OAD
Osservatorio
Attacchi Digitali
in Italia

Rapporto 2019 OAD

a cura di Marco R. A. Bozzetti

SPONSOR

advansys

par-tec
beyond the IT domain

QINTESI

Technology Estate

in collaborazione con Polizia Postale e delle Comunicazioni

Indagine effettuata da

aipsi

malabo
ICT Advisory

Media partner

Reportec

Ringraziamenti

Si ringraziano tutte le persone che hanno risposto al questionario ed i Patrocinatori che, con le loro idee e suggerimenti, hanno aiutato alla preparazione del Questionario OAD di questa edizione.
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: dott. Luca Bonadimani, Massimo Chirivì
- per Malabo Srl: dott. Andrea Bozzetti, Giuseppe Cesa Bianchi, dott. Francesco Zambon
- per Reportec: dott. Gaetano Di Blasio, dott.ssa Paola Saccardi

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

Dichiarazione di non responsabilità

I grafici ed i testi del presente rapporto sono stati elaborati e redatti con la massima accuratezza e correttezza possibile, partendo dalle risposte al questionario online totalmente anonimo e che pertanto non possono essere verificate. La loro affidabilità, dato il numero delle risposte, è significativa come tendenza, ma non sono in alcun modo di responsabilità da parte dell'autore, Marco R. A. Bozzetti, di Malabo Srl, di Reportec Srl, di AIPSI, né di alcun altro Sponsor e Patrocinatore. Tutte le informazioni pubblicate NON costituiscono in alcun modo un servizio di consulenza, né di offerta ai lettori. Marco R. A. Bozzetti, Malabo Srl, Reportec Srl, AIPSI, gli Sponsor ed i Patrocinatori di OAD 2019 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 2019 OAD.

Pubblicato a fine dicembre 2019.
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 aipsi@aipsi.org

Malabo Srl Sede operativa Via Savona 26 20144 Milano info@malaboadvisoring.it tel. 02 39443632

Reportec srl Via Marco Aurelio, 8 20127 Milano info@reportec.it tel.02.36580441

1 Sommario

2 Sintesi direzionale

L'Osservatorio Attacchi Digitali in Italia, OAD, con la presente edizione 2019 arriva all'undicesimo anno di indagini consecutive sugli attacchi digitali in Italia e si avvale, come negli anni precedenti, della preziosa collaborazione con la Polizia Postale e delle Telecomunicazioni. OAD costituisce l'unica indagine indipendente on line via web in Italia sugli attacchi digitali intenzionali ai sistemi informatici delle aziende e degli enti pubblici operanti in Italia.
L'indagine OAD non prevede un predefinito insieme di rispondenti, ma consente ai potenziali interessati un pieno e libero accesso al questionario in Internet via web, in maniera totalmente anonima; grazie al numero di risposte raccolte e alla loro bilanciata distribuzione tra aziende ed enti pubblici di varie dimensioni e appartenenti a vari settori merceologici, esso fornisce precise e contestuali indicazioni sul fenomeno degli attacchi digitali in Italia.
Secondo gli ultimi dati ISTAT[1], il numero di aziende in Italia è di 4.397.623: il 99,91% sono PMI, Piccole Medie Imprese, sotto i 250 dipendenti, e di queste il 95% sono sotto i dieci dipendenti. Per le pubbliche amministrazioni, poche sono le grandi strutture, la stragrande maggioranza sono sotto i 250 dipendenti. A fronte di questo contesto italiano, di fatto basato su piccole e piccolissime organizzazioni, il bacino di rispondenti emerso nel 2019 risulta costituito, in termini di numero di dipendenti, per il 62,6% da strutture sotto i 250, e di queste il 37,4% sotto i 50. Per le grandi organizzazioni, il 9% dei rispondenti ha più di 5000 dipendenti. Rispetto ai settori merceologici, i rispondenti al 18% appartengono a pubbliche amministrazioni, istruzione statale inclusa, il resto al settore privato: di questo, la maggior parte di aziende appartiene al settore ICT (25,7%) e a quello manifatturiero e delle costruzioni (16,4%), cui seguono con percentuali inferiori organizzazioni appartenenti a tutti gli altri settori merceologici, classificati secondo il codice ATECO[2]. Il campione emerso risulta quindi abbastanza ben bilanciato tra piccole strutture e quelle medio grandi; per i vari settori merceologici il campione è invece prevalente formato da aziende di servizi ICT e del manifatturiero.
I compilatori del questionario 2019 sono per il 18,3% i responsabili dei sistemi informatici (CIO), per il 17% il personale di terze parti cui è terziarizzata, in tutto o in parte, la gestione del sistema informatico e della sua sicurezza, e con una identica percentuale il personale di vertice dell'azienda/ente. Seguono con percentuali a scalare altri ruoli, incluso con il 7,2% quello di responsabile della sicurezza digitale (CISO).
In termini di attacchi digitali, per la prima volta negli undici anni di indagini dell'Osservatorio, la percentuale di rispondenti che ha subito-rilevato attacchi, il 55,7%, è superiore a chi non li ha subiti: importante indicatore della crescente diffusione degli attacchi digitali.
Le cinque tipologie di attacco più diffuse tra i sistemi informatici dei rispondenti sono state, in ordine di diffusione tra i rispondenti:

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

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

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

le possibili motivazioni degli attaccanti ed i tempi di ripristino a seguito degli attacchi più gravi. Tutti questi approfondimenti cambiano per ogni tipologia di attacco, cui si rimanda ai vari paragrafi del rapporto, ma in linea generale emergono i seguenti punti:

- la stragrande maggioranza di chi ha subito attacchi dichiara che gli impatti conseguenti sono stati nulli, o irrisori, o comunque ripristinabili in tempi brevi e a bassi costi; alcuni hanno invece subito impatti gravi, che hanno comportato disservizi, danni ai clienti con rimborsi, perdita di immagine e addirittura di business;
- le probabili motivazioni per gli attacchi subiti riguardano in primis la frode, cui segue ricatto/ritorsione, utilizzo dell'attacco per compierne ulteriori e più gravi;
- i tempi richiesti di ripristino dopo il più grave attacco confermano, per ogni tipologia, che la maggior parte degli attacchi non sono stati gravi e con forti impatti: infatti la maggior parte ripristina entro tre giorni, ma tra questi, in molti casi, il ripristino avviene in giornata. Nei casi più gravi e complessi, il ripristino può richiedere anche più di un mese.

Gli attacchi più temuti nel prossimo futuro sono correlati, almeno in parte, agli ultimi più gravi attacchi subiti: al primo posto si posizione pertanto l'attacco al controllo degli accessi, temuto dal 39,4% dei rispondenti, cui seguono il furto di informazioni da sistemi mobili con un 38%, l'attacco o uso non autorizzato di un completo sistema ICT con il 35,7%, il furto di informazioni da sistemi fissi con il 34,4%. Tutte le altre tipologie di attacco sono a decrescere sotto il 30%.
Le tecniche di attacco più temute nel prossimo futuro vedono al primo posto, con il 54,3%, la raccolta malevola di informazioni, e al secondo posto tra i rispondenti il malware e gli con il 53,8%.
L'indagine OAD cerca di fotografare, oltre agli attacchi digitali subiti, le misure di sicurezza che i sistemi informatici dei rispondenti hanno in atto, anche per meglio comprendere, pur in linea generale, quanto queste contromisure sono riuscite a prevenire e contrastare gli attacchi.
I sistemi informatici dei rispondenti e le misure di sicurezza che li proteggono, risultano essere, come percentuale di diffusione, nella fascia medio-alta per il livello di sicurezza digitale attuato, pur con qualche elemento di eccellenza e più numerosi elementi di debolezza. In non pochi casi mancano le più elementari e basilari misure sia tecniche sia, soprattutto, organizzative, e questo non solo nelle piccole e piccolissime strutture (anche se la loro prevalenza incide sulle percentuali complessive), ma anche in quelli medio grandi.
Per le misure tecniche della sicurezza digitale emerge che:

- relativamente poche le aziende/enti dei rispondenti che seguono un approccio architetturale basato su standard e best practice per la sicurezza digitale, il 13%, ed il 29,59% dichiara di disporre almeno delle risorse ICT più critiche in alta affidabilità (99,9%); la mancanza di una architettura per la sicurezza digitale porta alla non interazione e coordinamento tra i diversi strumenti;
- quasi il 14% ha un Piano di Business Continuity (continuità operativa) ed il 29,9% un piano di Disaster Recovery, ma solo il 15,4% di questi ultimi ha predisposto le risorse ICT alternative per attuarlo quando necessario;
- assai limitate le misure di sicurezza fisica;
- per la protezione delle reti, il 54,3 usa firewall di rete e DMZ, il 49,8% usa VPN, il 27,6% utilizza sistemi IPS/IDS e di analisi di traffico;
- per il controllo degli accessi, misure per lo più basate sul solo uso di identificatore d'utente e password, per il 60,2% dei rispondenti; il 50% circa usa Active Directory o LDAP; il 13,6% usa certificati e PKI; per il controllo delle autorizzazioni, il 26% usa tecniche di ACL, Access Control List, altre tecniche più sofisticate hanno percentuali molto basse;
- per la sicurezza logica dei singoli sistemi ICT, inaspettata bassa percentuale nell'uso di software anti-codici maligni ed antivirus, con solo un 55,7% dei rispondenti; il 36,2% effettua la sistematica gestione delle patch e delle versioni del software, solo il 42,5% archivia e gestisce i log degli amministratori di sistema, pur essendo obbligatoria dal 2008 per disposizione del Garante della Privacy;
- per la protezione delle applicazioni e dei dati trattati, ancora limitato utilizzo della crittografia sia nella trasmissione dati, 38,9%, sia nella archiviazione di quelli più critici, dati sensibili inclusi, 27,6%; abbastanza ampio uso di firewall e reverse proxy a livello applicativo con il 39,8%; solo

il 16,67% effettua il controllo della sicurezza del software prima della sua messa in produzione.
Le misure e gli strumenti di gestione della sicurezza digitale in uso nei sistemi informatici dei rispondenti sono percentualmente basse, anche per la forte incidenza delle piccole e medie organizzazioni:

- gli strumenti più diffusi sono il monitoraggio ed il controllo centralizzato delle funzionalità e delle prestazioni dei sistemi ICT con un 37,1% dei rispondenti;
- il 27,6% effettua l'analisi delle vulnerabilità, ed il 14% i test di penetrazione;
- il 42% dei rispondenti terziarizzano in parte o completamente il loro sistema informatico e la gestione della sua sicurezza, ed l'11,8% utilizza SOC e/o SCC. Relativamente pochi usano servizi in cloud: il 26,2% SaaS, il 19,9% IaaS, il 9,5% PaaS;
- molto basse le percentuali sull'utilizzo di sistemi di intelligenza artificiale, l'analisi comportamentale dei sistemi ICT e/o dei loro utenti.

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

- circa i ¾ dei rispondenti hanno nella propria organizzazione chi espleta de facto il ruolo di responsabile della sicurezza digitale (CISO), ma solo 1/3 lo ha ufficializzato;
- per il 40% circa sono definite e in uso policy per la sicurezza digitale, percentuali inferiori, a partire da 37,1%, per le relative procedure organizzative;
- scarse attività di sensibilizzazione e formazione sulla sicurezza digitale;
- scarso interesse sulle certificazioni professionali per la sicurezza digitale a livello aziendale e personale, sia all'interno della propria organizzazione sia verso i fornitori;
- l'analisi dei rischi è effettuata dal 54,5% dei rispondenti, una percentuale più alta rispetto a quelle rilevate nelle precedenti indagini OAD, dovuta sicuramente agli obblighi GDPR per la privacy. Il 18,9% ha già in essere una assicurazione per i rischi ICT, ed il 15,9% ha a piano di sottoscriverne una;
- il 43,4% dei rispondenti effettua auditing per il proprio sistema informatico e la sua sicurezza.

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

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

Per concludere, l'indagine OAD 2019 evidenzia l'incremento di attacchi digitali, talvolta con impatti e conseguenza serie, ma nella maggior parte dei casi le misure di contrasto in essere, pur avendo lacune, riescono a tamponarli. La realtà italiana, costituita da un grandissimo numero di piccole e piccolissime imprese, non fa rientrare il nostro paese tra quelli più appetibili per i criminali digitali, ma cyber warfare e gli attacchi massivi costituiscono un rischio crescente e grave, come in parte è già successo con la larga diffusione di ransomware su sistemi informatici cui mancano, o sono mal gestite, le misure di base. Ancora forte la sottovalutazione della sicurezza digitale, con la conseguente non implementazione delle idonee misure di difesa, soprattutto nelle pubbliche amministrazioni. Misure di difesa che rincorrono l'evoluzione, sempre più sofisticata e smart, degli attacchi, ma quasi sempre in ritardo. L'attuale alta densità di vulnerabilità richiede nuovi approcci e nuove logiche, con l'obiettivo di rendere intrinsecamente sicuri, by default e by design, tutti i sistemi ICT interconnettibili ad Internet. Ma alla data siamo ancora lontani da tale obiettivo, e per migliorare decisamente il concreto contrasto al cybercrime occorre ora accrescere la consapevolezza e le competenze sulla sicurezza digitale a tutti i livelli, la fattiva collaborazione tra le polizie a livello mondiale, l'etica professionale di chi si occupa (lato offerta) e di chi decide (lato domanda) sulla sicurezza digitale.

2b. Executive Summary

The Observatory on Digital Attacks in Italy, named in the following with the Italian acronym **OAD**, with this 2019 edition reaches the eleventh year of consecutive investigations on digital attacks in Italy and makes use, as in previous years, of the precious collaboration with the Italian Postal and Telecommunications Police. OAD is the only independent survey via web in Italy on intentional digital attacks on the IT systems of companies and public bodies operating in Italy.
According to the latest ISTAT[3] data, the number of companies in Italy is 4,397,623: 99.91% are SMEs, Small Medium Enterprises, under 250 employees, and of these 95% are under ten employees. For public administrations, there are few large structures, the vast majority are under 250 employees. In the face of this Italian context, the pool of respondents that emerged in 2019 is constituted, in terms of number of employees, for 62.6% of structures under 250, and of these 37, 4% under 50. For large organizations, 9% of respondents have more than 5000 employees. Compared to the product sectors, 18% of respondents belong to public administrations, including state education, the rest to the private sector: of this, most companies belong to the ICT sector (25.7%) and to the manufacturing and construction sector (16.4%), followed by organizations belonging to all other product sectors, classified according to the ATECO code[4], with lower percentages. The emerged sample is therefore quite well balanced between small and medium-large structures; for the various product sectors, on the other hand, it is mainly focused on ICT services and on the manufacturing sector.
18.3% of the compilers are CIO, 17% are the staff of third parties in charge of the management of the IT system and its security; with an identical percentage the top staff of the company / institution, such as owners, Presidents, CEOs. Other roles follow with percentages, including 7.2% of CISO.
In terms of digital attacks, for the first time in the Observatory's eleven years of investigation, the percentage of respondents who underwent and detected digital attacks, 55.7%, is higher than those who have not suffered them: an important indicator of the growing spread of digital attacks.
The five most common types of attack among respondents' IT systems were, in order of diffusion among respondents:

- attacks on IAA systems for access control, with a 54.21%
- attacks on the entire target ICT system, with 41%
- attacks on communication networks, with 34.65%
- theft of user mobile devices, with a 33.62
- saturation of ICT systems and resources (DoS, DDoS), with a 30.93%.

All the other types of attack are decreasing below 30%, as diffusion.
Considering all the types of attack in 2018, the most common and used attack technique was the unauthorized collection of information, typically through social engineering, followed by the malicious codes and by the toolkits. All the other techniques decrease with a much greater percentage distance.
The impacts following the most serious attacks are analyzed, 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 details change for each type of attack, see §6.1-§6.15, and globally the following points emerge:

- the overwhelming majority of those who have suffered attacks declare that the consequent impacts have been zero, or negligible, or in any case can be restored quickly and at low costs; some, on the other hand, suffered serious impacts, which led to disservices, damage to customers with reimbursements, loss of image and even of business
- the probable reasons for the attacks suffered primarily concern fraud, followed by blackmail / retaliation, use of the attack to perform further and more serious ones
- the recovery times required after the most serious attack confirm, for each type, that most of the attacks were not very critical and with strong impacts: in fact most recover within three

[3] ISTAT, Italian National Institute of Statistics.
[4] ATECO Code: alphanumeric combination that identifies an economic activity.

days, but among these, in many cases, the recovery takes place in only one day. In severe and complex cases, recovery can take up to a month.

The most feared attacks in the near future are related, at least in part, to the most serious attacks suffered: therefore, the attack on access control, feared by 39.4% of respondents, ranks first, followed by the theft of information from mobile systems with 38%, the attack or unauthorized use of a complete ICT system with 35.7%, the theft of information from fixed systems with 34.4%. All other types of attack are decreasing below 30%.

The OAD survey seeks to photograph, in addition to the digital attacks suffered, the security measures that the respondents' computer systems have in place. The IT systems of the respondents and the security measures that protect them are, as a percentage of diffusion, in the medium-high range for the digital security level implemented, albeit with some elements of excellence and more numerous elements of weakness. In many cases, the most basic measures are lacking both technical and, above all, organizational, and this not only in small and very small structures, but also in medium-large ones.

For the technical measures, it emerges that:

- relatively few the organizations which follow an architectural approach based on standards and best practices for digital security (13%), and 29.59% respondents claim to have at least the most critical ICT resources in high reliability; the lack of an architecture for digital security leads to non-interaction and coordination between the different security tools
- almost 14% have a Business Continuity Plan and 29.9% have a Disaster Recovery plan, but only 15.4% of these have prepared alternative ICT resources to implement it
- very limited physical security measures
- for network protection, 54.3% use network firewalls and DMZ, 49.8% use VPN, 27.6% use IPS / IDS and traffic analysis systems
- for access control, measures mostly based on user ID and password only, for the 60.2% of respondents; about 50% use Active Directory or LDAP; 13.6% use certificates and PKI; for authorization control, 26% use ACL techniques, Access Control List, other more sophisticated techniques have very low percentages
- for the logical security of each ICT system, unexpected low percentage in the use of anti-malicious code and antivirus software, with only 55.7% of respondents; 36.2% carry out the systematic management of patches and versions of the software, only 42.5% store and manage the logs of the system administrators
- for the protection of the applications and data processed, still limited respondents use encryption techniques both in data transmission, 38.9%, and in the storage of the most critical ones, including sensitive data, 27.6%; fairly extensive use of firewalls and reverse proxies at the application level with 39.8%; only 16.67% check the security of the software before it is put into production.

The digital security management is low in percentage terms, also due to the high incidence of small and medium-sized organizations of the respondents:

- the most popular tools are centralized monitoring and control of the functionality and performance of ICT systems with 37.1% of respondents
- 27.6% perform vulnerability analysis, and 14% penetration tests
- 42% of respondents partially or completely outsource their IT system and its security management, and 11.8% use SOC and / or SCC. Relatively few use clouds services: 26.2% SaaS, 19.9% IaaS, 9.5% PaaS
- very low percentages on the use of artificial intelligence systems, the behavioral analysis of ICT systems and of the users.

The organizational measures for the digital security are more deficient and less advanced than the technical ones:

- about ¾ of the respondents have in their organization a CISO role, but only 1/3 has made it formally defined
- approximately 40% of the digital security policies are defined and in use, lower percentages, starting from 37.1%, for the related organizational procedures
- very critical the poor awareness and training activities on digital security

- little interest and few requirements for the professional certifications in digital security at company and personal level, both within the organization and towards its suppliers
- the risk analysis is performed by 54.5% of respondents, a higher percentage than those found in previous OAD surveys, certainly due to the GDPR privacy obligations. 18.9% already have ICT risk insurance in place, and 15.9% have plans to take out one
- 43.4% of respondents perform audits for their IT system and its security.

The data provided by the Italian Postal and Communications Police confirm the growing criticality of digital attacks and above all the difficulties in fighting and repressing cybercrime:

- in the context of Critical Infrastructures, the alarms issued in 2018 were 80,777, more than double compared to 2017; 459 attacks were detected, just under half of 2017, 74 investigations, 14 people reported and of those only one arrested
- in contrast to the "financial cybercrime", fraudulent transactions in 2018 were blocked for a total value of € 38.4 million and € 9 million was recovered
- in the fight against cyber terrorism, 36,000 websites were checked, and 250 contents were deleted.

To conclude, the OAD 2019 survey highlights the increase in digital attacks, sometimes with serious impacts and consequences, but in most cases the existing contrast measures, despite having gaps, manage to buffer them. The Italian reality, made up of many small and very small enterprises, does not make our country one of the most attractive for cyber criminals, but cyber warfare and massive attacks pose a serious risk to the entire nation. The underestimation of digital security is still strong, with the consequent non-implementation of suitable defense measures, especially in public administrations. The security measures chase the evolution of attacks, increasingly sophisticated and smart, but almost always late. The current high density of vulnerabilities requires new approaches and new logics, with the aim of making all ICT systems intrinsically safe, by default and by design. But at the moment we are still far from this objective, and to definitely contrast the cybercrime it is now necessary to increase awareness and skills on digital security at all levels, to strengthen the effective collaboration among the cyber police and institutions worldwide, to request and seriously consider ethical behavior of who deals (offer side) and who decides (demand side) on digital security.

3. Introduzione al Rapporto 2019 OAD

OAD, Osservatorio Attacchi Digitali in Italia, costituisce l'unica indagine indipendente on line via web in Italia sugli **attacchi digitali intenzionali** ai sistemi informatici delle aziende e degli enti italiani, incluse le Pubbliche Amministrazioni Centrali e Locali.
Obiettivo primario di OAD è analizzare il fenomeno degli attacchi digitali specificatamente 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 2019 fa riferimento agli attacchi digitali intenzionali rilevati nel corso dell'intero 2018**,** e si congiunge ai precedenti Rapporti che coprono un arco temporale di undici anni consecutivi, dal 2007 al 2018. Fino al 2015 l'indagine era chiamata OAI, Osservatorio Attacchi Informatici in Italia, dal 2016 è stata chiamata OAD.
Tutti rapporti annuali pubblicati sono scaricabili gratuitamente, insieme alla documentazione prodotta e/o raccolta di articoli e presentazioni ad essi correlati, dallo specifico sito web www.oadweb.it, che costituisce l'archivio documentale completo di tutte le iniziative negli anni sull'Osservatorio.
Il Rapporto 2019 OAD è realizzato dall'autore Marco R. A. Bozzetti con la sua società Malabo Srl, sotto l'egida di e in collaborazione con l'associazione AIPSI, Capitolo italiano di ISSA, con l'editore Reportec Srl e con la Polizia Postale e delle Telecomunicazioni, che ha fornito i dati trattati nel Capitolo 11.
Per coprire almeno una parte dei costi, OAD 2019 è stata sponsorizzata dalle aziende dell'offerta ICT[5] Advansys, Par-Tec, 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 2019 annovera il patrocinio di numerose associazioni, il cui elenco, con una breve descrizione delle loro attività, è nell'Allegato D. Per OAD il ruolo attivo dei Patrocinatori è significativo per poter allargare e stimolare il bacino dei compilatori del questionario via web, tipicamente tramite i loro soci e simpatizzanti, oltre che per far conoscere e divulgare il rapporto annuale, contribuendo in tal modo anche alla diffusione della cultura sulla sicurezza ICT.

Il Rapporto OAD 2019 si basa sull'elaborazione e l'analisi delle risposte avute dal questionario on line via web reso liberamente disponibile su Internet da giugno a novembre 2019. Essendo libero l'accesso al questionario in Internet, il campione emerso non ha stretta valenza statistica, ma, dato il numero di risposte e la buona distribuzione per dimensioni e per settore merceologico delle aziende/enti dei rispondenti, esso fornisce precise e contestuali indicazioni sul fenomeno degli attacchi digitali in Italia. L'indagine rileva anche quali sono gli strumenti di prevenzione, protezione e ripristino in uso nei sistemi informatici dei rispondenti per contrastare e limitare tali attacchi, e come le aziende/enti reagiscono in caso di attacco.
Dalle elaborazioni ed analisi delle circa 300 risposte al questionario OAD 2019, costituito da 117 domande con risposte predefinite tra le quali scegliere, è stato prodotto il presente rapporto finale, costituito da 165 pagine A4 e da 135 figure tra grafici e tabelle.

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

5 ICT, Information and Communication Technology.

3.1 Le motivazioni dell'Osservatorio sugli Attacchi Digitali in Italia

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

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

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

Di qui la decisione di realizzare sotto l'egida e in collaborazione con AIPSI un Osservatorio Nazionale annuale, le cui caratteristiche metodologiche sono riportate nell'Allegato A, riprendendo anche l'esperienza passata avuta con OCI, Osservatorio Criminalità Informatica, in ambito FTI-Sicurforum[6]. L'approccio è simile: la raccolta dei dati avviene elaborando le risposte via web dei vari rispondenti, il rapporto è elaborato in maniera omogenea dall'autore, in collaborazione con alcune persone di AIPSI, Malabo, Reportec ed utilizzando anche i dati forniti dalla Polizia Postale e delle Telecomunicazioni, si veda Cap. 11.

[6] Per i Rapporti OCI del 1997, 2000 e 2004, pubblicati da Franco Angeli, si veda http://www.forumti.it/

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

Gli attacchi digitali sono un fenomeno, a livello mondiale, di portata crescente e in grado di portare incredibili guadagni illeciti ai cyber criminali: il progetto europeo di ricerca Hermeneut [7] sulla cybersecurity stima per il 2021 danni a livello mondiale per attacchi digitali pari a 6 trilioni di dollari, una cifra ben superiore ai danni per droga: danni che in gran parte costituiscono il guadagno per i criminali digitali e che si basano prevalentemente sulle vulnerabilità "umane" dell'utente informatico, con attacchi di social engineering quali spear phishing.
Il Global Risk Report[8] del World Economic Forum, WEF, pubblicato a gennaio 2019, evidenzia come i rischi digitali siano ai primi posti tra i rischi "globali" a livello mondiale, dopo le tensioni geo politiche ed economiche e gli eventi climatici estremi.
La fig. 4-1 dal rapporto WEF mostra il posizionamento assai critico del cyber rischio tra tutti gli altri, e lo mette in diretta correlazione con la caduta delle infrastrutture critiche, con il furto di dati e relative frodi, con le avverse conseguenze dell'innovazione tecnologica.

[7] https://www.hermeneut.eu/
[8] https://www.weforum.org/reports/the-global-risks-report-2019

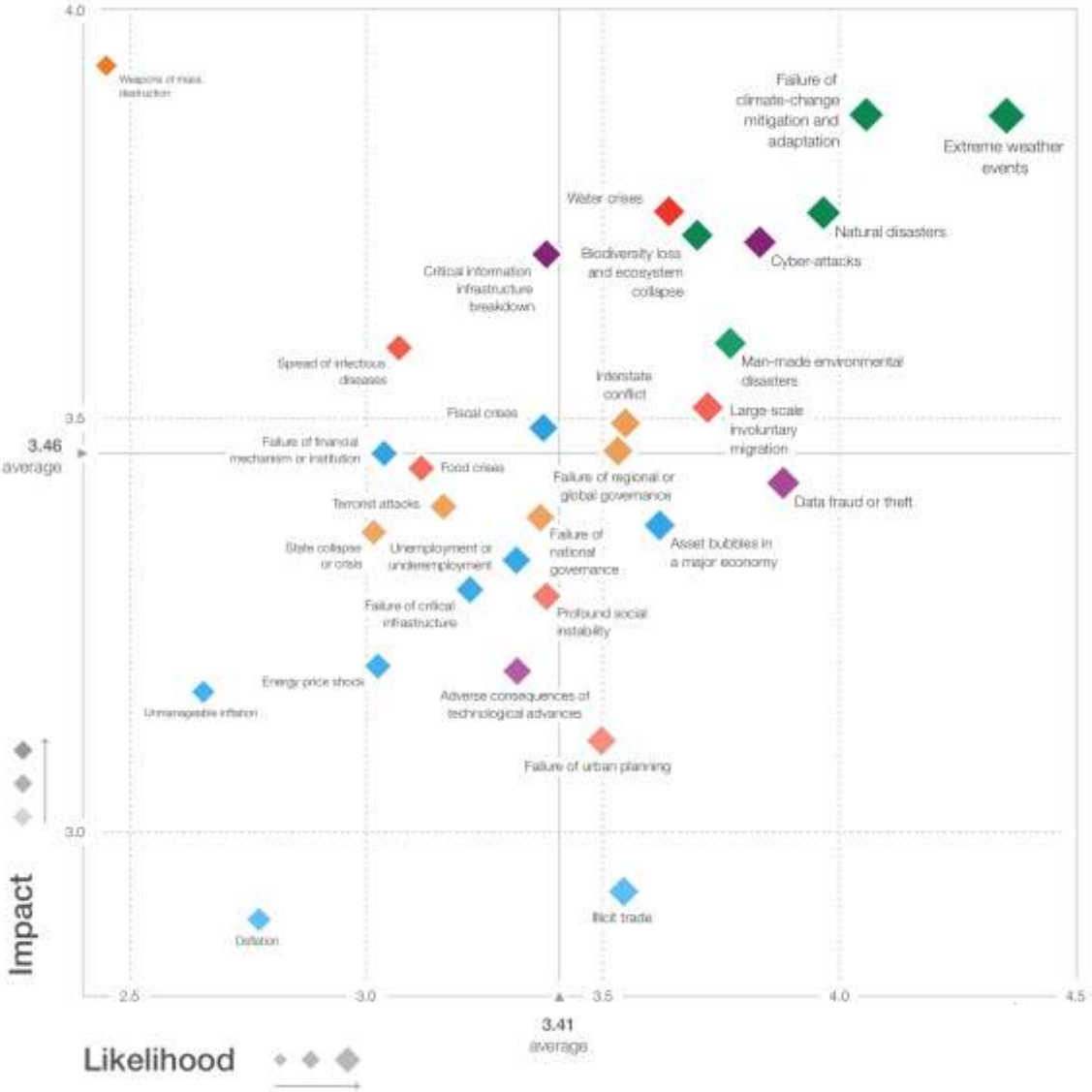

Fig. 4-1

Tale criticità è dovuta a molteplici fattori, di cui i principali sono le vulnerabilità tecniche e quelle organizzative, considerate nei paragrafi.
Le vulnerabilità tecniche crescono anche alla crescita della complessità dei moderni sistemi informatici, sempre più difficili da gestire anche se di piccole dimensioni e con limitate funzionalità, come sono normalmente quelli usati da piccole e piccolissime organizzazioni, che in Italia sono la stragrande maggioranza. Le vulnerabilità delle persone rappresentano il più delle volte rischi ancora più diffusi e gravi: e sono amplificate dalle vulnerabilità organizzative (si veda §5).

In questo contesto, l'Italia ha un forte ritardo nella trasformazione digitale, come evidenziato dall' indice DESI[9] della Comunità Europea. Dei 5 parametri principali considerati dall'indice, l'Italia ha valori bassi in tutti, ma particolarmente bassi nell'uso di Internet e sul capitale umano, che include le competenze ICT e l'inclusione digitale. E a livello business, considerando l'enorme numero di piccole e piccolissime aziende e amministrazioni pubbliche locali, il problema delle competenze

[9] DESI, Digital Economy and Society Index è un indice composito che sintetizza vari rilevanti indicatori sulle prestazioni digitali in Europa e traccia l'evoluzione dei vari membri EU nella competitività digitale. Si veda https://ec.europa.eu/digital-single-market/en/desi

ICT è più grave che in altri paesi dell'EU: le specifiche competenze per la sicurezza digitale sono ancor meno, lasciando ampio spazio all'incompetenza e al millantato credito di numerosi attori ed interlocutori, che rasenta sovente la truffa.

Il ritardo italiano nella trasformazione digitale

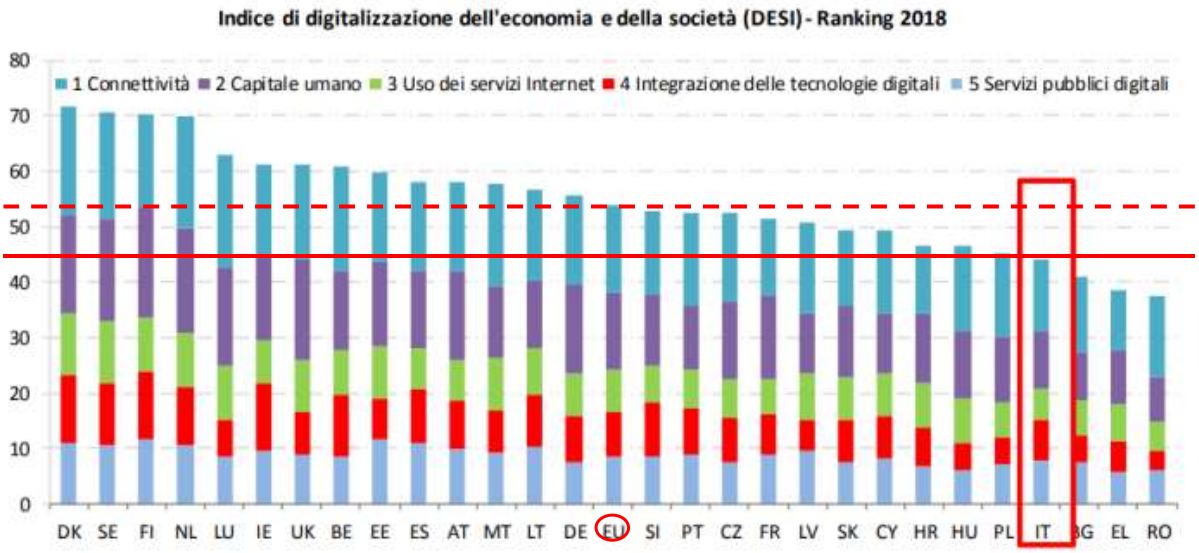

Fig. 4-2

Piccole e medie organizzazioni, ma soventi anche quelle grandi, difficilmente possono disporre al loro interno le aggiornate competenze tecniche ed organizzative per la gestione della sicurezza digitale: devono terziarizzarle, ma devono saperle controllare ed indirizzarle rispetto al loro specifico contesto. In caso contrario dipendono e dipenderanno sempre più dagli outsourcer, che a loro volta talvolta hanno scarse competenze nella cybersecurity: ed il ciclo di incompetenze così si chiude con possibili conseguenze molto negative per l'azienda/ente, anche al di fuori delle eventuali truffe.
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 è solo un problema tecnico, ma anche di business, dato che deve garantire la continuità operativa dell'azienda/ente.

Fino ad oggi le misure di sicurezza hanno rincorso i sempre nuovi e più sofisticati attacchi, facendo ricadere la responsabilità della loro occorrenza sull'incapacità e sugli errori degli utenti. Ma con vulnerabilità ad alta densità, molti esperti, a livello mondiale, quali ad esempio Dan Geer[10] e Bas Alberts[11], ritengono che non si debba più spendere prevalentemente per tali misure, ad oggi comunque ancora necessarie, ma decisamente orientarsi e richiedere al mercato sistemi ICT intrinsecamente sicuri, indipendentemente dal buono o cattivo uso da parte dell'utente. Sistemi ICT veramente sicuri by design e by default. Alcuni passi in questa direzione sono già stati compiuti, si pensi ai sistemi di autenticazione senza password, o si stanno compiendo, ma lo stato attuale dell'arte è ancora lontano da questi obiettivi.

[10] "*… If they [vulnerabilities] are dense, then finding and fixing one more is essentially irrelevant to security and a waste of the resources spent finding it.*"
[11] "**…** *But if you care about systemic security […] don't chase and fix vulnerabilities, […] design a system around fundamentally stopping routes of impact …*"

La sicurezza digitale assoluta non esiste, ma nel mondo ormai dominato dall'ICT in Internet, la sicurezza digitale è e deve essere un obbligo a livello nazionale, delle aziende/enti, dei singoli. In attesa dei sistemi intrinsecamente sicuri, 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;
- bloccare e reprimere l'hackeraggio/cyber crime, riducendo gli alti guadagni illegali con pochissimi rischi (si veda §11);
- una maggiore collaborazione internazionale per la repressione del crimine informatico, sia a livello legislativo sia a livello forze di Polizia;
- far crescere l'etica professionale di chi si occupa di sicurezza digitale sia lato offerta sia lato domanda.

5. Le vulnerabilità

Tutte le minacce ICT, intenzionali o non, si basano su vulnerabilità che possono essere categorizzate in tecniche, delle persone, dell'organizzazione.
Le vulnerabilità delle persone sono le più critiche, dato che riguardano il comportamento umano non sempre prevedibile e difficilmente limitabile/controllabile, in ambito digitale sia per gli utenti finali sia, soprattutto, per gli utenti privilegiati. 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.
A livello tecnico esistono qualificati ed aggiornati siti che elencano, classificandole, le vulnerabilità riscontrate, quali ad esempio CVE/MITRE e la statunitense NVD, National Vulnerability Database.
Per ogni vulnerabilità questi siti riportano, se esistono, le modalità per eliminarle.
L'Allegato E.2 fornisce un elenco, non esaustivo, delle principali fonti internazionali con aggiornati elenchi delle vulnerabilità tecniche ICT.

L'argomento delle vulnerabilità è molto ampio, a livello tecnico estremamente dettagliato, e si rimanda per approfondimenti alle citate fonti.
In termine generali, per le vulnerabilità tecniche:

- non tutte le vulnerabilità esistenti sono state individuate e classificate negli elenchi CVE e NVD: quelle non ancora individuate, ed indicate con il termine "zero-day", sono le più critiche, perché non hanno 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; esistono quindi vulnerabilità note ma senza una correzione disponibile;
- la tendenza negli anni è una leggera crescita delle vulnerabilità tecniche;
- non esiste prodotto ICT, di alcun fornitore, che non abbia delle vulnerabilità note.

Per le vulnerabilità personali l'unico strumento di contrasto 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.

Le vulnerabilità organizzative possono essere numerose, ed esercitare un fattore di leva sulle vulnerabilità personali. Le vulnerabilità organizzative sono causate da poca o nulla attenzione e considerazione da parte del vertice dell'azienda/ente sulla sicurezza digitale: e riguardano non solo le piccole-medie organizzazioni, ma anche le grandi.
I problemi tipici, e quindi le vulnerabilità, lato organizzazione partano dalla non chiara assegnazione dei compiti, con una altrettanto chiara separazione dei ruoli. Una seconda criticità è dovuta agli effettivi controlli di auditing sulla sicurezza digitale, sia all'interno dell'organizzazione, sia, soprattutto, per i fornitori. Una terza criticità è la pubblicazione di idonee policy e procedure organizzative, che devono essere non formali, ma non ambigue, sostanziali ed efficaci, e che devono essere seguite dal personale coinvolto.

Il problema di fondo è che una adeguata sicurezza digitale costa, e non poco: ma quanto costa la non sicurezza?

6. Gli attacchi digitali rilevati nell'indagine OAD 2019

Nel presente capitolo, ogni tipologia di attacco viene esaminata sulla base delle risposte ricevute da chi ha rilevato nell'intero arco del 2018, la specifica tipologia d'attacco, e che riguardano:

- il numero di attacchi di quel tipo nel 2018, se sopra o sotto la soglia di 10 attacchi rilevati nell'anno; la soglia di 10 per anno è un numero derivato dall'esperienza pluriennale dell'autore;
- le tecniche di attacco (come) che si ritiene siano state usate per portare quel tipo di attacchi, considerando in particolare gli attacchi più gravi per l'azienda/ente del rispondente;
- i principali impatti subiti dall'attacco più grave rilevato;
- le possibili motivazioni dell'attacco più grave rilevato;
- il tempo massimo richiesto per il ripristino ex ante nel caso del più grave attacco di quel tipo subito nell'anno 2018.

La fig. 6-1 mostra, percentualmente, il numero di attacchi rilevati dai rispondenti nel 2018: essa evidenzia come complessivamente gli attacchi siano aumentati nel 2018, per un totale di 55,7%, rispetto al 45,32% del 2017 ed al 41,57% del 2016. Una crescita significativa e confermata dai vari altri rapporti nazionali e internazionali, e che verrà approfondita nei prossimi paragrafi.

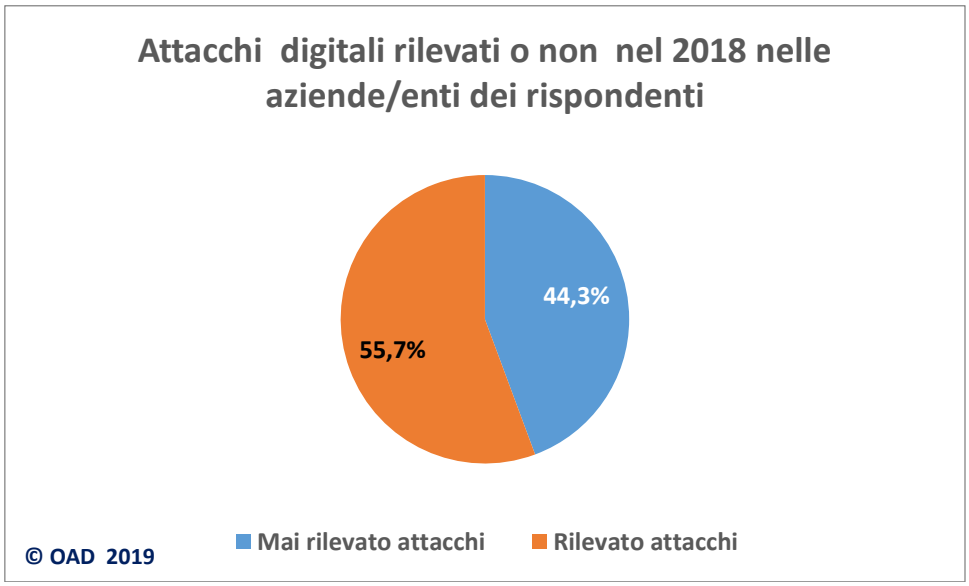

Fig. 6-1

La fig. 6-2 evidenzia se si sono rilevati più o meno di 10 attacchi per anno per azienda/ente, così da indicare la ricorrenza dello stesso tipo di attacco. In tale conteggio, come specificato nel questionario, non sono essere considerati i tentativi di spamming o di phishing, che in taluni periodi possono essere a decine in un solo giorno.

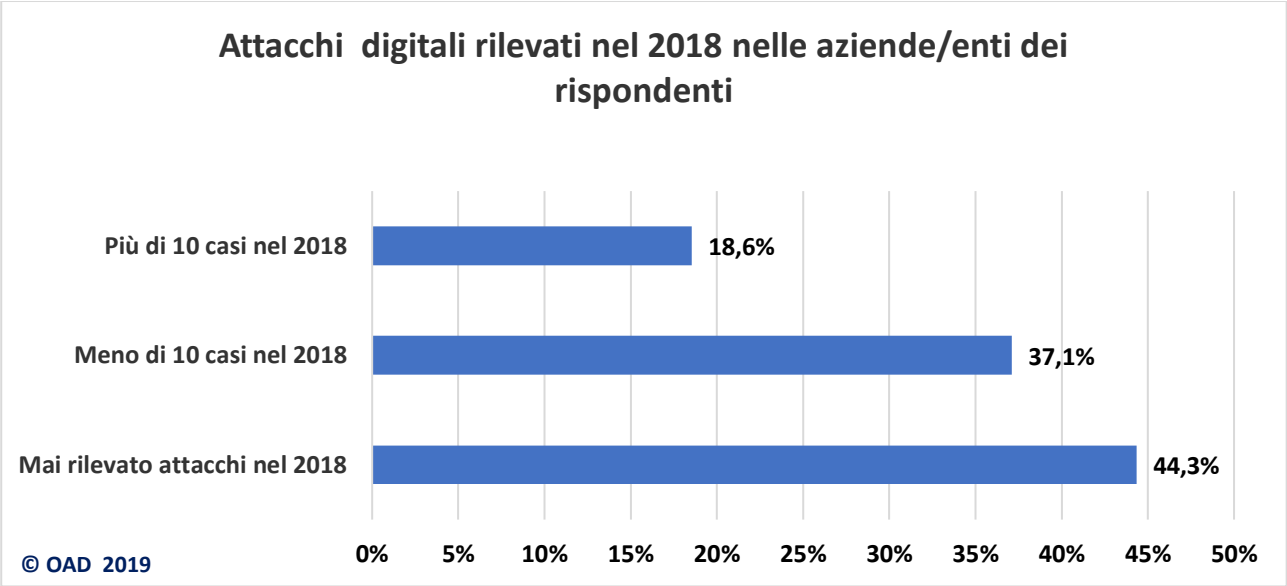

Fig. 6-2

La fig. 6-3 confronta il numero di attacchi rilevati nei diversi Rapporti OAI dal 2007 al 2018. Tale confronto non ha valenza statistica ed è da considerare come tendenza puramente indicativa, dato che i campioni dei rispondenti nei diversi anni sono diversi come mix e come numero. Nell'arco temporale considerato, la figura evidenzia come, a parte il 2008 che rappresentò il primo "annus horribilis" per la quantità di attacchi occorsi, dal 2007 al 2015 si è avuto un sali-scendi del numero di attacchi rilevati attorno a circa il 40% dei rispondenti, e dal 2015 è iniziata una continua crescita percentuale degli attacchi rilevati. Il 2018 rappresenta non solo il picco più alto, ma, per la prima volta negli 11 anni di indagine, la percentuale di attacchi rilevati supera, e di più di 10 punti, la percentuale di quelli non occorsi/rilevati.

Fig. 6-3

L'onda altalenante tra il 2007 ed il 2015 della percentuale di attacchi rilevati ben rappresenta la continua battaglia tra "guardie e ladri" e l'avvicendarsi di innovazioni sulle modalità d'attacco, cui poi seguono misure di difesa atte a contrastarli, ma con gli ovvi fisiologici ritardi.
Dal 2015 in avanti, il numero di aziende/enti che hanno rilevato attacchi è percentualmente sempre cresciuto: un chiaro indicatore della criticità degli attacchi portati, e delle misure di sicurezza di contrasto che non si sono rilevate adeguate.
Il 40% emerso fino al 2016 pur con campioni diversi di rispondenti, è un riferimento stabile negli anni in Italia, con oscillazioni relativamente contenute rispetto a questo numero. Da alcuni esperti questo numero è considerato troppo basso, dato che probabilmente molti attacchi non sono stati rilevati dai rispondenti. Questo è sicuramente possibile, a livello mondiale si stima addirittura che 2/3 degli attacchi lanciati non siano rilevati, anche se vanno a buon fine. Ma in merito l'autore ritiene il 40% sia una corretta valutazione "media" per la situazione italiana, dato che:

- Come indicato dalle più recenti statistiche ISTAT (fig. 6.4), in Italia è elevatissimo il numero di piccole e piccolissime imprese: 99,91% le imprese sotto i 250 dipendenti, le così dette PMI, e di queste il 95,22% è costituito da aziende con meno di 9 dipendenti. Queste piccole organizzazioni non costituiscono sicuramente un target per cyber criminali, se non per attacchi di massa, come spiegato nel seguito;
- Per le Pubbliche Amministrazioni italiane si calcolano circa 55000 enti, di cui solo poche centinaia hanno grandi dimensioni, come dipendenti; valgono per esse le stesse considerazioni espresse al punto precedente;
- Se l'azienda/ente non ha rilevato l'attacco portato, significa che il danno subito non era rilevante, a parte l'eventuale furto di informazioni.

Fig. 6-4

E quindi evidente che per gli attacchi mirati (targeted), le micro e le nano imprese sicuramente non rappresentano un obiettivo di interesse specifico per i cyber criminali. Esse possono essere coinvolte in attacchi di massa, come quelli basati sul phishing e sul ransomware, così come avviene tipicamente o per cogliere qualcuno nella massa, o per motivi ideologici o terroristici (per l'analisi delle possibili motivazioni si rimanda ai successivi paragrafi sulle singole tipologie di attacco, da §6.1 a §6.15).

Una sintesi della distribuzione percentuale degli attacchi subiti nel 2018 per dimensione e per fatturato delle aziende/enti dei rispondenti[12] è riportata nelle fig. 6-5 e 6-6. La prima mostra come gli attacchi digitali, e soprattutto quelli ripetuti, sono distribuiti sia sulle piccole che su grandi e grandissime organizzazioni, in qualche modo indipendentemente dalle loro dimensioni, come numero di dipendenti. La seconda mostra che gli attacchi si sono focalizzati su aziende/enti con i più elevati fatturati, confermando che le motivazioni degli attacchi sono prevalentemente di tipo economico.

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

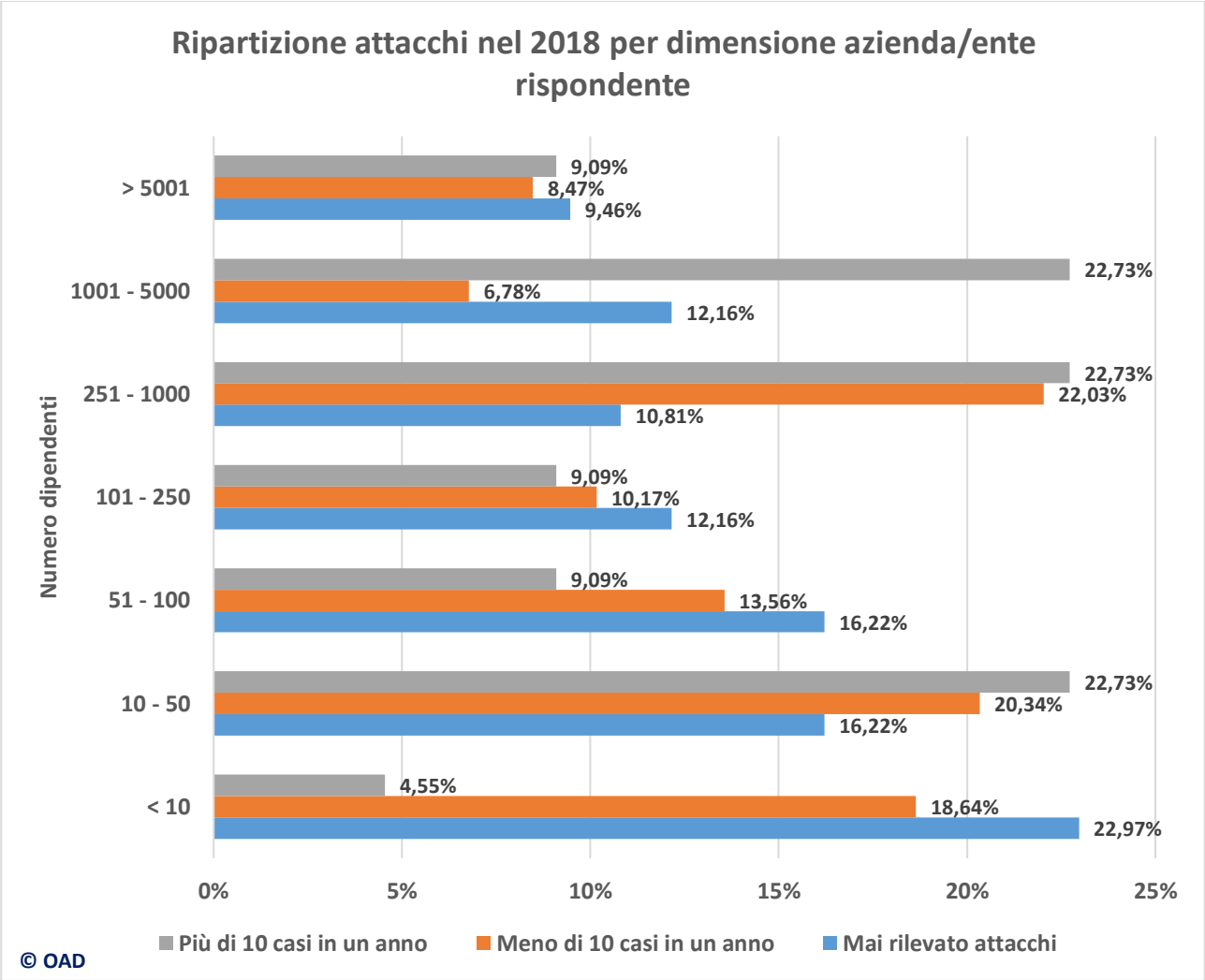

Fig. 6-5

Le strutture più grandi, percentualmente (a meno del settore tra 51-100 dipendenti) hanno subito meno attacchi ma con maggior frequenza.
Questo è ulteriormente confermato dall'analisi degli attacchi per fatturato nel 2017 (fig. 6-6). La maggior parte degli attacchi è per le organizzazioni piccole-medie, fino a 1 milione € di fatturato: ed è interessante come più del doppio di quelle della fascia più alta abbiano subito attacchi con frequenza >10 nell'anno.

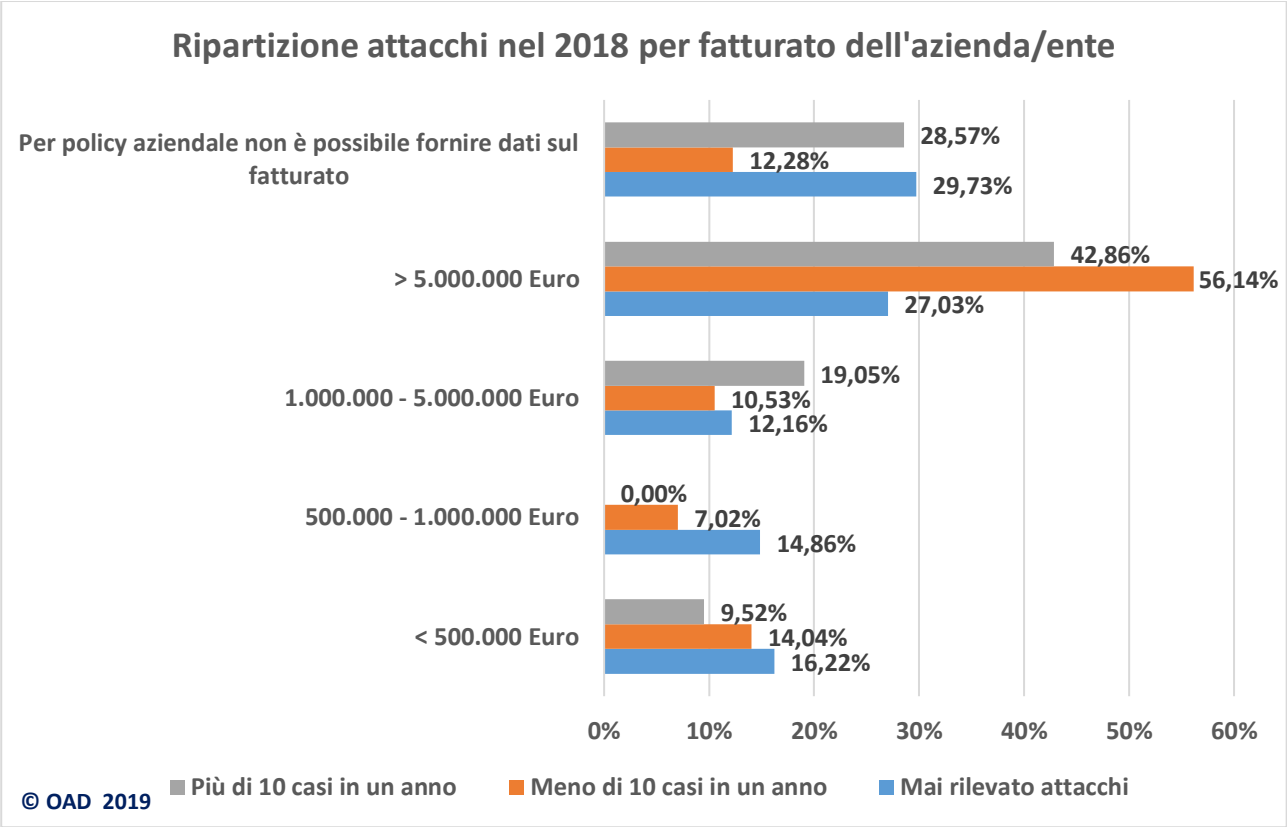

Fig. 6-6

Facendo riferimento alle tipologie di attacco, ossia al "che cosa" viene attaccato (si veda Allegato A), tipologie analizzate una per una nei paragrafi seguenti e a cui si rimanda per i vari dettagli, la fig. 6-7 mostra la diffusione in percentuale delle famiglie di attacchi rilevati nelle aziende/enti dei rispondenti nel 2018, con al primo posto **gli attacchi al controllo degli accessi (54,21%).** Tale famiglia di attacchi era al primo posto anche nell'indagine dell'anno scorso. Al secondo posto **l'attacco/uso non autorizzato di sistemi ICT** nel loro complesso, con una diffusione tra i rispondenti del **41%**. Al terzo posto gli **attacchi alle reti di comunicazione dati**, da quelle geografiche a quelle locali, con una diffusione tra i rispondenti del **34,65%.**
Per alcune tipologie di attacco, nella fig. 6-7 indicate con (*), molti rispondenti non utilizzano i sistemi/servizi ICT oggetto del tipo di attacco, e per tale motivo in questi casi la somma delle percentuali, tra attacchi rilevati e non, non raggiunge il 100%. Per i dettagli per ogni tipologia di attacco considerato si rimanda agli specifici paragrafi da §6.1 a §6.15.

La diffusione delle tipologie di attacchi rilevate nell'indagine si allinea nella sostanza con quelle rilevate nei principali rapporti internazionali sugli attacchi digitali, valori delle percentuali a parte, e conferma così la correttezza dei valori forniti dall'indagine OAD 2019.

La fig. 6-9 sintetizza, per le varie tipologie di attacco rilevate dai rispondenti nel 2018, le tecniche di attacco usate: come mostra la figura, esse sono state raggruppate in sette "macro" categorie, illustrate in dettaglio nell'Allegato A.1.1, tra le quali il rispondente poteva scegliere con risposte multiple.
Il valore in % sull'asse orizzontale del grafico costituisce un indice della loro diffusione nel 2018, chiamato nel seguito coefficiente di diffusione, nell'ambito delle 15 tipologie (famiglie) di attacchi considerati, e che cercano di coprire tutti i casi noti, senza entrare in troppi sotto-casi.
Al primo posto come tecnica più diffusa è la raccolta di informazioni, tipicamente basata su tecniche di social engineering. Al secondo posto i codici maligni e script, che includono anche i comandi diretti

al sistema operativo e/o alle banche dati**:** il perdurare in Italia di ransomware negli ultimi anni ha sicuramente contribuito al consolidamento di queste tecniche, che l'anno scorso erano al primo posto. I Toolkit raggiungono il terzo porto come diffusione, così come nell'anno precedente, grazie anche ai numerosi software gratuiti messi a disposizione su Internet.

