OAD
Osservatorio
Attacchi Digitali
in Italia

Rapporto 2021 OAD

Aggiornamento Aprile 2022

a cura di Marco R. A. Bozzetti

GOLD SPONSOR

QUINTESI

SILVER SPONSOR

Technology Estate

Ireth
Authentication & Digital Banking

in collaborazione con Polizia Postale e delle Comunicazioni

polizia delle comunicazioni

Indagine effettuata da

aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

malabo
ICT Advisory

Progetto scelto da

REPUBBLICA DIGITALE

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 OAD 2021. 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 ,dott. Francesco Zambon
- per Malabo Srl: dott. Andrea Bozzetti, Giuseppe Cesa Bianchi

oltre che alla Polizia Postale e delle Comunicazioni per i dati forniti per §8.

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 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, AIPSI, gli Sponsor ed i Patrocinatori di OAD 2021 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 OAD 2021.

OAD Extended è un progetto scelto da Repubblica Digitale
https://repubblicadigitale.innovazione.gov.it/it/i-progetti/

Rapporto OAD 2021 pubblicato il 29 aprile 2022.
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

OAD
Osservatorio
Attacchi Digitali
in Italia

Sommario

1. Sintesi direzionale

L'Osservatorio Attacchi Digitali in Italia, OAD, con la presente edizione 2022 giunge al quattordicesimo 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 informativi delle aziende e degli enti pubblici operanti in Italia. OAD non predefinisce uno specifico bacino di rispondenti, il medesimo negli anni, ma consente a chiunque, interessato e coinvolto nella gestione di un Sistema Informativo (SI) di una azienda/ente, un pieno e libero accesso al questionario online, in maniera totalmente anonima; grazie al numero di risposte raccolte e alla loro distribuzione tra aziende ed enti pubblici di varie dimensioni e appartenenti a diversi settori merceologici, l'indagine OAD fotografa "dal basso" il fenomeno degli attacchi digitali intenzionali in Italia ad imprese pubbliche e private, coinvolgendo nell'indagine anche le piccole e piccolissime realtà, che costituiscono la stragrande maggioranza delle imprese in Italia, e che altre indagini nazionali ed internazionali ben difficilmente considerano. L'indagine OAD è stata scelta tra i progetti di Repubblica Digitale, si veda https://repubblicadigitale.innovazione.gov.it/it/i-progetti/, per la sua importanza in termini di comunicazione, sensibilizzazione e formazione sulla cybersecurity.

L'indagine OAD 2021 si è svolta perdurando ancora la pandemia Covid-19, e questo ha reso ancor più difficile che negli anni precedenti motivare chi potesse compilare uno dei due questionari realizzati online, uno "ridotto" con circa la metà delle domande rispetto all'altro "completo". Nonostante questi due questionari disponibili, rigorosamente anonimi, e nonostante, come incentivo, una macro-valutazione qualitativa del livello di sicurezza digitale del Sistema Informativo (SI) oggetto delle risposte fornite a fine compilazione, oltre ad una più ampia e serrata campagna promozionale on line dell'indagine, si è dovuto ritardare la preparazione del presente rapporto finale, rispetto ai piani, per poter raggiungere un numero sufficiente di risposte perché l'indagine nel suo complesso avesse validità.

L'indagine online OAD 2021 fa riferimento all'intero anno 2020 ed al 1° semestre 2021, periodo nel quale era ancora in corso la pandemia del Covid-19, che ha continuato a causare numerosi attacchi digitali, dato l'ampio ricorso al lavoro da remoto da casa (*smart working*) ed il forte utilizzo di servizi su Internet. Dato il prolungarsi dell'indagine fino ad inizio 2022, il presente rapporto fornisce, oltre ai dati raccolti nel periodo considerato, anche informazioni su alcuni importanti attacchi digitali del 2° semestre 2021 e del 1° trimestre 2022, quando si fecero più evidenti gli attacchi cyber legati all'invasione dell'Ucraina.
Il bacino di rispondenti emerso copre tutti i settori merceologici, incluse le Pubbliche Amministrazioni, anche se più di 1/4 appartiene al settore ICT (26,0% del totale). In termini di dimensioni delle Aziende/Enti dei rispondenti, come numero di dipendenti, il bacino emerso è ben bilanciato tra quelle al di sotto dei 250 dipendenti e quelle più grandi. Si deve tener conto che in Italia il 99,91% delle imprese sono PMI, Piccole Medie Imprese, con meno di 250 dipendenti, e di queste il 95% sono sotto i dieci dipendenti; anche nell'ambito delle Pubbliche Amministrazioni, soprattutto locali, come numero di dipendenti la prevalenza è di organizzazioni simili alle PMI. Nell'indagine OAD 2021 il 71,4% dei rispondenti appartiene a strutture con un organico inferiore ai 250 dipendenti, e di queste il 28,6% sotto i 10.
Per il 2020 gli attacchi digitali ai Sistemi Informativi (SI) del bacino dei rispondenti sono ammontati al 59,1% del totale, e per il 1° semestre 2021 al 59,8%. Si arriva quindi vicini al 60% di attacchi ai SI delle aziende/enti rispondenti, con un notevole incremento rispetto al trend attorno al 40% rilevato nelle precedenti indagini OAD tra il 2007 ed il 2016, e con oscillanti incrementi tra il 45-55% dal 2017 al 2019.
La correlazione dei dati sugli attacchi rilevati con le dimensioni ed il fatturato delle aziende/enti rispondenti mostra anche in questo periodo la chiara tendenza all'aumento degli attacchi digitali per organizzazioni di dimensioni e per fatturato crescenti. Questo conferma che le piccole e piccolissime organizzazioni, sia private che pubbliche, non rappresentano un obiettivo di interesse specifico per i cyber criminali, soprattutto per i

così detti attacchi mirati (targeted attack), mentre 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.

La tipologia di attacco digitale più diffuso in entrambi i periodi considerati è stato quello ai sistemi di controllo degli accessi (IAA, Identificazione Autenticazione Autorizzazione), con un 30,0% nel 2020 e con un 28,2% nel 1° semestre 2021. Al secondo posto, con un 28,2% e un 25,9% di diffusione nel bacino di rispondenti nei due periodi considerati, l'attacco al singolo sistema ICT, ed al terzo posto la saturazione delle risorse, con un 17,6% e un 17,1% rispettivamente. Seguono, a decrescere in percentuale, le altre 11 tipologie d'attacco. Come tecniche di attacco, ossia come si attacca, tutte le sette famiglie considerate da OAD sono state largamente impiegate nei vari tipi d'attacco, anche contemporaneamente. La più diffusa percentualmente è risultata la raccolta malevole e non autorizzata di informazioni (ingegneria sociale, phishing, etc.) con un 76,5%, seguita con un 62,4% dall'uso di codici maligni e script.

Gli impatti, tecnici ed economici, a seguito degli attacchi più gravi sono raccolti 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, e nel complesso, tenendo conto di tutte le tipologie, emerge che:

- gli impatti tecnici e funzionali sul SI sono dichiarati non o poco rilevanti per il 38,1% nel 2020 e per il 32,3% nel 1° semestre 2021; gli impatti più gravi con interruzione dell'erogazione dei servizi digitali dal SI superiore ai tre giorni, hanno coinvolto il 15,3% ed il 13,8% dei SI nei due periodi considerati: percentuali alte che confermano la pericolosità dei più recenti attacchi digitali;
- l'impatto di costo sui budget sia del SI sia dell'intera azienda/ente a seguito dal più grave attacco subito è dichiarato nullo o irrilevante per il 88,7% nel 2020 e per il 79,4% nel 1° semestre 2021; gli impatti più forti incidono molto più sul budget dell'ICT (rispettivamente per il 43,3% e per il 42,3% dei SI), che sul bilancio dell'intera azienda/ente (rispettivamente per il 11,3% e per il 2,1%);
- i tempi di ripristino dopo il più grave attacco sono entro un solo giorno per circa 1/3 dei casi, ma per l'8,8% sono oltre un mese: un altro indicatore della pericolosità degli attacchi da un lato, e della mancanza o insufficienza delle misure di ripristino, dai backup al Disaster Recovery, in alcuni SI;
- le motivazioni degli attacchi digitali sono nella stragrande maggioranza dei casi di tipo economico, quindi per ricatto/ritorsione con un 93,8%: l'ampia diffusione in Italia dei ransomware ne è una chiara conferma.

Per i 2/3 delle aziende/enti rispondenti il SI è essenziale per il funzionamento delle loro attività e dei loro processi. Per questo motivo la sicurezza digitale del SI deve essere di alto livello ed infatti i SI oggetto dell'indagine 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 rispetto alle indagini OAD precedenti.
Gli obblighi normativi dettati dalla normativa GDPR per la privacy e dal NIS per i servizi essenziali-infrastrutture critiche, oltre agli attacchi subiti per la pandemia Covid 19, hanno sicuramente contribuito a rafforzare le misure di sicurezza digitale, ed un ulteriore miglioramento deriva dal crescente uso di servizi in cloud o terziarizzati, adottati dal 79,8% dei SI rispondenti, dove le misure di sicurezza sono normalmente di alto livello e allo stato dell'arte. Significativa la macro valutazione, in automatico alla fine della compilazione di uno dei questionari, del livello di sicurezza digitale: per il 54% dei SI è buono, con idonee misure, per il 10% è sufficiente, per il 13% è insufficiente e per il 23% è molto critico, e necessita di urgenti e significativi interventi.
Le misure organizzative per la sicurezza digitale, storicamente carenti e trascurate rispetto a quelle tecniche, sono complessivamente migliorate, confrontandole come trend con quelle degli anni scorsi. Il ruolo del CISO, Chief Information Security Officer, è ufficializzato e presente nel 61,2% delle aziende/enti rispondenti, e solo nel 54% dei casi opera all'interno dell'UOSI, Unità Organizzativa Sistemi Informativi, rispondendo quindi al

CIO, Chief Information Officer; negli altri casi è in altre strutture organizzative, un ulteriore indicatore del buon livello di sicurezza digitale in atto nel bacino dei rispondenti, che rispettano il principio della separazione delle responsabilità, evitando che il controllato per la sicurezza digitale, il CIO, controlli il controllore, il CISO. Solo il 20,4% dei rispondenti non ha attivato policy e procedure organizzative per la sicurezza digitale: quasi l'80% le ha, ma di questi il 53,4% le ha definite solo per talune aree o funzioni. Il 63,2% dei rispondenti ha definito un ERT, Emergency Response Team, l'86,2% effettua l'analisi dei rischi ICT, ed il 61,4% effettua audit sulla sicurezza digitale.
OAD 2021 analizza con un certo dettaglio, pur rimanendo a livelli generali, le misure e gli strumenti tecnici di sicurezza digitale in essere, e per le varie analisi elaborate si rimanda al Capitolo 7. In sintesi, sulle misure tecniche emerge che:

- si va consolidando l'adozione di specifica architetture per la sicurezza digitale integrate con quelle dell'intero SI e basate su standard e best practice mondiali (NIST, ISO, ANSI/TIA 942, etc.); il 59,4% dei SI con almeno un Data Center sono a livello Tier III TIA;
- le misure di sicurezza fisica e perimetrale di base sono presenti nella maggior parte dei SI anche non dotati di Data Center; alcune carenze, ad esempio per UPS e sistemi di allarme, per i SI molto piccoli;
- per le misure di IAA, Identificazione, Autenticazione, Autorizzazione, l'autenticazione debole è usata da 1/3 dei SI, anche per gli utenti privilegiati, e la gestione delle password è centralizzata per il 63% dei SI;
- la gestione ed il controllo della sicurezza per le reti locali e geografiche dei SI è centralizzata e vengono usati strumenti specifici quali DMZ, Firewall, DMZ, IPS/IDS, etc. per il 64,5% dei SI, ma solo il27% utilizza servizi in cloud, tipo SASE, per aumentare il livello di sicurezza;
- la protezione del software e degli applicativi dei sistemi ICT è prevalente attuata per gli applicativi più critici; il 70,1% dichiara che i software ad hoc sono stati sviluppati in maniera intrinsecamente sicura ed il 79,4% che effettua la manutenzione correttiva;
- diverse e complementari le misure per la protezione dei dati: per il 71% dei SI i dati sono classificati, i dati personali sensibili sono archiviati criptati per il 31,8% e quelli riservati (non personali) sono criptati nel 35,5% dei SI; il backup serio ed efficace è effettuato solo dal 50% dei SI, e le relative procedure di ripristino da backup esistono e sono seriamente seguite nel 46% dei casi;
- il controllo, monitoraggio e gestione della sicurezza digitale, nella maggioranza dei casi, non è ancora allo stato dell'arte, e manca o è insufficiente per lo più nei piccoli SI; questa gestione è centralmente effettuata, integrata con quella dell'intero SI, solo nel 32,1% dei SI;
- il 67,3% dei SI dell'indagine ha definito un Piano di Disaster Recovery, e di questi solo il 67,6% ha previsto, in diverse modalità, l'allocazione dei relativi ambiti e sistemi ICT alternativi da usarsi in caso di disastro.

I dati forniti dalla Polizia Postale e delle Comunicazioni confermano le crescenti criticità degli attacchi digitali, soprattutto verso le infrastrutture critiche – servizi essenziali e nel cyber crime finanziario; ed evidenziano le difficoltà nel contrastare e reprimere la criminalità informatica.

1.1 Executive Summary

The Digital Attacks Observatory in Italy, OAD, with this 2022 edition reaches the fourteenth year of consecutive investigations into digital attacks in Italy, making use, as in previous years, of 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

of various sizes and belonging to various product sectors, the OAD survey provides an accurate picture of the cyberattacks in Italy. The OAD survey was also chosen from among the projects of the Digital Republic, https://repubblicadigitale.innovazione.gov.it/it/i-progetti/, for its importance in terms of communication, awareness and training on cybersecurity.
OAD 2021 was carried out while the Covid-19 pandemic still persisted, and this 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, two questionnaires were carried out online, the first one "reduced" with about half of the questions compared to the other one "complete". Moreover, as in the previous year, a qualitative macro-assessment of the cybersecurity level of the informatics system object of the answers has been provided at the end of the compilation of both the questionnaires. And a broader and more intense online promotional campaign has been carried out too. But despite all this, the publication of the final report had to be severely delayed in order to reach an acceptable number of compilations.

The OAD 2021 online survey refers to the entire year 2020 and the first half of 2021, a period in which the Covid-19 pandemic was still ongoing, which continued to cause several cyberattacks, given the widespread use of remote working and the strong use of Internet services. Given the extension of the survey until the beginning of 2022, this report also provides information on some important digital attacks of the 2nd half of 2021 and the 1st quarter of 2022, when cyberattacks related to the invasion of Ukraine became more evident.
The emerged pool of respondents covers all product sectors, including Public Administrations, even if more than 1/4 belong to the ICT sector (26.0% of the total). The 2021 pool is 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, with less than 250 employees, and of these 95% are under ten employees. The situation is analogues for the public administrations, where the prevalence is from small organizations. In the OAD 2021 survey, 71.4% of respondents belong to structures with less than 250 employees, and of these 28.6% under 10 employees.
For 2020, cyberattacks on the IT systems of the respondent pool amounted to 59.1% of the total, and for the first half of 2021 to 59.8%. We therefore come close to 60% of cyberattacks, with a significant increase compared to the trend of around 40% detected in previous OAD surveys between 2007 and 2016, and with fluctuating increases between 45-55% from 2017 to 2019.
The correlation of data on detected attacks with the size and turnover of the respondent companies shows the clear trend of increasing digital attacks for large organizations and for those with big turnover. This confirms that small and very small organizations, both private and public, do not represent a specific target for cybercriminals, especially for targeted attacks, while they can be involved in mass attacks, such as those based on phishing and ransomware.
The most widespread type of digital attack (that refers to what is attacked) in the respondent basin, in both the considered periods, was that of access control systems, (IAA, Identification Authentication Authorization), with 30.0% in 2020 and with 28.2% in the first half of 2021.At second place, with 28.2% and 25.9% of diffusion, the attack on the single ICT equipment, and in third place the saturation of resources, with 17.6 % and 17.1% respectively. The other 11 types of attacks follow, decreasing in percentage. As attack techniques, that is, how to attack, all seven families considered by OAD have been widely used in all the attack types of, even simultaneously. The most widespread percentage was the malicious and unauthorized collection of information (social engineering, phishing, etc.) with 76.5%, followed with 62.4% by the use of malware and scripts.
The technical and economic impacts following the most serious attacks are collected for each type of attack, as well as the possible motivations of the attackers and the recovery times following the most serious attacks. All these insights vary for each type of attack, and, overall, it emerges that:

- the technical and functional impacts on the IT systems were declared insignificant for 38.1% of the emerged basin in 2020 and for 32.3% in the first half of 2021; the most serious impacts with

interruption of the IT systems operation of more than three days, involved 15.3% and 13.8% of the IT systems in the two periods considered: high percentages that confirm the danger of the most recent cyberattacks;

- the impact on the budgets of both the IT systems and the entire company, after following the most serious cyberattack, is declared irrelevant for 88.7% in 2020 and for 79.4% in the first half of 2021; the strongest impacts are more on the ICT budget (respectively for 43.3% and for 42.3%), than on the budget of the entire company (respectively for 11.3% and for 2.1%);
- recovery times after the most serious cyberattack are within a single day for about 1/3 of cases, but for 8.8% they are over a month: another indicator of the danger of cyberattacks on the one hand, and of the lack of o insufficient recovery measures, from backups to Disaster Recovery, in some IT systems;
- the reasons for cyberattacks are in the vast majority of cases of an economic nature, therefore for blackmail and frauds with 93.8%: the widespread diffusion of ransomware in Italy is a clear confirmation of this.

For 2/3 of the responded companies, the IT system is essential for the operation and the support of their activities and processes. For this reason, the cybersecurity must be of a high level, as is it results at the end for most the respondents. The regulatory obligations dictated by the GDPR legislation for privacy and by EU NIS Directive for essential services and critical infrastructures, in addition to the attacks suffered for the Covid 19 pandemic, have certainly contributed to strengthening cybersecurity, and a further improvement derives from the growing use of cloud or outsourced services, adopted by 79.8% of the respondents, where the security measures are usually at the top. The macro evaluation of the cybersecurity is provided automatically at the end of the compilation of each of the questionnaires: for 54% of the IT systems it is good, with suitable measures, for 10% it is sufficient, for 13% it is insufficient and for 23% is very critical and it requires strong improvements.
The organizational measures for cybersecurity, historically lacking and neglected compared to the technical ones, have improved overall, comparing them as a trend with those of previous OAD surveys. The role of the CISO, Chief Information Security Officer, is formalized and present in 61.2% of the responding companies s, and only in 54% of the cases it operates within the IT System Organizational Unit, managed by the CIO, Chief Information Officer; in other cases it is in other organizational structures, a further indicator of the good level of digital security in place in the respondent pool, which respect the principle of separation of duties.
Only 20.4% of respondents did not activate policies and organizational procedures for cybersecurity: almost 80% did, but of these 53.4% defined them only for certain areas or functions. 63.2% of respondents defined an ERT, Emergency Response Team, 86.2% carried out the analysis of ICT risks, and 61.4% carried out cybersecurity audits.
OAD 2021 analyzes in some detail, while remaining at general levels, the cybersecurity technical instruments in place in the IT systems of the respondents. In summary, on the technical measures it emerges that:

- it is being consolidated the adoption of cybersecurity architectures integrated with those of the entire IT system, based on world standards and best practices (NIST, ISO, ANSI / TIA 942, etc.); moreover 59.4% of the IT systems with at least one Data Center are at Tier III of the TIA level;
- the basic physical cybersecurity is implemented in most IT systems, even those without a Data Center; some shortcomings, for example for UPS and alarm systems, for very small IT systems;
- for access control (IAA, Identification, Authentication, Authorization), weak authentication is used by 1/3 of the IT systems, even for privileged users, and password management is centralized for 63% of the respondents;
- for 64.5% of the respondents the cybersecurity for the local and geographic networks is centralized and specific tools are used such as DMZ, Firewall, DMZ, IPS / IDS, etc.; only 27% use specific cloud services, such as SASE, to increase the level of this security;

- the protection of software and applications is mainly implemented for the most critical ones; 70.1% developed software ad hoc in an intrinsically secure manner and 79.4% carry out corrective maintenance;
- different and complementary measures for data protection: for 71% of the respondents the data are classified, privacy data are stored encrypted for 31.8% and confidential (non-personal) data are encrypted in 35.5% of the IT systems; an effectively secure backup is performed only by 50% of the IT systems, and the related restore can be performed in 46% of the cases;
- the control, monitoring and management of cybersecurity, in most cases, is not yet at the state of the art: it is lacking or insufficient mostly in the small IT systems; the management is carried out centrally, integrated with that of the entire informatics systems in 32.1% of the cases;
- 67.3% of the respondents has implemented a Disaster Recovery, but of these only 67,6% provided for the allocation of alternative ICT resources to be used in the event of a disaster.

The data provided by the Italian Postal and Communications Police confirm the growing criticality of cyberattacks, especially towards critical infrastructures - essential services and in financial cybercrime; moreover these data highlight the difficulties in tackling and suppressing cybercrime.

2. L'indagine OAD

OAD, Osservatorio Attacchi Digitali in Italia, è l'unica indagine indipendente online 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 2021 fa riferimento agli attacchi digitali intenzionali rilevati nel corso dell'intero 2020 ed al 1° semestre 2021, con alcuni aggiornamenti sui principali attacchi aggiornati ad aprile 2022, e si raccorda cronologicamente ai precedenti Rapporti che coprono un arco temporale di quindici anni consecutivi, dal 2007 al 2021 (per il 1° semestre nell'indagine online). 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.
La fig. 2-1 mostra le copertine dei Rapporti finali precedentemente pubblicati.
Tutti i 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 OAD 2021 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, e con la Polizia Postale e delle Telecomunicazioni, che ha fornito i dati riportati e commentati nel Capitolo 9.
L'indagine OAD 2021 è stata sponsorizzata dalle aziende Ireth, Qintesi 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 2021 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 finale, contribuendo in tal modo anche alla diffusione della cultura sulla sicurezza digitale.

1 ICT, Information and Communication Technology.

Fig. 2-1

Come per le edizioni precedenti, OAD 2021 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 finale, contribuendo in tal modo anche alla diffusione della cultura sulla sicurezza digitale.

Il Rapporto OAD 2021 si basa sull'elaborazione e l'analisi delle risposte ottenute dai due questionari, uno "completo" con 206 domande raccolte in 14 gruppi, e l'altro "ridotto" con 126 domande raccolte negli stessi 14 gruppi, entrambi posti online e resi liberamente disponibili su Internet da agosto 2021 a marzo 2022: l'arco temporale così lungo, e la conseguente pubblicazione del rapporto finale a fine aprile 2022 è dovuta alla forte difficoltà riscontrata nell'ottenere la compilazione completa di uno dei due questionari, seppur entrambi rigorosamente anonimi, e nonostante i numerosi inviti alla compilazione effettuati via email, promozione sui siti web, sui social e durante i webinar, fino a dirette chiamate telefoniche.

Essendo totalmente libero l'accesso ai questionari online su 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 ed interessanti indicazioni sul fenomeno degli attacchi digitali in Italia, difficilmente riscontrabili in altre indagine nazionali ed internazionali. Aspetto fondamentale dell'indagine è anche l'individuazione di quali sono gli strumenti di prevenzione, protezione e ripristino, tecnici ed organizzativi in uso nei sistemi informativi delle aziende/enti rispondenti, e come reagiscono in caso di attacco.

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.

2.1 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 informativi 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 ENISA a livello europeo e 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 aziende/enti, che in Italia sono la stragrande maggioranza.
Altre indagini a livello italiano o fanno riferimento solo a grandi organizzazioni o a un limitato numero di aziende per determinati settori merceologici, o elaborano dati forniti da aziende sugli attacchi avuti dai loro clienti. OAD ha intrapreso un diverso, anche se assai difficile, approccio: far compilare un questionario, o quello completo o quello ridotto nell'indagine 2021, al più ampio possibile numero di aziende ed enti, in modalità rigorosamente anonima, informati e sollecitati più volte attraverso diversi canali di comunicazione, anche attraverso le associazioni patrocinanti ed i media partner.
Per cercare di motivare i potenziali rispondenti, alla fine della compilazione di entrambi i questionari online viene mostrata una macro valutazione del livello di sicurezza digitale del sistema informativo (SI) oggetto delle risposte fornite (approfondimenti nell'Allegato A), oltre alla possibilità di scaricare due numeri prescelti dell'autorevole ISSA Journal, la rivista mensile riservata ai soci di AIPSI-ISSA.
Le difficoltà così forti riscontrate in questa ultima edizione nell'ottenere delle compilazioni ha costretto AIPSI e l'autore a ripensare totalmente la logica e le dimensioni dei questionari ma non l'approccio, che non considera un bacino predefinito di rispondenti, bensì cerca di far compilare un questionario, nelle future edizioni ulteriormente ridotto, al maggior numero possibile di aziende ed enti di ogni dimensione e settore merceologico.

3. Il quadro generale degli attacchi digitali intenzionali e della realtà italiana

3.1 Gli attacchi digitali nel periodo a livello mondiale

L'arco temporale di riferimento di OAD 2021 include l'intero anno 2020 ed il primo semestre 2021, durante il quale l'elemento dominante e caratterizzante gli aspetti di sicurezza digitale è stata la **pandemia Covid 19**. Fenomeno mondiale che è stato di forte impatto in Italia, soprattutto per l'enorme numero di piccole e piccolissime organizzazioni, sia private che pubbliche, come approfondito nel seguito al §3.6.1.
Il Covid ha spinto repentinamente anche in Italia alla diffusione del lavoro da remoto (chiamato anche smart working, agile working, ecc.) in tutte le organizzazioni, con collegamenti fissi o mobili via Internet. Questo ha enormemente ampliato l'area di vulnerabilità, dato anche il numero di aziende/enti di piccole dimensioni e i loro relativamente bassi livelli di sicurezza digitale, in media, in particolare:

- collegamenti non protetti tra i dispositivi d'utente e le applicazioni sui server, fisici o virtualizzati, on premise o terziarizzati/in cloud;
- aumento 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
- l'argomento Covid è divenuto la principale esca negli attacchi di phishing ed è un amplificatore di vari tipi di attacchi digitali.

Nel corso della pandemia, ancora in azione, è aumentato significativamente l'attacco ai sistemi informativi di ospedali e di strutture sanitarie, e in particolare ai centri di ricerca che si occupano di contrastare questa epidemia. In nome del Covid si sono inoltre diffusi vari siti web maligni, e sempre a causa della paura e dello stress anche professionale dovuto al Covid, sono avvenuti moltissimi incidenti nella gestione operativa dei sistemi ICT non intenzionali (i cosiddetti "non-malicious incidents"): estrema urgenza e fretta negli interventi, specialisti ammalati sostituiti da personale non sufficientemente preparato, difficoltà di cooperare efficacemente da remoto, e così via.
A fianco del fenomeno Covid 19 e dei suoi impatti, il periodo considerato è stato inoltre caratterizzato dal consolidamento ed ampliamento di attacchi digitali già conosciuti, e dal sorgere di nuovi attacchi: nel complesso tutti sempre più sofisticati e difficili da individuare e da contrastare, capaci di causare impatti significativi sul sistema informativo attaccato.
Si deve inoltre considerare che è bene classificare gli attacchi digitali per il target cui sono destinati, indipendentemente da che cosa si attacca e da come:

- gli attacchi "**mirati**", chiamati sovente anche in italiano "targeted": sono indirizzati specificamente ad un singolo, o ad un gruppo, di aziende/enti; il più delle volte sono attacchi sofisticati, sovente basati su logiche APT, e per i quali gli attaccanti hanno precisi obiettivi da perseguire e in molti casi ben conoscono la realtà informatica dl bersaglio;
- gli attacchi "**massivi**", portati ad un grande numero di potenziali bersagli e in molti casi non particolarmente sofisticati, nell'ipotesi che si possa far breccia nelle limitate misure di sicurezza di qualcuno; l'inoltro massivo di phishing che portano in allegato un ransomware è un esempio di questo tipo d'attacco che in Italia, per il grandissimo numero di piccole e piccolissime organizzazioni (si veda3.5.1), è fiorente per quelle con più limitate misure e scarsa attenzione alla sicurezza digitale.

Tra le novità e le evoluzioni degli attacchi digitali nel periodo considerato è bene evidenziare:

- la crescita degli attacchi "massivi", ed in tale ambito in Italia molto diffusi gli attacchi **ransomware**;
    - gli attacchi ransomware hanno in molti casi costituito una duplice o una multipla fonte di ricatto: nel caso della duplice, chiamata **double extortion,** la vittima non solo è costretta a pagare "subito" il riscatto per la decifratura dei suoi dati e la ripresa del funzionamento del

suo sistema informativo, ma è anche costretto a pagare un ulteriore riscatto per impedire che i suoi dati, il più delle volte di persone, di progetti, di accordi e di relativi contratti, vengano messi online, e magari in vendita, sul dark web. Nel caso di ricatto multiplo, chiamato **multiple extortion**, vengono ricattati anche persone ed aziende i cui dati sono stati estratti dagli archivi compromessi con l'attacco target iniziale;

- molti diffusi gli attacchi di **phishing** e di **spear phishing**, questi ultimi di difficile individuazione da parte dell'utente oggetto dell'attacco, in quanti riprendono assai fedelmente ambiti digitali noti ed usati dall'utente (la sua banca, siti web normalmente utilizzati, etc.). Gli allegati sovente contengono malware e link a siti web malevoli;
- crescita e sofisticazione degli attacchi alla posta elettronica aziendale, la cosiddetta "**Business Email Compromise**": la posta elettronica è il mezzo fondamentale non solo per scambio di informazioni, ma per ogni attività di business, dall'informativa ai clienti alle comunicazioni mirate, dall'emissione di offerte ed ordini alla loro accettazione, dall'emissione delle fatture alle conferme dei pagamenti, e così via. In base a quanto scambiato con la posta elettronica vengono prese decisioni e si attua buona parte del business per qualsiasi settore merceologico e per aziende/enti di qualsiasi dimensione. La compromissione di un messaggio di posta elettronica può essere l'elemento inziale di una frode, di un sabotaggio, di un attacco digitale;
- attacchi digitali all'azienda/ente target partendo dai fornitori tramite la "suppy chain" informatica che consente l'interoperabilità tra i loro sistemi informativi (**supply-chain attack**);
- evoluzione degli attacchi **Dos/DDoS**, sovente combinati con attacchi web based, che si rivolgono anche agli ambienti virtualizzati, ampliando e amplificando così fortemente il loro campo d'azione: si possono colpire più aziende/enti che fanno parte del cluster, tipicamente in ambienti cloud;
- crescente utilizzo di strumenti di **machine learning** (ML) e più in generale di **intelligenza artificiale** (AI, Artificial Intelligence) per individuare vulnerabilità e realizzare attacchi; ML ed AI, come tnti altri strumneti in ambito sicurezza digitale, possono servire sia come mezzi di difesa sia come mezzi di attacco;
- ulteriore sofisticazione degli attacchi **APT, Advanced Persistent Threat**, tra i più complessi e pericolosi, in grado di studiare e sfruttare in maniera multipla e contemporanea le vulnerabilità presenti in un sistema ICT, e ora tra i primi ad utilizzare tecniche avanzate come quelle di ML e IA;
- diffusione di **cryptojacking** (chiamata anche hidden cryptomining) al crescere dell'uso di criptovalute. Con tecniche di hijacking vengono illegalmente estratte (mining) ed usate criptovalute dai computer di ignari possessori delle stesse. Consiste in una frode finanziaria con le criptovalute, realizzata e realizzabile tramite tecniche di hijacking e con l'uso di malware;
- crescente diffusione di **cyberattack as a service** e di hacker "a pagamento", indicati come "**hacker for hire**". Da un lato si diffondono Ransomware as a Service, DoS as a Service, Phishing as a Service, etc non solo nel darkweb. Molti degli hacker for hire fanno parte di ben noti gruppi che hanno un nome che li contraddistingue, altri sono degli esperti che si offrono come freelance.

A fianco degli attacchi "massivi" e "specifici", un grave rischio per i sistemi informativi è data dalla **disinformazione** e talvolta anche dalla **mala-informazione** (fake news) sulle loro funzionalità e sulla loro sicurezza da parte sia degli utenti, finali e privilegiati, sia dei decisori che si occupano di tali sistemi informativi, in termini di budget, di acquisti, di nuovi progetti e sviluppi, e così via. Significativi in tal senso i dati dell'ultima indagine europea DESI considerati in §3.2.2.

3.1.1 I principali attacchi a livello mondiale nel 2020 e nel 1° semestre 2021

Numerosi gli attacchi digitali significativi nel periodo considerato, i principali[2] dei quali sono elencati suddividendoli tra quelli mondiali e quelli occorsi specificatamente in Italia. Molti gli attacchi rilevati contro enti e siti web dell'Ucraina, la maggior parte dei quali facenti parte della cyber warfare condotta dalla Russia, e sempre in logica cyber warfare quelli condotti ai paesi occidentali da hacker legati alla Corea del Nord, da quelli legati alla Cina e da quelli dell'Iran verso paesi occidentali.

Tra gli attacchi digitali a livello mondiale, e che quindi possono aver coinvolto in taluni casi anche sistemi informativi italiani, l'autore ha scelto alcuni dei più significativi mese per mese:

- Giugno 2021: attacco all'accesso da remoto a reti di molte agenzie governative statunitensi, incluse Verizon e il Metropolitan Water District californiano.
- Maggio 2021: attacco ransomware con REvil alla brasiliana JSB, la più grande azienda di lavorazione carne al mondo, con blocco di suoi stabilimenti in US, Canada, Australia.
- Maggio 2021: attacco all'intero sistema sanitario nazionale irlandese HSE (Health Service Executive), utilizzando il Conti Ransomware-as-a-Service (RaaS);
- Maggio 2021: attacco ransomware alla statunitense Colonial Pipeline, la più grande conduttura di petrolio negli US. La compagnia ha pagato un riscatto di 5 milioni US $.
- Aprile 2021: attacco ai sistemi di prenotazione di più di 20 aerolinee low cost a livello mondiale.
- Aprile 2021: attacco tramite un VPN vulnerabile a fornitori europei e statunitensi della difesa US.
- Marzo 2021: scoperta di attacchi all'EMA, European Medicines Agency, probabilmente effettuati fin dal 2020, con furto di documenti relativi al Covid 19.
- Febbraio 2021: attacco con malware ad un sistema di file sharing del governo ucraino.
- Febbraio 2021: attacco DDoS di più giorni al sito web del Security Service ucraino.
- Gennaio 2021: attacco per l'accesso a fornitori di servizi di telecomunicazioni e hosting, con furto di informazioni, in numerosi paesi mediorientali, US e UK.
- Gennaio 2021: attacco ransomware a cinque paesi noti per il gioco d'azzardo, con la richiesta di più di 100 milioni di riscatto.
- Dicembre 2020: attacco via supply chain alla piattaforma Orion di Solarwinds, sfruttando una vulnerabilità su un processo di gestione e monitoraggio delle reti e consentendo l'esfiltrazione di una notevole quantità di dati.
- Novembre 2020: attacco con phishing ed allegati malware ad AstraZeneca.
- Novembre 2020: attacco con furto di credenziali ed uso di back door ad un target di aziende/enti del Sud Asia.
- Ottobre 2020: sofisticato attacco al sito web e alla rete dell'IMO, International Maritime Organization, facente parte dell'ONU.
- Aprile 2021: attacco a Facebook.
- Aprile 2021: attacco a LinkedIn.
- Settembre 2020: grave attacco ransomware alla statunitense Universal Health Systems, con forti impatti sui backup, sulle destinazioni delle ambulanze e sulla schedulazione degli interventi operatori;
- Agosto 2020: pesante attacco DDoS alla borsa della Nuova Zelanda, che ha causato parecchi giorni di blocco;
- Luglio 2020: attacco alla rete del Vaticano per accedere alle informazioni e alle agende dei vescovi cinesi.
- Giugno 2020: attacchi DDoS a banche ed enti indiani nell'ambitio della disputa tra India e Cina per la valle Galwan.
- Maggio 2020: attacco sofisticato e "targeted" a numerose ed importanti aziende fornitrici di hardware e software in Giappone, Germania, Italia e UK.

[2] La scelta degli attacchi digitali riportati è dell'autore, e non ha alcuna pretesa di essere esaustiva.

- Maggio 2020: attacco al sistema di prenotazione e rilascio biglietti aerei dell'inglese EasyJet, con il coinvolgimento di più di 9 milioni di clienti in tutti il mondo.
- Aprile 2020: attacco ad agenzie governative e missioni diplomatiche cinesi grazie ad una vulnerabilità zero-day delle loro VPN.
- Aprile 2020: attacco con riferimento al Covid 19 all' U.S. Department of Health and Human services e a numerose case farmaceutiche ed ambienti sanitari.
- Marzo 2020: esteso cyber spionaggio a più di 75 importanti organizzazioni mondiali nel campo della sanità, dei media, del manifatturiero, del no profit.
- Febbraio 2020: attacco con data breach alla U.S. Defense Information Systems Agency con grave furto di informazioni individuali.
- Gennaio 2020: esteso e duraturo attacco alla Mitsubishi che ha coinvolto più di 8000 persone e numerose aziende fornitrici e clienti.
- Gennaio 2020: attacco al ministero degli esteri austriaco.

3.1.2 Cyber warfare e gli eventi recenti relativi all'invasione dell'Ucraina

Come anticipato nell'introduzione, mentre si elaboravano i dati faticosamente raccolti coi due questionari OAD e si iniziava la stesura del presenta rapporto, è iniziata l'invasione dell'Ucraina da parte della Russia.
E' difficile, nella maggior parte dei casi, individuare e classificare un attacco digitale come parte di una guerra informatica. In primo luogo perché chi attacca normalmente non si palesa, anzi cerca di mascherare il suo attacco, affiancandolo spesso con varie "fake news" fuorvianti. Gli indizi per poter individuare e classificare una attacco digitale come parte di una cyber warfare includono la sofisticazione dell'attacco stesso, che richiede risorse ICT ed economiche di cui un "normale" hacker ben difficilmente potrebbe disporre, il target dell'attacco ed il momento e contesto in cui viene portato. La cyber warfare è definita dalla Enciclopedia Treccani[3] come "Uso di computer e di reti, come Internet, per attaccare o difendersi nel cyberspazio", molto simile alla definizione data da Wikipedia[4]: "'insieme delle attività di preparazione e conduzione di operazioni di contrasto nello spazio cibernetico". Entrambe introducono il concetto di "cyberspazio": dopo terra, mare, cielo e spazio, esso costituisce una nuova area strategica e geopolitica, nella quale si confrontano e si contendono non solo nazioni ma anche gruppi terroristici. Il target principale sono le infrastrutture critiche.
Negli anni scorsi si erano avuti attacchi digitali inquadrabili in guerre cibernetiche, soprattutto tra Stati Uniti, Corea del Nord, Iran, Russia. L'attacco a livello mondiale ai sistemi di posta elettronica Exchange Microsoft è considerato un tipico esempio di cyber warfare da parte della Cina ai paesi occidentali, ed in particolare agli Stati Uniti.
L'invasione dell'Ucraina in ambito cyber era iniziata già sul finire del 2021 con specifici attacchi digitali, inquadrabili in una guerra cibernetica, e che tuttora è in corso a fianco di quella sul campo. Gli attori coinvolti sono da una parte gli attaccanti, strutture cyber governative russe, bielorusse e gruppi di hacker e di cybercriminali ad essi collegati, che includono il Gruppo Conti e il Gruppo Sandworm, ben noti per la creazione di diffusi ransomware, oltre alle strutture dei servizi segreti quali Gru, in ambito militare, Svr, e Fsb, ex KGB. Dall'altra parte operano strutture ucraine piuttosto deboli, affiancate da gruppi di hacker internazionali, tra i quali Anonymous, GhostSecurity, Cyber Partisans, e molto probabilmente con il supporto di strutture governative cyber di paesi occidentali che non vogliono essere individuate.
La guerra in atto ha portato ad una forte "cyber escalation", che può facilmente e velocemente estendersi a vari paesi occidentali, tra cui l'Italia, che hanno preso una precisa posizione contro Putin e la sua invasione: tutti gli enti cyber statali occidentali hanno diramato precisi e severi allarmi ed inviti a potenziare le misure di sicurezza cibernetica in essere. Dal punto di vista tecnico, oltre ai vari "tradizionali" attacchi digitali portati dalla Russia, in particolare numerosi DoS/DDoS, di particolare interesse i nuovi malware distruttivi chiamati

[3] https://www.treccani.it/enciclopedia/cyberwar_%28Enciclopedia-della-Scienza-e-della-Tecnica%29/
[4] https://it.wikipedia.org/wiki/Guerra_cibernetica#:~:text=Una%20guerra%20cibernetica%20(nell'arte,di%20contrasto%20nello%20spazio%20cibernetico.&text=Tale%20guerra%20si%20caratterizza%20per,e%20dei%20sistemi%20di%20telecomunicazione

wiper. Wiper in inglese significa tergicristallo, e il verbo wipe, più in generale, significa "pulire": questo tipo di malware manipola e/o cancella il driver di un hard disk, eliminando tutti i dati archiviati e non consentendo più il suo utilizzo. Tra i primi wiper realizzati in ambito e pro Federazione Russa in questa guerra cyber ci sono l'HermeticWiper, chiamato anche FoxBlade, e il WhisperGate, chiamato anche WhisperKill.
Il primo wiper manipola il MBR, Master Boot Record, in ambito Windows ed è riconoscibile come Win32/KillDisk.NCV. Sfrutta le vulnerabilità di Microsoft SQL Server (CVE-2021-1636), utilizzando (almeno negli attacchi ai sistemi ucraini) i driver di EaseUS Partition Master, software per la creazione/gestione di partizionamento ed il ridimensionamento del disco rigido (hard disk). Cancellando il MBR, non è poi possibile effettuare l'operazione di avvio (accensione, boot) del sistema operativo Windows sui dispositivi infettati.
Il secondo, WhisperGate, è un malware distruttivo molto sofisticato, studiato per i sistemi Windows, in grado di autoproteggersi e che si camuffa da ransomware. WhisperGate sfrutta l'ambiente di sviluppo Minimalist GNU for Windows (MinGW) che supporta il compilatore GNU Compiler Collection (GCC) 6.3.0 negli ambiti Windows. Opera in tre fasi: con questi strumenti viene sovrascritto l'MBR originale, poi, alla riaccensione del sistema, esso parte dal falso MBR e da un lato chiede all'utente un riscatto di $ 10.000,00 in Bitcoin, fingendosi un ransomware, e dall'altro riscrive le sezioni di ogni driver. Nella seconda fase scarica dei file per non farsi riconoscere come malware e per bloccare Windows Defender e altri software di difesa presenti sul sistema. Nella terza fase acquisisce i diritti di amministratore di sistema. Individuati i driver logici del sistema, considera tutte le possibili estensioni dei file (.bat , .docx, .exe, .pptx, .zip, etc.) e scrive per ciascuno di essi il primo milione di Byte con 0xCC byte distruggendo tutti i loro contenuti. Alla fine il malware si auto cancella dal sistema.

3.2 Le vulnerabilità causa degli attacchi

Tutte le minacce cibernetiche, intenzionali e non, si basano su vulnerabilità che possono essere categorizzate in tecniche, delle persone e 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.

3.2.1 Le vulnerabilità tecniche

A livello tecnico esistono qualificati ed aggiornati siti che elencano, classificandole, le vulnerabilità riscontrate, quali ad esempio CVE/MITRE e la statunitense NVD, National Vulnerability Database, che fa riferimento alla numerazione CVE. Per ciascuna vulnerabilità questi siti riportano, se presenti, le modalità per eliminarle o ridurle. Ogni prodotto/servizio ICT, di qualsiasi produttore, ha delle vulnerabilità tecniche individuate. Al momento della stesura finale del presente rapporto, la banca dati CVE/MITRE ha un insieme di record di vulnerabilità accertate pari a 173.884.
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, è bene evidenziare che:

- 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.

L'Allegato E.2 fornisce un elenco, non esaustivo, delle principali fonti internazionali che forniscono aggiornati dati ed elenchi delle vulnerabilità tecniche ICT, ivi incluse CVE/MITRE e NVD.

3.2.2 Le vulnerabilità delle persone

Le vulnerabilità delle persone rappresentano per il mondo digitale rischi ancora più diffusi e gravi rispetto a quelle tecniche: e sono amplificate dalle vulnerabilità organizzative di cui in §3.2.3
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 di "competenze umane " di DESI 2021 mostrato in fig. 3.2.2-1.

