✔ Neutralizza gli attacchi a velocità macchina e con precisione chirurgica
- ✔ Automatizza le indagini sulle minacce in modo rapido e su vasta scala, riducendo i tempi di triage del 92%



> "La capacità di Darktrace di vedere e rispondere autonomamente a minacce conosciute e sconosciute non ha eguali e ha reso Darktrace il leader del gruppo nell'analisi delle minacce di rete."
>
> **- Aite Group**

Milano: +39 02 5821 5328 Roma: +39 06 3671 2329 UK: +44 (0) 1223 394 100 US: +1 415 229 9100 E: info@darktrace.com www.darktrace.it

Qintesi

www.qintesi.com

Qintesi – con un organico di circa 270 dipendenti – è una *Tech-Company* che eroga servizi di *management consulting* e *system integration*. Contribuisce ad accrescere il valore e migliorare la competitività dei clienti supportandoli nei processi di digitalizzazione ed innovazione, attraverso una *value proposition* basata su soluzioni applicative SAP e Google, implementate con l'utilizzo di metodologie certificate ed il costante riferimento alle *best practices* di settore.

Qintesi è Gold Partner SAP con la qualifica di "Service Partner" e "Build Partner"; ha ottenuto differenti riconoscimenti da parte di SAP: sei Solution Service Authorizations in SAP S/4HANA Cloud, SAP Analytics, SAP Business All-in-One, Database and Data Management, SAP HANA, SAP S/4HANA; una Build Authorization in On-premise e ben undici certificazioni SAP REX, tra cui due di Industry – Insurance ed Engineering & Construction – e, tra le prime in Italia e a livello EMEA, su SAP S/4HANA, SAP HANA e SAP Real Estate Management.

Qintesi è Google Cloud Partner e ha realizzato alcuni tra i primi progetti a livello europeo di migrazione a SAP S/4HANA su piattaforma Google Cloud Platform; è attiva inoltre in importanti progetti di digital transformation basati sulla piattaforma Google.

Nell'ambito della consulenza direzionale comprende la Service Line dedicata "Management & Consulting", per offrire al mercato servizi professionali idonei a supportare le imprese nei loro percorsi di crescita, portando competenze manageriali ed efficaci strumenti operativi in ottica "best practice" di settore.

Il Network è costituito da Qintesi SpA, che si posiziona come player di riferimento nel panorama italiano dei system integrator; la controllata Qintesi Technology & Services, che disegna e realizza innovative infrastrutture tecnologiche, gestisce servizi di maintenance, di outsourcing amministrativo e provisioning di servizi esterni; la collegata BF Partners, che opera in particolare nei settori retail/GDO e pubblica amministrazione locale, affiancando a SAP applicativi per il facility management come Infocad o sistemi evoluti per la gestione commerciale; la collegata IT-Link, system integrator SAP e rivenditore ufficiale dei prodotti SAP, con competenze verticali nel settore manufacturing e solide competenze nelle applicazioni Industry 4.0 e IoT; infine Huware, azienda "change & cloud" che crede nella tecnologia Google Cloud come fattore chiave della trasformazione digitale. La sua missione è l'adozione della tecnologia per aiutare le aziende a crescere ed evolversi.

Qintesi opera su tutto il territorio con sedi a Milano, Bergamo, Venezia, Genova, Brescia e Mantova oltre ad intervenire abitualmente in contesti internazionali. I mercati di riferimento sono i financial services, in particolare il mondo assicurativo; engineering & construction, manufacturing, services & utilities, consumer products, fashion, transportation.

Il Network copre in maniera sinergica molteplici aree funzionali, declinando ciascuna soluzione in base alle specificità di settore che contraddistinguono i differenti business. Oltre a coprire l'infrastruttura IT (con annessi servizi di manutenzione, project e process management), ha solide competenze in particolare in area finance & treasury, controlling, compliance & risk, sourcing & procurement e manufacturing.

Con riferimento a tematiche attuali per le imprese, come i processi di *Governance, Risk & Compliance*, anche in ottica di *business continuity*, Qintesi si propone come un player specializzato su questi contenuti che richiedono un mix di competenze funzionali e normative relative ai processi di *Compliance* e *Risk Management*, insieme a competenze tecnologiche legate alla *Cyber Security* e alla *Data Governance*. In collaborazione con SAP ha avviato un ciclo di webinar nel corso del 2020 dedicato per trasferire al mercato il proprio *know-how*, in cui sono state approfondite le best practice in ambito SAP Cyber Security per tenere al sicuro i dati aziendali tramite i seguenti tool:

– SAP UI Logging e Masking per la tracciatura degli accessi ai dati e il Masking degli stessi per gli utenti non autorizzati

– SAP Enterprise Threat Detection per la identificazione e la prevenzione di potenziali attacchi

– SAP Code Vulnerability Analyzer per individuare le vulnerabilità nel codice SAP

La roadmap progettuale di Qintesi sul tema Cyber Security prevede un approccio integrato metodologico-applicativo a supporto di concrete necessità di sicurezza digitale perseguite dai propri Clienti, con l'obiettivo di rispondere alle più attuali richieste in tema di sicurezza e protezione del patrimonio informativo aziendale.