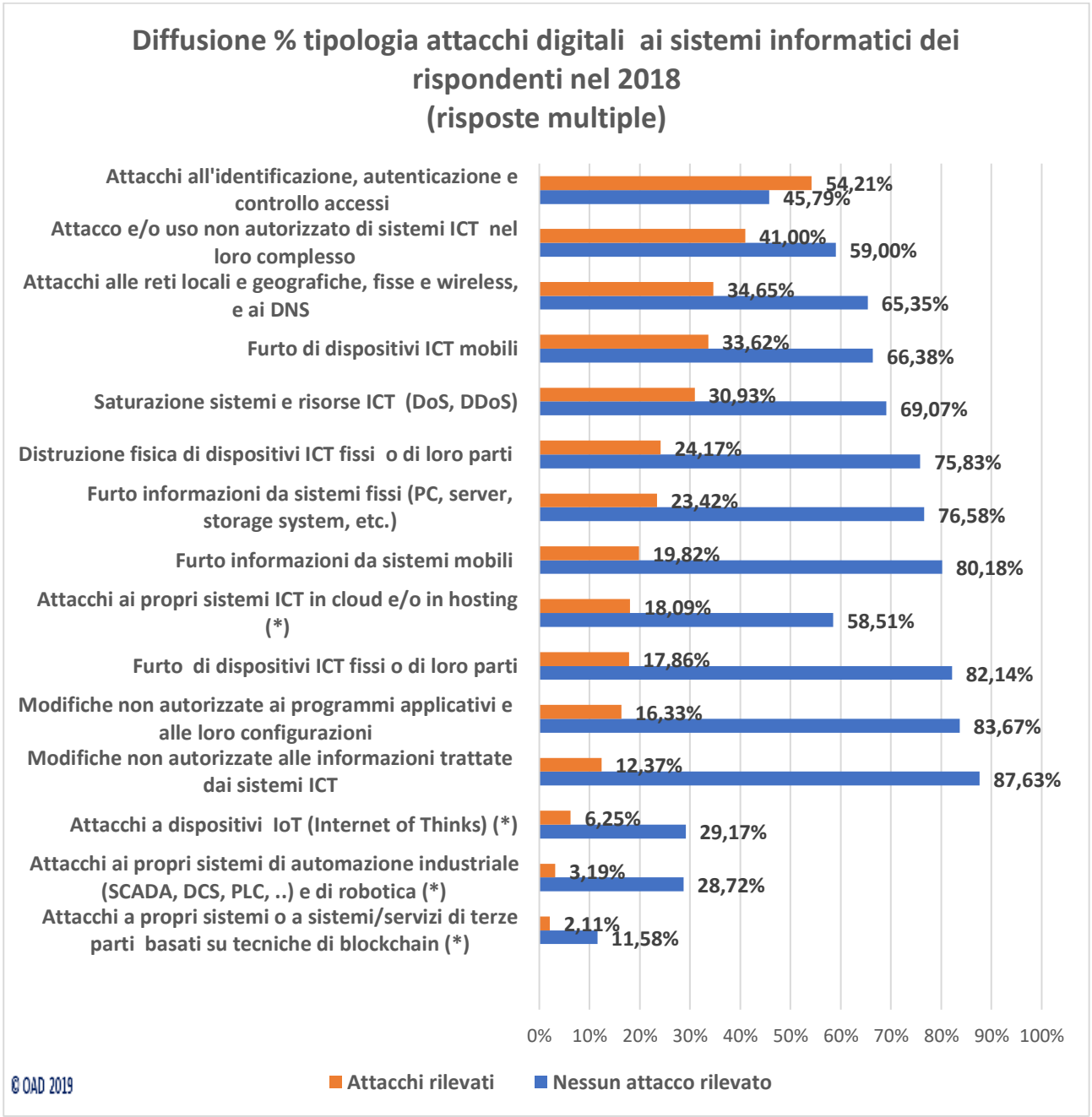

Fig. 6-7

(*) taluni rispondenti non utilizzano questo tipo di sistemi/risorse ICT

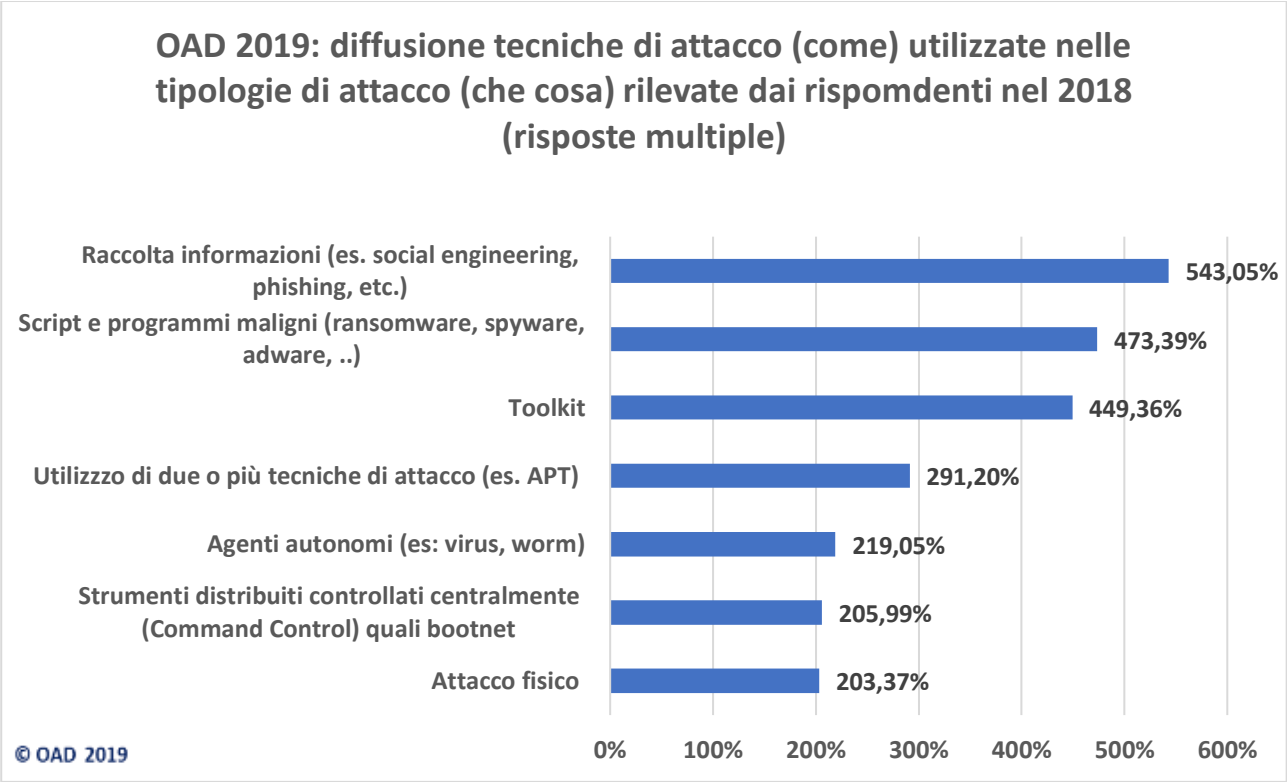

Fig. 6-8

Queste tre prime tecniche sono state individuate dai rispondenti come le più diffuse, ed hanno un coefficiente di diffusione a scalare, ma abbastanza vicino tra loro. L'utilizzo di più tecniche di attacco si stacca fortemente come coefficiente di diffusione rispetto alle prime tre, e così le altre tecniche, con coefficienti tra loro più vicini.

La tabella in fig. 6-9 mappa le tecniche di attacco che i rispondenti ritengono siano state usate nei con i diversi tipi di attacco digitale che hanno subito. In neretto rosso è evidenziata la tecnica più usata per tipologia di attacco (in taluni casi ce n'è più di una a parità di coefficiente di diffusione), in neretto rosso incorniciato il coefficiente più alto ottenuto per quella tecnica.
È opportuno considerare che i coefficienti di diffusione delle tecniche d'attacco per le tipologie d'attacco a IoT, automazione industriale e robotica, blockchain, sono da considerarsi come indicatori di alcuni casi specifici, avendo avuto pochi rispondenti che hanno subito tali tipologie d'attacco nel bacino di rispondenti di OAD 2019.

La fig. 6-10 mostra la distribuzione percentuale degli attacchi e della loro numerosità per settore merceologico delle aziende/enti dei rispondenti. In §10.2 è dettagliata la tipologia e la numerosità dei rispondenti per settore merceologico, avendo preso a riferimento la classificazione ufficiale ATECO[13].
Grazie ai ripetuti inviti a compilare il questionario on line, ed anche al voluto protrarsi della chiusura del questionario ben oltre la scadenza pianificata per poter raggiungere un numero "minimo" di rispondenti, tutti i settori merceologici hanno risposto, ma solo per due raggruppamenti merceologici si è avuto un significativo numero di risposte (come negli anni precedenti): il settore dei sevizi ICT ed il settore manifatturiero. Questi due settori merceologici hanno un numero sufficiente di risposte, e le indicazioni percentuali loro relative forniscono indicatori significativi e credibili. Tutti gli altri contribuiscono numericamente all'inquadramento generale del fenomeno degli attacchi digitali in Italia, sono interessanti, ma sono troppo pochi per poter effettuare specifiche analisi settoriali e

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

considerarli indicatori di riferimento della situazione degli attacchi digitali del loro settore.

Tassonomia attacchi digitali (che cosa attacco) nel 2018	Attacco fisico	Raccolta informazioni (es. social engineering, phishing, pharming, hoax,scanning, indagini su Internet, ecc.)	Script e programmi maligni (ransomware, spyware, adware, ..)	Agenti autonomi: programmi maligni che si replicano e diffondono autonomamente, come virus e worm	Toolkit: programmi in grado di scoprire e sfruttare vulnerabilità (rootkit, metaexploit, ..)	Strumenti distribuiti controllati centralmente (Command Control) quali bootnet	Utilizzzo di due o più delle precedenti tecniche (APT, Advanced Persistent Threat)	Non sono state individuate le tecniche di attacco
Distruzione fisica di dispositivi ICT fissi o di loro parti	24,17%							
Furto di dispositivi ICT mobili	33,62%							
Furto di dispositivi ICT fissi o di loro parti	17,86%							
Furto informazioni da sistemi fissi (PC, server, storage system, etc.)	15,4%	53,8%	46,2%	30,8%	26,9%	7,7%	7,7%	3,8%
Furto informazioni da sistemi mobili	18,2%	31,8%	36,4%	8,3%	22,7%	2,8%	8,3%	8,3%
Attacchi all'identificazione, autenticazione e controllo accessi	1,7%	65,5%	44,8%	15,5%	19,0%	12,1%	17,2%	15,5%
Attacchi alle reti locali e geografiche, fisse e wireless, e ai DNS	40,0%	45,7%	37,1%	28,6%	25,7%	25,7%	2,9%	8,6%
Attacco e/o uso non autorizzato di sistemi ICT nel loro complesso	2,4%	48,8%	53,7%	19,5%	29,3%	17,1%	19,5%	9,8%
Modifiche non autorizzate ai programmi applicativi e alle loro configurazioni	0,0%	43,8%	62,5%	6,3%	31,3%	6,3%	6,3%	6,3%
Modifiche non autorizzate alle informazioni trattate dai sistemi ICT	0,0%	41,7%	50,0%	25,0%	33,3%	8,3%	8,3%	16,7%
Saturazione sistemi e risorse ICT (DoS, DDoS)	0,0%	26,7%	13,3%	6,7%	20,0%	46,7%	20,0%	10,0%
Attacchi ai propri sistemi ICT in cloud e/o in hosting (*)	0,0%	35,3%	29,4%	11,8%	41,2%	29,4%	17,6%	11,8%
Attacchi a dispositivi IoT (Internet of Thinks) (*)	16,7%	50,0%	33,3%	16,7%	100,0%	16,7%	50,0%	16,7%
Attacchi ai propri sistemi di automazione industriale (SCADA, DCS, PLC, ..) e di robotica (*)	33,3%	100,0%	66,7%	0,0%	100,0%	33,3%	33,3%	0,0%
Attacchi a propri sistemi o a sistemi/servizi di terze parti basati su tecniche di blockchain (*)	0,0%	0,0%	0,0%	50,0%	0,0%	0,0%	100,0%	0,0%
Indice complessivo diffusione tecnica di attacco	*203,37%*	*543,05%*	*473,39%*	*219,05%*	*449,36%*	*205,99%*	*291,20%*	*107,37%*

Fig. 6-9

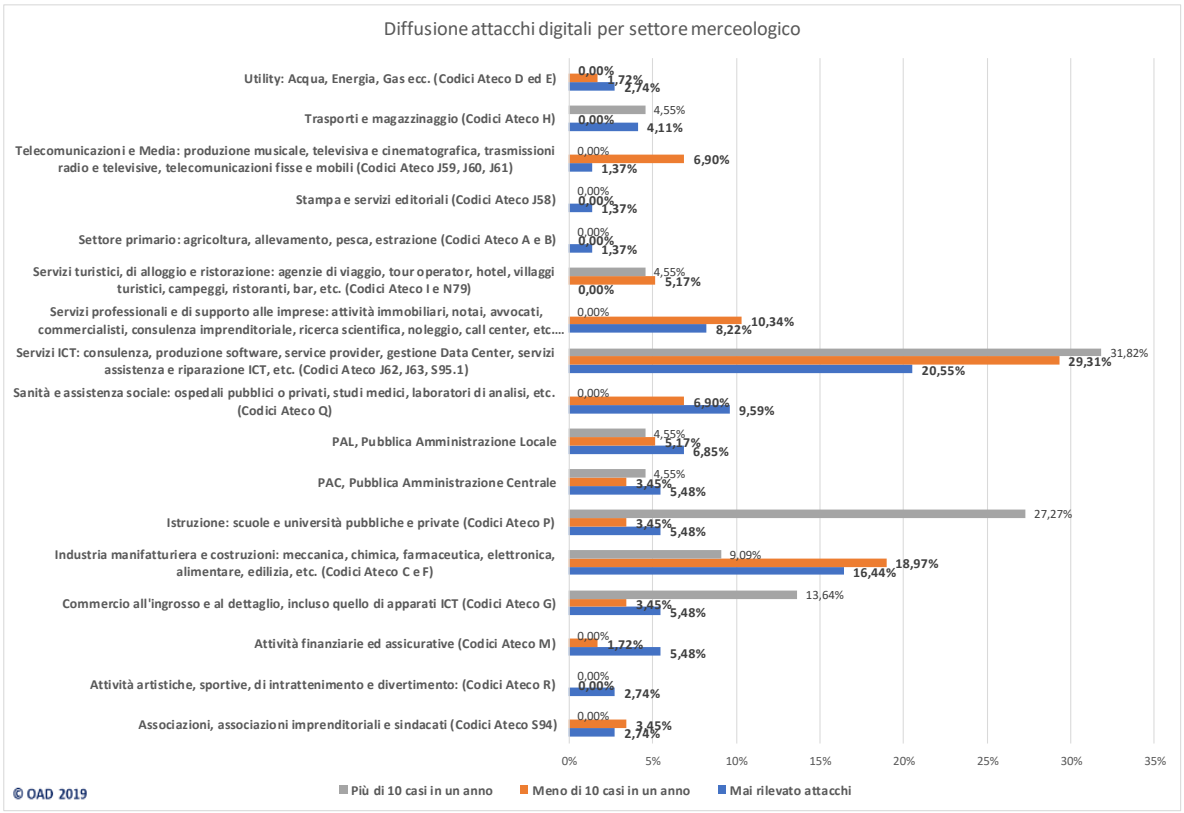

Fig. 6-10

I referenti di alcune aziende/enti non hanno risposto ad alcune delle domande del questionario, talvolta a tutte, trincerandosi dietro le policy aziendali che impediscono il fornire questo tipo di informazioni classificate come riservate, anche se il questionario è totalmente anonimo.
Per questo motivo si è ritenuto più significativo correlare con le dimensioni delle aziende/enti in termini di numero di dipendenti e in termini di fatturato annuo, come mostrato nelle fig. 6-5 e 6-6.

Ogni tipologia di attacco viene analizzata e commentata nel relativo paragrafo del presente Capitolo 6, cui si rimanda, ma nell'analisi complessiva alcune interessanti considerazioni emergono, sintetizzate nei punti seguenti.

- L'indagine 2019 OAD ben rappresenta, percentualmente, la situazione italiana (si veda fig. 6-4 e §10.2): il 62,6% dei rispondenti è di aziende/enti di medio piccole dimensioni (fino a 250 dipendenti), e di queste il 37,4% sotto i 50. Per le grandi organizzazioni, il 9% da da strutture con più di 5001 dipendenti.
- I due macrosettori merceologici che hanno avuto più rispondenti, servizi ICT e manifatturiero, sono quelli che evidenziano una maggior percentuale di attacchi subiti.
- Le aziende del settore manifatturiero che hanno risposto al questionario, per meno del 30% dispongono di sistemi di automazione industriale e di robot (si veda §6.14, §6.13, §10.3).
- Il furto di dispositivi ICT mobili, tipicamente smartphone e tavolette, rimane alto, al 33,6% dei rispondenti, confermando i dati dei precedenti rapporti OAD. Le motivazioni sono soprattutto per impossessarsi e/o rivendere questi costosi dispositivi, come anche evidenziato dalla ben più bassa percentuale di furto delle informazioni contenute, pari al 19,89%.

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

6.1 Distruzione fisica di dispositivi ICT o di loro parti

La distruzione fisica intenzionale di dispositivi ICT o di loro parti, e non dovuta quindi a calamità naturali, crolli o esplosioni accidentali nei locali ove operano, non può che essere attuata tramite un attacco di tipo fisico, svolto da persone che entrano, con o senza permessi, nei locali ove sono situati questi sistemi, e volutamente li danneggiano a livello fisico: forti colpi per scassare la loro struttura, rottura delle connessioni e delle parti elettroniche, rottura delle ventole di raffreddamento e della parte di alimentazione, etc.
Nel Questionario OAD 2019, essendo la tecnica di attacco solo di tipo fisico, non sono state riportate le sotto-domande sulle possibili tecniche di attacco usate.

La fig. 6.1-1 evidenzia quanti rispondenti hanno subito tale attacco nel 2018: nel complesso il 24,17% dei rispondenti, quasi un quarto del bacino, una percentuale elevata.

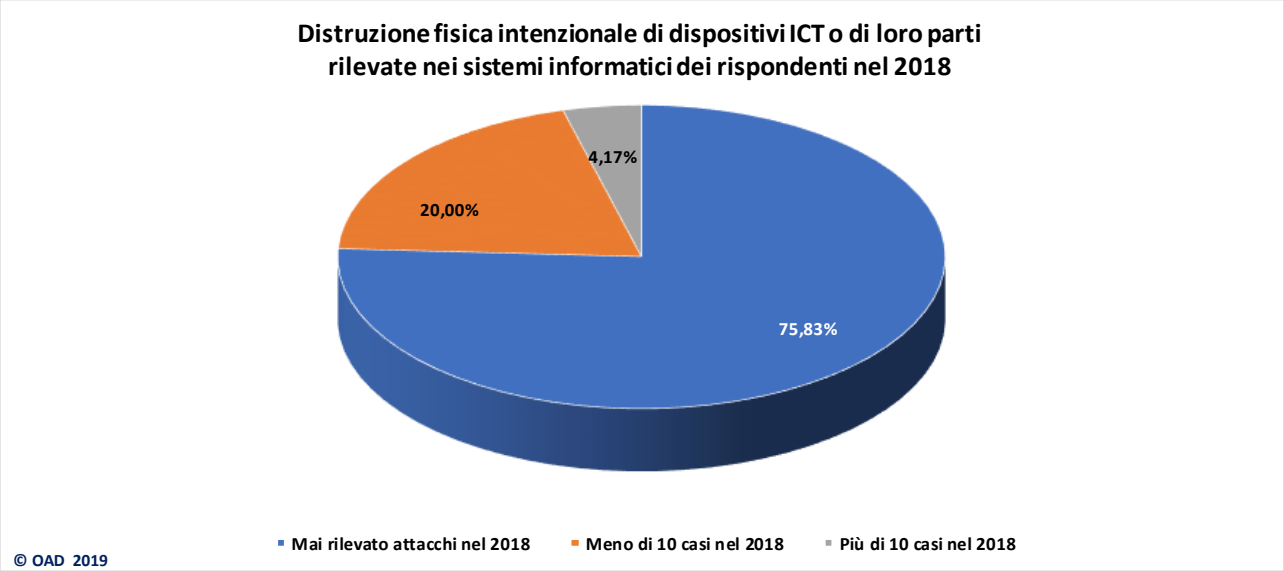

Fig. 6.1-1

La fig. 6.1-2 evidenzia, con risposte multiple, che per il 56,67% dei rispondenti gli impatti, pur nei casi più gravi, siano stati irrilevanti. Più di ¼ ha subito una parziale interruzione, ma con un ripristino in tempi brevi. impatti più gravi hanno percentuali molto basse. Il 17,24% ha subito gravi impatti.

La fig. 6.1-3, con risposte multiple, elenca le principali motivazioni dell'attacco: al primo posto la ritorsione e/o il ricatto, al secondo il vandalismo, in molti casi probabilmente correlato alla ritorsione, al terzo l'hacktivism. Interessante evidenziare che il 10,3% indica il sabotaggio.

La fig. 6.1-4 mostra il tempo di ripristino della situazione ex ante nel caso del peggior attacco subito. Il 92,3% ripristina entro 3 giorni, e di questi il 61,5% entro il primo giorno.
Questo significa che i rispondenti hanno dispositivi di scorta e/o contratti di manutenzione che consentono una veloce sostituzione dei sistemi e dispositivi ICT rovinati.

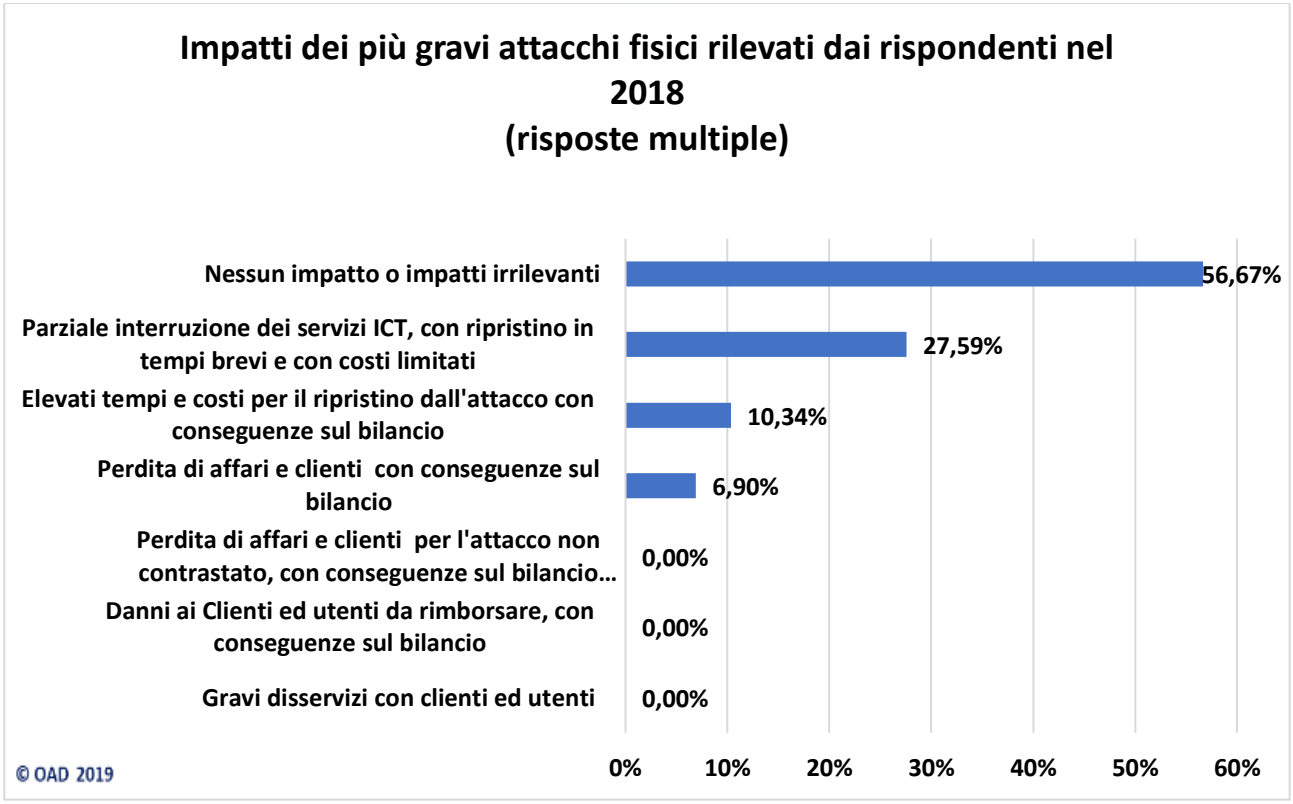

Fig. 6.1-2

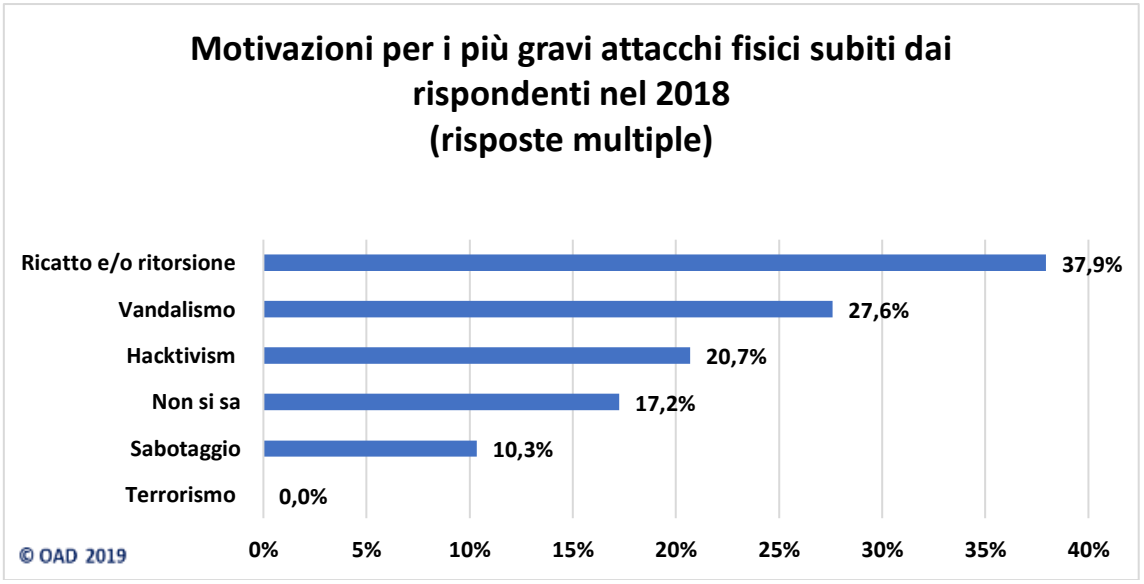

Fig. 6.1-3

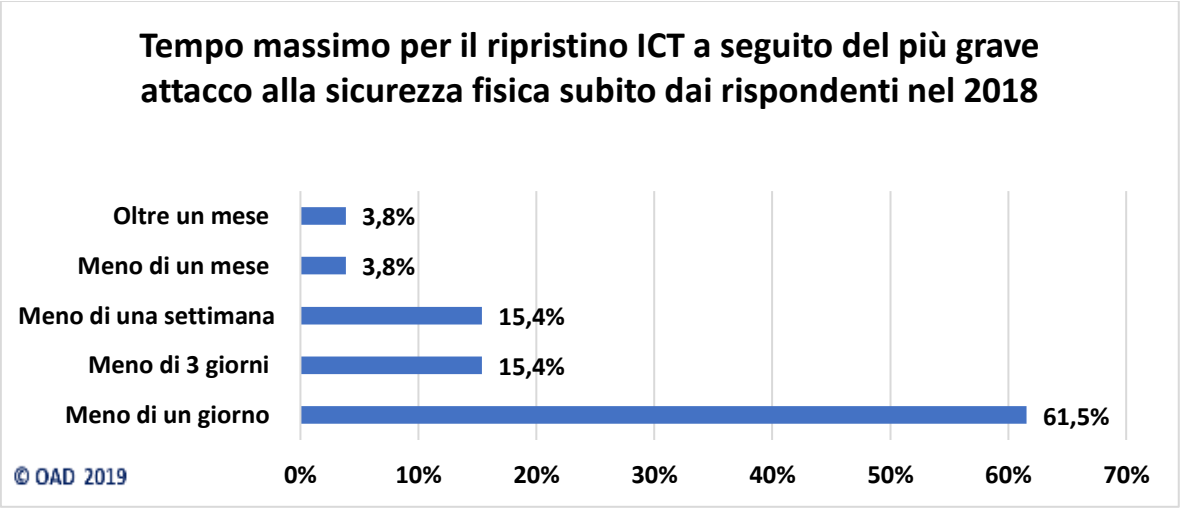

Fig. 6.1-4

6.2 Furto di dispositivi ICT mobili

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

La fig. 6.2-1 riporta che poco più di 1/3 dei rispondenti, 33,6%, ha subito un furto di dispositivi ICT mobili nel 2018: una percentuale alta, che indica come ancora gli utenti non pongano la dovuta attenzione alla protezione, anche solo fisica, di questi dispositivi, che invece sono tecnicamente sempre più potenti e che di fatto sono sempre più utilizzati in sostituzione dei PC, anche di tipo lap top.

La tecnica d'attacco per rubare dispositivi mobili può essere solo l'attacco fisico: per tale motivo nel questionario OAD 2019, per questa tipologia di attacco non sono state riportate le sotto-domande sulle possibili tecniche di attacco usate.

La fig. 6.2-2, con risposte multiple, mostra gli impatti subiti a seguito del furto di dispostivi ICT mobili: per la maggior parte dei rispondenti gli impatti sono stati irrilevanti o di facile risoluzione. Qualcuno ha invece avuto problemi più seri, forse perché il dispositivo conteneva dati riservati non duplicati su altro strumento, o perché i dati contenuti sono stati poi usati per specifici attacchi (si veda §6.5).

La fig. 6.2-3, con risposte multiple, elenca le principali motivazioni, stimate, dell'attacco: il 67.6% dei rispondenti ritiene che il motivo sia il valore della risorsa ICT rubata da rivendere, e il 23,1% per il furto del contenuto informativo dell'oggetto rubato. A decrescere percentualmente le altre possibili motivazioni.

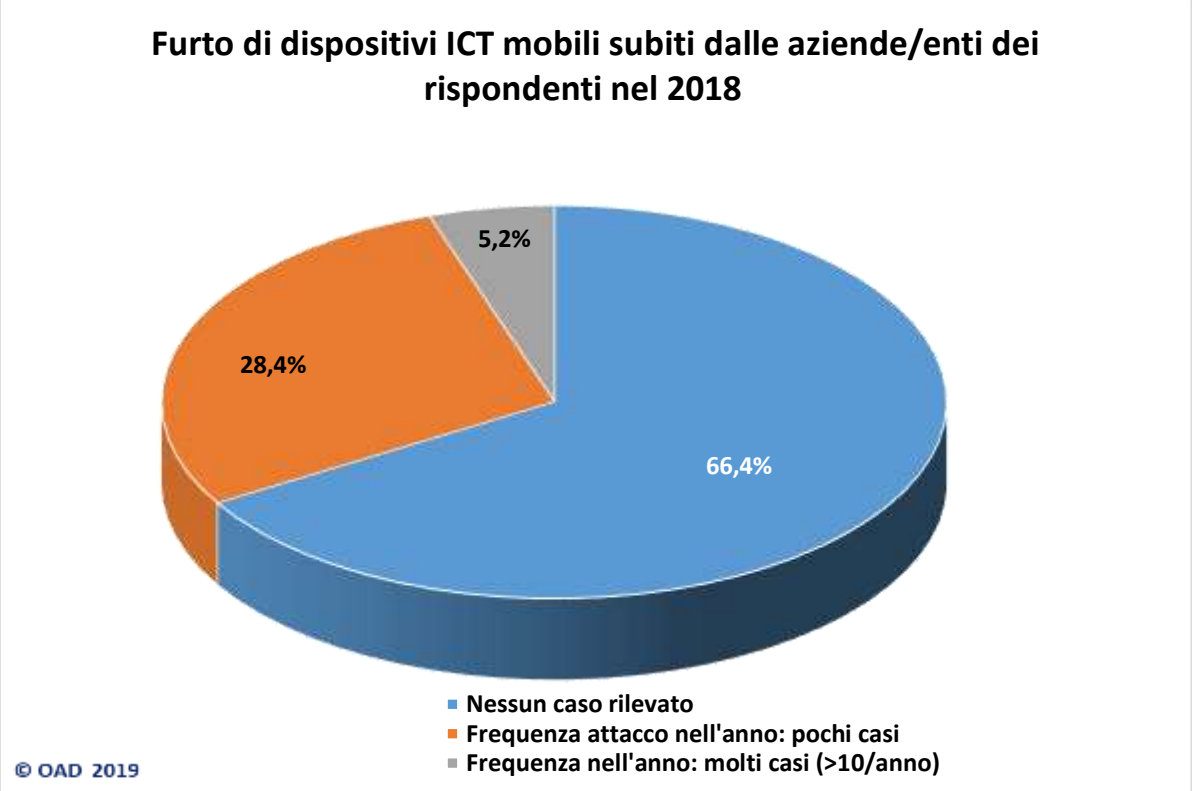

Fig. 6.2-1

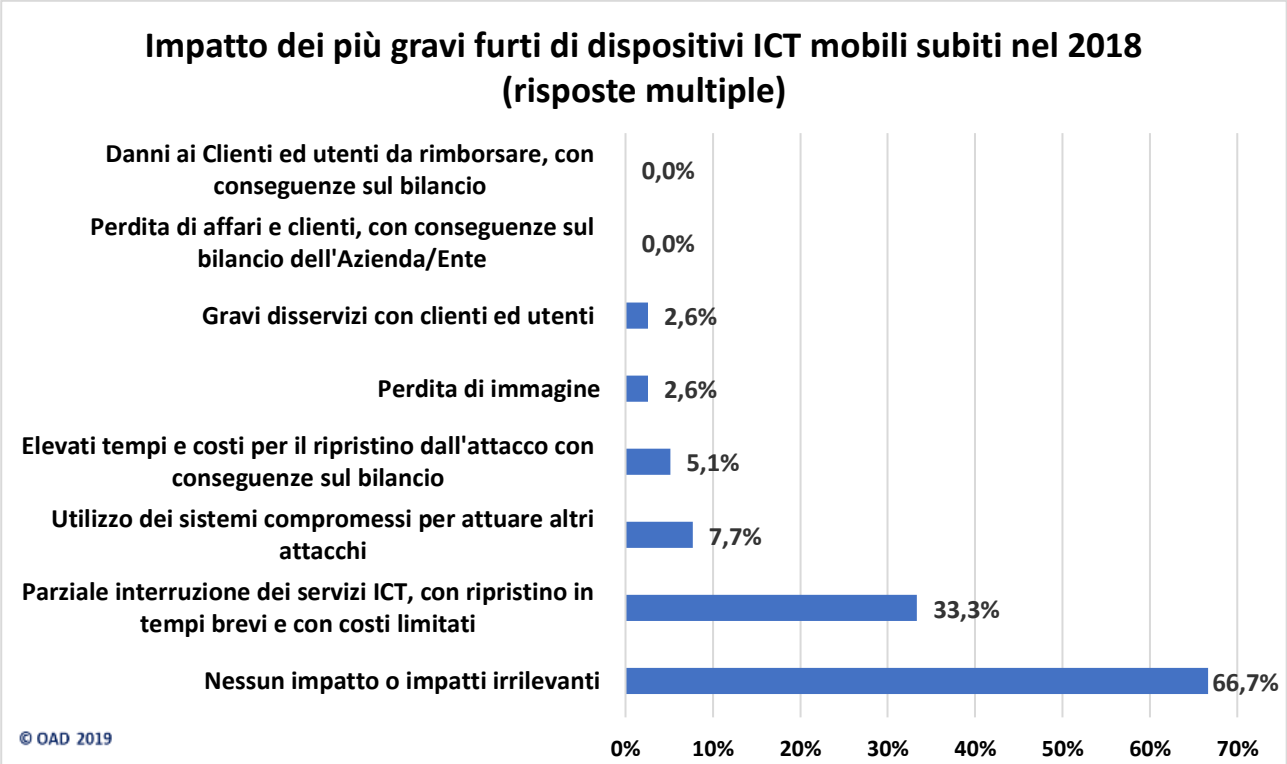

Fig. 6.2-2

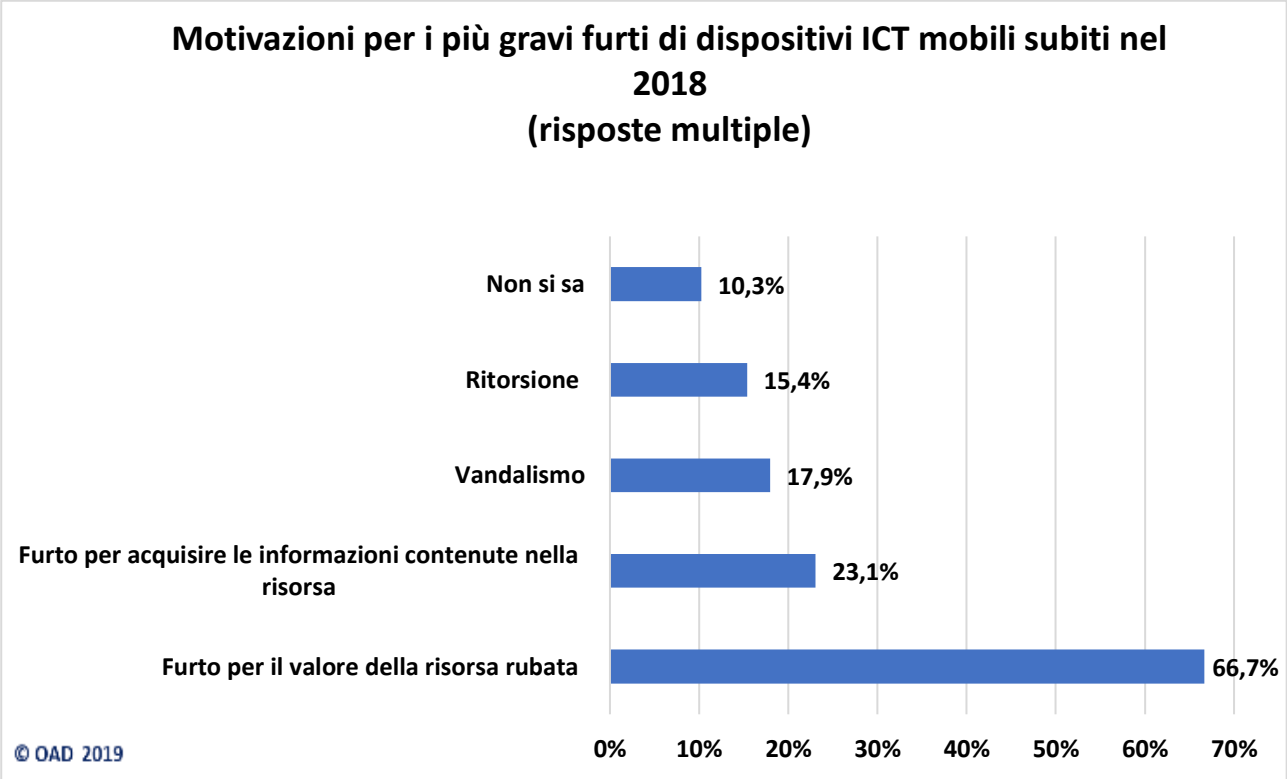

Fig. 6.2-3

La fig. 6.2-4 mostra il tempo di ripristino nel caso del peggior caso nell'anno di furto di un dispositivo mobile. Data la semplicità del ripristino, tutti i casi peggiori occorsi sono stati risolti entro una settimana, e per più della metà dei rispondenti in un solo giorno.

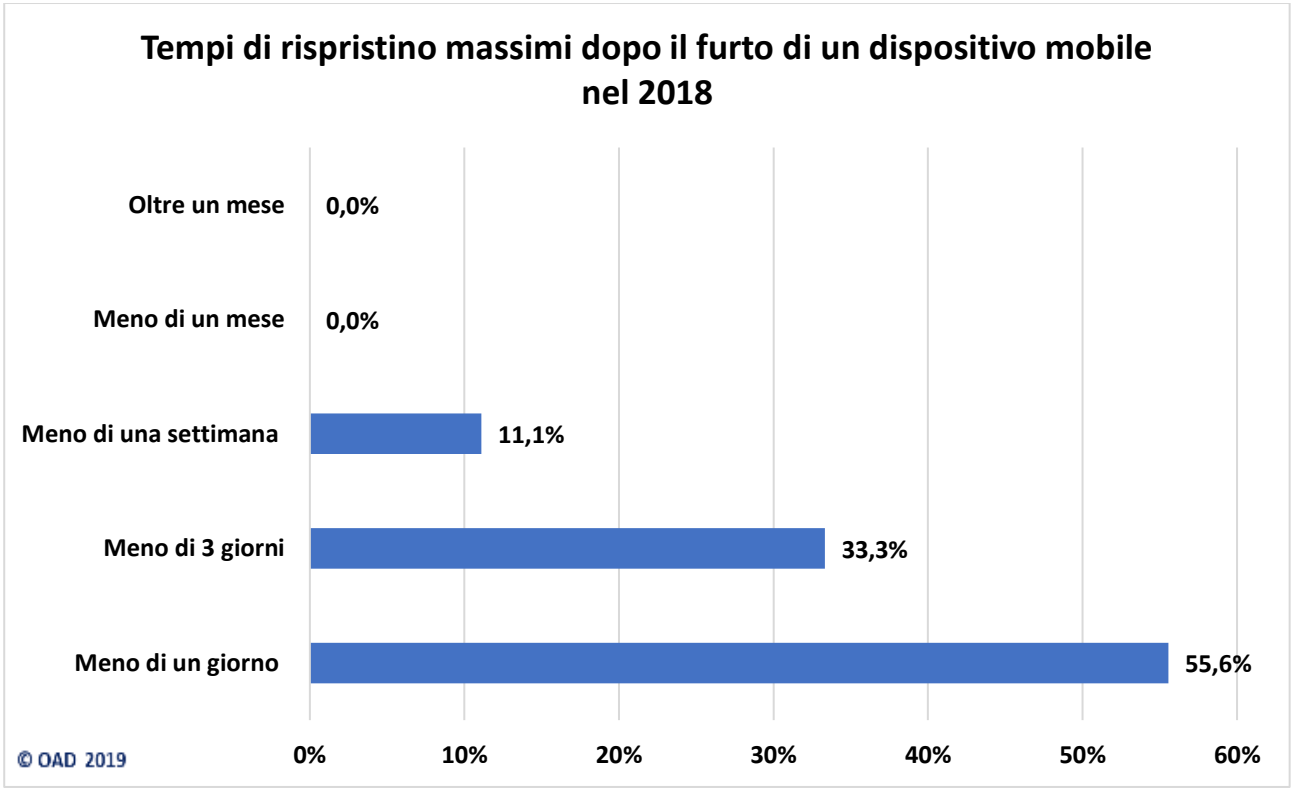

Fig. 6.2-4

6.3 Furto di dispositivi ICT fissi o di loro parti

Anche per il furto di dispositivi ICT o di loro parti, che includono server, sistemi di storage, unità di rete, dispositivi d'utente fissi quali PC e workstation; le loro parti includono i vari componenti dalla scheda madre ai connettori, dai singoli chip alle periferiche quali ad esempio l'hard disk (non quello removibile o chiavette USB), il mouse e/o il video. La tecnica d'attacco può essere solo quella dell'attacco fisico: per tale motivo nel questionario OAD 2019, per questa tipologia di attacco non sono state riportate le sotto-domande sulle possibili tecniche di attacco usate.

Il 17,9% dei rispondenti ha rilevato questo tipo di attacco, come mostrato nella fig. 6.3-1

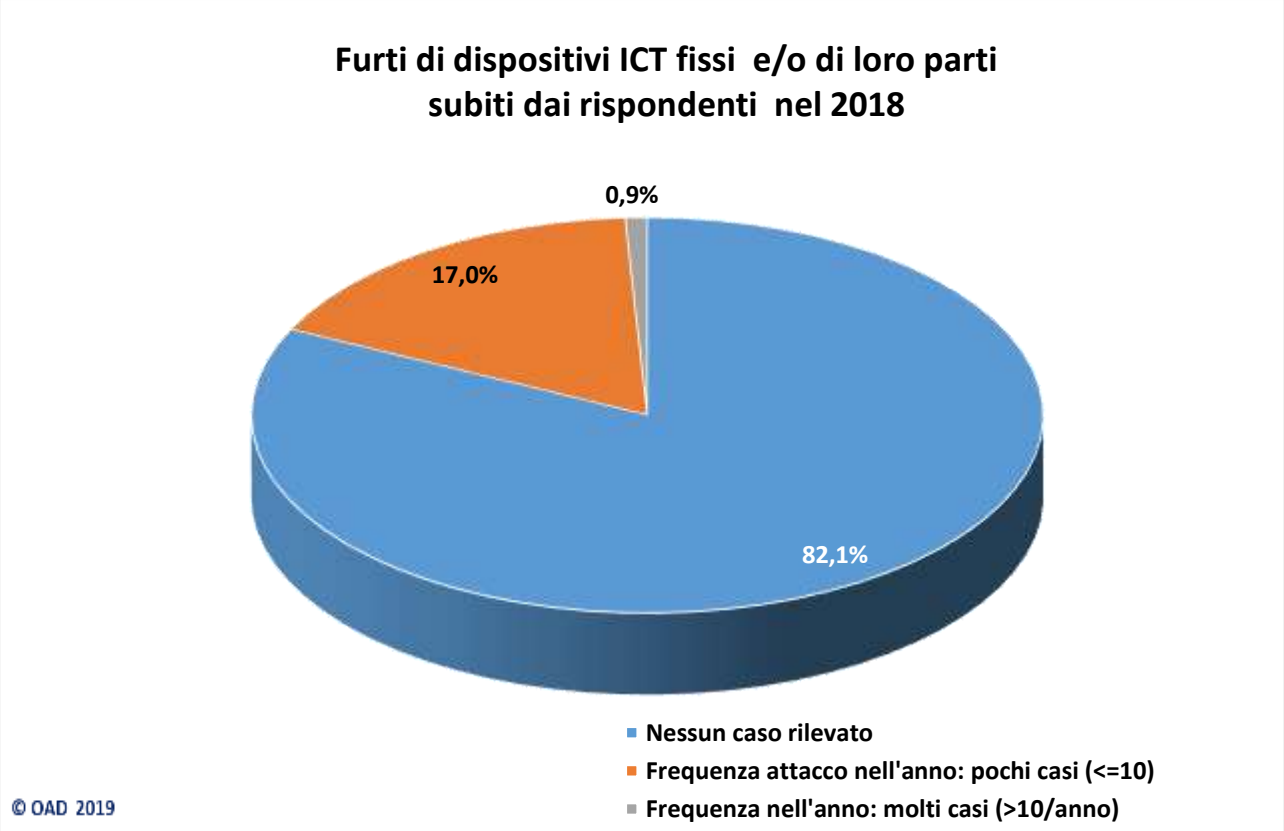

Fig. 6.3-1

La fig. 6.3-2 mostra gli impatti subiti a seguito del furto di dispostivi ICT fissi o di loro parti: per la metà dei rispondenti gli impatti sono stati irrilevanti o di facile risoluzione. Il 10% ha avuto problemi seri, con elevati tempi e costi per il ripristino: sicuramente sono state sottratti hardware non sostituibili a breve, con un blocco forse perché il dispositivo conteneva dati riservati non duplicati/backappati su altro strumento, o perché i dati contenuti sono stati poi usati per più specifici e gravi attacchi.

La fig. 6.3-3 elenca le principali possibili motivazioni dell'attacco, molti simile a quelle indicate per i sistemi mobili. Per il 50% dei rispondenti la motivazione principale è il valore della risorsa ICT fissa rubata, e per il 25% il furto del contenuto informativo. Nella voce "Altro" i rispondenti hanno indicato il furto da parte di personale di terze parti, fornitori e/o manutentori dei dispositivi stessi. Anche se la percentuale emersa è piccola, il problema del controllo delle Terze Parti è un problema crescente soprattutto per la sicurezza digitale e per le piccole e piccolissime aziende, se non del settore ICT.

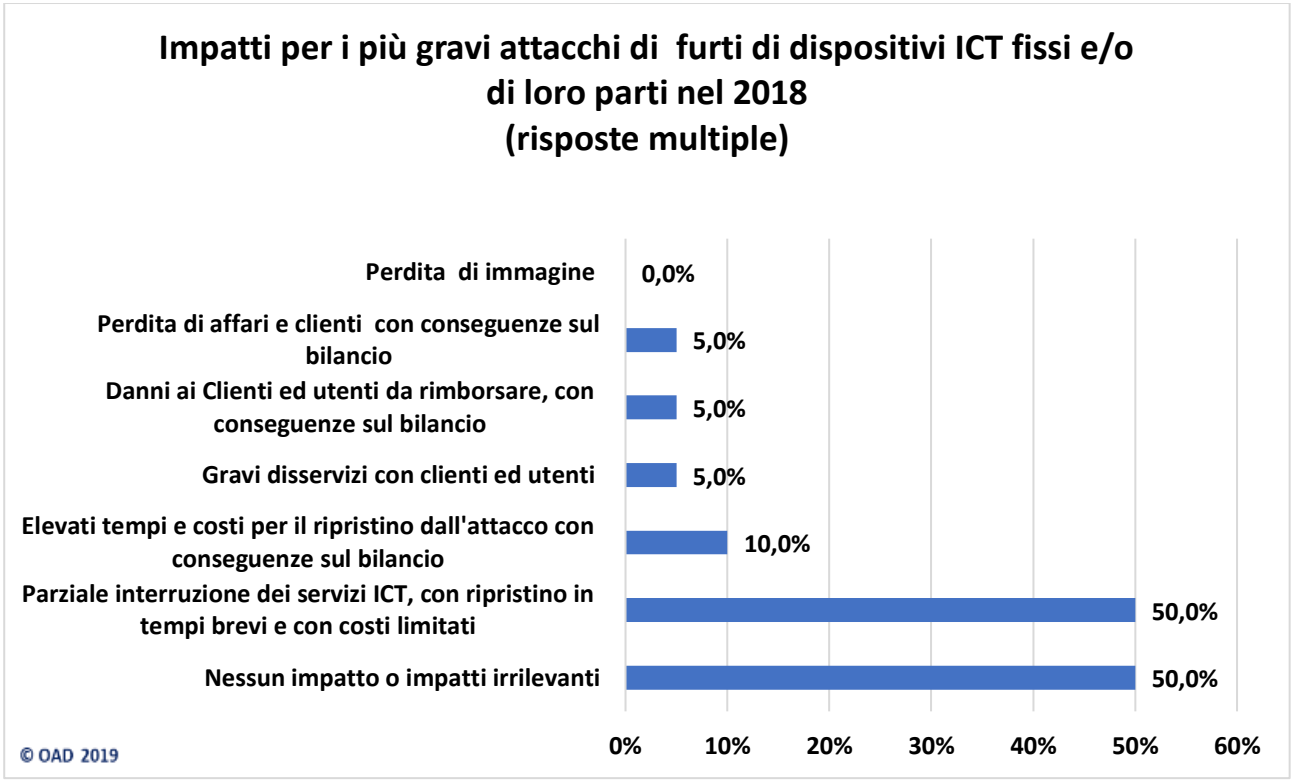

Fig. 6.3-2

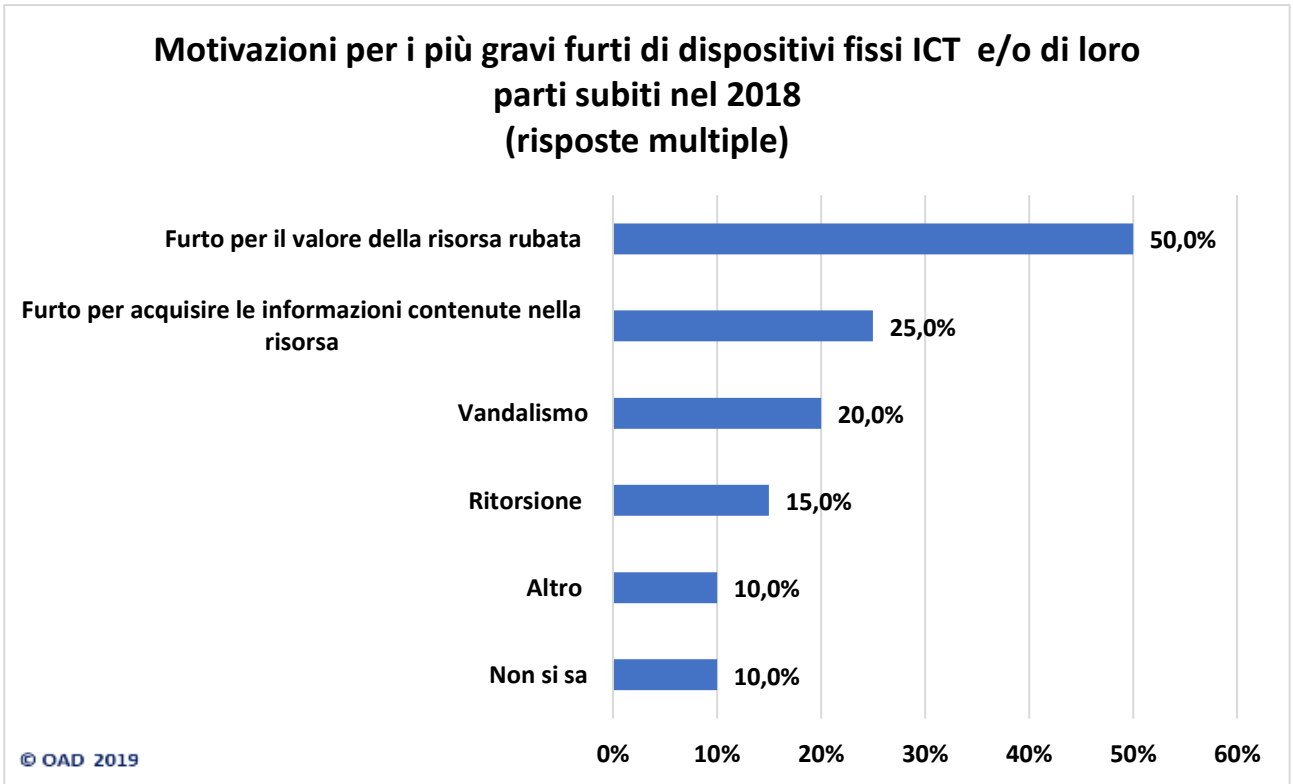

Fig. 6.3-3

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

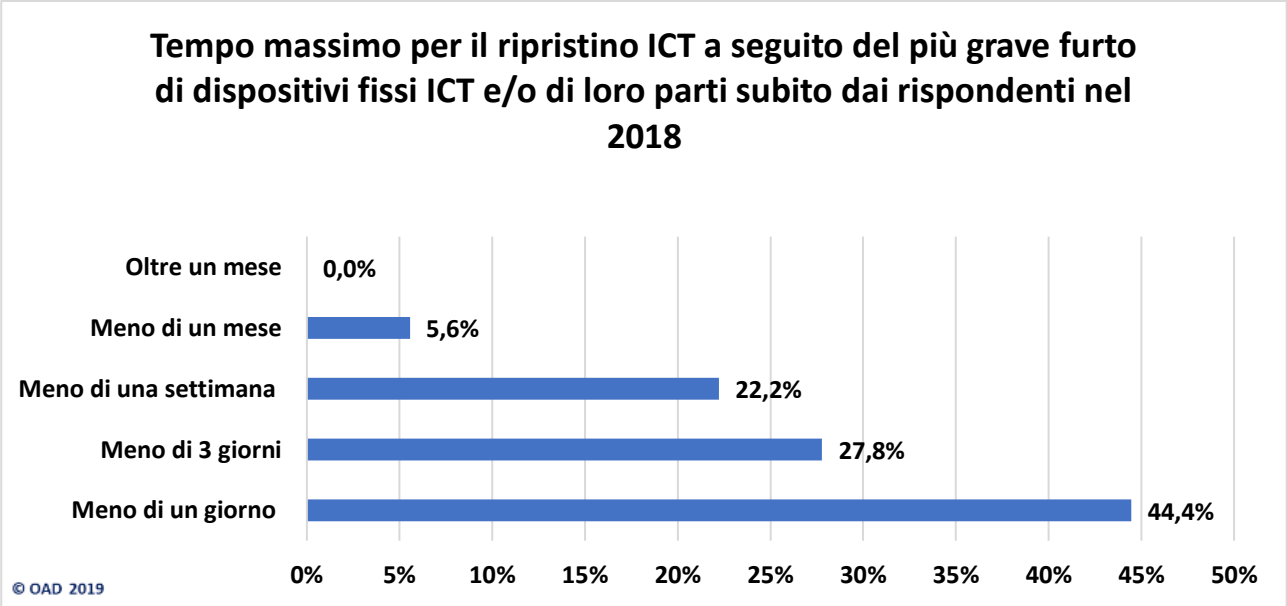

Fig. 6.3-4

6.4 Furto informazioni da sistemi ICT fissi

Il furto di informazioni da sistemi fissi implica che l'attaccante sia stato in grado di accedere, senza averne i diritti, al sistema ICT ed una volta entrato di acquisire le informazioni, tipicamente archiviate in file o su banche dati, e di copiarle: il contesto tipico è il PC, la workstation fissa, il telefono VoIP nell'ufficio/studio, dato che rubare informazioni da sistemi ICT quali un server o uno storage è (o dovrebbe essere) ben più difficile, anche se concettualmente analogo.
È difficile individuare il furto di un'informazione, dato che, al contrario di un bene materiale, con il suo furto non viene a mancare l'informazione originale (a meno che non sia cancellata dopo la copia): scoprire il furto non è quindi semplice e lo si fa prevalentemente in maniera indiretta, verificando i log degli accessi, scoprendo se l'informazione è presente in altri sistemi esterni, se è stata pubblicata, etc.
L'unico modo per proteggere un'informazione dal suo furto (o anche da una sua lettura non autorizzata) è di crittografarla, come anche il GDPR[14] indica: si veda anche §9.2 sulle misure tecniche di contrasto in atto da parte dei rispondenti.

La fig. 6.4-1mostra quanti rispondenti hanno subito tale tipo di attacco nel 2018: nel complesso il 23,4% dei rispondenti, di fatto simile a quanto rilevato nella precedente edizione di OAD, entrambe ben superiori al solo 1,54% del 2016. Il mantenimento nel 2018 del forte incremento avuto nel 2017 è un chiaro indicatore di come dal 2017 gli attacchi anche nella realtà italiana siano cresciuti significativamente per numero e gravità di attacchi digitali. La percentuale rilevata è superiore, ma

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

non di molto, a quella relativa ai furti di informazioni dai dispositivi d'utente mobili (19,8%), di cui in §6.5. Sembrerebbe più facile il furto fisico di un dispositivo mobile, e da questo cercare di entrare nei file e dei dati ivi contenuti. Ma essendo ben nota tale vulnerabilità, chi ha dati critici sui sistemi mobili molto probabilmente li protegge adeguatamente, anche crittandoli; e non passa il proprio dispositivo a colleghi. Le possibilità d'attacco per il furto di dati sono molto più ampie, comprendendo dai dispositivi d'utente fissi ai server, dalle unità di rete ai servizi terziarizzati e in cloud. Il posto di lavoro fisso, essendo molto diffuso, è anche più vulnerabile e può contenere dati critici, soprattutto con gli applicativi di informatica individuale, e può essere talvolta usato da più utenti diversi; ed i dati contenuti non sono il più delle volte crittati.