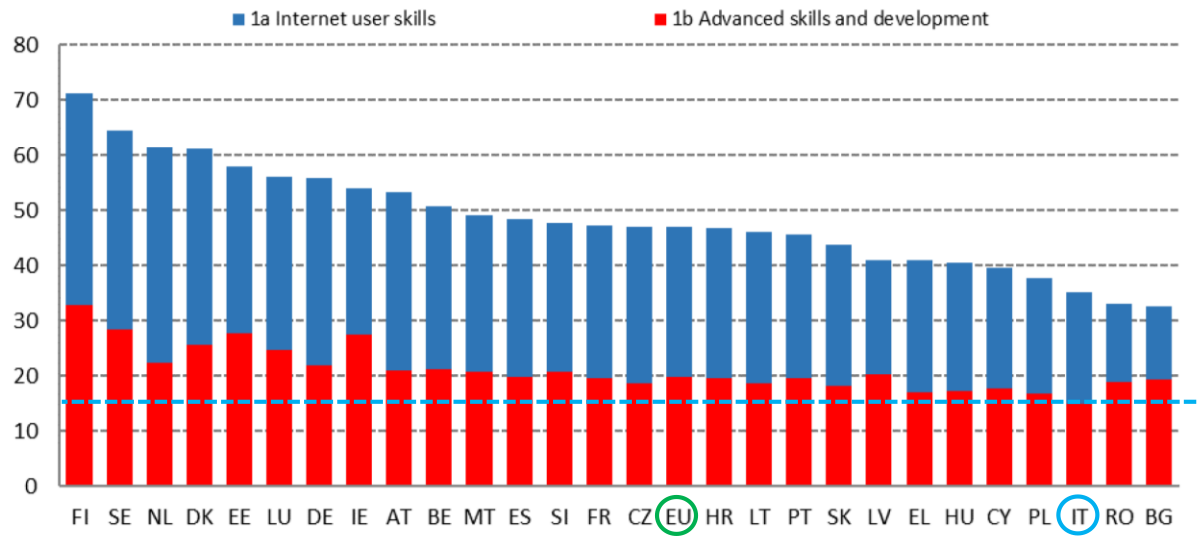

Fig. 3.2.2-1 (Fonte: DESI – Commissione Europea)

La linea tratteggiata nella figura evidenzia chiaramente come l'Italia sia ancora all'ultimo posto, tra tutti i paesi europei, nelle competenze più avanzate riguardanti il mondo digitale, sia lato utenti sia lato specialisti ICT: 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 singole 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. 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.
La fig. 3.2.2-2 fornisce il quadro generale di confronto tra tutti i paesi europei dell'intero indice DESI, che fornisce il livello di digitalizzazione dell'economia e della società. Esso è costituito dal 2021 da 4 indicatori

(rispetto ai 5 degli anni precedenti, per meglio allinearlo con gli obiettivi europei di digitalizzazione al 2023 stabiliti nel Digital Compass[5]) che valutano:

- il capitale umano: capacità di accedere ed usare Internet, e le competenze specialistiche in ambito digitale, che comprendono le capacità di sviluppo di programmi software ed anche quelle relative alla sicurezza digitale;
- la connettività: è misurata da Fixed broadband take-up, fixed broadband coverage, mobile broadband and broadband prices
- l'integrazione delle tecnologie digitali: la digitalizzazione del business e l'e-commerce;
- i servizi pubblici digitali: e-Government[6].

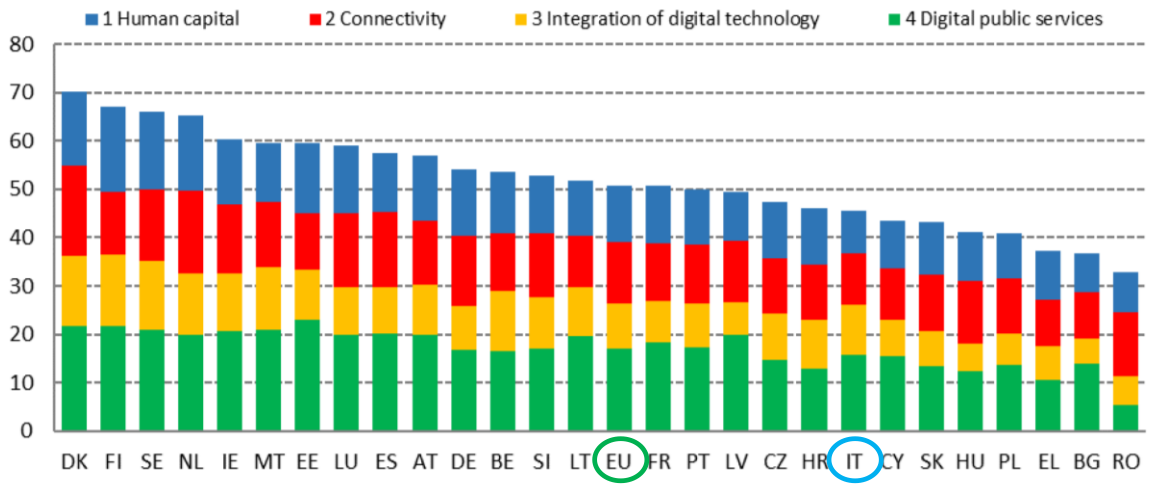

Fig. 3.2.2-2 (Fonte: DESI – Commissione Europea)

L'Italia si trova agli ultimi posti di questa classifica europea basata sull'indice DESI, anche se nel 2021 il suo posizionamento è leggermente migliorato di qualche posizione rispetto agli anni precedenti. La fig. 3.2.2-3 fornisce un chiaro posizionamento dell'Italia in termini di crescita e di miglioramento nel mondo digitale: si è vicini alla media europea, ma ben lontani dai paesi europei più avanzati nel mondo digitale. Come già sottolineato, questo grave "minus" si fa già sentire, e si farà sempre più sentire nel prossimo futuro, sulla competitività

[5] COM (2021) 118 final: si veda https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX:52021DC0118

[6] "e-Government" ha il generale significato di "uso dell'ICT nei processi amministrativi che le PA svolgono per migliorare ed innovare i servizi forniti ai cittadini". L'OCSE in particolare lo definisce come "l'uso delle nuove tecnologie dell'informazione e della comunicazione (ICT) da parte delle pubbliche amministrazioni applicato ad un vasto campo di funzioni amministrative. In particolare, il potenziale networking offerto da internet e dalle sue tecnologie ha il potenziale di trasformare le strutture e le procedure amministrative" e la Commissione Europea come "usare le nuove tecnologie per aumentare la partecipazione al processo democratico".

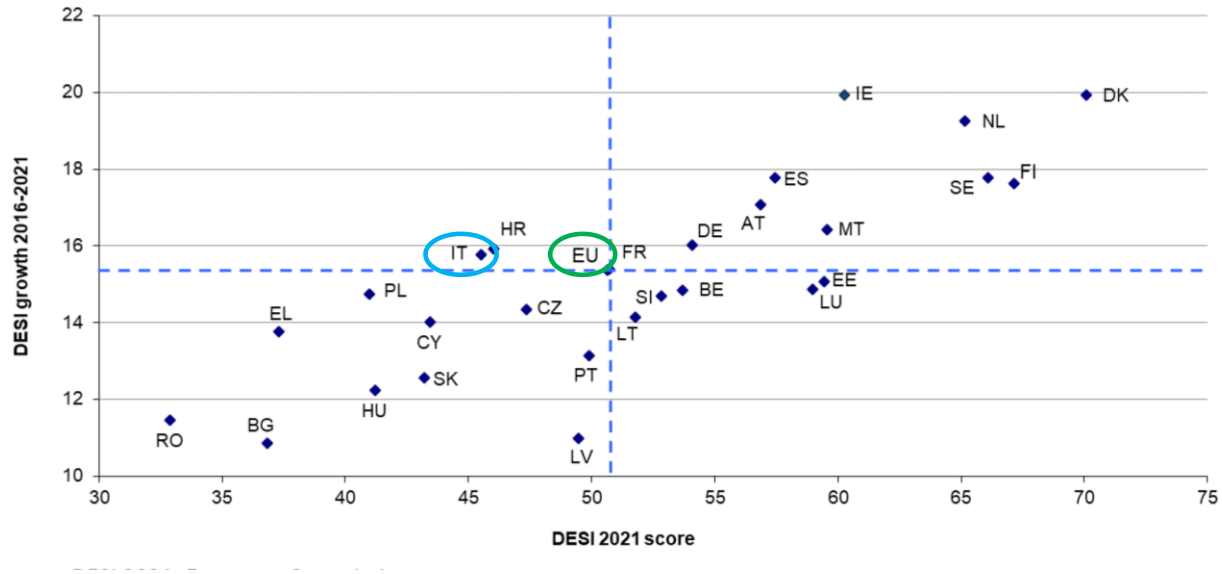

Fig. 3.2.2-3 (Fonte: DESI – Commissione Europea)

3.2.3 Le vulnerabilità organizzative e delle strutture predisposte alla sicurezza digitale

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 e dagli altri fornitori esterni, in primis i consulenti, 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.

In termini di figure e ruoli preposti alla sicurezza digitale, in Italia solo alcune organizzazioni medio grandi hanno la figura del responsabile della sicurezza digitale formalizzata ed operativa, indicata prevalentemente con l'acronimo **CISO**, Chief Information Security Officer: nella maggior parte dei casi questo responsabile opera nell'ambito della struttura dei sistemi informativi, indicata con l'acronimo UOSI , Unità Organizzativa Sistemi Informativi, alle dipendenze del suo responsabile, il **CIO**, Chief Information Officer, ma l'orientamento è ora di porre il CISO nell'ambito di altre strutture, non in UOSI, per cercare di garantire una corretta separazione delle responsabilità. Se fosse in UOSI, come potrebbe il CISO realmente controllare, anche solo per la sicurezza digitale, la struttura da cui dipende?

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.

Le misure di sicurezza, tecniche ed organizzative, attuate dalla maggior parte delle imprese pubbliche e private, potenziali target di attacchi, hanno limitato gli attaccanti a specifiche organizzazioni in grado di portare attacchi così sofisticati da superare le misure in essere.

3.3 Gli attaccanti e le loro motivazioni

Nel tempo la tipologia degli attaccanti si è profondamente evoluta: dai singoli che per verificare le proprie capacità e talvolta per dimostrare che un determinato codice software non era sicuro, gli attuali ethical hacker, o che si volevano vendicare di un presunto torto subito, o perorare una propria ideologia, a gruppi di specialisti con ampie risorse tecniche e finanziarie che operano a livello mondiale con fini criminali o per governi nell'ambito e nell'ottica di guerre informatiche. Il cybercrime è ormai un business ad alto rendimento, data anche la difficoltà di contrastarlo, nonostante le varie leggi e normative in atto a livello italiano ed europeo. Alcuni malware si trovano facilmente in Internet, e sta emergendo un mercato di "Cyber Attack as a Service" e di specialisti che si offrono, a pagamento, per condurre attacchi digitali.
ENISA, nel suo ultimo rapporto "Threat landscape 2021"[7], considera le seguenti categorie di attori che minacciano la sicurezza digitale:

- attori sponsorizzati da stati
- cyber criminali
- hacker a noleggio (for-hire actors)
- hacktivist.

Chi effettua un attacco digitale lo fa per precise sue motivazioni, che posso variare di caso in caso. Il singolo specialista che opera in uno di questi gruppi può operare anche per altri. E rimane, anche se sempre più in minoranza, la singola persona che effettua un attacco per vendicarsi di torti subiti, o il giovane, anche poco esperto ma con parecchio tempo libero a disposizione, che prova in maniera casuale e quasi massiva ad attaccare persone, enti ed aziende per vedere cosa può ottenere.
Nei questionari OAD 2021 a fronte di ogni tipologia di attacco rilevata, venivano chieste le possibili e probabili motivazioni e chi poteva essere l'attore. Il risultato, riportato nella fig. 4-14 del §4, evidenza che la principale e più diffusa motivazione è la ritorsione economica, che rientra nelle frodi. La fig. 4-13 mostra, come risultato complessivo dell'indagine OAD 2021, che l'attore percentualmente più diffuso dell'attacco digitale è un'organizzazione esterna all'azienda/ente rispondente.
Nel periodo di riferimento OAD 2021, intero anno 2020 e 1° semestre 2021, gli attacchi digitali hanno avuto come punto focale l'epidemia Covid 19 ed hanno pertanto riguardato ospedali, strutture sanitarie, studi medici, aziende farmaceutiche, centri di ricerca immunologici, per catturare informazioni personali e sui vaccini, per spionaggio industriale, oltre che per fare da esca per attacchi massivi con phishing sull'argomento e relativi malware e ransomware.
Sul finire del 2021 ed all'inizio del 2022 si è poi rilevato un incremento di attacchi digitali ad enti ed istituzioni ucraine e di altri paesi occidentali, che erano il preludio dell'invasione armata dell' Ucraina e che costituivano una cyber warfare, effettuati direttamente dai servizi segreti della Federazione Russa, quali probabilmente Gru e Fsb (ex KGB) [8], e gruppi da questi ultimi pilotati come il gruppo Conti, ben noto per i vari ransomware creati e diffusi con alti guadagni sui relativi ricatti ed il gruppo Sandworm pilotato da Gru.
Difficile poter individuare i vari gruppi di cyber criminali, dato che i più ben si camuffano e si nascondono, ma alcuni si palesano e addirittura si fanno pubblicità su loro siti web. Tra i più noti gruppi di hacker, oltre al già citato gruppo Conti e Sandworm, Anonymous, che si è schierato contro la Federazione Russa dopo l'invasione dell'Ucraina, Cult of the Dead Cow, storicamente uno dei primi gruppi US, Chaos Computer Club, ritenuto il più grande gruppo europeo di ethical hacker, Dark Side tra i primi ad offrire servizi RaaS, Ransomware as a Service, Equation Group operante per la statunitense NSA (National Security Agency), Fancy Bear pilotato dal governo russo e probabilmente anch'esso coinvolto in vari attacchi contro paesi e personaggi occidentali oltre che contro l'Ucraina, Lazarus guidato dalla Nord Corea insieme a Bureau 121 creatore di Wannacry, Machete operativo prevalentemente nei paesi sudamericani, PLA Unit 61398 guidato dalla Cina ed autore di numerosi attacchi ad enti ed imprese US, Shadow Brokers probabili co-autori di Stuxnet e diffusori di

[7] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021
[8] Per approfondimenti si veda l'articolo dell'autore: https://www.agendadigitale.eu/sicurezza/ucraina-come-agisce-la-guerra-cyber-e-quali-impatti-sulleuropa/

Wannacry e NotPetya, Unit 8200 alle dipendenze del governo israeliano e probabilmente coinvolto nella creazione di Stuxnet. Per un più ampio elenco, non esaustivo, di gruppi cyber, governativi, criminali o altro, si veda: https://en.wikipedia.org/wiki/List_of_hacker_groups.
Per un elenco dei più noti criminali informatici si veda: https://en.wikipedia.org/wiki/List_of_computer_criminals.

3.4 Le contromisure per la sicurezza digitale 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 l'adozione crescente di soluzioni e piattaforme quali SIEM, SOAR, SESA, etc.;
- adozione di tecniche di autenticazione "forte" degli utenti , anche con identificazione biometrica e relative logiche "passwordless";
- realizzazione e crescente adozione di misure di sicurezza digitale "as a service";
- crescente terziarizzazione della sicurezza digitale, soprattutto a livello della gestione operativa;
- tendenza alla realizzazione di soluzioni di sicurezza digitale intrinseca (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 dei cyber criminali (si veda §8);
- una maggiore collaborazione internazionale per la repressione del crimine informatico, sia a livello legislativo sia a livello forze di Polizia;
- migliorare e promuovere 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 soluzioni e sistemi ICT obsoleti o non utili al cliente, approfittando della sua non competenza in merito.

Facendo riferimento alla presente indagine, i paragrafi del successivo §7 forniscono una fotografia delle misure in essere, tecniche ed organizzative, dei SI delle Aziende/Enti rispondenti.
Come negli anni precedenti, anche nell'edizione 2021 il bacino emerso di aziende/enti rispondenti si colloca in una fascia medio-alta per il livello complessivo di sicurezza digitale dei loro SI: 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 per la loro sicurezza digitale.
Per quanto indicato all'inizio di questo capitolo, tutto (o quasi tutto) è digitale e in tempo reale: e far fronte al fattore tempo, oltre alla massa di software interoperante e di dati, richiede una ampia ed efficace automazione della gestione della sicurezza digitale.

3.4.1 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 complessi e 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, ma la maggior parte, ed in particolare le strutture di medie e piccole dimensioni, terziarizzano in tutto o in parte la gestione della sicurezza digitale a MSSP.
Per ulteriori approfondimenti sull'argomento si rimanda all'articolo dell'autore "CyberSecurity as a Service e Managed Security Services: quali vantaggi per Pmi e PA", si veda https://www.aipsi.org/breaking-news/820-articolo-su-cybersecurity-as-a-service-e-managed-security-services-quali-vantaggi-per-pmi-e-pa-su-agenda-digitale.html

3.5 Il quadro di riferimento Italiano

3.5.1 Aziende e PA in Italia

Facendo riferimento ai più recenti dati ISTAT sulle imprese attive in Italia, che fanno riferimento al 2019, la situazione per numero di dipendenti è sintetizzata nella fig. 3.5-1.

CLASSE DI DIPENDENTI	Imprese per numero dipendenti	%
Senza dipendenti	2.755.872	**64,03%**
Con dipendenti	1.548.283	**35,97%**
di cui:		
1	*644.312*	**14,97%**
2-5	*571.714*	**13,28%**
6-9	*146.355*	**3,40%**
10-19	*108.633*	**2,52%**
20-49	*50.270*	**1,17%**
50-99	*14.635*	**0,34%**
100-249	*8.165*	**0,19%**
250 e più	*4.199*	**0,10%**
Totale	**4.304.155**	100,00%

Fig. 3.5-1 (ISTAT)

La figura evidenzia come solo il 0,10% sul totale è di aziende di medie-grandi dimensioni, con 250 o più dipendenti, che il 64,03% non ha alcun dipendente, e che il 35,87% è di PMI: tra queste quelle che hanno da 1 a 9 dipendenti rappresentano il 31,65%. Il 95,68% delle aziende è quindi tra 0 e 9 dipendenti: l'iper prevalenza di piccolissime aziende.

Complessa ed articolata la realtà delle Pubbliche Amministrazioni (PA) in Italia, con PA Centrali (PAC) e Locali (PAL). Il totale dei dipendenti pubblici, al 2020, risulta di circa 3.200.000, come indicato dalla Corte dei Conti nella "Relazione sul Costo del Lavoro Pubblico 2020" (https://www.corteconti.it/Download?id=fc101a7e-cc6c-4cd4-8561-a7cbcf05a1af), anche se con dati del 2018.

La PA italiana è costituita, in accordo con l'art. 1 comma 2 del D.lgs 30 marzo 2001 n. 165 (https://www.gazzettaufficiale.it/eli/id/2001/05/09/001G0219/sg) da:

- Presidenza del Consiglio dei ministri, i ministeri e le loro articolazioni centrali e locali, le istituzioni scolastiche, le agenzie[9] e le aziende autonome[10];
- le autorità amministrative indipendenti, che sono Enti pubblici con personalità giuridica: attualmente sono solo l'Amministrazione degli archivi notarili ed i Monopoli di Stato ;
- le regioni, le province, le città metropolitane, i comuni e gli altri enti territoriali locali quali ad esempio comunità montane, le comunità isolane, le unioni di comuni e i consorzi fra enti territoriali;
- gli altri enti pubblici, nazionali e locali, tra cui le istituzioni universitarie, gli enti pubblici di ricerca, le camere di commercio, industria, artigianato e agricoltura e gli enti che compongono il Servizio Sanitario Nazionale.
- Nel complesso le strutture organizzative della PA sono nell'ordine di 55.000, e di queste (2021):
  - Comuni: 7.904
  - Province e Città Metropolitane: 80 province, 14 città metropolitane e 6 liberi consorzi comunali in Sicilia) 2 province autonome in Trentino-Alto Adige

[9] Una Agenzia è distinta dall'organizzazione ministeriale, svolge una funzione pubblica ed è sottoposta a direzione o vigilanza da parte di un organo politico. Esempi: Agenzia delle Entrate, Agenzia del Demanio, AIFA, etc.; nel settore ICT AgID e ACN.

[10] Una Azienda Autonoma è una organizzazione che parte dello Stato o di altro ente pubblico e che è normalmente priva di personalità giuridica, ma possiede caratteri che le conferiscono un certo grado di compiutezza e separatezza. Il suo compito è di fornire e gestire servizi di pubblico interesse. Testo unico delle leggi sull'ordinamento degli enti locali- D.Lgs. 18 agosto 2000, n. 267 (https://web.camera.it/parlam/leggi/deleghe/testi/00267dl.htm). Molte Aziende Autonome nel passato sono state privatizzate o trasformate in Ente pubblico economico o in Agenzia.

- Regioni: 20 di cui 5 a statuto speciale
- Scuole pubbliche: **40.749**
- Università pubbliche: 67
- USL del Servizio Sanitario Nazionale[11](SSN): 650.

AgID realizza un Piano Triennale per l'informatica nella PA, arrivato ora con l'aggiornamento 2021-23 (si veda https://www.agid.gov.it/it/agenzia/piano-triennale), ed effettua sulla spese e sull'attuazione dei vari progetti dei controlli su circa il 50% della PA, Difesa esclusa.
La fig. 3.5-2 fornita dall'ISTAT su un suo parziale censimento sulle PAC e PAL (si veda https://www.istat.it/it/archivio/264488), evidenzia che la maggior parte di esse sono piccolissime organizzazioni, e che il 95% è costituito da strutture fino a 249 dipendenti, paragonabili quindi alle PMI private. Questo censimento è del 2018, ed è l'ultimo disponibile alla data.

CLASSI DI DIPENDENTI	Istituzioni per numero dipendenti	%
da 0 a 9	6.383	47,6
da 10 a 49	4.595	34,3
da 50 a 249	1.751	13,1
da 250 a 999	362	2,7
da 1,000 a 24,999	306	2,3
25,000 e oltre	9	0,1
Totale	**13.406**	**100,0**

Fig. 3.5-2 (ISTAT)

3.5.2 Il PNRR ed il suo impatto nella trasformazione digitale del Paese

Il PNRR[12], Piano Nazionale di Ripresa e Resilienza, è il piano italiano per poter usufruire dei finanziamenti, in parte a fondo perduto, del Next Generation dell'Unione Europea (NGEU)[13] che rappresenta la risposta europea alla grave crisi pandemica del Covid 19, con importanti investimenti e riforme per:

- accelerare la transizione ecologica e digitale;
- migliorare la formazione delle lavoratrici e dei lavoratori;
- conseguire una maggiore equità di genere, territoriale e generazionale.

Per l'Italia il NGEU è un'imperdibile opportunità di sviluppo, ma richiede, a fronte dei finanziamenti forniti, l'attuazione effettiva di importanti riforme da tempo indispensabili. L'Italia è fragile dal punto di vista economico, sociale ed ambientale , e tra le cause di questa fragilità c'è l'arretratezza nel digitale, dovuta sia ai ritardi e all'arretratezza/mancanza di idonee infrastrutture ICT (in particolare connessioni ad Internet in

[11] Il Servizio sanitario nazionale non è un'unica amministrazione, ma un insieme di enti ed organi che concorrono al raggiungimento degli obiettivi di tutela della salute dei cittadini. Lo compongono:

- Organismi centrali dello stato: Ministero della Sanità, Consiglio Superiore di Sanità, Istituto Superiore di Sanità, Conferenza Stato-Regioni, Agenzia Italiana del Farmaco, Istituti Zooprofilattici Sperimentali, Agenzia nazionale per i servizi sanitari regionali.
- Organismi regionali: assessorato alle attività sanitarie, Conferenza regionale permanente
- Organismi territoriali: Aziende Sanitarie Locali e Aziende Ospedaliere, Istituti di Ricovero e Cura a Carattere Scientifico

[12] https://www.governo.it/sites/governo.it/files/PNRR.pdf
[13] https://ec.europa.eu/info/strategy/recovery-plan-europe_it

larga banda) sia la prevalenza di piccole e piccolissime organizzazioni, private e pubbliche, che sono state ed ancora sono piuttosto lente nell'adottare efficacemente l'innovazione tramite il digitale, sia l'incapacità di parte del management, pubblico e privato, di effettuare le giuste scelte e di sfruttare le opportunità dell'innovazione digitale per le scarse competenze in materia, sovente associate a scorretti consigli di consulenti e fornitori. La digitalizzazione e l'innovazione di processi, prodotti e servizi rappresentano un fattore determinante della trasformazione dell'Italia e devono caratterizzare ogni politica di riforma del Piano.

Il PNRR, congruentemente con il NGEU, si articola in sedici Componenti, raggruppate in sei Missioni e sintetizzate nella tabella di fig. 3.5.2-1 (per i dettagli si rimanda a https://italiadomani.gov.it/it/home.html). La Tabella evidenzia le risorse assegnate a missioni e componenti del PNRR. A tali risorse, si aggiungono quelle rese disponibili dal REACT-EU che, come previsto dalla normativa UE, vengono spese negli anni 2021-2023 nonché quelle derivanti dalla programmazione nazionale aggiuntiva.

La digitalizzazione è un asse strategico e trasversale all'intero PNRR, definita nella Missione 1 ed articolata nella Componente 1 per le PA e nella Componente 2 per il sistema produttivo delle aziende. Questa Missione ha l'obiettivo di dare un impulso decisivo al rilancio della competitività e della produttività del Sistema Paese. Si deve comunque tener conto, come evidenziato nel PNRR, che "Lo sforzo di digitalizzazione e innovazione è centrale in questa Missione, ma riguarda trasversalmente anche tutte le altre. La digitalizzazione è infatti una necessità trasversale, in quanto riguarda il continuo e necessario aggiornamento tecnologico nei processi produttivi; le infrastrutture nel loro complesso, da quelle energetiche a quelle dei trasporti, dove i sistemi di monitoraggio con sensori e piattaforme dati rappresentano un archetipo innovativo di gestione in qualità e sicurezza degli asset (Missioni 2 e 3); la scuola, nei programmi didattici, nelle competenze di docenti e studenti, nelle funzioni amministrative, della qualità degli edifici (Missione 4); la sanità, nelle infrastrutture ospedaliere, nei dispositivi medici, nelle competenze e nell'aggiornamento del personale, al fine di garantire il miglior livello di assistenza sanitaria a tutti i cittadini (Missioni 5 e 6)."

Gli aspetti di sicurezza digitale sono evidenziati nella Componente 1 della Missione 1, focalizzata in particolare nei sistemi informativi delle PA, ma sono da considerarsi anche per tutti gli altri Componenti nelle varie Missioni. "La trasformazione digitale della PA contiene importanti misure di rafforzamento delle difese *cyber*, a partire dalla piena attuazione della disciplina in materia di "Perimetro di Sicurezza Nazionale Cibernetica". Gli investimenti sono organizzati su quattro aree di intervento principali. In primo luogo, sono rafforzati i presidi di *front-line* per la gestione degli alert e degli eventi a rischio intercettatati verso la PA e le imprese di interesse nazionale. In secondo luogo, sono costruite o rese più solide le capacità tecniche di valutazione e audit continuo della sicurezza degli apparati elettronici e delle applicazioni utilizzate per l'erogazione di servizi critici da parte di soggetti che esercitano una funzione essenziale. Inoltre, si investe nell'immissione di nuovo personale sia nelle aree di pubblica sicurezza e polizia giudiziaria dedicate alla prevenzione e investigazione del crimine informatico diretto contro singoli cittadini, sia in quelle dei comparti preposti a difendere il paese da minacce cibernetiche. Infine, sono irrobustiti gli asset e le unità cyber incaricate della protezione della sicurezza nazionale e della risposta alle minacce cyber. Tutto ciò è svolto in pieno raccordo con le iniziative Europee e alleate, per assicurare la protezione degli interessi comuni dei cittadini e delle imprese. Come investimento sulla sicurezza digitale in questo solo M1C1 sono previsti 0,62 Miliardi di €.

M1. DIGITALIZZAZIONE, INNOVAZIONE, COMPETITIVITÀ, CULTURA E TURISMO	PNRR (a)	React EU (b)	Fondo complementare (c)	Totale (d)=(a)+(b)+(c)
M1C1 - DIGITALIZZAZIONE, INNOVAZIONE E SICUREZZA NELLA PA	9,75	0,00	1,40	11,15
M1C2 - DIGITALIZZAZIONE, INNOVAZIONE E COMPETITIVITÀ NEL SISTEMA PRODUTTIVO	23,89	0,80	5,88	30,57
M1C3 - TURISMO E CULTURA 4.0	6,68	0,00	1,46	8,13
Totale Missione 1	**40,32**	**0,80**	**8,74**	**49,86**
M2. RIVOLUZIONE VERDE E TRANSIZIONE ECOLOGICA	**PNRR (a)**	**React EU (b)**	**Fondo complementare (c)**	**Totale (d)=(a)+(b)+(c)**
M2C1 - AGRICOLTURA SOSTENIBILE ED ECONOMIA CIRCOLARE	5,27	0,50	1,20	6,97
M2C2 - TRANSIZIONE ENERGETICA E MOBILITA' SOSTENIBILE	23,78	0,18	1,40	25,36
M2C3 - EFFICIENZA ENERGETICA E RIQUALIFICAZIONE DEGLI EDIFICI	15,36	0,32	6,56	22,24
M2C4 - TUTELA DEL TERRITORIO E DELLA RISORSA IDRICA	15,06	0,31	0,00	15,37
Totale Missione 2	**59,47**	**1,31**	**9,16**	**69,94**
M3. INFRASTRUTTURE PER UNA MOBILITÀ SOSTENIBILE	**PNRR (a)**	**React EU (b)**	**Fondo complementare (c)**	**Totale (d)=(a)+(b)+(c)**
M3C1 - RETE FERROVIARIA AD ALTA VELOCITÀ/CAPACITÀ E STRADE SICURE	24,77	0,00	3,20	27,97
M3C2 - INTERMODALITÀ E LOGISTICA INTEGRATA	0,63	0,00	2,86	3,49
Totale Missione 3	**25,40**	**0,00**	**6,06**	**31,46**
M4. ISTRUZIONE E RICERCA	**PNRR (a)**	**React EU (b)**	**Fondo complementare (c)**	**Totale (d)=(a)+(b)+(c)**
M4C1 - POTENZIAMENTO DELL'OFFERTA DEI SERVIZI DI ISTRUZIONE: DAGLI ASILI NIDO ALLE UNIVERSITÀ	19,44	1,45	0,00	20,89
M4C2 - DALLA RICERCA ALL'IMPRESA	11,44	0,48	1,00	12,92
Totale Missione 4	**30,88**	**1,93**	**1,00**	**33,81**
M5. INCLUSIONE E COESIONE	**PNRR (a)**	**React EU (b)**	**Fondo complementare (c)**	**Totale (d)=(a)+(b)+(c)**
M5C1 - POLITICHE PER IL LAVORO	6,66	5,97	0,00	12,63
M5C2 - INFRASTRUTTURE SOCIALI, FAMIGLIE, COMUNITÀ E TERZO SETTORE	11,17	1,28	0,34	12,79
M5C3 - INTERVENTI SPECIALI PER LA COESIONE TERRITORIALE	1,98	0,00	2,43	4,41
Totale Missione 5	**19,81**	**7,25**	**2,77**	**29,83**
M6. SALUTE	**PNRR (a)**	**React EU (b)**	**Fondo complementare (c)**	**Totale (d)=(a)+(b)+(c)**
M6C1 - RETI DI PROSSIMITÀ, STRUTTURE E TELEMEDICINA PER L'ASSISTENZA SANITARIA TERRITORIALE	7,00	1,50	0,50	9,00
M6C2 - INNOVAZIONE, RICERCA E DIGITALIZZAZIONE DEL SERVIZIO SANITARIO NAZIONALE	8,63	0,21	2,39	11,23
Totale Missione 6	**15,63**	**1,71**	**2,89**	**20,23**
TOTALE	191,50	13,00	30,62	235,12

I totali potrebbero non coincidere a causa degli arrotondamenti.

Fig. 3.5.2-1 (Fonte: Governo Italiano, valori in miliardi di €)

3.5.3 I principali attacchi digitali in Italia nel 2020, nel 1° semestre 2021 e oltre

Scelti dall'autore, sono nel seguito elencati alcuni dei principali attacchi digitali occorsi in Italia nel periodo considerato di OAD 2021, e che hanno avuto in taluni casi forte evidenza anche sui media non tecnici.

In termini generali in Italia si sono avuti numerosi attacchi ransomware, associati a phishing e a spear phishing, e attacchi collegati in vario modo alla pandemia Covid 19, da siti web malevoli con presunte informazioni sul Covid a phishing e malware targati Covid.

I seguenti principali attacchi digitali in Italia, nel periodo considerato, sono stati soventi ripresi dai media nazionali, e confermano il trend emerso dall'indagine.

- Dicembre 2020: attacco a livello mondiale alla catena del freddo per i vaccini Covid-19, basato su email di phishing in vari paesi occidentali, prese di mira organizzazioni, anche italiane, collegate alla Cold Chain Equipment Optimisation Platform (CCEOP) di **Gavi**, l'alleanza internazionale per i vaccini.
- Novembre 2020: attacco al **gruppo Campari**, con ransomware Ragnar-Locker, con furto di oltre 2 Terabit di dati e la richiesta di un riscatto di 15 milioni di US $;
- Ottobre 2020: attacco all'**Enel** con il virus Netwalker;

- Settembre 2020: attacco all' **Università Tor Vergata** con ransomware attivato da spear phishing, che ha bloccato l'intera infrastruttura ICT e colpito in particolare documenti su ricerche in ambito Covid19.
- Settembre 2020: attacco a **Luxottica** con ransomware/malware Nefilim, che ha portato al blocco degli stabilimenti della società in Cina, ed a quelli italiani in Agordo e Sedico.
- Luglio 2020: attacco all'**ENAC**, **Ente Nazionale per l'Aviazione Civile** con un ransomware che ha portato al blocco della posta elettronica, distrutto degli archivi digitali e reso inaccessibile il sito web.
- Giugno 2020: attacco all'**Enel** con il ransomware Skake/Ekans, che ha portato al furto di 5 TB di dati ed alla richiesta di un riscatto di circa 14 milioni di bitcoin, che la società dichiara di non aver pagato. Sul dark web sono stati pubblicati dati anche tecnici. Si noti che contemporaneamente è stato attaccato con lo stesso ransomware il Gruppo Honda.
- Giugno 2020: attacco con ransomware a **Geox**, con blocco dei suoi stabilimenti di calzature.
- Aprile 2020: attacco con ransomware installato via Telegram alla società italiana **Axios**, sviluppatrice di software per l'ambito scolastico, con richiesta di varie migliaia di € per il riscatto.
- Marzo 2020: tentativo di accesso all'infrastruttura ICT dell'**Istituto Ospedaliero Spallanzani**, in particolare ai file sulle ricerche sul Covid-19.

Nel 1° semestre 2021 non sono stati segnalati dai media significativi attacchi digitali in Italia, che sono invece occorsi nel 2° semestre 2021, che esula dall'arco temporale dell'indagine OAD 2021 ma che confermano i trend emersi. Tra questi attacchi digitali, quelli che hanno avuto maggior evidenza mediatica, anche per l'importanza dell'azienda/ente coinvolta, sono qui elencati.

- L'attacco ai SI della **Regione Lazio,** iniziato il 30 luglio 2021, che ha causato l'interruzione di servizi molto importanti per circa un mese: il sistema sanitario online, il servizio per la vaccinazione Covid-19 e il rilascio dei green pass, oltre al blocco di molte macchine in forza agli uffici tecnici dell'ente pubblico. Gli effetti nefasti del ransomware che ha messo in ginocchio il CED e i servizi informatici della Regione Lazio sono con buona probabilità dovuti all'incredibile ingenuità di un dipendente di una partecipata, a cui sarebbero stati rubati i dati di accesso al sistema, utilizzati per caricare il ransomware, prendere il controllo delle macchine e cifrare i dati.
- Un nuovo attacco ai SI **Enel** il 19 ottobre 2021 mediante il ransomware Netwalker, per il quale sono stati chiesti 14 milioni € in Bitcoin di riscatto e che ha causato il furto di 5 Tera Byte di dati, alcuni dei quali pubblicati nel darkweb.
- L'attacco ai SI della **SIAE,** Società Italiana degli Autori ed Editori, avvenuto nell'ottobre 2021, che ha portato all'esfiltrazione di circa 60 terabyte di dati, comprendenti documenti di identità, dichiarazione di paternità di alcune opere e variazione dei recapiti domiciliari forniti dagli artisti alla società nel corso degli anni. L'attacco è iniziato con un phishing, rivendicato dal gruppo Everest, che ha richiesto il riscatto di tre milioni di euro in bitcoin per la restituzione dei dati, che la SIAE, dopo aver informato la Polizia Postale e il Garante della privacy, ha affermato di non aver pagato. Questo attacco è interessante poiché rappresenta un caso significativo della "multiple extortion": si induce la vittima a pagare il riscatto prima per la decifratura dei dati, poi a pagarne un secondo per impedire che i dati sottratti vengano pubblicati o messi in vendita sul dark web. L'attaccante sovente non rispetta totalmente la seconda estorsione, o non viene pagato: contatta quindi direttamente le persone di cui ha ottenuto illegalmente informazioni per ricattarle direttamente, soprattutto se sono personaggi noti al pubblico.
- L'attacco ransomware a settembre 2021 all' **Ospedale San Giovanni di Roma**, che ha posto fuori uso per parecchi giorni tutti i server e i pc utilizzati dalla struttura medica, bloccando completamente i vari servizi, dalle prenotazioni online via web alle cartelle cliniche e agli esami radiologici. Il personale medico è stato costretto a gestire i dati in maniera totalmente cartacea.
- L'attacco ransomware Cryptolocker a ottobre 2021 all'azienda alimentare **San Carlo,** storica produttrice di patatine e snack.

Nel primo trimestre 2022, mentre AIPSI completava l'indagine OAD 2021 e si iniziava la stesura del presente rapporto, sono occorsi vari attacchi, quasi tutti basati su ransomware, sia per aziende che per le PA. Tra queste sono state attaccate con ransomware alcune **Aziende Sanitarie**, quali ULSS6 Padova e ASL Napoli 3 Sud, le **Ferrovie dello Stato**, il Comune di Villafranca, Enit, Arpa Veneto, Arpa Marche. La **Regione Lazio** ed il **Ministero della Salute** sono stati attaccati via smishing, e la **Regione Sardegn**a ha subito un data breach. Nell'ambito privato aziende della moda, come Moncler, dei trasporti, manifatturiere, della vendita e distribuzione soprattutto online.
In questo primo trimestre 2022, Lockbit 2.0 è stato il ransomware più diffuso in Italia, seguito da ALPHV (BlackCat), Grief e Conti.

3.5.4 Le istituzioni per la sicurezza digitale

In Italia è stata effettuata una importante riorganizzazione dei vari enti pubblici dedicati alla sicurezza digitale, attualmente in fase di completamento operativo, a partire dalla Legge 124/2007 che ha riordinato tutti i servizi segreti italiani, che si occupano anche della cyber intelligence.
La fig. 3.5.4-1 schematizza gli enti preposti e loro relazioni: tutti fanno riferimento alla Presidenza del Consiglio dei Ministri, con il CISR, Comitato interministeriale per la sicurezza della Repubblica ed il COPASIR, Comitato parlamentare per la sicurezza della Repubblica, quale organo di controllo parlamentare.

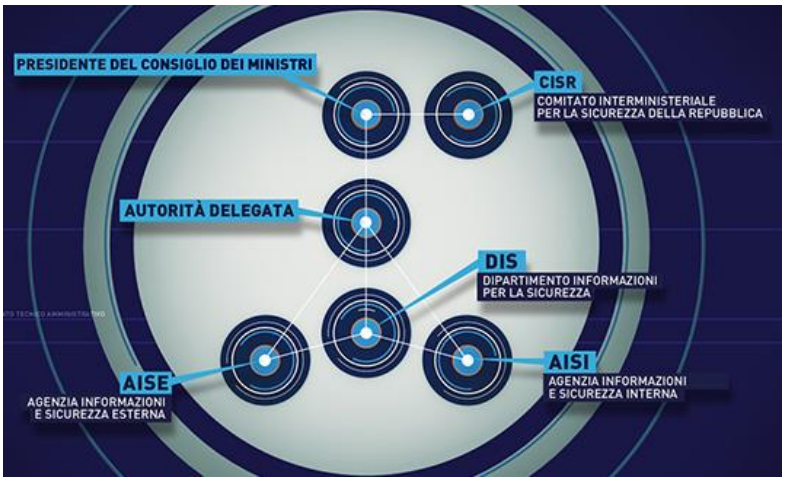

Fig. 3.5.4-1

La figura evidenzia le due Agenzie operative, l'**AISI** per l'intelligence in ambito interno al paese, e l'**AISE** per l'intelligence in ambito esterno, quindi all'estero negli altri paesi europei e non. A quest'ultima fanno riferimento, quando operano all'estero, anche gli organismi militari italiani di intelligence.
Questa logica di centralizzazione decisionale è stata recentemente applicata dal Governo con la creazione dell'**Agenzia Cybersicurezza Nazionale, ACN**, con compiti di resilienza e sicurezza in ambito informatico, anche ai fini della tutela della sicurezza nazionale nello spazio cibernetico, e assicura il coordinamento tra i soggetti pubblici coinvolti nella materia (https://www.acn.gov.it/). Ad ACN rispondono ora i seguenti enti:

- **NCS**, Nucleo per la cybersicurezza: ha funzioni di prevenzione e preparazione ad eventuali situazioni di crisi e per l'attivazione delle procedure di allertamento
- **CSIRT**, Computer Security Incident Response Team Italia (https://csirt.gov.it/)
- **CVCN,** Centro di Valutazione e Certificazione Nazionale.

A livello militare la struttura operativa è il **COR**, **Comando Operazioni in Rete**: sotto la supervisione del Capo di Stato Maggiore della Difesa (Casmd), coordina le attività di sicurezza e difesa cibernetica delle Forze Armate e del Ministero della Difesa (https://www.difesa.it/SMD_/COR/Pagine/default.aspx).
A livello di contrasto dei crimini e delle frodi informatiche operano le strutture già esistenti:

- **Polizia Postale e delle Comunicazioni**: preposta al contrasto delle frodi postali e del crimine informatico (https://www.commissariatodips.it/)
    - **CNAIPIC**, Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (https://www.commissariatodips.it/profilo/cnaipic/index.html)
- **NSTPFT,** Nucleo Speciale Tutela Privacy e Frodi Tecnologiche: Reparto Speciale della Guardia di Finanza che si occupa di contrastare le frodi telematiche ed informatiche, nonché tutelare la privacy (https://www.reportdifesa.it/tag/nucleo-speciale-tutela-privacy-e-frodi-tecnologiche-nstpft/)

A livello dell'Unione Europea (UE) due sono i principali organismi per la sicurezza digitale:

- **CRRT**, Cyber Rapid Response Teams and mutual assistance in cyber security (https://pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/#:~:text=Cyber%20Rapid%20Response%20Teams%20(CRRTs,operations%20as%20well%20as%20partners), nell'ambito di Pesco, Permanent Structured Cooperation, per migliorare la difesa anche cybernetica dei vari paesi membri dell'UE
- **ENISA**, European Union Agency for Cybersecurity: ha l'incarico di di creare le condizioni per un elevato livello comune di cibersicurezza in tutta l'Unione Europea. Si focalizza in particolare su: sensibilizzazione e responsabilizzazione delle comunità europee, politiche di cybersecurity, cooperazione operativa, rafforzamento delle capacità, soluzioni affidabili, previsioni (https://www.enisa.europa.eu/about-enisa/about/it)

4. Gli attacchi digitali in Italia dall'indagine OAD 2021

Il presente capitolo presenta e commenta con opportuni grafici i più importanti dati emersi dall'indagine.
Particolare importanza ed enfasi viene data in questo rapporto all'analisi delle correlazioni tra i dati raccolti, rigorosamente anonimi, quali ad esempio gli attacchi digitali rilevati per tipo di azienda/ente, per sue dimensioni, per suo fatturato, etc.
La fig. 4-1 mostra, percentualmente, il numero di attacchi rilevati dai rispondenti nel 2020 e nel 1° semestre 2021: gli attacchi rilevati superano di quasi 10 punti percentuali il valore di attacchi non subiti (o non rilevati) e confermano il trend di **forte incremento degli attacchi digitali intenzionali** per i rispondenti ai questionari OAD 2021 rispetto agli anni precedenti, trend approfondito nell'analisi effettuata commentando la fig. 4-3.
Si rammenta che, pur con un differente bacino di rispondenti, in OAD 2020 il 1° quadrimestre 2020, durante il quale era iniziata ed esplosa in Italia la pandemia Covid-19, aveva riportato un 44,8% di attacchi digitali rilevati, ora giunto per l'intero anno 2020, con l'indagine OAD 2021, a ben 59,1%.

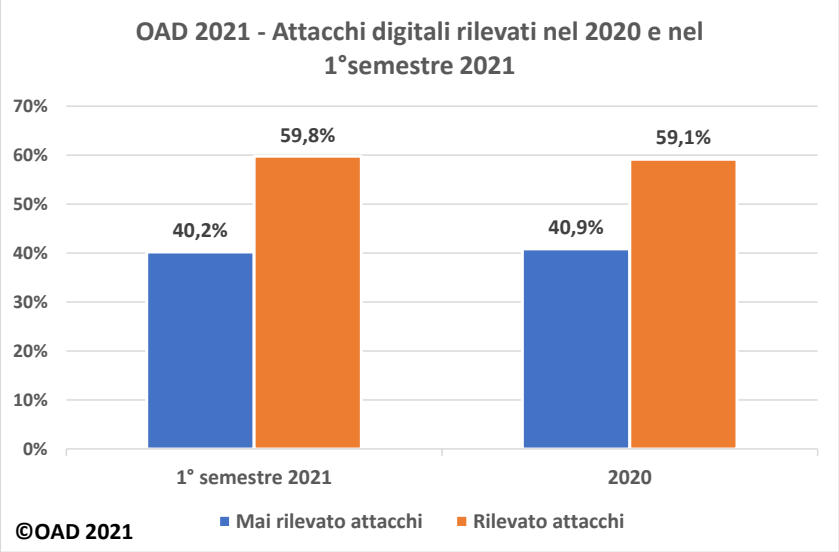

Fig. 4-1

La fig. 4-2 dettaglia la percentuale di attacchi rilevati nei due periodi considerati tra attacchi frequentemente ripetuti ed attacchi digitali meno frequenti, indicati nella figura come "saltuari". Questi ultimi, come è ragionevole, sono di gran lunga prevalenti.