Sophos

www.sophos.it

SOPHOS

Cybersecurity evolved.

Oggi, gli ambienti IT sono in continua evoluzione e diventano ogni giorno sempre più complessi, proprio come le tattiche e le tecniche utilizzate dai cybercriminali. Quindi, anche le esigenze di sicurezza informatica delle organizzazioni devono evolvere. Dalla protezione della rete aziendale e degli endpoint fino alla cloud security, i nostri prodotti sono realizzati per accogliere e rispondere alle sfide odierne e future.

I sistemi di sicurezza tradizionali non sono in grado di tenere il passo con il panorama delle minacce, il quale è in continua evoluzione. Le soluzioni Sophos offrono la migliore protezione disponibile sul mercato, grazie alla combinazione tra il più potente motore di intelligenza artificiale e una protezione antiexploit e antiransomware che non ha rivali. Continuiamo a introdurre innovazioni rivoluzionarie e a migliorare costantemente la sicurezza, minimizzando i falsi positivi e automatizzando la risposta agli incidenti grazie a prodotti di sicurezza in grado di interagire gli uni con gli altri come un unico sistema.

Network Protection

I nostri prodotti di protezione della rete sono semplici da installare e da gestire, e offrono agli amministratori pieno controllo sulle funzionalità di sicurezza indispensabili per gestire gli ambienti cloud, on-premise o ibridi. E in più, l'intero sistema viene monitorato con un'unica console di gestione.

XG Firewall
Firewall next-gen con Synchronized Security e SD-WAN integrate.

SG UTM
Protezione della rete con Unified Threat Management.

Sophos Wireless
Wireless intelligente, sicuro e gestito dal cloud.

Secure Web Gateway
Il massimo in termini di sicurezza web, controllo e analisi.

Sophos Email
Un'e-mail security più intelligente, con tecnologie di intelligenza artificiale.

Phish Threat
Simulazioni di phishing e corsi di sensibilizzazione sulla sicurezza.

Cloud Security

La possibilità di trasferire dati, risorse e app sul cloud pubblico può essere un enorme vantaggio. Le soluzioni Sophos per il cloud risolvono i principali problemi delle aziende, e consentono di visualizzare e proteggere con estrema precisione, ed in maniera ininterrotta ed accurata, tutti gli ambienti dell'infrastruttura cloud.

Sophos Cloud Optix
Visibilità, rispetto della conformità e risposta alle minacce in ambienti cloud.

Sophos Central
Una piattaforma estremamente efficace per la gestione centralizzata della sicurezza.

Endpoint e Server Protection

Dai PC e server fino ai tablet, laptop e smartphone , la nostra protezione garantisce la sicurezza degli utenti senza interferire con il loro lavoro, sia che venga implementata nel cloud, on-premise o in un sistema ibrido.

Intercept X Endpoint
Una protezione endpoint con intelligenza artificiale che non ha rivali.

Intercept X Advanced with EDR
Rilevamento e risposta alle minacce endpoint insieme alla migliore protezione endpoint in assoluto.

Intercept X for Server
Protezione per ambienti server in cloud, on-premise o ibridi.

Sophos Mobile
Protezione con Unified Endpoint Management.

Sophos Central Device Encryption
Proteggi i tuoi dati dati in caso di furto o smarrimento dei computer.

Sophos Home
Una cybersecurity di classe Business, disponibile per utenti privati.

Servizi gestiti

I cybercriminali adattano le proprie tecniche sfruttando metodi molto ingannevoli, che richiedono l'intervento umano per essere smascherati e per bloccare gli attacchi. Sophos Managed Threat Response (MTR) offre un team di sicurezza dedicato e operativo 24h su 24 e 7gg su 7, in grado di intraprendere azioni adeguate per conto dei clienti, al fine di neutralizzare anche le minacce più sofisticate e complesse.

Managed Threat Response
Identificazione e risposta alle minacce 24x7

Cybersecurity evolved.

Synchronized Security

Sophos Synchronized Security è il primo sistema di cybersecurity in assoluto. Ed è anche il migliore. I prodotti Sophos interagiscono l'uno con l'altro, condividendo attivamente informazioni in tempo reale e rispondendo automaticamente agli incidenti. Questo sistema eleva il livello di protezione, semplificando la gestione e offrendo opzioni di scalabilità per la sicurezza, senza intaccare le risorse.