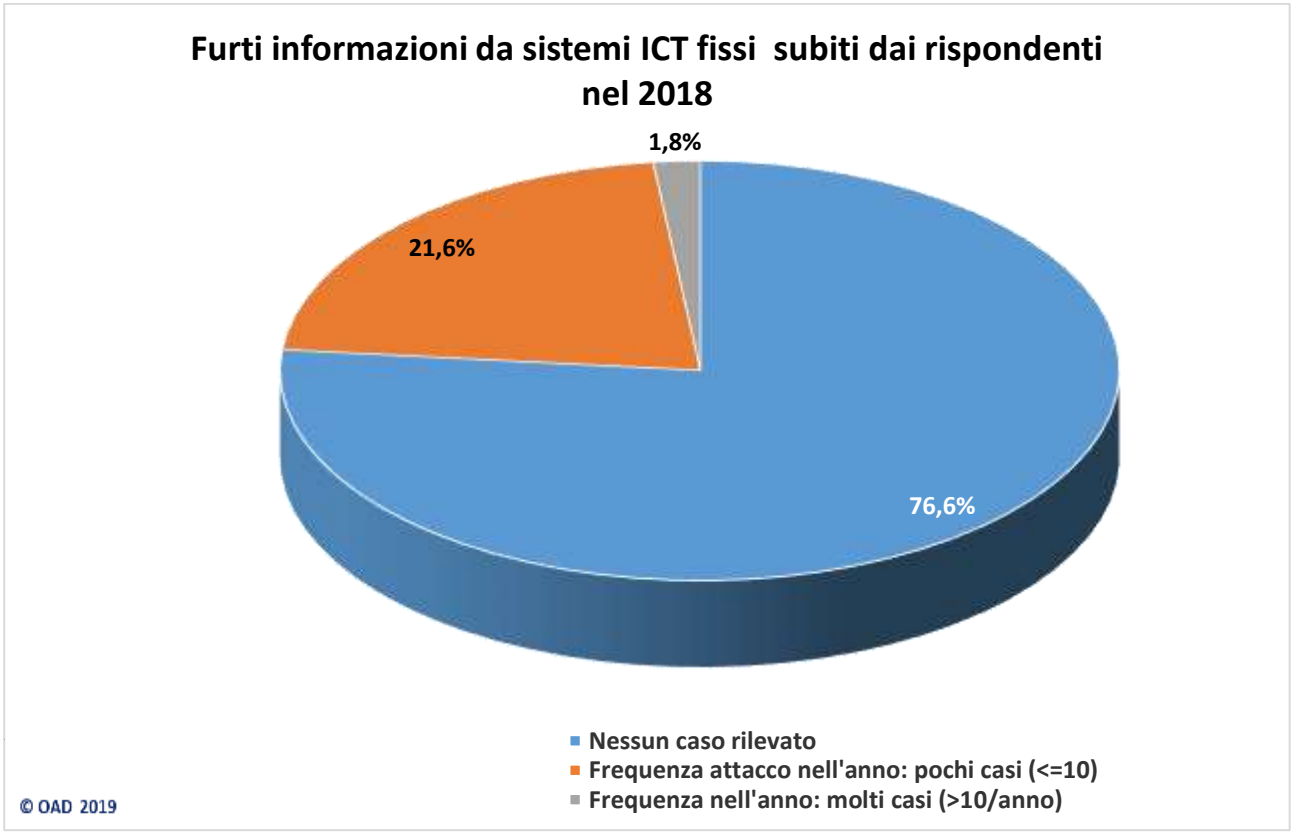

Fig. 6.4-1

La fig. 6.4-2 dettaglia le tecniche d'attacco per il furto di informazioni da sistemi ICT fissi, con risposte multiple. Al primo posto, con 53,8%, le tecniche di social engineering, cui seguono, con 46,2%, le tecniche che raggruppano malware, script e "command". Con maggior distacco in percentuale, a scalare, le altre tecniche.

Nella Fig. 6.4-3, con risposte multiple, quasi il 70% dei rispondenti non ha avuto impatti, o sono stati irrilevanti. Il 7,7% ha avuto una parziale interruzione dei servizi ICT, ma di breve durata e di relativamente facile ripristino. Gli impatti più gravi hanno tutti percentuali assai inferiori. E tali dati sono confermati dalla successiva fig. 6.4-5 sui tempi di ripristino necessari.

Le motivazioni stimate dai rispondenti per i furti di informazione da sistemi fissi ICT sono riportate nella fig. 6.4-4, con risposte multiple: la principale motivazione, con il 57,7%, è il furto per utilizzare in proprio o per rivendere le informazioni. Segue, con il 53,8%, l'uso di tali informazioni per effettuare ulteriori specifici attacchi digitali. Una percentuale non trascurabile, il 34,6%, riguarda ritorsi e ricatti.

La fig. 6.4-5 mostra che, a seguito del più grave furto di informazione da sistemi fissi, sono occorsi per il ripristino della situazione ex ante 3 giorni nel 72% dei casi, di cui il 44% ripristina nella stessa giornata, e nessuno dei rispondenti ha avuto bisogno di più di un mese. Tali dati confermano quanto indicato nella precedente fig. 6.4-3.

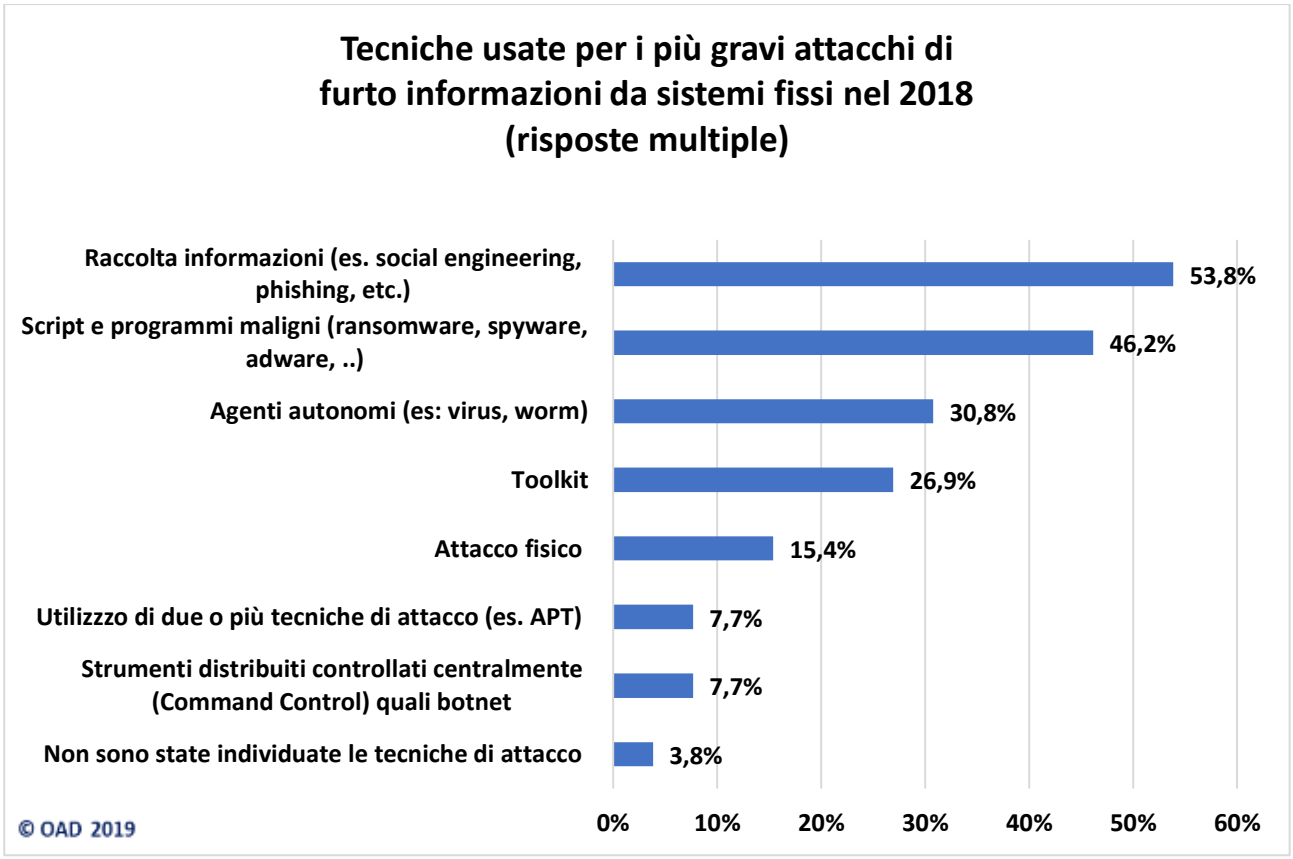

Fig. 6.4-2

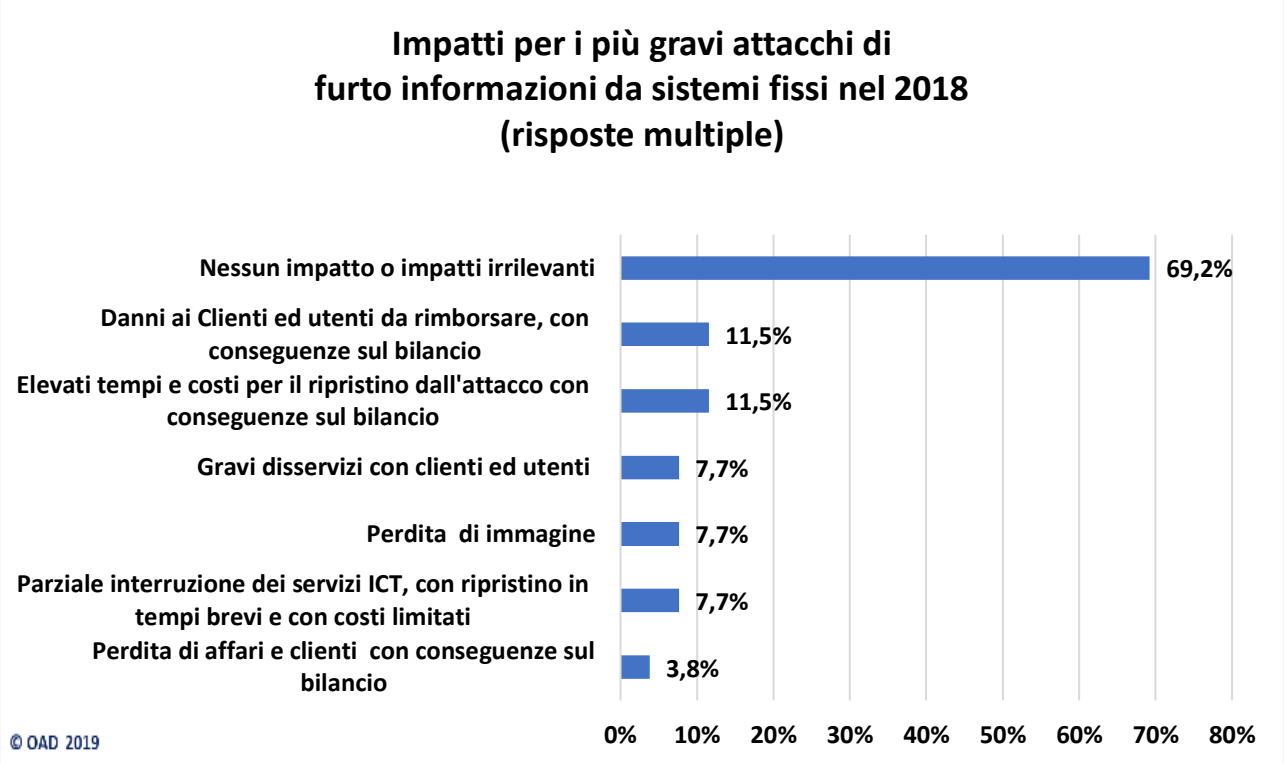

Fig. 6.4-3

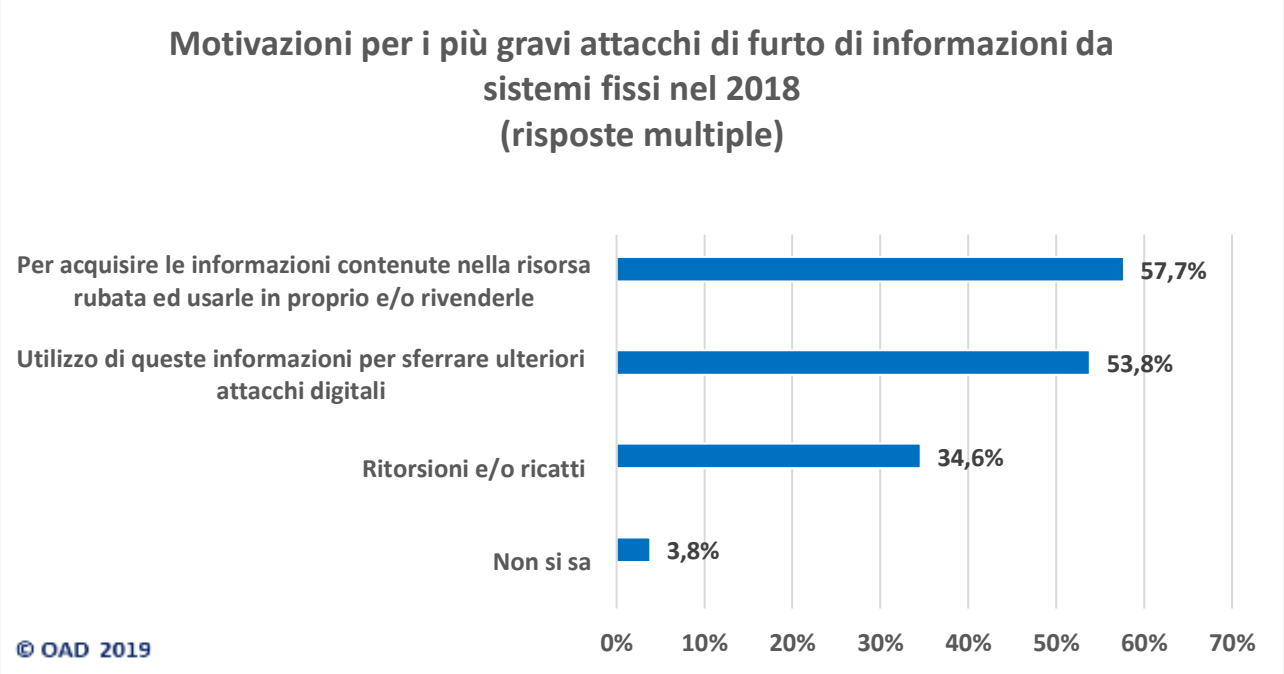

Fig. 6.4-4

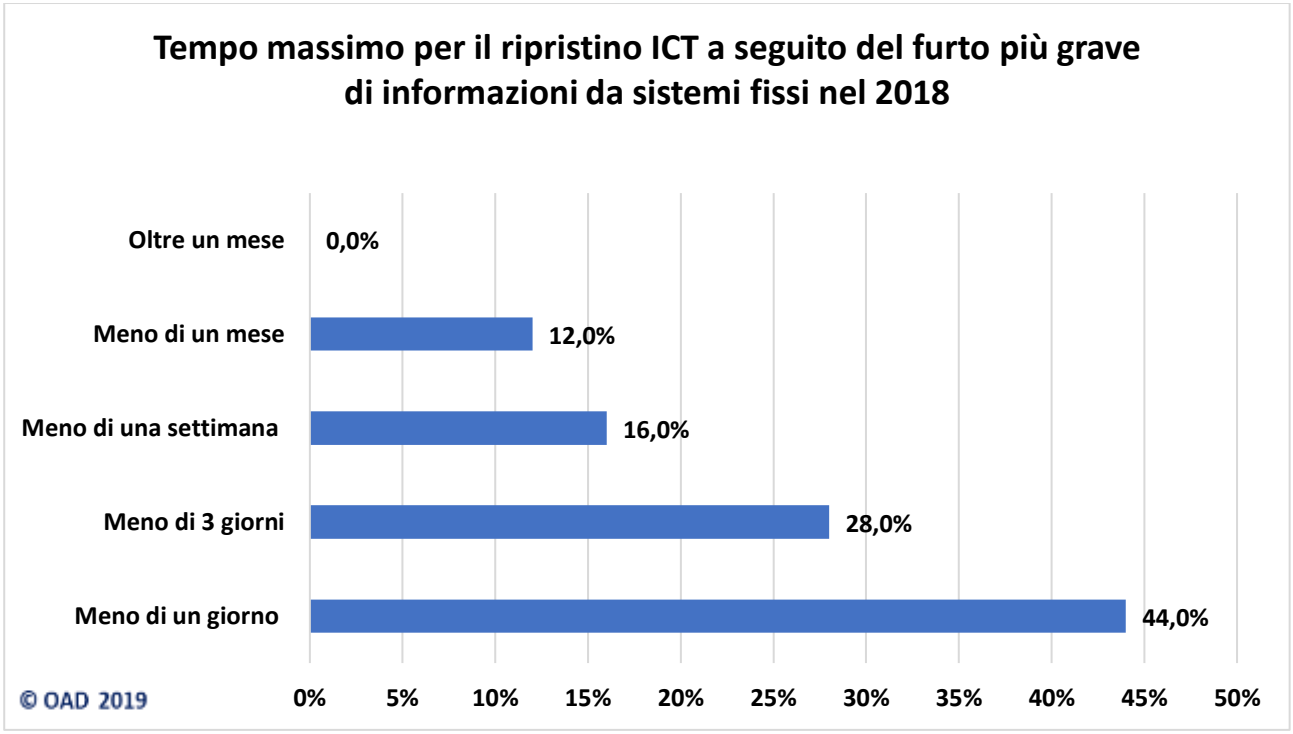

Fig. 6.4-5

6.5 Furto informazioni da sistemi ICT mobili

Con il termine di "sistemi ICT mobili" si intendono i vari dispositivi d'utente mobili, che includono tipicamente smartphone, tablet, i piccoli e leggeri laptop, le chiavette e gli hard disk removibili con interfaccia USB, che hanno raggiunto e stanno superando i 2 Tera Byte a prezzi ragionevoli, con dimensioni tascabili e senza alimentazione separata a supporto. Con una simile capacità di memoria e con dimensioni fisiche tali da poter essere occultati facilmente in una tasca, è veramente facile poter copiare interi file system da server, da piccole unità di storage, oltre che da singoli PC e workstation.

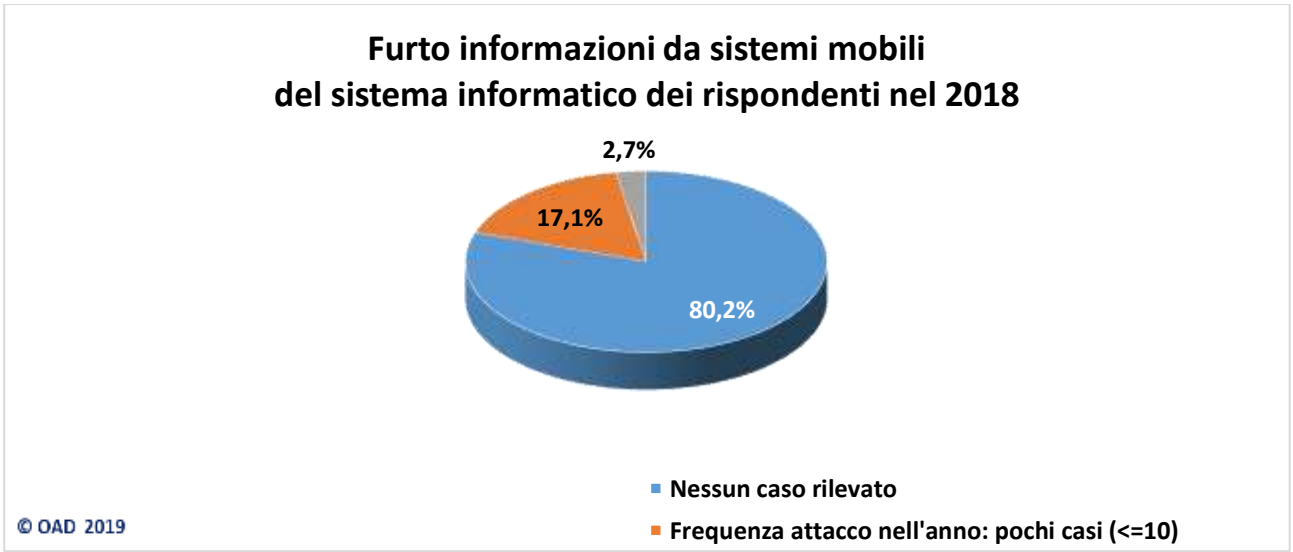

Fig. 6.5-1

Come mostrato nella fig. 6.5-1, poco meno del 20% dei rispondenti ha rilevato attacchi di questo tipo. Si deve considerare che il furto delle informazioni dai sistemi ICT mobili può avvenire sostanzialmente in due modi: o rubando il dispositivo, per poi cercare di carpire le informazioni contenute, oppure accendo al dispositivo ma senza sottrarlo. Il primo caso implica il furto dell'intero dispositivo mobile, considerato in §6.2: ed i dati emersi sono tra loro congruenti.

La fig. 6.5-2, con risposte multiple, evidenzia che la tecnica più diffusa, almeno nel caso dell'attacco più grave, è l'uso di script o di programmi maligni, cui segue il social engineering e l'uso di toolkit. L'attacco fisico, ossia il furto fisico del dispositivo mobile (18,2% dei rispondenti) è solo al quarto posto. Questo significa che gli attacchi, anche sui dispostivi mobili, sono in prevalenza logici ed effettuati con opportuni strumenti informatici. Infatti, se sui dispositivi mobili ci sono informazioni appetibili, essi sono protetti, con i dati anche crittati: così il semplice furto non consente di accedere alle informazioni che vi sono contenute; con opportuni script o malware, magari attivati via phishing, è ben più probabile raggiungere le informazioni contenute.

La fig. 6.5-3, con risposte multiple, evidenza come il 50% dei rispondenti che hanno subito tale attacco, non ha riscontrato impatti, o solo impatti irrilevanti. Ma una percentuale non trascurabile ha riscontrato impatti significativi anche sul business, a partire dalla perdita di immagine con un 22,7%.

Dalle possibili motivazioni in fig. 6.5-4, con risposte multiple, emerge al primo posto l'attuazione di ritorsioni/ricatti con il 40,9%. Le altre motivazioni seguono a scalare, con non grandi differenze percentuali.

La fig. 6.5-5 sul tempo massimo per il ripristino (nel caso più grave) conferma che la maggior parte di questi attacchi non ha avuto significativi impatti: più della metà dei rispondenti ha ripristinato il caso peggiore nella stessa giornata, e i ¾ entro 3 giorni.

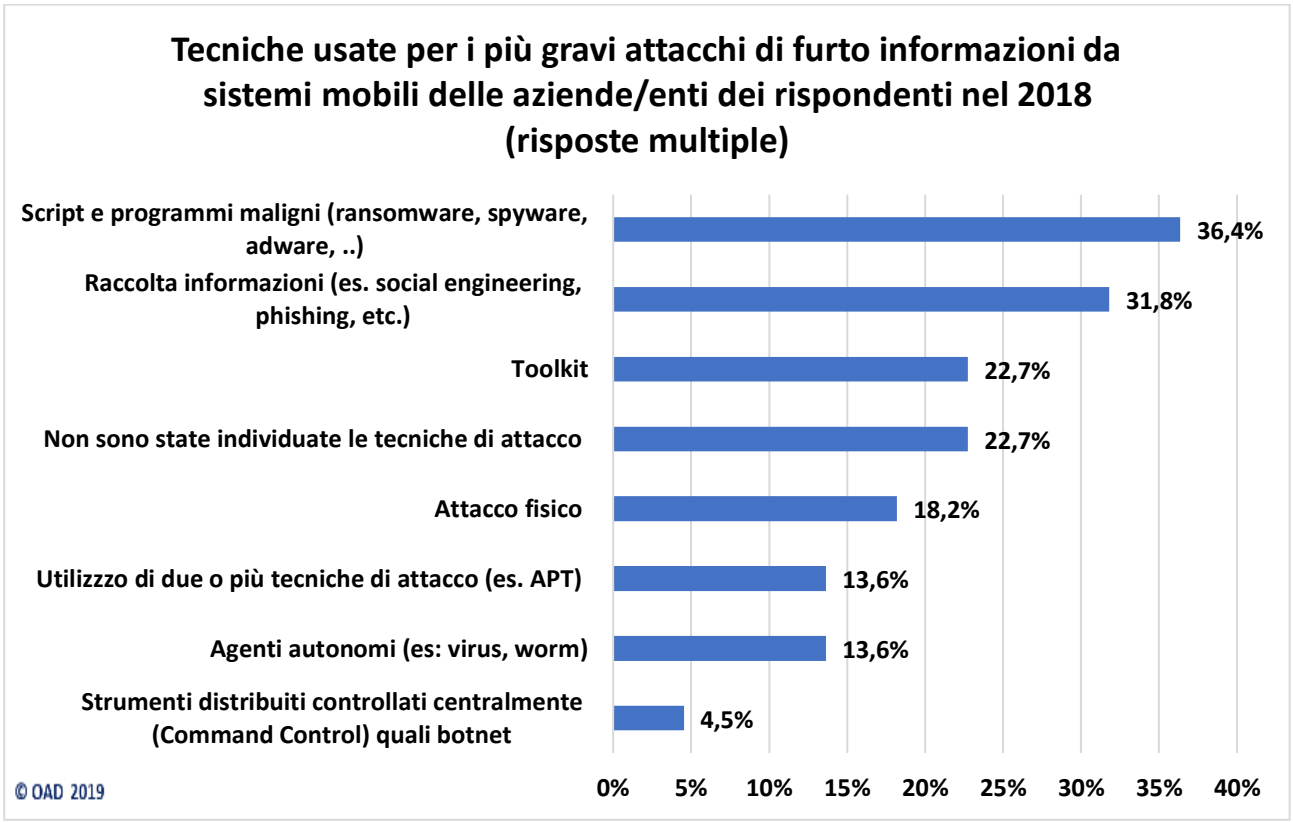

Fig. 6.5-2

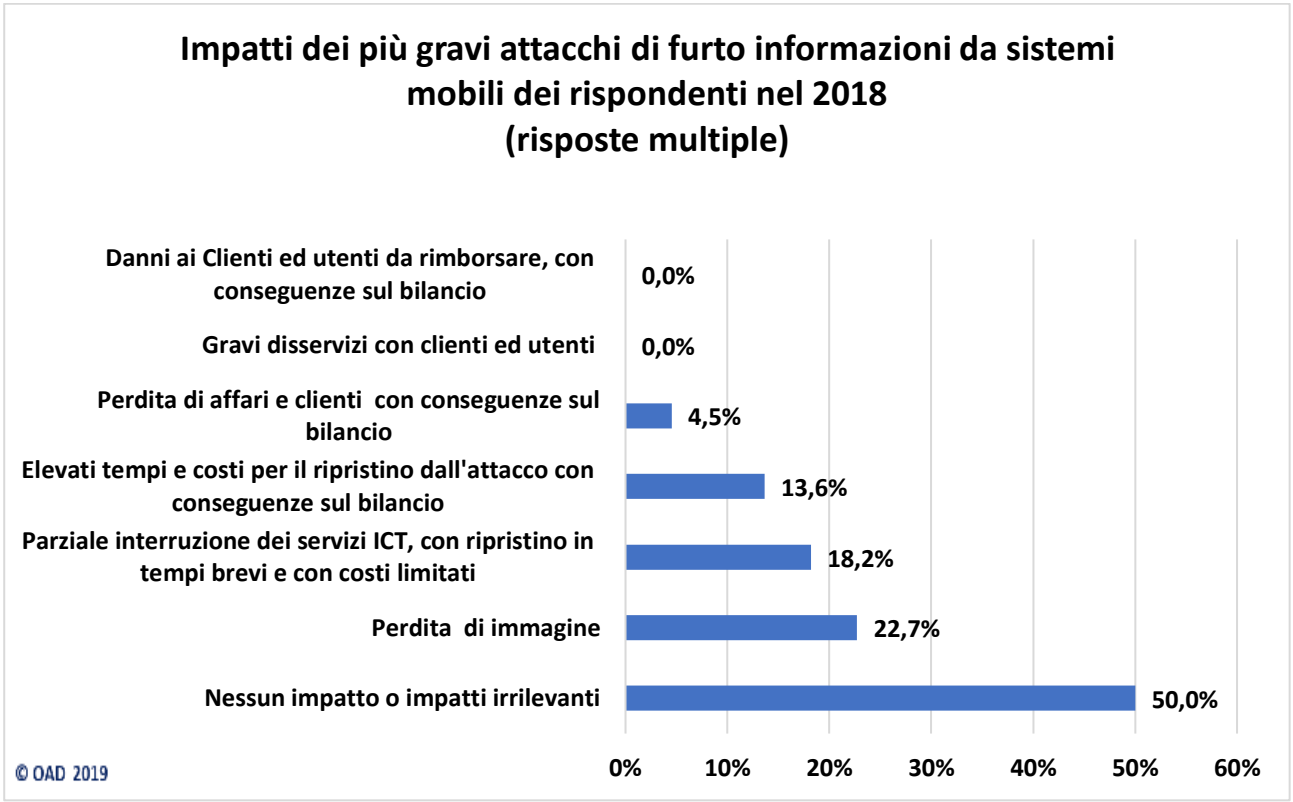

Fig. 6.5-3

Fig. 6.5-4

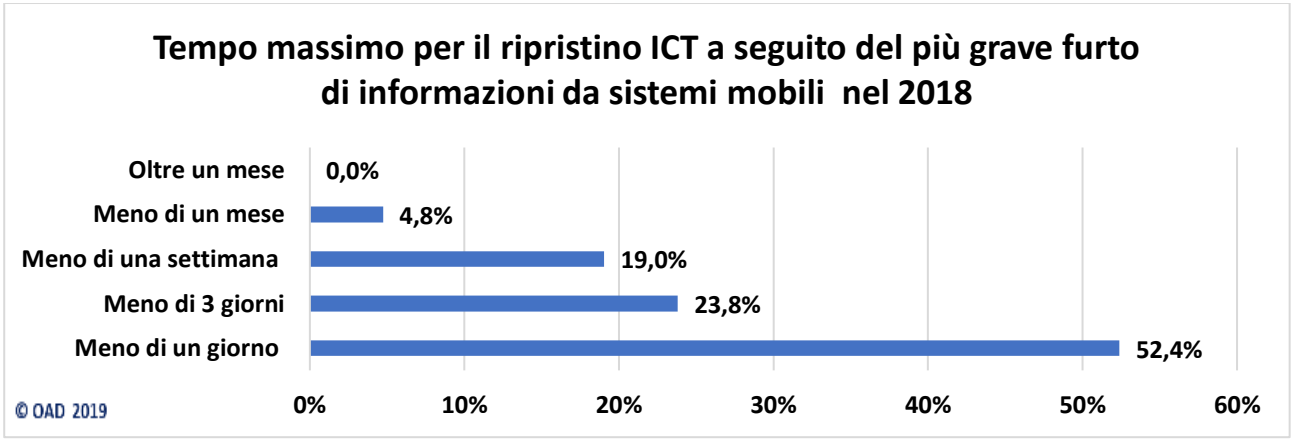

Fig. 6.5-5

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

Questa tipologia di attacco risulta la più diffusa tra i rispondenti nel 2018, come evidenziato in fig. 6-7. Questa tipologia di attacchi è alla base del furto dell'identità digitale sia a livello di utenti finali sia a livello degli utenti privilegiati, ossia dei vari livelli di amministratori e tecnici dei sistemi informatici interni all'organizzazione o di terze parti, quali consulenti, fornitori, manutentori, etc.
Riuscendo ad acquisire i diritti per accedere ad un sistema ICT, a seconda del livello di tali diritti, si possono poi compiere specifiche azioni malevole, dall'inserimento di malware e/o di bot all'uso non autorizzato di applicazioni, acquisendo informazioni e/o manipolandole o eleminandole.
Rubare l'identità digitale di una persona significa acquisire, in maniera illegale, uno o più dei suoi account per poi spacciarsi sui sistemi informatici dell'azienda/ente e su Internet per tale persona e in tal modo effettuare, ad esempio transazioni sui conti correnti, usare le sue carte di credito, entrare, con suoi diritti, nei sistemi aziendali ed accedere a informazioni riservate, e così via. L'acquisizione degli account degli utenti privilegiati consente di alterare, anche in maniera diffusa e grave, i sistemi informatici dell'azienda/ente e le informazioni da questi trattate. In taluni casi questo mascherarsi digitalmente non richiede abili social engineering o sofisticate tecniche; i dati per accedere all'account possono essere forniti dallo stesso utente, ad esempio quando richiede che un suo collega, di cui (erroneamente) si fida, lo sostituisca in qualche attività informatica. E' un atteggiamento abbastanza diffuso, ma estremamente rischioso e che dovrebbe essere evitato.
Nell'ambito generale del controllo degli accessi, si fa riferimento ai tre livelli gerarchici di identificazione, autenticazione e autorizzazione, indicati nel seguito con la sigla IAA.

La fig. 6.6-1 riporta l'alta percentuale di diffusione tra i rispondenti del 54,2% per gli attacchi IAA, nel 2018 in testa alla già citata classifica, e che come tendenza (non strettamente a livello statistico) ha un forte incremento rispetto al 39,39% del 2017 ed ancor più forte rispetto al 6,67% del 2016.
In §9.2 sono riportate le misure e le tecniche di sicurezza per IAA usate dai rispondenti, cui si rimanda per alcune specifiche considerazioni.
Se ben più della metà dei rispondenti subisce attacchi all'IAA significa che le misure in atto non sono sufficienti: numerose ricerche anche a livello internazionale, ma anche e soprattutto l'esperienza professionale sul campo dell'autore, evidenziano come le misure di base per IAA sono troppo spesso non o malamente attuate. Si pensi, solo per citare i più diffusi problemi nella realtà italiana, gli account non personali, le password troppo semplici, troppo corte e/o raramente cambiate, l'uso della stessa password per accedere a diversi sistemi informatici, il lasciare identificativi d'utente per gli amministratori di sistema di default, e così via

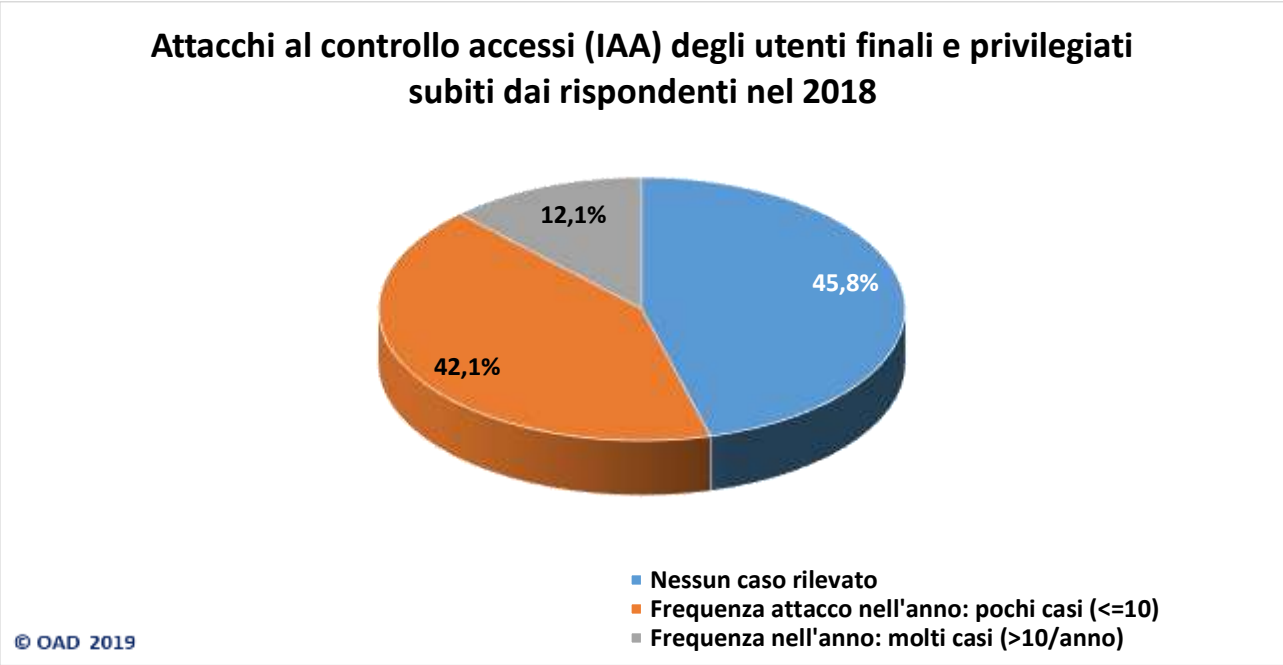

Fig. 6.6-1

Significativo che nel 54,21%, il 12,1% rappresenta attacchi ripetuti nell'anno per più di 10 volte: l'autore si sarebbe aspettato un valore ancora più alto, ma già questo indica come l'IAA sia considerato dagli attaccanti come uno dei primi sistemi di protezione da abbattere per poter effettuare le azioni illegali poste come target.

La fig. 6.6-2, con risposte multiple, mostra come la tecnica di attacco più diffusa tra i rispondenti sia il social engineering per il 65,5% dei rispondenti, cui segue l'uso di script e di codici maligni, con un 44,8%. Queste due tecniche nettamente staccano, come percentuali, tutte le altre. Abbastanza alto, ma credibile e ragionevole, il 15,5% di rispondenti che non sono stati in grado di capire /ipotizzare le tecniche usate nell'attacco IAA rilevato.

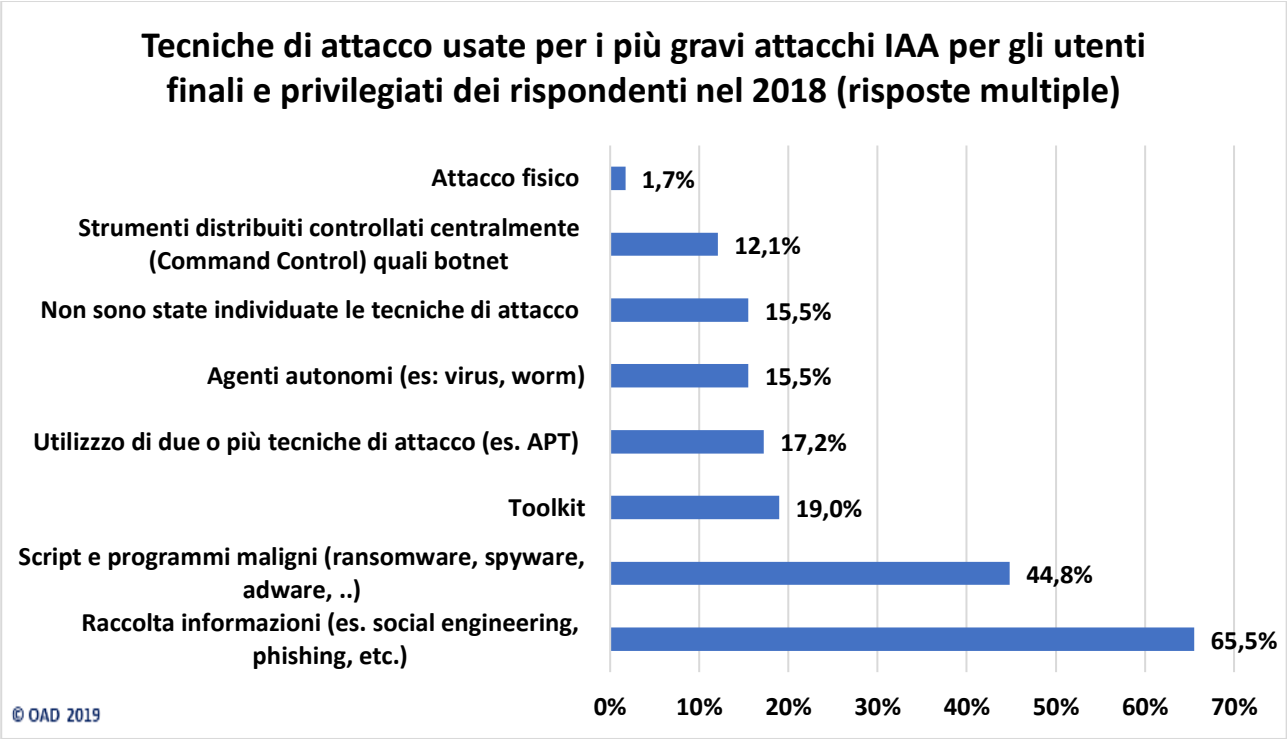

Fig. 6.6-2

La fig. 6.6-3, con risposte multiple, mostra che nella maggioranza dei casi gli impatti riscontrati sono stati irrilevanti o comunque risolti in breve tempo ed a costi limitati. Tutti gli altri impatti gravi hanno percentuali molto più basse.
Nella voce "altro" alcuni rispondenti hanno dettagliato aspetti specifici sugli impatti rilevati (si rammenta che la domanda consentiva risposte multiple) ed appartenenti alle altre voci predefinite: ad esempio che il re settaggio degli account ha richiesto tempi ben più lunghi rispetto al normale, che è stato necessario attivare una nuova più stringente procedura organizzativa che regoli l'IAA, che la gestione e la correlazione dei log degli utenti privilegiati ha richiesto tempi e costi significativi, etc.

Le principali possibili motivazioni indicate, con risposte multiple, in fig. 6.6-4, evidenziano al primo posto la frode, cui segue l'utilizzo di queste informazioni per altri attacchi e, con maggior distacco, la ritorsione/ricatto. Nella voce "Altro" alcuni rispondenti hanno specificato che un'ulteriore motivazione è stata "l'ignoranza" degli utenti e l'acquisizione di informazioni (senza specificare per farne che cosa).

Come indicato in fig. 6.6-5, quasi la metà dei rispondenti è riuscita a ripristinare il sistema IAA attaccato in un solo giorno, e la quasi totalità, 94,3% entro una settimana. Tali dati confermano quanto indicato nella fig. 6.6-3: nella grande maggioranza dei casi gli impatti riscontrati sono stati irrilevanti o comunque risolti in breve tempo.

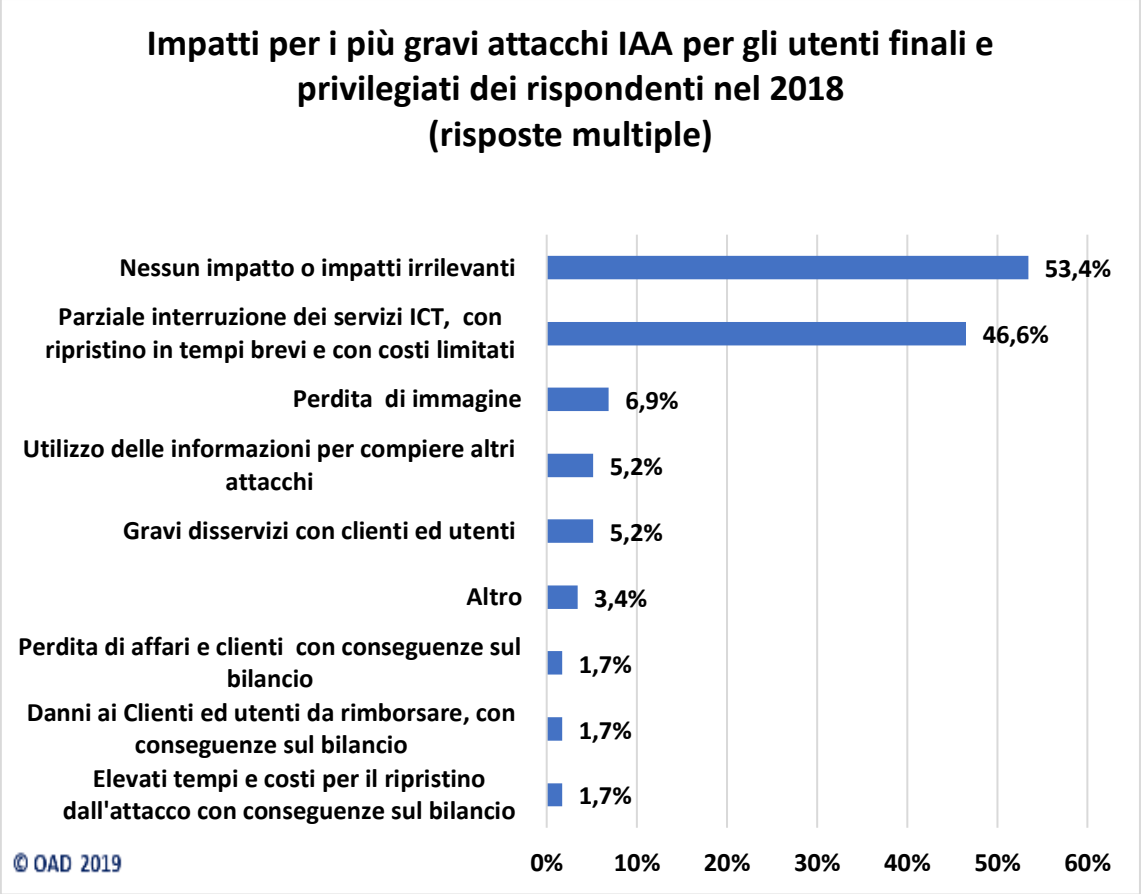
Impatti per i più gravi attacchi IAA per gli utenti finali e privilegiati dei rispondenti nel 2018 (risposte multiple)
Nessun impatto o impatti irrilevanti
53,4%
Parziale interruzione dei servizi ICT, con ripristino in tempi brevi e con costi limitati
46,6%
Perdita di immagine
6,9%
Utilizzo delle informazioni per compiere altri attacchi
5,2%
Gravi disservizi con clienti ed utenti
5,2%
Altro
3,4%
Perdita di affari e clienti con conseguenze sul bilancio
1,7%
Danni ai Clienti ed utenti da rimborsare, con conseguenze sul bilancio
1,7%
Elevati tempi e costi per il ripristino dall'attacco con conseguenze sul bilancio
1,7%
© OAD 2019
0%
10%
20%
30%
40%
50%
60%

Fig. 6.6-3

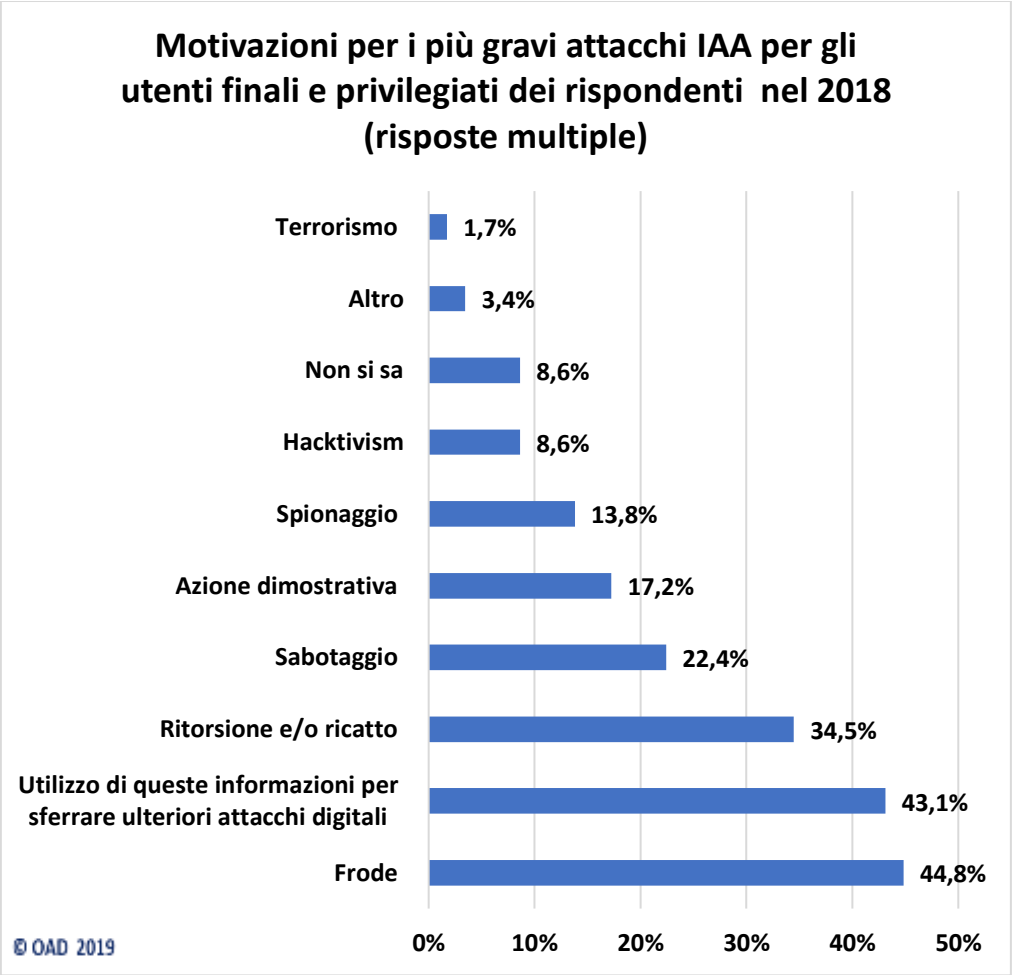

Fig. 6.6-4

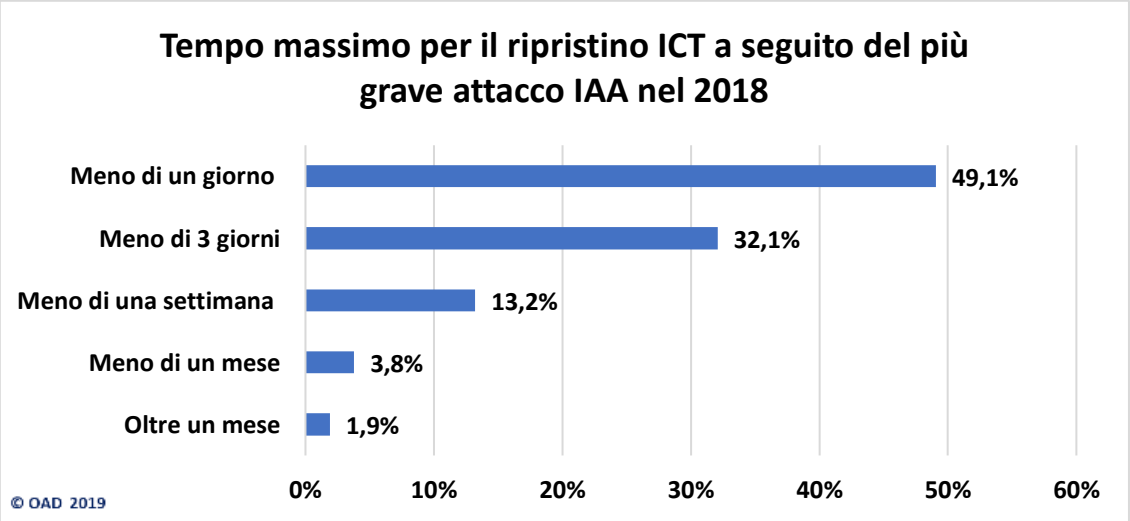

Fig. 6.6-5

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

In questa tipologia, gli attacchi si differenziano significativamente, sia come obiettivo che come modalità d'attacco, in funzione del tipo di rete e dei protocolli usati: reti geografiche e reti locali, reti fisse e senza fili (wireless). Queste ultime, sia locali (WLAN, WiFi) che geografiche per la telefonia mobile[15], sono quelle che consentono la mobilità sia del lavoro che degli usi personali/domestici e di intrattenimento. Sono quelle più cresciute negli ultimi anni, e che hanno portato a nuovi tipi di vulnerabilità, rischi e possibili attacchi. Data la complessità tecnica del moderno mondo delle telecomunicazioni e delle reti, volutamente il questionario 2019 OAD ha raggruppato in un'unica tipologia l'ampia e diversificata famiglia degli attacchi alle reti, che costituiscono uno dei punti di ingresso al sistema informatico sia per specifici attacchi alle reti, sia, soprattutto, per ulteriori e più mirati attacchi digitali ai sistemi ICT e alle loro applicazioni ed informazioni. Tali attacchi includono modifiche al routing per l'instradamento del traffico, le modifiche ai DNS che modificano il nome della risorsa ICT associata all'indirizzo IP, l'attacco al DHCP, lo sniffing del traffico, la saturazione della rete per un attacco DoS/DDoS che ha come obbiettivo un'applicazione web me che satura la connessione della rete al server che supporta l'applicazione attacca (si veda §6.11), e così via.
Negli ultimi anni, come hanno rilevato anche vari rapporti internazionali, gli attacchi ai DNS sono aumentati significativamente e si sono differenziati non solo per rindirizzare il traffico destinato ai server, ad esempi o dirottandolo su un server dell'attaccante, ma anche per sferrare attacchi DoS/DDoS.

La fig. 6.7-1 mostra che il 34,7% dei rispondenti ha rilevato attacchi di reti nel 2018, ponendo questa tipologia di attacco, come diffusione, al terzo posto (si veda fig. 6-7). Si ricorda che nel 2016 questa tipologia d'attacchi è risultata al primo posto per diffusione tra gli attacchi digitali, nel bacino dei rispondenti di OAD 2018.

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

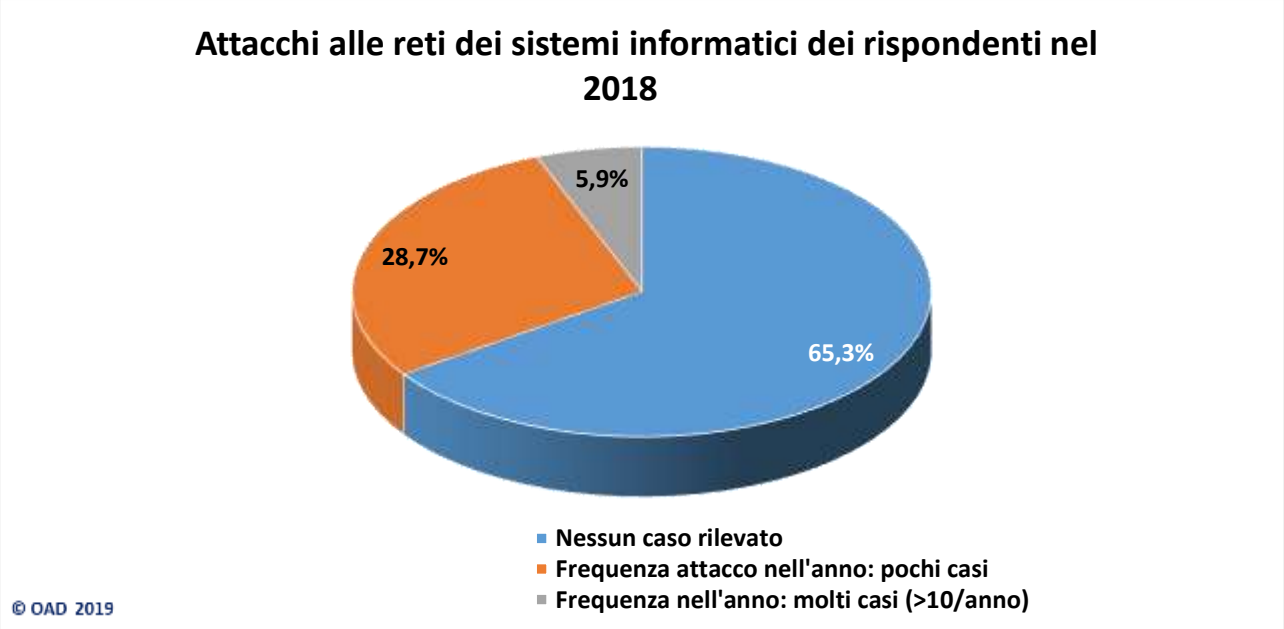

Fig. 6.7-1

La fig. 6.7-2 evidenzia, con risposte multiple, che la tecnica di attacco più usata per questa tipologia è stata la raccolta di informazioni, tipicamente con il social engineering. Al secondo posto, si è posizionato l'attacco fisico: probabilmente questo significa la sostituzione o la diretta manipolazione, da parte dell'attaccante, di uno o più dispositivi di rete: si pensi ad esempio, al cambio delle posizioni nelle porte degli switch e dei router. Al terzo posto l'uso di script e codici maligni. Seguono a scalare le altre tecniche di attacco. Interessante sottolineare come l'uso di più tecniche di attacco sia all'ultimo posto: questo significa, almeno per il campione dei rispondenti, che normalmente viene usato una sola tecnica per un attacco diretto a reti e DNS.

La fig. 6.7-3 mostra, con risposte multiple, gli impatti causati dai più gravi attacchi alle reti: la maggior parte dei rispondenti che hanno subito tali attacchi non hanno avuto impatti, o sono stati trascurabili, ed anche se hanno avuto una momentanea interruzione dei servizi ICT erogati, essi sono stati ripristinati in breve tempo e con bassi costi. Il restante 1/3 ha subito danni ben più gravi, ma che non hanno causato perdita di clienti o danni per questi ultimi da rimborsare.

La fig. 6.7-4 mostra, con risposte multiple, le possibili motivazioni, almeno per i più gravi attacchi alle reti: per il 23% dei rispondenti che hanno subito tali attacchi il poter accedere così ad altre risorse ICT più critiche. Seguono a scalare le altre possibili motivazioni. Nessuno ha stimato motivazioni di terrorismo cibernetico. Con "Altro" alcuni rispondenti hanno precisato che l'attacco alle loro reti faceva parte di un attacco su larga scala che aveva come target varie sistemi informatici di diverse organizzazioni.