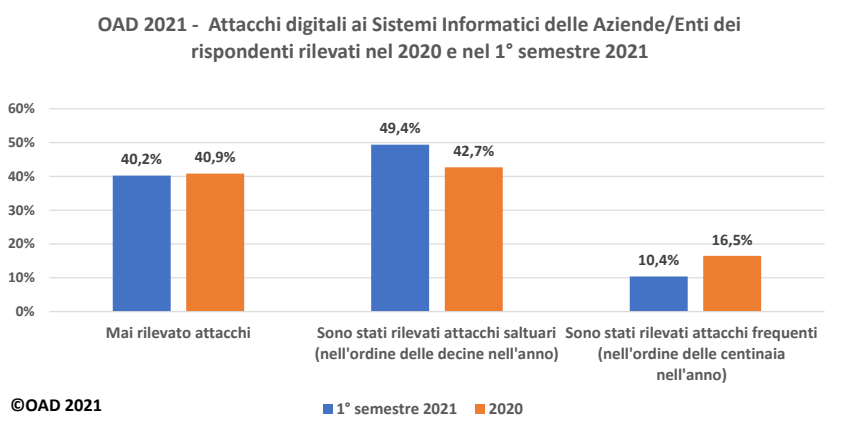

Fig. 4-2

La fig. 4-3 confronta il numero di attacchi rilevati nei diversi Rapporti OAI dal 2007 al 1° semestre 2021. 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.

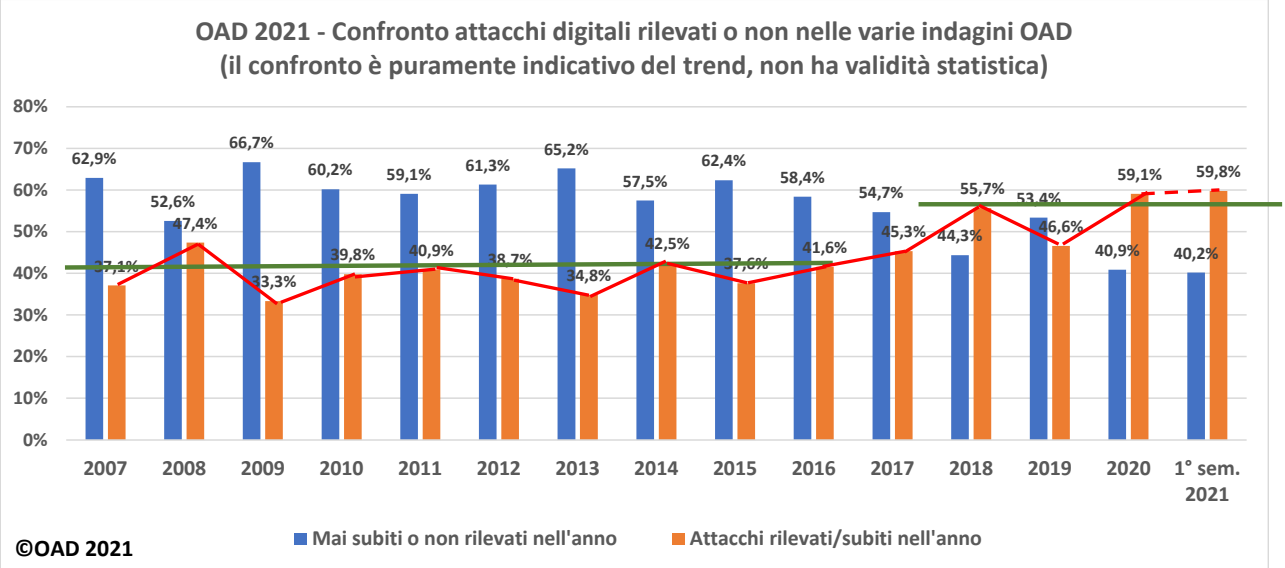

Fig. 4-3

Nell'arco temporale considerato, la figura evidenzia come, a parte il 2008 che rappresentò il primo *annus horribilis* per la quantità di attacchi digitali subiti, dal 2007 al 2016 si è avuto un sali-scendi, evidenziato in figura dalla riga rossa, del numero di attacchi rilevati attorno a circa il 40% dei rispondenti: la riga verde evidenzia in tale periodo questo trend: l'onda altalenante delle percentuali di attacchi digitali rilevati dalle indagini OAD evidenzia il rincorrersi di guardie e ladri: si avvicendano periodicamente, come è logico, l'innovazione sulle modalità d'attacco, e le conseguenti "nuove" (o semplicemente attuate) misure di difesa atte a contrastarli.

Nel 2017 e nel 2018 la figura evidenzia la forte crescita percentuale degli attacchi rilevati, che nel 2018 raggiunge il primo picco di 55,7%, la prima volta 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%, confermando ancora il trend di rafforzamento delle misure di sicurezza dopo una fase di maggiori e più sofisticati attacchi. Nel 2020 e nel 1° semestre 2021 la percentuale di attacchi rilevati cresce ancora, arrivando quasi al 60%: si veda la seconda riga verde in figura.

Anche l'indagine OAD 2021 rileva un reale salto, sia come numero sia come sofisticazione, e quindi pericolosità, negli attacchi digitali intenzionali ad aziende ed enti in Italia nell'ultimo quadriennio, confermando quanto rilevato dalle varie indagini nazionali ed internazionali: un chiaro indicatore della criticità degli attacchi digitali portati, e delle misure di sicurezza di contrasto che non sono ancora adeguate e sufficienti. Si deve tener conto, per quest'ultimo aspetto, dell'enorme numero di piccole e piccolissime organizzazioni in Italia sia in ambito privato che pubblico. Organizzazioni che nella maggior parte dei casi non hanno, e non possono di fatto avere, competenze e sovente capacità economiche per acquisire e gestire gli strumenti di sicurezza digitale, tecnici ed organizzativi, necessari.

Come descritto in §5.3.1, in Italia l'elevatissimo numero di piccole e piccolissime imprese pubbliche e privati, non rappresentano un obiettivo di interesse specifico per i cyber criminali, soprattutto per i così detti attacchi mirati (targeted attack), mentre 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.

Questo è confermato analizzando le fig. 4-4 e 4-5 che mostrano la distribuzione percentuale degli attacchi

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

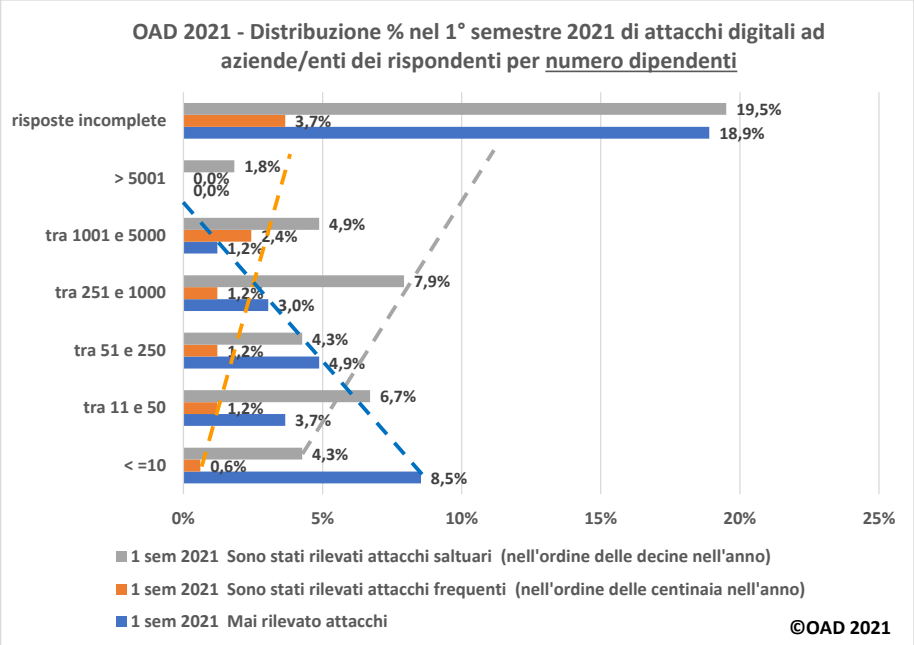

Fig. 4-4

La fig. 4-4 e la fig. 4-5 mostrano rispettivamente per il 1° semestre 2021 e per l'intero 2020 la distribuzione percentuale degli attacchi digitali, subiti o non, correlate alle dimensioni delle aziende/enti dei rispondenti per numero di dipendenti. La voce "risposte incomplete" nel grafico è mostrata solo per dimostrare la correttezza dei calcoli percentuali con i dati delle figure precedenti. Dato che alcuni rispondenti non hanno completato fino alla fine i questionari, il numero di rispondenti per le domande alla fine dei due questionari, che includono quelle sulle caratteristiche, sempre anonime, sul tipo di azienda/ente, sono minori di quelle fornite all'inizio dei questionari, che comprendono quelle relative agli attacchi. In entrambe le figure le linee tratteggiate arancioni e grigie evidenziano la tendenza all'aumento degli attacchi digitali per aziende di dimensioni crescenti, ed ancor più chiaramente la linea tratteggia blu mostra il decrescere di attacchi non subiti/rilevati al crescere delle dimensioni dell'azienda ente.

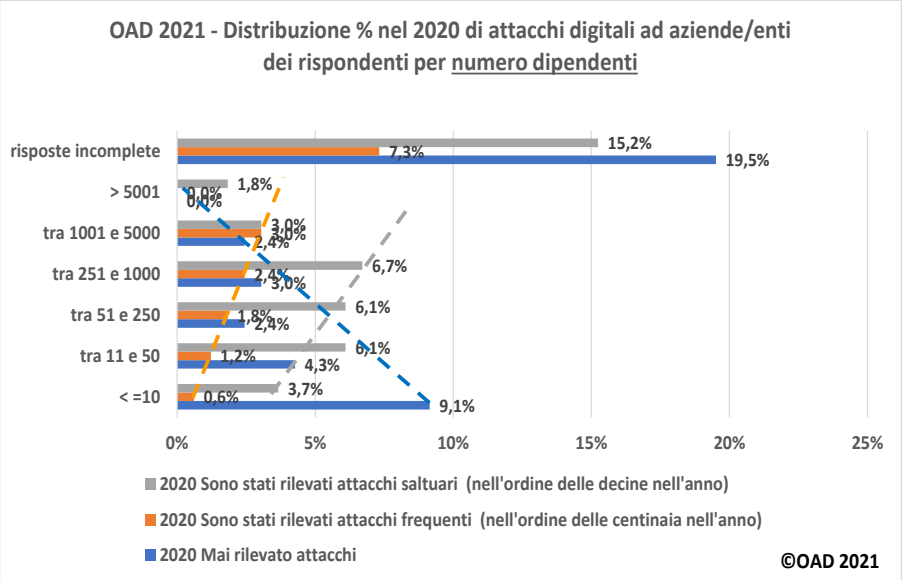

Fig. 4-5

Un'ulteriore conferma viene dalle fig. 4-6 e 4-7 che mostrano in percentuale, per il 1°semestre 2021 e per il 2020 rispettivamente, la ripartizione degli attacchi digitali per il fatturato dell'azienda o per il giro economico delle PA secondo l'ultimo bilancio disponibile. Nelle due figure le linee tratteggiate arancioni e grigie evidenziano la tendenza all'aumento degli attacchi digitali per aziende/enti con un crescente giro d'affari, ed ancor più chiaramente la linea tratteggia blu mostra il decrescere di attacchi non subiti/rilevati al crescere del fatturato o giro economico di aziende/enti dei rispondenti.

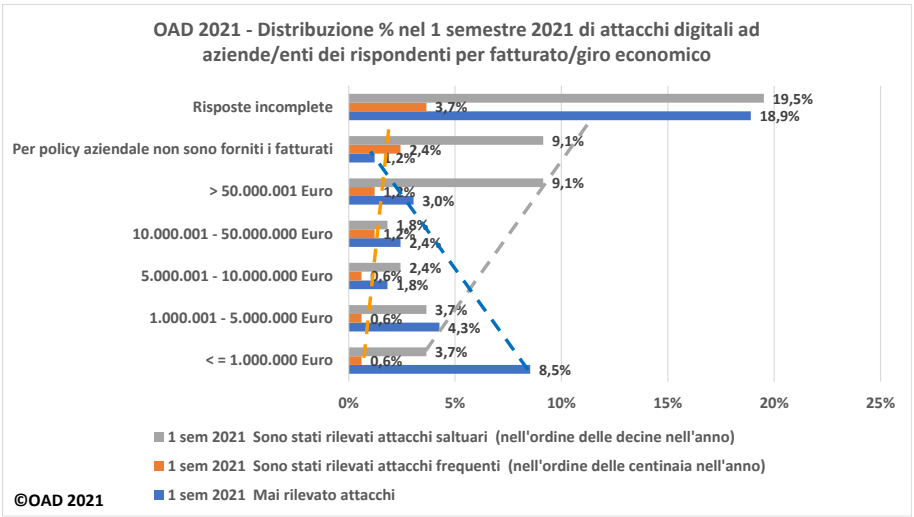

Fig. 4-6

La fig. 4-8 mostra i tempi massimi richiesti per il ripristino del funzionamento del Sistema Informativo a seguito dal più grave attacco subito. La domanda era solo nel questionario OAD completo, e quindi solo i rispondenti ad esso sono il bacino di riferimento della figura. Due i dati più importanti che emergono: l'82,9% dei rispondenti ripristina entro una settimana, e tra questi circa 1/3 ripristina entro un giorno dall'attacco, ma per l'8,8% il ripristino ha richiesto più di un mese. Questo da un lato significa che i Sistemi Informativi delle aziende/enti rispondenti hanno dei medio-buoni livelli di disponibilità in grado di riprendersi in tempi brevi almeno dai più diffusi e noti attacchi (si veda anche §7 e §8), ma per gli attacchi più sofisticati l'8,8%, quasi un decimo del totale, rimane bloccato per oltre un mese, in tempo lunghissimo che può comportare il

blocco complessivo, o di alcune sue parti, dell'azienda/ente che ha subito questo attacco senza aver capacità di ripristino in tempi brevi .

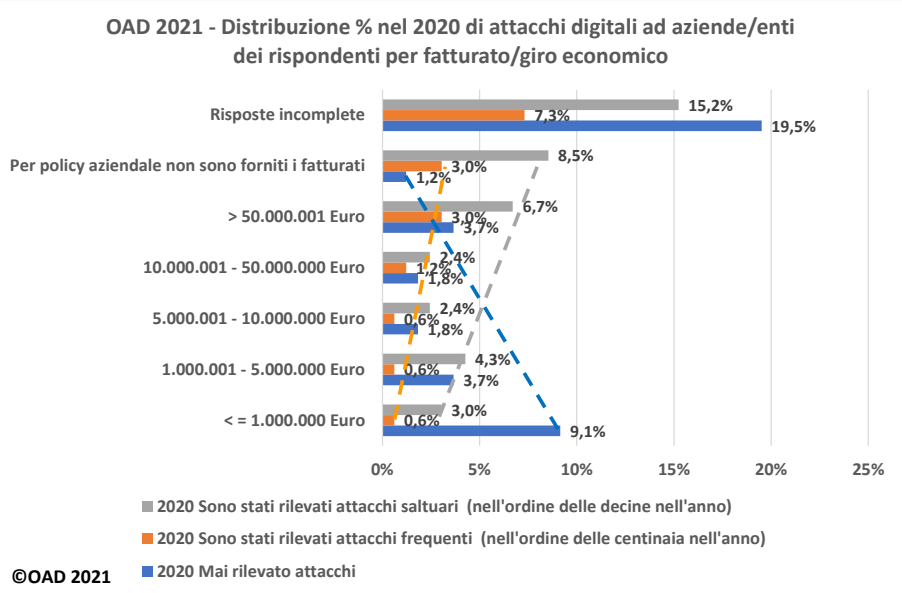

Fig. 4-7

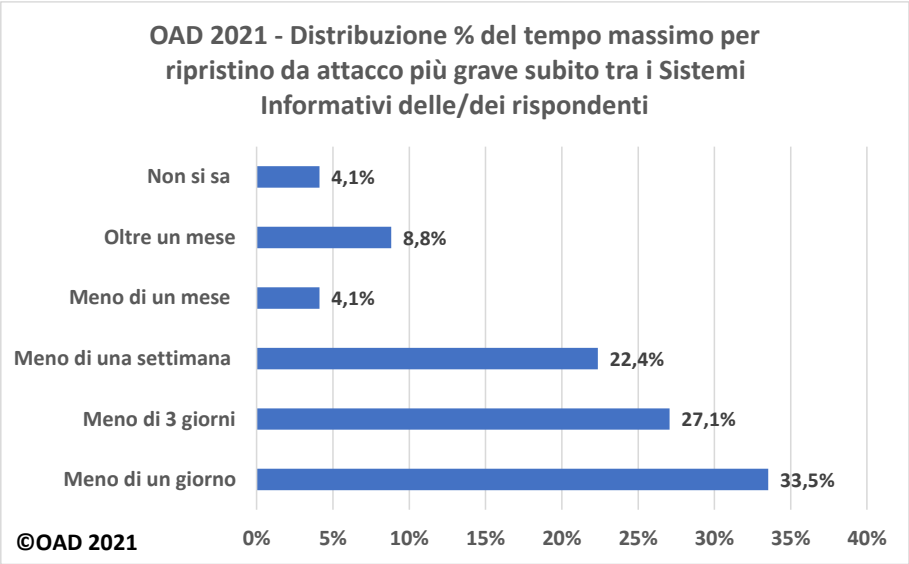

Fig. 4-8

La fig. 4-9 mostra gli impatti "tecnici" e funzionali che il SI hanno avuto a seguito dal più grave attacco subito. I dati della figura sono indipendenti dal tipo di attacco subito e rappresentano una media di quanto indicato dai rispondenti per ogni tipologia di attacco rilevata.

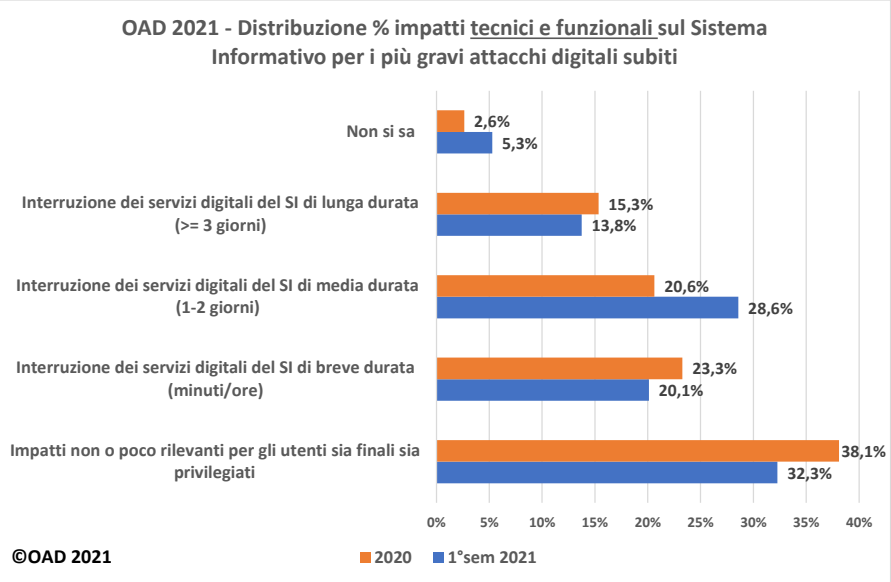

Fig. 4-9

La fig. 4-10 mostra gli impatti di costo sui budget sia del SI sia dell'azienda/ente a seguito dal più grave attacco subito. Questa domanda era presente solo sul questionario completo. Come è ragionevole, l'impatto è prevalentemente sul budget del SI, e ben più bassa la % di impatti economici sul bilancio dell'intera azienda/ente.
I dati della figura sono indipendenti dal tipo di attacco subito, e rappresentano una media di quanto indicato dai rispondenti per ogni tipologia di attacco grave rilevata.

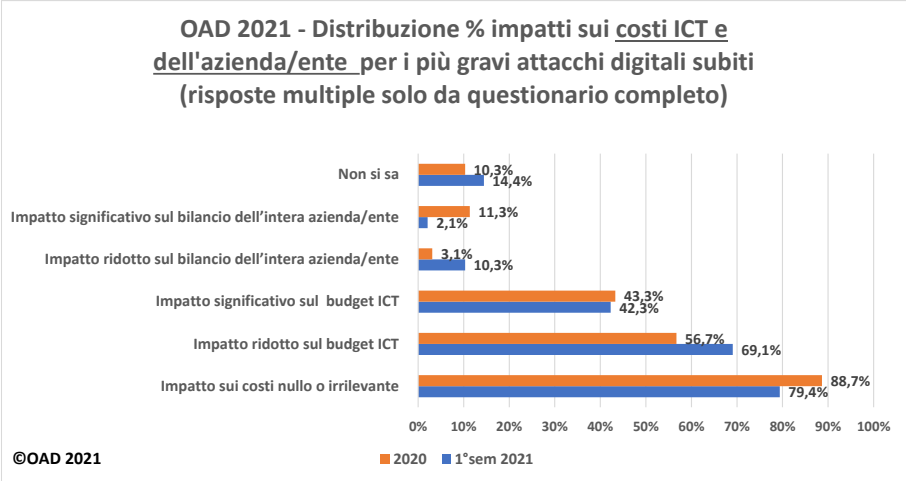

Fig. 4-10

In termini di valori "assoluti" in € dell'impatto economico subito a seguito del più grave attacco digitale o complessivamente nell'arco temporale considerato, intero anno 2020 e 1 semestre 2021, pochissime le risposte avute, dato che la maggior parte ha indicato che non ci sono stati impatti economici, o che non si è stati in grado, o non si è voluto, calcolarli.
Tra i pochissimi che hanno indicato dei valori, in €:

- il danno complessivo nell'intero 2020 dall'insieme degli attacchi digitali subiti è indicato con valori tra i 200.000 e i 1.000.000 € da appartenenti al settore del commercio, attività finanziarie ed assicurative, servizi turistici, di alloggio e ristorazione;

- il singolo attacco che ha causato i maggiori danni economici ha provocato un danno economico che varia tra gli 80.000 ed i 300.000 €, come indicato dalle stesse aziende dei settori merceologici del punto precedente.

Il dato di maggior interesse di ogni indagine OAD è la tipologia di attacco digitale di maggior diffusione tra il bacino di aziende/enti rispondenti. La fig. 4.11 mostra che anche per OAD 2021 la tipologia d'attacco che ha avuto la maggior diffusione sia nell'intero anno 2020 sia nel primo semestre 2021 è quella sui sistemi IAA, Identificazione-Autenticazione-Autorizzazione, seguita a pochi punti percentuali dall'attacco/uso non autorizzato di un intero sistema ICT, sia fisico che virtuale. Al terzo posto, ma con molti punti di distacco, la saturazione delle risorse ICT, il DoS/DDoS, Deniel of Service/Distributed DoS.

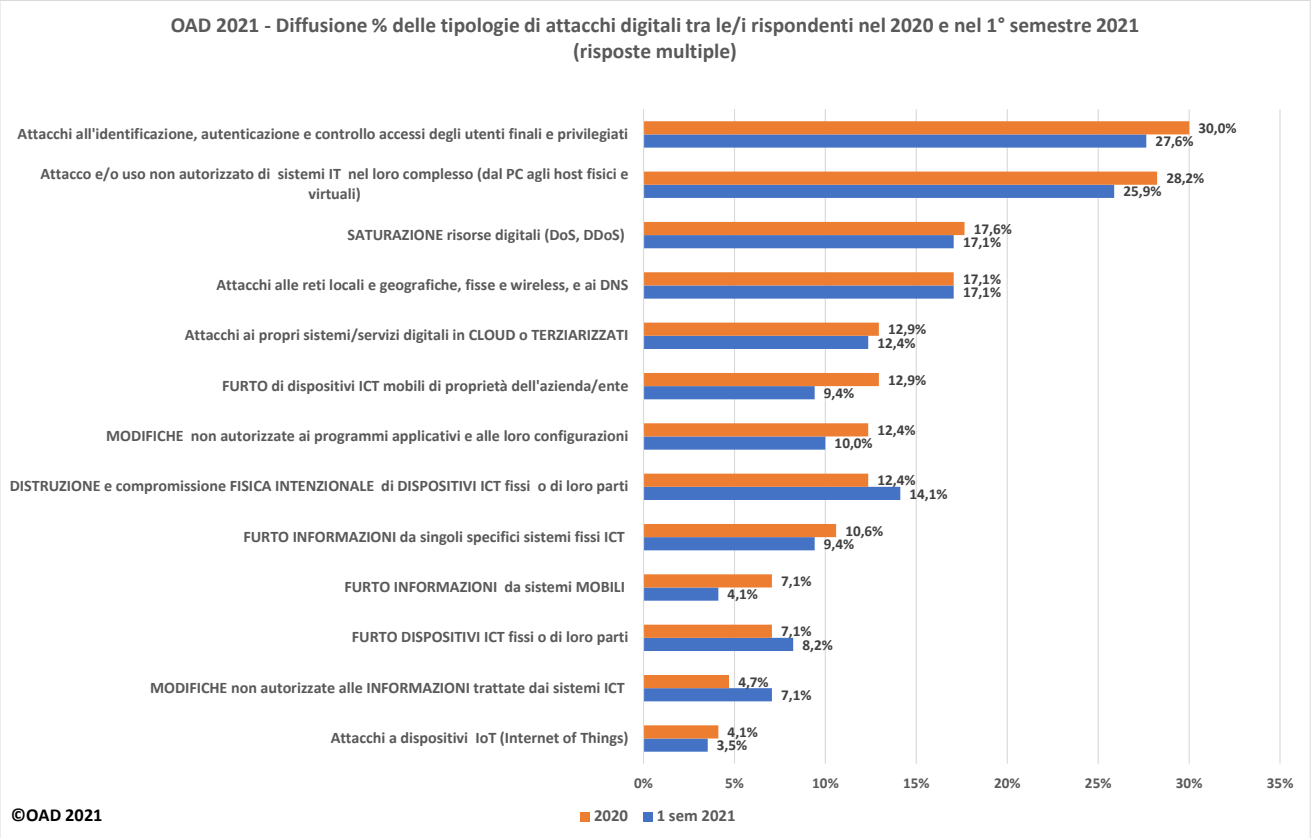

Fig. 4-11

Seguono poi, come % di diffusione, gli attacchi alle reti ed ai sistemi/servizi terziarizzati e in cloud, e tutte le altre tipologie di attacco digitale considerate con percentuali a decrescere. Nella lettura di questi dati si deve considerare che le tipologie di attacco a sistemi in Cloud, a sistemi IoT, a sistemi di automazione industriale/robotica, riguardano solo alcuni SI delle aziende/enti rispondenti, che non li utilizzano e/o che non sono necessari per le loro attività (si veda anche §7).
Gli attacchi IAA sono i più diffusi e tra i più critici in quanto consentono il furto dell'identità digitale di un utente, e se è un utente privilegiato, consentono di effettuare ulteriori gravi manomissioni al SI, o a quella parte del SI, che l'utente privilegiato gestisce: inserimento di programmi non autorizzati, copia o modifica di dati, eliminazione di programmi (in particolare quelli tipici della sicurezza digitale), e così via.
In termini di trend emersi negli anni dalle indagini OAD, gli attacchi digitali sul controllo degli accessi (IAA), sui singoli sistemi ICT, sulle reti, sono stati, pur con % diverse, ai primi posti come diffusione tra i SI oggetto delle indagini.
La diffusione delle **tipologie di attacchi digitali** di OAD 2021 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 e la congruenza dei valori emersi dalla presente indagine OAD.
La fig. 4-12 riporta la diffusione percentuale delle **tecniche di attacco** usate nelle diverse tipologie di attacco: diffusione data dalla media dell'occorrenza di una data tecnica in tutte le tipologie di attacchi rilevate ai SI. Non si distingue tra occorrenza nel 2020 o nel 1° semestre 2021, dato che volutamente le domande nei due questionari chiedevano di selezionare, con risposte multiple, le tecniche individuate o presunte negli attacchi digitali più gravi riscontrati, indipendentemente dal periodo specifico in cui erano occorsi.

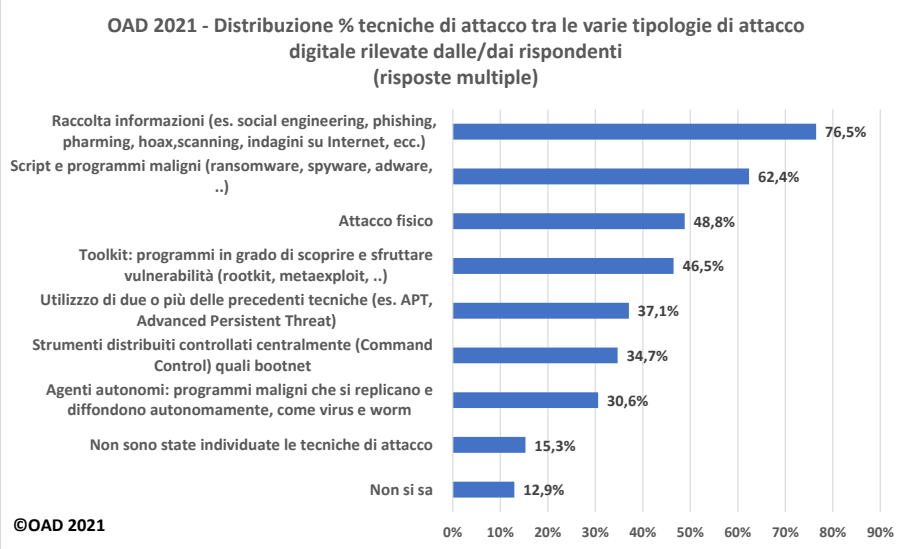

Fig. 4-12

Al primo posto le varie tecniche di raccolta di informazioni non autorizzata, tipicamente il social engineering, al secondo posto l'uso di script e malware, ed al terzo posto, con molti punti di differenza %, l'attacco fisico ai sistemi ICT. Al quarto posto l'uso di toolkit. Le altre tecniche e meccanismi di attacco vanno a fortemente degradare percentualmente.
A parte l'attacco fisco, le altre tre tecniche di attacco sono state sempre ai primi posti nelle precedenti indagini OAD, pur con % e posizionamenti diversi, comunque ai vertici di questa classifica. Per l'attacco "fisico" è bene tener presente che esso include non solo la distruzione o il furto di parti fisiche di un sistema ICT, tipicamente un hard disk, ma anche sottrazione di dati in maniera "fisica" tramite chiavette USB. Le porte USB di molti sistemi non sono bloccate/controllate, e le attuali "chiavette USB", purstando in una tasca, hanno capacità di più Terabyte.
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: i ransomware sono ancora molto diffusi in Italia, e perniciosi. 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 sofisticati e partano da una attenta analisi delle configurazioni e delle vulnerabilità sui sistemi ICT target dell'attacco.
L'attacco fisico al terzo posto come diffusione % nel bacino dei rispondenti, può sembrare strano o fuori luogo, ma ha senso, soprattutto se correlato al secondo posto degli attacchi all'intero singolo sistema ICT del SI e alla compromissione o distruzione di sistemi ICT fissi o di loro parti, posizionata come diffusione all'ottavo posto, come evidenziato nella fig. 4-11. L'uso non autorizzato di un sistema ICT, oltre alla sua compromissione fisica, può essere attuata con un attacco "fisico", che non solo è implica la rottura di un dispositivo o di una sua parte, ma anche, ad esempio, la copia "fisica" dei suoi contenuti tramite chiavette USB.

La fig. 4-13 mostra la probabile origine degli attacchi digitali più critici rilevati nel periodo considerato. Come distribuzione percentuale, la maggior parte, il 71,1%, dichiara onestamente di non saperlo indicare. Il 69,1% indica enti esterni: la larga esposizione su Internet dei moderni SI, offre ampie possibilità d'attacco ad enti esterni, che sovente hanno grandi capacità e competenze sia per crimini informatici sia per hactivism e addirittura guerre elettroniche (si veda in merito §3.1.2).

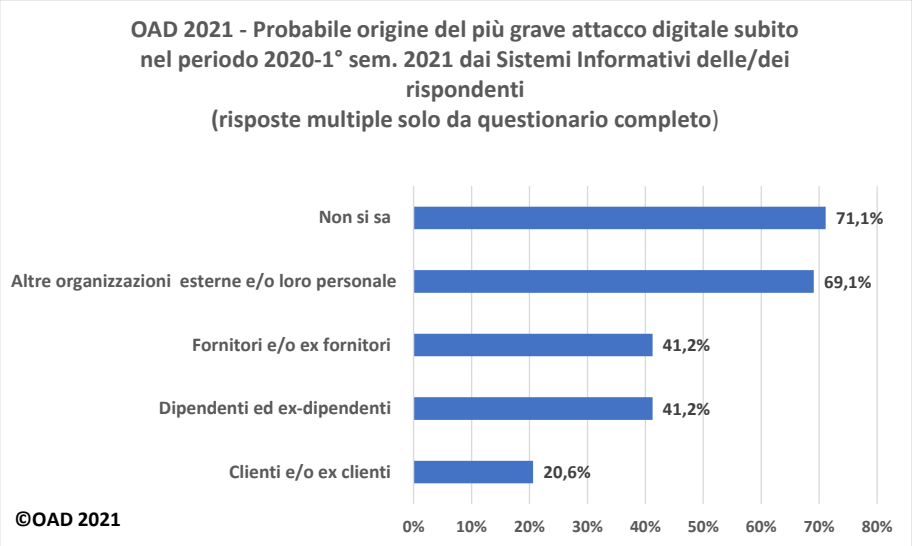

Fig. 4-13

Con la medesima percentuale, ma a molti punti di distanza dai precedenti con il 41,2%, la possibile origine può provenire da fornitori, o ex fornitori, così come da propri dipendenti, o ex dipendenti. Ancora più distanziati i clienti o ex clienti.

La fig. 4-14 fornisce, con risposte multiple, la distribuzione percentuale delle possibili motivazioni per gli attacchi digitali più gravi subiti e rilevati: la domanda relativa era solo nel questionario completo. La stragrande maggioranza, 93,8%, indica come motivazione il ricatto/ritorsione, seguita al 50% dallo spionaggio e/o per motivi di concorrenza. Seguono, a scalare e con percentuale molto più basse, le altre motivazioni considerate. L'autore ha trovato relativamente basso il valore per la "frode", ma probabilmente chi ha risposto ha di fatto incluso questa motivazione nel ricatto/ritorsione.

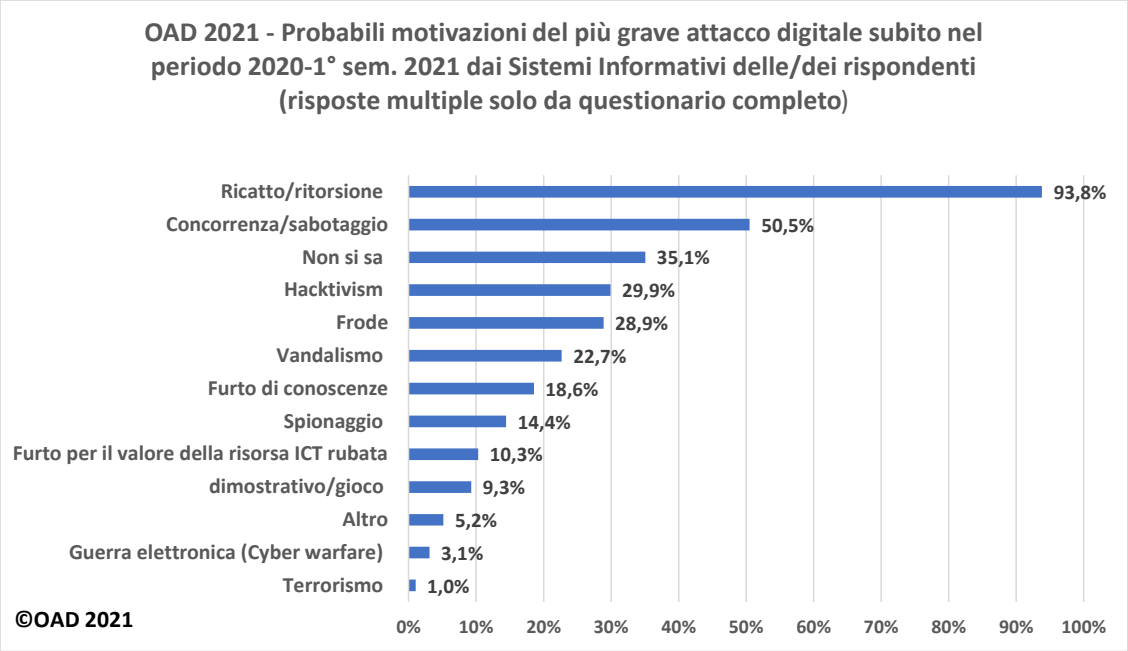

Fig. 4-14

4.1 La rilevazione e la gestione degli attacchi digitali nei SI delle aziende/enti rispondenti

L'attacco digitale intenzionale portato ad un SI deve essere immediatamente rilevato per poterlo contrastare e gestire. E' ben noto invece che molti attacchi non vengono rilevati, almeno fino a quando i loro impatti sul SI e sulle attività e business dell'azienda/ente non divengono palesi. Come per le precedenti edizioni, anche OAD ha posto delle specifiche domande in merito sia nel questionario completo che in quello ridotto.
La fig. 4.1-1 mostra chi ha individuato l'occorrenza dell'attacco digitale, e come, con risposte multiple. Dato che il SI può aver subito più attacchi nel periodo considerato, la risposta fornita dà un'indicazione di chi prevalentemente individua che il SI è sotto attacco o che quest'ultimo è già avvenuto.

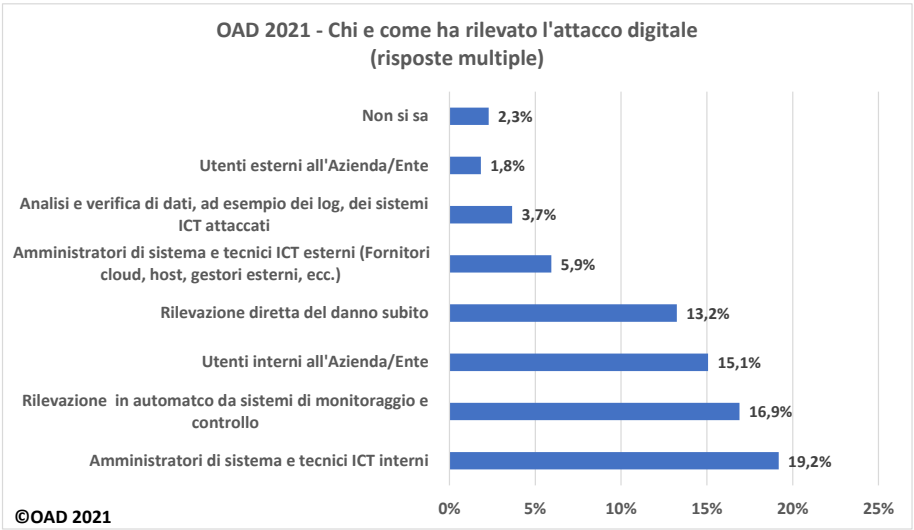

Fig. 4.1-1

Il valore più alto, nel 19,2 %, indica che sono gli amministratori di sistema ed i tecnici informatici interni all'azienda/ente ad accorgersene, e per il 16,9% su segnalazione in automatico dai sistemi di monitoraggio e controllo della sicurezza digitale che gestiscono. Per il 15,1% dei casi sono gli stessi utenti finali interni ad accorgersene, e ad avvertire chi gestisce la sicurezza digitale.
Nel caso degli attacchi più gravi, soprattutto come impatti su determinati dati come quelli personali o sulle funzionalità del SI, in particolare se rientra tra le infrastrutture critiche che forniscono servizi ICT essenziali per la nazione, è necessario per legge, o è comunque opportuno, comunicarlo a determinati enti/agenzie. Le agenzie e gli enti di riferimento, anche a livello italiano, sono in corso di ristrutturazione in accordo con le più recenti direttive europee, come indicato in §3.5.4. La domanda in merito, di tipo abbastanza generale, era presente in entrambi i questionari OAD 2021, ed i risultati, con risposte multiple, sono mostrati nella fig. 4.1-2. Una quota parte delle segnalazioni, il 18,7%, lo comunica ad una delle autorità preposte, e tra questi il 6,8% lo comunica all'Autorità Garante della privacy, dato che l'attacco ha coinvolto dati personali. Il 16,9%, comunica l'attacco digitale, grave o non, ai suoi fornitori e consulenti informatici, per avere da loro indicazioni ed interventi per rimediare all'attacco e per eliminare le vulnerabilità che l'hanno permesso. Nel 13,2% dei casi non viene comunicato a nessuna autorità o ente, per specifici motivi che sono elencati nella fig. 4.1-3.
Si deve tener conto che le percentuali emerse sono relativamente basse, dato che le risposte sono multiple. Al di là di questo aspetto, le comunicazioni alle autorità e/o ai fornitori e consulenti non sono sistematiche e frequenti: probabilmente se l'impatto non è stato significativo e non ci sono obblighi normativi stringenti, la comunicazione è considerata una inutile pratica burocratica che fa solo perdere tempo.

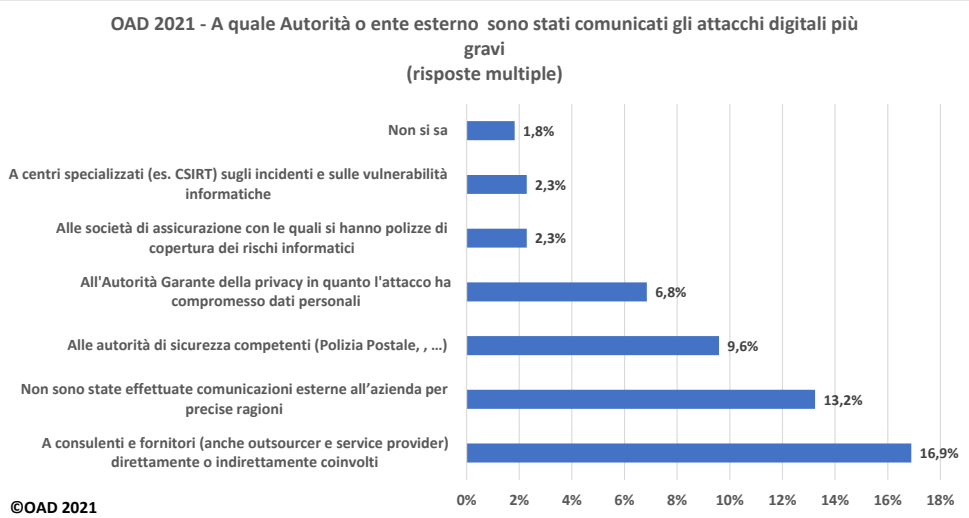

Fig. 4.1-2

Per il 13,2%, come singola voce al secondo posto come diffusione percentuale, la comunicazione dell'attacco non viene effettuata per le ragioni specifiche selezionate ed elencate, con risposte multiple, nella fig. 4.1-3.

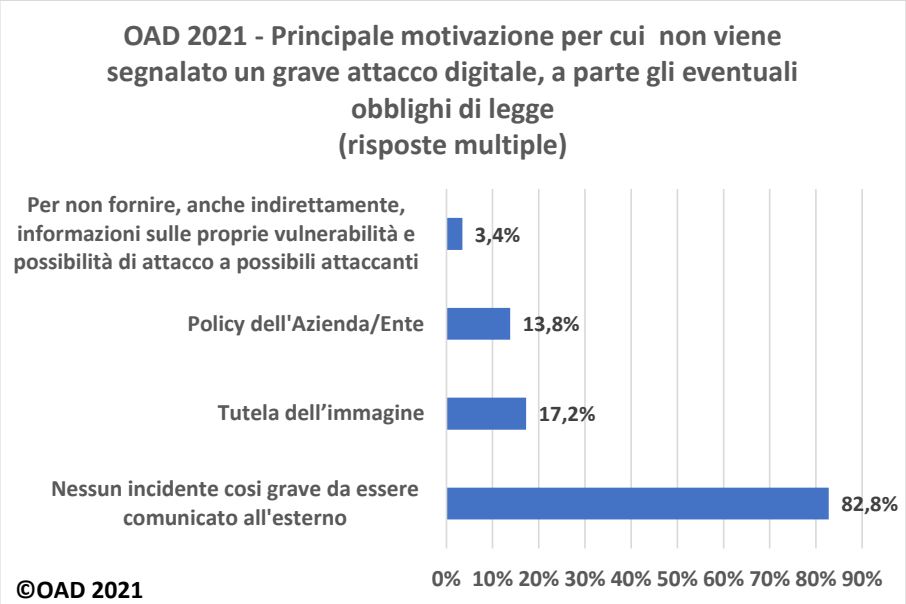

Fig. 4.1-3

Per la gran parte, l'82,8%, la ragione è ovvia: nessun attacco è stato così grave e significativo che valesse la pena di comunicarlo. In una risposta è stato specificato che "Tutti gli attacchi sono stati gestiti (quindi prevenuti) ancor prima che potessero essere attivati". Al secondo posto, ma a grande distanza con un 17,2%, la tutela dell'immagine dell'azienda/ente che ha subito l'attacco. In determinati settori merceologici, ed anche nelle PA, aver subito un attacco informatico è un'onta, fa presupporre che non fossero presenti le idonee misure di sicurezza, quindi perdita di affidabilità, autorevolezza: meglio quindi non comunicare alcuna informazione, che potrebbe essere diffusa dai media.
Le azioni intraprese dalle aziende/enti rispondenti dopo aver subito un attacco digitale, a parte l'eventuale comunicazione ad enti esterni, sono mostrate nella fig. 4.1-4, 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 una diffusione del 22,8%, l'installazione di patch e di aggiornamenti ai software in uso, per eliminare le loro vulnerabilità, con il 22,4%, e la messa in produzione di nuovi strumenti di sicurezza digitale con il 16,4%.
A scalare seguono gli altri interventi attuati. Da evidenziare come l'attivazione di legali, interni o esterni, e di investigatori siano agli ultimi posti. Nella voce "Altro" sono stati indicati il cambio delle password e la richiesta di informazioni per assicurazioni sul rischio informatico.