Sophos Central

Sophos Central è una piattaforma cloud di protezione unificata che permette alle aziende di qualsiasi dimensione di gestire tutti i prodotti Sophos da una sola interfaccia. Inoltre, con Sophos Central i partner possono gestire installazioni multiple per i clienti, tutto da un'unica interfaccia intuitiva. Rispondere agli avvisi, gestire le licenze e tener traccia delle date di rinnovo imminenti diventa così un processo molto più semplice.

SophosLabs

I SophosLabs, il nostro team internazionale di esperti di data science e di intelligence sulle minacce, sfruttano le tecnologie più avanzate e le analisi basate sul Machine Learning per elaborare milioni di messaggi, URL, file e altri dati sospetti alla velocità della luce, per garantire un'analisi completa delle minacce e del malware. Con sedi operative in tre continenti, il nostro team è in azione 24h su 24, per individuare e bloccare minacce sconosciute, per indagare sui casi più estremi, per analizzare i trend e per ottimizzare i prodotti Sophos in modo da garantire massimi livelli di protezione.

Riconoscimenti ufficiali degli esperti di settore

Analisi e recensioni a cura di esperti riconoscono ufficialmente Sophos come leader di settore. I nostri premi più recenti includono:

1. La nomina di Leader nel Quadrante magico di Gartner per le piattaforme di protezione endpoint[1] per l'undicesimo report consecutivo. Gartner ha collocato Sophos tra i Visionari nel Quadrante Magico per i Firewall di rete del 2019[2]
2. Sophos si è guadagnata l'ambitissima valutazione "Recommended" nel Next-Generation Firewall Group Test del 2019 a cura degli NSS Labs
3. 1° posto per la protezione antimalware e antiexploit, secondo MRG Effitas
4. Migliore efficacia complessiva e minore costo totale di proprietà (Total Cost of Ownership, TCO) nell'Advanced Endpoint Protection Test del 2019 a cura degli NSS Labs
5. Valutazione AAA per la Protezione delle grandi aziende, secondo gli SE Labs
6. Titolo di migliore soluzione di protezione endpoint per le piccole imprese, secondo gli SE Labs
7. Leader nella "Forrester Wave™": Endpoint Security Suites, Q3 2019[3]
8. Nel "CRN Partner Program Guide", The Channel Company ha dato una valutazione a cinque stelle al nostro Partner Program
9. Sophos si è assicurato i premi "CRN ® Annual Report Card", negli ambiti di sicurezza della rete, degli endpoint e della protezione complessiva dei dati
10. Nomina dei leader di Sophos nella Top 100 dei dirigenti compilata da CRN, con 11 dirigenti nominate tra le CRN Women of the Channel per il 2019
11. Riconoscimento come Network Technology Partner di AWS Partner per l'anno 2019

[1] Gartner Magic Quadrant for Endpoint Protection Platforms, Peter Firstbrook, Prateek Bhajanka, Lawrence Pingree, Paul Webber, Dionisio Zumerle, 23 agosto 2019.
[2] Gartner Magic Quadrant for Network Firewalls, Rajpreet Kaur, Adam Hils, Jeremy D'Hoinne, John Watts, 17 settembre 2019. Gartner non appoggia non sostiene alcun fornitore, produttore o servizio citato all'interno delle sue pubblicazioni di ricerca e non consiglia agli utenti delle tecnologie di selezionare solo i fornitori con le valutazioni più alte o altre designazioni. Le pubblicazioni di Gartner riflettono solamente le opinioni dell'organizzazione, e non devono pertanto essere considerate come affermazioni di fatto. Gartner rinuncia a qualsiasi garanzia, implicita o esplicita, in merito a questa ricerca, incluse le garanzie sulla commerciabilità o sull'idoneità a un particolare scopo.
[3] The Forrester Wave™: Endpoint Security Suites, Q3 2019 di Chris Sherman, lunedì 23 settembre 2019.

SOPHOS
I DATI SALIENTI

1985
ANNO DI FONDAZIONE

3.500
DIPENDENTI
IN TUTTO IL MONDO

90%+
TASSO DI RINNOVO

350.000
AZIENDE

100 milioni
UTENTI

150
PAESI

+ di 47.000
CHANNEL PARTNER

Vendite per Italia:
Tel: (+39) 02 94 75 98 00
E-mail: sales@sophos.it

07/10/19 CO-NA (GH)

SOPHOS

Allegato C2 Profili SILVER SPONSOR

Technology Estate

Technology Estate è una società italiana di Information & Communication Technology specializzata nello sviluppo, produzione e distribuzione di prodotti software di sistema (infrastructure products) ad elevato contenuto tecnologico.