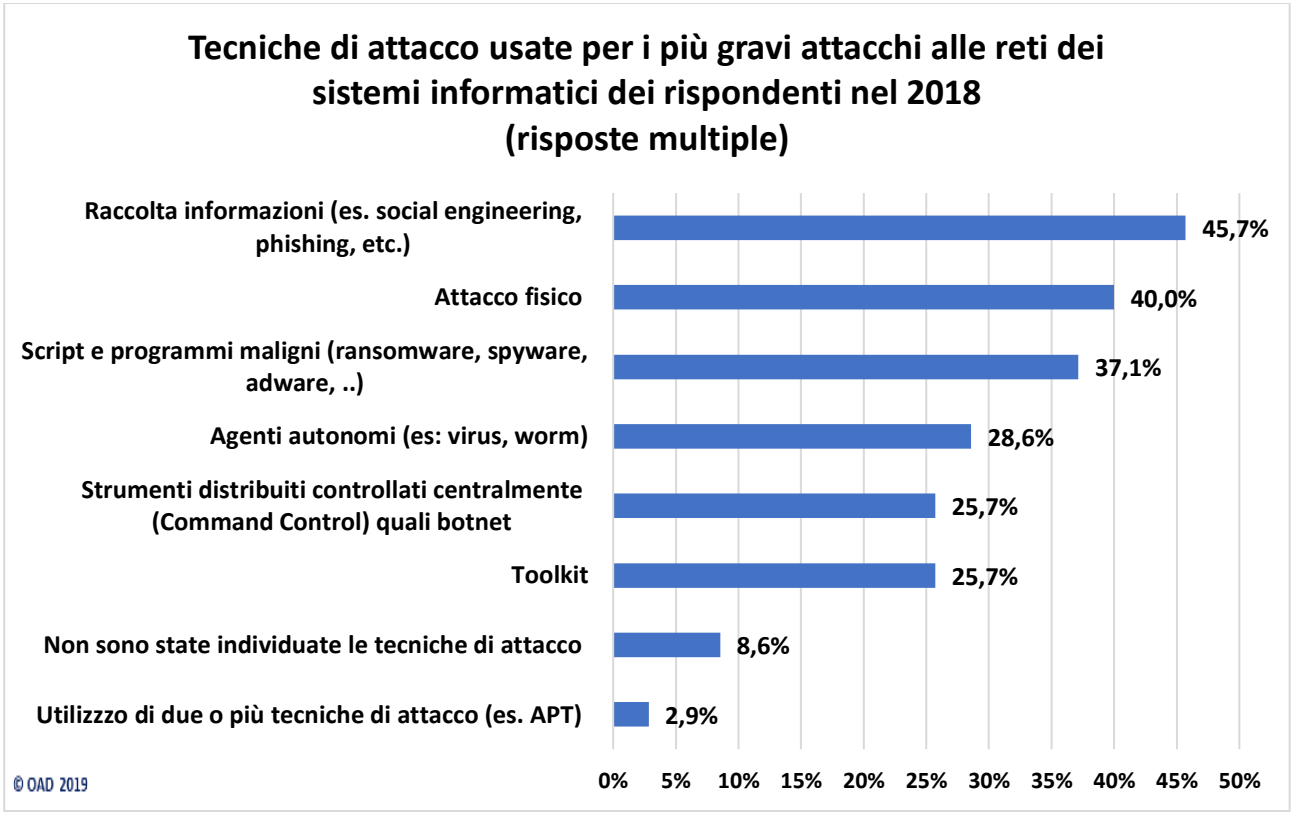

Fig. 6.7-2

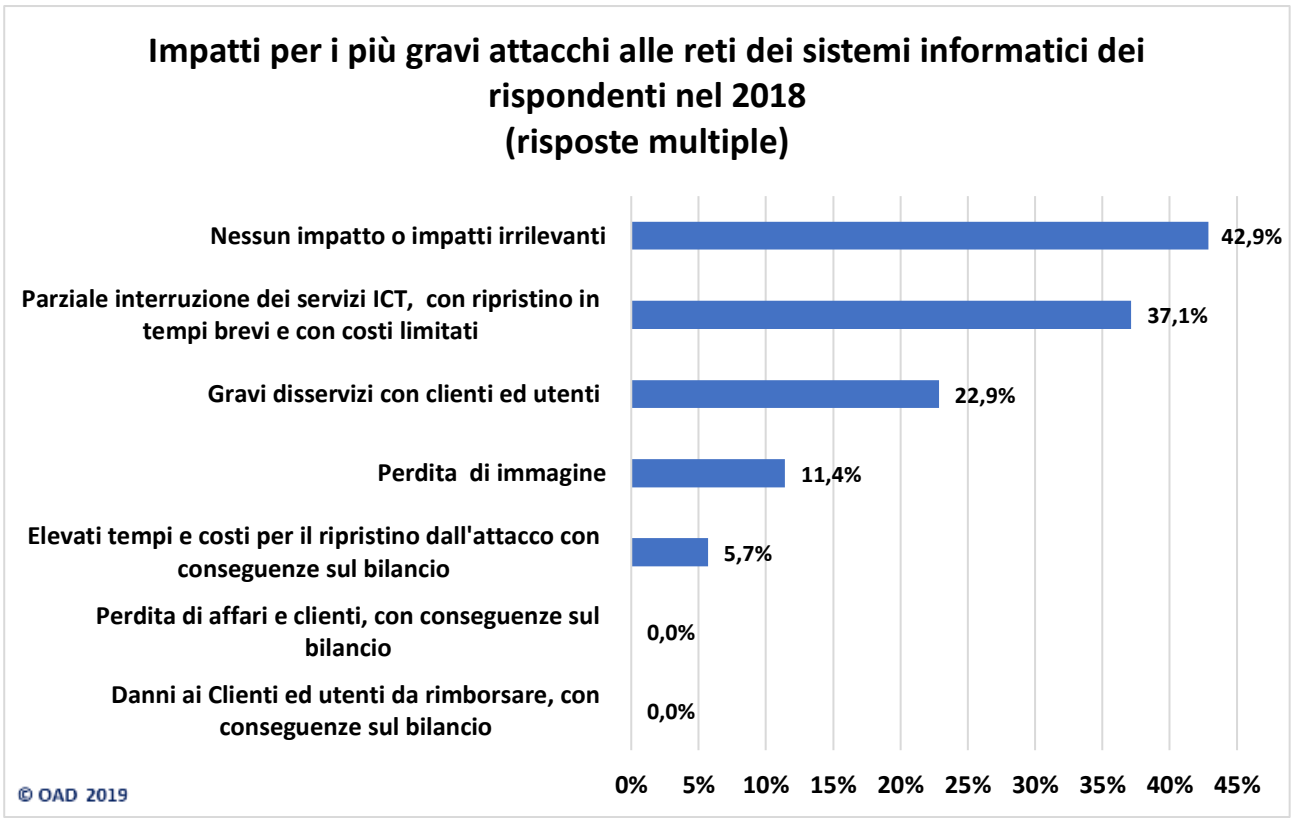

Fig. 6.7-3

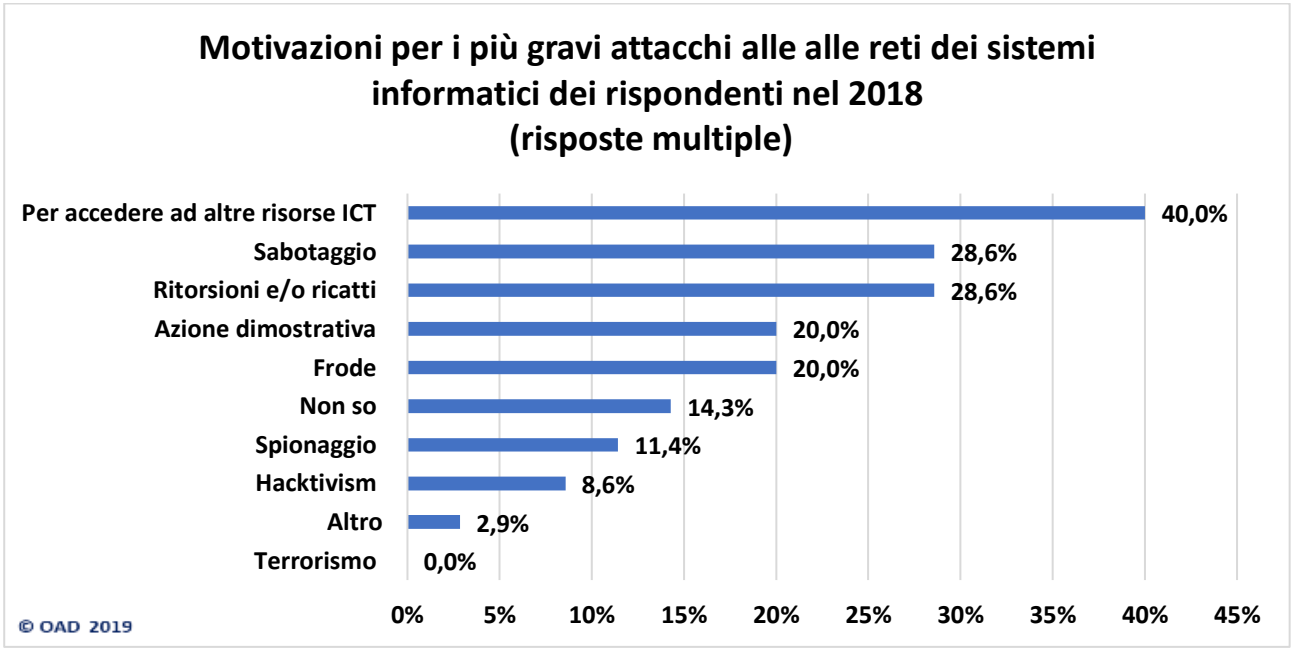

Fig. 6.7-4

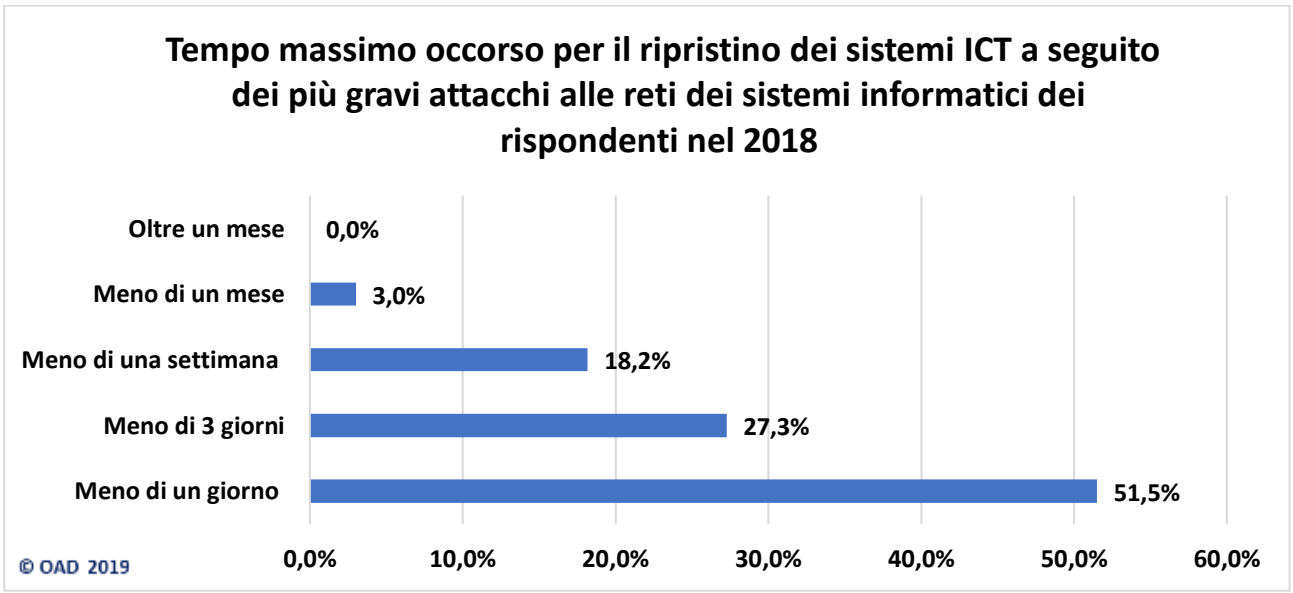

Fig. 6.7-5

Più della metà dei rispondenti ripristina la situazione ex ante in giornata, come mostrato in fig. 6.7-5: questo implica che i rispondenti sono dotati di efficaci strumenti di rilevazione in tempo quasi reale dell'attacco, e sono in grado di rispondere tempestivamente. Più dei 2/3 ripristina entro 3 giorni, e tra i rispondenti non viene superato il mese.

.

6.8 Uso non autorizzato sistemi ICT nel loro complesso

L'uso non autorizzato, di risorse ICT nel loro complesso, sia di quelli gestite internamente, on premise, sia di quelle in hosting/housing/cloud, nel 2018 si posiziona al secondo posto per diffusione tra i rispondenti, come già evidenziato nella classifica per diffusione delle tipologie di attacco in fig. 6-7. Tale ampia diffusione ha una sua logica, dato che questa tipologia di attacco è alla base di ogni attacco al software di base, agli applicativi, alle informazioni da loro trattate, ai sistemi di storage.

La fig. 6.8-1 dettaglia che il significativo 41% di questa tipologia d'attacco ha avuto poche frequenti ripetizioni tra i rispondenti, solo l'1% per più di 10 ripetizione nell'anno.
Questa percentuale di diffusione è più che raddoppiata (sempre in termini di tendenza, non statistici) rispetto a circa il 20% del 2017 e quasi quadruplicato rispetto al 11,79% del 2016 (si veda il §6.7 del Rapporto 2018 OAD).

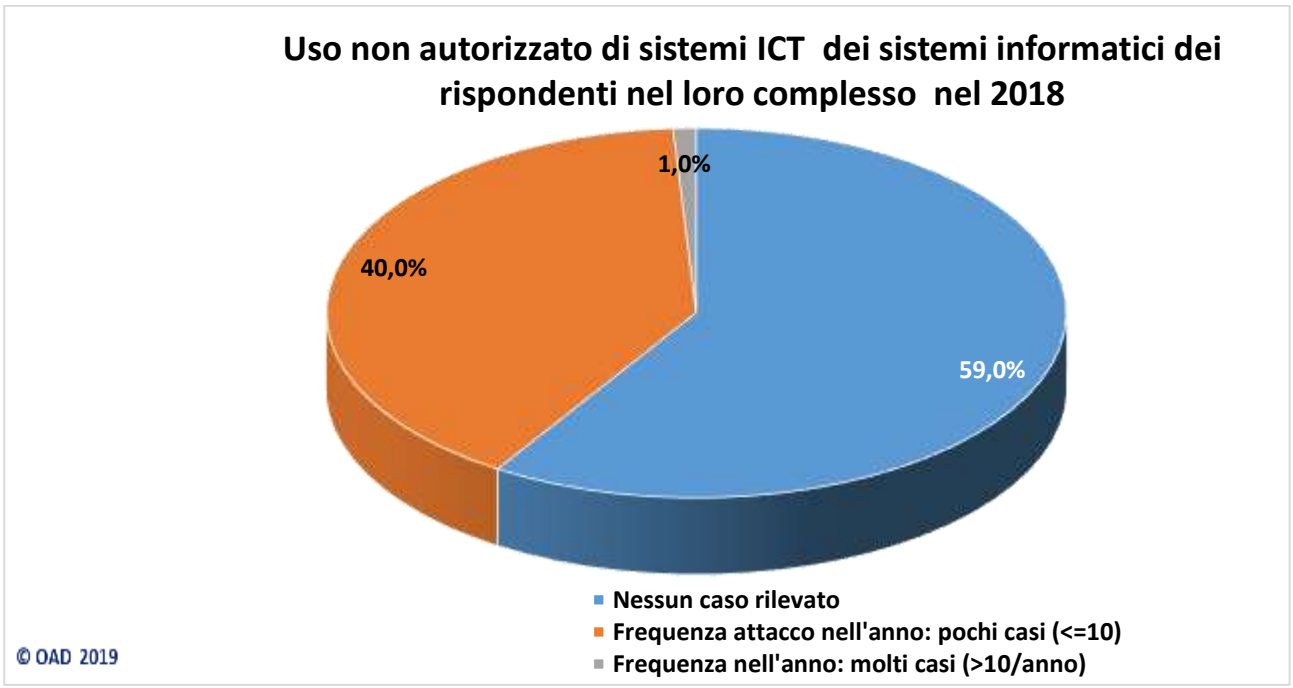

Fig. 6.8-1

La fig. 6.8-2, con risposte multiple, elenca le tecniche di attacco usate (tenendo conto delle risposte multiple dei rispondenti) per gli attacchi ai sistemi ICT nel loro complesso: anche per questa tipologia le tecniche più usate includono script e malware per più della metà dei rispondenti (53,7%) cui segue a breve distanza la cattura illecita di informazioni (48,8%); le altre tecniche seguono a scalare.

La fig. 6.8-3 evidenzia, con risposte multiple, che questa tipologia d'attacco ha causato in percentuale più danni che non danni o danni irrilevanti. Il 36,6% dei rispondenti lamenta come conseguenza la perdita di affari, cui si aggiunge la perdita d'immagine per il 24,4%, lunghi e costosi tempi di ripristino per il 22%, danni ai clienti per 4,9%. Non danni o danni irrilevanti per il 31,7%, e ripristini in brevi tempi e bassi costi per il 7,3%.

La fig. 6.8-4, con risposte multiple, mostra le probabili motivazioni degli attaccanti: ai primi tre posti, a scalare tra loro di circa 5 punti percentuali, il sabotaggio, le frodi, la base per altri attacchi.

La gravità di questo tipo di attacco per i rispondenti è confermata dai tempi massimi di ripristino per il più grave di questi attacchi subiti, mostrati in fig. 6.8-5: solo la metà dei rispondenti ha ripristinato i sistemi ICT entro i 3 giorni, e per un 5% è stato necessario più di un mese.

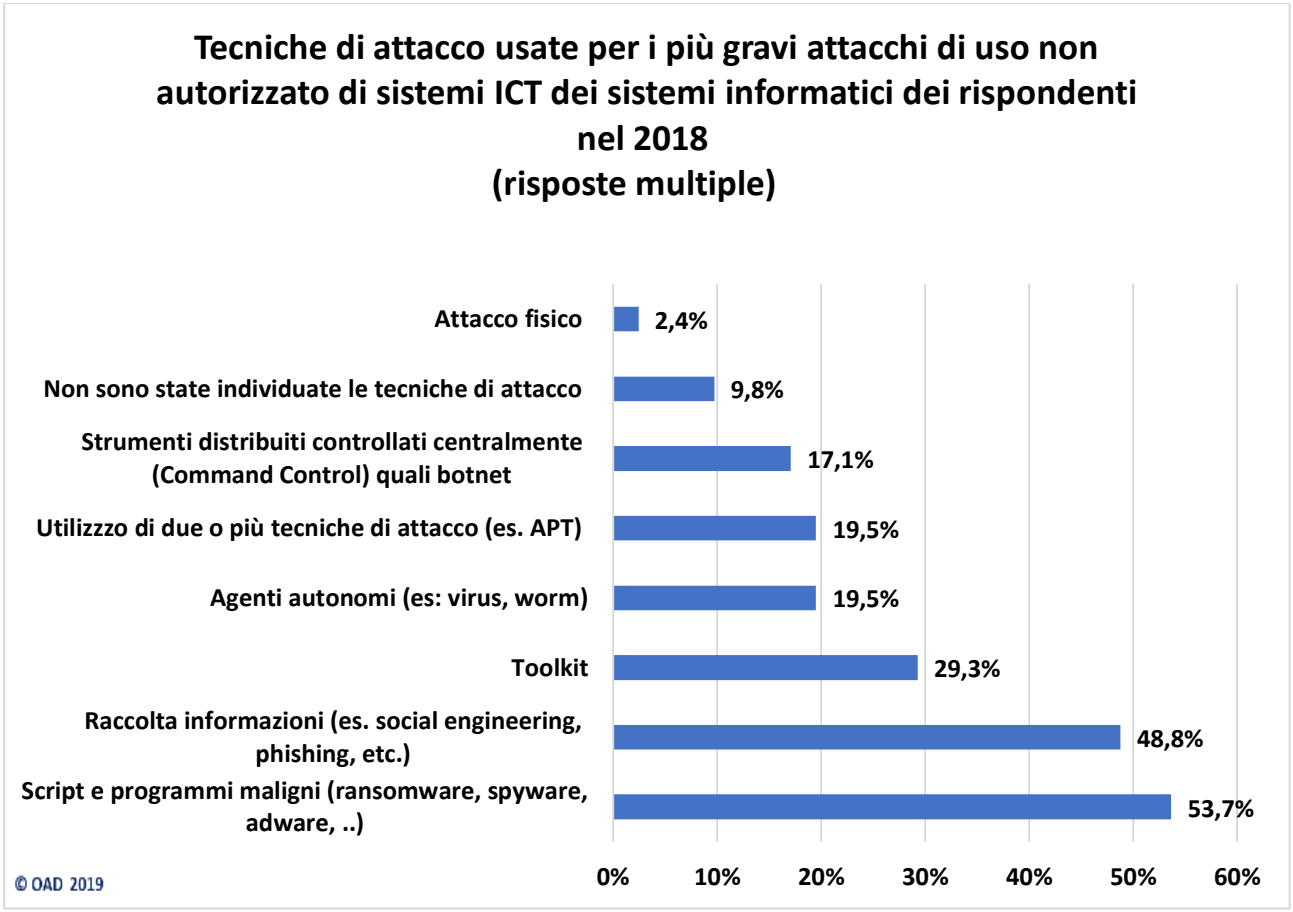
Tecniche di attacco usate per i più gravi attacchi di uso non autorizzato di sistemi ICT dei sistemi informatici dei rispondenti nel 2018
(risposte multiple)
Attacco fisico
2,4%
Non sono state individuate le tecniche di attacco
9,8%
Strumenti distribuiti controllati centralmente (Command Control) quali botnet
17,1%
Utilizzzo di due o più tecniche di attacco (es. APT)
19,5%
Agenti autonomi (es: virus, worm)
19,5%
Toolkit
29,3%
Raccolta informazioni (es. social engineering, phishing, etc.)
48,8%
Script e programmi maligni (ransomware, spyware, adware, ..)
53,7%
0%
10%
20%
30%
40%
50%
60%
© OAD 2019

Fig. 6.8-2

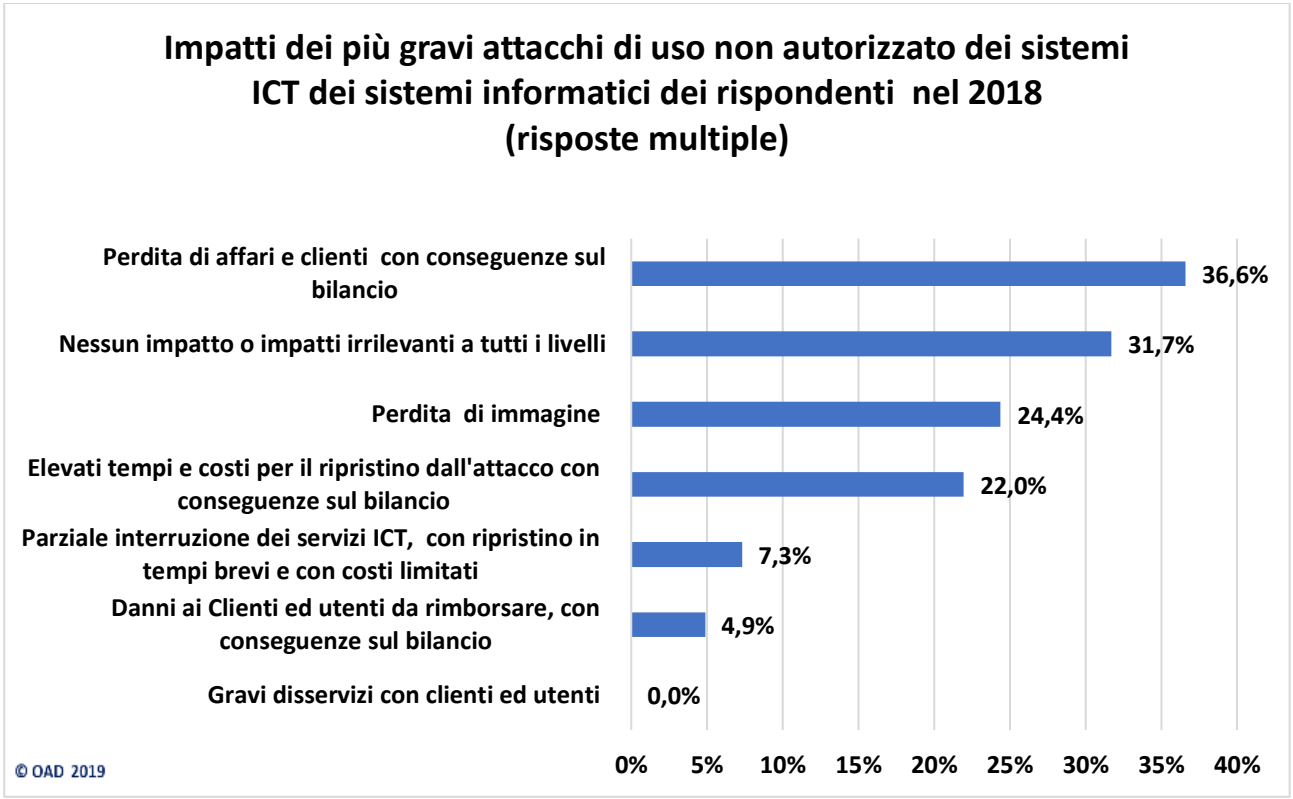
Impatti dei più gravi attacchi di uso non autorizzato dei sistemi ICT dei sistemi informatici dei rispondenti nel 2018 (risposte multiple)
Perdita di affari e clienti con conseguenze sul bilancio
36,6%
Nessun impatto o impatti irrilevanti a tutti i livelli
31,7%
Perdita di immagine
24,4%
Elevati tempi e costi per il ripristino dall'attacco con conseguenze sul bilancio
22,0%
Parziale interruzione dei servizi ICT, con ripristino in tempi brevi e con costi limitati
7,3%
Danni ai Clienti ed utenti da rimborsare, con conseguenze sul bilancio
4,9%
Gravi disservizi con clienti ed utenti
0,0%
0% 5% 10% 15% 20% 25% 30% 35% 40%
© OAD 2019

Fig. 6.8-3

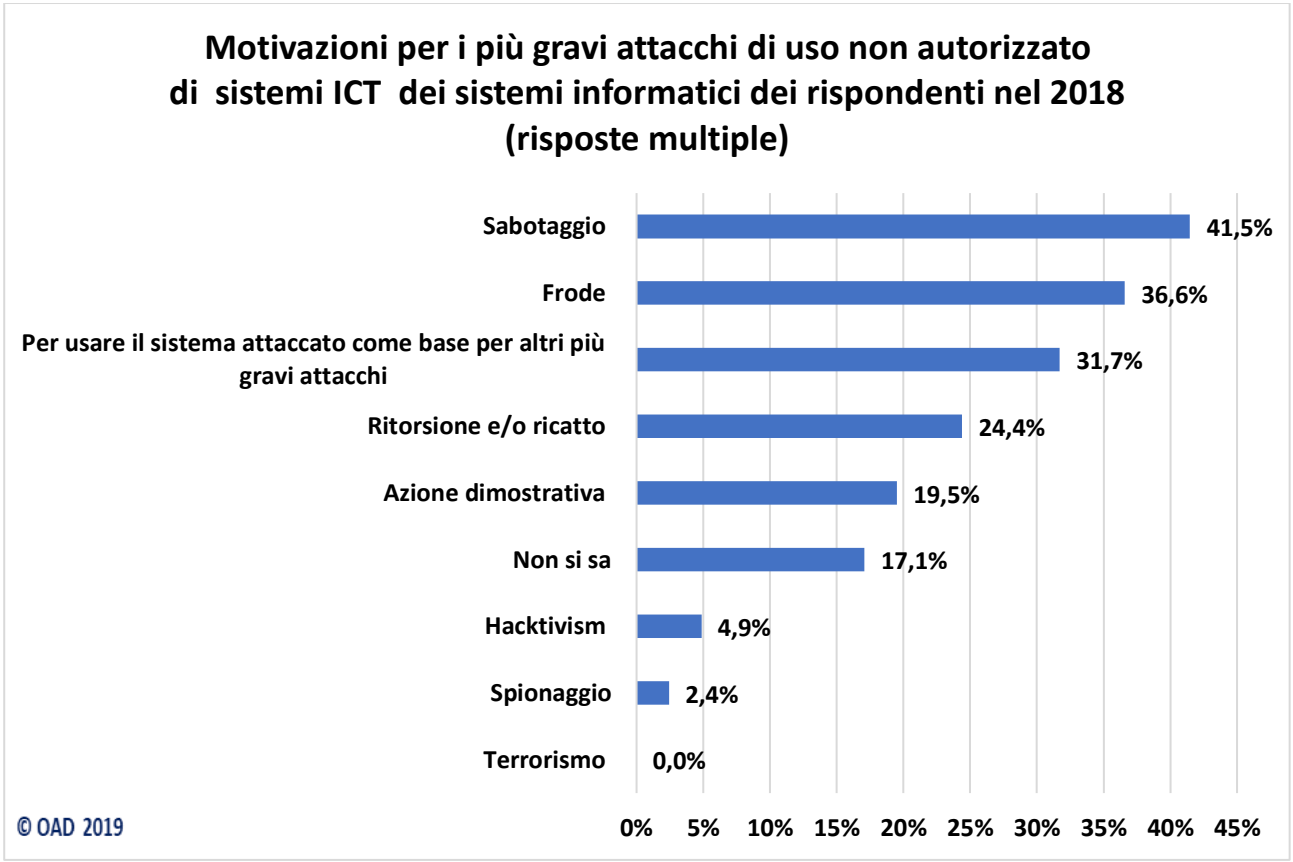

Fig. 6.8-4

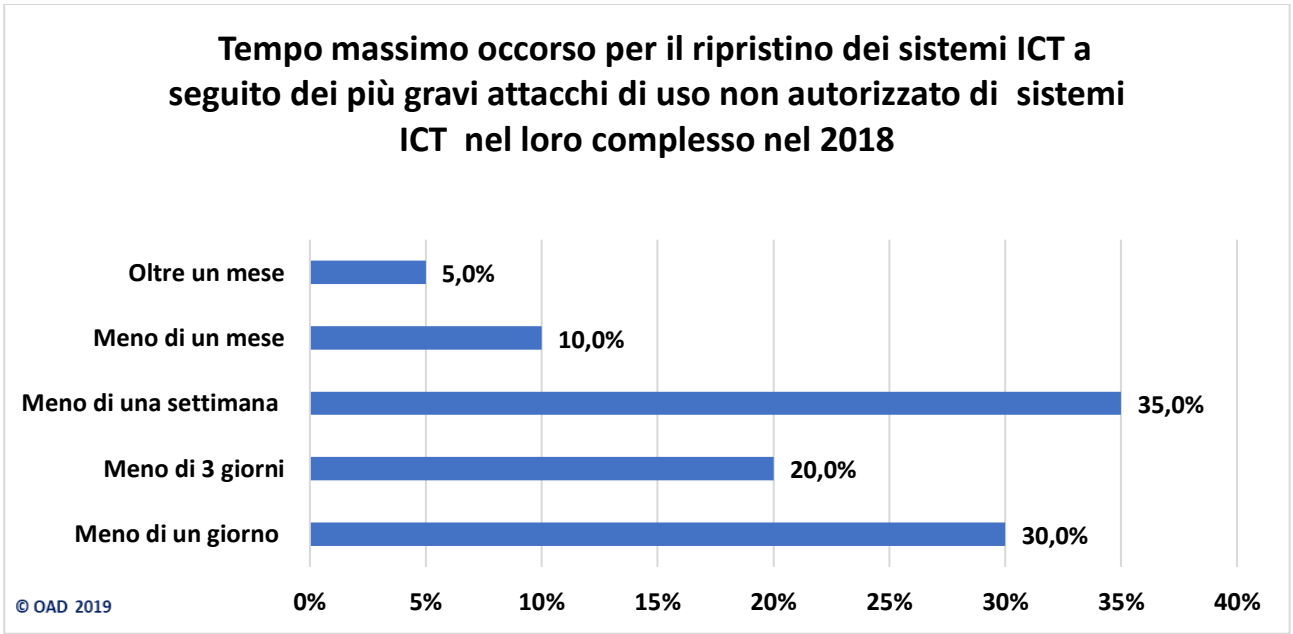

Fig. 6.8-5

6.9 Modifiche non autorizzate ai programmi applicativi e alle loro configurazioni

Per effettuare attacchi di questo tipo, che nella classifica di cui alla fig. 6-7 si posizionano all'undicesimo posto con un 16,33%, occorre di solito accedere illegalmente, mascherandosi da utente privilegiato, o, ancor più difficile su sistemi minimamente protetti, bypassando i vari controlli degli accessi; e come anticipato nel paragrafo precedente, occorre comunque utilizzare, non autorizzati, l'intero sistema ICT che si sta attaccando.
Nel 2017 OAD aveva effettuato una indagine solo e specificamente sugli attacchi agli applicativi, e si rimanda al rapporto elaborato, scaricabile dal sito di OAD, le cui considerazioni di fondo valgono ancora.

La fig. 6.9.1 mostra come il 16,3% dei rispondenti ha subito e rilevato nel 2018 questo tipo di attacchi, che sono stati sempre inferiori alle 10 ripetizioni.
La criticità riscontrata su questa tipologia di attacco è confermata dalle successive figure.

Fig. 6.9-1

Le tecniche più usate per condurre questi attacchi, secondo i rispondenti che li hanno subiti, sono riportate nella fig. 6.9-2, con risposte multiple, ed evidenziano al primo posto, come diffusione percentuale, script e malware, con un notevole 62,5%, cui segue, a notevole distanza percentuale, la raccolta illegittima di informazioni, e poi a decrescere l'uso di toolkit per individuare e sfruttare le vulnerabilità software, e le altre tecniche. Giustamente, non esiste attacco fisico: e questa indicazione conferma la sostanziale correttezza delle risposte raccolte.

Pur essendo questi attacchi gravi e assai rischiosi, più di 1/3 dei rispondenti dichiara di non aver avuto impatti, o impatti irrilevanti, o comunque risolvibili in breve tempo e con costi assai ridotti, come dettagliato, con risposte multiple, nella fig. 6.9-3. Gravi disservizi e perdita di immagine impattano comunque, con identica percentuale, un non piccolo 18,8%, e al 6,5% gli elevati tempi e costi per il ripristino dopo questo tipo d'attacco. Interessante notare che non sono stati considerati dai rispondenti come impatti per questo tipo d'attacco l'utilizzo dei sistemi compromessi per attuare altri attacchi, la perdita di clienti, danni ai clienti ed utenti da rimborsare.

La fig. 6.9-4, con risposte multiple, mostra le probabili motivazioni degli attaccanti: al primo posto, con un elevato 62,8%, la frode, cui segue con quasi 20 punti percentuali di distacco la ritorsione/ricatto e con il 31,3% il sabotaggio. Non trascurabile, ma comprensibile, che ¼ dei rispondenti non immagini le motivazioni per gli attacchi di questo tipo subiti.

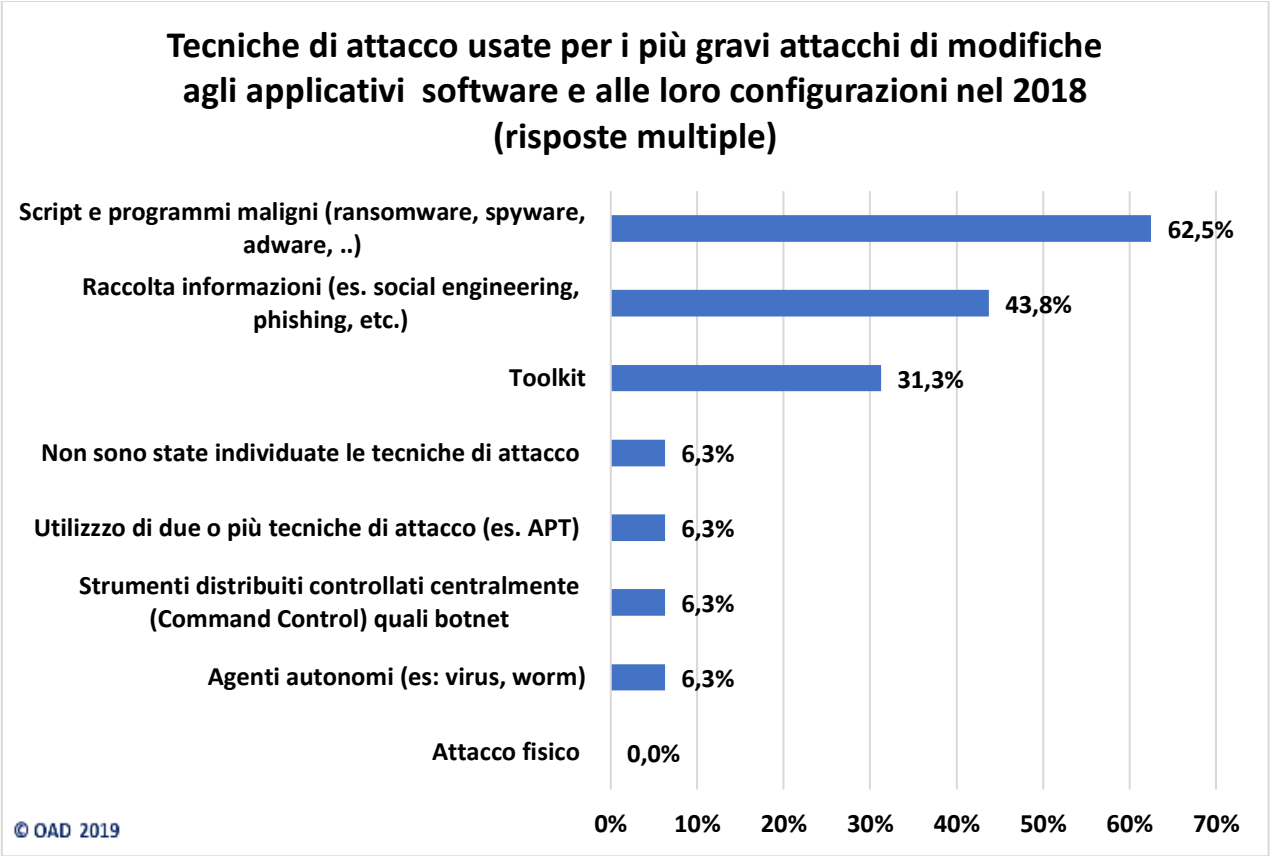
Tecniche di attacco usate per i più gravi attacchi di modifiche agli applicativi software e alle loro configurazioni nel 2018 (risposte multiple)
Script e programmi maligni (ransomware, spyware, adware, ..)
62,5%
Raccolta informazioni (es. social engineering, phishing, etc.)
43,8%
Toolkit
31,3%
Non sono state individuate le tecniche di attacco
6,3%
Utilizzzo di due o più tecniche di attacco (es. APT)
6,3%
Strumenti distribuiti controllati centralmente (Command Control) quali botnet
6,3%
Agenti autonomi (es: virus, worm)
6,3%
Attacco fisico
0,0%
0%
10%
20%
30%
40%
50%
60%
70%
© OAD 2019

Fig. 6.9-2

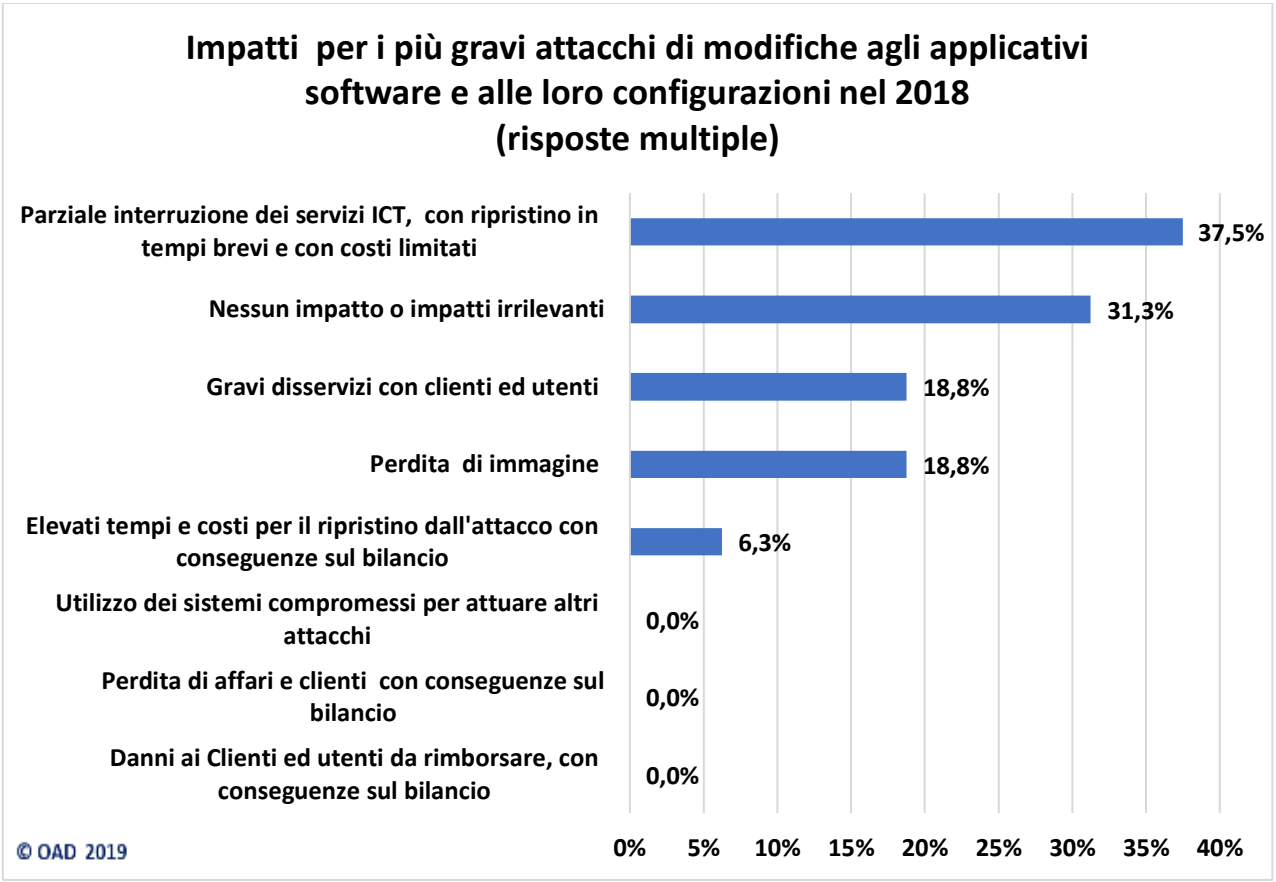

Fig. 6.9-3

La gravità di questo tipo di attacco è in parte confermata dai tempi massimi di ripristino nel caso peggiore di questo tipo d'attacco, come mostrato in fig. 6.9-5: in giornata solo il 37,5% dei rispondenti riesce a ripristinare, e la medesima percentuale tra 3 giorni ed una settimana. Il 93,8% dei rispondenti riesce a ripristinare entro una settimana. Nessun caso che richieda più di un mese.

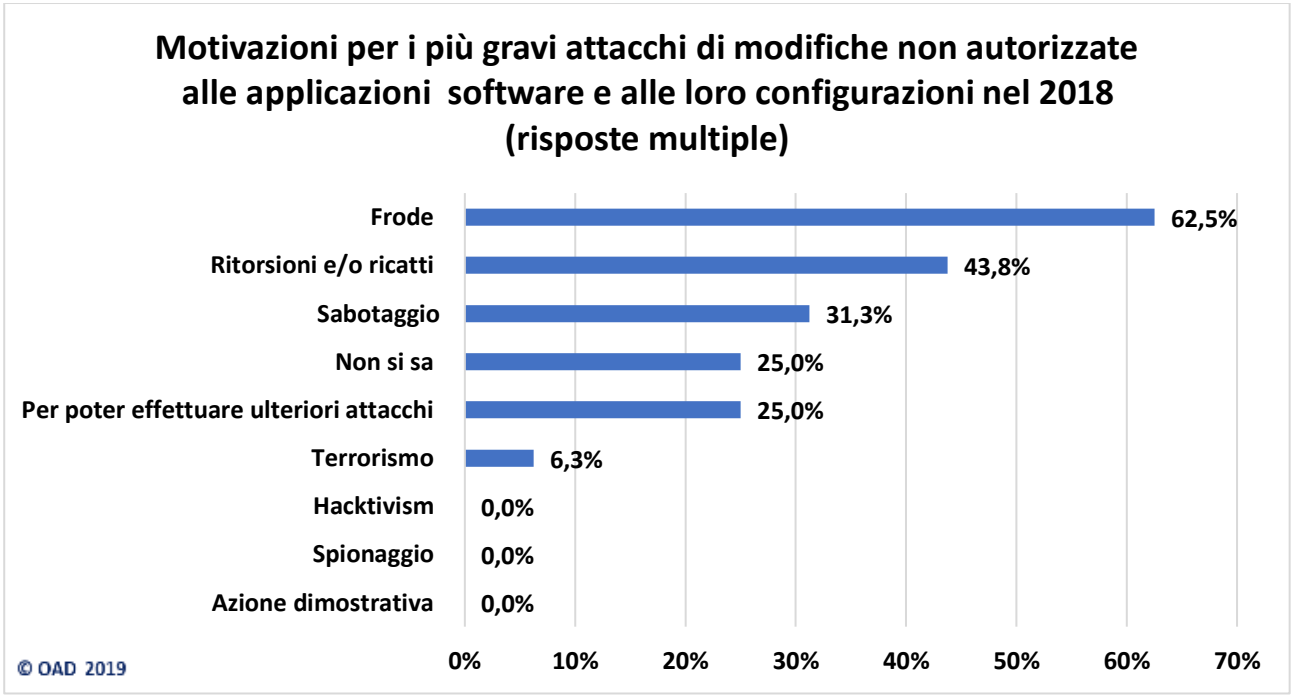

Fig. 6.9-4

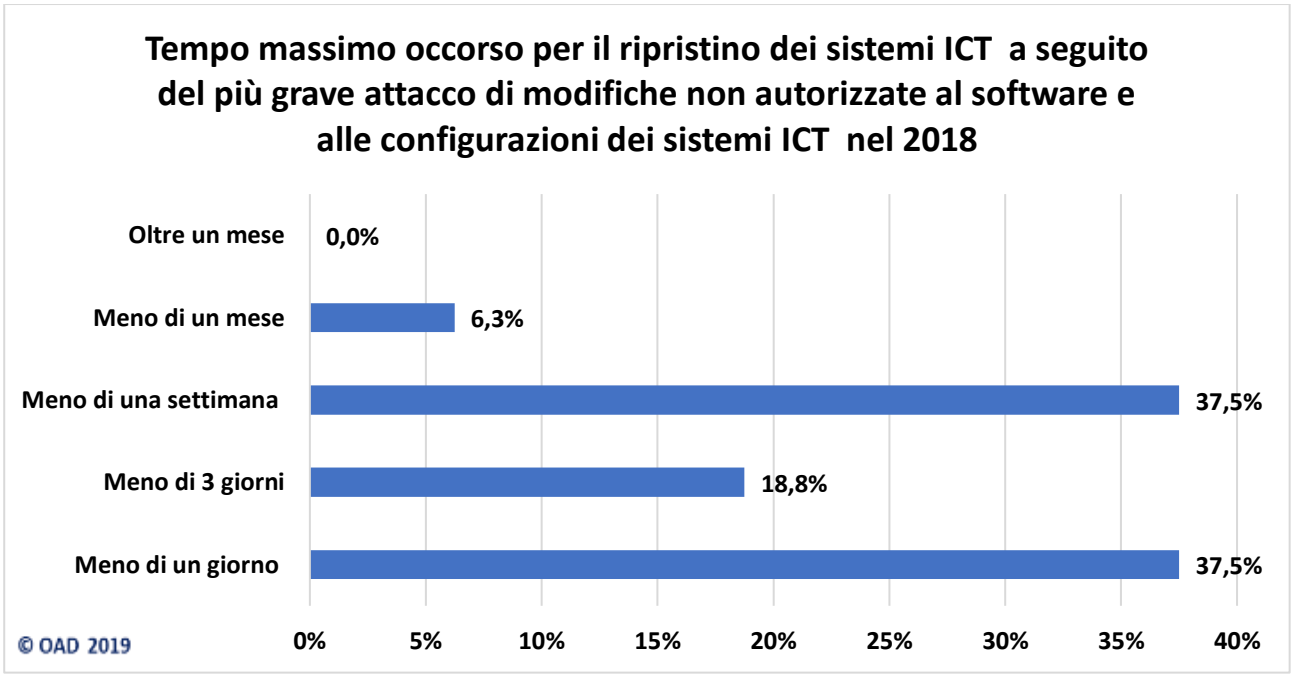

Fig. 6.9-5

6.10 Modifiche non autorizzate alle informazioni trattate dai sistemi ICT

Le modifiche non autorizzate alle informazioni trattate da un sistema informatico sono tra gli attacchi più subdoli e critici, in quanto minano l'integrità e la consistenza stessa dell'informazione,

che è uno dei principali asset (beni) dell'azienda/ente, ed in molti casi è difficile individuare, soprattutto in breve tempo, una alterazione non autorizzata dei dati.

La fig. 6.10-1 mostra che il 12,4% dei rispondenti ha rilevato questo attacco, e che questi attacchi non sono mai stati effettuati più di 10 volte nell'anno: ulteriore indice della difficoltà nell'effettuarlo.

In fig. 6.10-2 sono riportate le tecniche più diffuse per effettuare tali attacchi, almeno nei casi rilevati dai rispondenti: al primo posto quelle basate su codici maligni/script, cui seguono la raccolta di informazioni ed i toolkit, ciascuna con circa 5 punti percentuali di distacco rispetto al precedente.

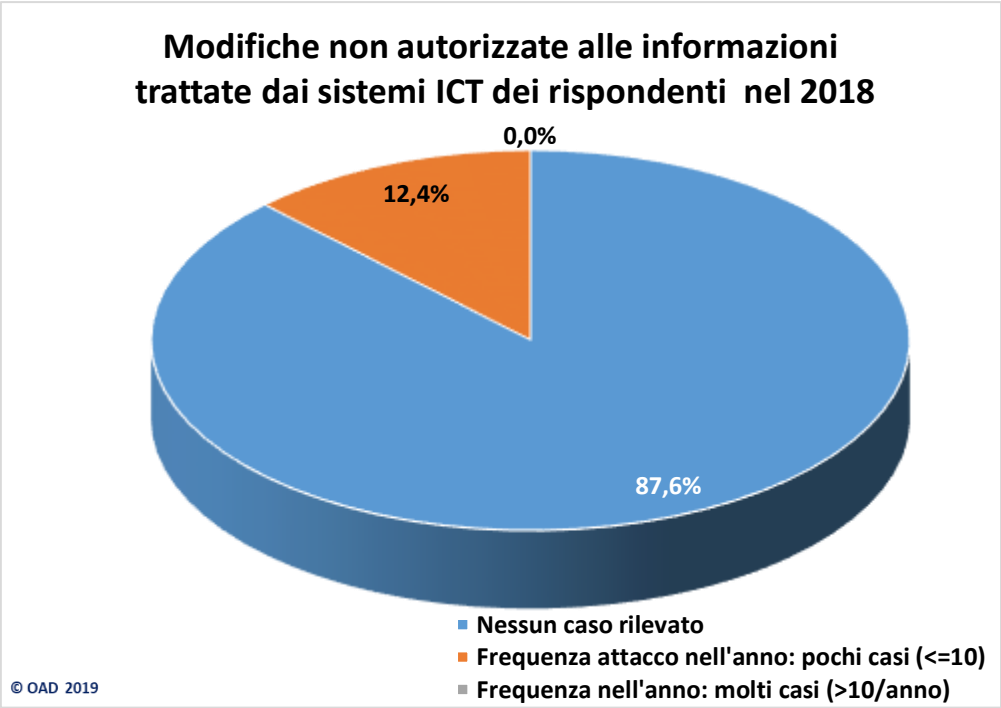

Fig. 6.10-1

La fig. 6.10-3, con risposte multiple, mostra gli impatti causati dagli attacchi di questo tipo più gravi subiti dai rispondenti, sempre con possibilità di risposte multiple. Più della metà dei rispondenti, 53,8%, non ha subito impatti o li ha subiti irrilevanti. Con pari percentuale, il 20%, la perdita di immagine e gravi disservizi informatici per gli utenti ed i clienti.
Quasi il 60% non ha avuto impatti, ma poco meno della metà ha avuto interruzione dei servizi ICT più o meno gravi e prolungati: e oltre ai disservizi, circa il 18% ha avuto perdita di immagine e costi e tempi elevati per il ripristino, Il 11,76%, ha dovuto rimborsare danni ai Clienti, ed il 5,88% ha addirittura perso affari e clienti.

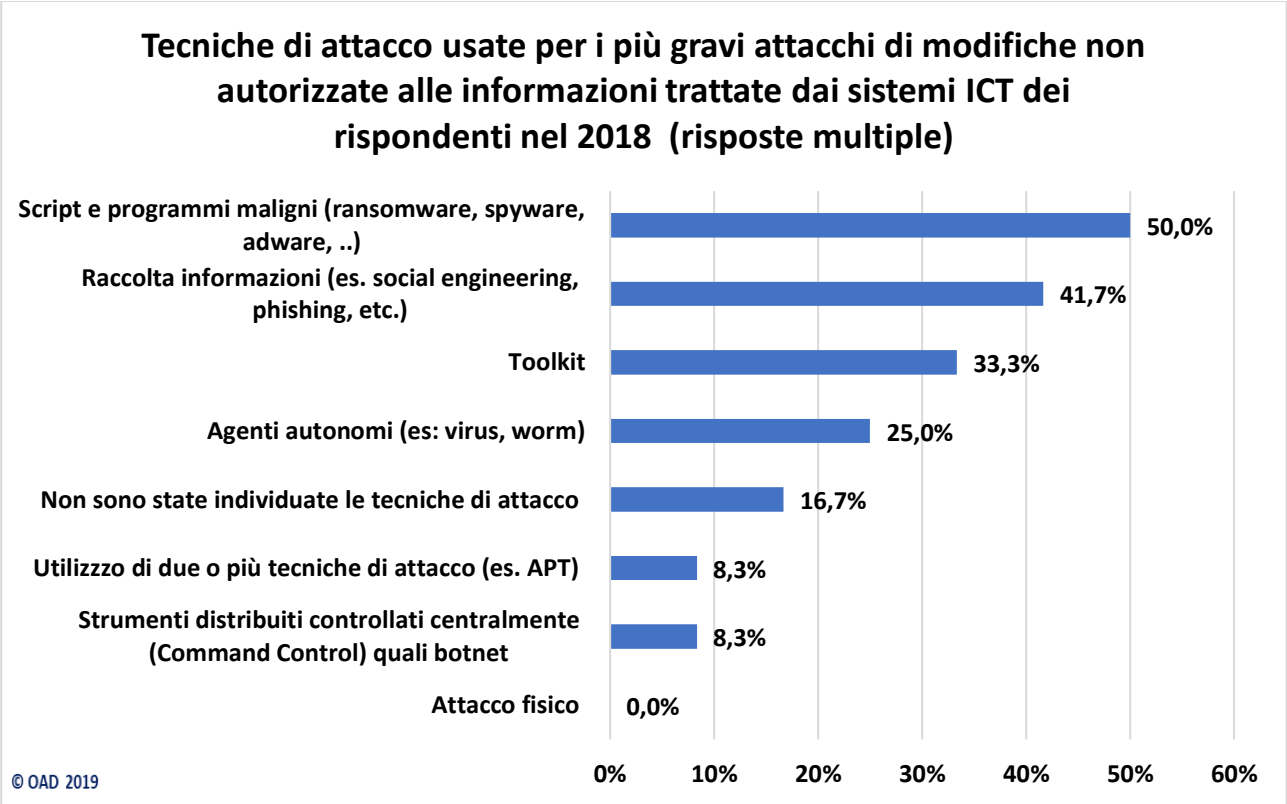

Fig. 6.10-2

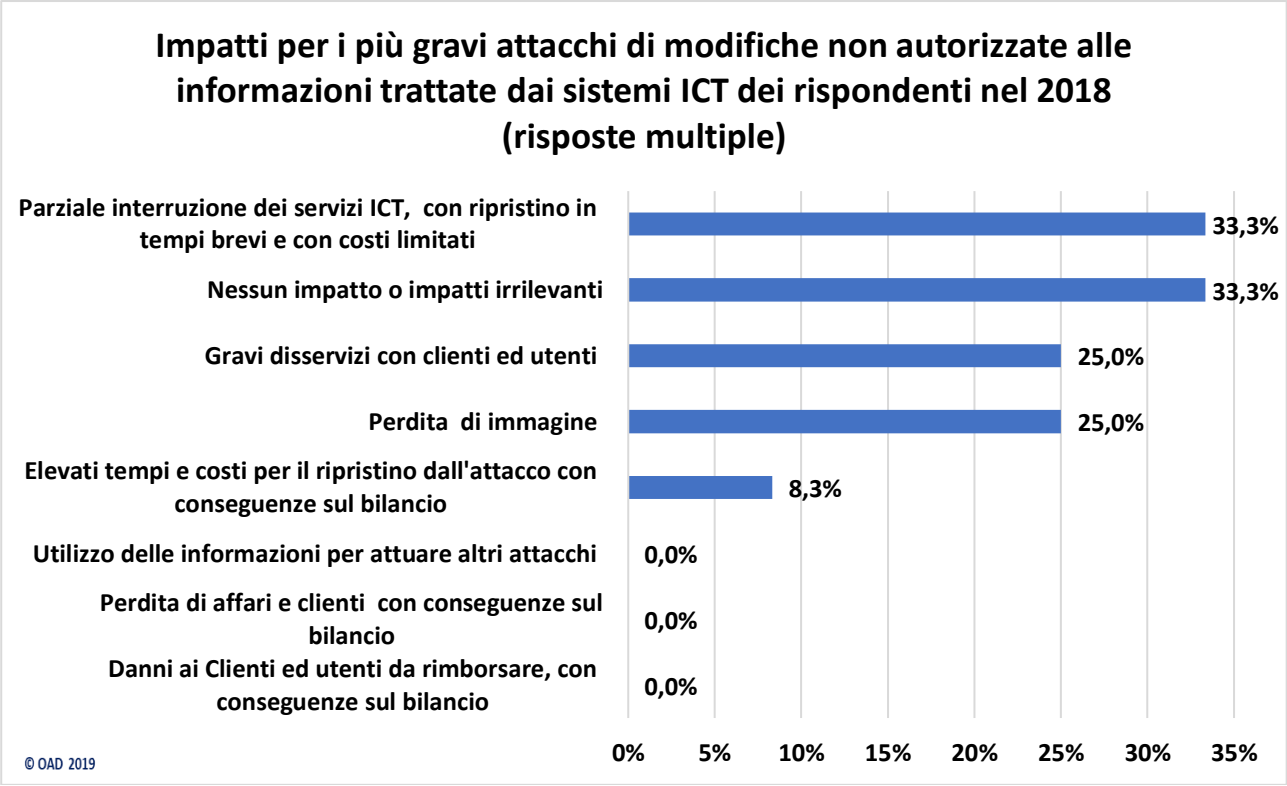

Fig. 6.10-3

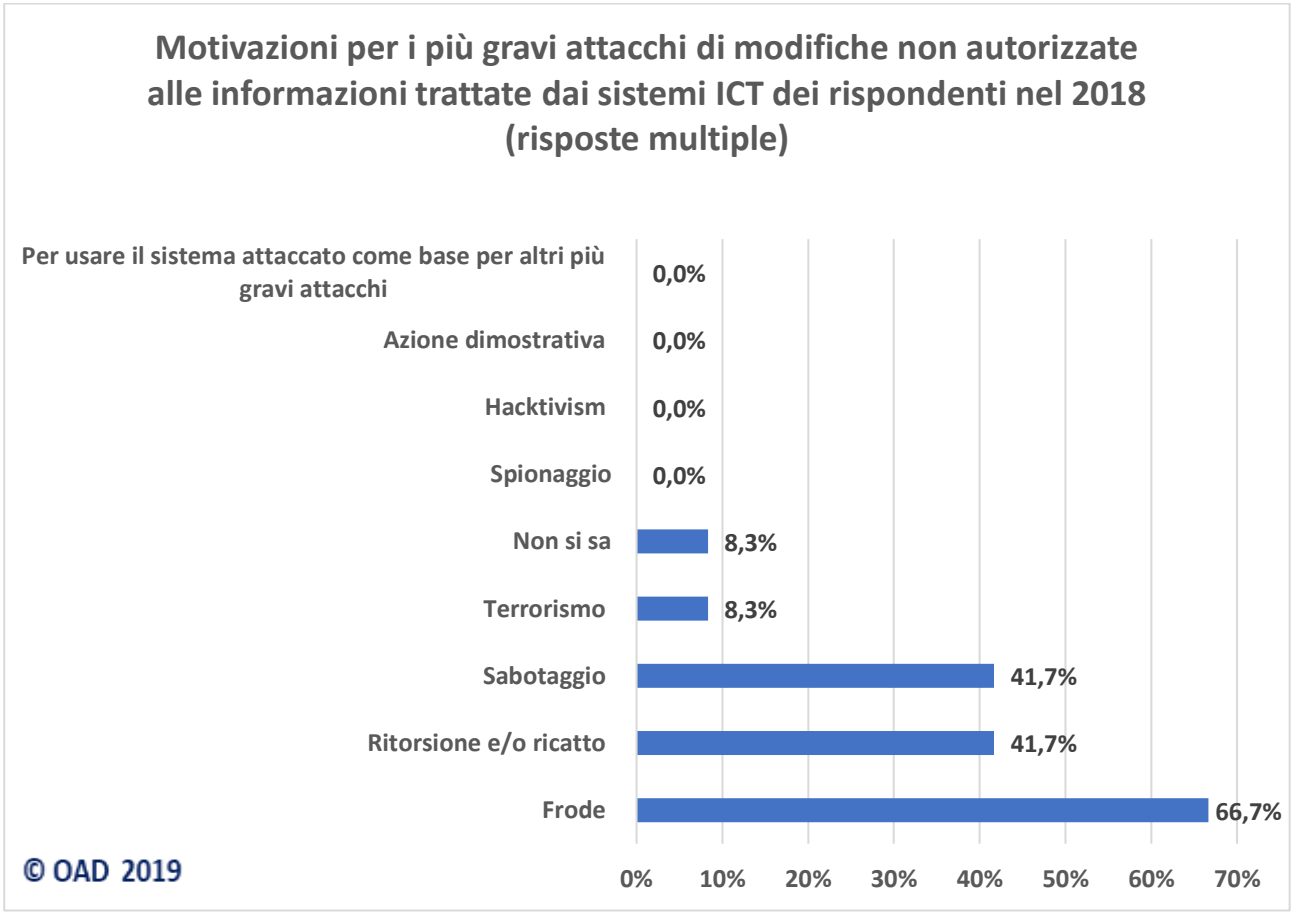

Fig. 6.10-4

La fig. 6.10-4, con risposte multiple, schematizza le possibili motivazioni per questi attacchi, con risposte multiple: al primo posto la frode, per circa i 2/3 dei rispondenti, cui segue ritorsione/ricatto e sabotaggio con la medesima percentuale del 41,7%. Per l'8,3% la motivazione può essere dovuta a cyber terrorismo.