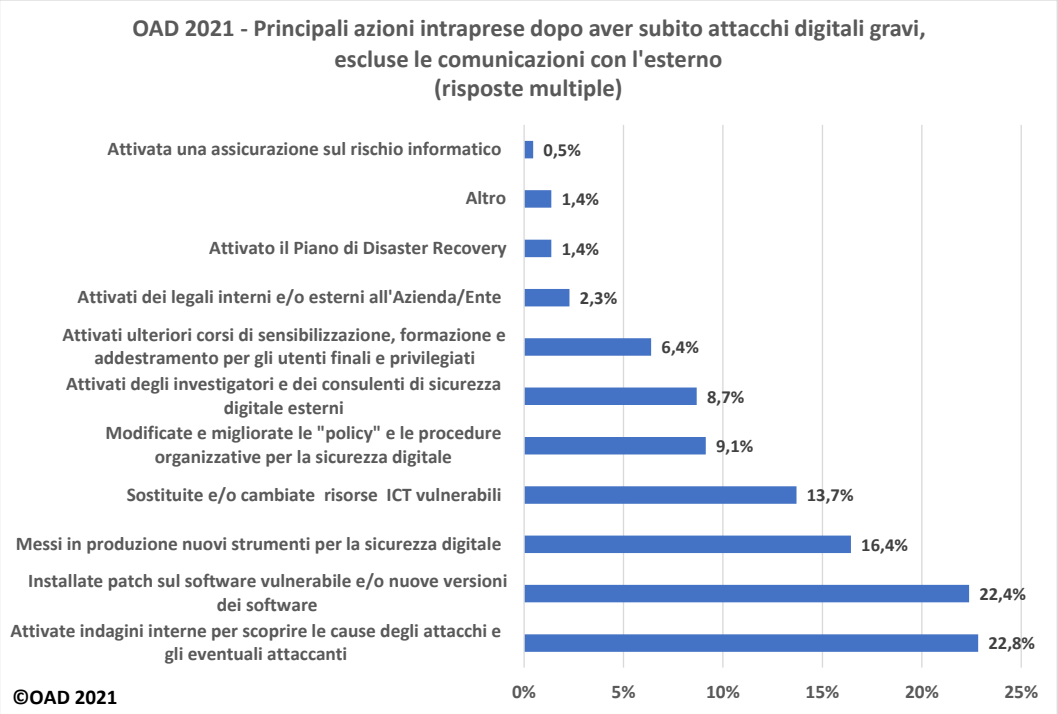
OAD 2021 - Principali azioni intraprese dopo aver subito attacchi digitali gravi, escluse le comunicazioni con l'esterno (risposte multiple)
Attivata una assicurazione sul rischio informatico
0,5%
Altro
1,4%
Attivato il Piano di Disaster Recovery
1,4%
Attivati dei legali interni e/o esterni all'Azienda/Ente
2,3%
Attivati ulteriori corsi di sensibilizzazione, formazione e addestramento per gli utenti finali e privilegiati
6,4%
Attivati degli investigatori e dei consulenti di sicurezza digitale esterni
8,7%
Modificate e migliorate le "policy" e le procedure organizzative per la sicurezza digitale
9,1%
Sostituite e/o cambiate risorse ICT vulnerabili
13,7%
Messi in produzione nuovi strumenti per la sicurezza digitale
16,4%
Installate patch sul software vulnerabile e/o nuove versioni dei software
22,4%
Attivate indagini interne per scoprire le cause degli attacchi e gli eventuali attaccanti
22,8%
0%
5%
10%
15%
20%
25%
©OAD 2021

Fig. 4.1-4

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

La fig. 5-1 mostra che, percentualmente sul bacino di aziende/enti rispondenti e con risposte multiple, la tipologia di attacco più temuta nel prossimo futuro è l'uso non autorizzato di sistemi ICT, con il 27,4%, seguita con il 25,1% dall'attacco ai sistemi di IAA, Identificazione-Autenticazione-Autorizzazione.

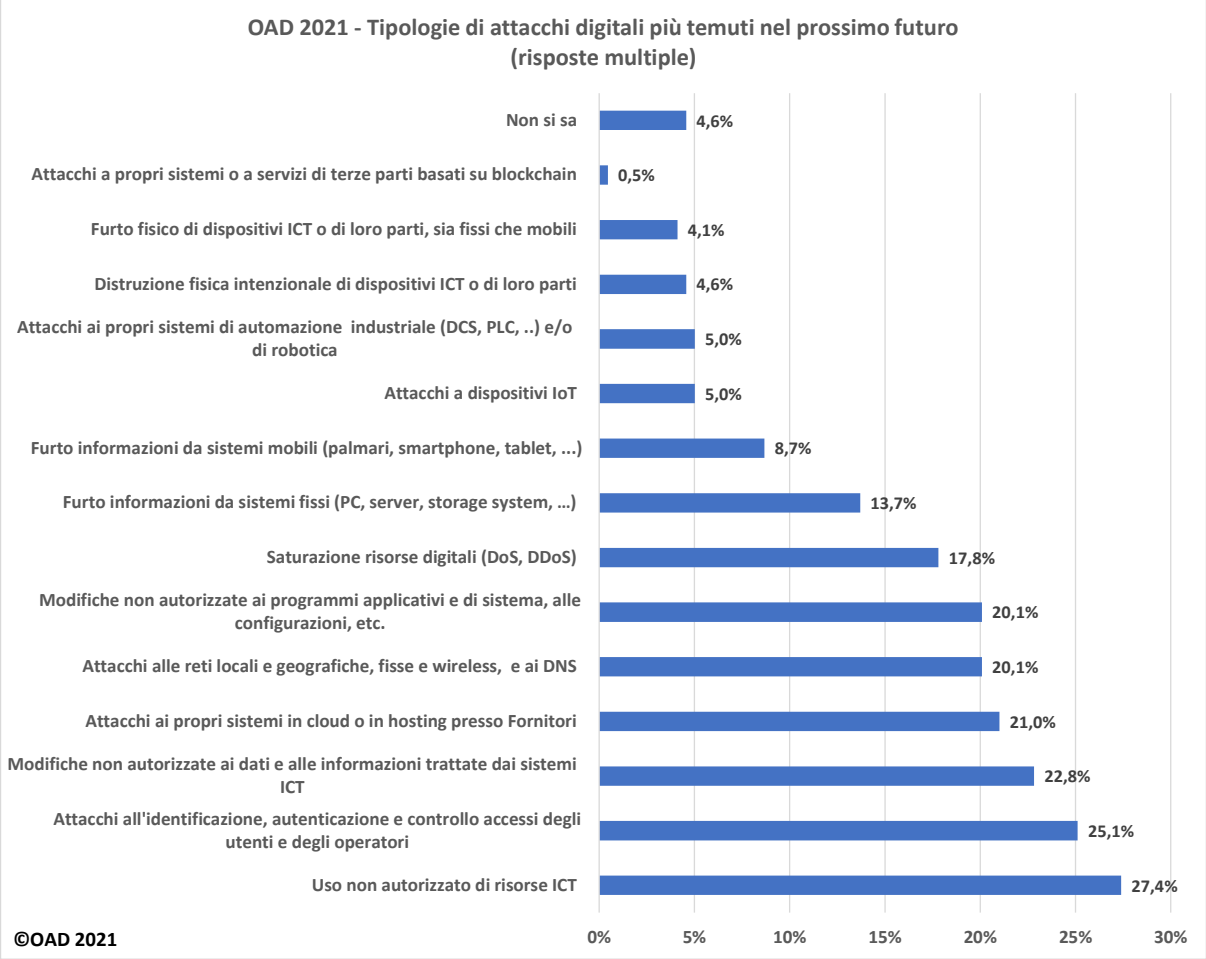

Fig. 5-1

Scendono a scalare i timori per le altre tipologie di attacco. Si deve sempre tener conto che alcuni dei SI dell'indagine non usano sistemi terziarizzati /cloud, e non includono specifiche tecnologie e soluzioni digitali, quali IoT, sistemi di automazione industriale robotica, blockchain, dato che le aziende/enti rispondenti non hanno bisogno o usano questi tipi di attività/processi.

Il 4,6% delle/dei rispondenti ai due questionari ha preferito non sbilanciarsi, ed ha selezionato la risposta "non so". Come nelle indagini precedenti, le/i rispondenti temono soprattutto attacchi che già hanno subito, e la classifica in fig. 5-1 esprime soprattutto questo timore. Interessante evidenziare come gli attacchi digitali ai propri sistemi e servizi ICT terziarizzati, e quindi anche in cloud, si posizioni al quarto posto con un non trascurabile 20%: una chiara indicazione che gli outsourcer, ed in particolare i provider di servizi cloud, sono anch'essi vulnerabili, e soprattutto possono essere un target importante per gli attaccanti. In controtendenza rispetto agli attacchi subiti, gli attacchi alla sicurezza "fisica" per i dispositivi ICT.

La fig. 5-2, con risposte multiple, mostra le famiglie di tecniche di attacco digitale più temute nel prossimo futuro. Come facilmente prevedibile, la tecnica più temuta, per il 33,3%, è il malware, seguita a brevissima

distanza percentuale dalla raccolta di informazioni non autorizzata, con un 32,9%. E' bene sottolineare che la raccolta di informazioni include social engineering, phishing, pharming, hoax, scanning, indagini su Internet, ecc. Seguono a scalare, ma con diversi punti di differenza, le altre famiglie di tecniche considerate.
La fig. 5-3, sempre con risposte multiple, riporta le possibili motivazioni che le/i rispondenti ipotizzano per gli attacchi digitali del prossimo futuro. In cima alla lista le frodi, con un 38,4%, seguita dalle ritorsioni, tipiche dei ransomware ancora assai diffusi in Italia.

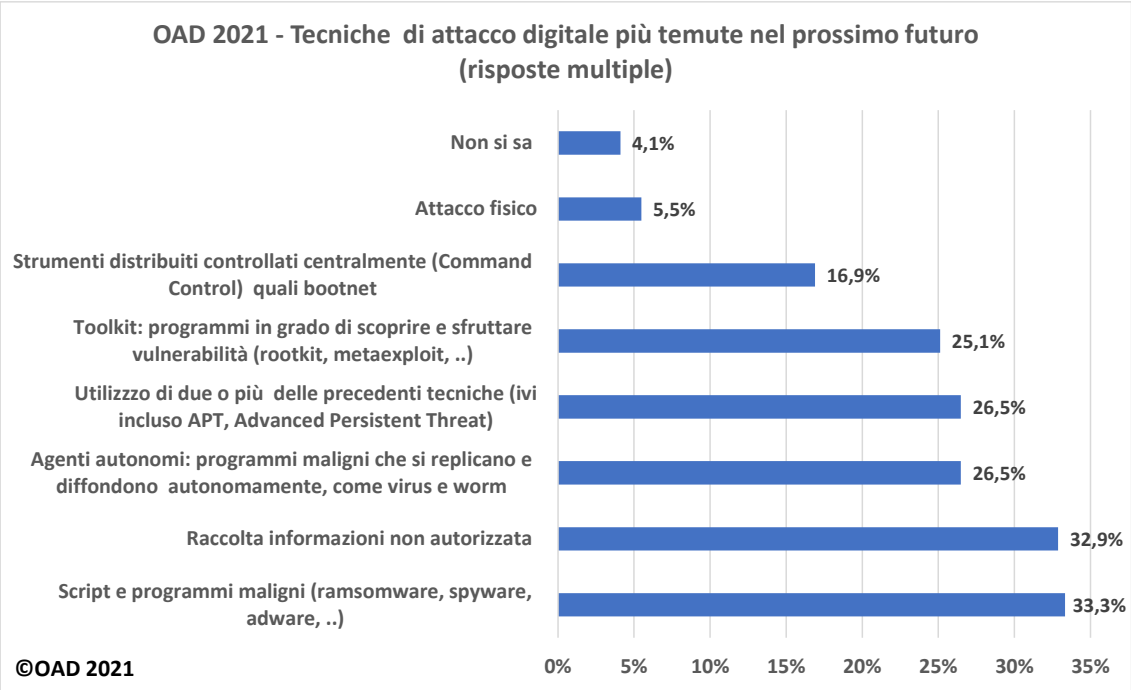

Fig. 5-2

Le altre probabili motivazioni scalano con diversi punti percentuali di scarto. All'ultimo posto, con la voce "altro", è stata indicata la guerra cibernetica, in inglese cyber warfare. Si deve ricordare che la presente indagine online copriva l'intero anno 2020 ed il 1° semestre 2021, quando ancora erano minimali, e considerati "normali" gli attacchi digitali verso l'Ucraina ed altri paesi occidentali, che furono invece il preludio all'invasione dell'Ucraina e le prime mosse della relativa cyber warfare. Inoltre a questa indagine hanno risposto relativamente pochi enti finanziari e quasi nessuna PA, che sono i primi target di una guerra informatica.

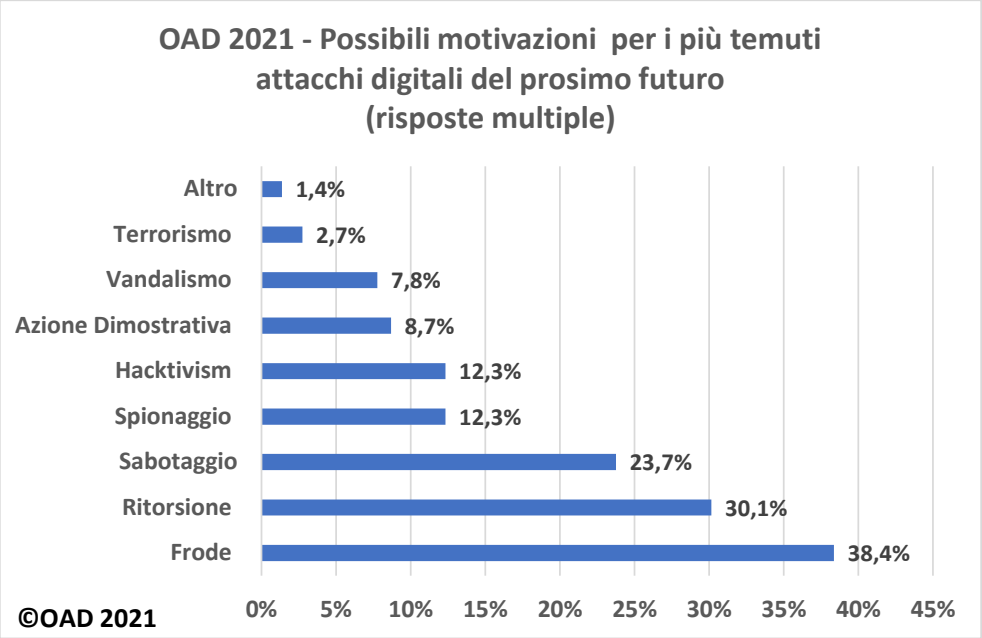
OAD 2021 - Possibili motivazioni per i più temuti attacchi digitali del prosimo futuro (risposte multiple)
Altro
1,4%
Terrorismo
2,7%
Vandalismo
7,8%
Azione Dimostrativa
8,7%
Hacktivism
12,3%
Spionaggio
12,3%
Sabotaggio
23,7%
Ritorsione
30,1%
Frode
38,4%
0%
5%
10%
15%
20%
25%
30%
35%
40%
45%
©OAD 2021

Fig. 5-3

6. Il campione delle Aziende/Enti rispondenti e dei loro SI emerso dall'indagine

Le risposte avute e sommate dei due questionari 2021 sono state 221, rispetto alle 310 di OAD 2020, alle 296 di OAD 2019 e alle 269 di OAD 2018. Con OAD 2021 la crescita degli anni precedenti si è bruscamente interrotta, nonostante la creazione di un questionario "ridotto" che richiedeva la metà del tempo per la sua compilazione, ed una ben più estesa promozione sia diretta da parte di AIPSI e Malabo, sia tramite le associazioni patrocinanti. Il motivo, come già indicato nei capitoli precedenti, è probabilmente dovuto all'impegno dei potenziali rispondenti oberati di lavoro per cercare di far fronte alla timida ripresa negli ultimi mesi del 2021, e da una certa intrinseca difficoltà a rispondere, seppur in maniera strettamente anonima, alle domande dei due questionari.
La difficoltà nel far rispondere ha causato il forte ritardo nella pubblicazione del presente rapporto finale, che ha dovuto attendere, prima ancora della sua stesura completa, il raggiungimento di un numero accettabile di compilazioni per essere in grado di fornire indicazioni e trend attendibili sugli attacchi digitali intenzionali ai Sistemi Informativi (SI) in Italia e su quali sono le principali misure di contrasto messe in atto.

6.1 Ruolo della/del rispondente nell'azienda/ente

La fig. 6.1-1 mostra la ripartizione % dei compilatori dei questionari OAD 2021 per ruolo: al primo posto, in percentuale, il CIO o altre figure all'interno dell'UOSI, Unità Organizzativa Sintemi Informativi. Al terzo posto come rispondente una figura di vertice dell'azienda/ente. Per le piccole e piccolissime organizzazioni è il vertice che decide sul SI e sul suo budget, e che di fatto coordina e supervisiona i fornitori ed i consulenti che vi operano. I CISO, Chief Information Security Officer, i responsabili della sicurezza digitale, che dovrebbero essere i rispondenti più diffusi, sono al quinto posto con un 12,4% sul totale. Tale dato conferma che in Italia questo ruolo è formalizzato e ben definito prevalentemente nelle grandi organizzazioni ed in quelle per le quali il SI e la sua sicurezza digitale sono fondamentali per il business. Si deve inoltre tener conto che in talune organizzazioni l'UOSI dipende dal Responsabile Tecnologie, il CTO (Chief Technology Officer) ed in altre il Responsabile Sicurezza per l'intera Azienda/Ente (CSO, Chief Security Officer) è anche responsabile della sicurezza digitale, e svolge quindi il ruolo, o ne è il superiore, del CISO. All'ultimo posto i consulenti e/o il personale di terze parti che svolgono, in parte o in toto, la gestione della sicurezza digitale. Anche questo dato conferma che la terziarizzazione della gestione della sicurezza digitale, o di una sua parte, è ancora limitata in Italia, come discusso in §3.4.1. La stragrande maggioranza di imprese private e pubbliche è costituita da poche persone che non sono in grado, salvo rare eccezioni, di avere le adeguate competenze multidisciplinari necessarie per la sicurezza digitale, e più in generale per il loro SI. Da questo deriverebbe la convenienza di terziarizzare a persone/società dedicate e specializzate in questo specifico campo, sfruttando servizi quali MSS, Managed Security Services, e CSaaS, Cyber Security as a Service. Il problema, per la realtà italiana, deriva (a giudizio dell'autore) da un lato dall'effettiva consapevolezza da parte dei vertici delle aziende/enti sul serio problema della sicurezza digitale, dall'altro dalla effettiva difficoltà nello scegliere l'interlocutore/fornitore adeguato a risolvere problemi che il decisore ha difficoltà a seguire e "governare". Ma è il medesimo problema nella "giusta scelta" di qualsiasi fornitore ICT o non, e più in generale di un qualsiasi professionista, dal medico al commercialista, dall'avvocato all'amministratore condominiale.
Importante evidenziare che al terzo posto, con un 15,5%, delle figure rispondenti ai questionari sono le persone di vertice dell'azienda/ente: soprattutto per le piccole realtà sono loro che si occupano anche del SI e della sua sicurezza digitale.

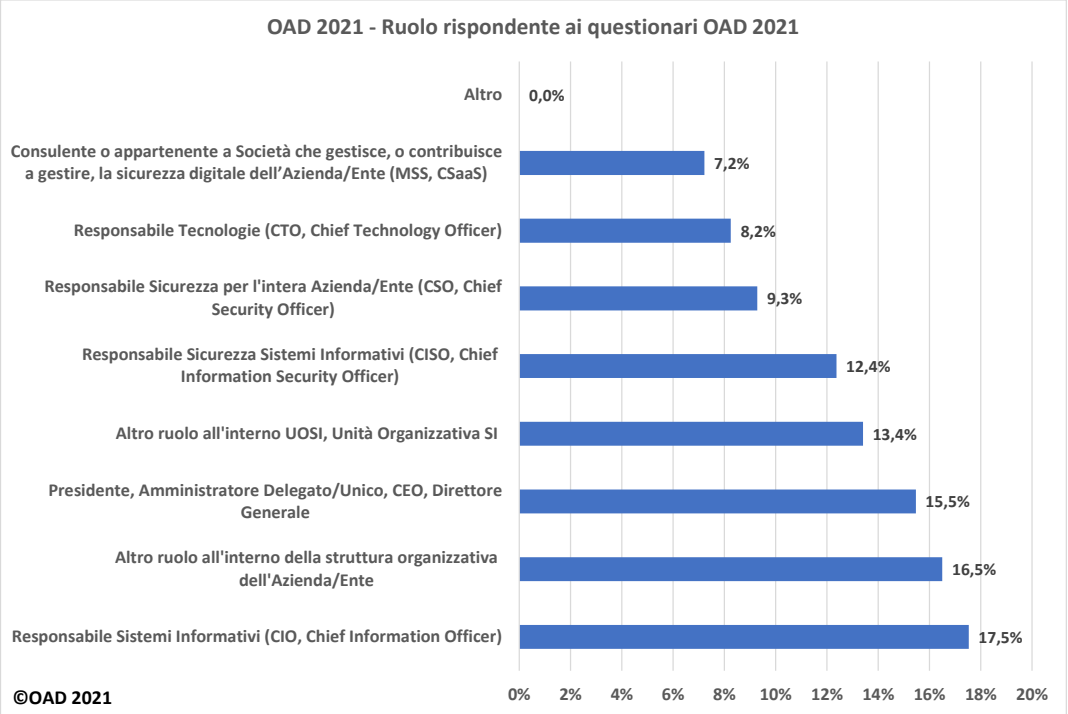

Fig. 6.1-1

6.2 L'Azienda/Ente rispondente

La fig. 6.2-1 riporta la tabella con i raggruppamenti dei settori merceologici considerati da OAD: essa fa riferimento alla classificazione ATECO[14], 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 necessaria per ridurre possibili errori di posizionamento dell'azienda/ente da parte delle/dei rispondenti, come era successo nei primi anni dell'indagine OAI/OAD.
La fig. 6.2-2 mostra la ripartizione % nei gruppi merceologici considerati (fig. 6.2-1) delle Aziende/Enti rispondenti. Due considerazioni emergono dai dati di questa figura: il bacino di rispondenti emerso copre tutti i settori merceologici considerati, PA incluse, ma solo il raggruppamento merceologico ICT ha avuto il maggior numero di compilazioni. Tutti gli altri raggruppamenti merceologici hanno avuto poche compilazioni. Le relativamente poche compilazioni non hanno permesso di effettuare specifiche analisi per settore, in quanto non sufficientemente rappresentative, in termini statistici, del settore, nemmeno per l'ICT: nel loro insieme sono state comunque valide e sufficienti per fornire una fotografia sulla attuale situazione e sui trend degli attacchi digitali in Italia, come analizzato in §4.
La fig. 6.2-3 mostra la ripartizione delle aziende/enti rispondenti in base al numero di loro dipendenti. In entrambi i questionari 2021 sono state considerate tre classi per organizzazioni con meno di 250 dipendenti, nell'ambito privato le PMI, Piccole Medie Imprese: fino a 10, tra 11 e 50, tra 51 e 250. Per le organizzazioni maggiori dimensioni si sono considerate analogamente tre classi: tra 251 e 1000, tra 1001 e 5000, con più di 5000 dipendenti. Il campione emerso dall'indagine OAD 2021 appartiene per il 71,2% a strutture fino a 250 dipendenti, praticamente tutte PMI (date le pochissime risposte avute dalle PA). Per le grandi organizzazioni, le percentuali decrementano per le tre classi considerate. Complessivamente il campione emerso rappresenta un buon mix della realtà italiana, pur con i limiti evidenziati in precedenza.

[14] ATECO, ATtività ECOnomiche, è la classificazione delle attività economiche in settori merceologici adottata dall'ISTAT per le rilevazioni statistiche nazionali di carattere economico. Si veda: https://ateco.infocamere.it/ateq20/#!/home

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. 6.2-1

La fig. 6.2-4 confronta i dati di cui sopra per classi di dipendenti con i più recenti dati forniti da ISTAT, già considerati in §3.5.1: si noti come ISTAT consideri una sola classe di addetti al di sopra delle 250 persone.
La fig. 6.2-5 mostra la ripartizione percentuale delle aziende/enti rispondenti per fatturato annuo (o l'analogo del fatturato per le pubbliche amministrazioni) nell'ultimo anno disponibile.
Nell'indagine 2021 sono state modificate, ampliandole, le classi di fatturato cui fare riferimento, portandole a 5[15]: fino a 1 Mln €, da 1 a 5 Mln €, da 5 a 10 Mln €, da 10 a 50 Mln €, oltre i 50 Mln €.

[15] Nelle precedenti indagini OAD erano considerate le seguenti 4 classi: fino a € 500.000, da € 500.000 a 1 Mln €, da 1 a 5 Mln €, oltre i 5 Mln €.

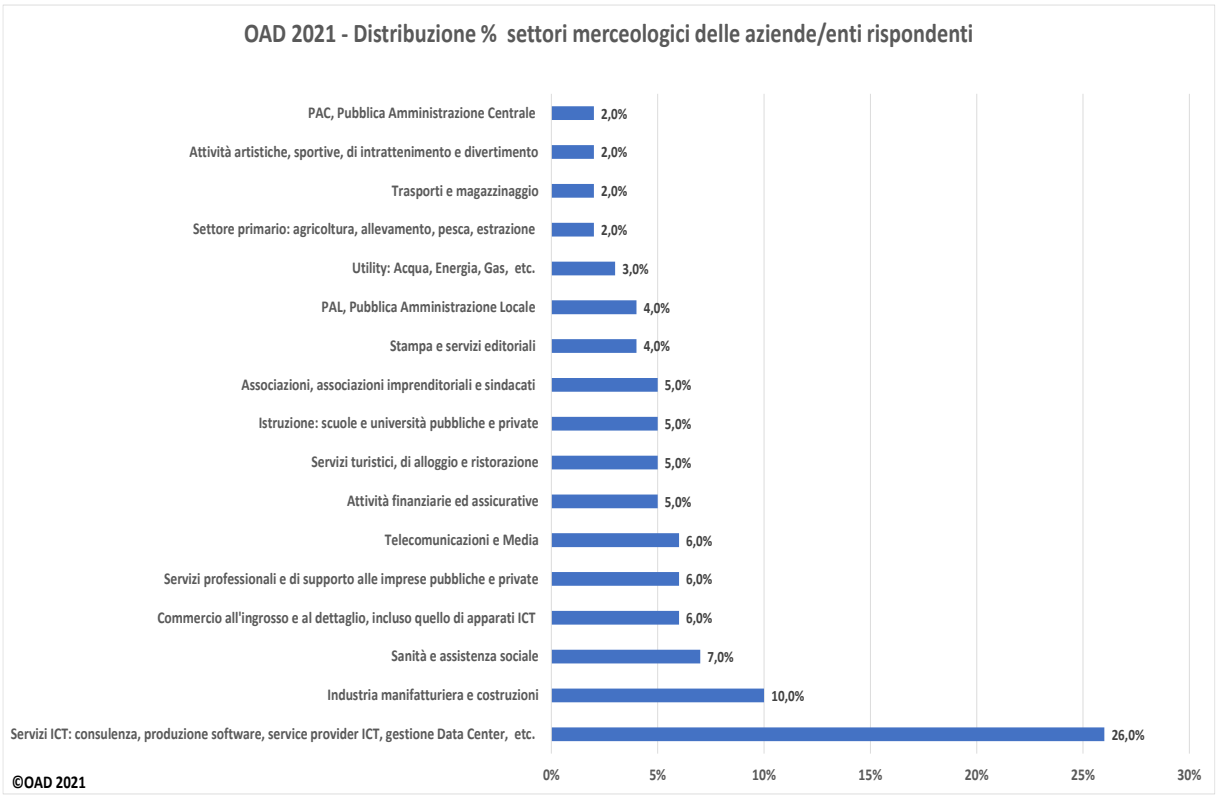

Fig. 6.2-2

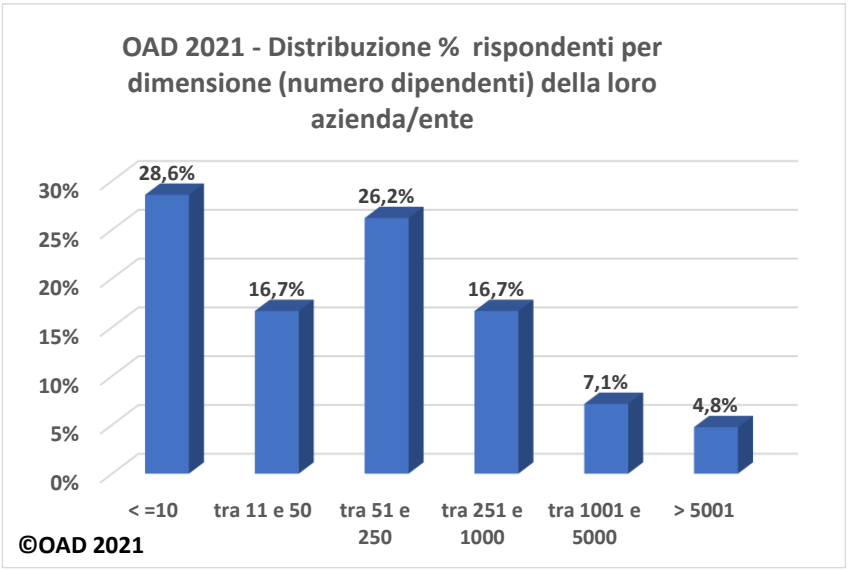

Fig. 6.2-3

Classi di addetti Imprese private	Dati ISTAT (%)	Rispondenti OAD 2021 (%)
< =10	95,68%	28,6%
tra 11 e 50	3,69%	16,7%
tra 51 e 250	0,53%	26,2%
tra 251 e 1000	0,10%	16,7%
tra 1001 e 5000		7,1%
> 5001		4.8%

Fig. 6.2-4

La fig. 6.2-6 mostra la distribuzione percentuale di dove si trovala principale sede del SI dell'azienda/ente, per regione italiana, sia esso il principale Data Center o la principale "computer room". Quasi ¼ ha sede in Lombardia, seguito, ma con una % assai inferiore, da Piemonte e Lazio. Sono presenti, con % decrescenti, tutte le regioni. Così come per i vari settori merceologici, tale copertura è dovuta allo sforzo di AIPSI e di Malabo di far rispondere ad uno dei questionari aziende/enti di diverse regioni ed appartenenti a diversi settori merceologici. Con OAD 2021 almeno l'obiettivo della copertura per regioni italiane e per settori è stato raggiunto.

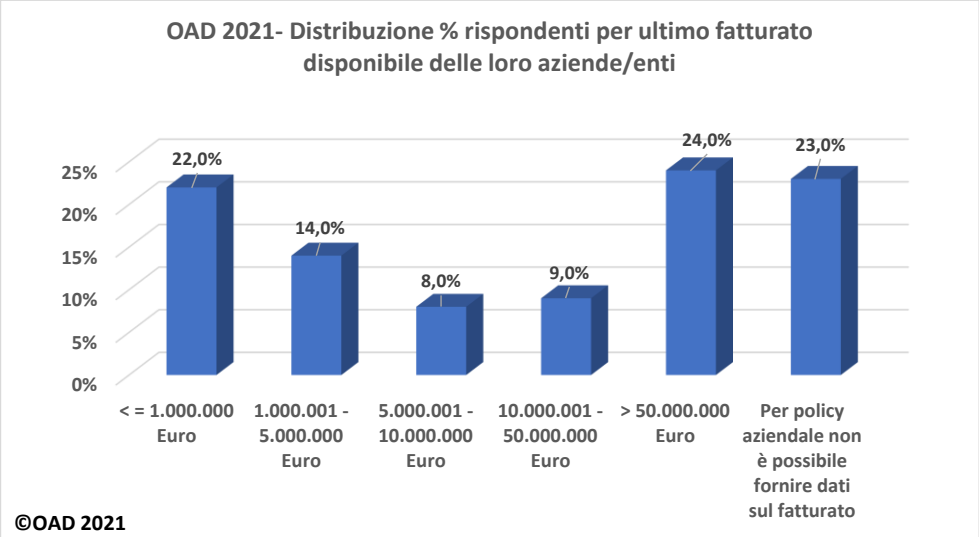

Fig. 6.2-5

Una risposta selezionabile nell'indagine 2021 era relativa all'impossibilità di fornire questo dato, anche se assai generico, per divieto dell'azienda/ente: il 23% delle/dei rispondenti ha selezionato questa risposta. Sempre la fig. 6.2-5 evidenzia come la maggior parte dei rispondenti si suddivida in aziende/enti con fatturati inferiori al milione di €, il 22%, e quelle con fatturati > 50 Mln €, che rappresentano il 24% del totale. In pratica il bacino emerso vede la maggior parte di aziende/enti rispondenti suddivise tra quelle piccole con bassi fatturati e quelli grandi con elevati fatturati. Minore, percentualmente, la presenza di quelle con fatturati intermedi tra questi due estremi.

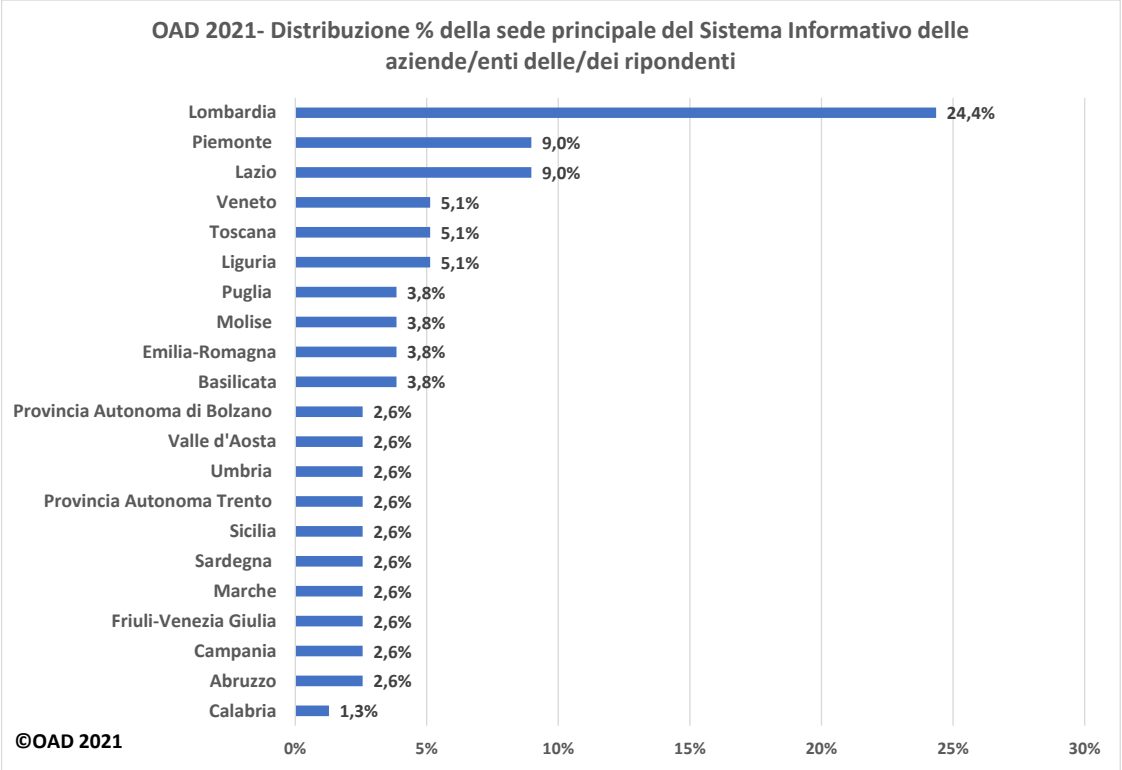

Fig. 6.2-6

In termini di copertura geografica delle attività dell'azienda/ente rispondente, la fig. 6.2-7 indica che il 79% opera in Italia, e di questi il 30% nel solo nord Italia, mentre il 21% opera a livello internazionale, sia in Europa sia nel resto del mondo.

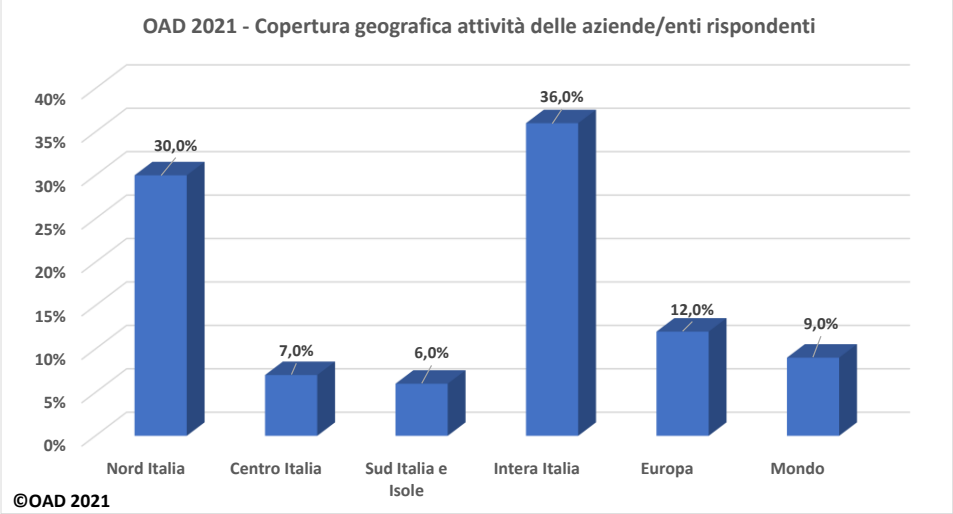

Fig. 6.2-7

6.3 Tipologia, ruolo e principali caratteristiche dei Sistemi Informativi (SI) delle aziende/enti rispondenti

In questo paragrafo vengo illustrate le principali caratteristiche dei SI delle aziende/enti rispondenti ai questionari di OAD 2021. Tali caratteristiche sono volutamente generali, l'approfondimento sulle misure di sicurezza digitale in atto nei vari SI sono dettagliate in §7.

La fig. 6.3-1 mostra che per il 43,2% di rispondenti il SI è di medie piccole dimensioni, non ha un Data Center, ed è gestito e controllato totalmente in Italia. Invece per il 53,4% di rispondenti il SI è di grandi dimensioni con almeno uno (o più) Data Center. Per il 22,1% il SI è di grandi dimensioni ed opera per una multinazionale, e copre quindi varie nazioni: di questi l'8,5% è gestito e controllato dall'Italia.

Per meglio comprendere il fabbisogno di sicurezza digitale per il SI oggetto delle risposte ai due questionari, è importante conoscere, almeno a livello qualitativo, quale è la sua strategicità per il business e per le attività dell'azienda/ente rispondente. La fig. 6.3-2 evidenzia che per i 2/3 delle aziende/enti rispondenti il SI è essenziale per il funzionamento delle loro attività e dei loro processi. E per questo motivo la sicurezza digitale del SI deve essere di alto livello, come rilevato ed analizzato in §7.

La fig. 6.3-3 mostra che il 86,8% dei SI delle aziende/enti rispondenti tratta dati personali, e di questi il 50% tratta dati sensibili. Meno del 10% dichiara che i SI non trattano dati personali, ed il 4,4% dichiara di non saper rispondere. Questa risposta è stata data prevalentemente nel questionario ridotto da pochi rispondenti con specifiche ma limitate competenze nell'ICT nella sicurezza digitale. Questa stessa ragione è applicabile ai "non so" o "non si sa"[16] selezionati anche per successivi temi sulle pur generiche caratteristiche del SI oggetto delle risposte ai questionari.

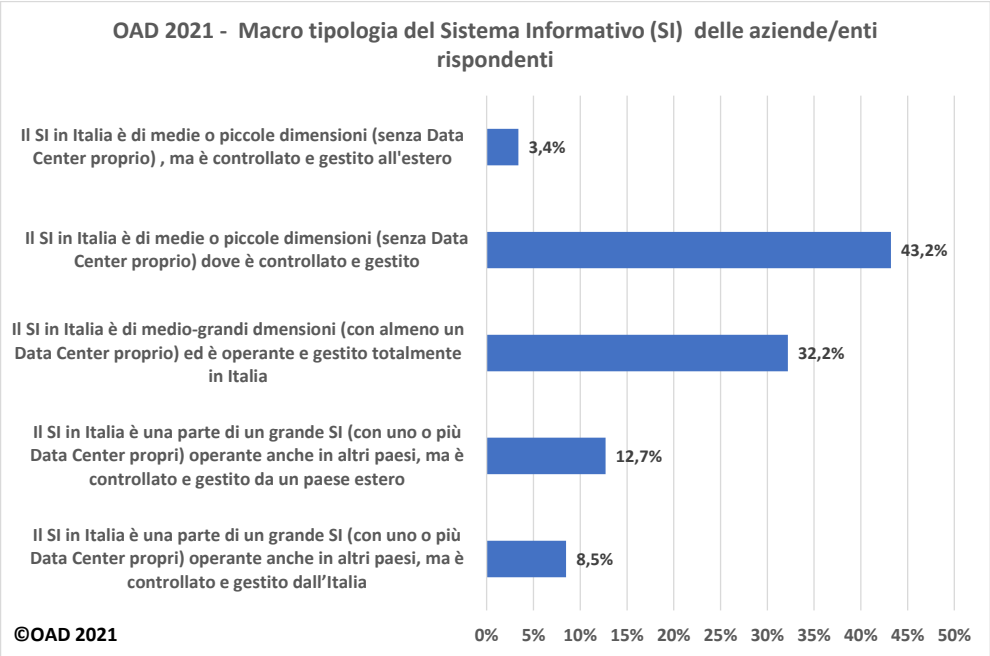

Fig. 6.3-1

[16] Le due possibili risposte legate al "non sapere" hanno una differente logica:

- la risposta "non so" dovrebbe indicare che la/il rispondente non conosce, a livello personale, il tema oggetto delle risposte;
- la risposta "non si sa" dovrebbe indicare che la/il rispondente non ha avuto specifiche informazioni dall'azienda/ente sul tema, dato che queste informazioni sono riservate o comunque non accessibili da livelli come quelli della/del rispondente.

E' assai probabile che in molti casi queste risposte saranno state date senza questa precisa distinzione: e questo vale anche per tutte le altre domande dei due questionari OAD 2021.

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. 6.3-4 mostra quali SI dei rispondenti trattano informazioni critiche e riservate, oltre a quelle personali soggette alla normativa sulla privacy, e che come tali richiedono un elevato livello di protezione digitale. Il 44,7% dei SI tratta informazioni critiche e riservate, il 49,1% informazioni necessarie ed importanti al funzionamento dell'azienda/ente, ma non ritenute molto critiche.