Technology Estate, grazie alla elevata professionalità e competenza maturata in anni di esperienza in campo nazionale ed internazionale, è una delle poche società italiane ad aver identificato e sviluppato una serie di tecnologie che consentono alle moderne realtà organizzate di raggiungere e mantenere nel tempo un reale vantaggio competitivo.

Technology Estate commercializza i propri prodotti direttamente e si avvale di una rete di partner certificati per poter offrire al Cliente un servizio completo e altamente qualitativo. Nell'ambito della sicurezza informatica è stata la prima società ad introdurre in Italia soluzioni complete di grafometria.

Grazie a Technology Estate alcune grandi aziende italiane hanno introdotto la grafometria con enormi risparmi nella gestione documentale: il documento con una o più firme "nasce" elettronico. Ma tali risparmi sono anche alla portata di medie e piccole aziende/enti con un elevato numero di documenti firmati e/o con la necessità di una identificazione biometrica dei firmatari.

Per maggiori informazioni: http://www.technologyestate.eu/

Allegato D Profilo Patrocinatori

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' ECDL e l'eCF (UNI EN 16234-1:2016): per quest'ultimo è accreditata come ente certificatore.

https://www.aicanet.it/

A.I.S.I.S.

Associazione Italiana Sistemi Informativi in Sanità, raggruppa i professionisti ICT nelle aziende sanitarie italiane pubbliche o private, e favorisce la crescita dell'attenzione sulle problematiche connesse all'utilizzo dell'ICT in sanità come leva strategica di cambiamento.

https://www.aisis.it/

AITASIT

AITASIT è un'associazione scientifica apartitica, apolitica e senza scopi di lucro che riunisce i tecnici sanitari di radiologia medica specialisti nella gestione dei sistemi informativi in diagnostica per immagini.

http://www.aitasit.org/

ASSI-Bologna

Associazione Specialisti Sistemi Informativi, è l'associazione senza fine di lucro di professionisti dell'ICT che favorisce e stimola l'incontro fra colleghi, in maniera del tutto informale, e realizza un piano di informazione periodico attraverso incontri e seminari scelti e finanziati dai Soci. Aderisce a FIDAInform.

www.assi-bo.it

Assintel

Associazione Nazionale Imprese ICT, è l'associazione di categoria in ambito Confcommercio: promuove incontri territoriali, gruppi di lavoro tematici e mette a disposizione un portale associativo per fare network tra le aziende che operano nel mercato dell'ICT.

http://www.assintel.it/

Assolombarda

Associazione territoriale di Confidustria, favorisce lo sviluppo delle imprese associate fornendo supporto, aggiornamenti costanti e occasioni di formazione sulle principali tematiche e problemi tecnici.

http://www.assolombarda.it/

AUSED

Associazione tra Utenti di Sistemi e Tecnologie dell'Informazione, è una associazione indipendente e senza scopi di lucro che raggruppa aziende e professionisti del lato domanda ICT, che operano in diversi settori, tra cui quello industriale, manifatturiero, dei servizi, nonché alcuni enti pubblici.

www.aused.org

Centro Ricerche sulla Scrittura

Associazione senza scopo di lucro che si occupa della formazione dei "Grafobiometristi", professionisti esperti con specifiche competenze sulla valutazione ed analisi della manoscrittura acquisita con le tecniche biometriche, oltre che effettuare ricerche sulle tecnologie biometriche ed il loro uso.

www.centroricerchesullascrittura.it

CIOClub

Libera associazione tra professionisti dell'IT per condividere conoscenza e confrontarsi per lavoro o per passione, nella gestione dei dipartimenti IT. Obiettivi: sviluppare idee comuni, realizzare grandi progetti, condividere iniziative di successo.

https://cioclubitalia.it/

Club Dirigenti di informatica Torino

Libera associazione apolitica senza scopi di lucro di professionisti dell'ICT dell'area torinese- piemontese, che si propone come punto di riferimento e di incontro per chi si occupa di information management. Aderisce a FIDAInform.

http://www.clubdi.org/

Club Dirigenti Tecnologie dell'Informazione di Roma

Libera associazione apolitica senza scopi di lucro di professionisti dell'ICT dell'area romana-laziale, che si propone di contribuire allo sviluppo sociale, economico e industriale del Paese tramite la promozione dell'uso delle tecnologie dell'informazione. Aderisce a FIDAInform.