Questo tipo di attacco, pur essendo critico, riesce ad essere ripristinato da tutti i rispondenti che l'hanno subito entro una settimana, come mostrato dalla fig. 6.10-5. L'alta percentuale di ripristini tra i 3 ed i 7 giorni, 41,7%, è un indicatore della criticità di questo tipo d'attacco.

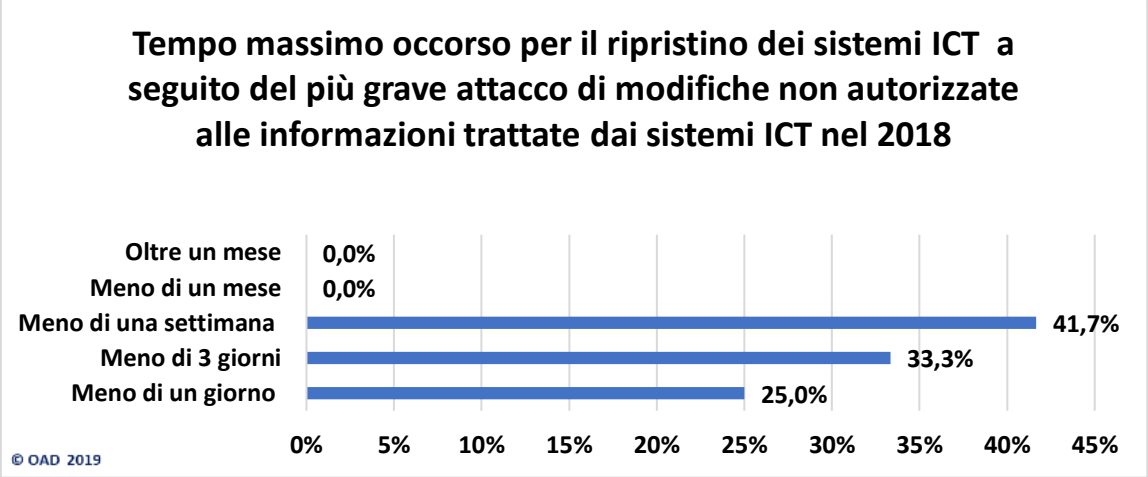

Fig. 6.10-5

6.11 Saturazione risorse digitali (DoS, DDoS)

La saturazione delle risorse ICT, indicata sovente anche in Italia con l'acronimo inglese DoS/DDoS, Denial of Service/Distributed DoS, è un tipo di attacco che nel 2018 si è posizionato, come diffusione tra i rispondenti, al quinto posto, come evidenziato nella fig. 6-7. Il 30,9% lo ha subito, come indicato nella fig. 6.11-1, ma nessuno dei rispondenti lo ha subito per più di 10 volte nell'anno: percentuale simile a quella rilevata nella precedente edizione per il 2017, per quasi il 30% degli allora rispondenti. DoS/DDoS è una tipologia di attacco ormai consolidata, assai critica per prevenirla-contrastarla, ma nel corso del 2018 non più ai primi posti come diffusione tra i rispondenti. Probabilmente, dopo i diffusi attacchi degli anni precedenti, molte aziende/enti dei rispondenti hanno attuato le misure per evitare e contrastare DoS/DDoS.

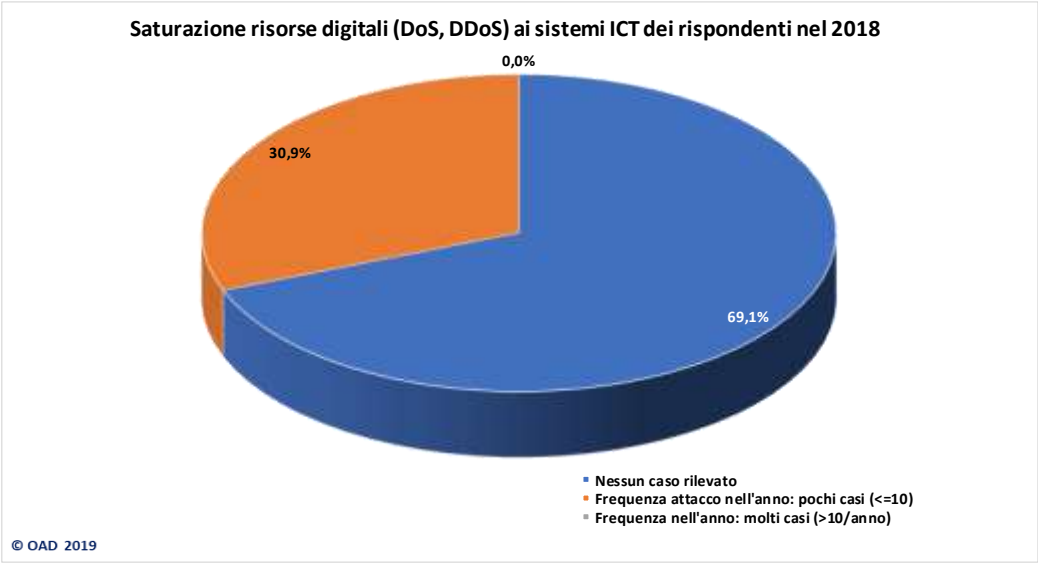

Fig. 6.11-1

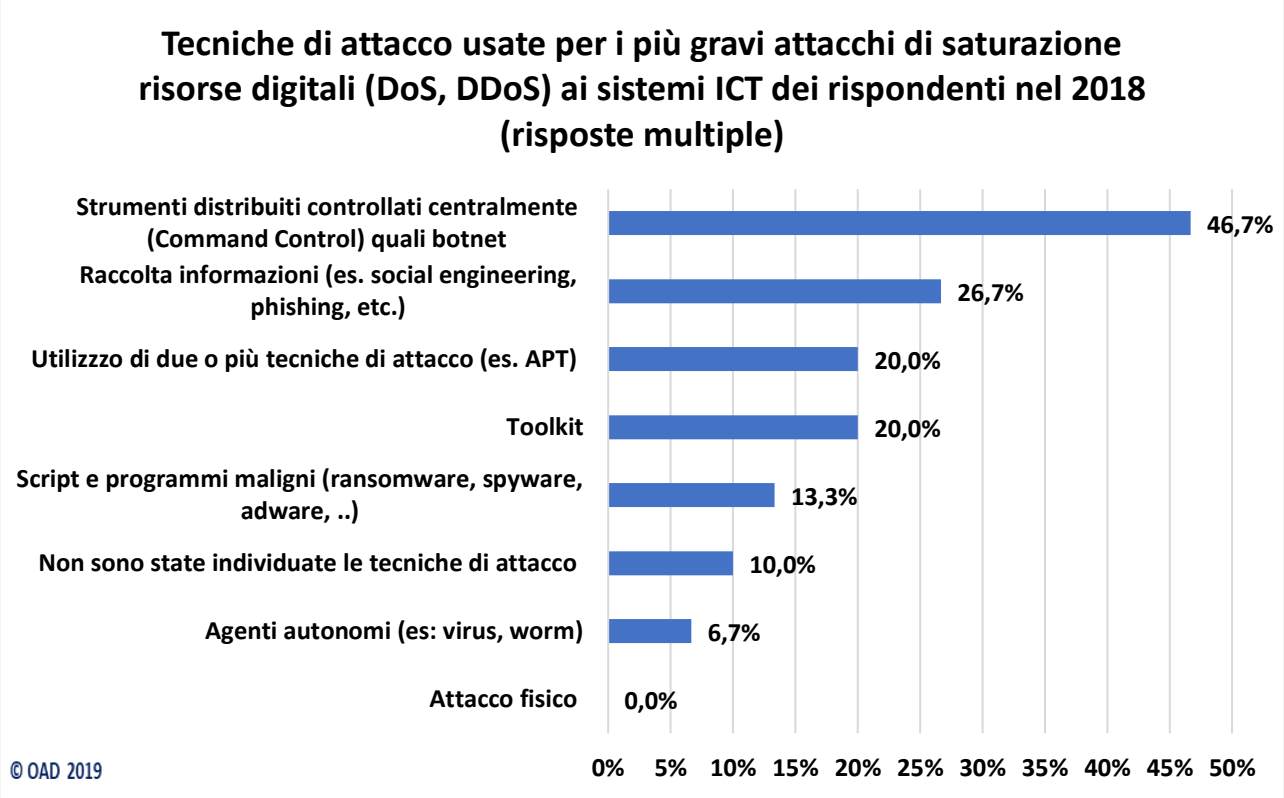

Fig. 6.11-2

Le tecniche usate per portare tali attacchi sono schematizzate, con risposte multiple, nella fig. 6.11-2. Correttamente, dal punto di vista tecnico, al primo posto con un 46,7%, le botnet, la modalità più usata per DDoS. Al secondo posto il social engineering, con un 26,7%, molto probabilmente per la raccolta di informazioni atte ad individuare gli applicativi target da saturare con SoS/DDoS. Al terzo posto l'uso in parallelo di più tecniche d'attacco, e con il medesimo 20% l'uso di toolkit, e a scalare le altre tecniche di attacco.

Le implicazioni causate da un DoS/DDoS ai sistemi informatici dei rispondenti che l'hanno subito, e nella maniera più grave, sono in fig. 6.11-3, con risposte multiple. La figura mostra chiaramente due diverse situazioni: la prima, con il 50% dei rispondenti, ha subito l'attacco ma senza alcun impatto, dato che, sicuramente, le loro reti erano protette da attacchi di questo genere, grazie ad accordi coi fornitori di TLC e networking. La seconda situazione ha portato a vari seri impatti, probabilmente non avendo concordato ed attuato coi fornitori di TLC le adeguate misure: 1/3 dei rispondenti perde business e clienti, quasi ¼ ha perdite di immagine, il 3,3% danni da risarcire.

La fig. 6.11-4 mostra, con risposte multiple, le percentuali delle motivazioni per l'attacco DoS/DDoS subito, a giudizio dei rispondenti e con risposte multiple.
Ragionevolmente, al primo posto si posiziona il sabotaggio e, con lo stesso valore del 28,3%, l'azione dimostrativa. Quest'ultima motivazione, anch'essa al primo posto, risulta per l'autore strana: dimostrativo un attacco DoS/DDoS? Dimostrativo per un successivo ricatto? La ritorsione-ricatto si posiziona logicamente al secondo posto con un 17,4%, al terzo posto hacktivism con un 13%.
Da sottolineare un 13% dei rispondenti che non hanno idea delle motivazioni per il più grave DoS/DDoS che hanno subito.

Che una buona parte dei rispondenti siano ben protetti anche per questa tipologia di attacchi, come già indica il 50% degli attaccati che non ha subito impatti (fig.6.11-3), è confermato dai tempi di ripristino, sempre per gli attacchi più gravi, mostrati nella fig. 3.11-5: ben il 66,7% è stato in grado di

ripristinare dopo l'attacco in un solo giorno, e complessivamente il 76,7% riesce a farlo nell'arco di 3 giorni.

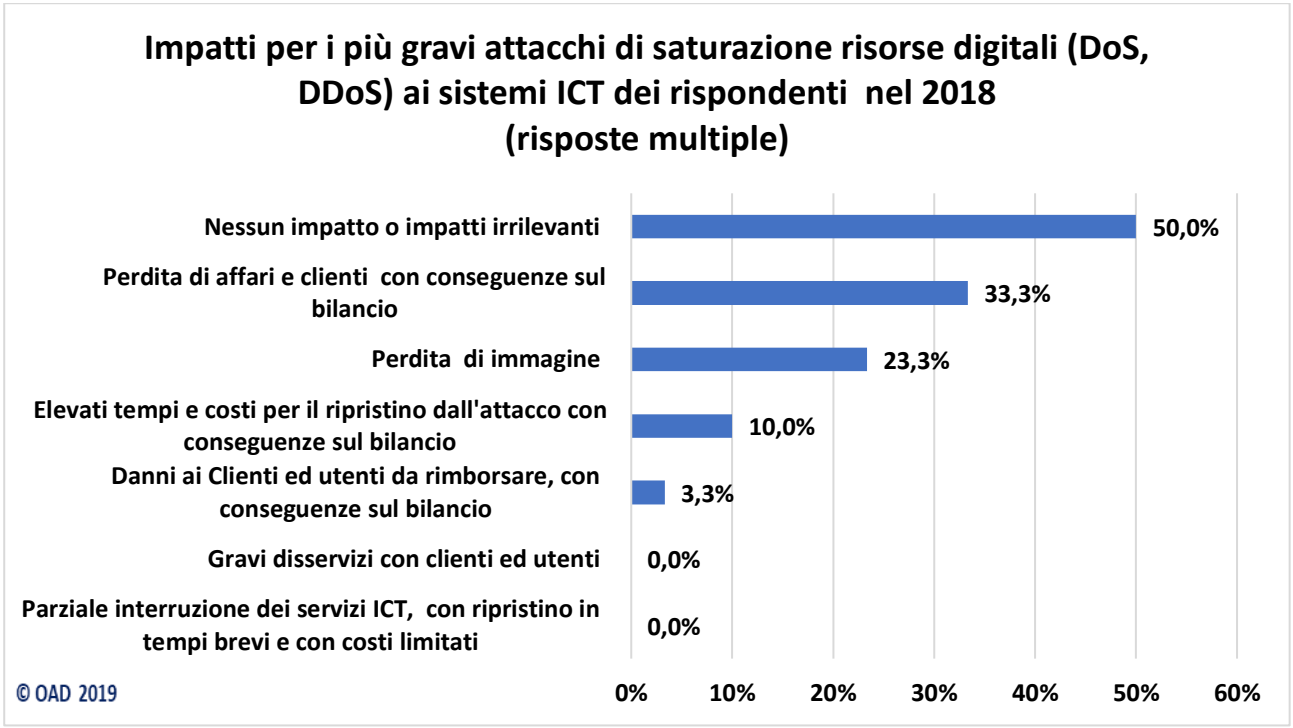

Fig. 6.11-3

Un blocco di più di 3 giorni, anche solo di alcuni servizi informatici, può essere letale per numerose aziende/enti di medie grandi dimensioni: e il 23,3% dei rispondenti, che hanno subito questo attacco, hanno impiegato da 3 giorni ad un mese per sbloccare la saturazione delle risorse ICT attaccate e ripristinare la situazione. Questi ultimi non avevano sicuramente predisposto le opportune misure coi loro fornitori di reti, e le conseguenze sono anche i tempi indicati.

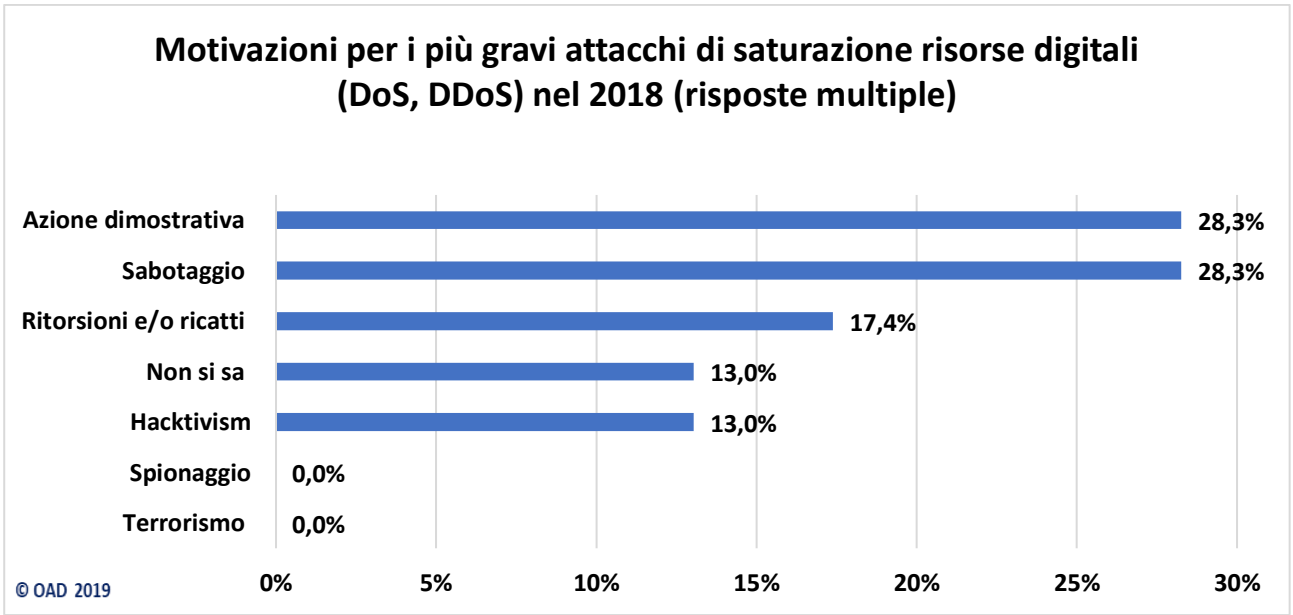

Fig. 6.11-4

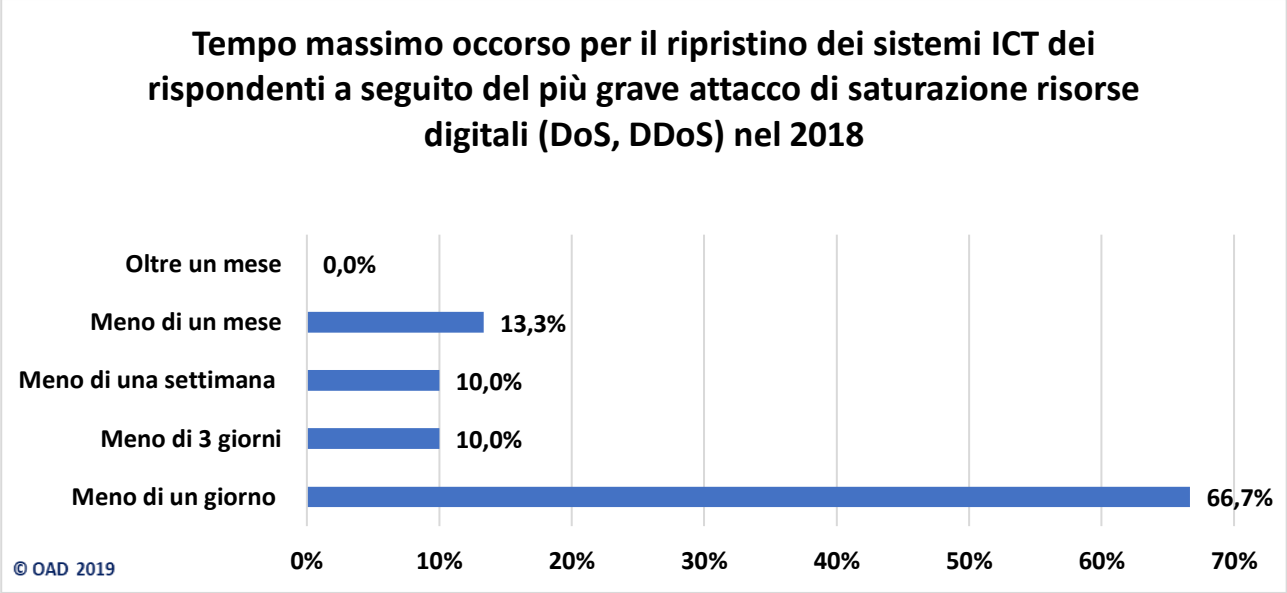

Fig. 6.11-5

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

Le aziende/enti italiani fanno un crescente uso della terziarizzazione di servizi ICT e di servizi in cloud: parte del, e in certi casi l'intero sistema informatico è presso terzi, a livello di software o anche di hardware (housing), così come la sua gestione operativa: un attacco digitale ai sistemi di questi fornitori di terziarizzazione ICT e di cloud, chiamati per brevità outsourcer, è anche un attacco al sistema informatico dell'azienda/ente cliente. Gli outsourcer sono medie e grandi imprese, anche a livello internazionale, conosciuti sul mercato e per questo loro stessi un interessante target di attacco. Nella maggior parte dei casi questi fornitori hanno serie e sofisticate contromisure di sicurezza, molto più potenti ed efficaci di quelle che potrebbero mettere in atto, nella media, i loro clienti. Ma per attaccanti con competenze e risorse, colpire e perforare un outsourcer significa conoscere e attaccare nello stesso tempo almeno una parte dei clienti operanti con quell'outsourcer, clienti che a loro volta possono essere significativi per l'attaccante.
Volutamente nell'elenco delle tipologie di attacchi declinate sul "che cosa attacco" si è inserita questa generica voce di attacco ai cloud ed alle risorse ICT terziarizzate, senza dettagliare le possibili differenti tipologie di attacco considerate nella tassonomia di attacchi di OAD: non sono state quindi richieste nel questionario on line le diverse possibili modalità di attacco, da quello fisico alle reti, dall'IAA agli applicativi e ai dati trattati, per non rendere troppo lunga e difficoltosa la sua compilazione.

La fig. 6.12-1 indica che hanno rilevato attacchi digitali sui loro sistemi in outsourcing il 18,1% dei rispondenti, e di questi il 5,3% con attacchi ripetuti nell'anno più di 10 volte. La figura indica inoltre che il 23,4% dei rispondenti dichiara di non terziarizzare propri sistemi, nemmeno in cloud: quasi ¼ del totale, ma che comunque conferma, rispetto agli anni passati, la crescita ed il consolidamento nell'uso di cloud e di outsourcing da parte dei rispondenti, che rappresentano, con un buon bilanciamento, la variegata realtà italiana di aziende/enti e dei loro sistemi informatici.

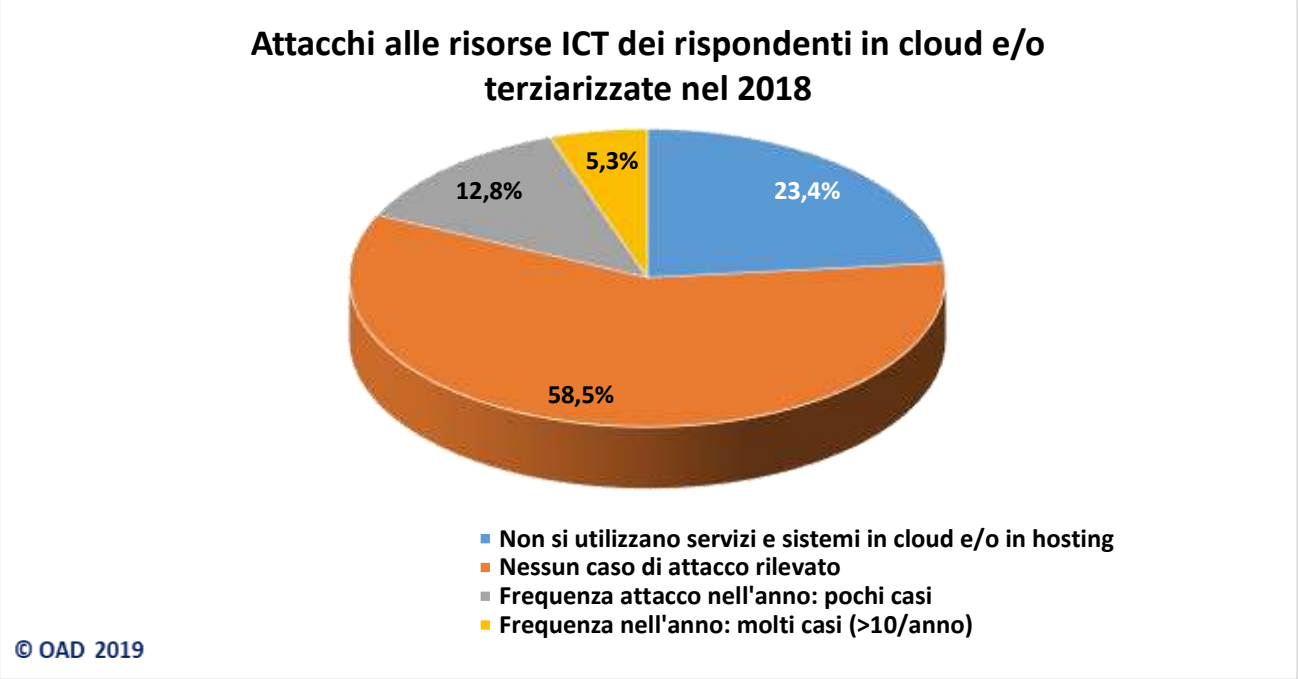

Fig. 6.12-1

La fig. 6.12-2 mostra, con risposte multiple, le tecniche probabilmente usate secondo i rispondenti che hanno subito questo attacco. Al primo posto per il 41,7% dei rispondenti i toolkit, necessari per esaminare possibili punti di ingresso e vulnerabilità dell'outsourcer, cui segue con il 35,3% la raccolta di informazioni: social engineering, phishing, etc. Con la medesima percentuale, 29,4%, si posizionano gli script-codici maligni e le botnet. A scalare seguono, con percentuali degradanti, l'uso di più tecniche contemporaneamente e l'uso di agenti autonomi quali i virus. Ovviamente, e correttamente, nessun attacco fisico. L'attacco ai sistemi ICT terziarizzati vede quindi un ampio spettro di tecniche d'attacco usate
La fig. 6.12-3 illustra, con risposte multiple, gli impatti riscontrati dai rispondenti a seguito dell'attacco all'outsourcer utilizzato; i dati esposti confermano che l'outsourcer dispone, nella maggior parte dei casi, di idonee livelli di sicurezza digitale. Infatti, più della metà dei rispondenti, il 52,9%, afferma di non aver avuto impatti, o di averli avuti irrilevanti; il 35,3% di averli superati in breve tempo, e questa risposta conferma che la maggior parte degli outsourcer ha i mezzi per prevenire/contrastare l'attacco, e soprattutto i mezzi per un veloce ripristino della situazione ex ante, così come confermato dal ripristino entro il primo giorno per il 64,7% dei rispondenti (fig. 6.12-5). Ma un altro insieme di rispondenti ha avuto impatti significativi: perdita di immagine con il 23,5%, gravi disservizi con il 11,8%, e con la stessa percentuale anche perdita di clienti e attacco come base per ulteriori attacchi. Questa situazione negativa è a sua volta confermata dal fatto che il 17,6% richiede per il ripristino dei casi peggiori da 3 giorni ad una settimana, ed il 5,9% tra oltre una settimana ma entro un mese, come da fig. 6.12-5.

Le possibili motivazioni per l'attacco più grave (fig. 6.12-4, con risposte multiple) portano al primo posto la frode, con il 35,3% dei rispondenti che l'hanno subita. Con la stessa percentuale i rispondenti che non sono in grado di stimare le possibili motivazioni. Seguono a scalare le altre possibili motivazioni indicate nel questionario. Nessuno dei rispondenti reputa il terrorismo cibernetico una possibile motivazione.

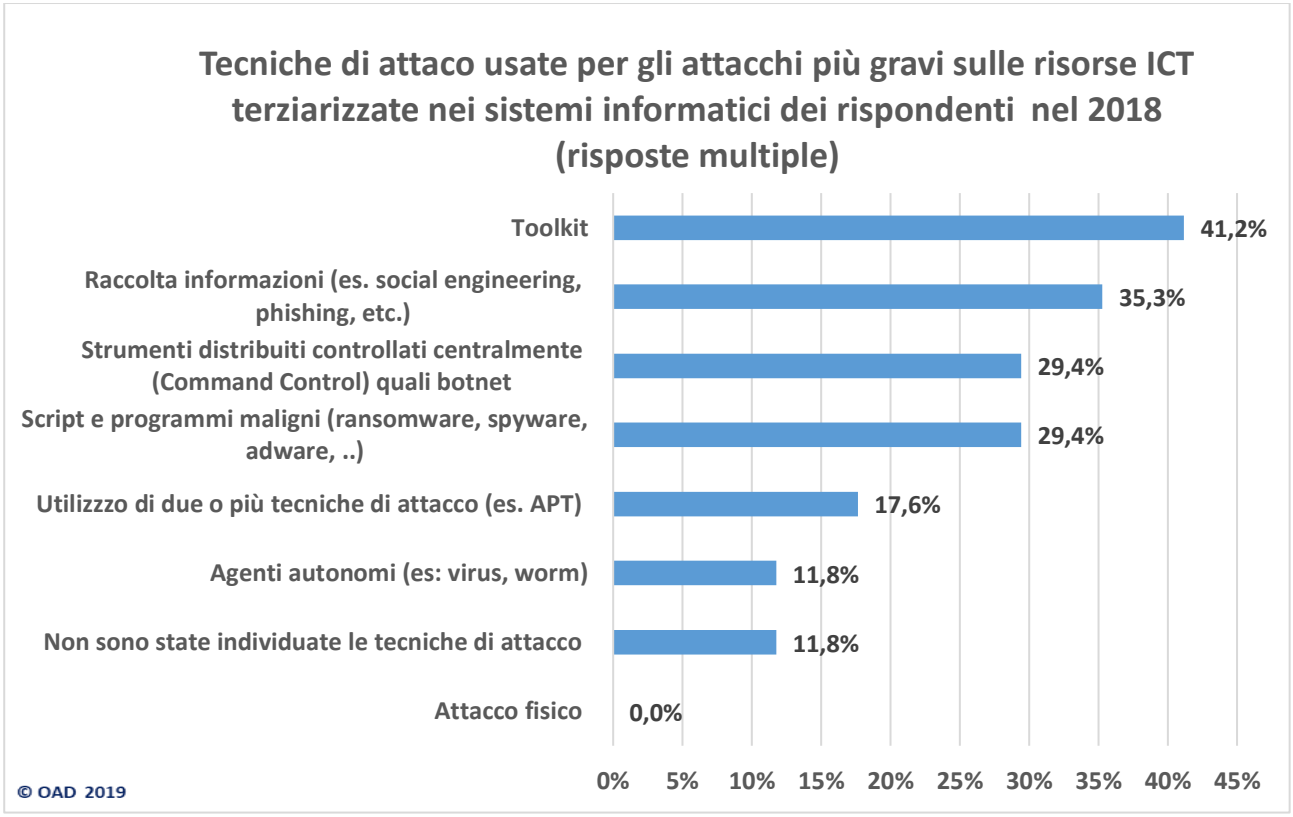

Fig. 6.12-2

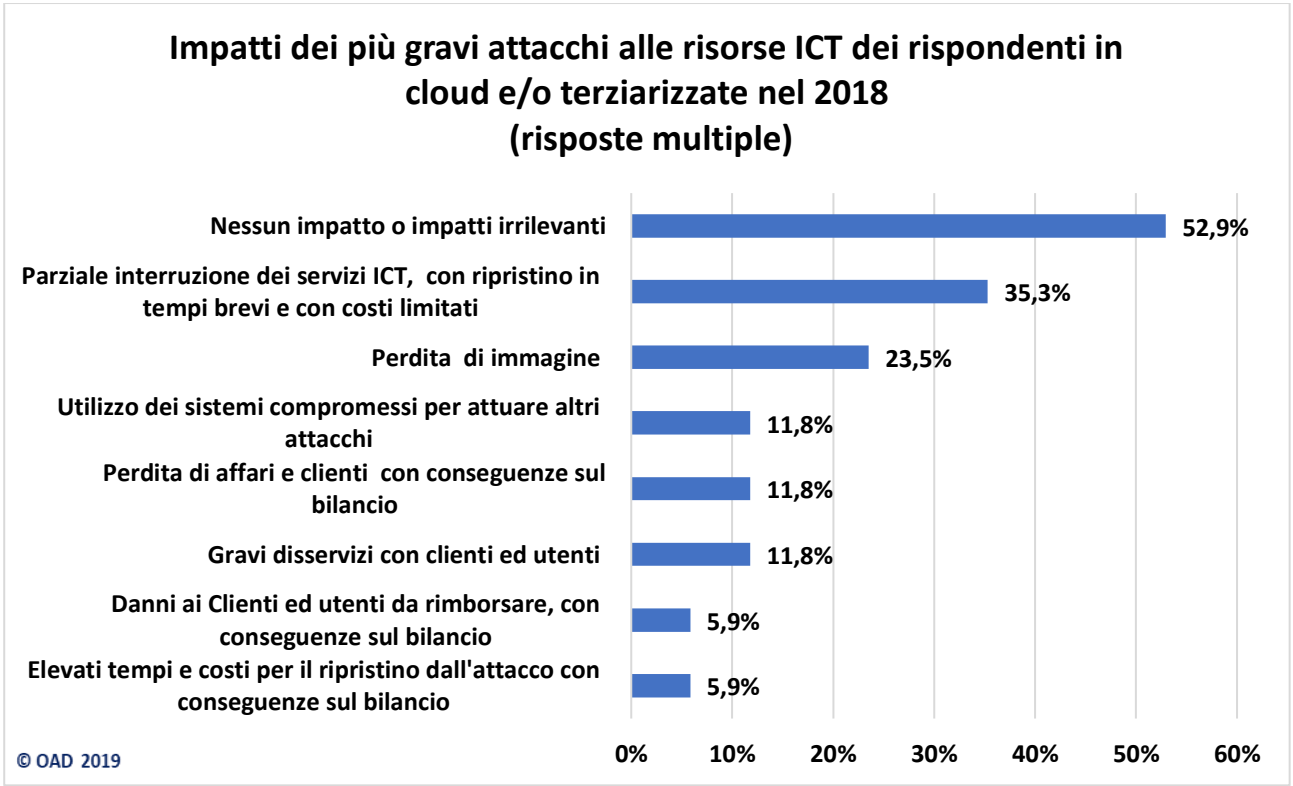

Fig. 6.12-3

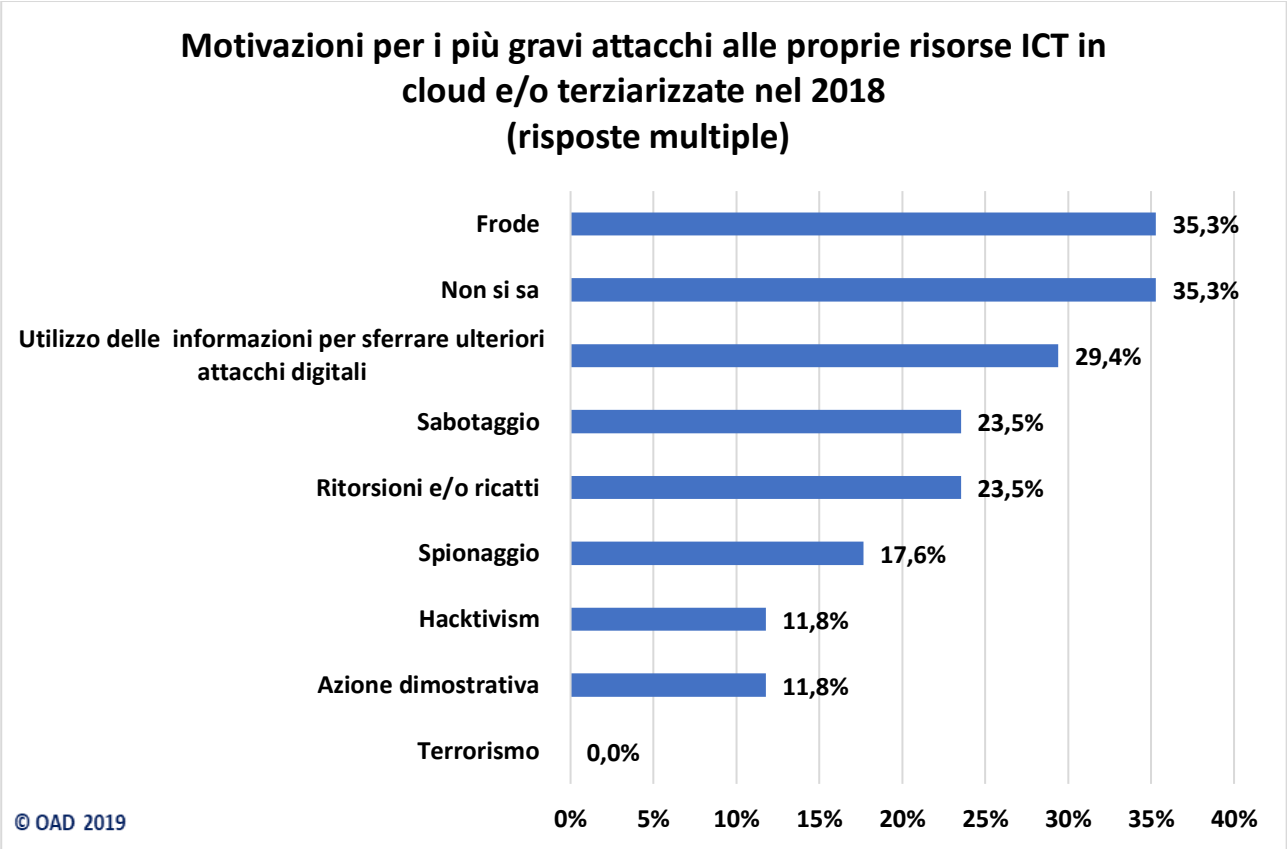

Fig. 6.12-4

La già citata fig. 6.12-5 mostra che più dei ¾ dei rispondenti che hanno subito questo tipo di attacco, il 76,5%, riescono a ripristinare entro 3 giorni, e di questi ben il 64,7% entro un solo giorno: e questo nel caso peggiore di attacco. Tali dati indicano che il livello di sicurezza digitale di almeno la maggior parte degli outsourcer è elevato sia in termine di prevenzione che di contrasto e ripristino. Per il 23,5% dei rispondenti che ha impiegato tempi più lunghi, e comunque entro un mese solare, significa o che hanno avuto, o sottoscritto, l'idoneo livello di sicurezza dall'outsourcer, e/o che il tipo di attacco è stato così sofisticato e critico, da aver richiesto tali tempi per poter riattivare la situazione ex ante.

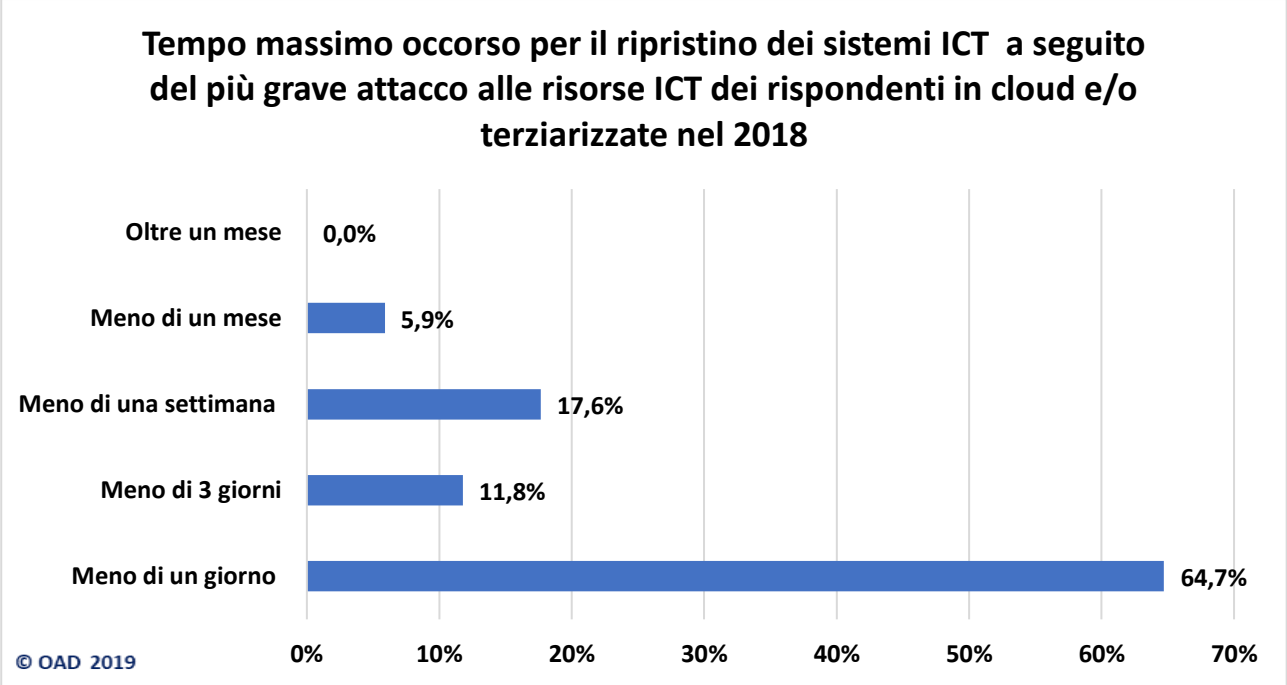

Fig. 6.12-5

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

Come già introdotto nei precedenti Capitoli 4 e 5, la pervasività di Internet e l'inserimento di capacità elaborativa e di comunicazione in un numero sempre più crescente di oggetti di uso comune ha allargato ampiamente l'area di interoperabilità e quindi l'area di possibili attacchi.
In tale ambito è esploso negli ultimi anni il fenomeno degli IoT, in italiano traducibile come Internet delle Cose. Al di là dell'inserimento di un piccolo sistema ICT con capacità elaborativa e di trasmissione, i così detti sistemi "embedded", qualsiasi oggetto senza ICT come un abito, un paio di scarpe, un giocattolo, un piatto e così via può divenire riconoscibile ed un poco "smart" grazie ad etichette di identificazione quali tag RFID[16] o codici QR[17], in grado di comunicare in rete e di essere riconosciuti da ed interagire con dispositivi mobili quali smartphone e tablet dotati delle opportune applicazioni. Queste etichette sono usabili anche per gli animali.
IoT indica quindi una rete di oggetti (o di loro parti) che, grazie alle loro capacità elaborative e di connettività, sono in grado di interoperare tra loro e con i sistemi informatici, abilitando nuove soluzioni e nuove integrazioni in moltissimi settori. Il singolo dispositivo IoT è un "oggetto smart", caratterizzabile da capacità funzionali quali l'identificazione, la connessione, la localizzazione, l'elaborazione di dati e la comunicazione a livello locale e/o geografico. Il mondo degli IoT sta esplodendo in innumerevoli settori, che includono (elenco non esaustivo) domotica, robotica, controlli industriali e del territorio, trasporti (dalle auto alle moto, dai pullman agli autocarri, dai muletti agli ascensori, dai treni alle navi), avionica, elettrodomestici, biomedicale, agricoltura e zootecnia, smartgrid, smartcity, telemetria, misurazioni da remoto (la così detta "smart metering" usata per i contatori intelligenti di gas ed energia elettrica), etc.

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

Si devono poi tenere conto della convergenza in corso tra il mondo IoT e quello OT, Operational Technology, che include tutti i sistemi di automazione industriale (considerati nel prossimo paragrafo §6.14).
In termini di sicurezza digitale gli IoT sono balzati al centro della ribalta per la concomitanza di alcuni fattori: in primo luogo per la loro connessione ad Internet, poi per la loro numerosità ed infine perché gran parte degli IoT attualmente in uso non sono stati progettati tenendo conto dei problemi della sicurezza digitale ed i loro software, compreso il sistema operativo, non sono aggiornati tempestivamente, mantenendo per lungo tempo varie vulnerabilità anche già eliminabili con opportune patch o nuove versioni del software. Fin dal 2007, a livello mondiale, il numero di oggetti connessi ad Internet ha superato il numero delle persone connesse, e le previsioni di crescita al 2020 variano nell'ordine di decine di miliardi di IoT connessi. Il Global Risk Report 2018 del World Economic Forum stimava che gli IoT, nel 2020, saranno 20,4 Miliardi, quasi tre volte il numero di abitanti nel mondo.

L'indagine OAD fa riferimento ai soli attacchi intenzionali ai sistemi informatici di aziende/enti, non considera attacchi ai sistemi ICT di persone, domestici e dei loro oggetti smart; questo riduce fortemente il numero di IoT da considerare per le indagini OAD, quella 2019 inclusa.

La fig. 6.13-1 mostra che il 35,4% dei rispondenti usa dei dispositivi IoT e di questi il 6,3% ha subito e rilevato attacchi, tutti ripetuti al max 10 volte nell'anno: una percentuale superiore, come tendenza, al 2,6% emerso nel 2017 e al 4,62% nel 2016 (si veda §6.12 del precedente Rapporto 2018 OAD, scaricabile da **https://www.oadweb.it/it/rapporti-e-relativi-convegni/2018.html).**

Dato il numero limitato, rispetto al totale, dei rispondenti che hanno subito attacchi ai loro i IoT/IIoT, i dati che seguono devono essere considerati come esempi di casi specifici, e non essere presi come riferimento medio della situazione in Italia degli attacchi a questi sistemi.

L'uso di IoT di fatto continua a crescere anche in ambito business, non solo per la domotica o per usi personali/ludici, e in ambito manifatturiero gli IoT usati per l'automazione vengono ora chiamati Industrial IoT, IIoT.
Analizzando e correlando le risposte al questionario OAD 2019, risulta che le aziende che hanno subiti attacchi IoT appartengono ai seguenti settori merceologici:

- Commercio all'ingrosso e al dettaglio, incluso quello di apparati ICT (Codici Ateco G)
- Industria manifatturiera e costruzioni: meccanica, chimica, farmaceutica, elettronica, alimentare, edilizia, ecc. (Codici Ateco C e F)
- Istruzione: scuole e università pubbliche e private (Codici Ateco P)
- Servizi turistici, di alloggio e ristorazione: agenzie di viaggio, tour operator, hotel, villaggi turistici, campeggi, ristoranti, bar, ecc. (Codici Ateco I e N79)
- Telecomunicazioni e Media: produzione musicale, televisiva e cinematografica, trasmissioni radio e televisive, telecomunicazioni fisse e mobili (Codici Ateco J59, J60, J61)
- Trasporti e magazzinaggio (Codici Ateco H).

Le tecniche di attacco indicate dai rispondenti che hanno subito e rilevato attacchi ai loro sistemi IoT sono elencate in percentuale nella fig. 6.13-2, con risposte multiple. Al primo posto, per la totalità dei rispondenti (100%), i toolkit, usati da remoto per verificare i possibili punti deboli e le vulnerabilità da cui sferrare poi l'attacco. Segue la raccolta di informazioni con un 50%, e con questa stessa percentuale gli attacchi basati su due o più tecniche di attacco. L'uso di codici maligni e di script è considerato da 1/3 dei rispondenti, e e le rimanenti tecniche d'attacco hanno tutte il medesimo 16,7%. Con quest'ultima percentuale anche i rispondenti che non sono stati in grado di individuare le tecniche usate per portare l'attacco ai loro IoT. Da evidenziare tra queste tecniche l'attacco fisico: anche gli outsourcer possono subire attacchi fisici che compromettono le risorse ICT terziarizzate.

Come mostrato in fig. 6.13-3, con risposte multiple, gli impatti causati dagli attacchi più gravi subiti sui sistemi IoT sono stati severi e critici per questi rispondenti: solo 1/3 di loro dichiara che gli impatti sono stati nulli o irrilevanti. Per gli altri 2/3, gravi disservizi, perdita di immagine, elevati tempi e costi per il ripristino della loro funzionalità, come confermato anche dalla fig. 6.13-5.

La fig. 6.13-4 mostra, con risposte multiple, le probabili motivazioni degli attaccanti per gli attacchi più gravi: al primo posto il sabotaggio, con il 66,7%, cui segue, a scalare percentualmente, ritorsioni/ricatti e l'uso degli IoT compromessi per portare altri attacchi. Quest'ultimo è un significativo indicatore di come l'area degli attacchi si sia estesa, e come da sistemi IoT si possano attaccare altri sistemi ICT del sistema informatico. Con lo stesso 16,7% sono considerati poi la frode, l'hacktivism e l'azione dimostrativa. Non sono considerate le motivazioni di spionaggio e di terrorismo.

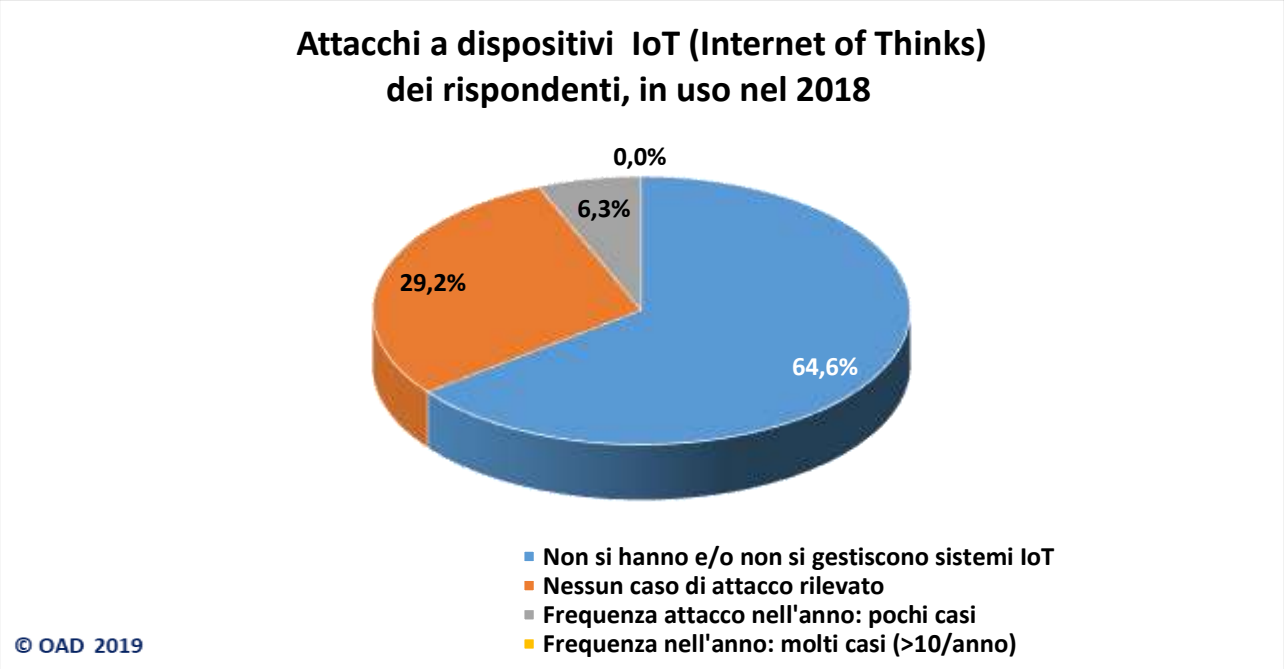

Fig. 6.13-1

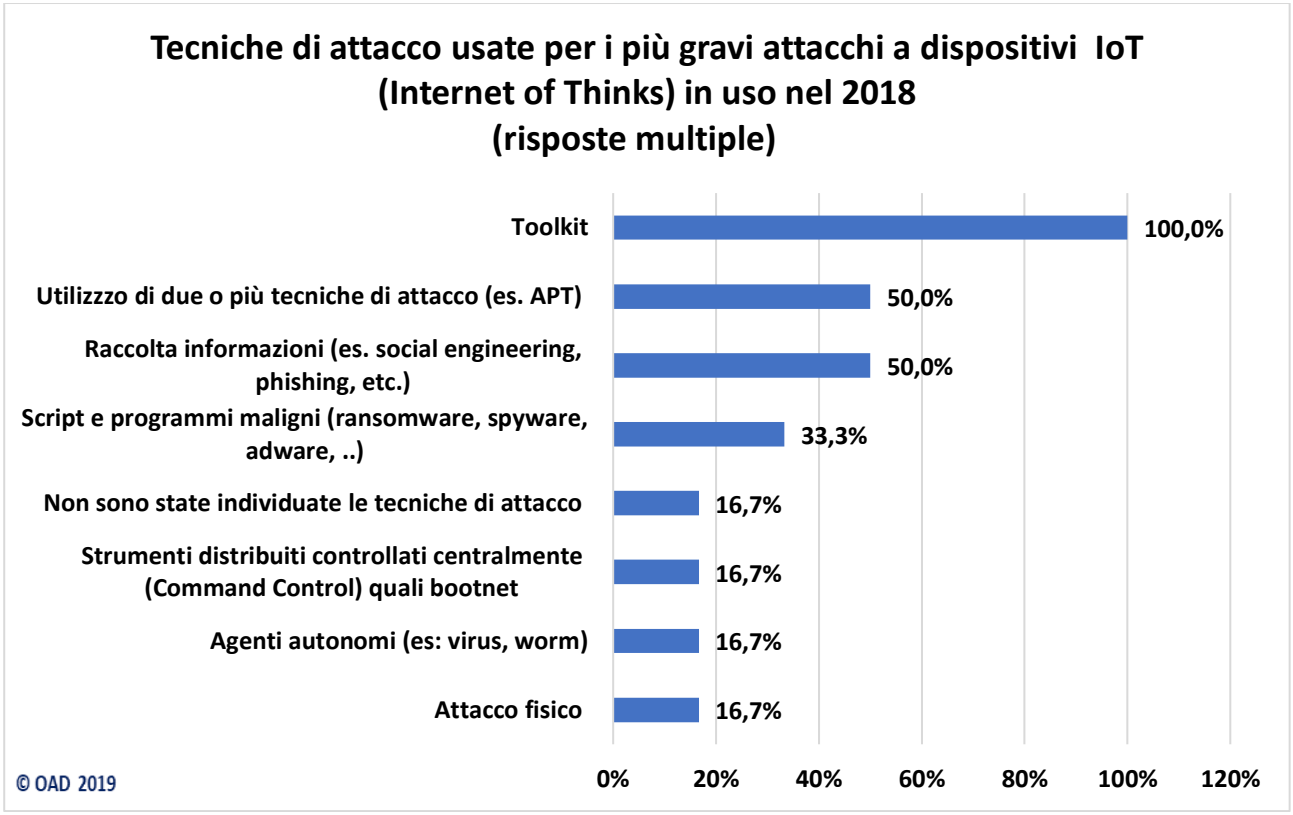
Tecniche di attacco usate per i più gravi attacchi a dispositivi IoT (Internet of Thinks) in uso nel 2018 (risposte multiple)
Toolkit
100,0%
Utilizzzo di due o più tecniche di attacco (es. APT)
50,0%
Raccolta informazioni (es. social engineering, phishing, etc.)
50,0%
Script e programmi maligni (ransomware, spyware, adware, ..)
33,3%
Non sono state individuate le tecniche di attacco
16,7%
Strumenti distribuiti controllati centralmente (Command Control) quali bootnet
16,7%
Agenti autonomi (es: virus, worm)
16,7%
Attacco fisico
16,7%
0%
20%
40%
60%
80%
100%
120%
© OAD 2019

Fig. 6.13-2

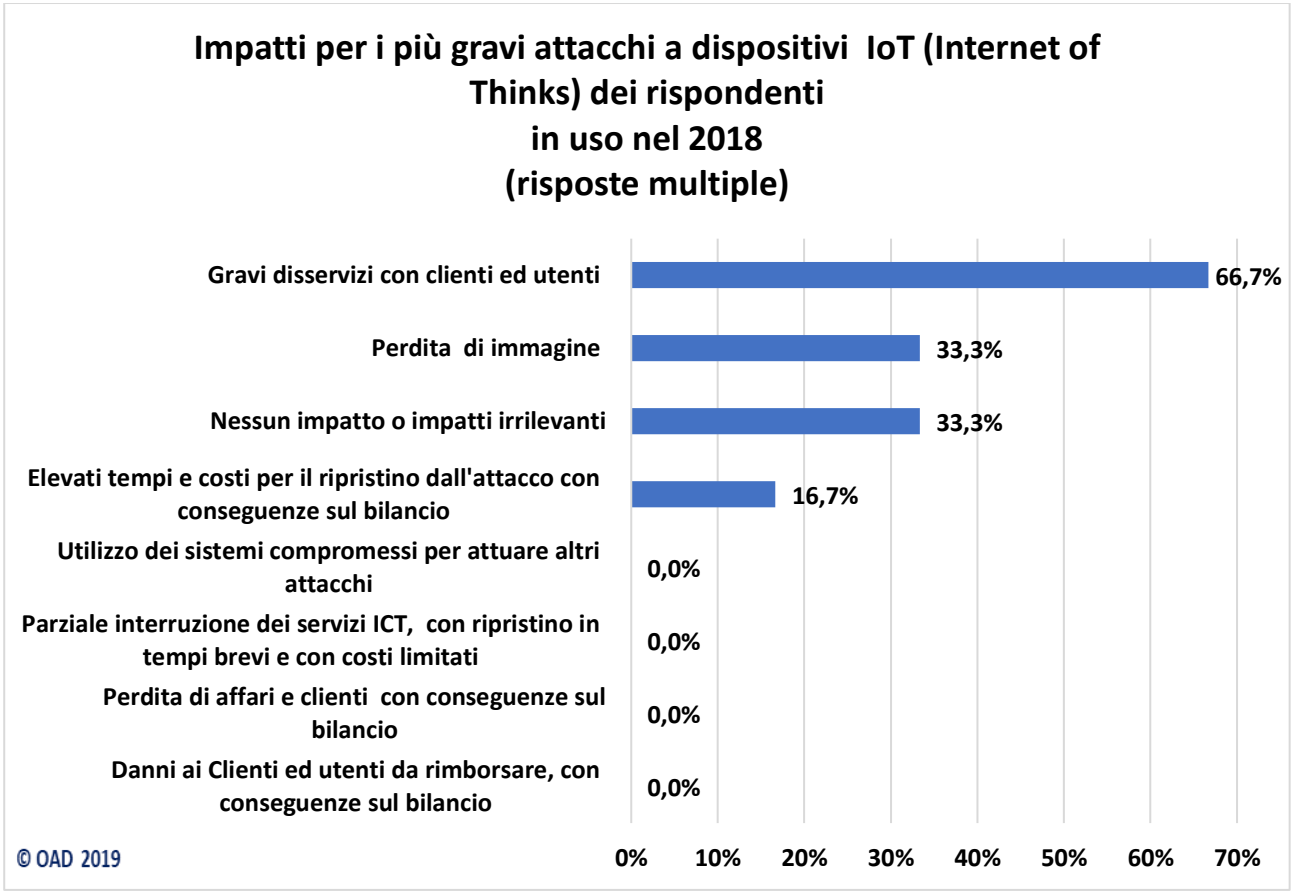
Impatti per i più gravi attacchi a dispositivi IoT (Internet of Thinks) dei rispondenti
in uso nel 2018
(risposte multiple)
Gravi disservizi con clienti ed utenti
66,7%
Perdita di immagine
33,3%
Nessun impatto o impatti irrilevanti
33,3%
Elevati tempi e costi per il ripristino dall'attacco con conseguenze sul bilancio
16,7%
Utilizzo dei sistemi compromessi per attuare altri attacchi
0,0%
Parziale interruzione dei servizi ICT, con ripristino in tempi brevi e con costi limitati
0,0%
Perdita di affari e clienti con conseguenze sul bilancio
0,0%
Danni ai Clienti ed utenti da rimborsare, con conseguenze sul bilancio
0,0%
© OAD 2019
0%
10%
20%
30%
40%
50%
60%
70%

Fig. 6.13-3

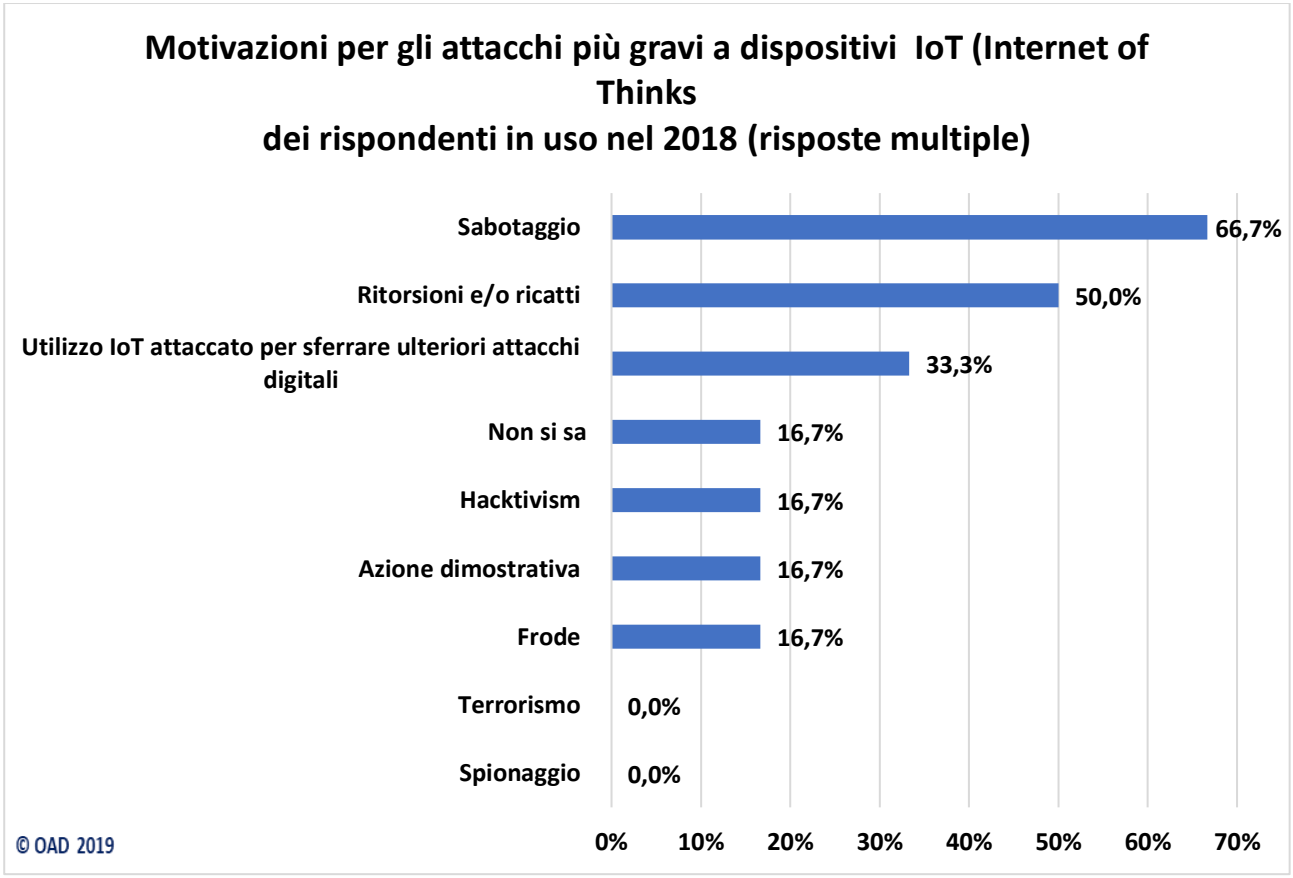

Fig. 6.13-4

La fig.6.13-5 mostra, con risposte multiple, i tempi massimi per il ripristino dopo gli attacchi più gravi rilevati. Interessante evidenziare che in nessun caso il ripristino ha richiesto più di una settimana, ma nella maggior parte dei casi, 66,7%, tra 3 giorni ed una settimana. Per 1/3 dei rispondenti, 33,3%, il ripristino è avvenuto entro 3 giorni. Come già sottolineato, senza alcuna pretesa di fornire statistiche generali sul fenomeno, dato il limitato bacino dei rispondenti che hanno subito attacchi all'IoT, i tempi indicati sono migliorativi rispetto a quelli emersi dalla precedente indagine OAD 2018, e risultano ragionevoli, tenendo conto che da un lato i dispositivi IoT non sempre sono monitorati e controllati centralmente in maniera continua e sistematica, dall'altro che alcuni dispositivi sono dislocati in punti non facilmente raggiungibili dalle persone che devono manutenerli e che possono aggiustarli.