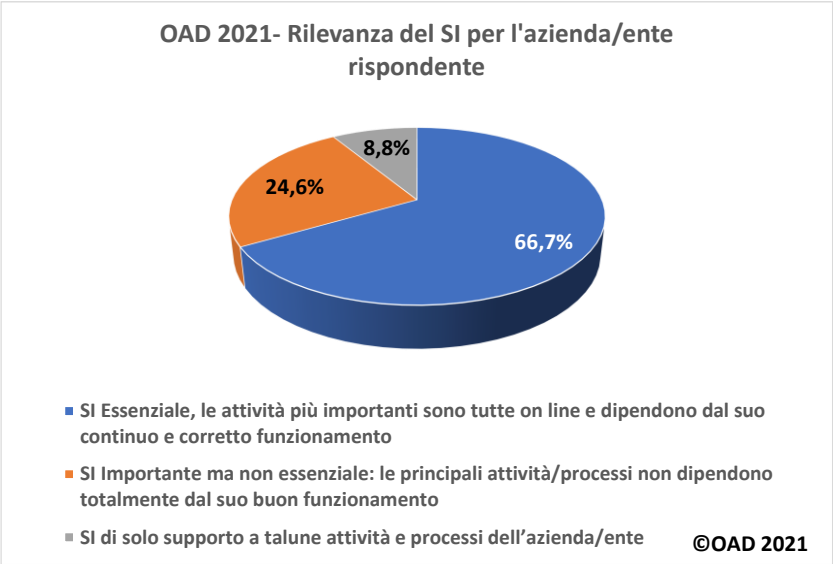

Fig. 6.3-2

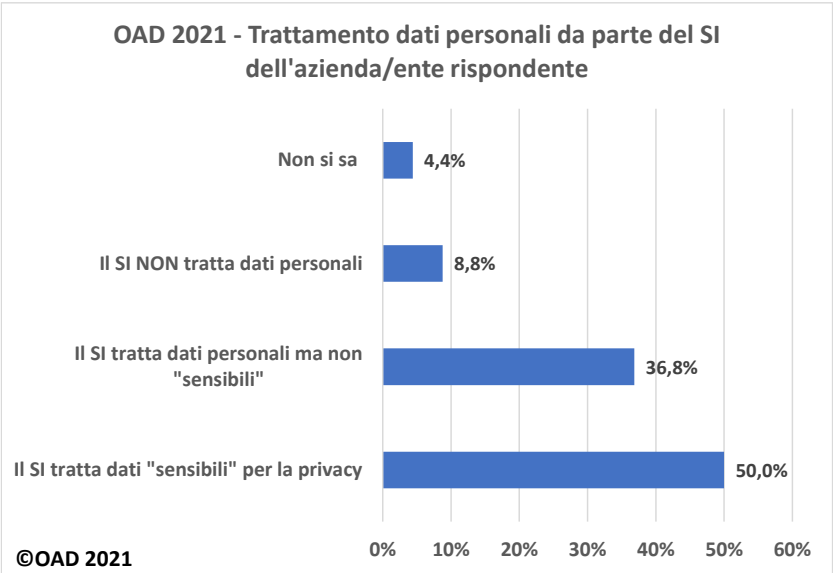

Fig. 6.3-3

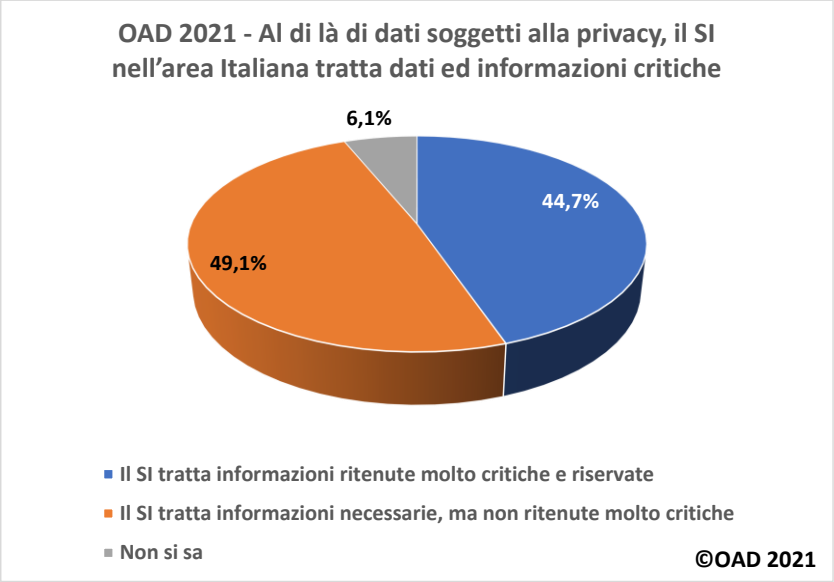

Fig. 6.3-4

La fig. 6.3-5 evidenzia che quasi l'80% dei SI delle aziende/enti rispondenti utilizza servizi e sistemi ICT terziarizzati. Questo dato è molto significativo come trend, dato che è man mano cresciuto negli anni, a partire dal 2007.

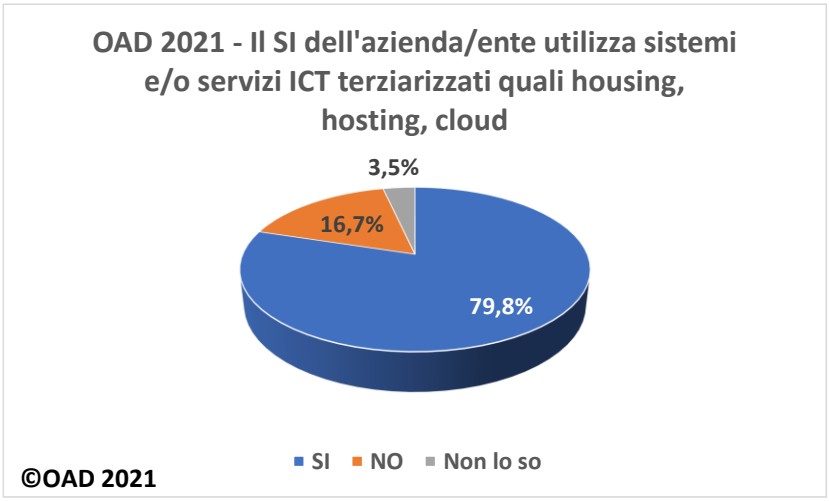

Fig. 6.3-5

Dato che la terziarizzazione dei sistemi e dei servizi ICT, in particolare con il cloud, è un elemento che fortemente caratterizza un SI e la sua sicurezza digitale, si è voluto correlare questo dato con le classi di dipendenti ed il fatturato delle aziende/enti rispondenti. Si deve tener conto che le % emerse da tali correlazioni dipendono anche dal numero di compilazioni ricevute per dimensioni e per giro d'affari (fatturato) delle aziende/enti rispondenti: altrimenti le % emerse possono essere fuorvianti. La principale considerazione che emerge dalle fig. 6.3-6 e 6.3-7 è che l'uso di servizi ICT terziarizzati è ormai diffuso in tutte le tipologie di aziende/enti, ma che le organizzazioni più piccole, e con minor fatturato, ne usino percentualmente in misura inferiore rispetto alle grandi. Attenzione inoltre a distinguere tra l'uso di sistemi e servizi terziarizzati e in cloud, assai diffusa, e l'uso della gestione terziarizzata della sicurezza digitale più avanti considerata.

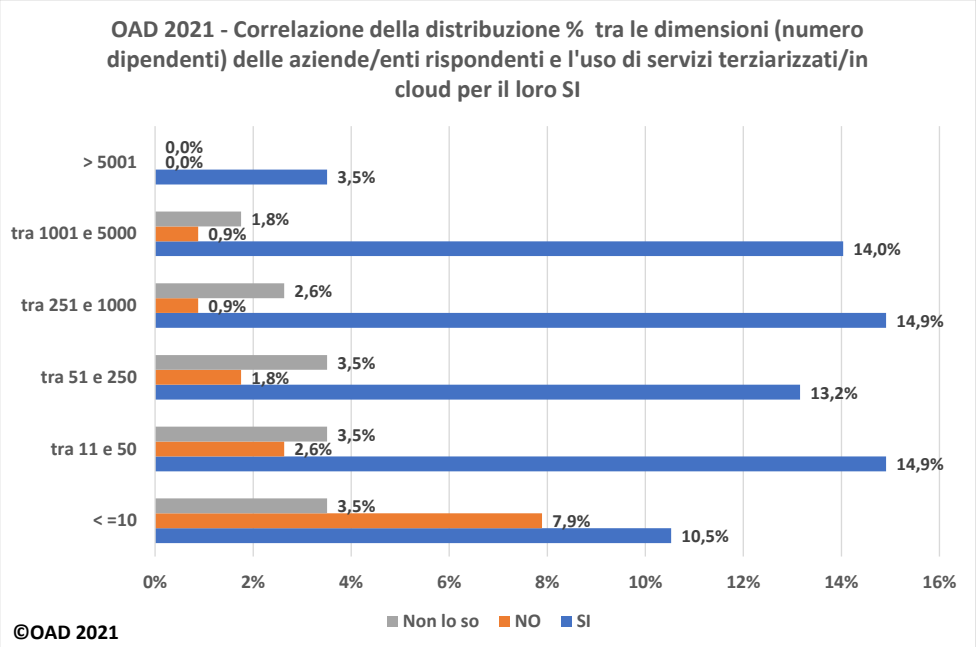

Fig. 6.3-6

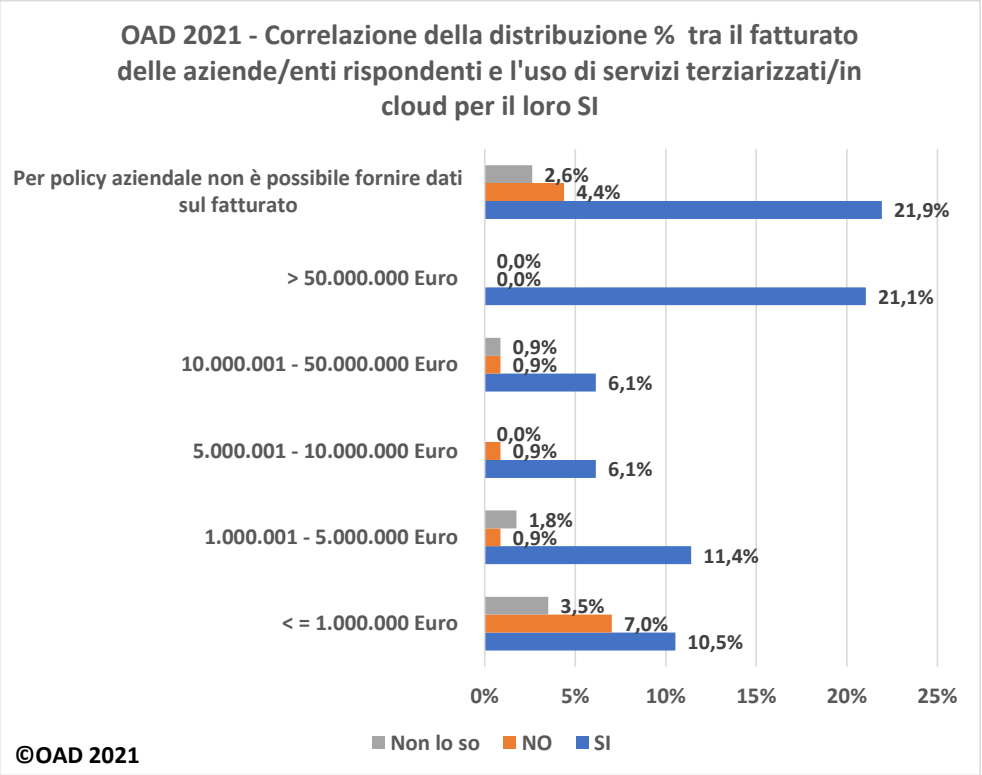

Fig. 6.3-7

E' infatti crescente l'importanza, in termini di terziarizzazione, della gestione operativa dell'intero SI e della sua sicurezza digitale. La gestione operativa terziarizzata del SI include tipici servizi quali (elenco non esaustivo) il continuo monitoraggio e controllo, sia funzionale sia prestazionale, delle varie unità del SI, apparati di rete inclusi, la gestione delle varie unità a livello hardware e software (aggiornamenti, patch e fix, gestione segnalazioni ed allarmi di sistema, etc.), la gestione delle applicazioni, la gestione degli utenti e del

provisioning per i nuovi utenti, la gestione dei back-up e l'eventuale ripristino, la gestione dell'help desk – trouble ticketing, la predisposizione e la gestione del Disaster Recovery, la gestione dei log dei sistemi e degli utenti finali/privilegiati, la gestione dei problemi e degli incidenti, etc. In numerosi casi nella terziarizzazione dell'ICT è inclusa anche la gestione operativa della sicurezza digitale per i sistemi/servizi ICT terziarizzati, e per la quale entrambi i questionari avevano predisposto una specifica domanda.
La fig. 6.3-8 mostra che il 45,6% delle aziende/enti gestiscono internamente (on premise) l'intero SI, mentre la metà esatta dei SI, il 50%, terziarizza in toto o in parte la sua gestione operativa. In tale ambito solo l'8,8% terziarizza in toto tale gestione, il resto usa una soluzione ibrida.
La terziarizzazione della gestione operativa della sicurezza digitale del SI è talvolta integrata nella gestione dell'intero SI di cui alla precedente figura, ma più sovente è attuata separatamente tramite aziende e consulenti specializzati. Con il crescere dell'importanza della sicurezza digitale, sta crescendo il mercato di questo tipo di terziarizzazione, indicato in inglese con i termini MSS e CSaaS.
MSS, Managed Security Services, indica la gestione terziarizzata dei servizi di sicurezza digitale. La terziarizzazione di questi servizi può essere totale o parziale, ed erogata da uno o più consulenti, o da una o più aziende specializzate. Può inoltre essere svolta con strumenti informatici inseriti all'interno del SI del cliente stesso, o esterni, di proprietà dei e/o utilizzati dalle terze parti coinvolte.
CSaaS, CyberSecurity as a Service, fa riferimento ai servizi di sicurezza digitale erogati in cloud, e che possono essere gestiti direttamente da chi si occupa della sicurezza digitale del SI, dal personale interno all'azienda/ente o dal personale esterno di terze parti, quali consulenti e società che li gestiscono in nome e per conto dei responsabili del Sistema Informativo del cliente.

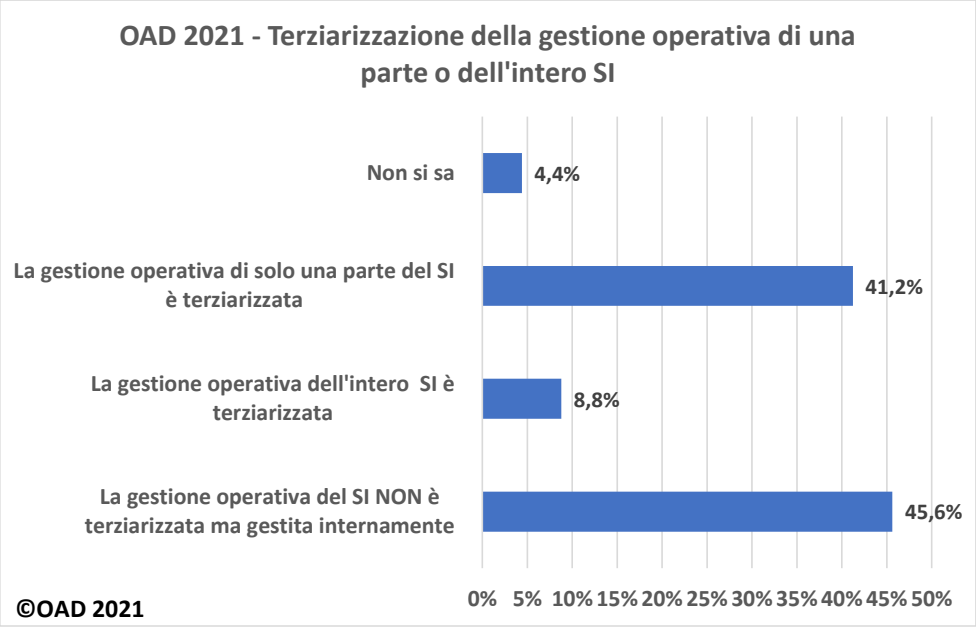

Fig. 6.3-8

I questionari OAD 2021 non entravano in questi dettagli, ponendo specifiche domande su MSS e CSaaS, ma richiedevano solo se la gestione della sicurezza digitale è, in toto o in parte, terziarizzata.
La fig. 6.3-9 fornisce i risultati emersi: poco più della metà dei SI, 50,4%, ha terziarizzato in parte o in toto la gestione operativa della sicurezza digitale. Il 12,4% l'ha terziarizzata in toto, ed è un valore superiore all'8,8% dell'analogo valore per la gestione totalmente terziarizzata del SI. Questi dati indicano che la terziarizzazione della gestione della sicurezza digitale, almeno per il bacino dei SI dell'indagine, sta consolidandosi.

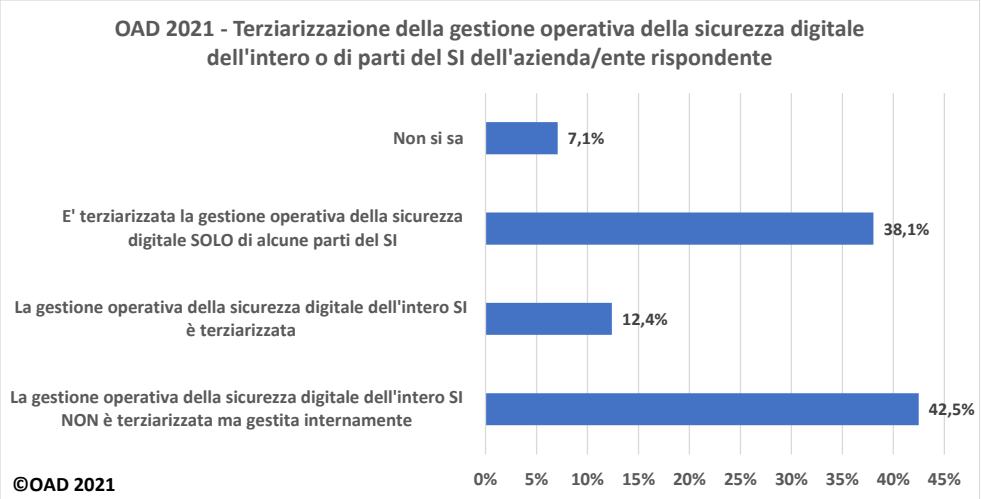

Fig. 6.3-9

Un'ultima considerazione sulla terziarizzazione della gestione operativa della sicurezza digitale: essa può e deve essere terziarizzata, in particolare per le piccole strutture, ma a condizione che sia terziarizzata alle corrette condizioni tecniche, economiche e normative, che sia trasparente e controllabile: in una parola che sia un "right-sourcing", un giusto approvvigionamento.

Cap. 7 Le misure di sicurezza digitale adottate nei Sistemi Informativi (SI) delle Aziende/Enti rispondenti

Il capitolo descrive gli strumenti di sicurezza in uso nei SI oggetto dell'indagine: le loro macro caratteristiche sono riportate nel precedente §6.3, così da poter meglio comprendere in quali ambiti e contro quali livelli di sicurezza digitale sono stati attuati gli attacchi rilevati ed analizzati in §4. Gli strumenti e le misure per la sicurezza digitale sono raggruppati in misure organizzative e in misure tecniche.
Il questionario "ridotto" di OAD 2021 ha ridotto e semplificato, rispetto a quello "competo", sia il numero di domande che di risposte su questo tema. Per entrambi i questionari, le domande e le relative preimpostate da selezionare, erano volutamente abbastanza generiche e non di dettaglio, sia per facilitare le risposte, sia per salvaguardare l'anonimato dell'aziende/ente rispondente. Questa parte dei questionari è sovente considerata da chi risponde come la più difficile ed ostica, dato che richiede una conoscenza almeno di base sulla sicurezza digitale per poter rispondere in maniera corretta e consapevole. Ma è altrettanto importante come la parte sugli attacchi digitali rilevati perché' fornisce chiare indicazioni su qaili misure, tecniche ed organizzative, sono in essere, e come, per contrastare gli attacchi.

7.1 Le misure organizzative per la sicurezza digitale in atto nei SI oggetto dell'indagine

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 come oneri burocratici e/o come spese di consulenza non necessarie: di interesse, di fatto, solo per le grandi organizzazioni. Al contrario, sono misure essenziali per l'effettivo funzionamento della sicurezza digitale, e necessarie per qualsiasi tipo di organizzazione, indipendentemente dalle sue dimensioni e dal settore merceologico cui appartiene, PA incluse: misure che devono però essere commisurate e calate nelle specifiche realtà di ogni azienda/ente.
Il regolamento europeo per la privacy, il GDPR[17], 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[18], 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 2021, 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.
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/smart working, ma prevalentemente con processi, procedure, logiche e modalità identiche a quelle applicate in ufficio anche per il lavoro da remoto, ossia da casa: perdendo così l'opportunità, almeno per il momento, di ripensare e riprogettare le modalità di lavoro

[17] Regolamento UE sulla privacy GDPR, UE 679/2016
[18] 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)

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.

7.1.1 La struttura organizzativa per la sicurezza digitale ed il ruolo di CISO nelle aziende/enti rispondenti

La prima misura organizzativa per la sicurezza digitale è la definizione ed assegnazione del ruolo e delle responsabilità di chi la deve gestire nell'ambito dell'azienda/ente, con la eventuale sua relativa struttura organizzativa. Il responsabile della sicurezza digitale, è indicato (anche nel seguito) con l'acronimo inglese CISO, Chief Information Security Officer. In Italia questo ruolo è ufficialmente definito ed attuato nelle medie grandi organizzazioni, nelle altre è prevalentemente espletato dal responsabile del SI, il CIO, o delegato a consulenti esterni.
La fig. 7.1.1-1 mostra che nel 38,8% delle aziende/enti rispondenti tale ruolo non è definito e/o attuato.
La fig. 7.1.1-2 mostra che nel bacino emerso di rispondenti la figura del CISO e la sua struttura organizzativa esistono sia nelle grandi che nelle piccole aziende/enti presente nelle piccole organizzazioni, come evidenziato dalle prevalenti barre blu, che indicano la presenza del ruolo nel grafico. La presenza significativa delle barre, in % rispetto al totale delle risposte raccolte, conferma che il campione emerso, con la presente indagine 2021, è di una fascia medio-alta nell'adozione delle misure di sicurezza, anche di tipo organizzativo.

Fig. 7.1.1-1

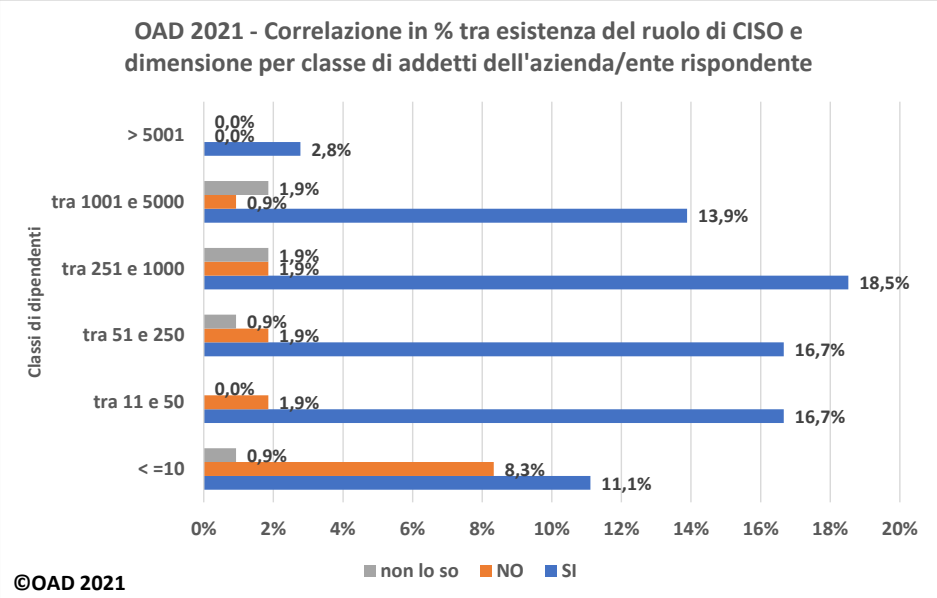

Fig. 7.1.1-2

La fig. 7.1.1-3 indica da chi dipende il CISO e la sua struttura organizzativa, per le realtà che hanno definito ed attuato ufficialmente tale ruolo. Tradizionalmente il CISO fa parte della struttura UOSI, Unità Organizzativa Sistemi Informativi, ed il 54% delle aziende/enti rispondenti ha attuato queta logica. Il posizionamento del CISO in ambito UOSI, e quindi sotto il CIO, di fatto lede 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 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[19].

[19] 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. 7.1.1-3

7.1.2 Policy e procedure organizzative per la sicurezza digitale

Una policy, nel contesto della sicurezza digitale, definisce le linee guida e gli indirizzi voluti e previsti, 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 può creare confusione, se non ben dettagliato.

Le procedure organizzative, da non confondere con le policy, sono operative e forniscono dettagliate istruzioni sia organizzative sia tecniche su come comportarsi per svolgere specifiche attività e per far fronte a determinate situazioni; sono rivolte sia alle persone che svolgono determinati ruoli, sia alle strutture organizzative che debbono espletare e/o controllare talune attività, funzioni e processi.

Sia le policy che 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 informativo con standard della famiglia ISO e best practice quali ITIL e COBIT.

Policy e procedure organizzative scritte, fatte conoscere ed aggiornate periodicamente, non sono da considerare una poco utile ma costosa burocrazia, e tantomeno 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 dell'intero SI o di sue parti. Sono inoltre essenziali per dimostrare l'accountability[20], così come richiesto ad esempio dal GDPR, e più in generale da varie leggi e normative, e non solo per l'ICT.

La fig. 7.1.2-1 evidenzia che la stragrande maggioranza delle aziende/enti rispondenti, il 79,6% ha definito ed usa policy e procedure organizzative per la sicurezza digitale, e di questi il 53,4% lo ha fatto solo per alcune misure e/o sue aree, generalmente quelle più necessarie o critiche; esempi tipici includono la gestione degli incidenti e dei problemi, la gestione dell'identificazioni ed autenticazione degli utenti, finali e/o privilegiati (che include anche la gestione delle password), la gestione dell'help desk e del "trouble ticketing".[21]

[20] Il termine "accountability" significa responsabilizzazione nei diversi ruoli assegnati: le persone che assumono un determinato ruolo sono tenute a dimostrare che le loro azioni ed attività sono coerenti con quanto richiesto (in funzione anche di eventuali normative in merito), che hanno piani ed iniziative per mettere in atto le idonee misure tecniche e organizzative, che possono comprovarne l'adeguatezza anche tramite adeguati strumenti.

[21] Il "trouble ticketing" è un'applicazione di supporto all'help/ervice desk 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 stessa 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.

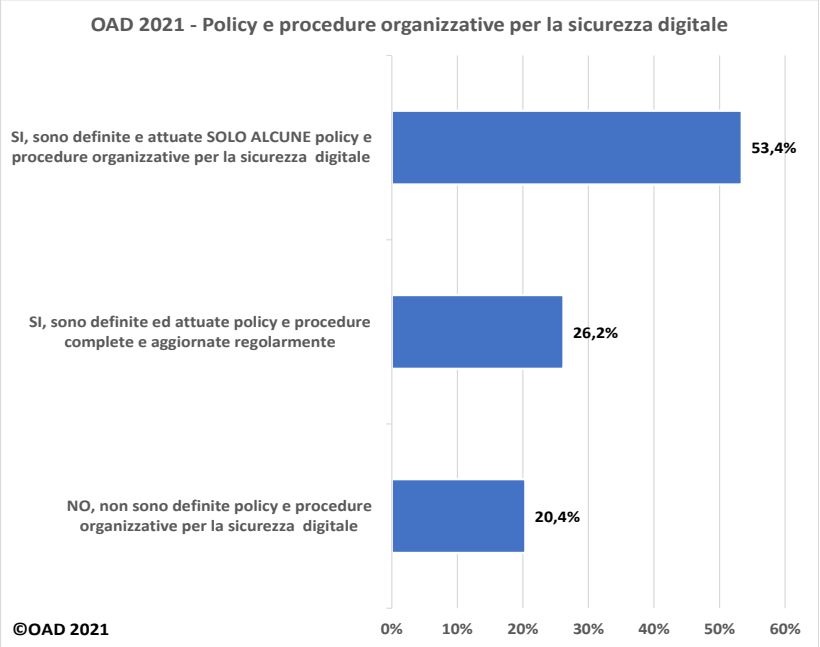

Fig. 7.1.2-1

Solo nell'ambito del questionario completo sono state poste specifiche domande su queste specifiche procedure organizzative. La fig. 7.1.2-2 evidenzia che la maggior parte delle aziende/enti che dispongono di procedure organizzative per la sicurezza digitale hanno attivato quelle per la gestione dei problemi e degli incidenti.

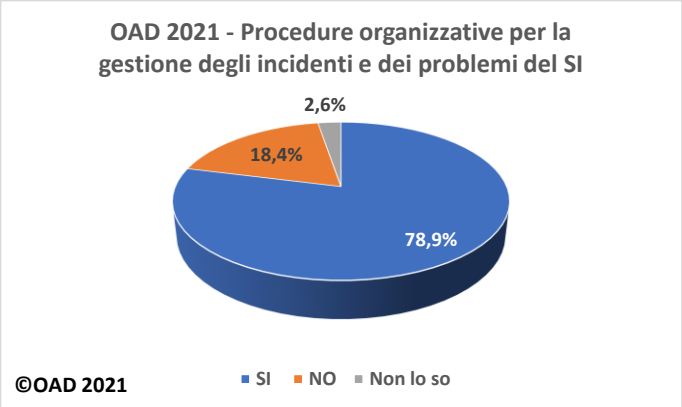

Fig. 7.1.2-2

Analogamente, l'84,2% ha attivato procedure organizzative per il supporto dell'utenza del SI, in particolare tramite help desk e trouble ticketing, e di questi il 52,6% le gestisce internamente ed il 31,6% le ha in parte o in toto terziarizzate, come mostrato nella fig. 7.1.2-3: quest'ultimo valore è indicativo della tendenza a terziarizzare la gestione della sicurezza digitale, o di sue aree.

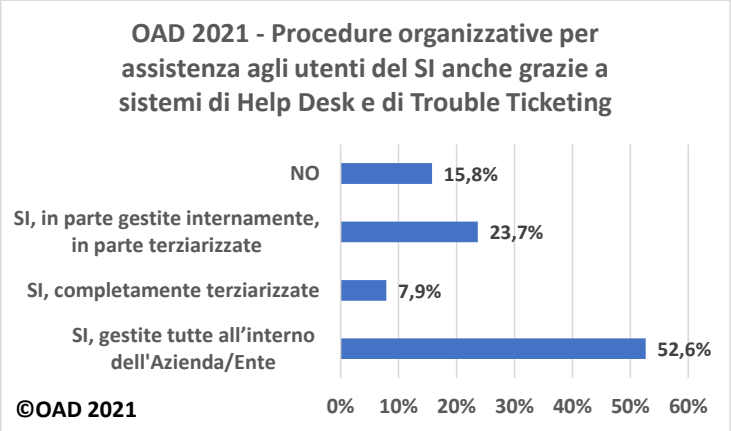

Fig. 7.1.2-3

La fig. 7.1.2-4 mostra la situazione dell'esistenza di un ERT, Emergency Response Team, e del suo utilizzo in caso di seri e gravi problemi ICT che potrebbero richiedere l'attivazione del Disaster Recovery per il SI.

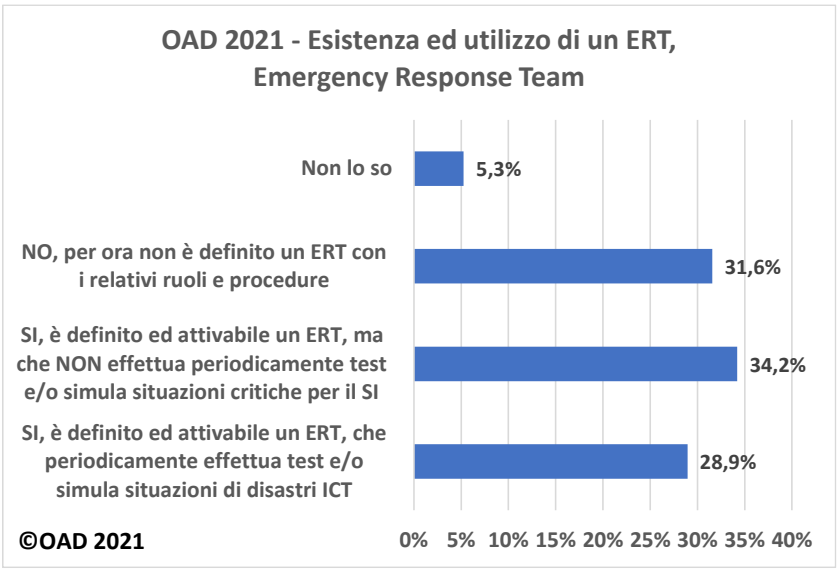

Fig. 7.1.2-4

Il 63,2% di chi ha realizzato policy e procedure organizzativa ha definito anche un ERT, che tipicamente coinvolge non solo il personale dell'UOSI, ma anche responsabili di altre direzioni e "business unit" dell'azienda/ente. La fig. 7.1.2-4 mostra la situazione dell'esistenza di un ERT, Emergency Response Team, e del suo utilizzo. Interessante evidenziare che di questa percentuale, il 40,2% ha sì definito formalmente l'ERT e, forse, le relative specifiche procedure organizzative, ma non effettua periodicamente prove e simulazioni di casi di emergenza, come invece dichiara di effettuare il 25,6%.

7.1.3 Analisi dei rischi digitali e dei possibili impatti

L'analisi dei rischi digitali e dei lori impatti sul SI, e più in generale sull'intero business e/o attività dell'azienda/ente 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 per la privacy. 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 §3.2.
Le domande sull'analisi dei rischi erano presenti su entrambi i questionari. La fig. 7.1.3-1 mostra il risultato emerso che risulta veramente positivo: il 72,8% delle aziende/enti rispondenti effettua nel complesso l'analisi dei rischi, ma di questi il 35,9% la effettua solo se richiesto e/o in maniera sporadica, ad esempio dopo aver subito un grave attacco digitale.

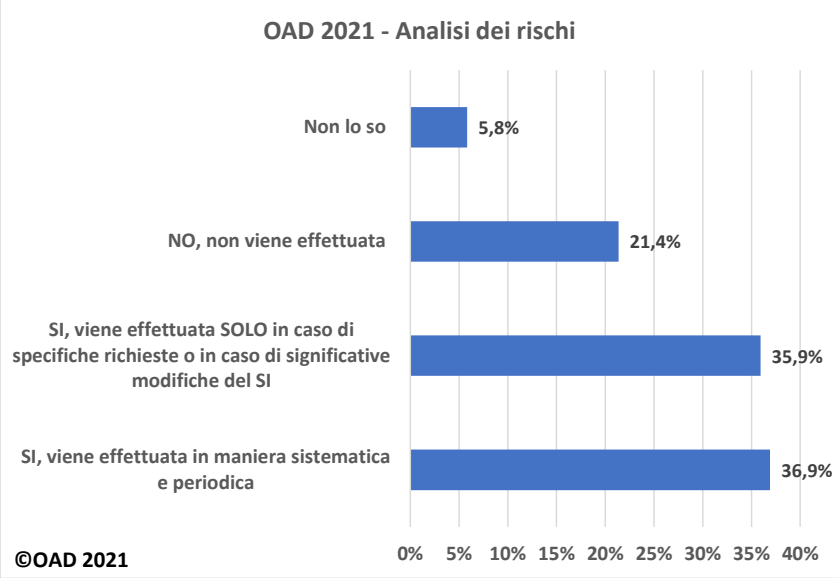

Fig. 7.1.3-1

Il 21,4% dichiara che nella sua azienda/ente non viene effettuata l'analisi dei rischi. Queste percentuali non solo confermano il livello medio-alto del bacino dei rispondenti, ma anche che hanno fortemente aiutato al raggiungimento positivo di tali % gli obblighi di conformità alle varie normative nazionali ed internazionali, in primis il GDPR per la privacy, oltre alle certificazioni aziendali e più in generale alla crescita e diffusione della cultura digitale e della cybersecurity. Alcune/i rispondenti dichiarano di non sapere se e come avviene l'analisi dei rischi digitali all'interno della loro azienda/ente.
Solo per il questionario completo erano previste ulteriori domande tecniche su come viene effettuata l'analisi dei rischi digitali e se viene effettuata l'analisi dei possibili impatti sul business/attività dell'azienda/ente: le figure di questo paragrafo dalla 2 alla 4 riflettono quindi le risposte avute da chi ha compilato il questionario completo.
La fig. 7.1.3-2 evidenzia che più di ¾ delle aziende/enti che effettuano l'analisi dei rischi lo fanno seguendo consolidati standard e best practice, quali NIST, ISO, CRAMM, Mehari, Octave Allegro, etc.
Una domanda richiedeva se l'analisi dei rischi fosse correlata e in accordo con le specifiche degli standard della famiglia ISO 27000. I risultati sono nella fig. 7.1.3-3: la quasi totalità, l'86,2%, fa riferimento ed effettua verifiche dell'analisi dei rischi. E di questi ben il 24,1%, ossia quasi ¼, lo fa ottenendo la specifica certificazione dello standard ISO di riferimento, tipicamente l'ISO 27001, per l'intero SI o per alcune sue parti più critiche.

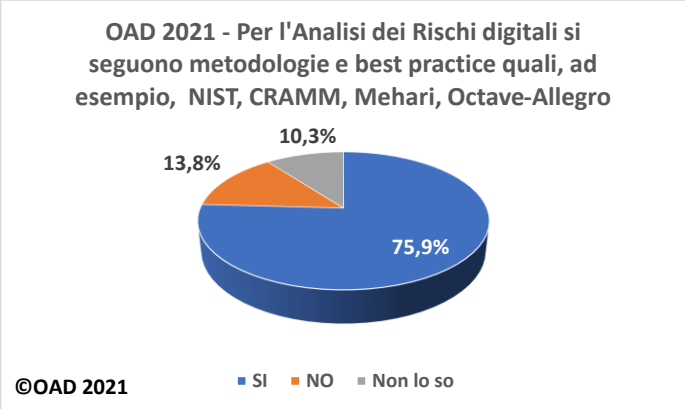

Fig. 7.1.3-2

Un'analisi dei rischi comporta anche l'analisi dei possibili impatti sui processi ed attività dell'azienda/ente, analisi chiamata BIA, Business Impact Analysis. Su questo tema, nell'indagine OAD 2021 per chi effettua l'analisi dei rischi, la situazione nel bacino di rispondenti è riportata nella fig. 7.1.3-4: il 79,3% la effettua, confermando ancora una volta il livello medio alto delle misure di sicurezza digitale dei SI oggetto delle risposte.

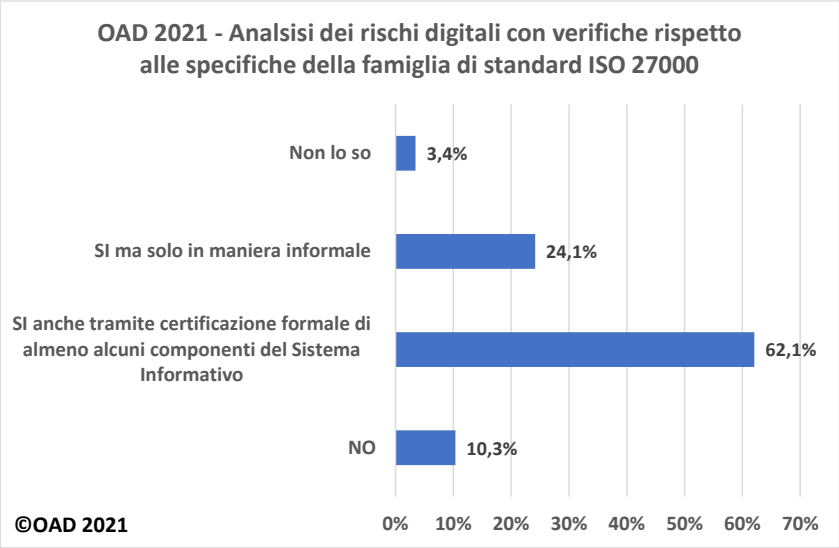

Fig. 7.1.3-3

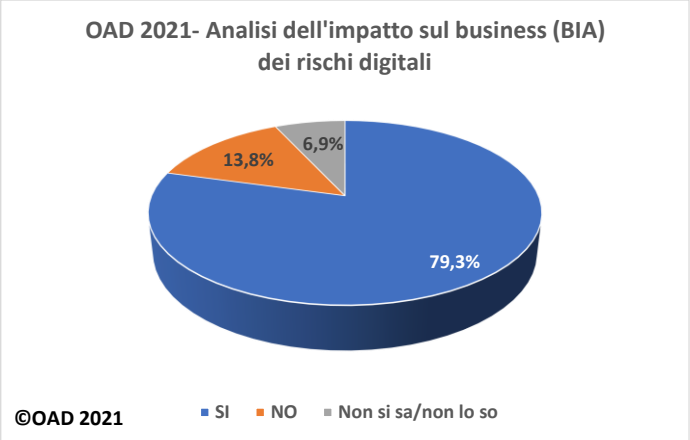

Fig. 7.1.3-4

Una domanda finale, sia nel questionario completo che in quello ridotto, riguardava l'assicurazione del rischio digitale, che richiede l'attuazione delle adeguate misure di sicurezza digitale. La fig. 7.1.3-5 mostra i risultati. Il 44,6% delle aziende/enti rispondenti ha attuato dei contratti assicurativi sulla sicurezza digitale, una % alta rispetto alle indagini OAD degli anni precedenti, il che conferma nuovamente il livello medio alto del bacino emerso per OAD 2021. Di questa % solo il 7,9% ha coperto con una o più assicurazioni i rischi digitali per l'intero SI, il 36,6% solo per le parti del SI ritenute più critiche. Risulta elevata, rispetto alle risposte date alle altre domande dei questionari OAD 2021, la % di chi non conosce o non sa di una tale assicurazione: è un aspetto manageriale ed organizzativo che molti rispendenti, probabilmente di taglio strettamente tecnico, non conoscono o di cui non sono interessati.

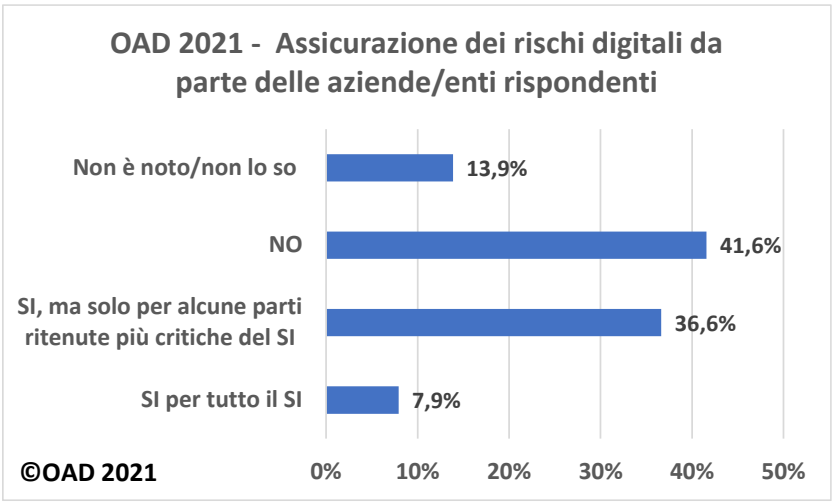

Fig. 7.1.3-5

7.1.4 Auditing della sicurezza digitale

Con il termine di "auditing" inerente la sicurezza digitale si intende il processo documentato di revisione (ossia verifica, controllo e valutazione) della efficacia delle misure in essere e della loro gestione, oltre che della conformità di tali misure alle leggi vigenti e alle normative, anche interne, che devono essere seguite. Con il termine di "audit" si intende il risultato di tale valutazione, rappresentato tipicamente da un rapporto all'alta direzione. Sovente, anche tra gli addetti ai lavori, i due termini vengono usati 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.

L'auditing della sicurezza digitale è normalmente effettuato come parte del più ampio auditing di un intero SI, o di una sua parte, volto a verificare che i dati trattati siano corretti, completi ed integri e che siano protetti con le idonee misure di sicurezza.

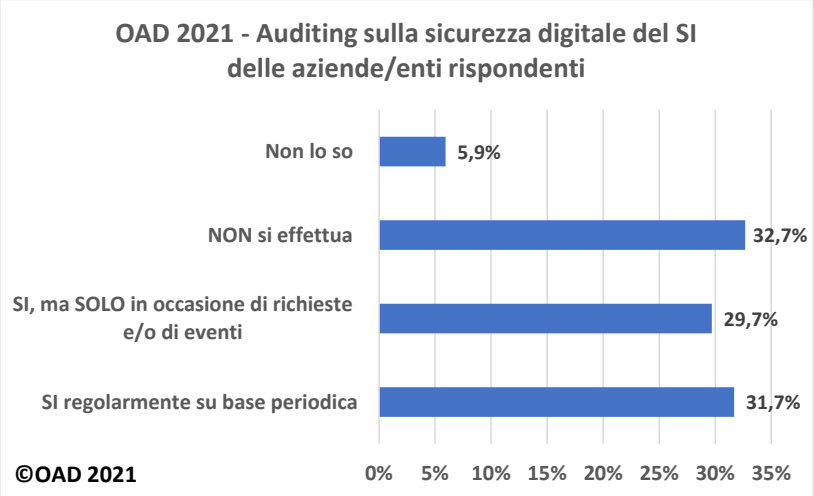

Fig. 7.1.4-1

La fig. 7.1.4-1 indica che il 61,4% effettua auditing per la sicurezza digitale, e più della metà di questi, il 31,7% lo effettua sistematicamente e periodicamente. 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 livello buono-medio nella sicurezza digitale dei SI delle aziende/enti rispondenti.
Nel questionario completo si poneva un' ulteriore domanda, per chi aveva indicato di effettuare auditing della sicurezza digitale, su chi la effettuasse. Il risultato di queste risposte è fornito dalla fig. 7.1.4-2. La maggior parte, 67,7%, effettua l'auditing sia con personale interno sia con esperti esterni. Una minoranza dl 12,9% utilizza solo i propri esperti interni, ed il 19,4% terziarizza totalmente l'auditing ad aziende e specialisti esterni.

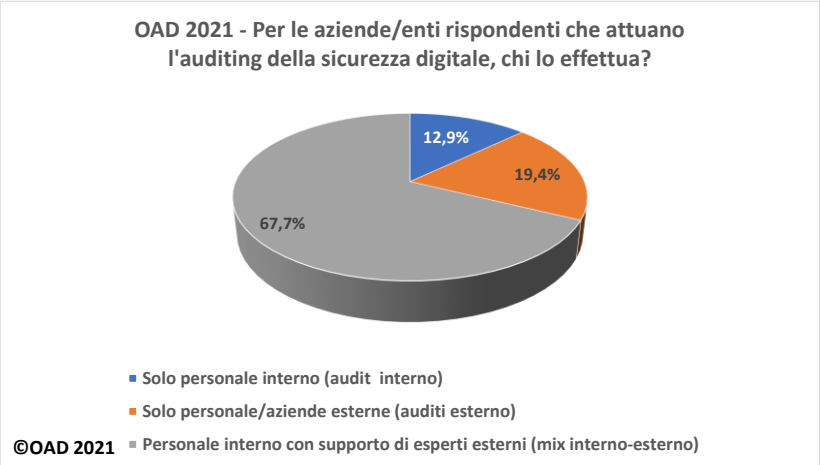

Fig. 7.1.4-2

7.1.5 Certificazioni aziendali e individuali 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 indicatore credibile della effettiva specifica competenza sulla sicurezza digitali e/o su suoi prodotti, servizi e soluzioni.