https://cdtiroma.ning.com/

Club per le Tecnologie dell'Informazione dell'Emilia-Romagna

Libera associazione apolitica senza scopi di lucro di professionisti dell'ICT dell'area regionale, i cui membri sono consulenti e professionisti manageriali del settore informatico. Primari obiettivi lo sviluppo sociale, economico e industriale del Paese attraverso la promozione di un corretto uso delle Tecnologie dell'Informazione.
http://www.clubtier.org/

Club per le Tecnologie dell'Informazione e dell'Innovazione Italia Centro

Libera associazione apolitica senza scopi di lucro di professionisti dell'ICT prevalentemente dell'area marchigiana-anconetana, per lo sviluppo professionale e culturale dei Soci relativamente **alle competenze IT e all'innovazione dei processi attraverso le tecnologie IT.**
https://www.clubticentro.it/

Club per le Tecnologie dell'Informazione di Milano

Libera associazione apolitica senza scopi di lucro di professionisti dell'ICT dell'area milanese-lombarda per la promozione delle discipline digitali attraverso la crescita professionale e lo scambio di competenze tra i soci. Aderisce a FIDAInform.
http://www.clubtimilano.net/

Club per le Tecnologie dell'Informazione della Liguria

Libera associazione apolitica senza scopi di lucro di professionisti dell'ICT dell'area genovese-ligure, per promuovere l'innovazione ICT e lo scambio di conoscenze tra i propri soci, che operano nel campo dell'ICT sia come utilizzatori che come fornitori. Aderisce a FIDAInform.
http://www.ctiliguria.it/

FIDAInform

Federazione Nazionale delle Associazioni Professionali di Information Management: è la federazione a livello nazionale dei vari Club della tecnologia dell'informazione operanti a livello regionale. Si propone come "nodo" attivo del Sistema-Paese per lo sviluppo del settore delle tecnologie dell'informazione e della comunicazione, promuovendo la professionalità dei Soci.
http://www.fidainform.it/

FiiF

Fondazione Italiana per l'Innovazione Forense, Fondazione del CNF, Consiglio Nazionale Forense, promuove l'innovazione digitale e l'aggiornamento tecnologico dell'Avvocatura italiana.

http://www.fiif.it

GIA

Grafobiometristi Italiani Associati, è l'associazione che raggruppa i professionisti grafometrici che operano con la grafobiometria, lo studio ed l riconoscimento della mano scrittura, in particolare di firme, su tablet ed altri dispositivi digitali tramite indicatori biometrici, e che trova applicazione in molteplici ambiti: forense, educativo e scientifico.
http://www.grafobiometristi.it/

IEEE Computer Society - Capitolo Italiano

Il capitolo italiano dell'associazione mondiale IEEE è il punto di contatto e incontro in Italia per gli interessati ai temi dell'informatica e delle relative applicazioni, per facilitare la diffusione e il reperimento di informazioni e opportunità.

http://sites.ieee.org/italy-cs/

Inforav

Istituto per lo sviluppo e la gestione avanzata dell'informazione, è una libera associazione senza scopi di lucro, a cui aderiscono Amministrazioni ed Enti pubblici, Associazioni, Fondazioni, Società Finanziarie, Commerciali ed Industriali di primaria rilevanza nazionale; promuove e sviluppa iniziative di interesse generale o della Pubblica Amministrazione, con la collaborazione dei propri Soci e anche di esperti di conclamata competenza, in diversi settori dell'ICT e dell'Organizzazione. Aderisce a FIDAInform.
http://www.inforav.it/cms/index.php

Allegato E Riferimenti e fonti

E.1 Dall'OCI all'OAI e a OAD: un po' di storia

- FTI: "Osservatorio sulla criminalità informatica – Rapporto 1997", Franco Angeli.
- M. R. A. Bozzetti, P. Pozzi (a cura di): "Cyberwar o sicurezza? Secondo Osservatorio Criminalità ICT", 2000, Franco Angeli.
- M. R. A. Bozzetti, R. Massotti, P. Pozzi (a cura di): "Crimine virtuale, minaccia reale", 2004, Franco Angeli
- M. R. A. Bozzetti: "Sicurezza Digitale - una guida per fare e per far fare", 2007, Soiel International
- R. Borruso, S. Russo, C. Tiberi : " L' informatica per il giurista. Dal Bit a internet", 2009, Giuffré Editore.
- G. Sartor: "L'informatica giuridica e le tecnologie dell'informazione", 2012, Giappichelli Editore
- M. R. A. Bozzetti, F. Zambon: "Sicurezza Digitale – una guida per governare un sistema informatico sicuro", Giugno 2013, Soiel International, ISBN 9788890890109
- I vari Rapporti annuali OAI e OAD: https://www.oadweb.it/it/main-it/rapporti-e-relativi-convegni.html
- Presidenza del Consiglio dei Ministri: "Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico", Dicembre 2013, http://www.agid.gov.it/sites/default/files/leggi_decreti_direttive/quadro-strategico-nazionale-cyber_0.pdf
- Presidenza del Consiglio dei Ministri: "Piano nazionale per la protezione cibernetica e la sicurezza informatica", Marzo 2017, https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf
- NIS, Network and Information Security, *Direttiva EU* 2016/1148, per la sicurezza digitale dei carrier TLC e delle infrastrutture critiche dei vari paesi europei; ripresa in Italia dal D.Lgs. 65/2018
- Cyber Security Act, Direttiva EU 2019/881, in vigore dal 27/6/2019.