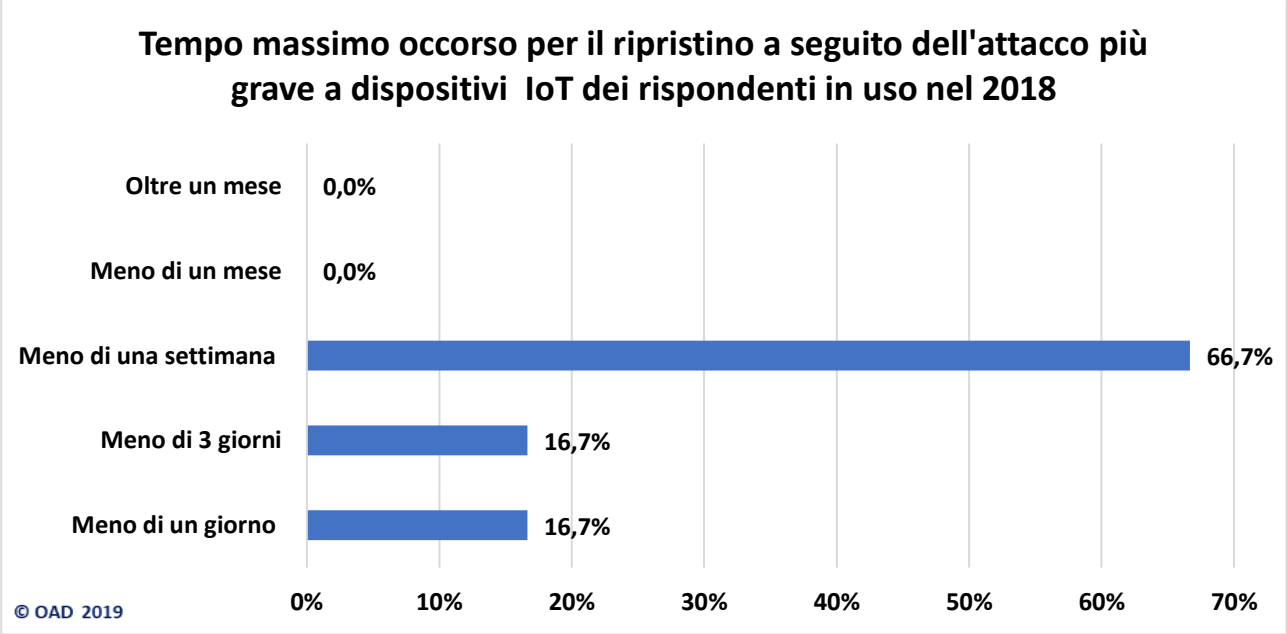

Fig. 6.13.5

6.14 Attacchi ai propri sistemi di automazione industriale e di robotica

I sistemi di automazione industriale e di robotica si vanno estendendo dal tradizionale e consolidato ambiente manifatturiero per l'automazione della produzione ad altri, quali l'automazione dei magazzini per la logistica, l'automazione delle facility di un Data Center, l'ambito ospedaliero soprattutto per sale operatorie robotizzate, la ricerca e sviluppo, e così via.
Per coprire con un unico termine questo ampio e complesso contesto, è emersa la sigla OT, Operational Technology, che nell'uso comune include anche i sistemi IoT/IIoT, trattati separatamente, data la loro numerosità e il loro potenziale di crescita, nel precedente §6.13.
Comunque, nel presente paragrafo e nei suoi grafici, verrà usato l'acronimo OT per la sua brevità: si deve tener conto che, in questo contesto, non contiene gli IoT
I sistemi per l'automazione della produzione e della robotica, che inizialmente operavano in modo autonomo e sovente non erano nemmeno considerati risorse del sistema informatico, ora sono quasi tutte collegate al sistema informatico per interoperare con le applicazioni centralizzate tipo ERP, oltre che direttamente ad Internet, per poter essere accedute da remoto per controlli e manutenzione.
La connessione ai Data Center e soprattutto ad Internet sono elementi che hanno aumentato la vulnerabilità di questi ambienti.
IIoT, sistemi di automazione della produzione e sistemi di robotica vanno sempre più integrandosi e ad interoperare via Internet, e gli apparati, ormai tutti smart e capacci di comunicare, si differenziano per le loro funzionalità ed i loro utilizzi.
Come per l'IoT, dato il numero relativamente esiguo di rispondenti, rispetto al totale, che hanno subito questo tipo di attacco, i dati che seguono devono essere considerati come esempi di casi specifici, e non essere presi come riferimento della situazione in Italia degli attacchi a questi sistemi.

La fig. 6.14-1 mostra che il 31,9% dei rispondenti utilizza sistemi OT, ma solo il 3,2% ha subito attacchi su di essi.
Correlando e analizzando i dati, emerge che i rispondenti che hanno rilevati attacchi a questi sistemi appartengo ai seguenti settori merceologici:

- Industria manifatturiera e costruzioni: meccanica, chimica, farmaceutica, elettronica, alimentare, edilizia, ecc. (Codici Ateco C e F)
- Trasporti e magazzinaggio (Codici Ateco H)
- Commercio all'ingrosso e al dettaglio, incluso quello di apparati ICT (Codici Ateco G)
- Servizi ICT: consulenza, produzione software, service provider ICT, gestione Data Center, servizi assistenza e riparazione ICT, ecc. (Codici Ateco J62, J63, S95.1)

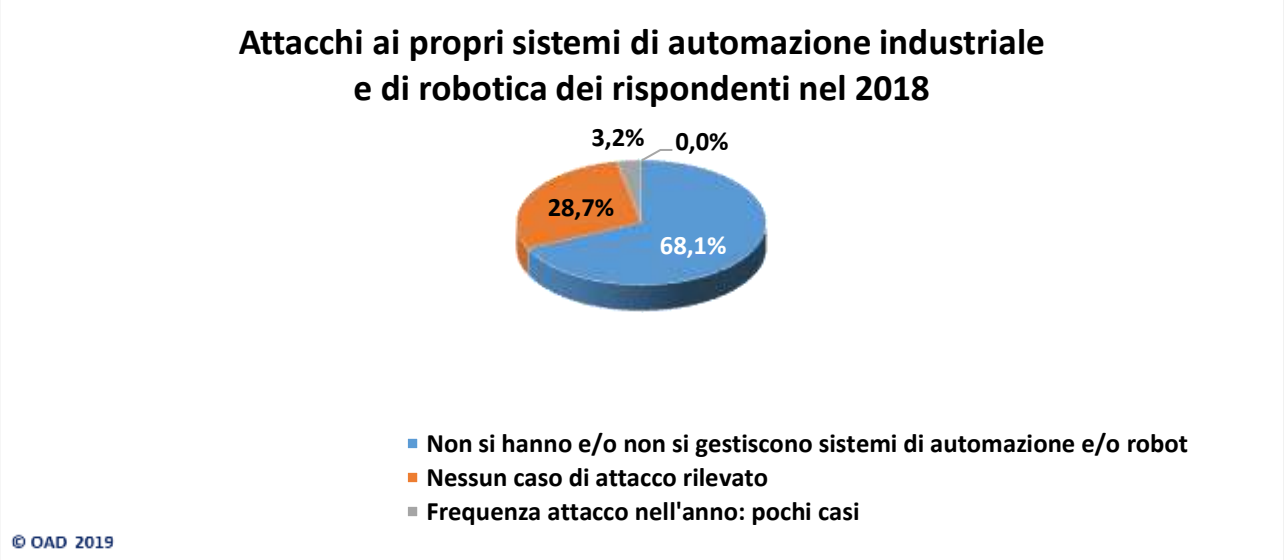

Fig. 6.14-1

La fig. 6.14-2, con risposte multiple, mostra che le tecniche di attacco più usate secondo i rispondenti che hanno subito tali attacchi sono, con il medesimo 100%, raccolta di informazioni e toolkit. Script e malware seguono al 66,7%, e a scalare, con il medesimo 33,3%, attacco fisico, botnet e APT. Stranamente gli agenti autonomi, in pratica i malware virali, non sono presenti.

Pur essendo relativamente pochi gli attacchi ai sistemi OT dei rispondenti, gli impatti sono stati tutti severi e gravi, come evidenziato in fig. 6.14-3 (con risposte multiple) e confermato nella fig. 6.14-5 sui tempi di ripristino.

La fig. 6.14-4 mostra, con risposte multiple, le possibili motivazioni degli attacchi più gravi, così come stimate dai rispondenti attaccati: il sabotaggio è al primo posto, considerato da tutti con un significativo 100%, seguito da ritorsioni/ricatti con un 66,6%. Spionaggio e hacktivism hanno il medesimo 33,3%.

La gravità degli attacchi ai sistemi OT dei rispondenti è confermata dalla fig. 6.14-5, dove 2/3 dei rispondenti riesce ad attuare il ripristino della situazione ex ante tra una settimana ed il mese, ed 1/3 tra 3 giorni ed una settimana. Nessuno riesce a ripristinare entro tre giorni

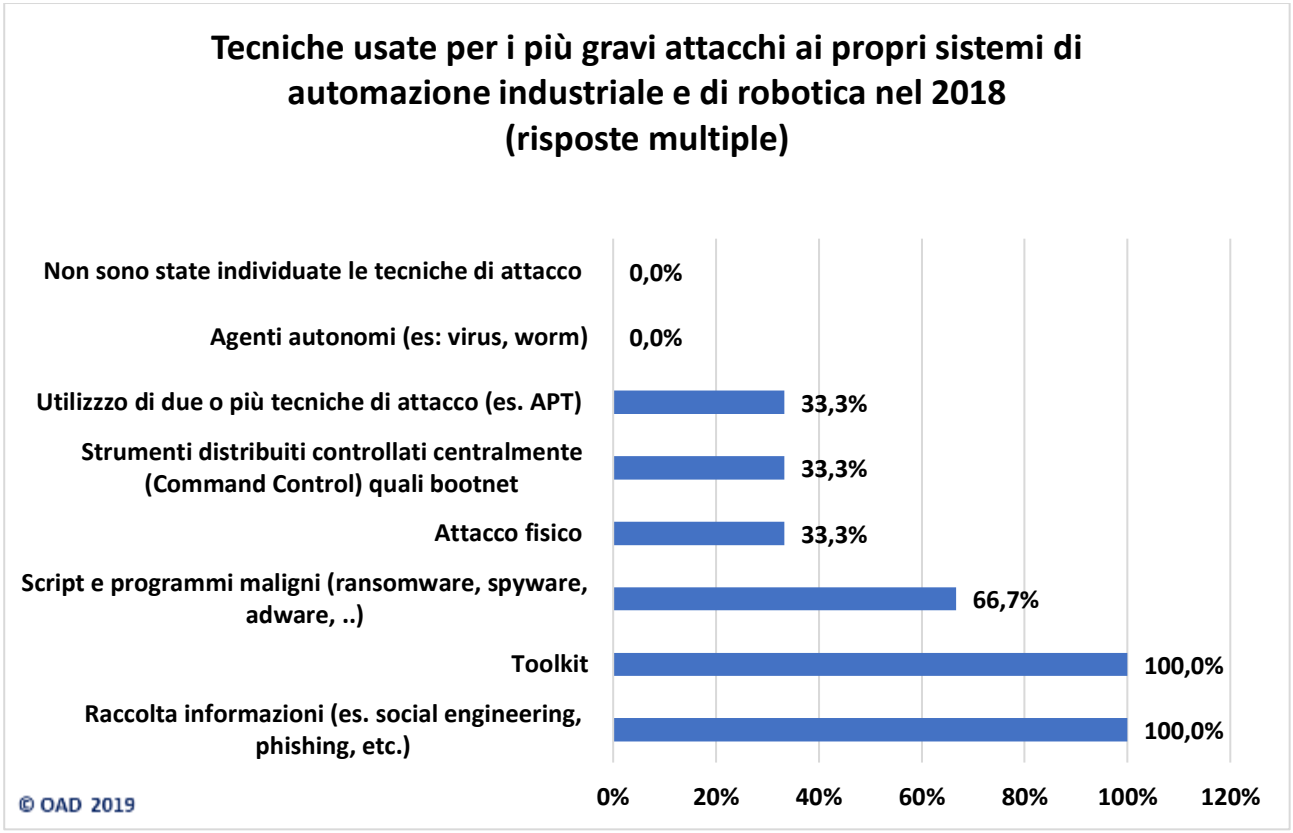

Fig. 6.14-2

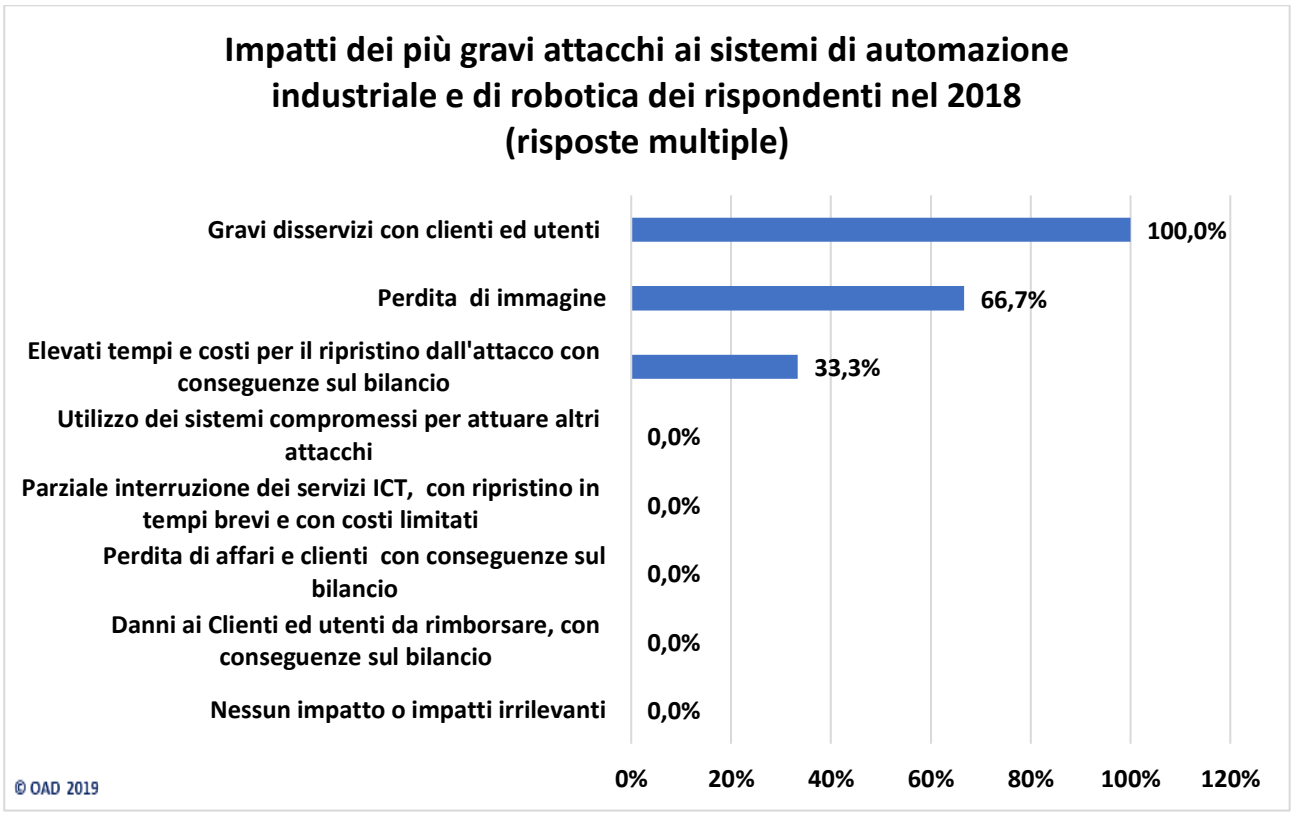

Fig. 6.14-3

Fig. 6.14-4

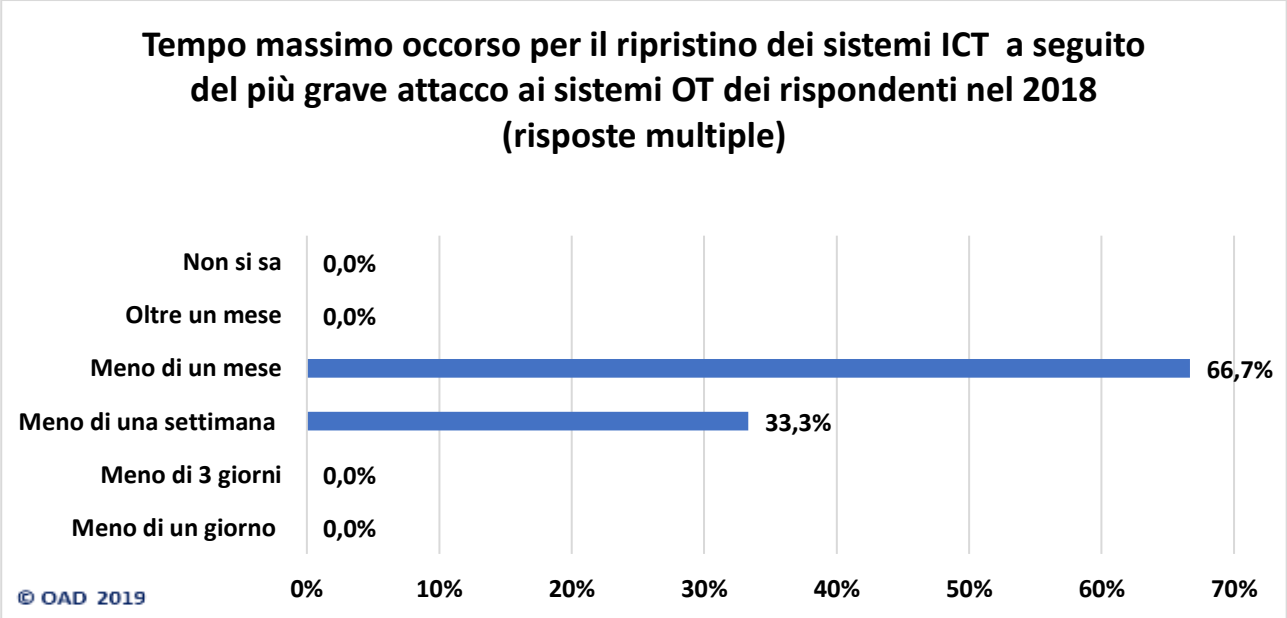

Fig. 6.14-5

6.15 Attacchi a sistemi e/o servizi basati su blockchain

La Blockchain è una tecnica introdotta nel 2008 per convalidare le transazioni e la generazione della cripto-valuta bitcoin, con l'obiettivo della libera circolazione della cripto-valuta tra gli utenti, senza o con bassi costi sulle operazioni e soprattutto senza il controllo di un organo centrale regolatore.

Questa tecnicateoricamente sicura “by design”, basata sull’elaborazione distribuita ad alta affidabilità (fault tolerance) su consolidate tecniche di moderna crittografia (KPI) e con il consenso decentralizzato, è stato poi utilizzata, personalizzandola, per diversi compiti in diversi settori, quali ad esempio la registrazione di eventi, dei record medicali, della gestione dell’identità, delle transazioni, della tracciabilità (in particolare del cibo), dell’IoT e così via.
Blockchain usa diverse tecniche crittografiche ed il suo approccio innovativo si basa sostanzialmente sull’assenza di ‘intermediari’, di un controllo centrale e sulla gestione della fiducia: la catena dei blocchi, questo il nome in italiano di blockchain, è un insieme di record (chiamati appunto blocchi), crescente (banca data distribuita), collegati tra loro e crittati.
Esistono sistemi di blockchain aperti, dove tutti possono partecipare scaricando l’opportuno programma (tipico esempio le cripto valute), e chiusi, dove solo determinati interlocutori possono partecipare: e soprattutto questi ultimi sono quelli presi in considerazione da grandi imprese ed istituzioni per implementare le loro proprie soluzioni, molte delle quali ancora in fase di prova.
Dato che anche in Italia varie aziende/enti hanno iniziato a sperimentare o ad usare tecniche di blockchain per specifiche soluzione informatiche, il questionario 2019, così come il precedente del 2018, ha considerato la blockchain come una tipologia di che cosa si attacca: ed infatti anche questa complessa tecnica è già stata attaccata, e può presentare varie vulnerabilità nelle sue diverse implementazioni ed applicazioni: la sicurezza digitale assoluta non esiste.
Come per l’IoT e l’OT, dato il numero relativamente esiguo di rispondenti, rispetto al totale, che hanno subito questo tipo di attacco, i dati che seguono devono essere considerati come esempi di casi specifici, e non essere presi come riferimento della situazione in Italia sull’uso e sugli attacchi digitali a sistemi ICT che fanno uso di blockchain.

Il 13,7% del campione dei rispondenti dichiara di usare tecniche di blockchain (fig. 6.15-1), e solo il 2,1 % di questi di aver subito degli attacchi a tali tecniche nel 2018.
Correlando ed analizzando i dati raccolti dal questionario sulla blockchain, è interessante notare che, dal bacino dei rispondenti, solo delle Pubbliche Amministrazioni hanno indicato di aver subito attacchi ai loro sistemi informatici basati su tali tecniche.

Nella fig. 6.15-2, con risposte multiple, le tecniche di attacco probabilmente usate secondo i rispondenti che hanno subito questo tipo di attacco: per la totalità dei rispondenti, 100%, sono state usate tecniche tipo APT, oltre ad agenti autonomi per il 50%. Nessuna altra tecnica di attacco è stata rilevata dai rispondenti.

Gli impatti avuti dagli attacchi più gravi (fig. 6.15-3, con risposte multiple) risentono sicuramente dall’uso ancora prototipale ed embrionale della blockchain da parte dei (pochi) rispondenti che hanno subito attacchi: infatti tutti dichiarano impatti irrilevanti o gestibili in breve tempo ed a costi bassi.

Essendo i rispondenti solo Pubbliche Amministrazioni, sono ragionevoli le possibili motivazioni per i più gravi attacchi subiti, indicate nella fig. 6.15-4, con risposte multiple: con un uguale 50%, azione dimostrativa e sabotaggio.

I tempi massimi di ripristino dei sistemi basati su blockchain dopo un attacco sono congruenti con gli impatti inesistenti o trascurabili, e con l’ipotesi che il loro utilizzo sia ancora prototipale, come mostrato in fig. 6.15-5: tutti i rispondenti sono riusciti a ripristinare i sistemi entro un solo giorno.

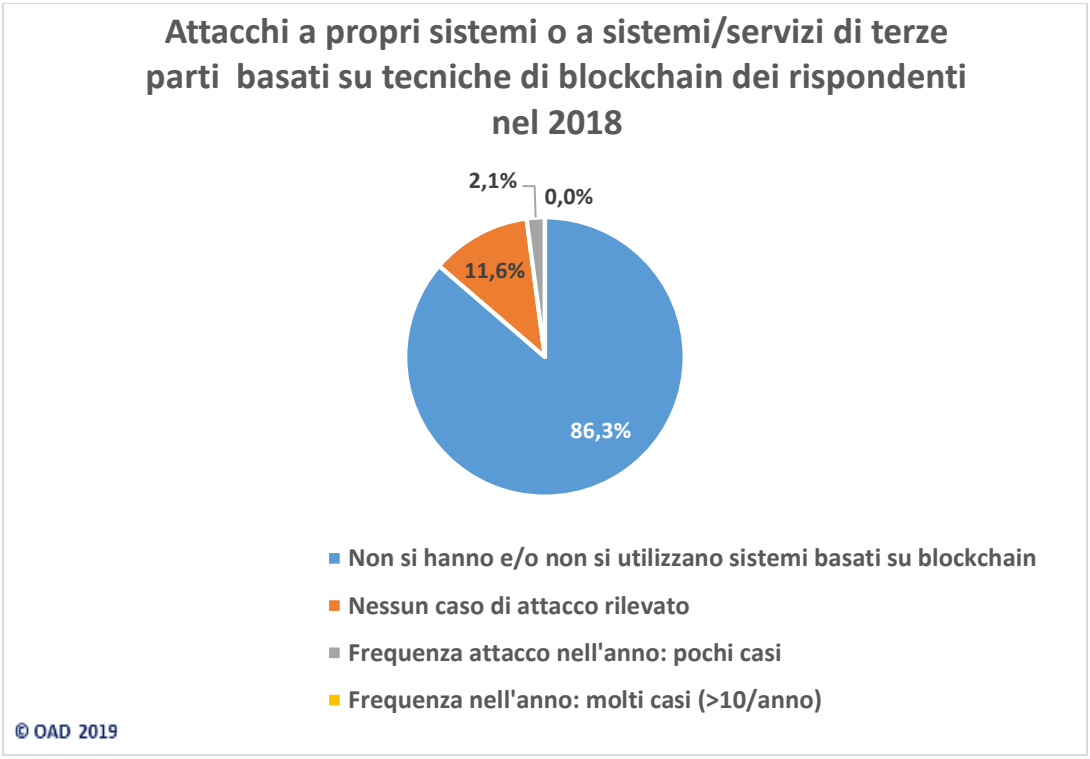

Fig. 6.15-1

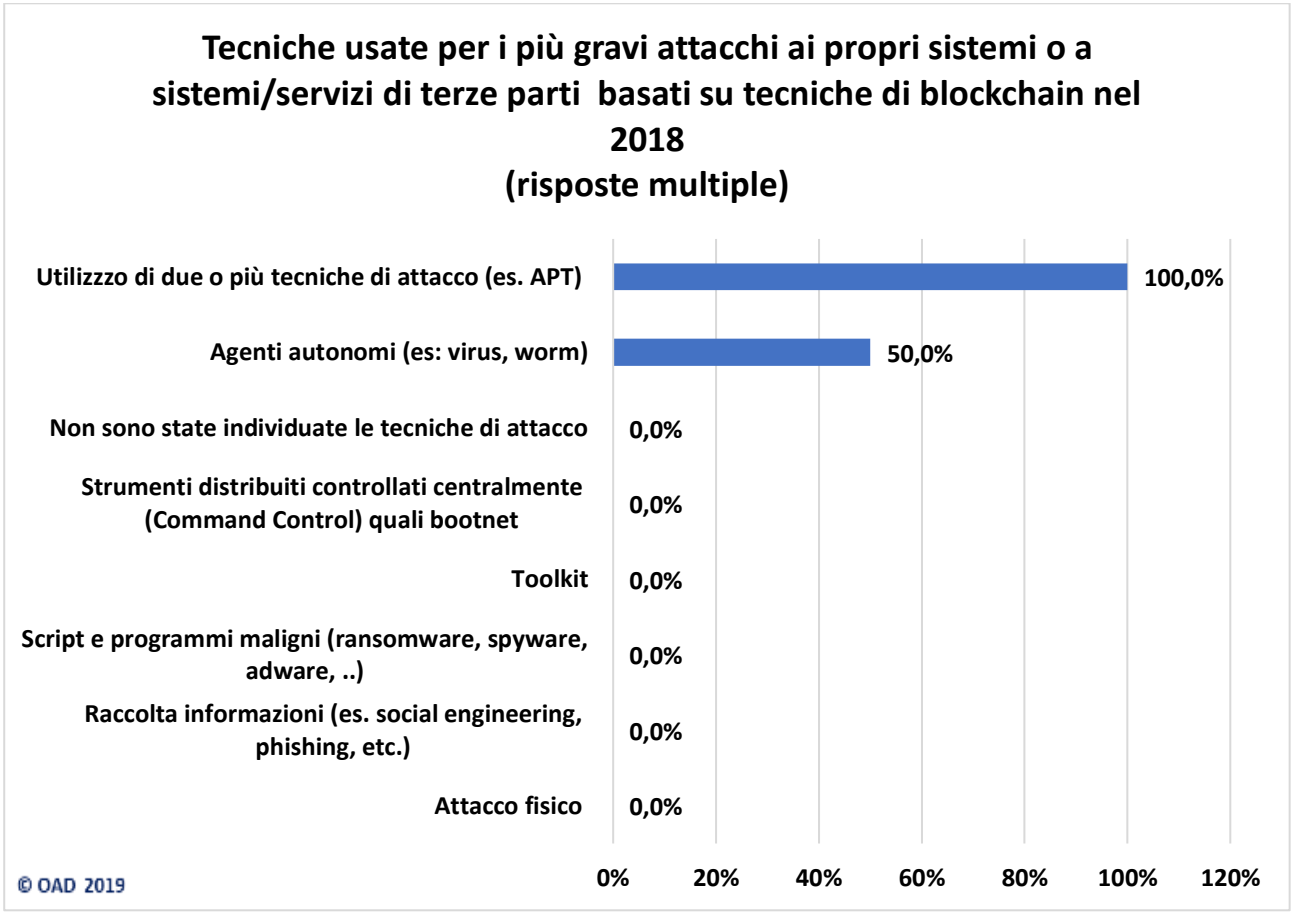

Fig. 6.15-2

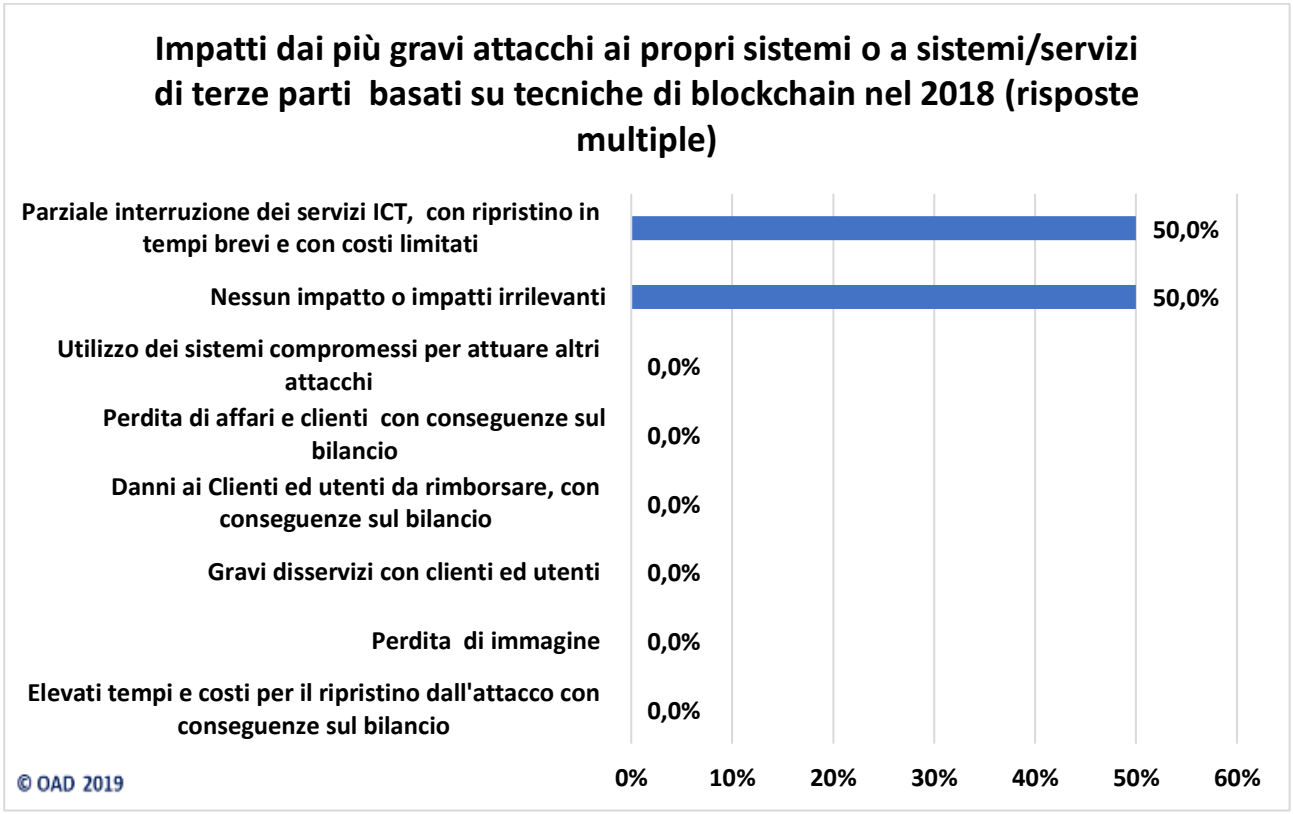

Fig. 6.15-3

Fig. 6.15-4

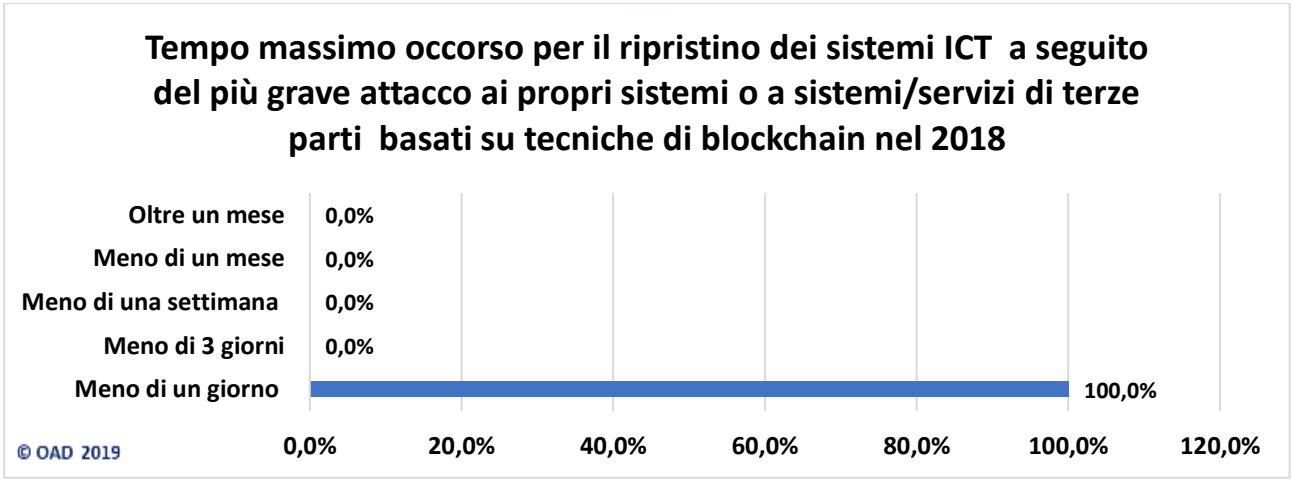
Tempo massimo occorso per il ripristino dei sistemi ICT a seguito del più grave attacco ai propri sistemi o a sistemi/servizi di terze parti basati su tecniche di blockchain nel 2018
Oltre un mese
Meno di un mese
Meno di una settimana
Meno di 3 giorni
Meno di un giorno
0,0%
0,0%
0,0%
0,0%
100,0%
© OAD 2019
0,0%
20,0%
40,0%
60,0%
80,0%
100,0%
120,0%

Fig. 6.15-5

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

Un insieme delle domande del questionario 2019 era rivolta a comprendere come e da chi vengono rilevati gli attacchi digitali e come sono gestiti.
La fig. 7-1, con risposte multiple, mostra la provenienza delle segnalazioni di un attacco che è concettualmente simile a quella rilevata in OAD 2018: per il campione dei rispondenti, il 31,9% delle segnalazioni arriva dagli utenti privilegiati interni (amministratori di sistema, operatori ICT, etc.) ed il 21,8% dagli utenti finali interni. Positivamente, 18,6% arriva dai sistemi di monitoraggio e controllo del sistema informatico ed il 10,6% dall'analisi dei dati, in particolare dei log di sistema. Relativamente bassa, 10,1% Segue con circa il 20% la segnalazione da parte degli operatori ICT esterni. Con percentuali decrescenti, seguono l'evidenza del danno a seguito dell'attacco ed infine, per fortuna ultimo, la segnalazione da parte di utenti esterni.

L'eventuale comunicazione all'esterno dell'azienda/ente dell'avvenuto e rilevato attacco, con risposte multiple, è indicata nella fig. 7-2. Più di ¼ dei rispondenti non comunica all'esterno per i motivi elencati in fig. 7-3. Poco meno di 1/4, il 23,7%, lo comunica ai propri fornitori e consulenti, così che gli esperti/addetti ai lavori possano intervenire per ripristinare la situazione ex ante, e comunque capire le ragioni e l'origine dell'attacco, quali contromisure non sono state sufficienti, come migliorare il livello di sicurezza digitale. Solo il 17,6% lo comunica alle autorità competenti, tipicamente alla Polizia Postale. Il 7,6% lo comunica alla propria assicurazione, il che significa che con essa ha assicurato il suo rischio informatico. Il 6,9% dichiara di comunicarlo all'Autorità Garante, in quanto l'attacco ha riguardato (anche) dati personali, così come richiesto dal regolamento europeo sulla privacy, il GDPR, in caso di "data breach" su dati personali.
Una percentuale piccola, 5,3%, ma non trascurabile, informa dell'attacco centri specializzati tipo Cert (si veda Allegato E2). Nella voce "Altro" alcuni rispondenti hanno indicato che la comunicazione è stata inviata alla Capogruppo/Holding cui appartiene la loro società, a studi legali, alla stampa.

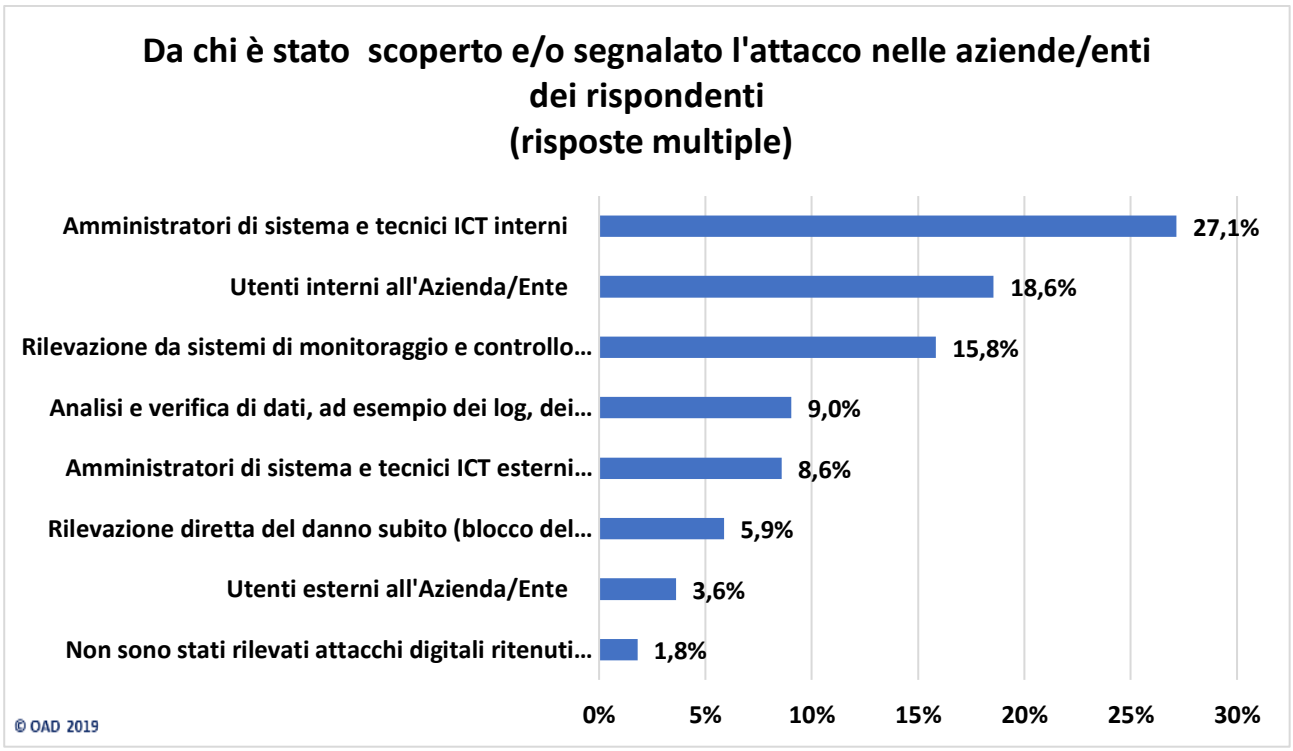

Fig. 7-1

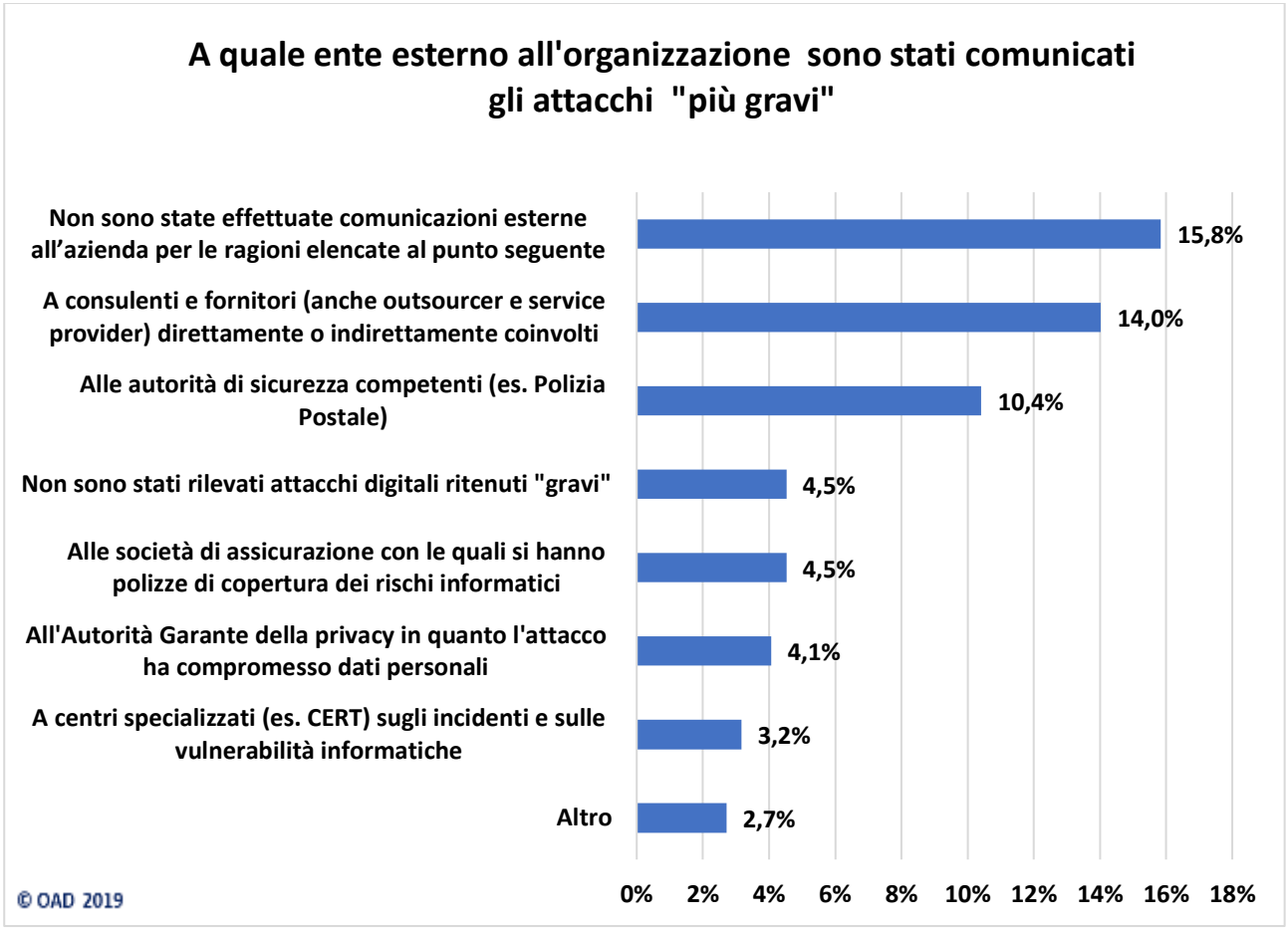

Fig. 7-2

Come indicato nella fig. 7-3, con risposte multiple, il motivo principale della non comunicazione dell'attacco, con un 63,4%, è esso era troppo poco significativo e, probabilmente, con impatti nulli o trascurabili. Al secondo posto, con un 16,8%, la tutela dell'immagine dell'azienda/ente. L'9,9% dichiara che il motivo è la policy di confidenzialità dell'azienda/ente, che non consente l'effettuazione di comunicazioni all'esterno: policy che con il GDPR, e soprattutto con il buon senso, dovranno essere profondamente modificate. Un 6,9% non lo ha comunicato per non fornire, direttamente o indirettamente, informazioni sulle vulnerabilità e sulle misure di sicurezza digitali in atto.
Un irrisorio, ma preoccupante, 3,0% per la mancanza di conoscenza dell'esistenza di autorità preposte: anche a livello di PMI e piccole strutture pubbliche, ancora non si conoscono ruoli e obblighi verso il Garante e la Polizia Postale?

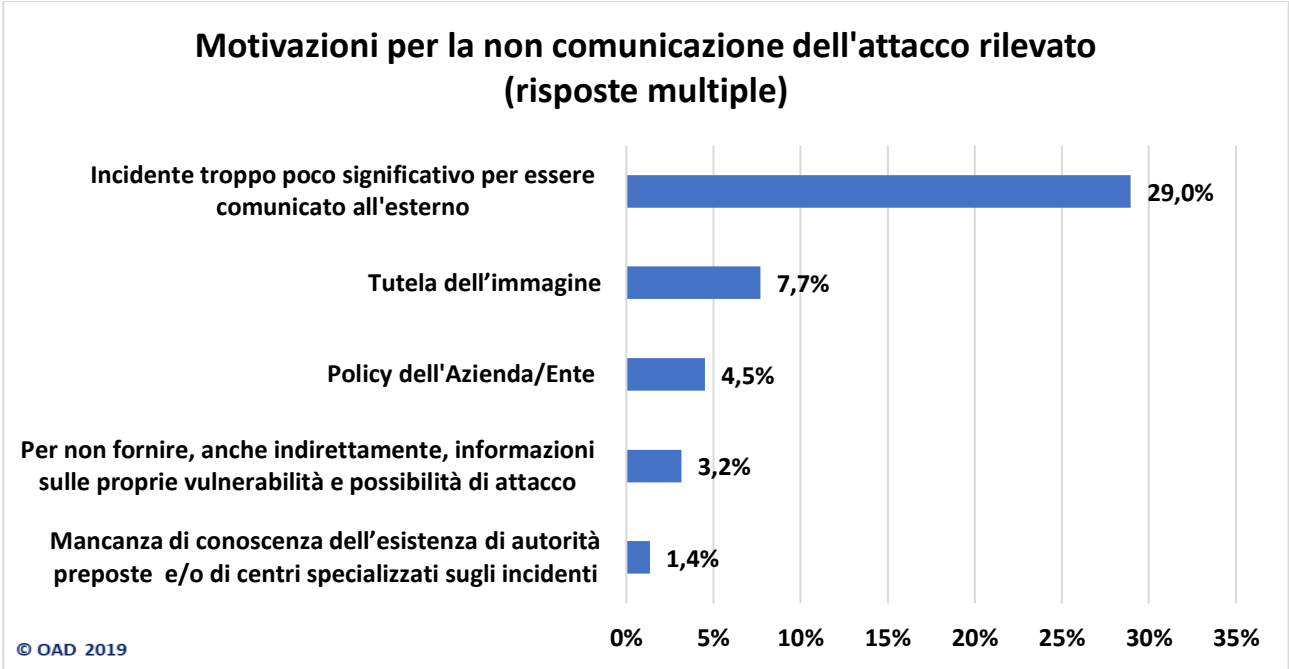

Fig. 7-3

Le azioni intraprese dalle aziende/enti rispondenti dopo aver subito un attacco, a parte la comunicazione ad enti esterni sopra trattata, sono mostrate nella fig. 7-4, con risposte multiple. Tali azioni sono tra le principali per una efficace ed efficiente gestione del "dopo attacco". I due interventi con le più alte percentuali sono l'attivazione di indagini, 20,7% e l'aggiornamento dei software vulnerabili, 20,3%.
Seguono a scalare l'eliminazioni/sostituzione delle risorse ICT non sufficientemente sicure, 13,5%, la messa in produzione di nuovi strumenti per rafforzare la sicurezza digitale, 13,1%, il miglioramento delle policy e delle procedure organizzative, 11%. A decrescere, sotto il 10%, altri interventi: l'attuazione di corsi di formazione, sensibilizzazione e addestramento per gli utenti finali e privilegiati, l'attuazione di un Piano di Disaster Recovery (ma solo per il 2,5%), l'attivazione di legali, di investigatori privati e di consulenti di sicurezza digitale. Infine, per solo un 1,3%, l'attivazione di polizze assicurative sul rischio informatico. Nella voce "Altro" i rispondenti hanno segnalato il rimpiazzo dei dispositivi ICT rubati, ed un rispondente in particolare la forte riduzione dei dati residenti sui PC portatili e la stessa loro riduzione, assegnandone il meno possibile.

Al terzo posto come diffusione, con il medesimo 26,45% di diffusione, l'introduzione di ulteriori strumenti di sicurezza digitale ed il miglioramento delle policy e delle procedure organizzativa per la sicurezza digitale. Seguono poi intorno al 20% la sostituzione di dispositivi ICT vulnerabili e la formazione e l'addestramento sia degli utenti finali sia degli utenti privilegiati. Per la sicurezza digitale ed il suo governo è fondamentale la sensibilizzazione e la formazione continua oltre che lo specifico addestramento per saper usare in maniera sicura gli strumenti informatici utilizzati.
Con percentuali sempre più basse gli altri interventi considerati nel questionario, con risposte multiple. Nella voce "altro" è stato specificato da alcuni rispondenti il rimpiazzo dei dispositivi ICT rubati e le modifiche di configurazione del software di base ed applicativo, per renderlo più sicuro.

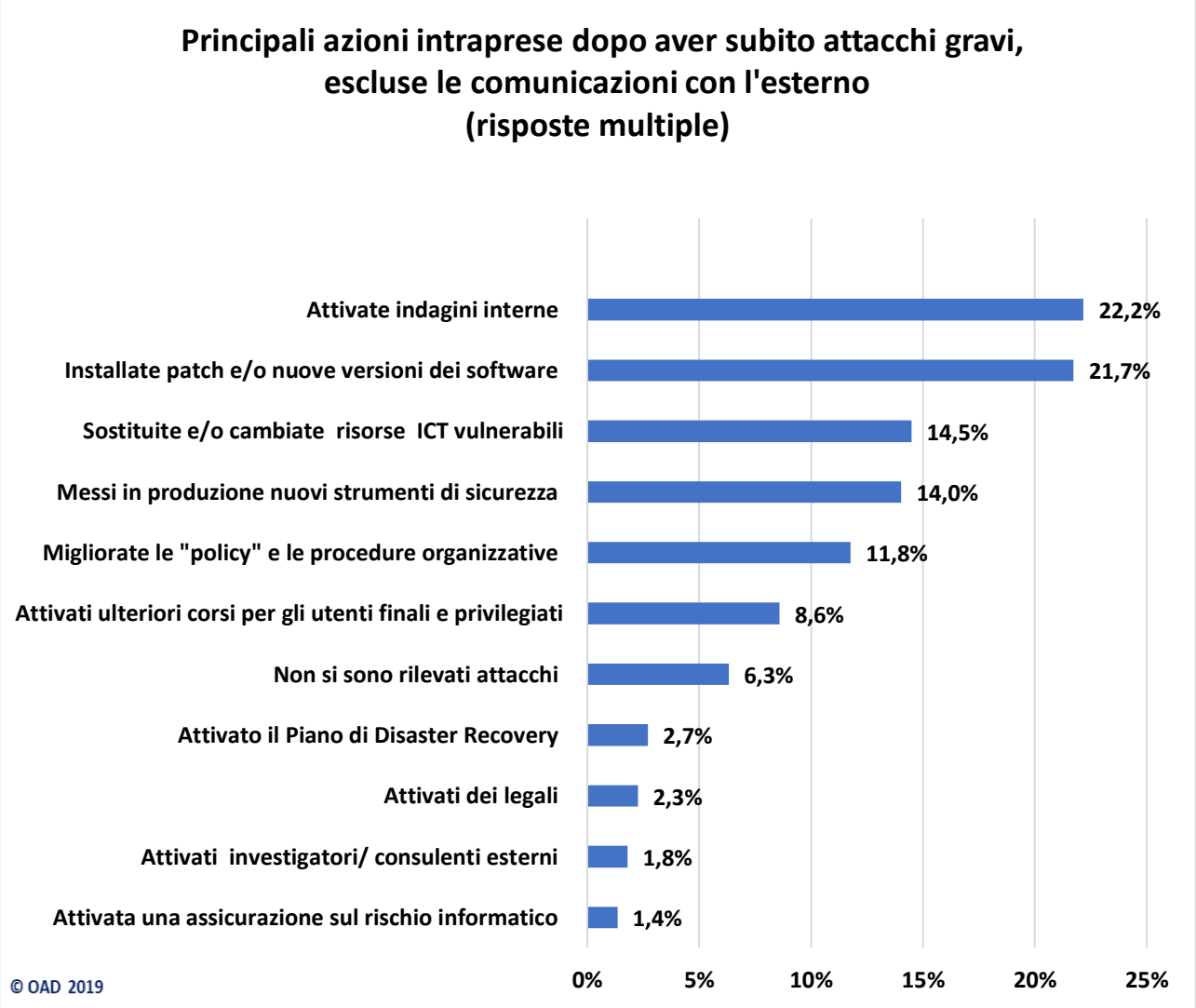

Fig. 7-4

7.1 L'impatto economico degli attacchi subiti

In termini di impatto, il danno economico causato da un attacco è l'elemento determinante: ogni tipo di danno, da quello del disservizio a quello di immagine, dal tempo uomo speso per rimediare ai nuovi eventuali strumenti da utilizzare, può essere valorizzato in termini economici. Come per l'impatto richiesto per ogni tipologia di attacco, anche per il danno economico è stata lasciata libertà al rispondente di considerarlo e stimarlo secondo le sue abitudini e prassi.
Nei paragrafi del Capitolo 6 si sono riportati, per ogni tipologia d'attacco, gli impatti causati al sistema informatico e/ all'intera organizzazione dall'attacco più grave. Volutamente, per ogni tipologia d'attacco, non si è chiesto il danno economico per il più grave attacco subito di quel tipo, per non rendere troppo lunga, e difficile, la compilazione del questionario. Si è preferito chiedere in questa sezione, e senza rendere obbligatoria la risposta: la stima del costo complessivo degli attacchi per l'intero anno e/o il costo economico dell'attacco più grave, indipendentemente dalla sua tipologia. Come nelle edizioni precedenti, in pochi hanno risposto e con valori molti differenti, anche per le diverse loro dimensioni, fatturati e settori merceologici: e magari anche per l'inserimento di dati errati. Essendo il questionario assolutamente anonimo, non ci sono possibilità di verifica dell'attendibilità di dati che risultano fortemente anomali rispetto a quelli degli altri rispondenti.