In ambito sicurezza digitale esistono numerosi tipi di certificazioni: da quelle indipendenti ed internazionali, quali ad esempio eCF (l'unica con validità legale in Europa, EN 16234-1:2016 (UNI 11506)), Eucip, CISSP, SSCP, CISA, CSSLP, ISO 27001 Lead Auditor, CISM, CRISC, etc., a quelle "proprietarie" rilasciate da fornitori, prevalentemente focalizzate a validare la buona conoscenza tecnica e sistemistica dei loro prodotti; praticamente ogni fornitore di prodotti inerenti la sicurezza digitale fornisce certificazioni sui suoi prodotti. Esistono poi certificazioni individuali, rilasciate alla singola persona, come quelle elencate sopra, ed aziendali, rilasciate ad un'azienda/ente nel suo complesso o ad una sua parte: esempi di queste ultime includono ISO 27001 e ISO 20000.
La fig. 7.1.5-1 riporta la richiesta di specifiche certificazioni sulla sicurezza digitale da parte dell'azienda/ente per il suo personale interno, che se ne occupa. Il 60,4% delle aziende/enti rispondenti non le richiede per il proprio personale: le richiede il 32,7%, una % elevata, quasi un 1/3 del totale, ma di questi la maggior parte, pari al 26,7%, le richiede solo per le figure professionali più importanti e di riferimento, quali ad esempio il CIO ed il CISO.
Come indicato in fig. 7.1.5-2, il 40,6% dei rispondenti le richiede alle aziende/ente cui terziarizza, o che coinvolge, nella sicurezza digitali: una percentuale nettamente maggiore rispetto al 32,7% che le richiede al proprio personale interno. E di questo 40,6%, il 27,7% le richiede sia a livello aziendale che delle singole persone che interagiscono con il personale interno.
Oltre alle aziende/enti lato offerta sicurezza digitale, che dovrebbero tutte avere una o più certificazioni per dimostrare la loro competenza in materia, un numero crescente di aziende/enti lato domanda per la sicurezza digitale acquisiscono specifiche certificazioni aziendali anche per la cyber sicurezza, prevalentemente ISO 27001. Rientrano tra questi lato domanda ICT le infrastrutture critiche ed i servizi essenziali, ad esempio assicurazioni, aeroporti, banche, ferrovie, ospedali, pubbliche amministrazioni.

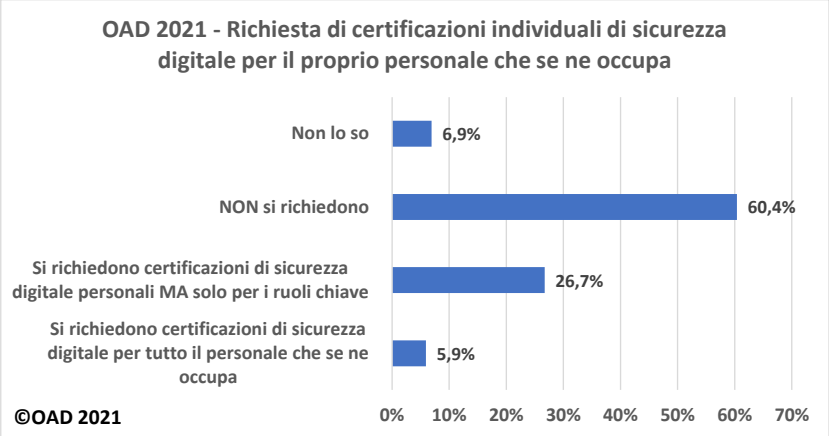

Fig. 7.1.5-1

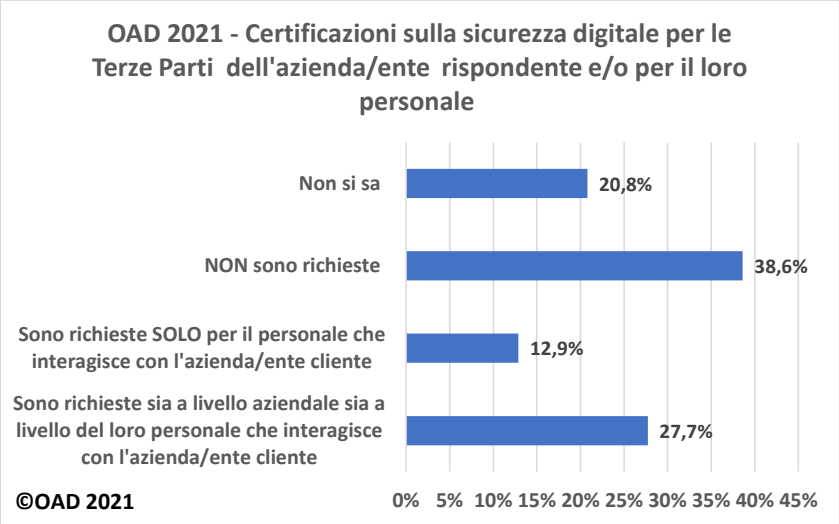

Fig. 7.1.5-2

La fig. 7.1.5-3 mostra che più della metà, il 50,5%, delle aziende/enti rispondenti ha una o più certificazioni aziendali sulla sicurezza digitale, ed il 16,8% ne ha già a piano uno a breve.

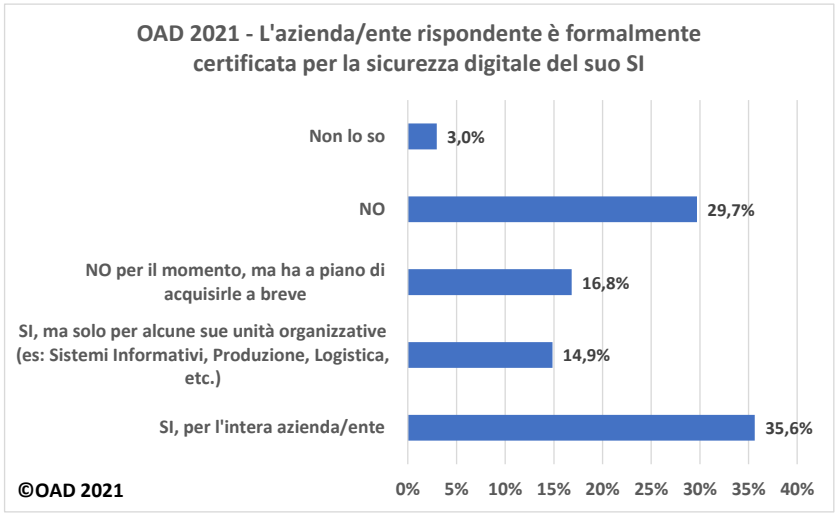

Fig. 7.1.5-3

Tra il 50,5% di aziende/enti certificati per la sicurezza digitale, 2/3 lo sono per l'intera struttura ed i suoi processi, 1/3 lo sono solo per alcune aree ed unità organizzative, quali ad esempio i Sistemi Informativi, la logistica, il marketing e la vendita, la produzione e l'erogazione di servizi.

7.2 Le misure tecniche di sicurezza digitale

Le domande sulle misure tecniche in uso nei SI delle aziende/enti rispondenti riguardavano le seguenti misure tecniche, ed erano presenti in entrambi i due questionari, a parte la prima sulle architetture, posta solo nel questionario completo:

- 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.

Nel questionario ridotto mancavano alcune domande di approfondimento e dettaglio relative alle misure tecniche elencate, presenti nel questionario completo.

7.2.1 Architetture per la sicurezza digitale

La fig. 7.2.1-1 mostra le risposte raccolte solo dal questionario completo relativa alle architetture per la sicurezza digitale[22] definite ed implementate nei SI oggetto delle risposte. Più di ¾ dei SI delle/dei rispondenti, il 77,6%, ha definito un'architettura per la sicurezza digitale, e di questi il 30,6% solo per le parti del SI più critiche.

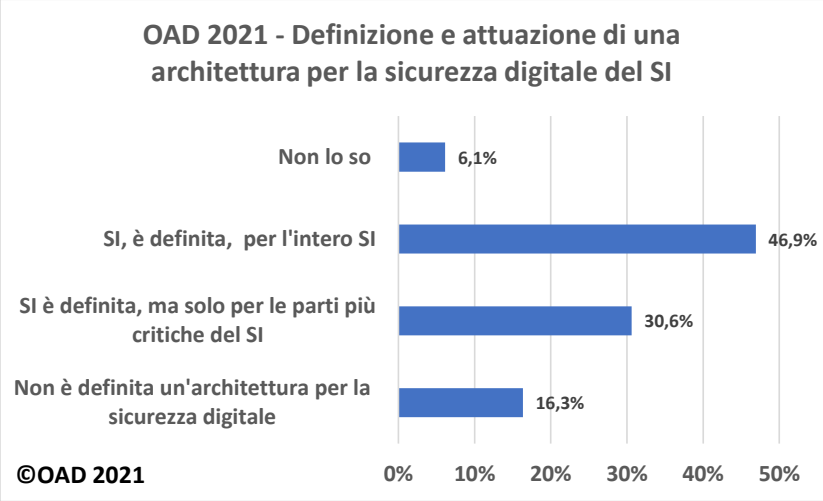

Fig. 7.2.1-1

Ulteriori domande sulle architetture del SI, presenti solo nel questionario completo, riguardano il livello di affidabilità e disponibilità del SI, e per chi ha almeno in Data Center in Italia, il livello di affidabilità secondo lo standard ANSI/TIA 942, e la eventuale certificazione di questo livello.
La fig. 7.2.1-2 evidenzia che quasi il 90% ha una architettura ad alta affidabilità, e di questi il 36,7% l'ha per l'intero SI. Percentuali molto alte che evidenziano l'elevato grado di sicurezza digitale dei SI dell'indagine.
Lo standard ANSI/TIA 942 definisce quattro differenti livelli di affidabilità, chiamati "tier" che fanno riferimento alle misure di sicurezza fisica, in particolare:

- **Tier I**: Data Center dotato di un solo sistema di alimentazione e un solo sistema di raffreddamento con affidabilità al 99,671% l'anno, ovvero un tempo di fermo (imprevisto, non schedulato) di 28,8 ore annue
- **Tier II**: Data Center dotato di un solo sistema di alimentazione e un solo sistema di raffreddamento ma con componenti ridondati e sistemi di backup e con affidabilità al 99,741%, ovvero circa 22 ore di fermo (imprevisto, non schedulato) nell'anno

[22] Le architetture per la sicurezza digitale si basano su standard, best practice e framework internazionali quali gli standard della famiglia ISO 27000, NIST, OSA (Open Security Architecture), CIS (Center for Internet Security), etc.

- **Tier III**: Data Center dotato di più sistemi di alimentazione e più sistemi di raffreddamento, componenti ridondati e sistemi di backup e con affidabilità 99,982% ovvero 1,6 ore di fermo(imprevisto, non schedulato) all'anno
- **Tier IV**: Data Center totalmente fault tolerant, affidabilità 99,995% e downtime (imprevisto, non schedulato) minore di 26,3 minuti all'anno.

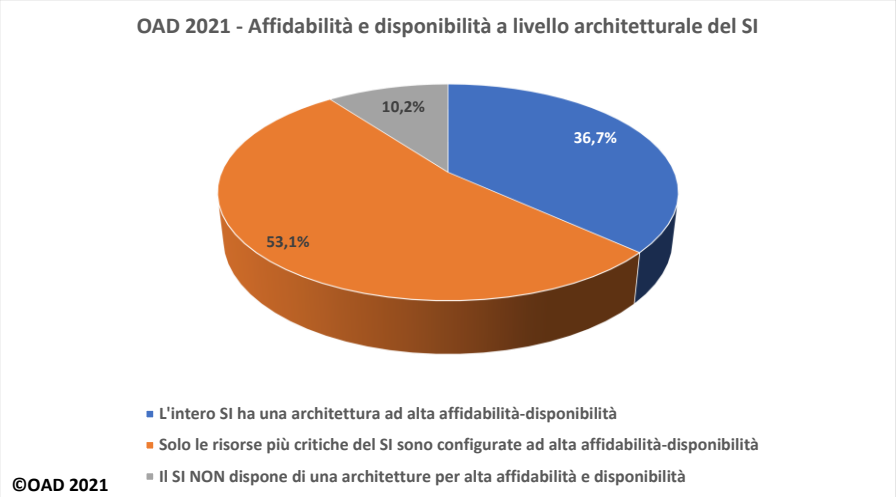

Fig. 7.2.1-2

La fig. 7.2.1-3 mostra i livelli di affidabilità del Data Center in Italia del SI così come dichiarato dalle/dai rispondenti secondo lo standard ANSI/TIA 942.

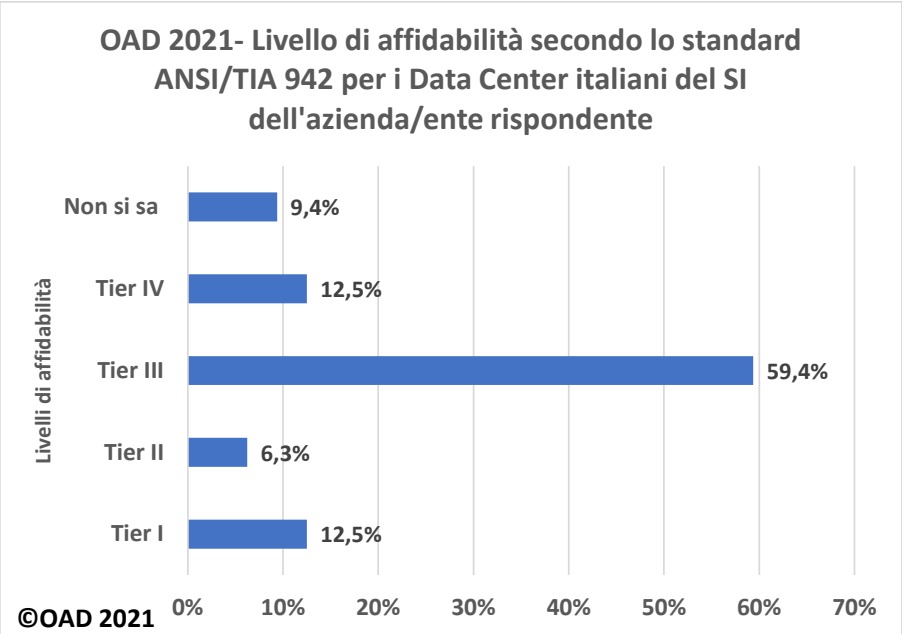

Fig. 7.2.1-3

Hanno risposto a questa domanda le aziende/enti che hanno nel loro SI almeno un Data Center sul suolo italiano. La maggior parte, 59,4%, dichiara il Tier III, ed il 12,5% la classe più elevata, il 12,5%. Per essere nel questionario completo, stupisce il 9,4% di "Non si sa", un valore piuttosto alto: probabilmente questo standard, molto legato alla sicurezza fisica, non è conosciuto dagli informatici, che trattano normalmente la

sicurezza "logica". Tale spiegazione è confermata dall'alta percentuale di "non so", 39,3% emersa dalla domanda se il principali Data Center italiano del SI siano formalmente certificati con questo standard, ed evidenziata nella fig. 7.2.1-4: solo ¼ dei Data Center in Italia dei SI considerati è certificato ANSI/TIA 942.

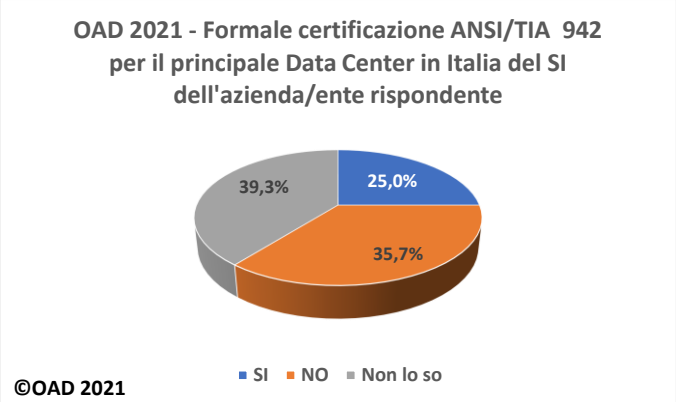

Fig. 7.2.1-4

7.2.2 Misure tecniche di sicurezza fisica e perimetrale

Le misure tecniche per la sicurezza fisica e perimetrali includono (elenco non esaustivo) i controlli per l'accesso delle persone autorizzate nei locali ove si trovano raggruppati i sistemi ICT, quali la guardiania, le bussole d'ingresso, i lettori di badge ed i sistemi di riconoscimento biometrico, etc., i sistemi per garantire la continuità elettrica (dagli UPS ai gruppi di continuità), i sistemi di climatizzazione dei locali, i sistemi rilevatori di fumo, gas, e umidità, le protezioni perimetrali passive e attive, dalle recinzioni anti-scavalcamento, inferiate alle finestre e alle porte, ai sistemi di allarme antintrusione a radar o a micro onde, i sistemi di videosorveglianza. 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.

Viene dato per scontato che l'accesso del personale autorizzato ai locali di un Data Center siano adeguatamente controllati. Pertanto la prima domanda di entrambi i questionari di OAD 2021 fa riferimento ai locali, spesso chiamati "computer room" ove sono allocati insiemi di risorse ICT destinati, per le piccole realtà, e per gli ambienti dipartimentali di SI di medie e grandi dimensioni, che dispongono anche di uno o più Data Center. La fig. 7.2.2-1 mostra la situazione emersa dal bacino di rispondenti ad OAD 2021: circa un ¼ di loro non prevede specifiche misure per il controllo dell'accesso di persone nei locali con sistemi ICT.

Sempre escludendo i Data Center, la fig. 7.2.2-2 mostra che quasi il 70% dei rispondenti utilizza sistemi di controllo perimetrale per i locali tipo "computer room", e di questi il 35,8% li utilizza per tutti i locali delle varie sedi, mentre il 33,9 lo fa solo per i locali con sistemi ICT più critici, quali server e storage locali.

La fig. 7.2.2-3 mostra la situazione dei sistemi di controllo e prevenzione di interruzioni dell'energia elettrica (black out energetico) per l'alimentazione dei sistemi ICT nelle computer room del SI dei rispondenti, esclusi gli eventuali Data Center per i quali si dà per scontato che esistano tutte queste misure di sicurezza fisica. Poco più dei ¾ dei SI delle aziende/enti rispondenti, una % veramente alta, ha sistemi di controllo e prevenzione per garantire l'energia elettrica nei locali tipo "computer room", ma di questi il 45% le ha realizzate solo per i locali con sistemi ICT più critici.

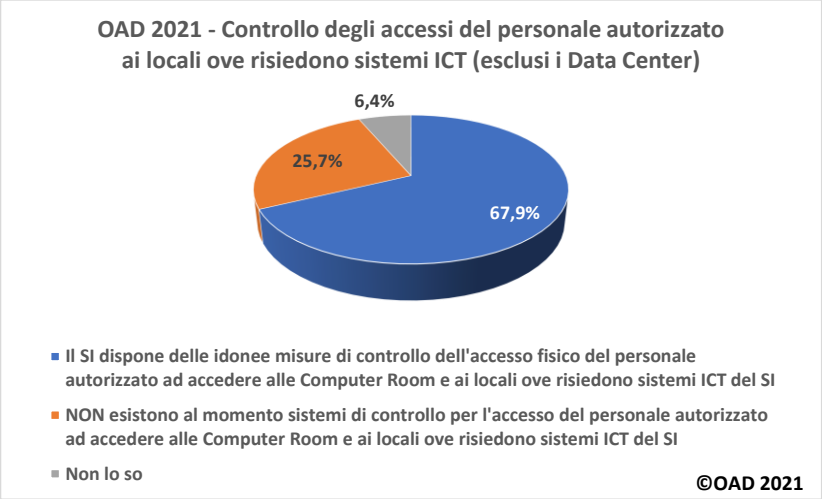

Fig. 7.2.2-1

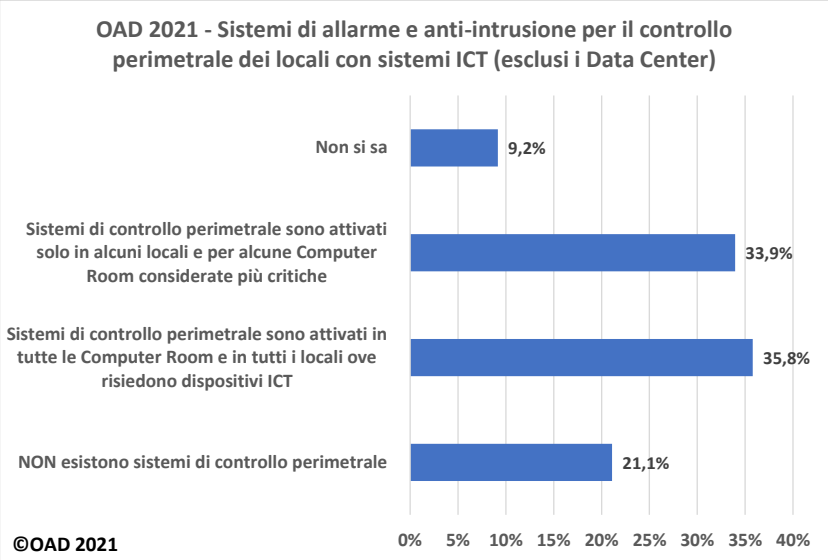

Fig. 7.2.2-2

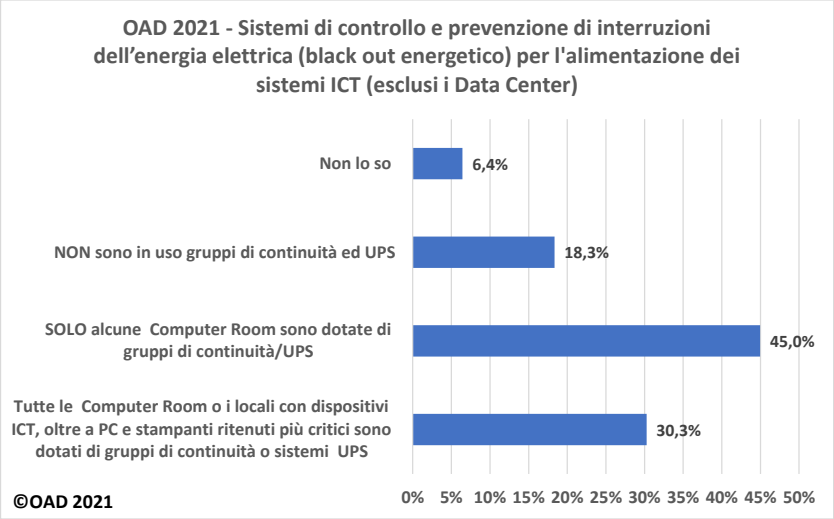

Fig. 7.2.2-3

Solo nel questionario completo OAD 2021 erano previste due ulteriori domande sulla sicurezza fisica, riguardanti una l'uso di rack nei locali tipo "computer room", l'altra sul fissaggio/blocco fisico dei dispositivi d'utente fissi, tipicamente i PC, e le stampanti locali.

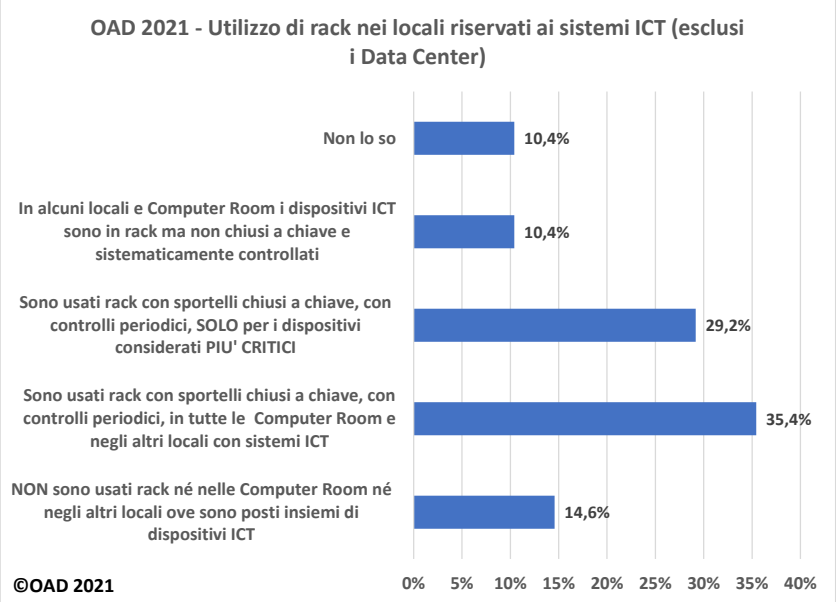

Fig. 7.2.2-4

Nella fig. 7.2.2-4 la sintesi delle risposte avute sull'uso dei racket per i sistemi ICT nelle computer room e più in generali nei locali ove sono posti sistemi ICT d'uso comune in locale, quali switch, router, server, etc.
Oltre che nei Data Center, anche negli altri locali dove sono sistemati sistemi ICT l'uso dei racket è molto diffuso: Le risposte avute, pur solo dal questionario completo, indicano che ¾ delle aziende/enti rispondenti le usa: una % alta, ma di questi il 29,2% li usa solo per i sistemi ICT più critici e il 10,6% li usa, ma non sempre li chiude a chiave e li controlla saltuariamente, riducendo e vanificando l'effettiva protezione fisica dei dispositivi inseriti nei racket. Nel complesso comunque la situazione del bacino emerso dall'indagine è buona.
Il fissaggio "fisico", ad esempio al tavolo di lavoro, dei dispositivi d'utente fissi e delle stampanti è uno strumento che riduce la facilità di furto di questi dispositivi. La maggioranza delle risposte, il 64,6%, è

negativa, non vengono utilizzate queste misure. Sono utilizzati nel 31,3% dei casi, e di questi il 27,1% solo per i PC e le stampanti più critiche ed importanti, non per tutto il parco macchine.

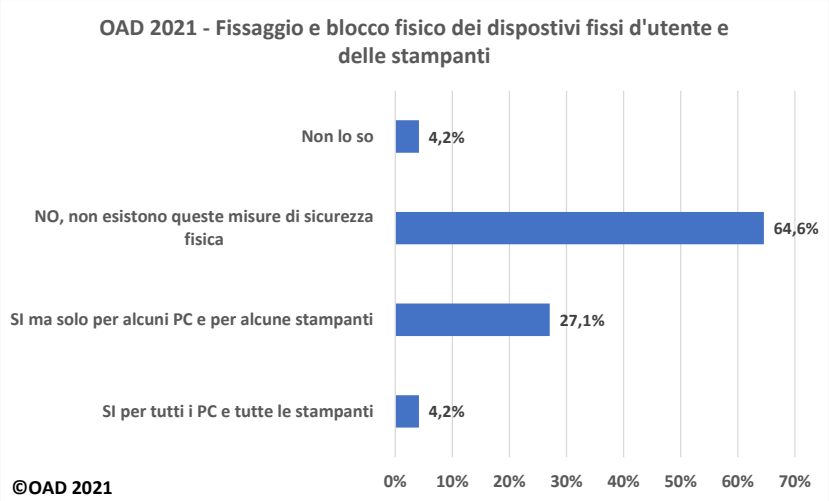

Fig. 7.2.2-5

7.2.3 Identificazione, autenticazione e autorizzazione degli utenti

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 SI, tenendo anche conto che gli attacchi digitali all'IAA sono i più diffusi per OAD 2021 (si veda §4) ed anche nelle indagini dei quattro anni precedenti (2020, 2019, 2018 e 2017).

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[23], 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.

La prima domanda nei questionari OAD 2021 considera l'uso dell'autenticazione forte per gli utenti privilegiati, ed i risultati emersi sono rappresentati nella fig. 7.2.3-1. Il 64,2 % dei SI rispondenti utilizza l'autenticazione forte per gli utenti privilegiato, ma di questi il 41,3% la usa solo per alcuni ambiti ritenuti i più critici; è ben il 30,3%, un valore assai alto, non usa tecniche di autenticazione forte. Ed anche il 5,5% di "non so" è una percentuale troppo alta, a giudizio dell'autore, per chi risponde su una misura di sicurezza digitale così importante ed essenziale.

Per l'autenticazione degli utenti finali, il 46,8% utilizza un mix di autenticazione forte e debole a seconda del tipo di applicativo, prevalentemente in funzione della sua criticità e riservatezza per le informazioni trattate, come mostrato nella fig. 7.2.3-2. Un terzo dei SI rispondenti utilizza solo autenticazione debole, ed il 12,8% utilizza sempre autenticazione forte. Per il "non so" il valore della % è più basso rispetto a quello sopra sull'utenza privilegiata.

[23] 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

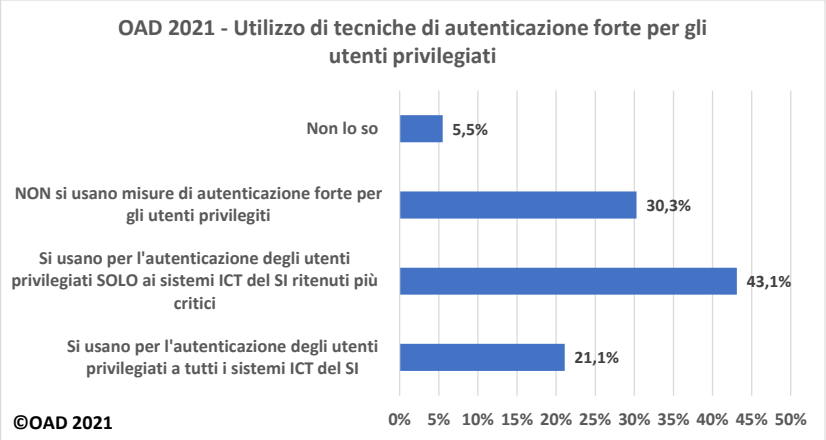

Fig. 7.2.3-1

La gestione delle password degli utenti finali e privilegiati è effettuata centralmente per il 63% dei SI rispondenti: una percentuale abbastanza elevata rappresenta un ulteriore indice del buon livello della sicurezza digitale in essere, come mostrato nella fig. 7.2.3-3. Interessante notare che per il 16,7% è gestita e controllata centralmente solo la password dell'utente privilegiato, che in termini di sicurezza digitale è il più critico. Ancora un 14,8% dei SI lascia la gestione delle password senza controlli centrali e alla responsabilità del singolo utente, sia esso finale o privilegiato. Trascurabili le % dei SI che utilizzano SPID, sicuramente per la mancanza di Pubbliche Amministrazioni rispondenti a OAD 2021, ed i SI che delegano IAA a servizi esterni come Google e Amazon.

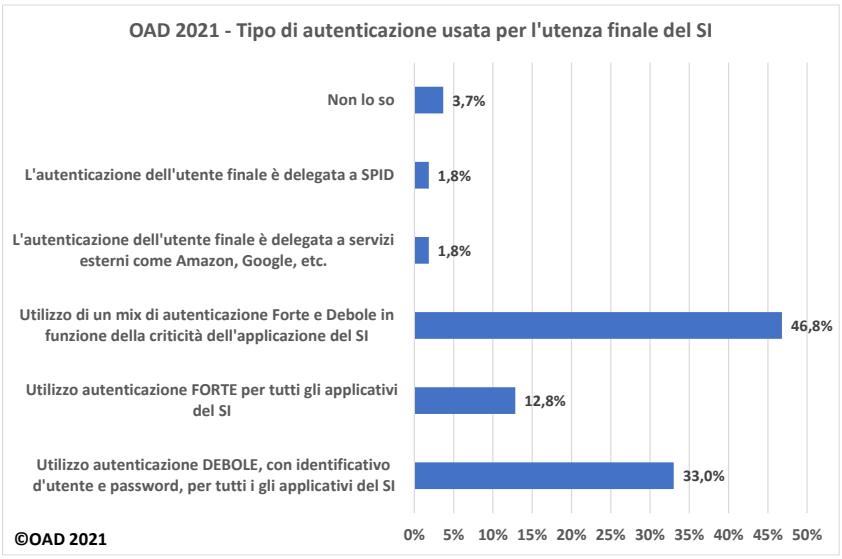

Fig. 7.2.3-2

Solo nel questionario completo era richiesto l'eventuale utilizzo di tecniche passwordless per l'autenticazione degli utenti.

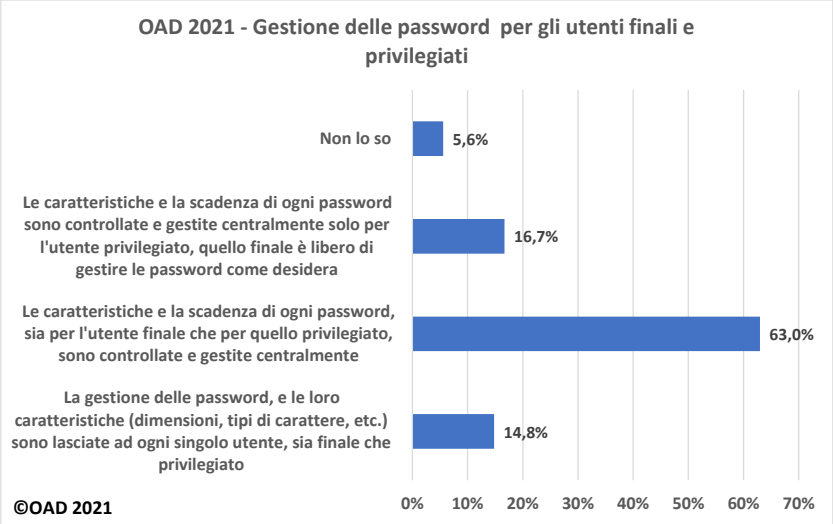

Fig. 7.2.3-3

Tali tecniche si basano tutte sull'identificazione biometrica dell'utente, ed hanno l'obiettivo sia di migliorare la sicurezza dell'IAA sia di semplificare e facilitare l'uso degli account: ormai sono centinaia le password da gestire individualmente, tra ambiente lavorativo e domestico, ed il loro uso sta di fatto diventando ingestibile per i più. Tecniche biometriche sono disponibili e stanno diffondendosi grazie ai moderni cellulari, ma il loro uso, in particolare in ambito business, deve passare sotto le normative sulla privacy e dell'Autorità Garante, rendo più complesso il loro uso. Nonostante questi vincoli, a livello iniziano ad essere usate e stanno acquisendo interessanti quote di mercato le autenticazioni "*passwordless*" basate, ad esempio, sul 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. Come mostrato dalla fig. 7.2.3-4, il loro uso in Italia è ancora limitato, visti i vincoli della normativa sulla privacy, ma il 12,8% che già utilizza tali tecniche ed il 14,9% che le sta sperimentando sono percentuali non basse ed indicano che l'identificazione biometrica con autenticazione senza password sarà nel prossimo futuro anche in Italia un'innovazione di crescente diffusione.

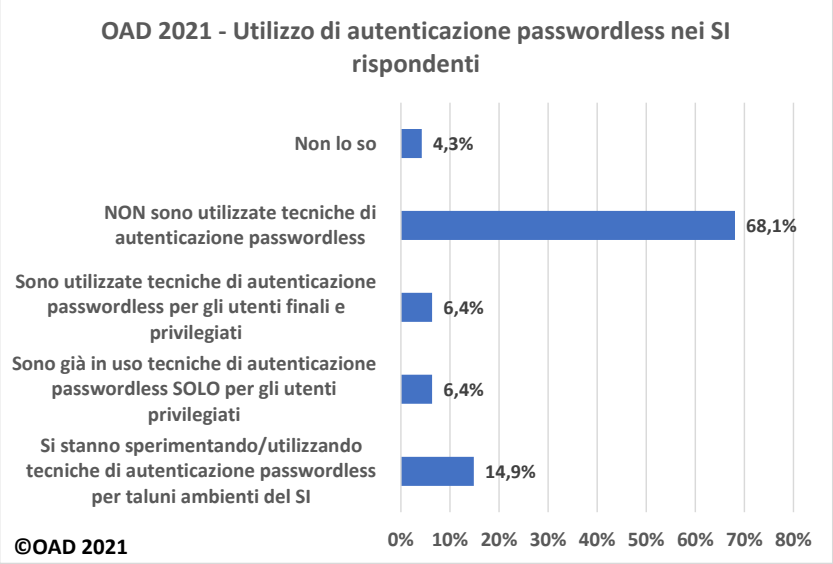

Fig. 7.2.3-4

7.2.4 Misure tecniche di sicurezza delle reti dei SI

Le reti per i SI includono le connessioni ad Internet, le reti locali (LAN e WLAN) ed eventuali reti e connessioni dedicate per il SI, che ormai tendono ad essere dei casi eccezionali, dati anche i loro costi. 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. 7.2.4-1 evidenzia come la maggior parte delle connessioni ad Internet dei SI delle aziende/enti rispondenti ha in essere connessioni multiple per garantire una alta affidabilità e disponibilità dei collegamenti a Internet: solo il 12,1% delle risposte dichiara di non avere connessioni multiple, e queste risposte sono fornite da realtà piccole.

Come riportato nella fig. 7.2.4-2, la maggior parte dei SI, il 64,5%, monitora e controlla centralmente funzionalità e prestazioni delle proprie reti "interne", ed utilizza strumenti di sicurezza digitale quali DMZ, FireWall, IPS/IDS, VPN, etc. Il 24,3% non monitora e controlla centralmente le proprie reti interne, ma ha alcuni degli strumenti di sicurezza digitale.

Per ¾ delle reti e delle connessioni ad Internet dei SI oggetto dell'indagine, il traffico transita crittografato, prevalentemente con IPSec, quindi per i siti web con HTTPS. Lascia perplesso l'autore una così alta % di "non so", prevalentemente scelta da chi ha compilato il questionario ridotto, così come riscontrato per numerose altre domande del questionario.

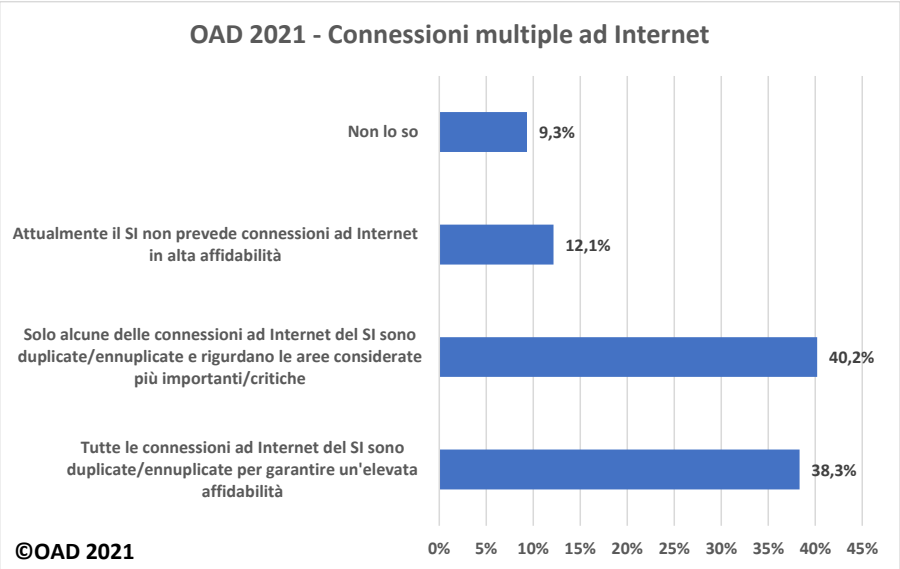

Fig. 7.2.4-1

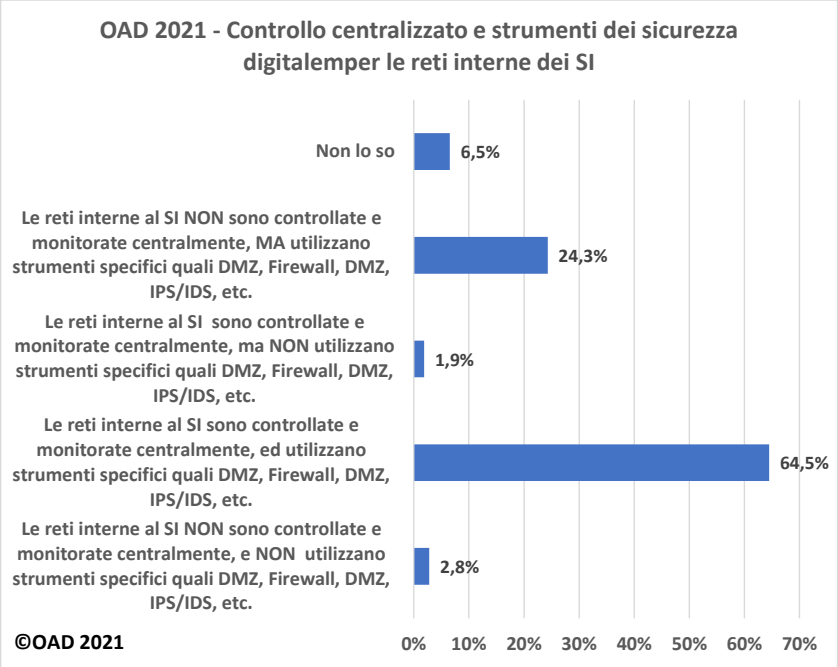

Fig. 7.2.4-2

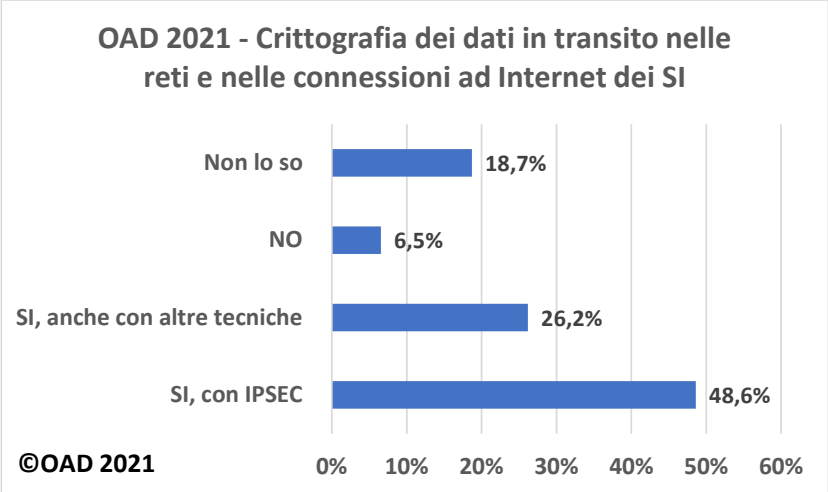

Fig. 7.2.4-3

Un'ulteriore domanda sulla sicurezza era posta solo nel questionario completo, e riguarda l'uso di servizi di Terze Parti, di norma in cloud, per potenziare il livello di sicurezza digitale delle reti e delle connessioni ad Internet, quali ad esempio i servizi delle architetture SASE, che consentono di far fronte ad attacchi tipo Dos/DDos. Le risposte sono sintetizzate nella fig. 7.2.4-4: anche se il 55,3% dei SI non usa oggi tali servizi, è molto significativo, e promettente come trend, che già il 27,7% li usi. Alto il numero di "non so", dovuti probabilmente ad una domanda "specialistica".

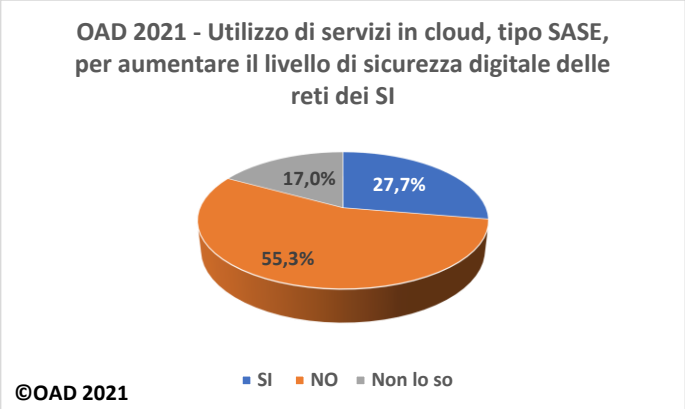

Fig. 7.2.4-4

7.2.5 Misure di sicurezza delle applicazioni del SI

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.
La fig. 7.2.5-1 mostra che il 70,1% dei software applicativi è stato sviluppato secondo i moderni criteri per avere un codice intrinsecamente sicuro, ossia senza bachi, porte aperte, ed altre vulnerabilità. Di questa % estremamente positiva, se veritiera, il 41,1% dichiara che tale sviluppo digitalmente sicuro è stato effettuato solo per gi applicativi più importanti e più critici per l'azienda/ente. Anche in questo caso molto alto il 23,4% dei "non so", dovuti per lo più a chi ha risposto al questionario ridotto.