E.2 Le principali fonti sugli attacchi e sulle vulnerabilità

L' elenco, in ordine alfabetico, non ha alcuna pretesa di essere esaustivo e completo: le fonti citate sono quelle indipendenti, ossia di nessun fornitore di sicurezza digitale, e quelli considerati più autorevoli a livello mondiale.

- ABILAB - Centrale d'allarme per attacchi informatici per l'ambito bancario, accessibile solo agli iscritti: www.abilab.it
- CSIRT, Computer Security Incident Response Team – Italia: https://csirt.gov.it/
- CVE, Common Vulnerabilities and Exposures, è un elenco aggiornato di tutte le vulnerabilità note pubblicamente, identificate da un numero univoco: https://cve.mitre.org/
- ENISA, European Union Agency for Network and Information Security: http://www.enisa.europa.eu/

- First, Forum for Incident Response and Security Team, fornisce aggiornate informazioni su attacchi e vulnerabilità, classificandole in base al CVSS, Common Vulnerability Scoring System[29]: http://www.first.org/
- Internet Crime Complaint Center (IC3) è una partnership tra FBI (Federal Bureau of Investigation), il National White Collar Crime Center (NW3C) e il Bureau of Justice Assistance (BJA), e fornisce, oltre alla possibilità di denunciare negli US attacchi digitali, informazioni sugli attacchi stessi e sui trend in atto per i crimini digitali: http://www.ic3.gov/default.aspx
- NVD, National Vulnerability Database, è l'archivio statunitense di informazioni sulla vulnerabilità standardizzate e gestibili in maniera automatizzata con il protocollo SPAC: https://nvd.nist.gov/
- OECD, Organisation for Economic Co-operation and Development, produce rapporti sui rischi e gli attacchi digitali che impattano sull'economia delle nazioni in Europa: http://www.oecd.org/sti/ieconomy/security.htm
- OWASP, Open Web Application Security Project, progetto open source per la sicurezza delle applicazioni web, fornisce vari rapporti e linee guida sul tema, tra cui, periodicamente, le "top ten", le vulnerabilità ed i rischi più critici per le applicazioni web: https://www.owasp.org/
- SANS Institute fornisce sistematicamente segnalazioni su vari tipi di attacchi e di vulnerabilità, oltre all'aggiornato elenco 20 prioritari controlli di sicurezza per le norme Federali US FISMA: www.sans.org
- Sistema di informazione per la sicurezza della Repubblica Italiana, insieme di organi e autorità che hanno il compito di assicurare le attività di informazione per la sicurezza, allo scopo di salvaguardare la Repubblica da ogni pericolo e minaccia proveniente sia dall'interno sia dall'esterno del Paese, inclusa la sicurezza digitale: http://www.sicurezzanazionale.gov.it/
- WASC, Web Application Security Consortium, effettua vari progetti indipendenti sulla sicurezza digitale per le applicazioni web, e fornisce il WASC Threat Classification Online, simile a OSWAP: http://www.webappsec.org/,
- World Economic Forum, realizza un annuale rapporto sui rischi globali, che includono anche i rischi ICT e le cyberwar; http://www.weforum.org/issues/global-risks.

[29] CVSS è un sistema di valutazione delle vulnerabilità attribuendo loro un punteggio in base numerico che rifletta la sua gravità. Il punteggio numerico può quindi essere tradotto in una rappresentazione qualitativa (come bassa, media, alta e critica) per aiutare le organizzazioni a valutare e prioritizzare in modo adeguato i loro processi di gestione delle vulnerabilità. I punteggi vengono calcolati in base a una formula che dipende da diverse metriche che approssimano la facilità di exploit e l'impatto dell'exploit. I punteggi vanno da 0 a 10, con 10 è il più grave. Mentre molti utilizzano solo il punteggio CVSS Base per determinare la severità, i punteggi temporali e ambientali esistono anche, per tenere conto della disponibilità di mitigazioni e di come i sistemi vulnerabili diffusi sono all'interno di un'organizzazione, rispettivamente.