Alcuni rapporti internazionali forniscono indicazioni sui costi complessivi degli attacchi digitali / data breach subiti, evidenziando la difficoltà, per le aziende/enti, di considerare tutti i costi diretti, indiretti e consequenziali. Il Ponemon Institute, ad esempio, in una sua recente indagine per conto di IBM[18], valuta per le aziende italiane (di grandi dimensioni) un costo complessivo per data breach di 3,52 Mlni US$, ed un costo medio di $ 146 per record compromesso. Per le aziende italiane considerate, Ponemon ha rilevato che un data breach dell'azienda/ente attaccato.

La fig. 7.1-1, con risposte multiple, mostra le risposte sulla valutazione dell'impatto economico degli attacchi subiti. Il primo significativo dato è che quasi i 2/3 dei rispondenti dichiarano di non poter o di non essere in grado di fornire valutazioni economiche sugli attacchi subiti. Dato che non dipende solo dalla maggioranza dei rispondenti appartenenti a piccole strutture organizzative: anche strutture medie, grandi e grandissime non sono in grado, o non vogliono, valutare il costo complessivo che l'attacco subito ha comportato. Il 14,9% dichiara che non ha subito significati danni economici per gli attacchi subiti, ed il 14,5% che non ha rilevato alcun danno economico.

Nella medesima domanda del questionario veniva inoltre richiesto di indicare la stima del costo di tutti gli attacchi subiti nel 2018, ed il costo dell'attacco più grave e a maggior costo subito.
Come indicato in figura, solo l'8,1% ha risposto alla prima domanda, e, stranamente, solo il 3% ha fornito la stima del costo del singolo attacco più grave.
Nel primo caso, il costo complessivo di tutti gli attacchi, una Pubblica Amministrazione Centrale (PAC) ha indicato una cifra molto più alta di tutti gli altri, € 1.500.000,00, anche se più vicina alla valutazione del Ponemon Institute di cui sopra. La media aritmetica di tutti gli altri rispondenti che hanno fornito queste stime, esclusa la PAC di cui sopra, porta ad un valore di € 187.850,00 per anno per azienda/ente.
Nel secondo caso, il costo complessivo rispetto al singolo più grave attacco subito, la cifra più alta emersa è di € 80.000, e la media aritmetica tra chi ha indicato una stima del costo più elevato è di € 17.700. Si noti che la PAC che ha indicato il più alto valore complessivo di tutti gli attacchi nell'anno, non ha indicato il costo più alto del singolo attacco più critico: e questo rende meno credibile l'alto valore di cui sopra.

La fig. 7.1-2 mette in relazione le risposte avute per l'impatto economico degli attacchi nel 2018 con le dimensioni dell'azienda/ente, dimensioni in termini di numero di dipendenti. Come per l'anno precedente, i dati emersi sfatano il fatto che solo le strutture di grandi dimensioni sono attente e capaci di rilevare i danni economici: i vari rispondenti appartengono ad aziende/enti di ogni dimensione, incluse le più piccole.

[18] 2019 Cost of a Data Breach Report

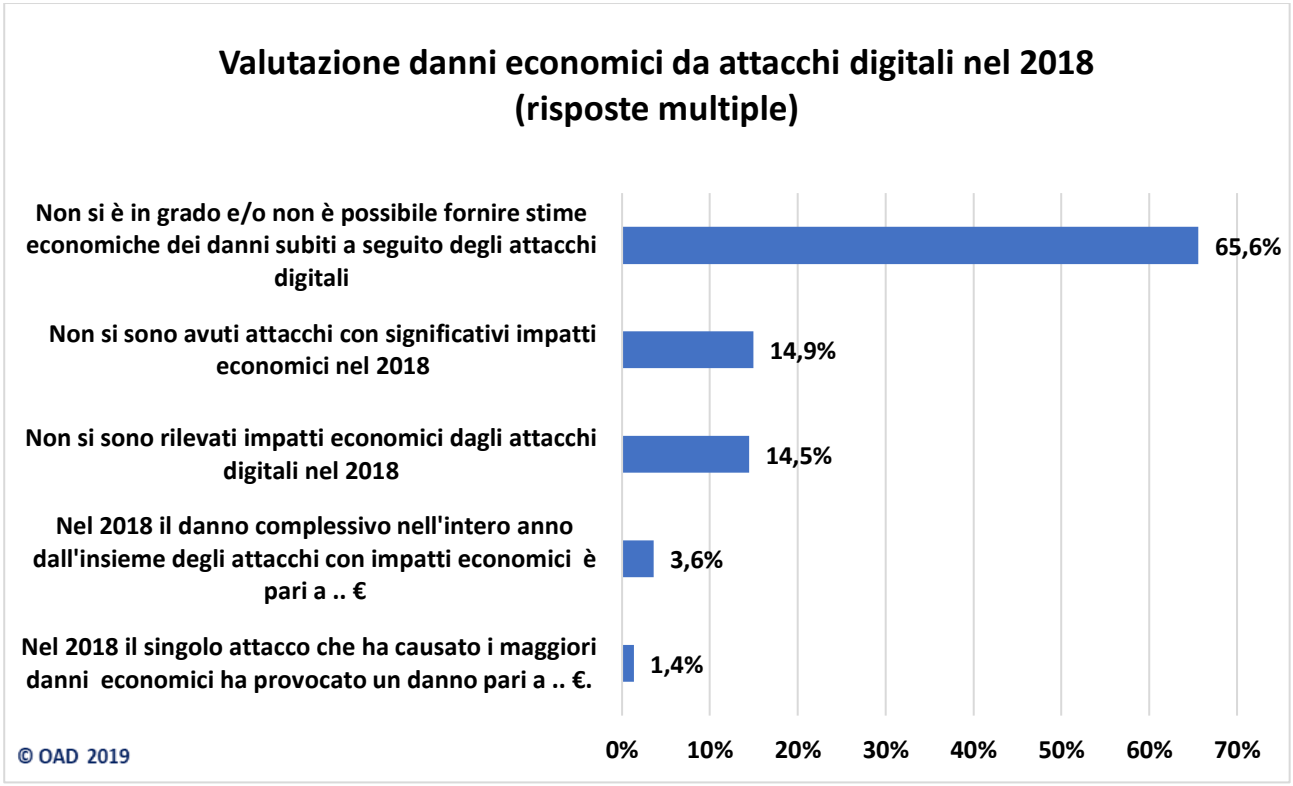

Fig. 7.1-1

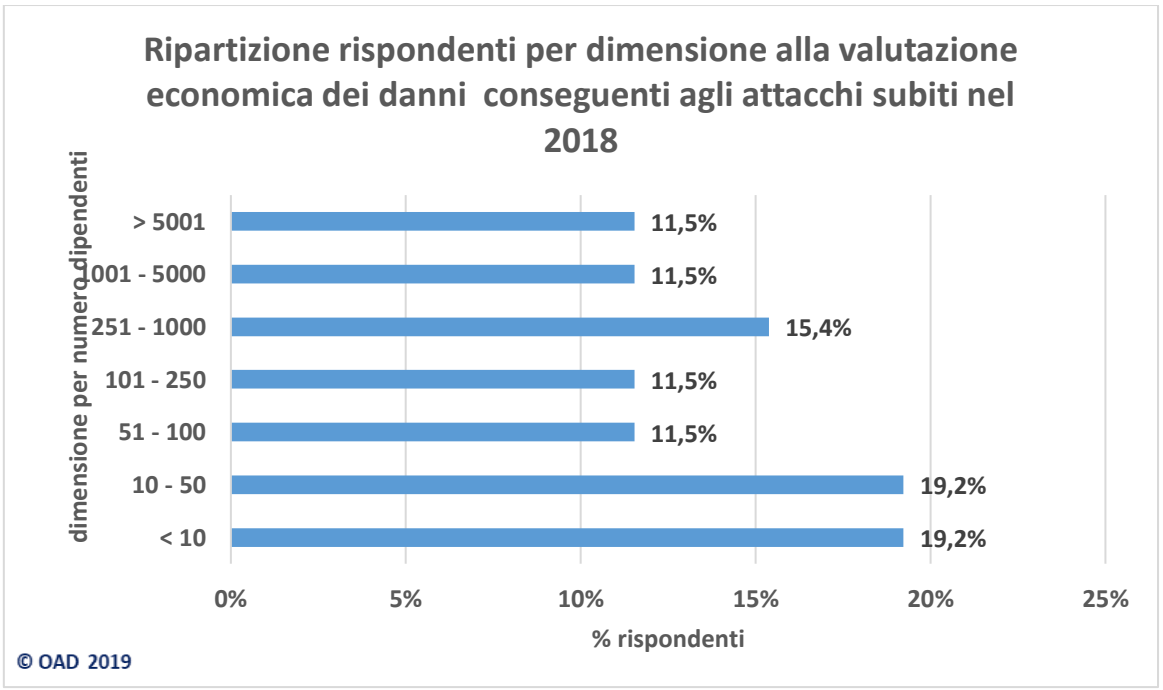

Fig. 7.1-2

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

La fig. 8-1, basata sulle risposte multiple dei rispondenti, mostra quali sono le tipologie di attacco (che cosa) ritenute più pericolose, e quindi più temute nel prossimo futuro, indipendentemente dagli attacchi eventualmente subiti.

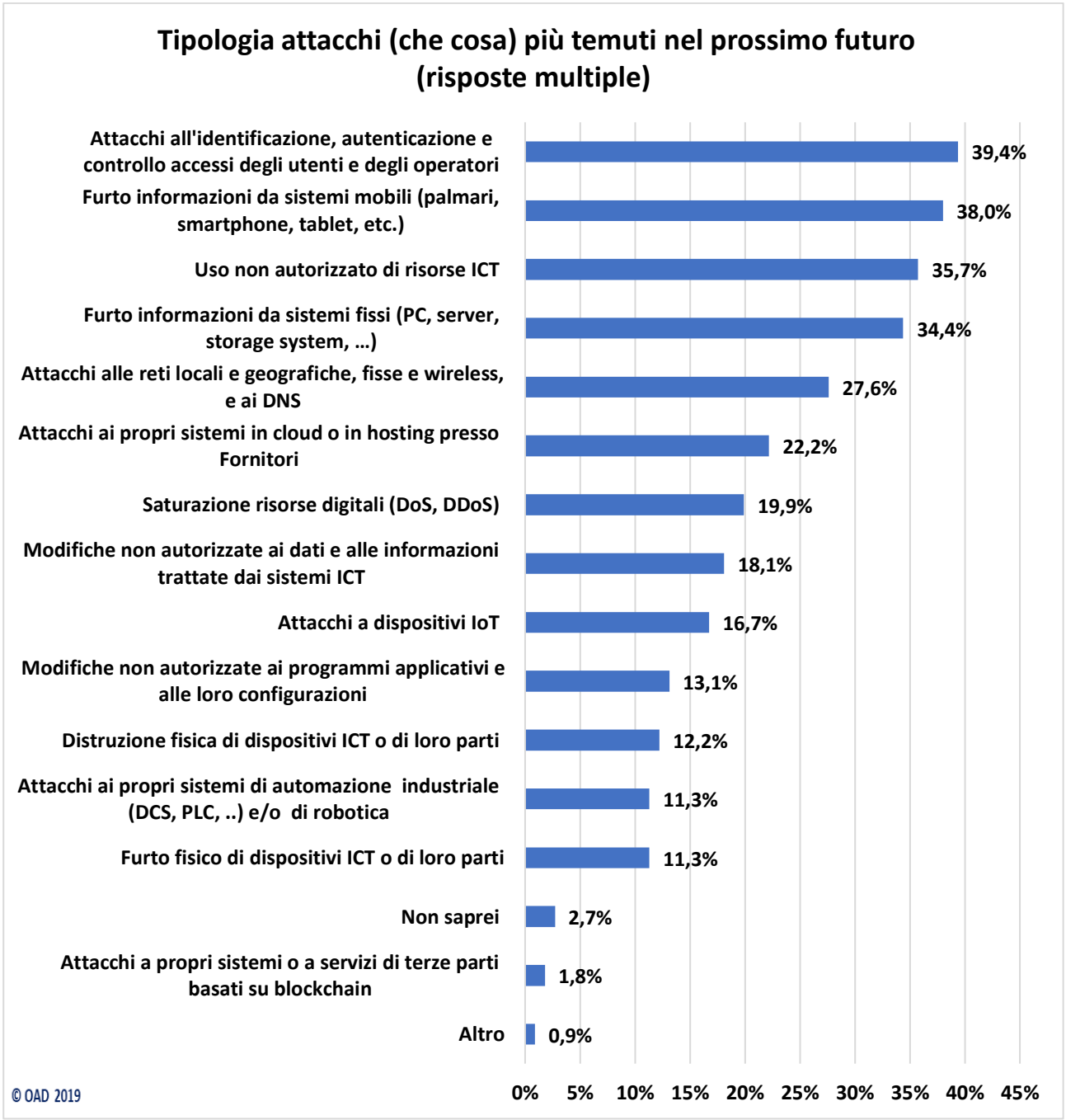

Fig. 8-1

Anche in questo caso, come per le domande sugli impatti in ogni tipologia d'attacco del Cap. 6, non si è volutamente specificato quali sono i criteri per considerare un attacco più pericoloso e critico,

lasciando libertà al rispondente (sempre strettamente anonimo) di rispondere secondo il suo giudizio e la sua esperienza.
Come è ragionevole aspettarsi e come si è verificato anche nelle precedenti indagini di OAD/OAI, rimangono per il futuro forti timori per alcuni degli attacchi più diffusi rilevati nell'ultimo anno considerato, il 2018 (si veda fig. 6-7). Rispetto alle indagini precedenti, la fig. 8-1 mostra una distribuzione di risposte sulle varie tipologie di attacco, sempre a scalare ma con pochi punti percentuali. Non c'è una singola tipologia di attacco che emerga prepotentemente, ma le preoccupazioni sono distribuite su tutte le varie tipologie, pur considerando che la maggior parte dei rispondenti sono PMI, quindi più attente ai più comuni e diffusi attacchi. La fig. 8-1 fornisce quindi una chiara indicazione di come gli attacchi cibernetici, almeno tra i rispondenti al questionario dell'indagine 2019, indipendentemente dalla loro tipologia, sono sempre più critici, più articolati e più temuti.
Al primo posto, con un 39,4% gli attacchi a IAA, cui seguono a brevissima distanza percentuale, e con decrementi tra l'uno e l'altro, il furto di informazioni da sistemi mobili (un serio e perdurante problema per la sicurezza digitale di quasi tutte le aziende/enti), l'accesso ed uso non autorizzato ai sistemi ICT, il furto di informazioni da sistemi ICT fissi. Con maggior distacco percentuale gli attacchi alle reti, l'attacco ai propri sistemi terziarizzati, Sotto il 20%, è bene evidenziare il DoS/DDoS e gli attacchi ai sistemi IoT. Sotto "Altro" alcuni rispondenti hanno specificato il timore di attacchi ai sistemi elettromedicali, alle reti ad altissima velocità, e ai sistemi VoIP.

La fig. 8-2, con risposte multiple, mostra le tecniche di attacco ritenute più temute nel prossimo futuro dai rispondenti.

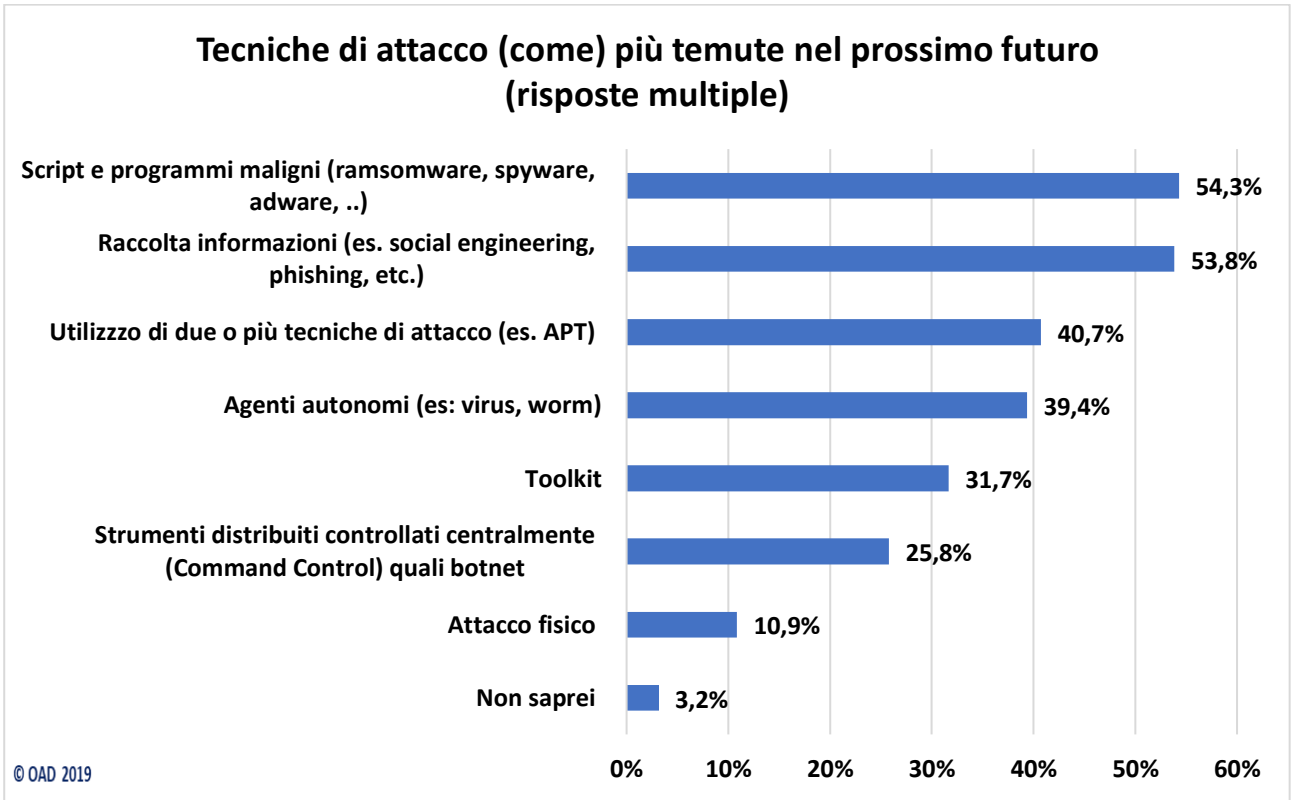

Fig. 8-2

Le due tecniche di attacco più temute, con percentuali assai prossime, sono, ragionevolmente, gli script-malware ed il social engineering, le due tecniche più diffuse negli attacchi rilevati nel 2018, come indicato in fig. 6-8. All'ultimo posto l'attacco fisico.

La fig. 8-3, con risposte multiple, mostra le principali motivazioni ipotizzate per i futuri attacchi: la frode è di gran lunga la motivazione più votata, cui seguono, con percentuali tra loro vicine ma che sono circa la metà della frode, il sabotaggio e la ritorsione. Seguono, decrescendo, le altre possibili motivazioni, e all'ultimo si posiziona il terrorismo. Con "Altro" alcuni rispondenti indicano la cattura di informazioni, senza specificare il perché: assai probabilmente per rivenderle o usarle per ulteriori attacchi.

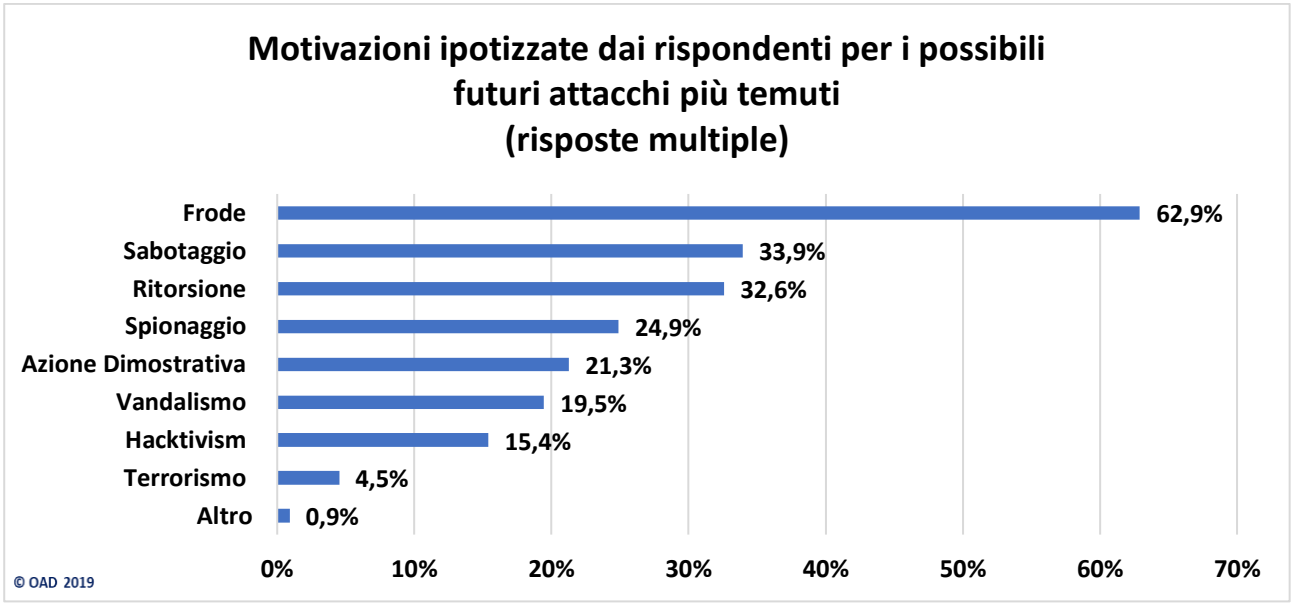

Fig. 8-3

9 Strumenti e misure di sicurezza ICT adottate nelle aziende/enti dei rispondenti

Il seguente capitolo descrive gli strumenti di sicurezza in uso nei sistemi informatici, le cui macro-caratteristiche descritte in §10.3, delle aziende/enti dei rispondenti, così da poter meglio comprendere in quali ambiti e con quali livelli di sicurezza di contrasto sono stati attuati gli attacchi rilevati e di cui al Capitolo 6. Gli strumenti e le misure per la sicurezza digitale sono raggruppati in tre sezioni: misure organizzative, misure tecniche, misure per il governo ("governance") della sicurezza digitale.
Le misure di gestione sono un mix di misure organizzative e di strumenti tecnici: l'attribuzione di alcune misure in quale sezione, sempre discutibile, è stata effettuata dall'autore nell'ottica di una maggior chiarezza concettuale e sulla base della sua esperienza.

9.1 Misure organizzative per la sicurezza digitale

Gli aspetti organizzativi sono determinanti per l'attuazione e la gestione di una effettiva ed efficace sicurezza digitale, dato che le maggiori vulnerabilità, e le più difficili da eliminare o ridurre, sono proprio quelle delle persone e delle organizzazioni.
Gli aspetti organizzativi sono talvolta trascurati, soprattutto dalle piccole strutture, perché considerati prevalentemente come burocrazia e/o di interesse solo per le grandi e grandissime organizzazioni.
Le misure organizzative considerate nel questionario OAD includono la struttura organizzativa per la sicurezza digitale interna all'azienda/ente, il suo posizionamento nell'organigramma complessivo, l'esistenza di policy e di procedure organizzative, i ruoli, le competenze e le certificazioni richieste all'interno della struttura ed ai fornitori ICT, le best practice e gli standard seguiti, la sensibilizzazione, formazione e addestramento sia degli utenti finali sia degli utenti privilegiati interni ed esterni (operatori ed amministratori di sistema, sviluppatori software, manutentori sistemi ICT, system integrator, etc.), attività di audit interno e/o esterno.
Il regolamento europeo per la privacy, il GDPR, richiede l'attuazione di gran parte delle misure organizzative considerate, e l'obbligatorietà della conformità ad esso, in vigore dal 25/5/2018 per tutte le aziende/enti della Comunità Europea, con le relative salatissime multe in caso di inadempienza[19], 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 dalla risposte conferma che le aziende/enti del campione, pur diversificato, rappresentano anche in questa edizione, come nelle precedenti, una fascia medio-alta nel contesto italiano per quanto riguarda la sicurezza digitale e la sua gestione, 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 dato e stanno dando i loro frutti. Ma le percentuali rilevate sono ancora basse, a giudizio dell'autore, e molta strada deve essere ancora fatta per attivare le misure necessarie per un sistematico e corretto uso della sicurezza digitale, oltre che per una reale conformità al GDPR.

Nei paragrafi seguenti si notano delle percentuali talvolta non minimali di "Non si sa". A giudizio dell'autore, questo dipende da chi ha risposto al questionario (si veda §10.1): sovente se è un tecnico non conosce molto degli aspetti organizzativi.
Inoltre, correlando i dati sull'organizzazione con quelli delle dimensioni dell'azienda/ente dei rispondenti (troppo poche le risposte per molti settori tecnologici, pertanto si è preferito fare riferimento alle dimensioni come numero di dipendenti, che sono note e comuni per tutti i

[19] 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)

rispondenti), si evince che le mancanze organizzative riguardano in percentuale prevalentemente le organizzazioni piccole e piccolissime, come è d'altronde facilmente immaginabile.

9.1.1 La struttura organizzativa per la sicurezza digitale interna all'azienda/ente

Il ruolo centrale per la sicurezza digitale e la sua gestione è quello del responsabile della sicurezza digitale, indicato con l'acronimo inglese di CISO, Chief Information Security Officer, acronimo che sarà nel seguito usato.
Come si evince dalla fig. 9.1.1-1, il 41,2% non ha formalizzato il ruolo, ma questo viene di fatto attuato in vari modi, come dettagliato nella fig. 9.1.1-2. 1/3 dei rispondenti ha formalizzato il ruolo di CISO (ossia ufficializzato con una lettera di incarico, avente una posizione nell'organigramma e uno specifico mansionario), ed anche in tal caso espletato in modi differenti, mostrati nella fig. 9.1.1-3.
Ma per meno di un quarto delle organizzazioni dei rispondenti, il ruolo di CISO non è definito e nemmeno espletato da una qualche specifica figura professionale interna o esterna. Questo significa che le sue mansioni sono di volta in volta espletate da qualcuno che può cambiare a seconda dei casi.
Interessante l'indicazione in "Altro": alcuni dei rispondenti, essendo società di consulenza e servizi di sicurezza digitale, hanno vari specialisti con competenze anche di CISO, che le espletano anche per taluni loro clienti.

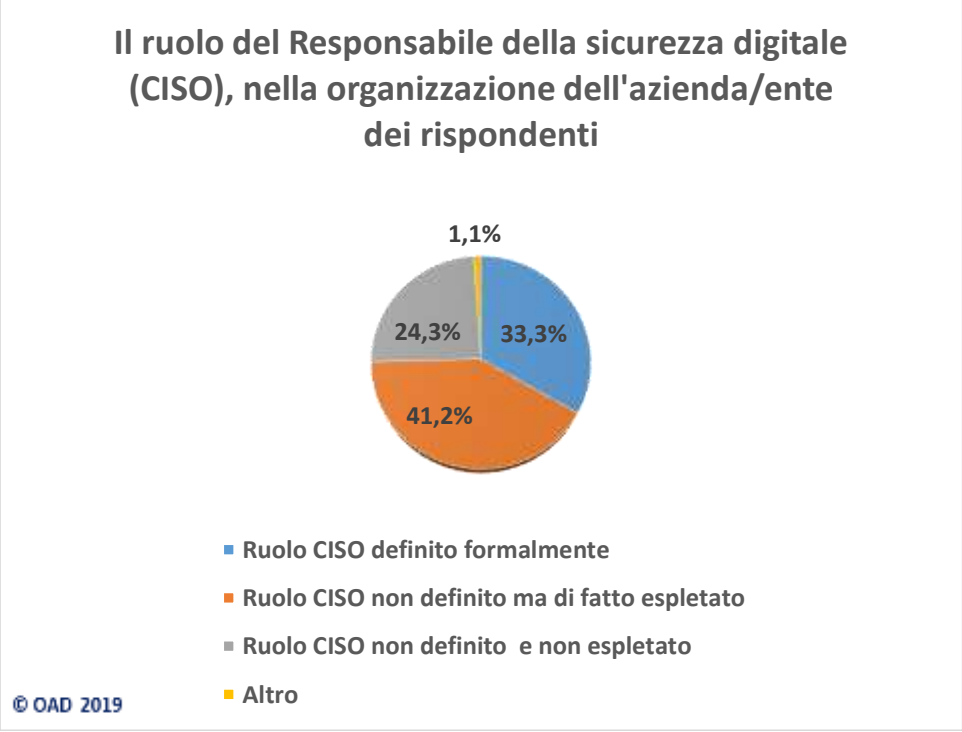

Fig. 9.1.1-1

Per le aziende/enti che non hanno formalizzato il ruolo del CISO, la fig. 9.1.1-2 mostra a quale altra figura dell'organizzazione viene affidato e di fatto svolto. Per quasi la metà dei rispondenti il ruolo è de facto assunto dal CIO, e per il 23,3% è terziarizzato. Questo dato è importante in quanto assai più alto di quello rilevato nelle precedenti indagini OAD, ed indice che, correttamente, le aziende/enti che non possono avere tali competenze all'interno, le terziarizzano. Con uguale percentuale, il ruolo

non formalizzato del CISO è svolto da personale della struttura UOS, e solo dal 5,5% e svolto internamente da personale di altre strutture dell'azienda/ente, non dell'UOSI.

La fig. 9.1.1-3 dettaglia, per i rispondenti che hanno indicato l'esistenza del ruolo formalizzato del CISO nella loro struttura organizzativa, da chi esso viene svolto. Nel 50,8% dei casi il ruolo è espletato da una persona all'interno dell'UOSI, e nel 23,3% dei casi è svolto direttamente dal CIO, la figura di vertice dell'UOSI. In questa struttura organizzativa, quindi il CISO è collocato per il 71,2% dei rispondenti. Il 13,6% dei rispondenti ha il ruolo di CISO, in altre strutture interne (ad esempio nell'ambito della struttura del CSO o in staff alla Direzione Generale), e per le aziende facenti parti di holding questo ruolo è svolto nell'ambito della struttura organizzativa della holding stessa (10,2%). Solo per il 5,1% il ruolo del CISO viene terziarizzato a consulenti o società specializzate.
Questo dato è strano: stando alle risposte al questionario raccolte, se il ruolo è formalizzato in pochi casi è terziarizzato. Se invece il ruolo CISO non è ufficialmente definito, aumentano significativamente i casi di terziarizzazione: da 5,1% a 23,3%.

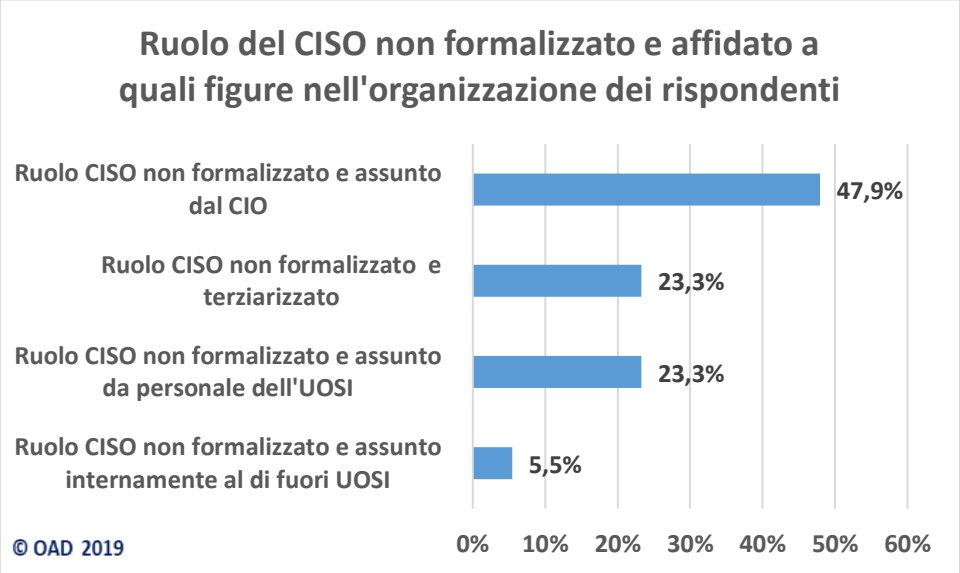

Fig. 9.1.1-2

Fig. 9.1.1-3

Ma quali sono le aziende/enti nelle quali sembrerebbe che nessuno si occupi di sicurezza digitale? La fig. 9.1.1-4 fornisce una risposta per il bacino dei rispondenti, correlando, chi ha risposto con un "no" totale con il numero di dipendenti della sua azienda/ente. Come è prevedibile, le piccole e piccolissime organizzazioni, sotto i 50 dipendenti, non hanno il ruolo del CISO per il 52% dei rispondenti. Nel complesso le PMI, fino a 250 dipendenti non hanno definito nè assegnato il CISO ad altre figure professionali interne o esterne nel 72% dei casi dei rispondenti. Ma la mancanza di tale ruolo si trova anche nelle grandi imprese fino a 5000 dipendenti. Solo le grandissime organizzazioni, con più di 5000 dipendenti hanno sempre un CISO, almeno nell'ambito dei rispondenti.

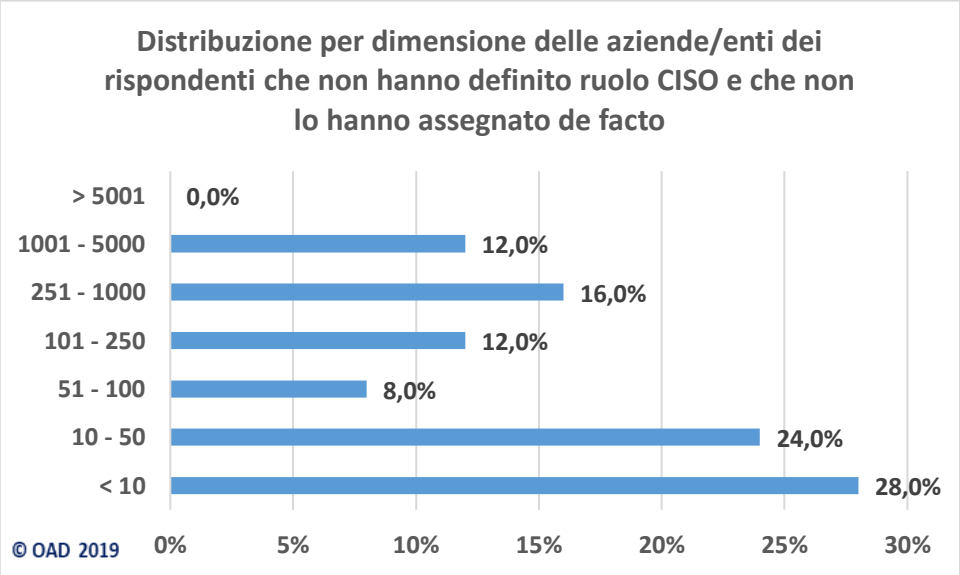

Fig. 9.1.1-4

9.1.2 Policy e procedure organizzative per la sicurezza digitale

Una policy su un determinato tema, nel nostro contesto la sicurezza digitale, definisce le linee guida e gli indirizzi, il più delle volte con valenza pluriennale e strategica, ed è rilasciata dal vertice dell'azienda/ente. Le procedure organizzative forniscono dettagliate istruzioni sia organizzative sia tecniche su come comportarsi per svolgere specifiche attività e per far fronte a determinate situazioni, e sono rivolte sia alle persone che svolgono determinati ruoli, sia alle strutture organizzative che debbono espletare e/o controllare talune attività, funzioni e processi: ad esempio, dalla effettuazione dei back up ai ripristini, dalla creazione e gestione degli account alla gestione delle emergenze e dei problemi.
Le policy e le procedure organizzative fanno spesso riferimento a normative che occorre rispettare per legge o per avere specifiche certificazioni, ad esempio per la sicurezza digitale o per la governance del sistema informatico con standard della famiglia ISO e best practice quali ITIL e COBIT.
Policy e procedure organizzative scritte, fatte conoscere ed aggiornate periodicamente, non sono da considerare una inutile e costosa burocrazia, e nemmeno attività solo per aziende/enti di grandi dimensioni: sono necessarie ed utili per formalizzare e divulgare documentazione su come usare e gestire le risorse ICT e la loro sicurezza ad utenti finali e privilegiati, e fornire specifiche indicazioni alle terze parti che possono essere coinvolte nella gestione e/o nel governo del sistema informatico. Sono inoltre essenziali per dimostrare l'accountability[20], così come richiesto ad esempio dal GDPR, e più in generale da varie leggi e normative (non solo per l'ICT).

La fig. 9.1.2-1, con risposte multiple, fornisce la situazione dichiarata dai rispondenti sulla presenza nelle loro aziende/enti di policy e di quale tipo e conferma come il bacino emerso dei rispondenti appartenga, indipendentemente dal settore merceologico e dalle dimensioni, ad una fascia medio-alta in quanto ad adozione di misure di sicurezza digitale: solo il 7,7% dei rispondenti non ha definito policy, e per il 24,4%, quasi ¼ dei rispondenti, sono in corso di definizione, probabilmente sotto la spinta del GDPR.

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

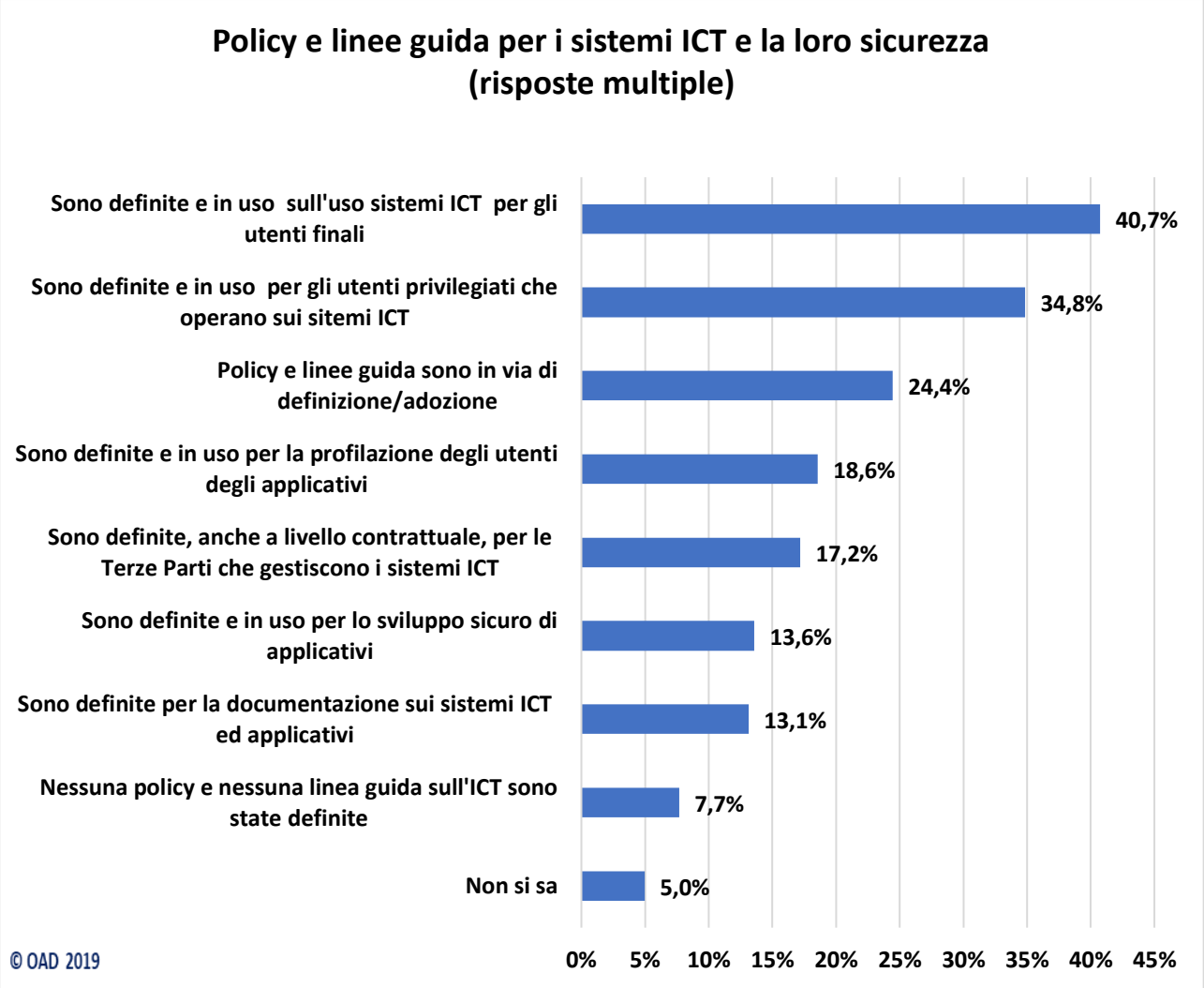

Fig. 9.1.2-1

La fig. 9.1.2-2, con risposte multiple, presenta la situazione tra i rispondenti sulle procedure organizzative inerenti l'ICT e soprattutto la sua sicurezza. Percentualmente l'uso di procedure organizzative risulta di poco inferiore rispetto a quelle delle policy della figura precedente: questo dato conferma la tendenza purtroppo assai diffusa in ogni tipo di azienda/ente in Italia a definire, magari in maniera molto generica, succinte policy così da poter dimostrare il formale adempimento a obblighi di leggi e normative, ad esempio del GDPR, ma a non definire procedure operative, assai più utili e necessarie per l'operatività sui sistemi informatici, ma che richiedono ben maggior impegno sia nella stesura che nell'aggiornamento. Le procedure più diffuse tra i rispondenti sono quelle per gli utenti finali con il 37,1%, mentre quelle per gli utenti privilegiati, nella pratica assai più importanti, scendono al quinto posto con il 21,7%. Con la medesima percentuale le procedure organizzative sono in fase di stesura, e il 12,7% ammette che non esistono. Interessante evidenziare come al secondo posto, con il 25,8%, siano le procedure per il Disaster Recovery, DR, probabilmente all'intero di un più generale piano di continuità operativa (business continuity).

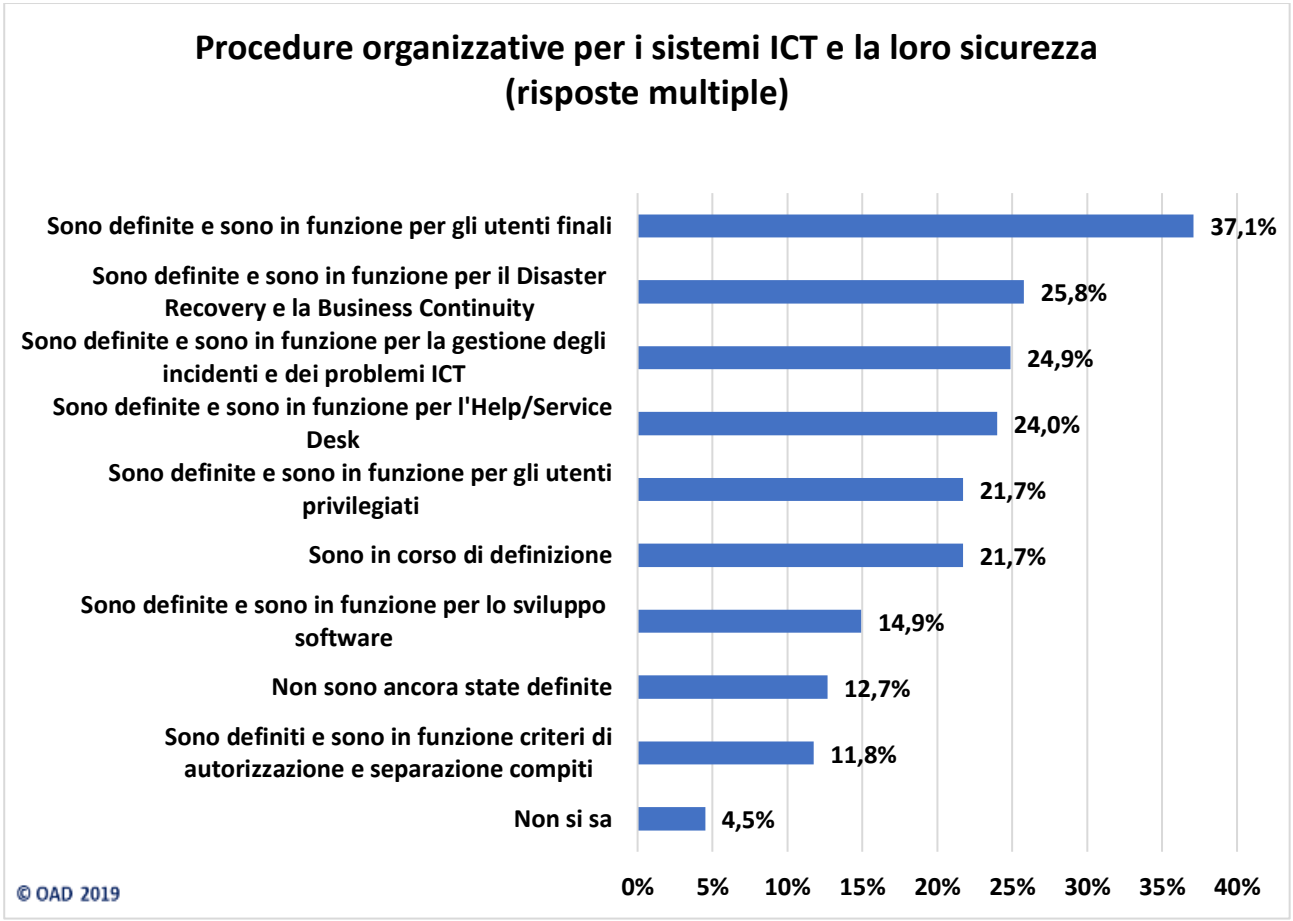

Fig. 9.1.2-2

9.1.3 Sensibilizzazione, formazione ed addestramento sulla sicurezza digitale

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

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

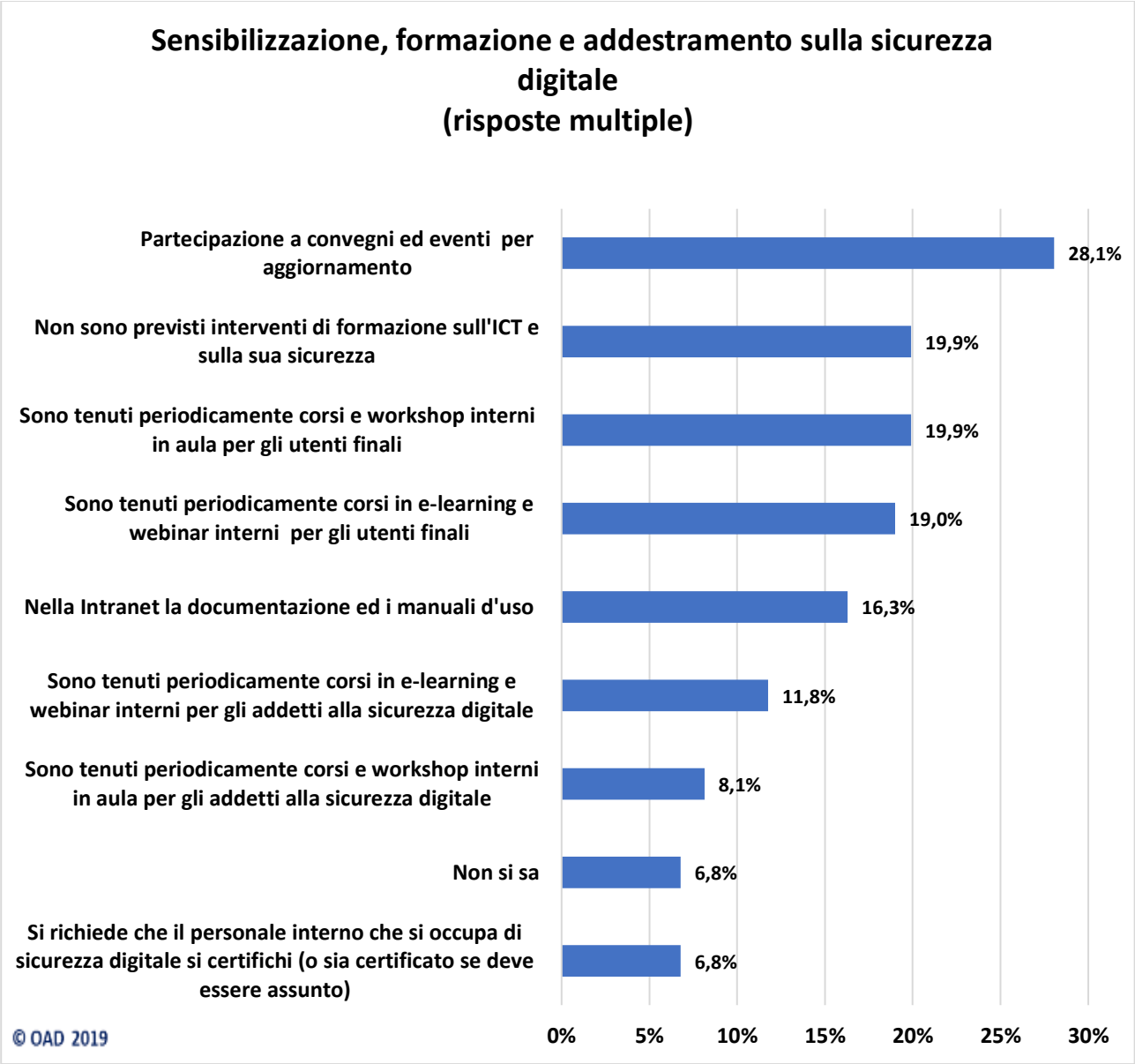

Fig. 9.1.3-1

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

9.1.4 Certificazioni sulla sicurezza digitale

Un concreto ausilio nell'organizzazione della sicurezza digitale e nella scelta di qualificati fornitori e outsourcer dell'ICT è fornito dall'uso di una intelligente e contestuale adozione di standard e di "buone pratiche" ("best practice") metodologiche ed operative, consolidate a livello internazionale e nazionale: tipici esempi la famiglia di standard ISO 27000 per la gestione della sicurezza ICT, il COBIT per la gestione tattico-strategica allineata al business, ITIL e l'ISO 20000 per la gestione operativa dell'ICT, l'ISO 9001 per la gestione della qualità dei servizi, le misure per la sicurezza digitale dell'AgID per le Pubbliche Amministrazioni.

Tali standard e best practice possono essere adottati formalmente, ossia certificandosi a livello di intera azienda/ente o di alcune sue figure professionali, o informalmente all'interno delle proprie strutture. L'adozione di certificazioni sta iniziando a crescere anche in Italia come richiesta ai fornitori ICT, a livello aziendale e/o dei singoli dipendenti persone, per potersi garantire un livello di preparazione ed esperienza qualificato e comprovato.
In ambito sicurezza digitale esistono numerosi i tipi di certificazioni indipendenti ed internazionali, quali ad esempio eCF (l'unica con validità legale in Europa), Eucip, CISSP, SSCP, CISA, CSSLP.
Esistono poi innumerevoli certificazioni "proprietarie" da parte di fornitori e costruttori ICT, prevalentemente focalizzate a validare la buona conoscenza tecnica e sistemistica dei loro prodotti, soluzioni e servizi ICT. Anche se buona parte dei professionisti italiani operanti nell'ambito della sicura digitale ha acquisito a livello personale una o più certificazioni specialistiche, le aziende/enti sono su questo tema ancora in una fase quasi "embrionale": tre le cause principali, a giudizio dell'autore, oltre ai costi e agli impatti organizzativi e sui processi, la poca cultura informatica delle persone di vertice, e soprattutto sulla sicurezza digitale.
Come evidenziato dalla fig. 9.1.4-1, con risposte multiple, il 41,2 % dei rispondenti segnala che la propria azienda/ente non è interessata e non richiede certificazioni. Un dato percentualmente analogo a quello emerso nell'indagine del 2018 con circa il 40%, e che conferma che in Italia le certificazioni, soprattutto per la sicurezza ICT e per le piccole-medie organizzazioni, non siano considerate come uno strumento necessario, anche se non sufficiente, per dimostrare un minimo livello di garanzia sulle effettive competenze a livello di persone e di aziende. Il 5,9% ha in corso una certificazione aziendale sulla sicurezza digitale, Il 15,1% è già in possesso di una certificazione digitale aziendale sulla sicurezza digitale, e di questi il 10% per ISO 27000, mentre lo stesso campione dichiara che 17,2% già è certificata ISO 9001 per la qualità totale (che solo marginalmente tratta della sicurezza digitale). Quest'ultima percentuale più alta è dovuta all'obbligo dell'ISO 9001 per aziende/enti che vogliono rispondere a bandi di gara pubblici. Purtroppo, l'obbligo per legge, con le relative sanzioni, è uno dei pochi strumenti efficaci, in Italia, per forzare e educare a logiche e comportamenti per migliorare competenze e professionalità.

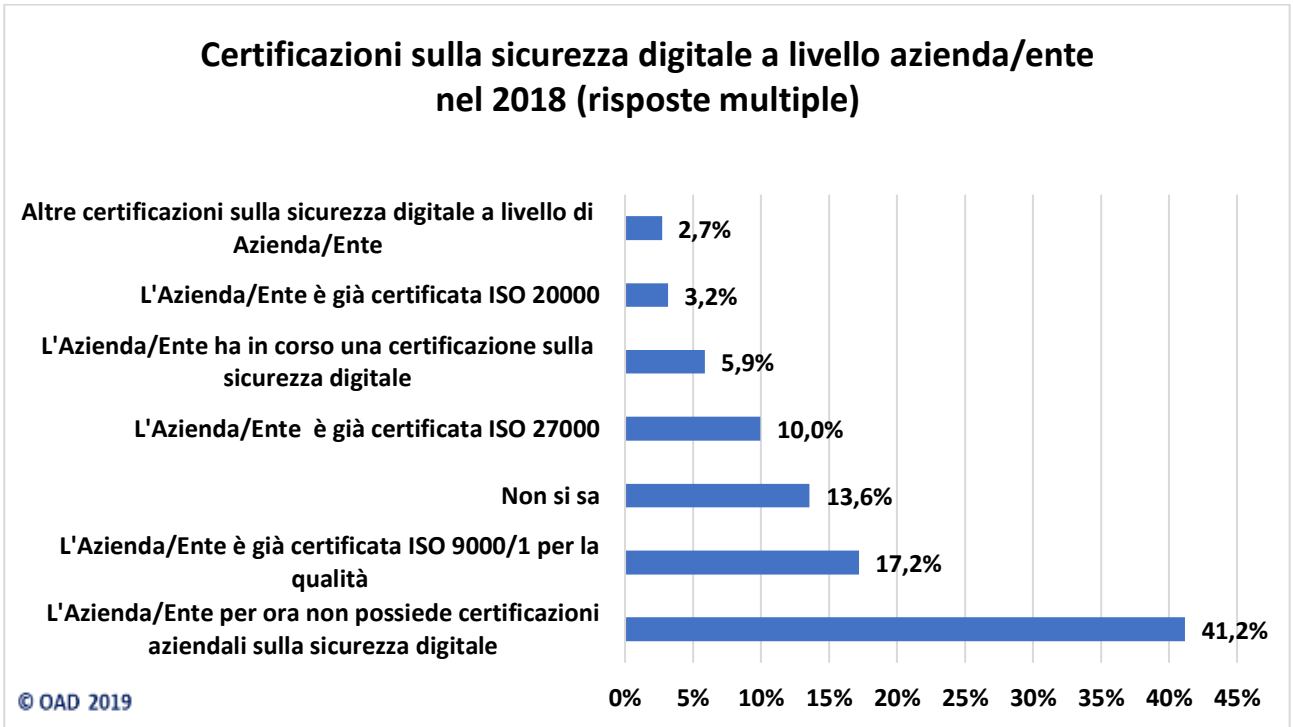

Fig. 9.1.4-1

La fig. 9.1.4-2, con risposte multiple, evidenzia che quasi la metà dei rispondenti non richiede certificazioni individuali per il proprio personale interno, ma il 11,3% ha già personale con certificazioni sulla sicurezza digitale, e il 3,8% le richiede per le nuove assunzioni. Il 9% le prevede nel prossimo futuro.