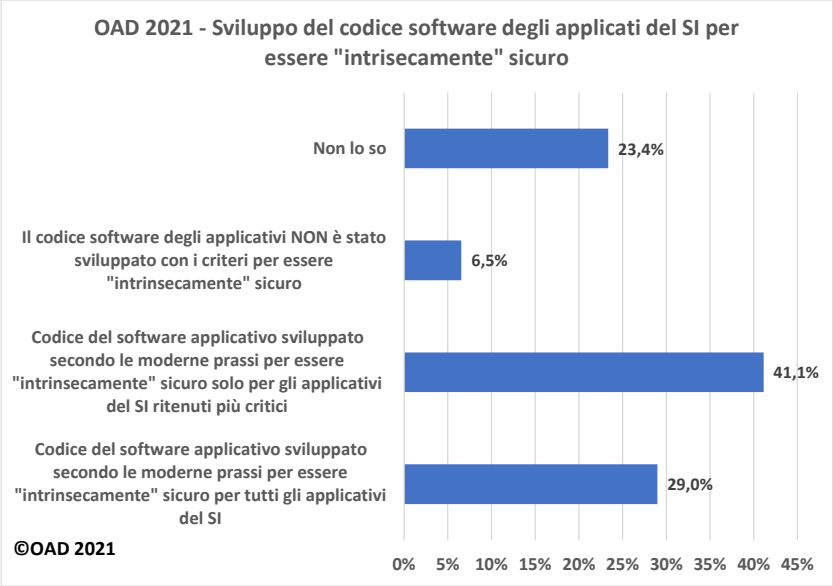

Fig. 7.2.5-1

Una specifica domanda, presente solo nel questionario completo, riguarda la verifica ed il test della sicurezza del codice software sviluppato ad hoc prima della sua messa in produzione. Si noti che questa importante verifica è considerato solo per gli sviluppi ad hoc di applicativi effettuati/richiesti dall'azienda/ente, e volutamente non si fa riferimento ai software applicativi commerciali, 2,3% di chi sviluppa o fa sviluppare software ad hoc per un determinato applicativo effettua che dovrebbero essere sicuri e per i quali è complesso, se non impossibile, effettuare tali controlli, a parte delle analisi di vulnerabilità. Come mostrato nella fig. 7.2.5-2, il 72,3% degli sviluppi ad hoc viene testato prima della sua messa in produzione, una % veramente alta, e di cui il 48,9% riguarda verifiche e test solo delle applicazioni sviluppate considerate più importanti e critiche. Anche in questo caso una % di "non so" veramente alta, giustificabile forse dal fatto che chi compila il questionario completo OAD 2021 è più a conoscenza di come si gestisce il SI, e molto meno sullo sviluppo del software.

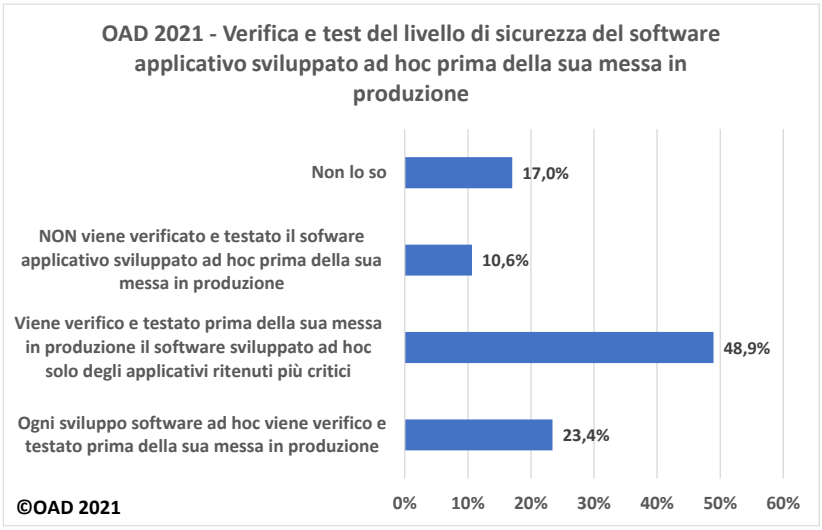

Fig. 7.2.5-2

Quasi tutti gli applicativi del SI, il 91,6%, utilizzano tecniche di autorizzazione perché gli utenti possano correttamente operare su di essi: leggere, scrivere, modificare, cancellare, copiare, etc., e ben il 55,1% lo fa

per tutti gli applicativi del SI. Ancora una % molto alta che caratterizza i SI del bacino di aziende/enti rispondenti con un elevato livello di sicurezza.

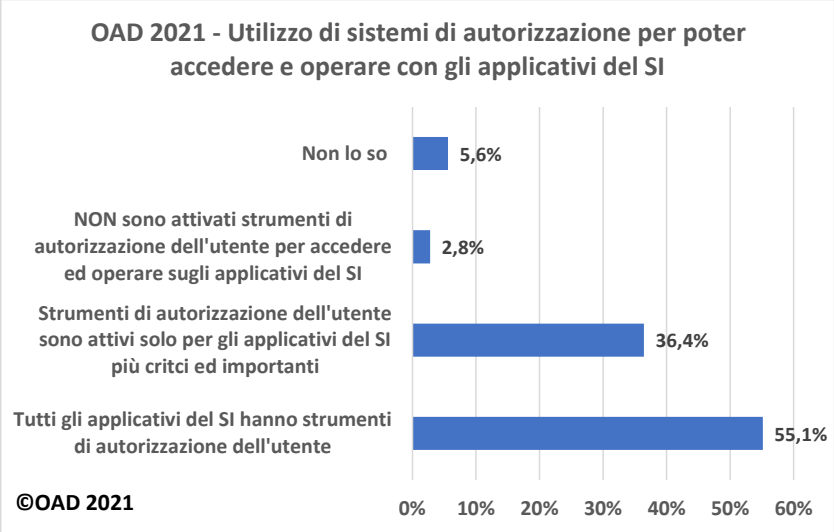

Fig. 7.2.5-3

Uno degli strumenti più efficaci nella protezione degli applicativi in produzione è l'uso di FWA, Firewall Applicativi. La fig. 7.2.5-4 mostra che il 47,7% dei SI li usa, ma il % solo davanti ai server che supportano gli applicativi più importanti e/o più critici per l'azienda/ente rispondente. Anche qui, molto alto il numero di "non so", causati soprattutto dalle risposte ai questionari ridotti.

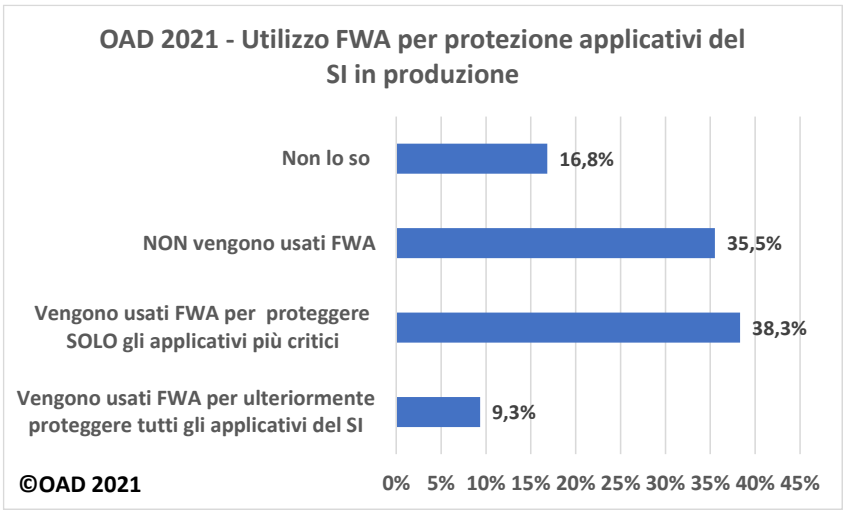

Fig. 7.2.5-4

Un altro aspetto fondamentale per la sicurezza digitale degli applicativi di un SI è la loro continua manutenzione correttiva: tempestivo aggiornamento delle versioni rilasciate, installazione tempestiva di fix e patch, e così via. La fig. 7.2.5-5 mostra che quasi l'80% dei SI gestisce la manutenzione correttiva degli applicativi, e di questi più della metà la effettua per tutti gli applicativi presenti nel SI.

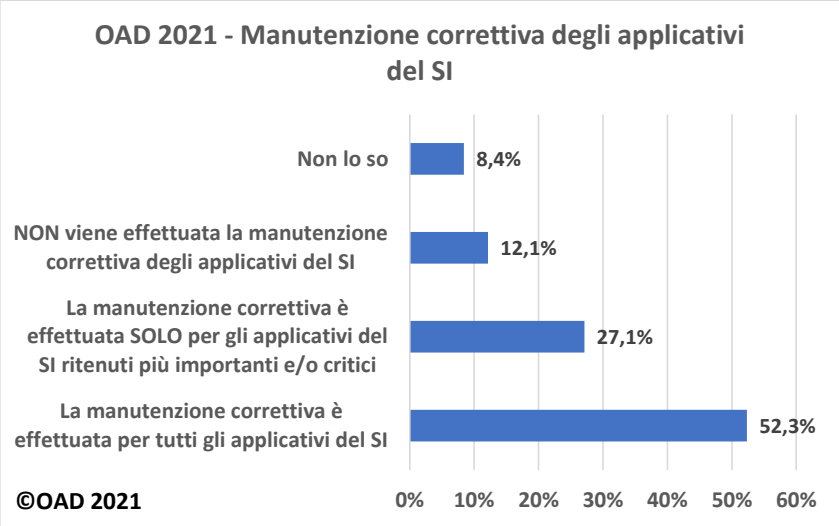

Fig. 7.2.5-5

7.2.6 Misure tecniche di sicurezza digitale per la protezione dei dati

I dati trattati dal SI costituiscono un reale ed importante bene (asset) per l'azienda/ente, e come tali devono essere protetti e gestiti. Numerose le tecniche e gli strumenti per la loro protezione, a partire 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", cui seguono la crittografia dei dati critici e riservati, inclusi quelli personali e sensibili per la privacy, e le tecniche di back up e di ripristino.
La situazione della classificazione dei dati per i SI delle aziende/enti rispondenti è evidenziata nella fig. 7.2.6-1. Ben il 71% dichiara di aver classificato i dati, e di questi il 45,8% dichiara di averlo fatto solo per i dati trattati da alcune applicazioni; tipicamente dati personali, confidenziali per il business e/o per le attività, etc. Quasi il 20% non li ha (ancora) classificati.

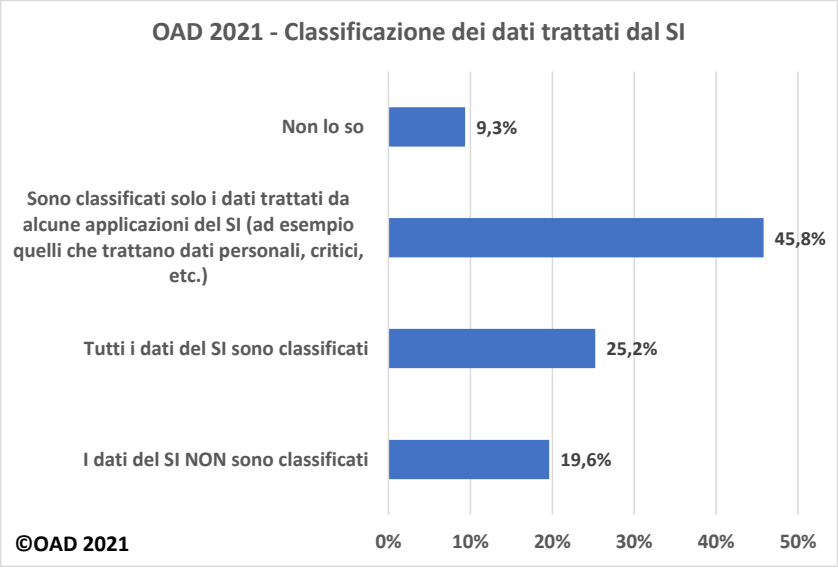

Fig. 7.2.6-1

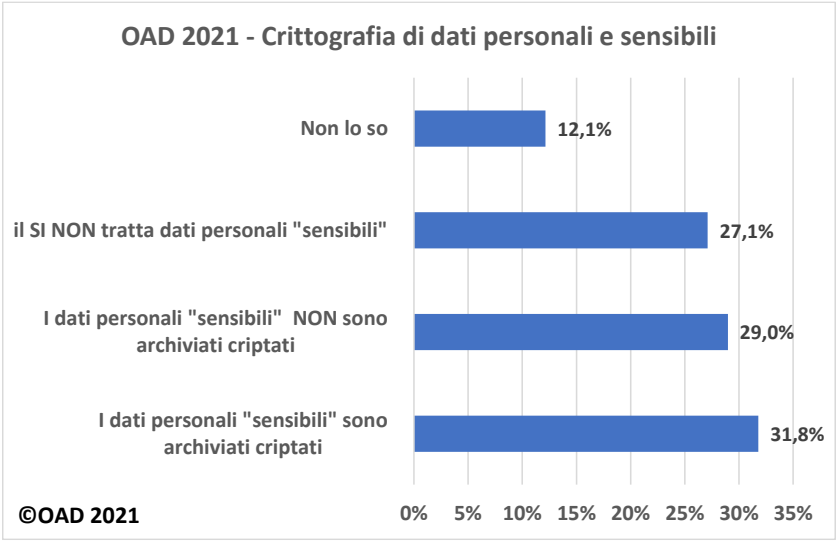

Fig. 7.2.6-2

I dati da tenere più riservati e quelli inerenti i dati personali normati dalla direttiva GPDR sulla privacy dovrebbero essere crittografati per garantire la loro effettiva confidenzialità, in particolare quando archiviati. Come si evince dalla fig. 7.2.6-2, il 27,1% dei SI delle aziende/enti rispondenti non trattano dati personali ed il 31,8 % che li tratta, li cripta anche.
Vengono poi criptati dati ritenuti riservati e confidenziali, non di tipo personale, dal 35,5% delle aziende/enti rispondenti, come mostrato nella fig. 7.2.6-3.

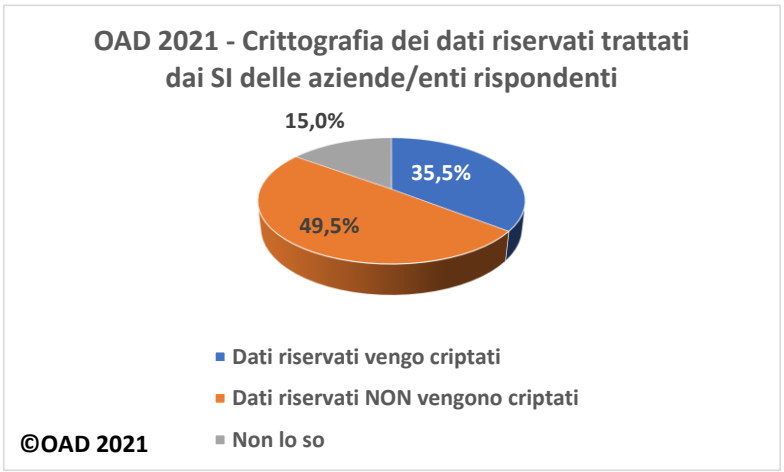

Fig. 7.2.6-3

Le chiavette USB sono un comodo strumento per copiare file, e date le loro attuali grandi dimensioni, anche per copiare directory di qualche Tera Byte. Quasi tutti i sistemi ICT, dal PC al server e ad uno storage di grandi dimensioni, hanno porte USB per default aperte ed utilizzabili. Le chiavette sono quindi un utile strumento per fare delle copie dei propri file, archiviandoli in maniera sicure crittografandoli, o anche per rubare significative quantità di dati.

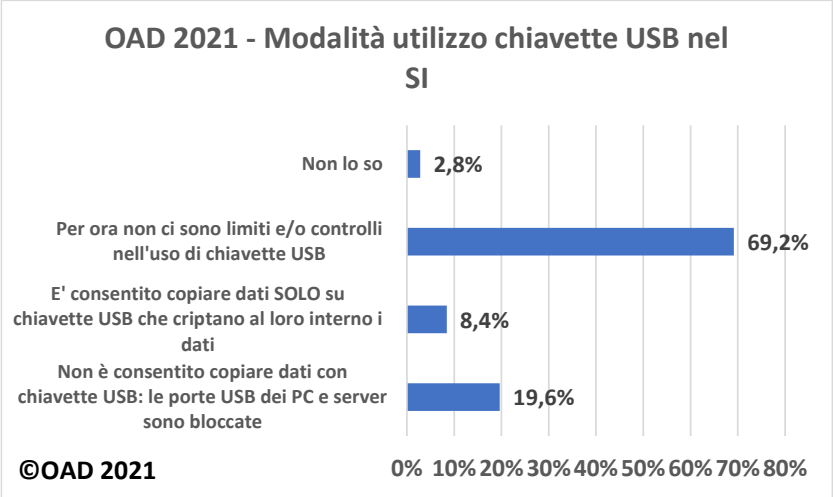

Fig. 7.2.6-4

La fig. 7.2.6-4 mostra che la maggior parte, il 69,2%, delle porte USB nei dispositivi ICT sono liberamente utilizzabili, anche se è possibile bloccarle configurando opportunamente lo stesso sistema ICT. Dal grafico due interessanti dati emergono, con % piccole ma significative per un trend che andrà a consolidarsi nel prossimo futuro: quasi il 20% di porte bloccate, e l'uso, ancora marginale per ora, di chiavette USB con capacità di crittografare, le uniche con le quali è possibile copiare file o directory di file (cartelle).
L'effettuazione dei backup è una ulteriore importante misura per la protezione dei dati e dei programmi del SI.
La fig. 7.2.6-5 mostra che la metà dei SI effettua il backup "a regola d'arte": tutti i dati ed i codici software sono regolarmente e periodicamente backuppati in maniera automatica, con copie dei backup criptate su media removibili (es: hard disk removibile e off line) e allocate in sedi geograficamente diverse da quelle dei Data Center/Computer room. Poco più di 1/5 dei SI effettua regolarmente i backup, ma non cripta le copie e non trasferisce questi dati su media removibili, allocate in sedi diverse dal Data Center/Computer room. Solo il 10,4% non gestisce in maniera omogenea ed automatizzata il backup per tutti i sistemi ICT del SI, e l'1,9% lascia la responsabilità del backup al singolo utente: questo in caso di SI molto piccoli.
Nel complesso una situazione buona che ancora indica come il bacino dei SI considerati nell'indagine OAD 2021 abbia in media un elevato livello di sicurezza digitale.
Per una effettiva disponibilità dei dati del SI non solo occorre effettuare frequenti, periodici e sistematici backup, ma anche saper ripristinare uno o più sistemi ICT, in malfunzionamento o bloccati, tramite i dati di backup. La fig. 7.2.6-6 mostra che il 46% delle aziende/enti rispondenti ha definito come ripristinare i vari sistemi dai dati dei backup ed è in grado di usare correttamente tali procedure, provandole periodicamente: tale % è congruenti coi dati emersi con la precedente domanda sul backup.

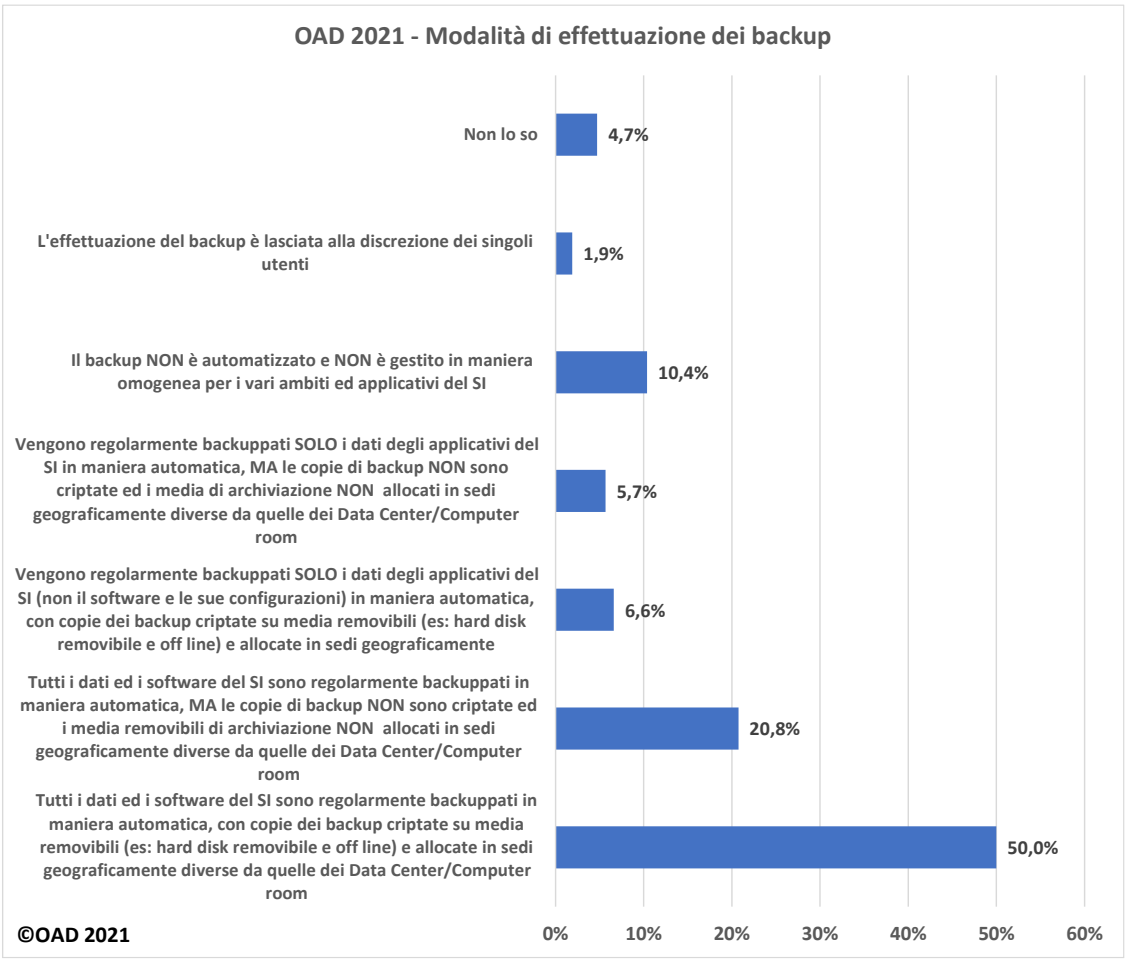

Fig. 7.2.6-5

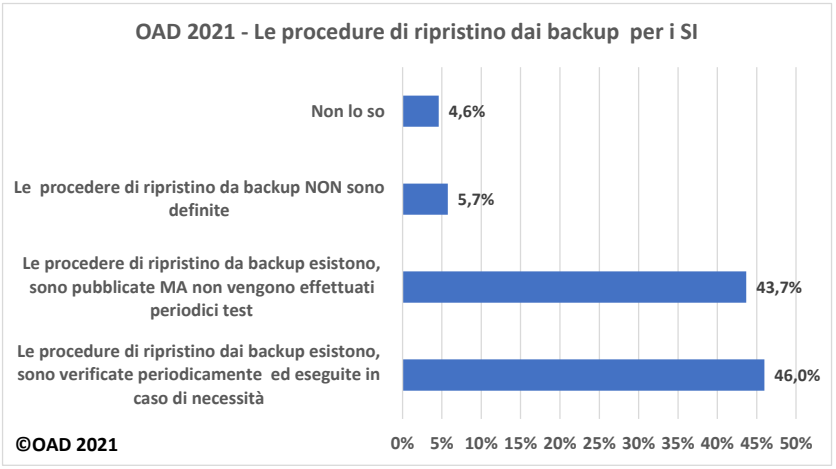

Fig. 7.2.6-6

Il 43,7% ha definito tali procedure, ma non le prova periodicamente. Solo il 5,7 % dei SI non le ha definite.

7.2.7 Misure e strumenti per la gestione ed il controllo della sicurezza digitale dei SI

Le misure e gli strumenti per la gestione della sicurezza digitale di un SI nel suo complesso sono un mix di strumenti tecnici ed organizzativi, ed alcune possono essere considerate anche come misure di contrasto specifiche. L'autore ha preferito evidenziare in un paragrafo a sé stante gli strumenti tipicamente usati per la gestione operativa della sicurezza digitale, che sovente sono integrati ed in parte coincidono con quelli per la gestione del sistema informatico e/o 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[24].
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.

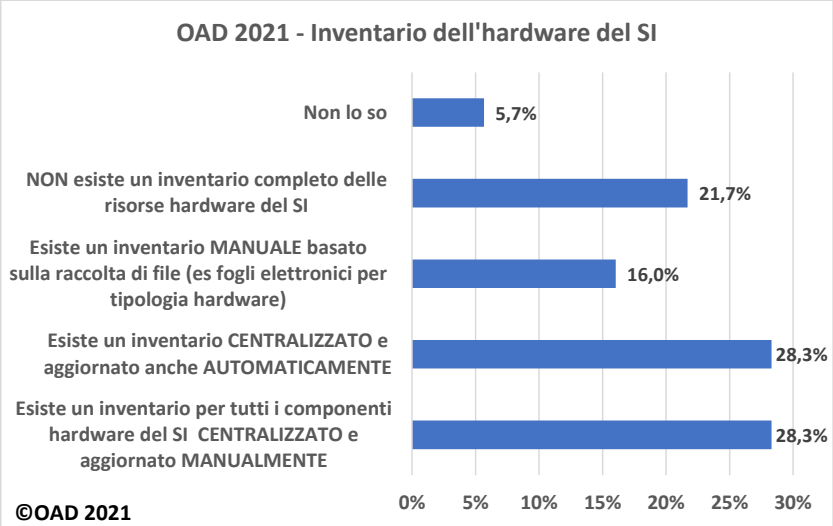

Fig. 7.2.7-1

La fig. 7.2.7-1 mostra la situazione per l'inventario hardware delle risorse ICT del SI dell'azienda/ente rispondente. Solo il 21,7% non ha un inventario delle risorse hardware. Il 72,6% ne ha uno, ma realizzato con logiche diverse: il 16% realizza una raccolta manuale in fogli elettronici o in altri tipi di documenti dell'hardware presente, probabilmente gestiti in modalità diverse e forse locali per i diversi tipi di hardware.

[24] 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.

Il 56,6% ha un inventario centralizzato, ma solo la metà di questi lo alimenta e lo aggiorna automaticamente con appositi software.

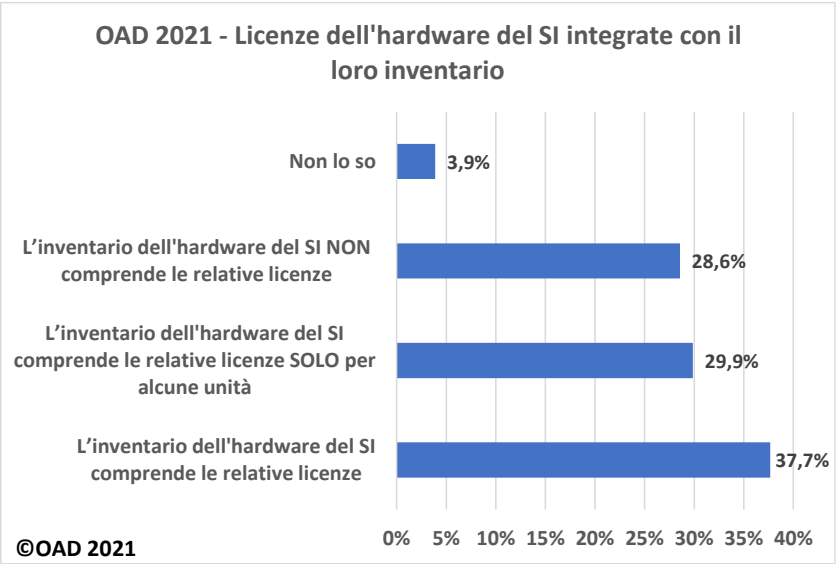

Fig. 7.2.7-2

Le licenze per l'hardware, in particolare per la sua manutenzione, dovrebbero essere associate all'inventario, per una loro efficace gestione. La fig. 7.2.7-2 mostra che tale associazione esiste nel 67,5% dei casi, ma di questi solo il 37,7% è effettuata per tutte le risorse hardware, e nel 28,6% dei casi tale associazione non esiste.
Per quanto riguarda i programmi software del SI, sia di base sia applicativo, la fig. 7.2.7-3 evidenzia che il 30,2% dei SI rispondenti ha un inventario del software centralizzato ed automatizzato, e che il 26,4% dei SI non lo ha. Si noti che questa % è superiore di qualche punto all'analoga per l'hardware: questo è logico, dato che il numero di software presenti in un SI è di molto superiore a quello dell'hardware.

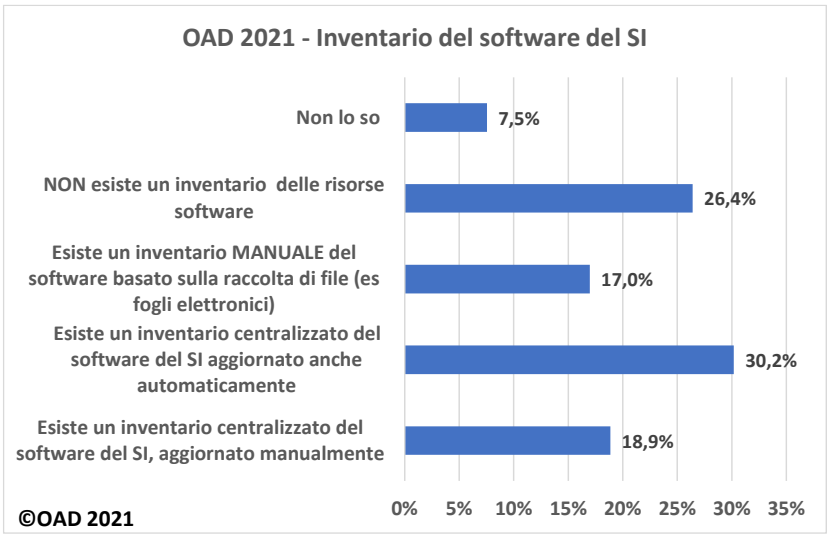

Fig. 7.2.7-3

Il 35,8% dispone di un inventario manuale, di cui il 17% è effettuato con un insieme di file, ad esempio fogli elettronici, gestiti anche localmente.

Soprattutto per il software, le licenze di manutenzione dovrebbero essere associate all'inventario.
La fig. 7.2.7-4 mostra che questo avviene, per tutti i software presenti, nel 28,6% dei casi, e solo per alcuni software nel 37,1% dei casi. Confrontando questi dati con gli analoghi per l'hardware di fig. 7.2.7-2, si notano per il software % più basse. Come già evidenziato, la probabile causa è data dal numero assai maggiore di programmi software in esercizio in un SI, e che in alcuni casi non sono considerati i software sui dispositivi d'utente, degli IOT e dell'automazione industriale.
Gli inventari dell'hardware e del software dovrebbe infine essere correlati ed integrati, per poter saper su quale hardware sono in funzione determinati programmi. La situazione su tale integrazione per i SI emersi dall'indagine OAD 2021 è mostrata in fig. 7.2.7-5. Quasi i 2/3 dei SI hanno correlati/integrati i due inventari. Un altro indice del buon livello medio di sicurezza digitale dei SI emersi nel sondaggio 2021.
Nell'ambito della gestione operativa della sicurezza digitale, lo strumento chiave è il sistema di monitoraggio e controllo, il più delle volte integrato con quello dell'intero SI. Ed infatti così avviene per il 32,1% dei SI delle aziende/enti rispondenti, che lo gestiscono al loro interno con loro personale (on premise), mentre il 13,2% monitorizza internamente la sola sicurezza digitale, come mostrato nella fig. 7.2.7-6.

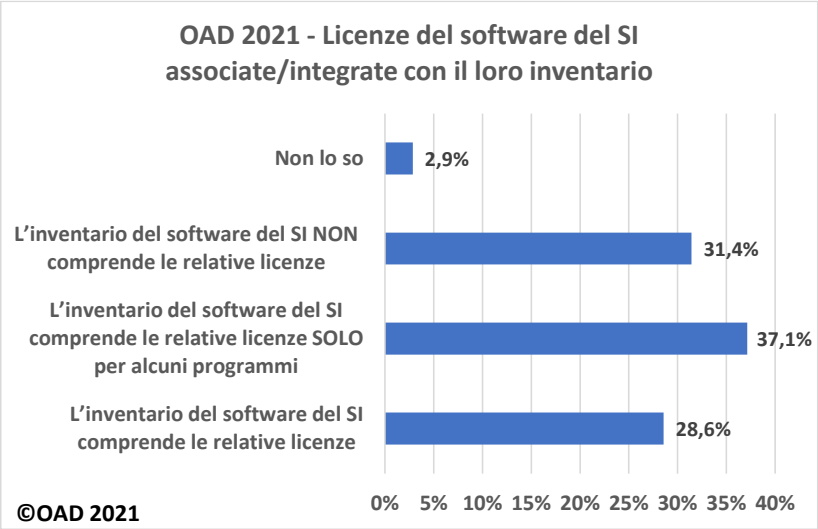

Fig. 7.2.7-4

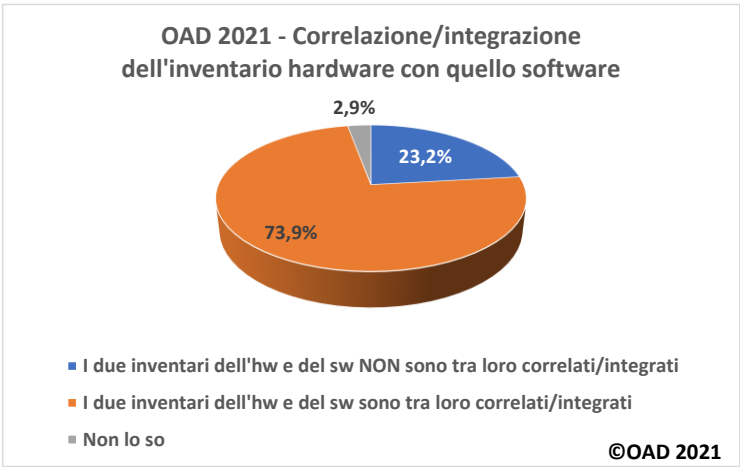

Fig. 7.2.7-5

L'8,5% ha terziarizzato la gestione della sicurezza digitale ed il 17% controlla separatamente i vari strumenti ed i vari sistemi dedicati alla sicurezza digitale. Solo il 18,9% dei casi non ha strumenti di monitoraggio e

controlli on premise o terziarizzati. Nel complesso quindi, pur se in modalità differenti, il 70,8% dei SI effettua un monitoraggio e controllo del funzionamento e delle prestazioni degli strumenti ICT per la sicurezza digitale.

Una domanda, presente solo nel questionario completo, precisa se e come sia gestita la configurazione dei sistemi ICT in merito alla sicurezza digitale, e le risposte avute sono evidenziate nella fig. 7.2.7-7. Nel 53,2% dei SI delle aziende/enti rispondenti le configurazioni per la sicurezza digitale nei sistemi ICT sono sistematicamente aggiornate, manualmente o in maniera automatica, ma nel 17% dei casi non sono configurate alla prima installazione, come avviene per il 23,4% dei SI, e tanto meno con gli eventuali, successivi aggiornamenti del software.

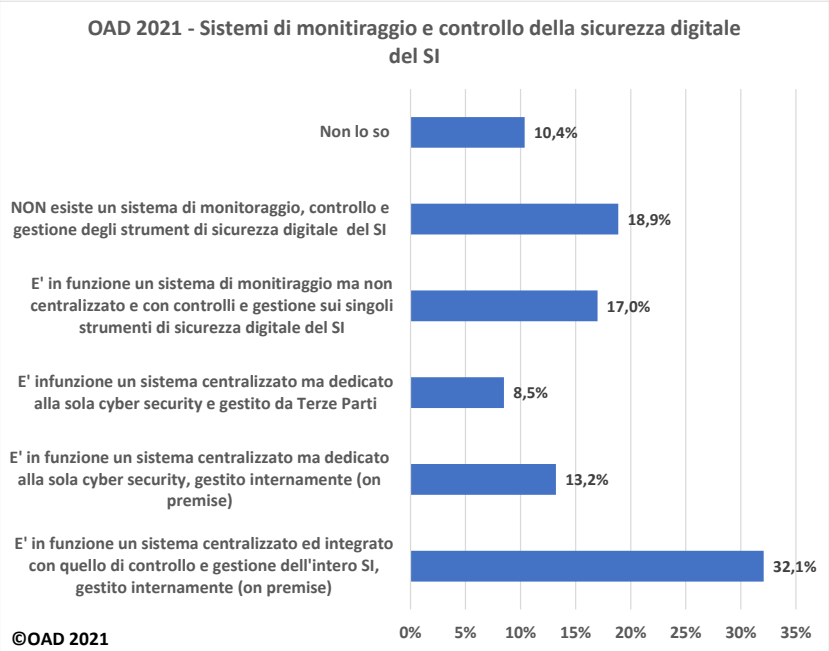

Fig. 7.2.7-6

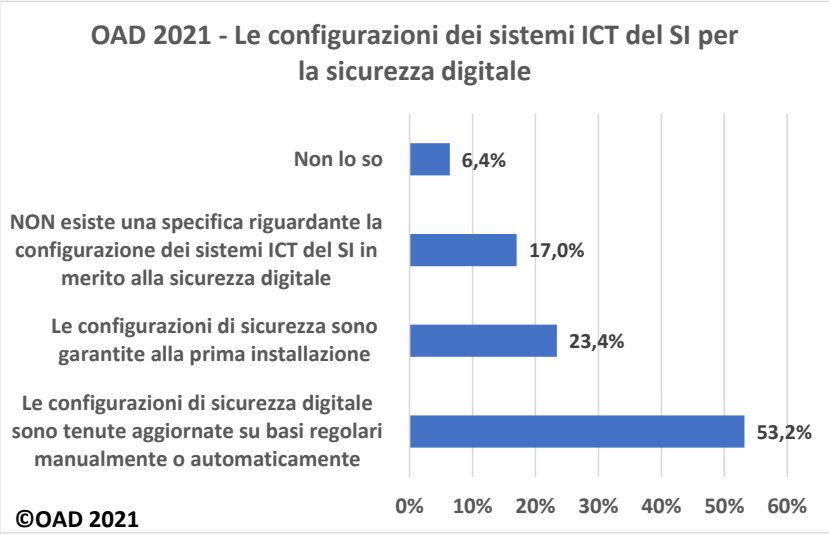

Fig. 7.2.7-7

Nell'ambito della gestione operativa della sicurezza digitale rientrano anche le periodiche analisi di vulnerabilità ed i penetration test, chiamati anche per brevità "pentest".
Come mostrato nella fig. 7.2.7-8, per il 71,4% dei SI l'analisi delle vulnerabilità viene effettuata, ma solo per il 37,1% di questi tale analisi è sistematica e periodica, per il resto viene effettuata o quando richiesto dal vertice dell'azienda/ente o in caso di eventi o necessità specifiche: ad esempio dopo un attacco, per verifiche in caso di specifiche certificazioni, e così via.

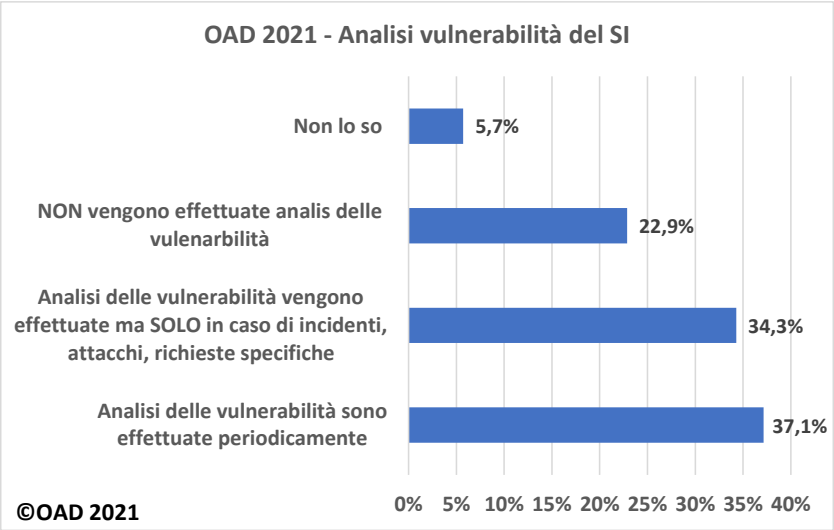

Fig. 7.2.7-8

A fianco dell'analisi delle vulnerabilità, e in particolare dopo aver effettuato opportuni aggiornamenti dei software in uso, è opportuno effettuare dei pentest per verificare che le vulnerabilità individuate siano state soppresse e che le misure di prevenzione e protezione della sicurezza digitale siano correttamente in grado di reagire ai tentativi di penetrazione di prova.

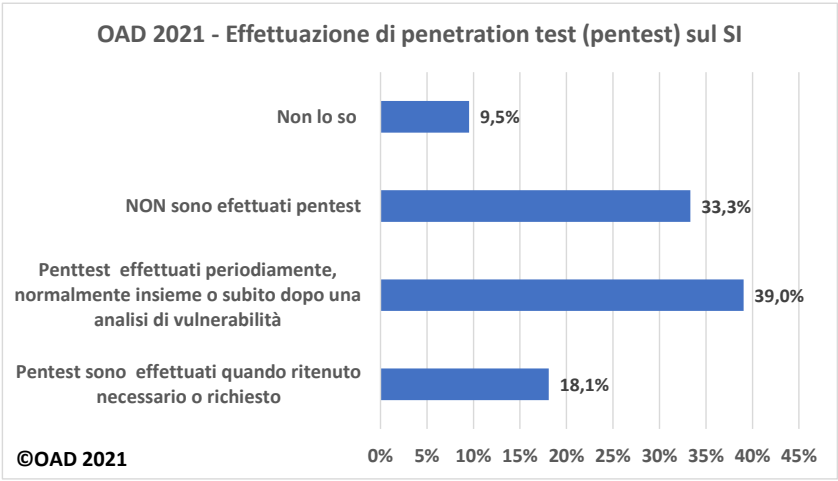

Fig. 7.2.7-9

La fig. 7.2.7-9 mostra che il 39% dei SI effettua periodicamente e regolarmente questa verifica, e che il 18,1% li effettua solo quando ritenuto necessario: ad esempio su richiesta, per contribuire ad una certificazione aziendale, etc.
Nell'ambito della gestione della sicurezza digitale un aspetto importante è la definizione di un Piano di

Disaster Recovery (DR) del SI, 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; e a questo si è aggiunta ora, e in maniera preoccupante e forse perdurante, la cyber warfare. 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. 7.1.2-3 e in fig. 7.1.2-4).
La fig. 7.2.7-10 evidenzia che il 67,3% dei SI delle aziende/enti rispondenti ha un Piano di DR.

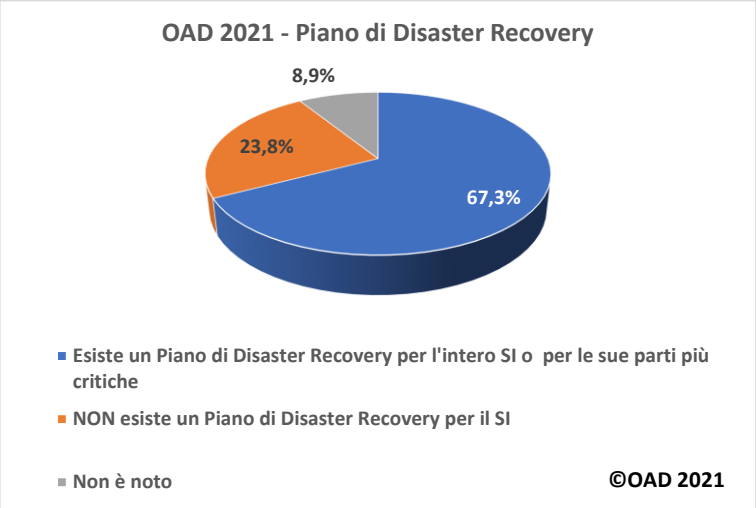

Fig. 7.2.7-10

Ulteriori domande sul DR sono state poste solo nel questionario completo. La prima, per chi ha un piano di DR, riguarda l'allocazione o la prenotazione a fornitori terzi delle risorse necessarie per poterlo realmente attuare in caso di disastro. La fig. 7.2.7-11 mostra che poco più di ¼ delle aziende/enti rispondenti, pur avendo un piano di DR, non ha previsto alcuna risorsa ICT alternativa da utilizzare. Il piano di DR è quindi solo sulla carta, di fatto non subito attuabile nel momento in cui si verificasse un disastro; occorrerebbe trovare ed attivare le risorse alternative per il DR: senza il piano di DR è un mero documento burocratico. Il 67,6% dei SI ha previsto le risorse alternative per il DR, con diverse modalità: solo l'11,8% ha risorse ICT in "stand by caldo", ossia già attivate, configurate e pronte ad entrare in azione in tempo molto brevi. Il 29,4% ha le risorse a "freddo", ossia preparate ma da attivare in caso di DR. Il 26,5% ha "prenotato" le risorse ICT alternative da utilizzare, e questo richiede tempi di attivazione ben più lunghi rispetto allo stand by a freddo.