Allegato F Profilo dell'autore Marco R. A. Bozzetti

Marco Rodolfo Alessandro Bozzetti, ingegnere elettronico laureato al Politecnico di Milano, è fondatore e amministratore di Malabo S.r.l (www.malaboadvisoring.it), società di consulenza direzionale sull'ICT (Information and Communication Technology) creata nel 2001.
Attraverso Malabo, Marco ha condotto e conduce interventi consulenziali presso Aziende ed Enti lato sia offerta sia domanda ICT.
Marco ha operato con responsabilità crescenti presso primarie imprese di produzione, quali Olivetti ed Italtel, e di consulenza, quali Arthur Andersen Management Consultant e GEA/GEALAB, oltre ad essere stato il primo responsabile dei sistemi informativi dell'intero Gruppo ENI a livello mondiale (1995-2000). In tale posizione ha realizzato la terziarizzazione delle infrastrutture ICT dell'intero Gruppo (più di 22 Data Center) e della rete di comunicazione italiana in fibra ottica: a quella data una delle più grandi terziarizzazioni in Italia e in Europa. Agli inizi della sua carriera, in ambito Olivetti e del CREI del Politecnico di Milano, è stato uno dei primi ricercatori a livello mondiale ad occuparsi di internetworking, a partire dalla sua tesi di laurea.
A livello consulenziale innumerevoli gli interventi tecnici-organizzativi sui sistemi informatici di medie e grandi Aziende private, oltre che di alcuni Enti pubblici. aventi il principale obiettivo di allineare l'ICT al business, di innovarlo e di generare valore effettivamente misurabile.
I principali campi di intervento includono la governance ICT, la sicurezza digitale, l'analisi e gestione dei rischi ICT e dei loro impatti (BIA), il disegno di architetture ICT, la razionalizzazione e la gestione del sistema informatico, la definizione ed il supporto di strategie ICT, l'assessment delle tecnologie, delle competenze e dei ruoli ICT, l'analisi del valore per l'ICT, l'innovazione tramite l'ICT, la riorganizzazione di strutture e processi, il supporto per la compliance alle varie normative, in particolare alla privacy e al suo recente regolamento europeo GDPR (General Data Protection Regulation).
Dal 2009 Marco, in collaborazione con Malabo, AIPSI, Polizia Postale ed altri Enti ed associazioni, ha ideato e realizza OAD, Osservatorio Attacchi Digitali in Italia: è un'indagine via web, totalmente anonima e rivolta a tutti i settori merceologici, Pubbliche Amministrazioni incluse, che produce annualmente uno o più Rapporti sul fenomeno degli attacchi digitali intenzionali in Italia.

Marco è stato Presidente e VicePresidente di FidaInform, di SicurForum in FTI e del ClubTI di Milano, oltre che componente del Consiglio del Terziario Innovativo di Assolombarda.
È attualmente Presidente di AIPSI, Associazione Italiana Professionisti Sicurezza Informatica e Capitolo Italiana della mondiale ISSA, e nel Consiglio Direttivo di FIDAInform, socio fondatore e componente del Comitato Scientifico dell'FTI, socio e revisore dei conti del ClubTI di Milano.
È certificato ITIL v3 ed EUCIP Professional Certificate "Security Adviser". È Commissario d'Esame in AICA per le certificazioni eCFPlus (EN 16234-UNI 11506).
Ha pubblicato articoli e libri sull'evoluzione tecnologica, la sicurezza digitale, gli scenari e gli impatti dell'ICT.

Allegato G Malabo Srl

Malabo Srl opera dal 2001 nell'ambito della consulenza direzionale per la digitalizzazione, basandosi su una rete consolidata di esperti "senior" e di società ultra-specializzate, per clienti lato sia offerta sia domanda ICT, Information and Communication Technology. Malabo dispone di un piccolo laboratorio ICT, in parte in cloud e in parte on premise, con il quale può installare e testare la maggior parte di sistemi e piattaforme presenti sul mercato.
Grazie alle competenze interdisciplinari del suo staff, Malabo si è specializzata nella progettazione, realizzazione e gestione di misure tecniche ed organizzative per la sicurezza digitale, ivi inclusa l'analisi e la gestione dei rischi ICT.

Malabo è in grado di fornire, ai Clienti sia della domanda che dell'offerta ICT:

- interventi consulenziali e di coaching
  - presso il responsabile del sistema informatico (CIO) e del suo staff: riorganizzazione della sua struttura, rapporti con l'alta direzione e con le altre direzioni, miglioramento della gestione operativa e della "governance" del Sistema Informatico, ruolo di supervisore o di capo progetto in progetti critici, Piano di Disaster Recovery e suo periodico test, etc.
  - presso l'Alta Direzione ed i suoi componenti operativi (Board of Director, Consiglio di Amminsitrazione, Amministratore, Direttore Generale, CEO, COO, CTO, etc.) per la valutazione dell'efficacia e dell'efficienza dell'attuale struttura organizzativa (e delle sue competenze e capacità) del Sistema Informatico, per rmigliorare ed accelerale la trasformazione digitale, per migliorare la governance del Sistema Informatico, Piano di Business Continuity e suo periodico test, analisi del valore dell'ICT, etc.
  - presso il responsabile commerciale e/o di marketing (ma sovente anche con l'AD/DG) delle aziende dell'offerta, individuazione di tecnologie e soluzioni innovative su cui investire e/o da acquisire, indiacazioni e supporto per riposizionamento sul mercato, etc.
- interventi di formazione e di sensibilizzazione sia in aula che con webinar/web live/e-learning
- l'attivazione e la gestione di specifici strumenti informatici di supporto, sviluppati e personalizzati da Malabo nel corso della consulenza, o acquisiti dal Cliente (come uno dei risultati della consulenza stessa) o preesistenti presso il Cliente.

Il denominatore comune di ogni intervento è aiutare concretamente il cliente nell'uso efficace ed efficiente dell'ICT in modo da incrementare l'effettivo e misurabile valore per il suo business e per le sue attività.

Le principali aree di eccellenza e competenza di Malabo includono le tecnologie e le architetture ICT, la sicurezza digitale (Cybersecurity), il governo e gestione ICT (Sistema Informatico), la conformità a normative e standard (compliance), le competenze, profili e ruoli ICT nell'organizzazione.
I principali vantaggi competitivi di Malabo, percepiti dai suoi Clienti, includono l'effettiva, consolidata esperienza e l'aggiornata competenza dei Partner, da cui deriva la semplicità, la velocità e l'economicità dell'intervento, la contestualizzazione dell'intervento sulla realtà del Cliente con la realizzazione di soluzioni su misura e di effettivo trasferimento di conoscenza, il riferimento agli standard e alle best practice internazionali, l'utilizzo di strumenti informatici di supporto, i servizi on line e la formazione.

Per maggiori informazioni: **www.malaboadvisoring.it**

Allegato H Reportec

Dal 2002 Reportec è attiva nell'editoria specializzata, in particolare per il settore ICT, realizzando e pubblicando riviste, report, survey, e-magazine, Webinar, video, libri sull'ICT e prodotti personalizzati per aziende. La redazione, composta da giornalisti professionisti, è anche impegnata nell'alimentare siti Web specializzati con notizie quotidiane pubblicate su www.reportec.it e https://www.tomshw.it/business/ Testate di riferimento sono Direction, dal 2003 la rivista per i CIO e i manger aziendali alle prese con i processi di business alimentati dalle tecnologie digitali, e Partners, la rivista per i manager del canale trade ICT. Security & Business, dal 2005, informa professionisti e manager sulle problematiche relative alla sicurezza informatica e alla protezione dei dati e degli asset aziendali. Reportec possiede un database con oltre 50mila nominativi di manager di alto livello in aziende end user e operatori di canale di tutte le dimensioni: dalla grande impresa alla medio-piccola azienda, su tutto il territorio nazionale e in vari settori. Un database "abituato" a ricevere pubblicazioni di alto spessore e a essere coinvolto in indagini e analisi sul mercato e le tecnologie. Reportec è in grado di interpretare specifiche esigenze di informazione nel settore dell'Information e Communication Technology professionale, attraverso l'impiego di mezzi funzionali ai bisogni del marketing e adatti anche a soddisfare i nuovi paradigmi di comunicazione multicanale. Reportec interpreta in un modo nuovo sistemi di comunicazione specifici per il Canale e per coloro che al Canale vogliono fare arrivare il loro messaggio con un approccio innovativo e qualificato. Nel 2015 Reportec ha costituito una nuova divisione dedicata al mondo agroalimentare, food e beverage, che realizza e pubblica notizie e approfondimenti su www.de-gustare.it, un sito dedicato agli appassionati di enogastronomia e agli addetti al settore, risultando spesso fonte per le stesse agenzie stampa, come ANSA.

Per maggiori informazioni: **www.reportec.it**

Allegato I 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.
AIPSI ha creato un "gruppo speciale di interesse" sulla realtà professionale delle donne nella sicurezza digitale in Italia: CSWI, Cyber Security Woman Italy, e con il quale effettua un'indagine annuale.
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: www.aipsi.org e www.issa.org

OAD
Osservatorio
Attacchi Digitali
in Italia

I Patrocinatori di OAD 2020