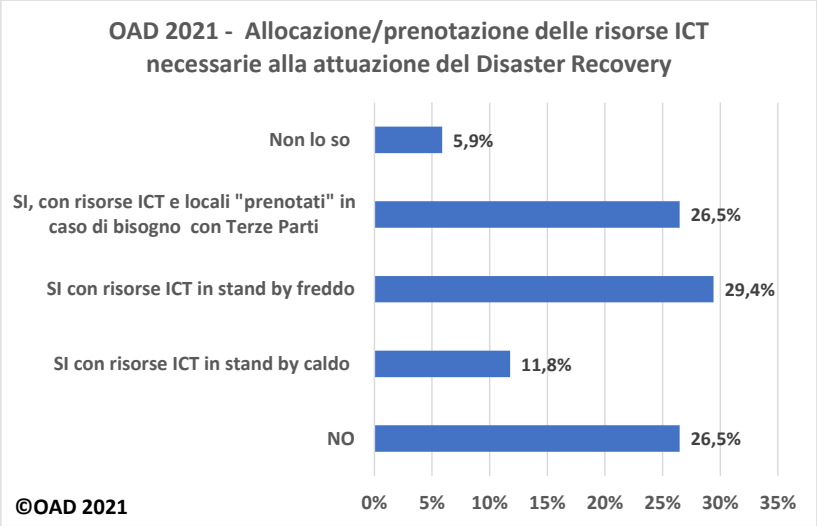

Fig. 7.2.7-11

Con l'indagine OAD 2021 il DR nel complesso risulta presente nella maggior parte dei SI, anche di piccole dimensioni, con un netto miglioramento rispetto a quanto emerse con le indagini OAD degli anni scorsi, ed anche del più recente 2020. Per ottenere un simile risultato ha sicuramente contribuito il "disastro" della pandemia Covid-19 con i suoi lockdown ed il forte incremento nell'uso dei servizi online e nella larga diffusione del lavoro da remoto, lo smart working. La seconda domanda del solo questionario completo riguarda l'effettuazione di esercitazioni periodiche (tipicamente a tavolino, chiamate DTE, Desk Top Exercise), ad esempio su base semestrale, o annuale, per verificare la corretta impostazione delle procedure organizzative e la preparazione del personale da coinvolgere in un DR: senza periodiche sperimentazioni e senza la pre-allocazione delle risorse ICT alternative, il piano di DR ben difficilmente potrà essere attivato nei tempi necessari ed a costi ragionevoli.
La fig. 7.2.7-12 mostra che più di ¼, 26,5% delle aziende/enti rispondenti al questionario completo e che hanno definito un Piano di DR non effettuano simulazioni e prove di test di DR. Il 50% effettua queste prove di DR solo su per alcune parti del SI, quelle più importanti e critiche, e di questi il 32,4% in maniera periodica.

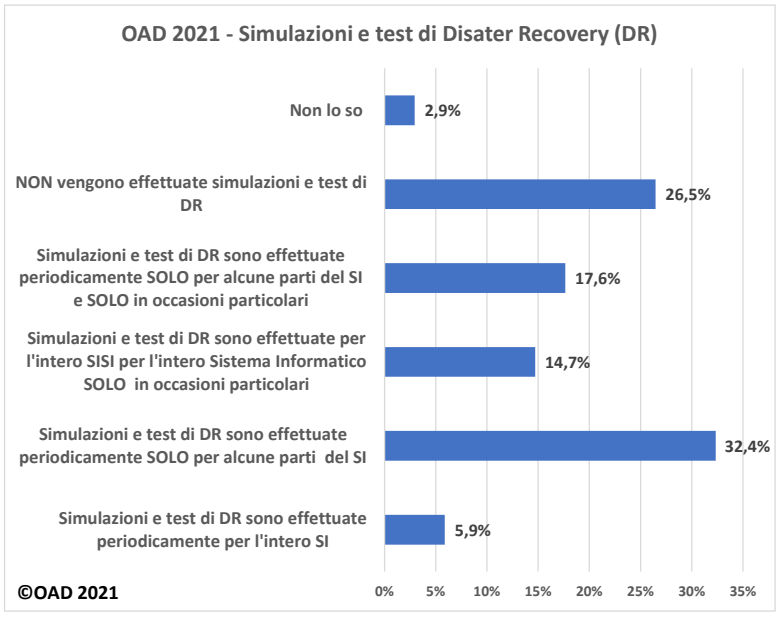

Fig. 7.2.7-12

7.3 La macro valutazione qualitativa del livello di sicurezza digitale del SI oggetto delle risposte

In vari precedenti capitoli ed in questo, §7, si è evidenziato come i SI oggetto delle risposte alla presente indagine OAD 2021 abbiano, tranne qualche eccezione, nel complesso un buon livello di sicurezza digitale.
Oltre ai specifici dettagli di questo e dei precedenti capitoli, questa valutazione è confermata dai risultati della macro valutazione qualitativa del livello di sicurezza digitale che veniva automaticamente ed in tempo reale evidenziata a chi completava i questionari online. Questa valutazione è stata introdotta dalla edizione OAD 2020 come una delle motivazioni per compilare uno dei questionari online.
L'Allegato A2 illustra la logica ed i criteri per questa macro valutazione e la fig. 7.3-1 mostra i risultati di questa macro valutazione, ottenuti sommando le valutazioni emerse dal questionario completo e da quello ridotto.
Più della metà dei SI, il 54%, per le risposte fornite e che OAD ovviamente non può verificare, dato in primo luogo la rigorosa anonimità dell'indagine, hanno un buon livello di misure di sicurezza digitale in funzione delle esigenze dell'azienda/ente che li possiede. Il 36% dei SI hanno invece misure insufficienti e non idonee per una effettiva sicurezza digitale, sempre in funzione delle esigenze.

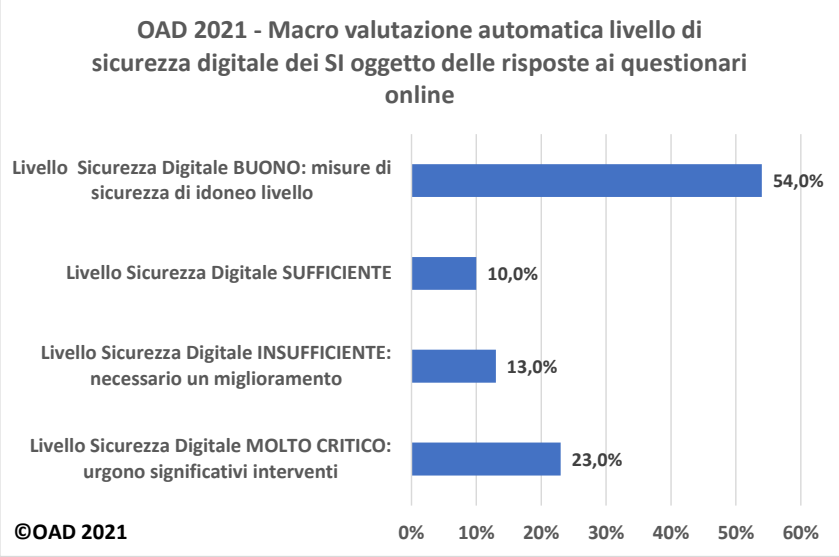

Fig. 7.3-1

8. Attacchi alle infrastrutture critiche, cyber/financial crime e cyber terrorismo dai dati della Polizia Postale e delle Comunicazioni

La Polizia Postale e delle Comunicazioni da anni collabora con AIPSI per OAD, fornendo significativi dati sulle azioni svolte in Italia nel 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 sia a livello regionale, per organizzazioni imprenditoriali ed enti, sia a livello nazionale.

Il C.N.A.I.P.I.C., Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche[25], 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, chiamate "**infrastrutture critiche**" ed indicate inizialmente dalla Direttiva 2008/114/CE[26], recepita in Italia con il D.Lgs n. 61 dell'11 aprile 2011[27]. Quest'ultima Direttiva è stata poi superata dalla Direttiva UE 2016/1148[28], recepita in Italia dal D. Lgs. n. 65 del 18/5/2018[29], ed amplia il concetto di "infrastrutture" con quello di "servizi essenziali": chiamata **NIS**, **Network and Information Security, essa** elenca gli obblighi in termini di cybersecurity per le reti ed i sistemi informativi degli operatori dei servizi essenziali in modo da omogeneizzare la loro cyber security in tutti i paesi dell'Unione Europea.
La Direttiva NIS è applicata agli OSE[30], Operatori di Servizi Essenziali, e ai FSD[31], Fornitori di Servizi Digitali, coinvolgendo cinque Ministeri ove sono state designate le "Autorità competenti NIS": Sviluppo Economico (MISE), infrastrutture e trasporti, economia, salute e ambiente). A logica o funzionale del NIS in Italia è schematizzata nella fig. 8-1. Il NIS richiede di garantire ai servizi essenziali una reale cyber resilienza basata su solide misure di sicurezza digitale, che includano misure preventive adeguate contro il cyber rischio, oltre a strumenti e sistemi adeguati per gestire e segnalare incidenti e violazioni dei dati. Da un punto di vista tecnico, per la gestione della sicurezza digitale richiede l'integrazione dello standard ISO/IEC 27001 che specifica le richieste e le misure di sicurezza con lo standard ISO/IEC 22301 per la gestione della continuità operativa dei sistemi informativi (business continuity).

[25] https://www.commissariatodips.it/profilo/cnaipic/index.html
[26] https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32008L0114
[27] https://www.gazzettaufficiale.it/eli/gu/2011/05/04/102/sg/pdf
[28] https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32016L1148
[29] https://www.gazzettaufficiale.it/eli/id/2018/06/09/18G00092/sg
[30] Sono i soggetti, pubblici o privati, che forniscono servizi essenziali per la società e l'economia nei settori sanitario, dell'energia, dei trasporti, bancario, delle infrastrutture dei mercati finanziari, della fornitura e distribuzione di acqua potabile e delle infrastrutture digitali.
[31] Sono persone giuridiche che forniscono servizi di *e-commerce*, *cloud computing* o *motori di ricerca*, con stabilimento principale, sede sociale o rappresentante designato sul territorio nazionale. Gli obblighi previsti per gli FSD non si applicano alle imprese che la normativa europea definisce "piccole" e "micro", quelle cioè che hanno meno di 50 dipendenti e un fatturato o bilancio annuo non superiore ai 10 milioni di Euro.

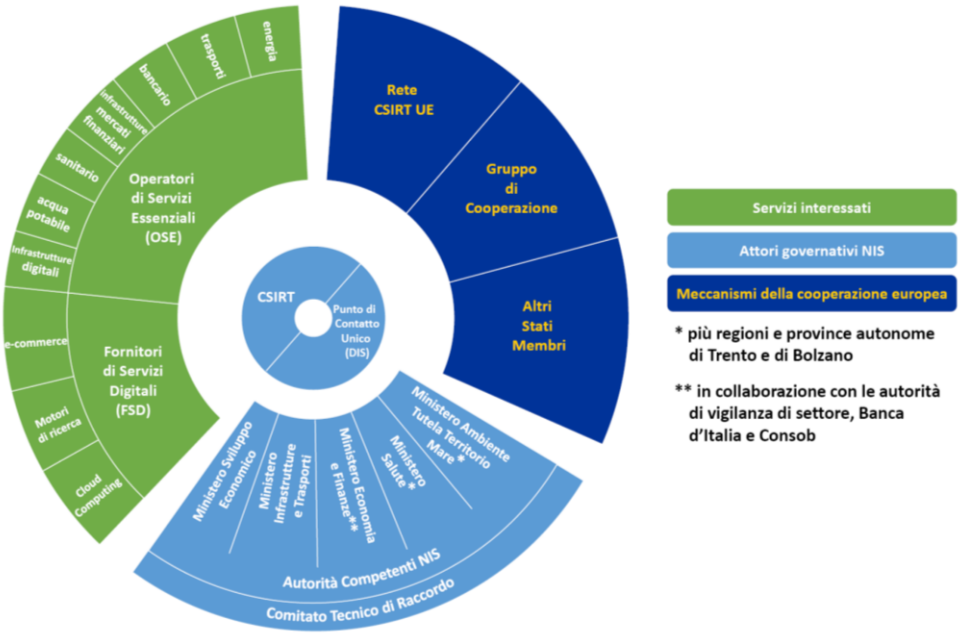

Fig. 8-1(Fonte: Presidenza del Consiglio)

Dopo i primi anni di applicazione nei vari paesi europei della direttiva NIS si sono evidenziate varie difficoltà nell'effettiva sua attuazione, e soprattutto nel suo controllo. Queste difficoltà hanno portato alla necessità urgente di aggiornarla e potenziarla con una nuova direttiva europea chiamata NIS 2, che dovrebbe sostituire la precedente NIS agli inizi del 2023. I miglioramenti e potenziamenti previsti includono:

- eliminare la distinzione tra OSE e FSD e fornire una nuova classificazione tra "essenziali" (es. cloud) ed "importanti" (es. social net) con diversi regimi di controllo;
- ampliare i servizi essenziali, includendo la produzione di prodotti farmaceutici, i dispositivi medici e prodotti chimici, il settore alimentare, la gestione delle acque reflue e dei rifiuti, i servizi postali, la pubblica amministrazione;
- rafforzare i requisiti di sicurezza digitale;
- migliorare la sicurezza in particolare nelle supply chain;
- semplificare gli obblighi di segnalazione di attacchi digitali;
- introdurre misure di supervisione più rigorose e requisiti di applicazione più severi;
- meglio integrarsi e non sovrapporsi con altre normative e direttive europee sulla sicurezza digitale, quali ad esempio quelle sulla privacy del GDPR.

Con riferimento ai dati forniti dalla Polizia Postale, la tabella in fig. 8-2 confronta i dati inerenti alle attività svolte dal C.N.A.I.P.I.C. nel periodo 2016-2021 (1° quadrimestre) sulle infrastrutture critiche italiane.

Protezione strutture critiche	1 gen - 30 apr 2021	1 gen - 31 dic 2020	1 gen - 31 dic 2019	1 gen – 31 dic 2018	1 gen – 31 dic 2017	1 gen – 31 dic 2016
Attacchi rilevati	282	509	1181	459	1.032	844
Alert diramati	24.824	83.416	82.484	80.777	31.524	6.721
Indagini avviate	34	103	155	74	72	70
Persone arrestate	0	n.d.	3	1	3	3
Persone denunciate/indagate	0	105	117	14	1.316	1.226
Perquisizioni	n.d.	n.d.	n.d.	n.d.	73	58
Richiesta di cooperazione internazionale in ambito Rete 24/7 High Tech Crime G8 (Convenzione Budapest)	17	69	79	108	83	85

Fig. 8-2 (Fonte Polizia Postale e delle Comunicazioni)

Si evidenzia la crescita degli allarmi emanati e diramati, che vanno ad assestarsi con piccoli tassi di crescita dal 2019.

Diverso il tema degli attacchi rilevati alle infrastrutture che dovrebbero essere le più sicure in assoluto in Italia, e che oscilla tra incrementi e decrementi come evidenziato nella fig. 4 sul trend degli attacchi digitali rilevati nelle indagini OAI/OAD dal 2007 al 1° semestre 2021. Oltre al ben noto inseguimento tra guardie e ladri cibernetici, ormai giocato a livello mondiale, possono influire su questi dati il riposizionamento di NIS 2 con l'estensione anche del tipo di servizi essenziali e del perimetro[32] di cybersecurity nazionale.
Le indagini avviate dalla Polizia Postale sono in numero ben inferiore rispetto agli attacchi rilevati, ad ancora più basso il numero di persone denunciate, indagate e alla fine arrestate. 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 – in merito, e vi siano agenzie e forze specifiche come descritto in §3.5.4.

La tabella in fig. 8-3 sintetizza le attività della Polizia Postale in contrasto al Financial Cyber Crime.

Financial Cyber Crime	1 gen - 30 apr 2021	1 gen - 31 dic 2020	1 gen - 31 dic 2019	1 gen – 31 dic 2018	1 gen – 31 dic 2017	1 gen – 31 dic 2016
Transazioni Fraudolente Bloccate	€ 20.200.000	€ 33.186.674	€ 21.333.990	€ 38.400.000	€ 20.839.576	€ 16.050.813
Somme Recuperate	€ 8.700.000	€ 20.046.240	€ 18.000.000	€ 9.000.000	€ 862.000	nd
Recupero €/€ frodati	43,07%	60,40%	84,37%	23,44%	4,14%	

Fig. 8-3 (Fonte Polizia Postale e delle Comunicazioni)

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. Questo tipo di crimine informatico include anche attacchi indirizzati alle piattaforme di E-Commerce, ivi inclusi i relativi pagamenti on line. Nel 2020 le transazioni finanziarie bloccate sono aumentate rispetto all'anno precedente, e questo molto probabilmente a causa Covid 19. Sono aumentate anche le somme recuperate, il che denota il continuo miglioramento delle capacità di contrasto da parte della Polizia Postale.

Cyber Terrorismo	1 gen - 30 apr 2021	1 gen - 31 dic 2020	1 gen - 31 dic 2019	1 gen – 31 dic 2018
Spazi web monitorati	11.962	37.081	36.377	36.000

Fig. 8-4 (Fonte Polizia Postale e delle Comunicazioni)

La tabella in fig. 8-4 fornisce il dato sui controlli della Polizia Postale sui siti web, che insiemi ad alcune social net, sono alla base e contribuiscono al proselitismo, alla preparazione e al coordinamento di attacchi terroristici. Negli anni il numero di siti monitorati aumenta leggermente, ed è nell'ordine delle decine di migliaia, in innumerevoli lingue. Queste cifre forniscono una chiara indicazione della vastità e complessità del problema che quotidianamente occorre prevenire e contrastare.

[32] Con DPCM n. 131 del 30 luglio 2020 (https://www.gazzettaufficiale.it/eli/id/2020/10/21/20G00150/sg), entrato in vigore il 5 novembre 2020, è definito il "Perimetro di sicurezza nazionale cibernetica", che specifica disposizioni in materia di forniture di determinati beni, sistemi e servizi ICT per reti, sistemi e servizi informatici essenziali per la sicurezza nazionale.

ALLEGATI

Allegato A Aspetti metodologici dell'indagine OAD 2021

L'indagine OAD 2021, come le precedenti, è indirizzata da un lato all'analisi totalmente anonima degli attacchi digitali intenzionali ad aziende/enti in Italia e 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; dall'altro la rilevazione ed analisi, sempre in maniera anonima, delle principali caratteristiche dei sistemi informatici dei rispondenti, e delle loro misure di sicurezza in atto.
Sono considerati solo gli attacchi che sono stati effettivamente rilevati, e non è necessario che essi abbiano creato danni ed impatti negativi al SI 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 OAD 2021 si è basata sulle risposte, anonime, a due questionari con risposte predefinite da selezionare, uno "completo" con 206 domande raccolte in 14 gruppi, e l'altro "ridotto" con 126 domande raccolte negli stessi 14 gruppi, entrambi on line sulla piattaforma LimeSurvey installata sul sito web www.oadweb.it. In entrambi i due questionari i gruppi di domande relative ad ogni tipo di attacco venivano automaticamente saltate se quel tipo di attacco non era stato effettuato o rilevato. Questa logica implementativa dei questionari online riduce significativamente i tempi per completare l'intero questionario.
Entrambi i questionari sono anonimi: 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 e Malabo garantiscono inoltre la totale riservatezza sulle risposte raccolte, utilizzate solo per elaborare i grafici del presente del presente rapporto.
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 quindi 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, Malabo 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 tenuti da AIPSI.
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, che viene pubblicato sul sito 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 differisce a seconda che le risposte siano multiple (l'utente può selezionare più risposte per la stessa domanda) 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: per queste 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.
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 e creati i relativi grafici.
Tutti i grafici e le elaborazioni di OAD 2021 sono state effettuate "sommando" i rislutati ottenuti dai du questionari.
Entrambi i questionari OAD 2021 sono stati progettati e realizzati da Malabo Srl basandosi sul software open source Lime Survey nel dominio del sito OAD, https://www.oadweb.it/, realizzato e gestito da Malabo.

A.1 La tassonomia degli attacchi digitali (che cosa si attacca) per OAD 2021

L'edizione 2021 ha ripreso la logica della precedente edizione del 2020, migliorando alcune definizioni e riducendo a 14 le tipologie di attacco considerate: è stato eliminato l'attacco ai sistemi in blockchain, nei precedenti anni inserito come una interessante novità, ma che è una piattaforma applicativa, e pertanto gli attacchi ad essa rientrano in altre tipologie, più avanti elencate, quali ad esempio gli attacchi alle applicazioni e alle loro configurazioni (n.9 della lista) e ai dati da questi trattati (n.10)..
La classificazione degli attacchi in OAD 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, descritte in §A.1.1.
Le 14 tipologie di attacco considerate (il che cosa attacco) in OAD 2021 :

- Distruzione fisica di dispositivi ICT o di loro parti
- Furto di dispositivi ICT mobili
- Furto di dispositivi ICT fissi o di loro parti
- Furto informazioni da sistemi fissi (PC, server, storage system, etc.)
- Furto informazioni da sistemi mobili (palmari, smartphone, tablet, etc.)
- Attacchi all'identificazione, autenticazione e autorizzazioni degli utenti finali e privilegiati
- Attacchi alle reti, locali e geografiche, fisse e wireless, e ai DNS
- Uso non autorizzato sistemi ICT nel loro complesso (dai dispositivi d'utente ai server-storage e ai servizi in cloud)
- Modifiche non autorizzate ai programmi applicativi e alle loro configurazioni
- Modifiche non autorizzate alle informazioni trattate dai sistemi ICT
- Saturazione risorse digitali (DoS, DDoS)
- Attacchi ai propri sistemi in cloud o in housing/hosting presso fornitori terzi
- Attacchi a dispositivi IoT (Internet of Things) in uso
- Attacchi ai propri sistemi di automazione industriale e di robotica (OT, Operational Technology).

Le principali modalità di attacco, ossia il come, sono indicate nelle "tecniche di attacco" descritte nel prossimo paragrafo §A.1.1.

I due questionari OAD 2021 fanno riferimento agli attacchi digitali intenzionali ad aziende ed enti rilevati nell'intero 2020 e nel primo semestre 2021.
Per ogni tipo di attacco è stata creata, nel questionario completo, 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;
- il principale impatto subito dal SI e dai servizi ICT erogati a seguito dall'attacco più grave nel 2020 e nel 1° semestre 2021, con risposte multiple;
- il principale impatto subito in termini di costi sia per il SI sia per il bilancio dell'intera azienda/ente a seguito dall'attacco più grave nel 2020 e nel 1° semestre 2021, con risposte multiple;
- le possibili motivazioni dell'attacco più grave, nel periodo considerato, 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 nel periodo considerato.

Nel questionario ridotto queste "sotto domande" sono state ridotte alle sole:

- le "macro" tecniche di attacco
- il principale impatto subito dal SI e dai servizi ICT erogati a seguito dall'attacco più grave nel 2020 e nel 1° semestre 2021, con risposte multiple.

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

Facendo riferimento principalmente alle tassonomie sviluppate da CERT[33] e da Sandia[34], si sono categorizzate le tecniche di attacco sotto riportate per poter descrivere e richiedere nei questionari 2021 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 USB, sia per il loro valore sul mercato sia per i dati contenuti.
- tramite chiavette USB, scaricano i file del sistema ICT attaccato connettendole manualmente alle porte USB non disabilitate/protette presenti nel sistema ICT.

[33] Per CERT/CC si veda https://www.sei.cmu.edu/about/divisions/cert/index.cfm
[34] https://www.sandia.gov/

L'attacco fisico è considerato sia come tipologia d'attacco, in quanto vengono attaccati i dispostivi 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 un attacco digitale. Alcune sono "fisiche", come la personale interazione con le persone che usano o gestiscono un dispositivo o le applicazioni del SI, come l'acquisizione di informazioni da carte e stampe nei cestini dei rifiuti, come la richiesta di informazioni in maniera subdola sia de visu sia per telefono (anche questo è social engineering). Altre tecniche per raccogliere informazioni sono informatiche ed includono, ad esempio, 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) e/o malevoli atte a far compiere all'inconsapevole destinatario operazioni di ausilio all'attuazione dell'attacco. I canali principali per la diffusione malevola di informazioni sono prevalentemente i social network, seguite da spamming e spear phishing oltre che 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 di un sistema ICT, per rendere più dinamica una pagina web, per fornire comandi ad un sistema operativo (tipico dei così detti "script shell") e a data base, per personalizzare e rendere "smart" documenti Microsoft Office, Libre Office, o analoghi. 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 rimanda al 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 dei così detti "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. Come caso tipico di esempio, l'attaccante ha attivato una sessione Telnet con il bersaglio o, nel caso di "SQL injection", scritto alcuni 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. Per la loro basilare caratteristica di potersi diffondere sui sistemi in rete in maniera autonoma, vengono considerati una categoria, o sottocategoria, a parte rispetto ai malware.

A.1.1.5 Toolkit

Come dice il nome, sono una "cassetta degli attrezzi" di strumenti informatici che aiutano a compiere l'attacco: trovano le informazioni necessarie e le vulnerabilità presenti nel sistema ICT target, e possono essere usate per 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 carpendo informazioni via 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 bloccano o eludono i meccanismi di controllo delle licenze, di protezione delle copie e più in generale i meccanismi di sicurezza digitale.
Gli exploit sono attacchi ad una risorsa ICT basandosi sulle sue vulnerabilità ed il termine "meta exploit" indica strumenti software che facilitano la loro individuazione, verifica e realizzazione, anche con l'aiuto di 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. Questa categoria include tipicamente gli attacchi APT, Advanced Persistent Threat: sono attacchi persistenti, che possono durare nel tempo, soprattutto nella fase preparatoria e di individuazione delle vulnerabilità da sfruttare (persistent), e che utilizzano innovazioni tecnologiche (advanced).

Attacchi ATP sono realizzati ed usati prevalentemente da organizzazioni con grandi capacità e risorse, in taluni casi anche da stati.

A.2 La macro valutazione qualitativa del livello di sicurezza digitale del sistema informatico oggetto delle risposte al questionario

Con l'obiettivo di meglio e più fortemente motivare un potenziale rispondente a compilare uno dei due questionari online di OAD 2021, è stata fornita, in tempo reale a chi completa la compilazione, una macro valutazione qualitativa del livello di sicurezza digitale del SI oggetto delle sue risposte, rispetto alle esigenze di sicurezza dell'azienda/ente per la quale si risponde.
La macro valutazione è stata realizzata assegnando degli opportuni "pesi" numerici a tutte le opzioni di risposta previste in entrambi i questionari, rispetto alle domande relative:

- alle generali caratteristiche del SI (**A**);
- all'importanza e alla necessità del SI e della sua sicurezza, per le attività ed il business dell'azienda/ente rispondente (**B**);
- alle misure di sicurezza digitale, tecniche ed organizzative, in essere nel SI e selezionate scegliendo le varie opzioni di risposta predefinite presenti per ogni misura (**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:

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

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 a chi completa uno dei due questionari. Per chi ha completato il questionario "completo" vengono anche elencate le risposte che evidenziano la mancanza o l'insufficienza di misure di sicurezza digitale.

Allegato B Glossario

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.
ACN	Agenzia Cibernetica Nazionale
Active Directory	Sistema di directory della Microsoft, integrato nei sistemi operativi Windows dal 2000 in avanti. Utilizza SSO, LDAP, Kerberos, DNS, DHCP, etc.
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.
AIPSI	Associazione Italiana Professionisti Sicurezza Informatica.
AISE	Agenzia Informazioni e Sicurezza Esterna.
AISI	Agenzia Informazioni e Sicurezza Interna.
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	O specifico, 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	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.
Audit	Per la sicurezza digitale, il risultato di un auditing.
Auditing	Per la sicurezza digitale, il processo documentato di revisione (ossia verifica, controllo e valutazione) della efficacia delle misure in essere e della loro gestione, oltre che della conformità di tali misure alle leggi vigenti e alle normative, anche interne, che devono essere seguite.
Backdoor	Interfaccia e/o meccanismo nascosto che permette di accedere ad un programma superando le normali procedure e barriere d’accesso.

BIA	Business Impact Analysis.
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	Programmi, chiamati anche Drones o Zombies, usati originariamente per automatizzare talune funzioni nei programmi ICR, ma che ora sono usati per attacchi distribuiti.
Botnet	Insieme di computer in rete, 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".
CAaaS	Cyber Attack as a Service.
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	Certified Information Systems Auditor di ISACA.
CISO	Chief Information Security Officer: il responsabile della sicurezza digitale dell'intero sistema informatico.
CISR	Comitato interministeriale per la sicurezza della Repubblica
CISSP	Certified Information Systems Security Professional.
Cyber warfare	Guerra cibernetica, chiamata anche guerra informatica o guerra elettronica
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, all'interno della Polizia Postale e delle Telecomunicazioni.
COBIT	Control Objectives for Information and related Technology: consolidata best practice per il governo (governance) di un SI ed il suo audit.
Consumerizzazione	Si veda 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.
COPASIR	Comitato parlamentare per la sicurezza della Repubblica: è l'organo di controllo parlamentare sulle agenzie italiane di intelligence.
COR	Comando Operazioni in Rete (Ministero Difesa).
Cryptojacking	Utilizzo di capacità elaborativa di un inconsapevole sistema ICT target da parte di un cybercriminale per creare criptovaluta.
CSIRT	Computer Security Incident Response Team, italiano, ora sotto ACN
Crowdturfing	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.*
CSaaS	Cyber Security as a Service
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.
CVE	Common Vulnerabilities and Exposures: l'acronimo indica sia il programma di identificazione e classificazione delle vulnerabilità tecniche di ogni sistema e servizio ICT, sia l'elenco di record delle vulnerabilità identificate.
CVSS	Common Vulnerability Scoring System: metrica internazionale di vulnerabilità di un sistema ICT
DAC	Discretionary Access Control.
Darknet	Rete virtuale privata nella quale gli utenti si connettono solamente con persone di cui si fidano.
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 queste ultime correlate.
Data Center	Centro Dati: si veda CED.
DB	Data Base: banca dati.
DBMS	Data Base Management System.
DCS	Distributed Control System.
Deadlock	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.
Defacement o Defacing	In inglese significa deturpare, e nel gergo della sicurezza digitale indica un attacco ad un sito web per modificarlo o distruggerlo; spesso con tale attacco viene modificata solo la home-page a scopo dimostrativo.
DES	Data Encryption Standard

DoS/ DDoS	Denial of Service e Distributed Denial of Service: 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
DNS	Domain Name System.
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.
Download	Azione di scaricare file, tipicamente via Internet
Drive-by Downloads	Attacchi digitali causati dallo scaricare (anche inconsapevolmente) codici maligni o programmi malevoli.
Drones, Droni	Si veda bots.
e-Government	Uso dell'ICT nei processi amministrativi che le PA svolgono per migliorare ed innovare i servizi forniti ai cittadini
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.
EDR	Endpoint Detection and Response.
eIDAS	electronic IDentification Authentication and Signature: regolamento UE n. 910/2014 sull'identità digitale - mira a fornire una normativa di base a livello UE per i servizi fiduciari e l'identificazione elettronica degli Stati membri.
ENISA	European Union Agency for Cybersecurity.
ETACS	Extended TACS.
FTP	File Transfer Protocol: protocollo per il trasferimento di file.
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: 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.

Flooding	Letteralmente significa “allagamento” ed è un termini associato a varie tecniche per attacchi DoS/DDoS
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).
FSD	Fornitori di Servizi Digitali, così come definiti da NIS.
FTPS	File Transfer Protocol Secure: per il trasferimento di file crittati
FW	FireWall generico, normalmente di rete.
FWA	FireWall Applicativo.
GDPR	General Data Protection Regulation: Regolamento 2016/679 UE per la protezione dei dati personali delle persone fisiche (privacy).
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 italiano “bufala” o burla, indica la segnalazione di falsi virus; rientra tra le tecniche di social engineering.
Honeynet	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.
IDS	Intrusion Detection System
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.
IPS	Intrusion Prevention System

ISACA	Information Systems Audit and Control Association.
ISSA	Information Systems Security Association: AIPSI è il suo capitolo italiano
ITIL	Information Technology Infrastructure Library: consolidata best practice per la gestione operativa (management) di un SI
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	Media Access Control: sub strato del livello datalink del modello ISO/OSI.
MAC flooding	Tecnica di attacco tipo DoS/DDoS ad un dispositivo con indirizzo MAC per saturarlo e bloccarne il corretto funzionamento.
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 software di attacco.
MaaS	Malware as a Service: fornitura in cloud di malware (a pagamento).
MFA	Multi-Factor Authentication: autenticazione con più fattore, ad esempio con certificati, token diversi e identificazioni biometriche
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.
MSS	Managed Security Service
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.
NCS	Nucleo per la cybersicurezza ora operante in ambito ACN.

NFT	Non Fungible Token: è un gettone non riproducibile nell'ambito di una blockchain. Gli NFT sono associati a beni virtuali, da un documento a un'opera d'arte, e come tali hanno un mercato mondiale.
NIS	Network and Information Security: direttiva UE 2016/1148, recepita in Italia con il D. Lgs. n. 65 del 18/5/2018, che definisce le misure di sicurezza digitale necessarie a livello di ogni paese membro per le infrastrutture ICT critiche, chiamate anche "servizi essenziali".
NSTPFT	Nucleo Speciale Tutela Privacy e Frodi Tecnologiche della Guardia di Finanza contrastare le frodi telematiche ed informatiche, nonché tutelare la privacy.
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.
OSE	Operatori di Servizi Essenziali, così come definiti da NIS
OT	Operational Technology.
OTP	One Time Password: logica e/o dispositivo che genera password da usarsi una sola volta per sessione/transazione.
Outsourcer	Fornitore di servizi digitali terziarizzati.
PaaS	Platform as a Service.
PAC	Pubblica Amministrazione Centrale.
PAL	Pubblica Amministrazione Locale.
PAM	Privileged Access Management.
Payload	"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 digitale 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 digitale 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.
PNRR	Piano Nazionale di Ripresa e di Resilienza.
Port scanner	Programma software 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.
Provisioning	Attività grazie alle quale vengono fornite le opportune risorse ICT e la loro configurazione, in particolare i diritti d'accesso, ad utenti di un SI
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	Termine che 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	L'attacco digitale 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	L'attacco digitale 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 che a sua volta è 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 significa "raschiando", è il termine usato per indicare 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 motivi 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. Il termine indica quindi l'insieme dei sistemi ICT che lo costituiscono
Sistema Informativo	Indica il Sistema Informatico con tutte le informazioni che vi sono trattate.
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, ecc.
Smart grid	Grid è la rete elettrica di distribuzione di energia, che affiancata da una rete informatica che la gestisce diviene smart
Smishing	Attacco di social engineering per carpire informazioni riservate di un utente, basato sull'invio di SMS. E' l'analogo del phishing con la posta elettronica.
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: sistemi di automazione ed integrazione dei vari strumenti e processi di sicurezza digitale.
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.
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	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 (DoS/DDoS).
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.
UE	Unione Europea.
UEBA	User and Entity Behavioral Analytics.
UOSI	Unità Organizzativa Sistemi Informativi.
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	Utenti con diritti d'accesso privilegiati: includono operatori, manutentori ed amministratori di sistema di un sistema informativo, 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.
Vishing	Attacco di social engineering per carpire informazioni riservate di un utente, basato su chiamate telefoniche. E' l'analogo del phishing con la posta elettronica.
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.
Wiper	Malware distruttivo che manipola e/o cancella il driver di un hard disk, eliminando tutti i dati archiviati e non consentendo più il suo utilizzo.
Worm	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 ancora non note e/o a cui non è ancora stato trovato rimedio.
Zombies, zombi	Si veda bots.

Allegato C Profili Sponsor

C.1 Profili Sponsor Gold

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 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.

C.2 Profili Sponsor Silver

Ireth

Ireth nasce nel 2005 a servizio della Difesa come fornitore di hardware per la sicurezza, e dopo aver ceduto la sua business unit militare, si affaccia con successo al mondo bancario. Grazie alle nostre soluzioni di Strong Customer Autentication (SCA) oggi annoveriamo più di 200 banche tra i nostri clienti.

Grazie al nostro DNA di innovatori, da Luglio 2021 abbiamo intrapreso un percorso condiviso con Omnibek, società che, come IRETH, basa le sue fortune sull' innovazione tecnologica volta alla CyberSecurity con particolare focus ai servizi di Neobanking.
Alla luce di questo investimento siamo diventati proprietari di un'infrastruttura IT che ci permette di salvaguardare il dato dei clienti con un livello di sicurezza garantito da una infrastruttura "Security by design". Altro punto focale è la capacità di effettuare l'On-Boarding dei clienti (KYC) attraverso tecnologie di AI e di Autenticazione biometrica in "Password Less", con un check randomizzato sull' affidabilità rispetto a interrogazioni a base dati per la compliance AML.

Nello specifico, Ireth ha recentemente lanciato SB800, la nuova soluzione di NeoBanking White Label unica nel suo genere perché permette alle Aziende retail o large community, come Enterprise, Telco, Marketplace, Utilities e grandi Società Sportive, di ampliare i servizi rivolti alla propria Clientela "diventando Banca" con il proprio brand, rispettando pienamente le normative di riferimento.
La soluzione inoltre presenta elevate performance di fruizione dei servizi digitali sicuri grazie all'utilizzo delle tecnologie di blockchain privata, Smart Contract, Intelligenza Artificiale e Biometria, che garantiscono grande efficienza e sicurezza nelle interazioni con la clientela.
Questo approccio all'innovazione permette l'archiviazione e la gestione del dato personale con elevati standard qualitativi, e al contempo una elevata User Experience.

Si tratta di un vero processo di democratizzazione dei processi finanziari, perché il mondo finanziario e del business, in questo modo, non sono più divisi da una linea di demarcazione concettuale netta e infrangibile.
Il vantaggio è duplice sia per l'Azienda che per la propria Clientela: l'offerta di un simile servizio di banking consente all'Azienda di ampliare rapidamente la base clienti, oltre a fidelizzarla, e, per la Clientela, di contare su un servizio intuitivo, conveniente e sicuro.

Questi obiettivi si raggiungono attraverso un forte abbattimento dei costi finanziari grazie all'utilizzo dei pagamenti all'interno della stessa community che incide sullo stesso network (Peer to Peer, P2P), azioni che vanno inoltre a rafforzare il senso identitario legato all'immagine dell'Azienda-Banca.

Per maggiori informazioni: www.ireth.net

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

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
ASSOCIAZIONE ITALIANA
AMMINISTRATORI di SISTEMA
e TELEMEDICINA

Associazione ITaliana Amministratori di Sisteme e Telemedicina, associazione scientifica apartitica, apolitica e senza scopi di lucro, riunisce i tecnici sanitari di radiologia medica specialisti nella gestione dei sistemi informativi in diagnostica per immagini.

http://www.aitasit.org/

ANITEC-ASSINFORM

Anitec-Assinform

Associazione Italiana per l'Information and Communication Technology (ICT) - aderente a Confindustria e socio fondatore della Federazione Confindustria Digitale - è l'Associazione di settore oggi di riferimento per le aziende di ogni dimensione e specializzazione: dai produttori di software, sistemi e apparecchiature ai fornitori di soluzioni applicative e di reti, fino ai fornitori di servizi a valore aggiunto e contenuti connessi all'uso dell'ICT ed allo sviluppo dell'innovazione Digitale.
https://www.anitec-assinform.it/

ANORC

ANORC
ASSOCIAZIONE NAZIONALE PER
OPERATORI E RESPONSABILI
DELLA CONSERVAZIONE DIGITALE

Associazione Nazionale Operatori e Responsabili della Custodia di contenuti digitali, si esprime in due associazioni no profit, ANORC Mercato, rappresentativa del mondo aziendale, e ANORC Professioni, punto di riferimento per i professionisti: entrambe sono impegnate nel campo della digitalizzazione e della protezione del patrimonio informativo e documentale in ambito pubblico e privato.

https://anorc.eu/

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/

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

CIOClub Italia

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. Aderisce a FIDAInform
http://www.clubtier.org/

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

CSIG

Il Centro Studi Informatica Giuridica di Ivrea-Torino è un'associazione interdisciplinare indipendente e senza scopo di lucro che si occupa in particolare del diritto applicato alle nuove tecnologie.

http://www.csigivreatorino.it/

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

START 4.0

L'associazione tra imprese pubbliche e private è "Centro di Competenza per la Sicurezza e l'Ottimizzazione delle Infrastrutture Strategiche" per promuovere lo sviluppo tecnologico e digitale e la creazione di competenze specialistiche avanzate nel settore industriale, con particolare riguardo alle PMI.
https://www.start4-0.it/associazione/

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, 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 servizi essenziali e delle infrastrutture critiche dei vari paesi europei; sua adozione in Italia col D.Lgs. 65/2018
- Cyber Security Act, Direttiva EU 2019/881, in vigore dal 27/6/2019
- DPCM n. 181 del 30 luglio 2020, entrato in vigore il 5 novembre 2020, sul "Perimetro di sicurezza nazionale cibernetica"
- PNRR, Piano Nazionale Di Ripresa e Resilienza, in Italia: approvazione europea e stato della sua attuazione in https://temi.camera.it/leg18/pnrr.html
- DECRETO-LEGGE 14 giugno 2021, n. 82: Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale, https://www.gazzettaufficiale.it/eli/id/2021/06/14/21G00098/SG
- ACN, Agenzia Cybersicurezza Nazionale: https://www.acn.gov.it/

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.

- 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[35]: 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: https://www.ic3.gov/
- 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.

[35] 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 a febbraio 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 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. Nel corso della sua carriera Marco ha fondato e ha diretto o è stato partner di alcune aziende dell'offerta ICT, tra le quali CA.SI, Abiemme, Ibimaint System Engineering, ClickICT.
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 il governo e la gestione di un sistema informativo, la sicurezza digitale, l'analisi e gestione dei rischi ICT e dei loro impatti (BIA), il disegno di architetture ICT, la razionalizzazione, 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 secondo il GDPR. Negli anni '90 e fino al 2003 ha ideato e coordinato per SMAU EITO, European Information Technology Observatory, l'indagine annuale europea sul mercato ICT e sui suoi trend. Dal 2009 Marco, in collaborazione con AIPSI, ha ideato e realizza con Malabo 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 rapporto indipendente sugli attacchi digitali intenzionali ad aziende ed enti 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, nel Consiglio Direttivo di FIDAInform, socio e revisore dei conti del ClubTI di Milano, socio AICA
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 numerosi articoli e libri sull'evoluzione tecnologica, la sicurezza digitale, le normative, 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.
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 Amministrazione, 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 migliorare ed accelerare 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, così come percepiti dai suoi Clienti, includono l'effettiva, consolidata esperienza e l'aggiornata competenza dei suoi professionisti, 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, il fornire servizi on line e formazione per gli utenti finali e privilegiati.

Per maggiori informazioni: www.malaboadvisoring.it

Allegato H AIPSI, Capitolo italiano della mondiale ISSA

AIPSI, Associazione Italiana Professionisti Sicurezza Informatica, capitolo italiano di ISSA, è una associazione no-profit solo di persone fisiche che si occupano a qualsiasi livello e in qualsiasi ruolo di sicurezza digitale. Il principale obiettivo di AIPSI è di aiutare i propri soci nella crescita professionale e nel loro aggiornamento continuo sui temi tecnici, organizzativi, normativi e legislativi della sicurezza digitale. L'appartenenza al contesto internazionale ISSA permette ai soci 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, e per tali motivi è anche socio attivo di FidaInform, la Federazione italiana di varie associazioni a livello regionale come i ClubTI (https://fidainform.it/).
AIPSI ha realizzato, e sta realizzando, specifiche iniziative a livello italiano, che si affiancano a quelle erogate a livello internazionale da ISSA, e che includono l'autorevole rivista mensile ISSA Journal, webinar, facilitazioni per corsi e certificazioni, le opportunità di essere in una rete internazionale di professionisti, la possibilità di partecipare agli Special Interest Group, SIG, internazionali, gruppi di lavoro specialistici su temi specifici quali al momento "Women in Security" e "Cyber Resilience".

Le specifiche iniziative AIPSI in Italia si articolano in quelle riservate ai soli Soci e quelle aperte a tutti gli interessati, Soci e non. Le prime includono webinar di approfondimento e discussione, l'iniziativa AIPSI Giovani per coinvolgere i giovani interessati alla cybersecurity (https://www.aipsi.org/aree-tematiche/aipsi-giovani.html), e due indagini:

- OAD, Osservatorio Attacchi Digitali in Italia, per il quale è stato realizzato un sito ad hoc, https://www.oadweb.it/, quale punto di riferimento e repository di tutti i rapporti annualmente pubblicati e di tutta la documentazione, ultimamente anche i videostreaming, degli eventi tenuti per presentare e discutere i dati emersi dalle indagini;
- CSWI, Cyber Security Women's Italy, sul lavoro femminile nella cybersecurity in Italia. Il Rapporto CSWI 2021 è scaricabile da:

Le iniziative AIPSI riservate ai soli Soci includono alla data:

- il supporto, anche con specifiche mentorship tra soci, alla crescita professionale individuale secondo l'impostazione ISSA CSCL, Cyber Security Carrier Lifecycle, contestualizzata alla realtà italiana/europea;
- il supporto ed un significativo sconto per la certificazione eCF (UNI EN 16234-1:2016) per le figure di Security Manager e Security Specialist tramite AICA, accreditata Accredia;
- la possibilità di partecipare, per conto di AIPSI-ISSA, ad eventi e a tavoli istituzionali e pubblicare articoli, anche in collaborazione di altri Soci, su varie riviste, incluso il prestigioso ISSA Journal;
- i Gruppi di Lavoro specialistici (SIG italiani):
    - l'uso dell'Intelligenza Artificiale in ambito sicurezza digitale per strumenti di sicurezza, di gestione, di analisi vulnerabilità e rischi, etc.;
    - nuove logiche ed architetture per la sicurezza digitale, che includono ad esempio Zero Trust, SASE, SOAR, etc.;
    - crescita e percorsi professionali per la sicurezza digitale, con riferimento a CSCL, certificazioni individuali, corsi, mentosrhip tra Soci. In questo ambito iniziano ad essere importanti anche in Italia le onorificenze ISSA per i meriti acquisiti professionalmente e nella

vita dell'associazione, meriti che devono essere tutti documentati e valutati da apposite commissioni AIPSI ed ISSA.

Gli elementi che caratterizzano AIPSI, così come ISSA, includono:

- l'etica professionale dei soci, che devono firmare il codice etico ISSA, ed attenersi ad esso;
- la reale indipendenza ed autonomia di AIPSI da qualsiasi fornitore ed ente, anche in caso di sponsorizzazioni ad iniziative AIPSI;
- la qualità ed il livello professionale dei propri interventi e delle proprie iniziative;
- la focalizzazione sui temi più caldi e di maggior interesse con un continuo e sistematico aggiornamento;
- l' internazionalità che consente di avere contatti e di coinvolgere esperti dei vari Capitoli di ISSA a livello mondiale.

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

I Patrocinatori di OAD 2021