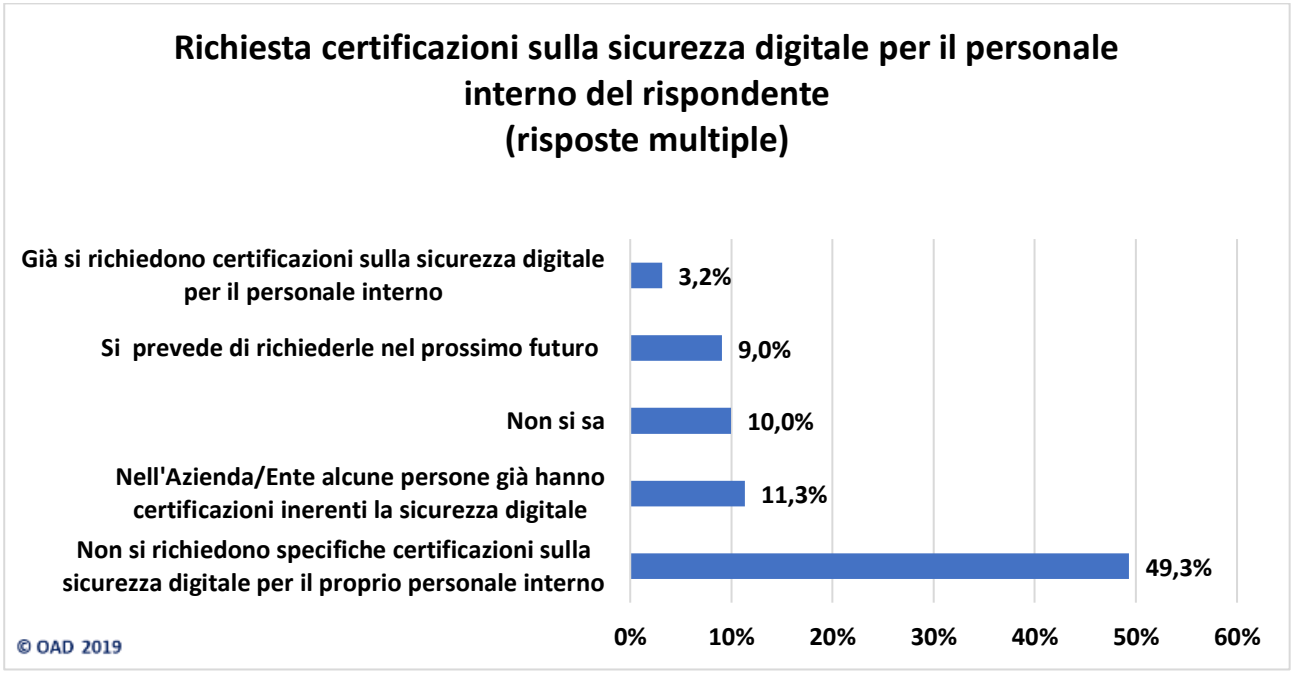

Fig. 9.1.4-2

La fig. 9.1.4-3, con risposte multiple, dettaglia ciò che l'azienda/ente del rispondente ai propri fornitori ICT per le certificazioni sulla sicurezza digitale. Il 33,9% non le richiede ed il 17,2%, anche se non le richiede formalmente, preferisce nelle scelte i fornitori di ICT che le hanno. Il 11,3% richiederà nel prossimo futuro certificazioni a livello aziendale per i fornitori ICT ed il 2,3% a livello individuale per il personale del fornitore.
Gran parte dei rispondenti non richiede certificazioni né al proprio interno né ai propri fornitori, ma è notevole la differenza percentuale a sfavore delle certificazioni interne. E' logico che per l'azienda/ente di un rispondente sia più importante che un proprio fornitore ICT sia certificato, piuttosto che lo sia la propria azienda o il proprio personale.
Numerose le certificazioni esistenti sulla sicurezza digitale, ed usate anche in Italia: CISSP, SSCP, CISA, CISP, OPSA, Eucip, eCF, etc. In Italia sono in vigore due leggi, quella n. 4/2013 sulle "professioni non regolamentate" ed il D. Lgs. n. 13/2013 sulla "certificazione delle competenze" che hanno definito le certificazioni personali con valore legale per le figure professionali non regolamentate da Ordini. La prima normativa di riferimento indicata da queste norme è EN 16234-1:2016 (UNI 11506), che riprende la certificazione europea eCF sulle competenze e sui profili professionali dell'ICT.

La fig. 9.1.4-4 evidenzia la percentuale delle aziende/enti dei rispondenti con obblighi di conformità (compliance) a specifiche normative, leggi e/o certificazioni: il 28,3% ha già tali obblighi, ed il 5,4% li avrà/dovrà adeguarsi nel prossimo futuro.

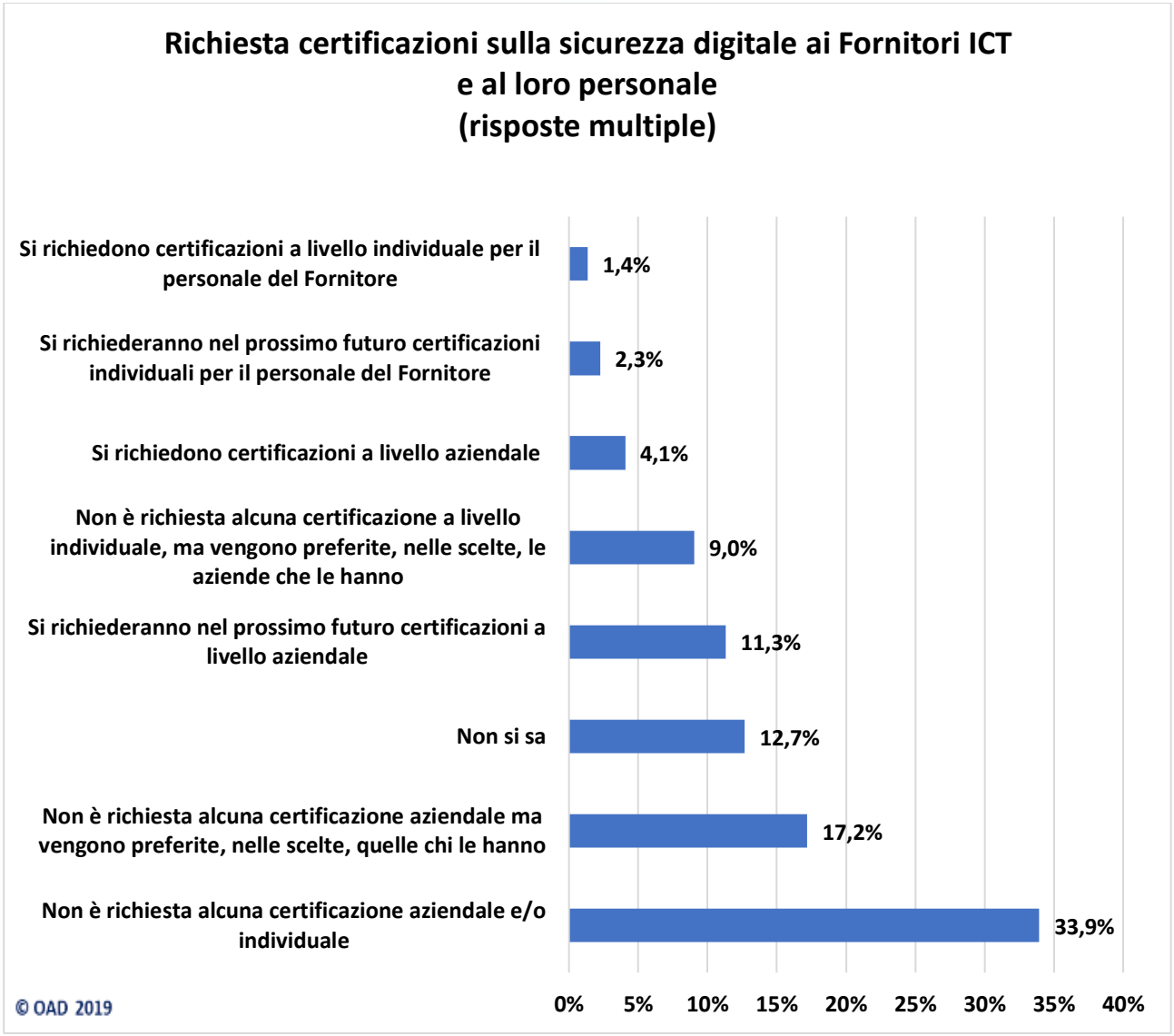
Richiesta certificazioni sulla sicurezza digitale ai Fornitori ICT
e al loro personale
(risposte multiple)
Si richiedono certificazioni a livello individuale per il personale del Fornitore
1,4%
Si richiederanno nel prossimo futuro certificazioni individuali per il personale del Fornitore
2,3%
Si richiedono certificazioni a livello aziendale
4,1%
Non è richiesta alcuna certificazione a livello individuale, ma vengono preferite, nelle scelte, le aziende che le hanno
9,0%
Si richiederanno nel prossimo futuro certificazioni a livello aziendale
11,3%
Non si sa
12,7%
Non è richiesta alcuna certificazione aziendale ma vengono preferite, nelle scelte, quelle chi le hanno
17,2%
Non è richiesta alcuna certificazione aziendale e/o individuale
33,9%
0%
5%
10%
15%
20%
25%
30%
35%
40%
© OAD 2019

Fig. 9.1.4-3

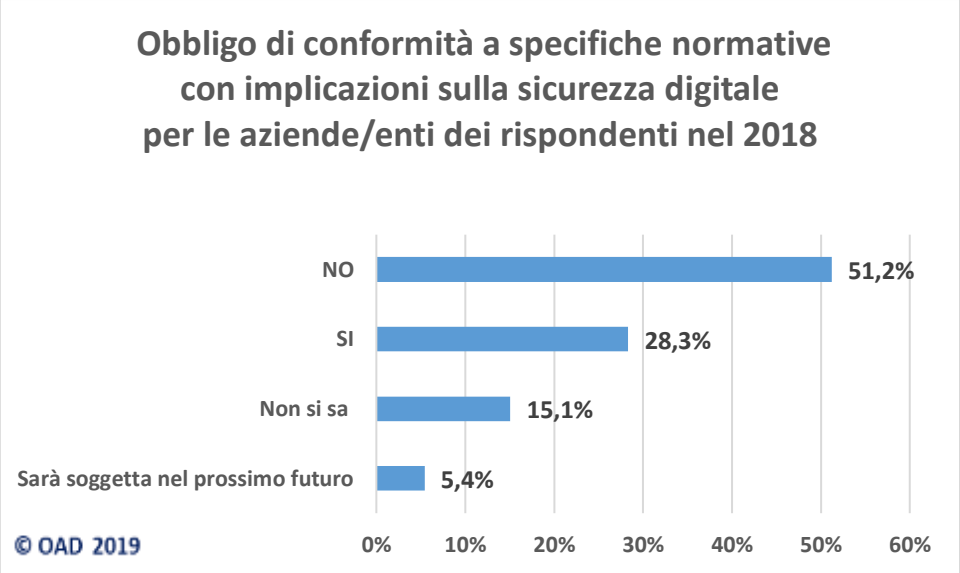

Fig. 9.1.4-4

9.1.5 Analisi e assicurazione dei rischi digitali

L'analisi dei rischi ICT è basilare per la progettazione delle misure di sicurezza contestualizzate sulla specifica realtà dell'azienda/ente. L'analisi dei rischi è inoltre richiesta per la conformità a varie norme e leggi, a partire dal GDPR. Sono ormai consolidate da anni varie metodiche, best practice e framework per effettuare tali analisi, pur con differenti livelli di dettaglio e di granularità: dallo standard ISO 27005 a NIST, CRAMM, Mehari, Octave-Allegro, etc. E vari aziende ed enti in Italia iniziano ad utilizzarli.
Dato che il processo di analisi dei rischi dovrebbe essere periodicamente ripetuto, soprattutto a seguito dell'introduzione di nuovi sistemi ICT e dell'evoluzione dell'azienda/ente (cambi organizzativi, nuove linee di business, profonde modifiche di taluni processi a seguito della loro digitalizzazione, etc.), sovente esso viene inserito tra gli strumenti per la gestione della sicurezza digitale. Data la sua rilevanza, si è ritenuto opportuno dedicare all'analisi dei rischi digitali un paragrafo a sé stante nell'ambito delle misure organizzative.

La fig. 9.1.5-1 mostra che il 54,5% delle aziende/enti dei rispondenti effettua l'analisi dei rischi, ma di questi il 24,8% la effettua periodicamente, il rimanente la effettua solo se richiesto e/o in maniera sporadica, ad esempio dopo aver subito un grave attacco digitale. Il 36,17% ha a piano di effettuarla nel prossimo futuro. Queste percentuali confermano che il bacino dei rispondenti, pur includendo in maggioranza PMI (si veda §10.2), sono nella fascia medio-alta in termini di misure di sicurezza digitali, e che a partire dal 2017 si è verificato un aumento delle percentuali delle aziende/enti rispondenti che dichiarano di effettuare l'analisi dei rischi digitali: un aumento sicuramente favorito dall'obbligo di conformità al GDPR.

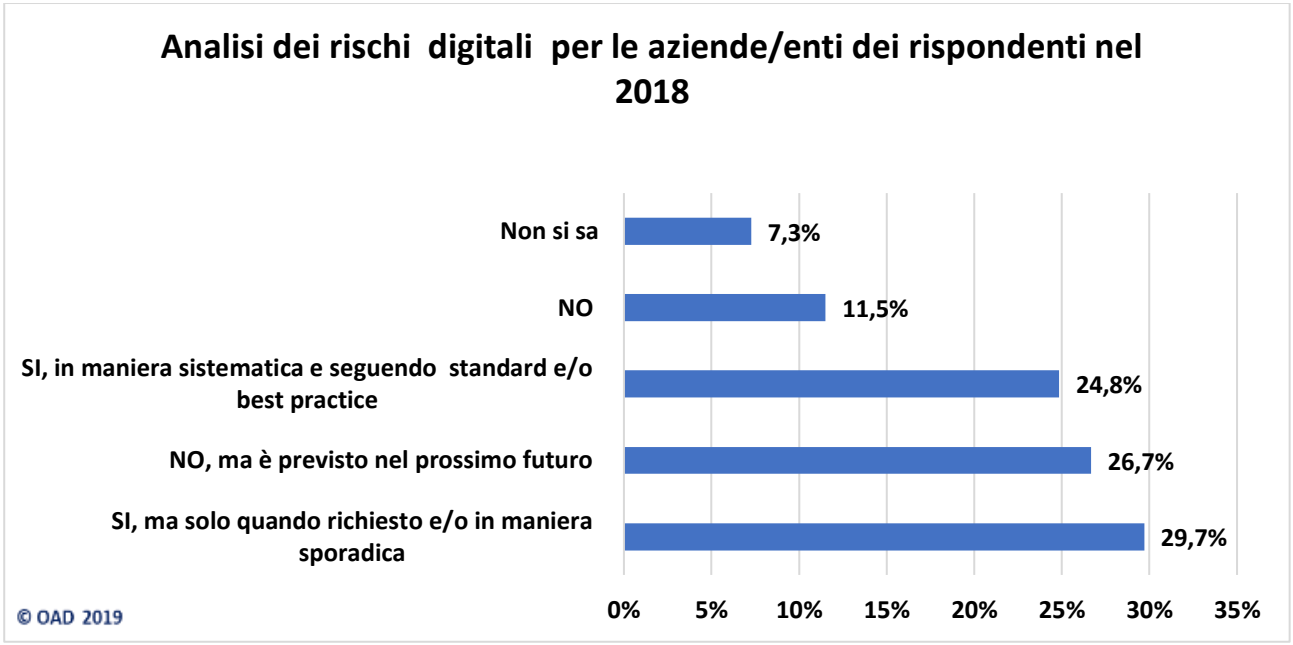

Fig. 9.1.5-1

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

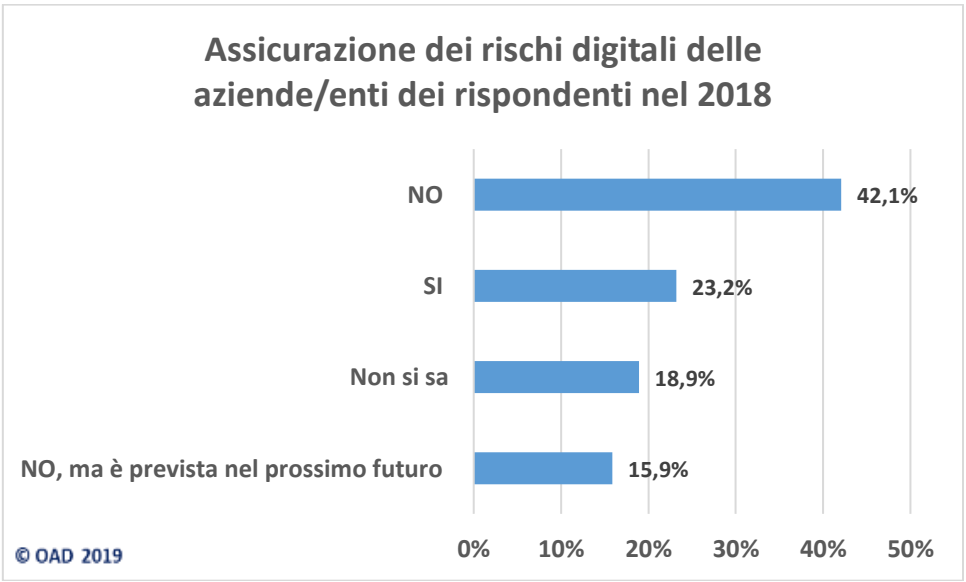

Fig. 9.1.5-2

La fig. 9.1.5-2 mostra che il 23,2% dei rispondenti ha già in essere nel 2018 una specifica assicurazione per i rischi ICT, mentre il 15,9% ha a piano di sottoscriverne una. Come tendenza, e senza valore statistico per la diversità dei bacini dei rispondenti, la percentuale di chi ha già nel 2018 una assicurazione sui rischi digitali è quasi doppia rispetto a quella del 2017: questo è un indice del crescente interesse, seppur lento, nell'assicurare il sistema informatico dell'azienda/ente.

9.1.6 Auditing sicurezza digitale

Con il termine di "auditing" si intende il processo di valutazione della sicurezza digitale, e della sua gestione, di una azienda/ente. Con il termine di "audit" si intende il risultato di tale valutazione, rappresentato tipicamente di un rapporto all'alta direzione. Sovente, anche tra gli addetti ai lavori, i due termini vengo usati, erroneamente, come sinonimi.

La fig. 9.1.6-1 indica che il 43,4% complessivo dei rispondenti già effettua auditing per il proprio sistema informatico, e ben il 25,3% lo ha a piano a breve. Valori percentuali alti, superiori come tendenza a quanto rilevato dalle indagini OAI/OAD negli anni precedenti, ed indice anche questo, come l'analisi dei rischi del precedente paragrafo, del buon livello medio di sicurezza digitale per i rispondenti di OAD 2018.
La percentuale complessiva di chi lo attua si articola nelle tre modalità indicate: il 18,7% sia interno che esterno (ossia con esperti di Terze Parti che effettuano un loro autonomo auditing, che sarà poi confrontato con quello effettuato da personali interno), il 15,1% effettuato solo da personale interno, il 9,6% effettuato solo da personale esterno.

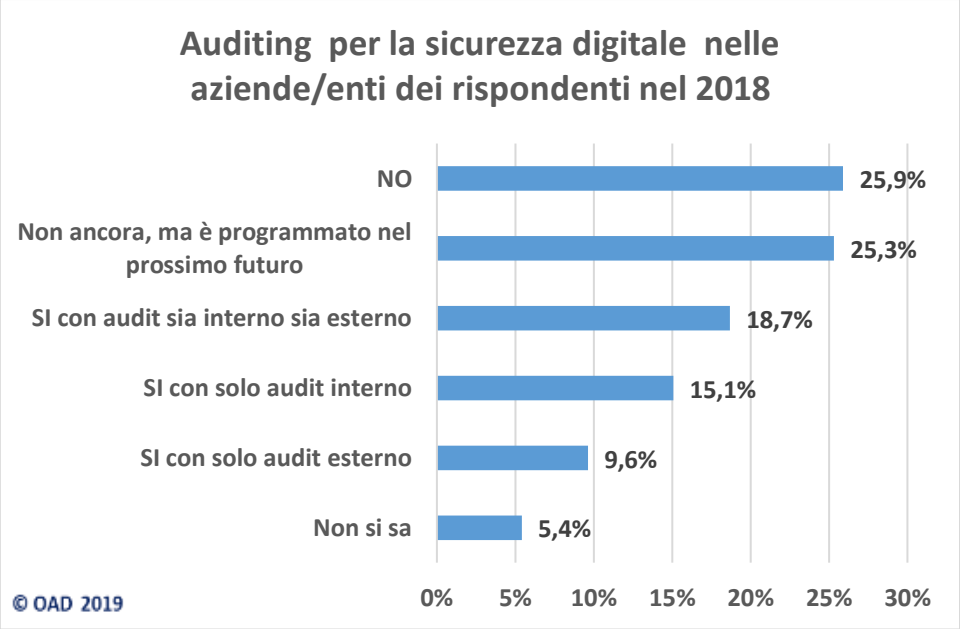

Fig. 9.1.6-1

9.2 Misure tecniche per la sicurezza digitale

Facendo riferimento alle macro-caratteristiche dei sistemi informatici e delle aziende/enti dei rispondenti illustrate in §10, nel seguito vengono descritti gli strumenti di sicurezza digitale in uso in

questi sistemi informatici, a livello sia tecnico sia organizzativo: è così possibile meglio comprendere in quali contesti e con quali livelli di sicurezza digitale siano potuti occorrere gli attacchi rilevati (§6). Nel questionario OAD 2019 le misure tecniche sono state raggruppate in:

- Architettura complessiva delle misure della sicurezza digitale, integrata con l'intera architettura del sistema informatico
- Contromisure fisiche
- Misure di Identificazione, Autenticazione, Autorizzazione (IAA)
- Contromisure tecniche sicurezza digitale a livello di reti locali e geografiche
- Contromisure tecniche per la protezione logica dei singoli sistemi ICT
- Contromisure tecniche per la protezione degli applicativi
- Contromisure per la protezione dei dati
- Sistemi di controllo, monitoraggio e gestione della sicurezza digitale
- Piano di Disaster Recovery (DR).

Il presente paragrafo presenta ed analizza le risposte avute dai rispondenti nell'ordine delle misure tecniche sopra elencate.

La prima domanda del questionario OAD 2019 fa riferimento, a grandi linee, alla architettura della sicurezza digitale posta in esercizio, e che dovrebbe essere integrata nell'architettura dell'intero sistema informatico. La domanda serve per inquadrare l'approccio tecnico che l'azienda/ente sta seguendo nella realizzazione della sicurezza digitale per i suoi sistemi ICT, tenendo conto che anche per l'architettura tecnica della sicurezza digitale esistono standard e best practice di riferimento, quali ad esempio gli standard ISO, quelli NIST SP 800, quelli SOA/OASIS, l'OSA, Open Security Architecture, e che da anni gli esperti di sicurezza digitale sottolineano l'importanza di una "security by design", richiesta anche dal GDPR per implementare una privacy by design e by default.

La fig. 9.2-1, con risposte multiple, mostra che il 27,1% circa dei rispondenti non ha definito e/o non segue alcuna architettura per l'implementazione della sicurezza digitale. Chi l'ha definita e la sta usando, lo ha fatto con i seguenti approcci, non esclusivi tra loro, date le risposte multiple:

- il 17,6% l'ha definita e la segue nell'ambito del piano regolatore dello sviluppo pluriennale dell'intero sistema informatico;
- il 13,1% l'ha definita utilizzando gli standard, le best practice ed i framework consolidati a livello internazionale sopra indicati;
- il 9,3% la definita e la segue solo per la parte del sistema informatico gestita al proprio interno, on premise, e tale architettura non tiene conto della terziarizzazione in uso;
- un identico 7,7% l'ha usata per realizzare, almeno per le parti più critiche, un sistema informatico ridondato per garantire un'alta affidabilità e disponibilità.

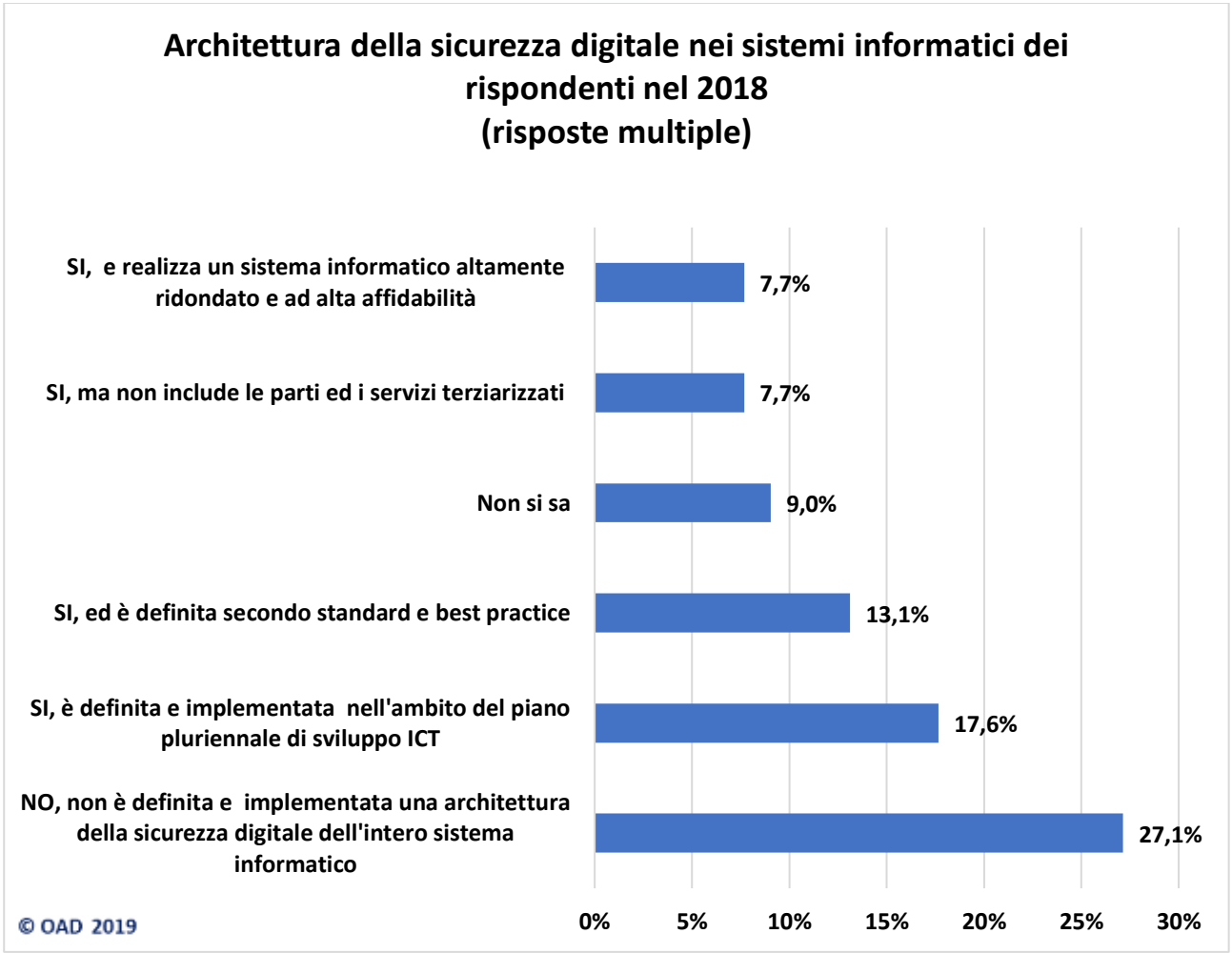

Fig. 9.2-1

I dati emersi confermano da un lato che il campione emerso dei rispondenti si colloca in una fascia media alta per quanto riguarda la sicurezza digitale, ma che ancora molto deve essere attuato per raggiungere una adeguata e diffusa security by design.

La fig. 9.2-2, con risposte multiple, elenca le principali misure in uso per la protezione "fisica" dei locali ove sono installate risorse ICT, dai Data Center alle "computer room" fino ai singoli locali dove si possono trovare unità di rete e dispositivi d'utente fissi.
Gli strumenti più usati dal campione emerso sono i sistemi per garantire la continuità elettrica (46,2%), da UPS ad autonomi gruppi di continuità, cui seguono a scalare con un pochissimi punti percentuali di differenza, i sistemi di climatizzazione nei locali ove sono concentrate le risorse ICT, i vari sistemi rilevatori di fumo, gas, e umidità, le protezioni perimetrali passive e attive, recinzioni anti-scavalcamento, inferiate alle finestre e alle porte, sistemi di allarme antintrusione a radar o a micro onde, la videosorveglianza.
Per il 34,4% vengono effettuati controlli degli accessi delle persone fisiche ai Data Center/Computer Room tramite diversi strumenti che includono bussole d'ingresso, lettori di badge, riconoscimento biometrico, etc. Il 33,5% dei sistemi informatici dei rispondenti ha aree dedicate ai sistemi ICT protette solo da porte chiuse a chiave, ed il 7,7% circa non ha di fatto alcuna misura di sicurezza fisica per i locali ove sono contenuti i sistemi ICT. Con "Altro" alcuni rispondenti hanno specificato che tutto il loro sistema informatico è tutto terziarizzato o in cloud, ed il fornitore eroga tutti gli idonei livelli di sicurezza fisica. Altri segnalano che la sicurezza fisica è terziarizzata a istituti di vigilanza.

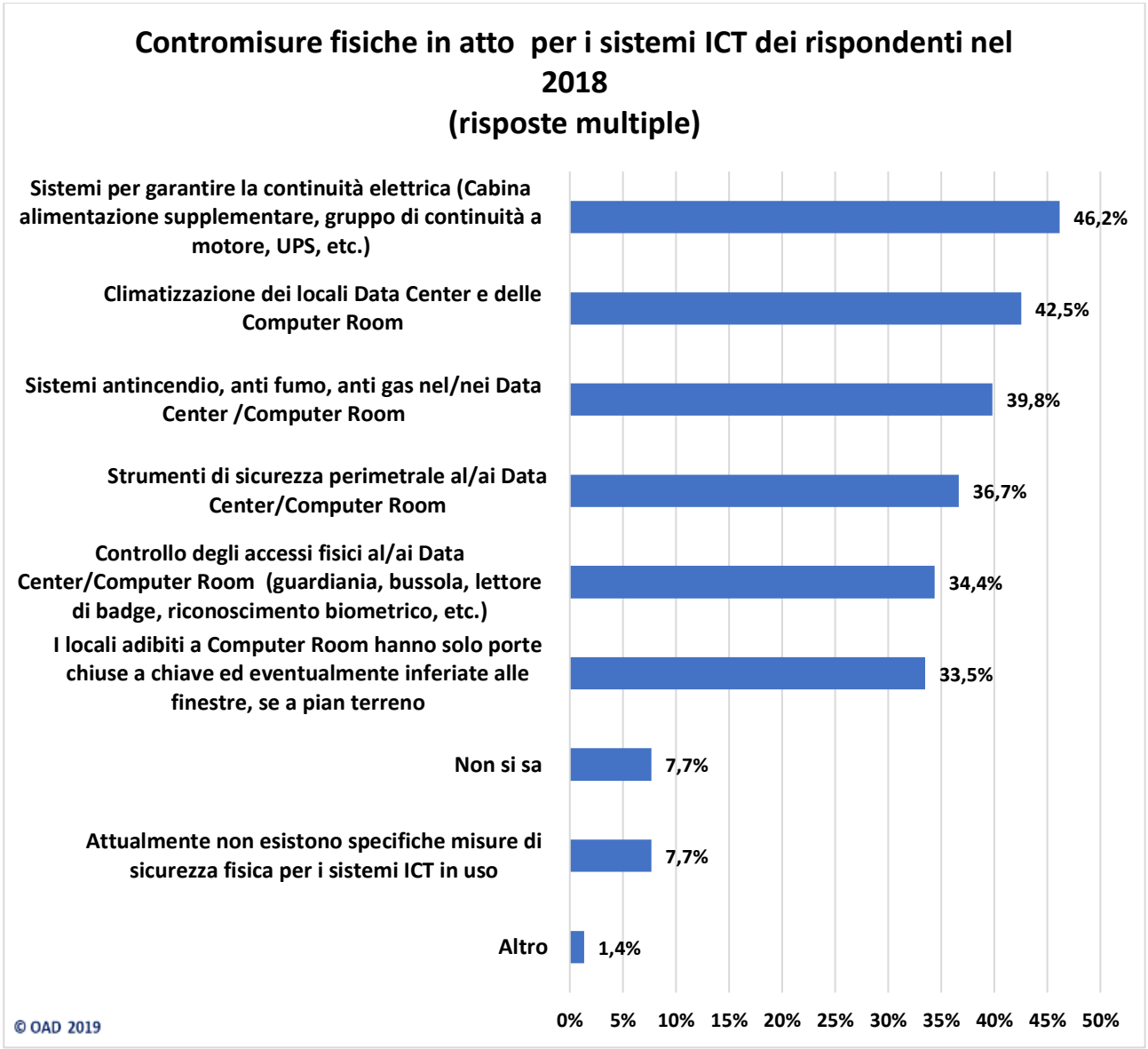

Fig. 9.2-2

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

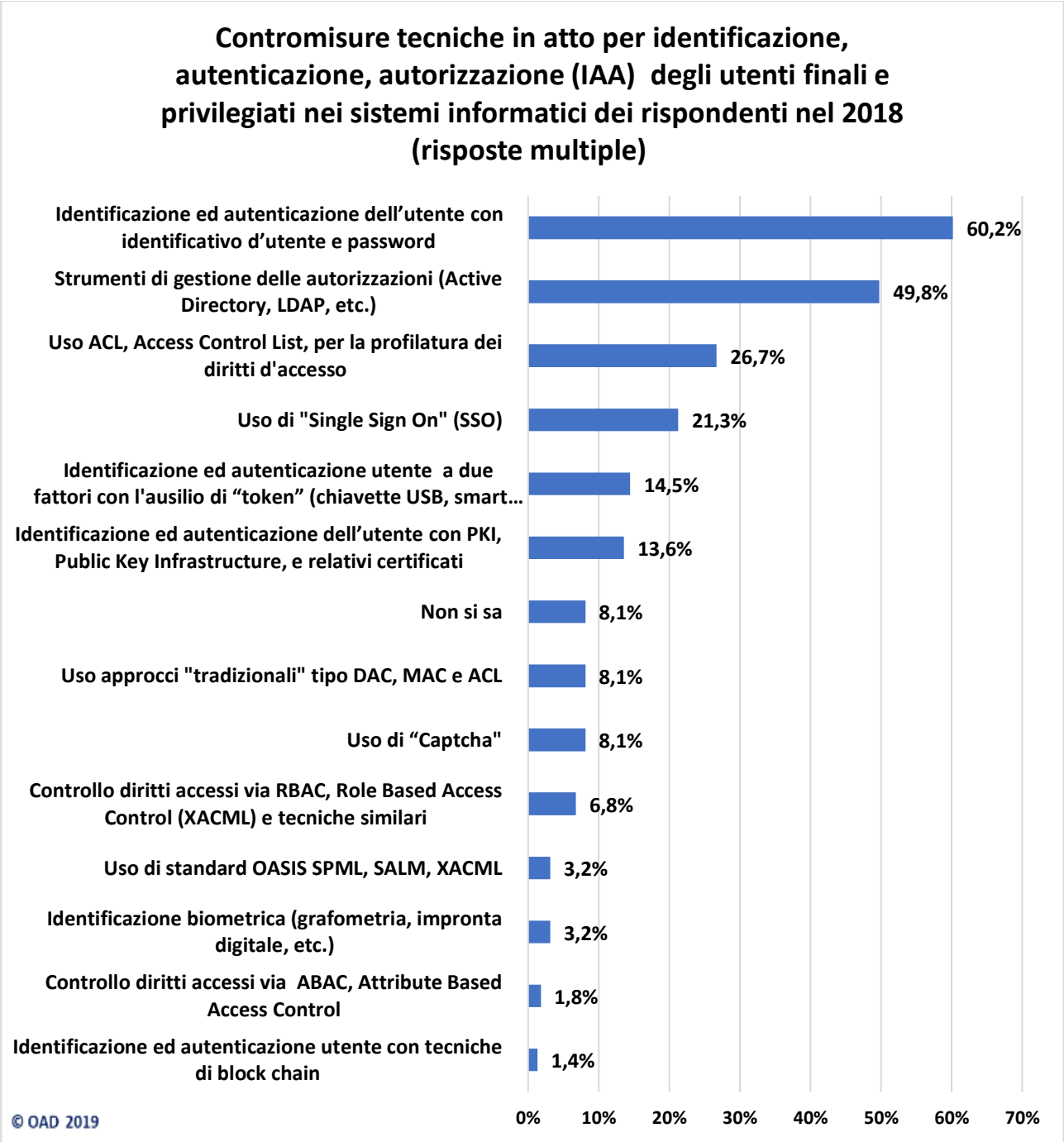

Fig. 9.2-3

La fig. 9.2-3, con risposte multiple, riporta le misure di IAA indicate dai rispondenti: il 60,2% fa uso del consueto "account" costituito dalla coppia identificatore utente e password, cui segue, con un 49,8%, l'uso di strumenti di gestione e controllo degli accessi quali i diffusi Active Directory di Microsoft e l'LDAP, e con il 26,7% l'uso delle ACL, Access Control List, per la verifica dei privilegi degli utenti abilitati alle applicazioni e ai vari sistemi informatici. Altre tecniche a decrescere. Interessante evidenziare come solo il 14,5% fa uso dell'autenticazione a due fattori, ad esempio con token e con controlli anche via cellulare, ed ancor meno, il 13,6% usa l'autenticazione forte con

certificati digitali, spinta in Italia soprattutto dallo SPID[21], il sistema unico di login che nella sua forma più forte di autenticazione, il livello 3, usa i certificati digitali e che dovrebbe essere d'obbligo per le pubbliche amministrazioni. Pur con tali spinte, e con le tecnologie sui certificati elettronici e digitali ben consolidate da molti anni, la percentuale emersa dai rispondenti è veramente bassa, come di fatto è ancora bassa la loro diffusione in Italia, al di là del bacino di rispondenti di OAD 2019.
Alta la percentuale di rispondenti che ha risposto "Non si sa": questo è sicuramente dovuto ai nomi delle varie tecniche di controllo degli accessi previsti come possibile risposta multipla a questa domanda sull'IAA nel questionario, che molti rispondenti non conoscono.

Nell'ambito delle contromisure per le reti, la fig. 9.2-4, con risposte multiple, evidenzia che il 54,3% dei rispondenti è dotata di dispositivi firewall e di DMZ, DeMilitarized Zone (in italiano zona demilitarizzata). Al secondo posto, con circa il 48,9%, l'uso di VPN, Virtual Private Network, per proteggere le comunicazioni criptando i dati in transito. Segue, con poco più del 37,6%, l'adozione di soluzioni ridondate per le connessioni alle reti, in modo da garantire alta affidabilità e disponibilità. A decrescere poi l'uso di strumenti più complessi, dal filtraggio delle URL (sovente effettuato dallo stesso firewall o da una appliance ad hoc) ai sistemi di IDS/IPS.
Solo una piccola percentuale dei rispondenti, il 2,7%, dichiara che il loro sistema informatico non è al momento dotato di alcuna specifica protezione per le reti.
Con "Altro" alcuni rispondenti hanno indicato che è l'outsourcer ad occuparsi anche del networking ed altri hanno indicato l'uso di strumenti di crittografia per trasmettere file.

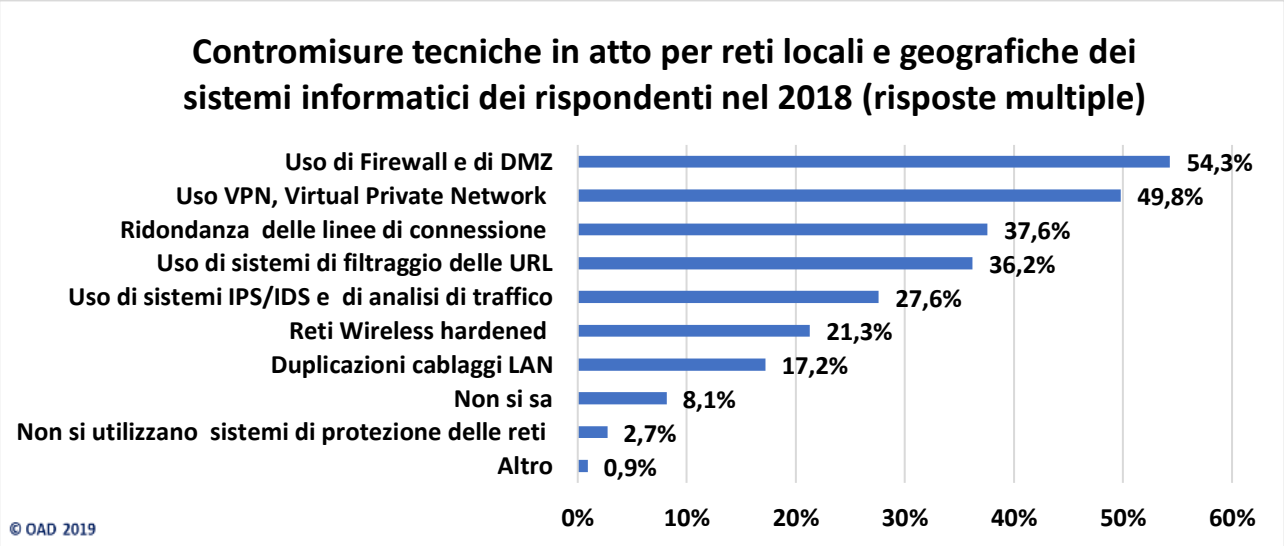

Fig. 9.2-4

La fig. 9.2-5 mostra la sintesi delle risposte multiple rilevate sulla sicurezza logica in essere sui singoli sistemi ICT, tipicamente server e storage, fisici e virtuali, posti di lavoro (PC), unità di rete intelligenti, etc.
Stranamente i sistemi anti-malware, pur essendo i più diffusi, sono usati solo dal 54,3% dei rispondenti; nell'indagine precedente erano praticamente usati da tutti (94,46%). Seguono a scalare, ma con percentuali inferiori al 50%, la virtualizzazione dei sistemi, la gestione delle versioni e delle patch. Non trascurabile la percentuale di rispondenti, 34,4%, che dichiara che almeno qualche configurazione di singoli sistemi sono in alta affidabilità sia hardware che software, anche (ad esempio) con uso di hard disk in RAID. Il 42,5% dei rispondenti raccoglie e gestisce i log degli

[21] 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.

accessi ai sistemi ICT degli amministratori di sistema (utenti privilegiati), obbligo in vigore dal 2008 per la disposizione del Garante della Privacy[22], obbligatorietà che continua anche con il GDPR. Percentuale alta, se si confronta con quanto rilevato nelle precedenti indagini OAD, bassa dato che questo è un obbligo per tutti i sistemi informatici. Nella voce "Altro" alcuni rispondenti hanno indicato la virtualizzazione centralizzata dei PC ed altri la frequente replica nella Intranet dei contenuti dei PC.

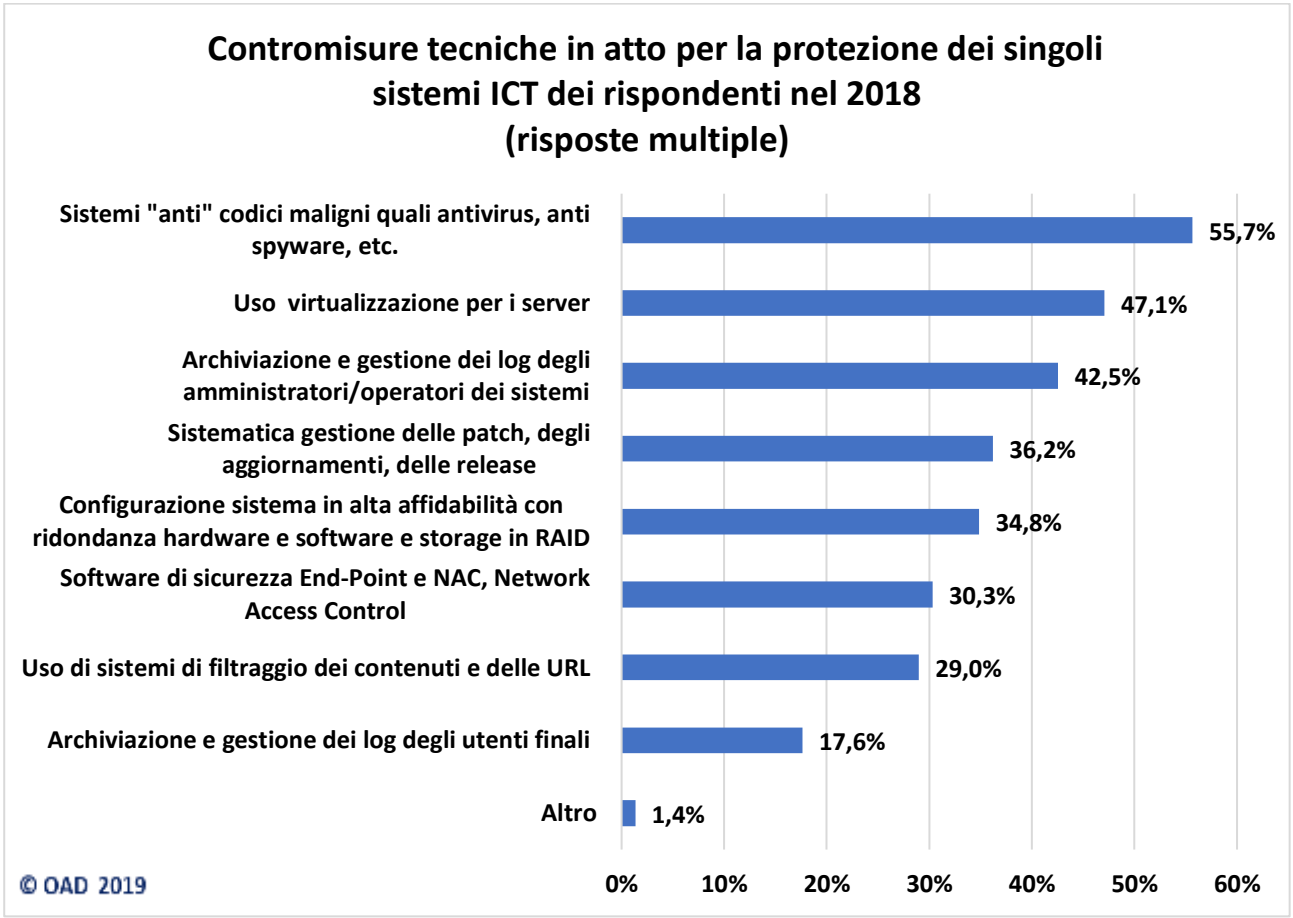

Fig. 9.2-5

Nelle contromisure a livello applicativo, con risposte multiple, emerge una relativamente alta percentuale, 39,8% di rispondenti che dichiarano l'uso di firewall applicativi (FWA), come mostrato in fig. 9.2-6, con risposte multiple. Con una percentuale ben minore, 20,4%, il controllo della sicurezza intrinseca del codice dell'applicativo, sia prima della sua messa in produzione, sia con controlli, ad esempio test di penetrazione ed analisi di vulnerabilità, quando è in esercizio. Sicuramente dovuta all'alta quota di rispondenti di piccole e piccolissime organizzazioni, che tipicamente acquistano applicazioni già presenti sul mercato, anche la percentuale, 14,9%, di specifiche clausole contrattuali sullo sviluppo sicuro di software coi fornitori, che è quasi il doppio di quella rilevata nell'indagine OAD 2018.

[22] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1577499

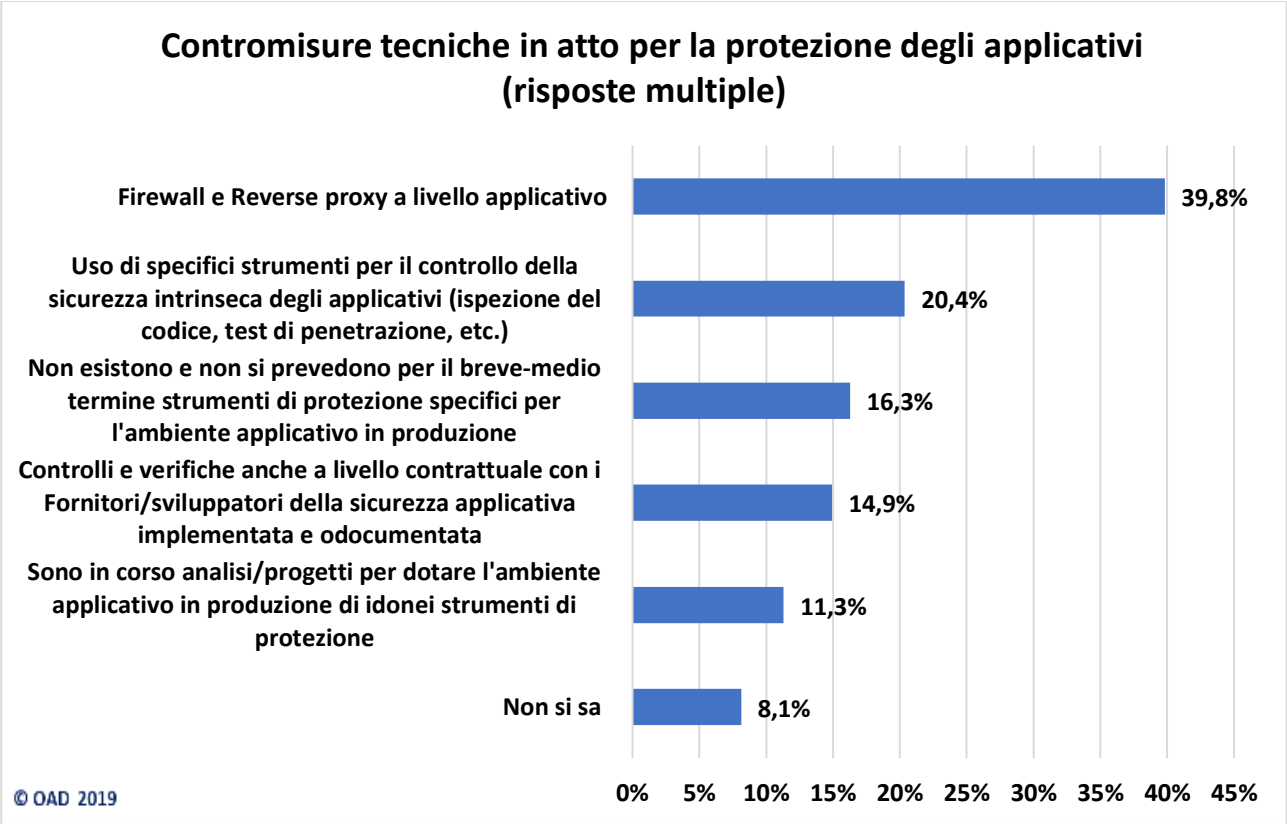

Fig. 9.2-6

Per la protezione dei dati, che costituiscono il reale e più importante "asset ICT" dell'azienda/ente, la fig. 9.2-7, con risposte multiple, mostra che il più diffuso tipo di misura sui dati riguarda, correttamente ma inaspettatamente rispetto alle indagini OAD precedenti, la classificazione dei dati in merito alle loro necessità di protezione. Tale classificazione, da sempre necessaria anche per l'individuazione dei dati personali e "sensibili" per la privacy, è la base sia per l'analisi dei rischi digitali sia per la corretta e contestualizzata scelta delle misure di sicurezza da adottare. Al secondo posto, con un 39,4% l'archiviazione sicura dei back up. Questo significa che il 60% dei rispondenti non fa back up? Secondo l'autore no, ma è il termine "sicura", e quindi completa, che ha ridotto, e di molto, la percentuale. È ben noto infatti che, soprattutto nelle piccole e medie organizzazioni, il back up viene sì effettuato, ma sovente in maniera non sistematica e/o solo per alcuni sistemi ICT e/o solo per alcuni dati/file.
Relativamente basse le percentuali di strumenti per la crittografia dei dati, sia quelli in transito su Internet dei dati (HTTPS, FTPS, VPN, etc.) con un 38,9%, sia per quelli, più critici, da archiviare, con un 27,6%. Le percentuali emerse sono superiori di circa 10 punti rispetto a quelle dell'indagine precedente, e questa è una positiva tendenza sicuramente aiutata dalla forte spinta alla crittografia data dal GDPR.

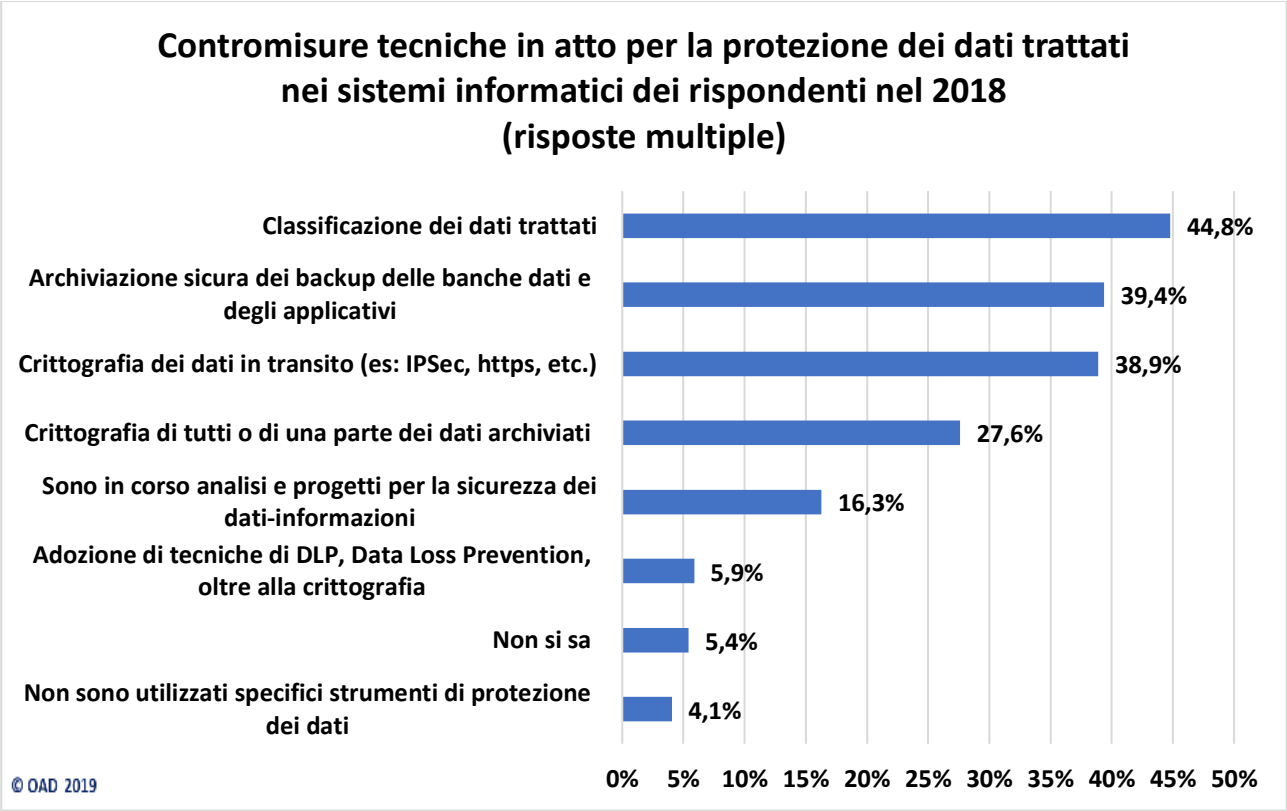

Fig. 9.2-7

9.3 Misure per la gestione della sicurezza digitale

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

Le misure e gli strumenti che sono stati fatti rientrare nell'ambito del governo della sicurezza digitale, e che sono un di cui della più generale gestione dell'intero sistema informatico, includono i sistemi di directory di tutte le risorse digitali e delle loro configurazioni e licenze (ICT Asset Management), i sistemi di monitoraggio e controllo delle funzionalità e delle prestazioni dei sistemi ICT, i sistemi di raccolta, correlazione e gestione di tutti gli eventi (SIEM) rilevati dai sistemi ICT, sistemi di analisi comportamentali di utenti e risorse ICT, 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[23].

Importante poi evidenziare che nel questionario 2019 OAD sono stati poste domande sull'utilizzo dei seguenti sistemi di tipo centralizzato:

[23] Risposte fortemente differenti sullo stesso tema fornite da un rispondente sono scartate.

- SGSI, Sistema Gestione Sicurezza Informatica: costituisce il sistema, normalmente centralizzato, per la gestione della sicurezza digitale di un sistema informatico, così come definito dagli standard della faglia ISO 27000. Può essere realizzato internamente (on premise) o terziarizzato ad un SOC, o suddiviso tra una parte on premise ed una o più parti terziarizzate.
- SoC, Security Operation Center: è un centro interno all'azienda/ente o esterno, terziarizzato a società specializzate, che attua la gestione operativa della sicurezza digitale, monitorando i sistemi ICT. gli utenti, le vulnerabilità ed i rischi digitali. Effettua quando necessario gli opportuni interventi di prevenzione, protezione e di ripristino.
- SCC, Security Command Center: questa sigla indica un tipo di piattaforma messa a disposizione, solitamente dai fornitori di cloud, per fornire ai clienti la visibilità delle loro risorse ICT terziarizzate, in termini di tipologia risorse e configurazioni, del loro livello di sicurezza digitale, e fornire strumenti per poter prevenire, rilevare e rispondere alle minacce.

La fig. 9.3-1, con risposte multiple, mostra la diffusione, in percentuale, dei principali strumenti di gestione della sicurezza ICT utilizzati dall'intero campione dei rispondenti, con risposte multiple. Al primo posto si colloca il monitoraggio ed il controllo centralizzato delle funzionalità e delle prestazioni dei sistemi ICT con un 37,1%, cui segue con meno di 5 punti percentuali il controllo "in locale" anche o solo a livello dei singoli sistemi, tipicamente quando ci si accorge di o viene segnalato un malfunzionamento. dei singoli sistemi.
Al terzo posto, con un 27,6%, l'analisi di vulnerabilità dei sistemi e delle applicazioni: la disponibilità di affidabili ed efficaci sistemi opensource, oltre alla spinta del GDPR, ha fatto significativamente crescere la sua diffusione tra i rispondenti, che nell'indagine dell'anno precedente si posizionava a poco più del 17%. Al quarto posto, con un 26,2%, l'uso di sistemi di gestione dei log degli utenti privilegiati (amministratori di sistema): tema già considerato tra le misure per la sicurezza di un sistema ICT in fig. 9.2-5, che raccoglieva un 42,5%. La non piccola differenza, nell'ambito dello stesso bacino di rispondenti, significa per l'autore che questi la considerano più uno strumento di protezione che di gestione, e probabilmente non l'hanno poi selezionato tra le possibili risposte alla domanda sugli strumenti di gestione della sicurezza. Seguono poi, con due punti percentuali a scalare, l'uso di sistemi IDS e IPS. Essi erano già stati considerati tra gli strumenti di sicurezza per le reti, in fig. 9.2-4, con una diffusione del 27,6%, congruente in percentuale con quelle qui emerse: la differenza, piccola, ha per l'autore gli stessi motivi sopra riportati.
L'utilizzo di SoC e di SCC ha un non trascurabile 11,8%, che vede coinvolto sia realtà di piccole-medie che di grandi dimensioni. La gestione della sicurezza digitale, richiedendo ampie e specializzate competenze e multidisciplinarietà, ben difficilmente può essere attuata direttamente all'interno di una azienda/ente anche di medio grandi dimensioni: diviene quasi obbligatorio farla effettuare da terze parte specializzate ed affidabili; e questo sarà sempre più necessario nel futuro soprattutto per le organizzazioni di piccole dimensioni.
L'implementazione di un SGSI significa la realizzazione di un sistema di gestione della sicurezza digitale conferme alle normative degli standard della famiglia ISO 27000, in particolare ISO 27001. Un SGSI può essere a sua volta gestito internamente, on premise, o terziarizzato in parte o completamente, ed utilizzare SoC e SCC. La realizzazione di un adeguato SGSI è necessaria per ottenere la certificazione a livello aziendale, spesso chiamata anche certificazione ISO 27001, e che è richiesta da alcune aziende/enti per poter partecipare a bandi di gara o per essere loro fornitori. Dati anche questi aspetti formali e organizzativi, solo un a piccala percentuale dei rispondenti, il 6,3% dichiara di avere un SGSI.
Sistemi di analisi comportamentale, e più in generale strumenti per la sicurezza digitale basati sull'intelligenza artificiale e su sistemi che auto apprendo nel tempo, le learning machine, iniziano ad essere usati, soprattutto dalle strutture di maggiori dimensioni e da chi ha sistemi informatici sofisticati e con gran numero di utenti, ma per ora le percentuali di diffusione tra i rispondenti sono basse, ma è già significativo che non siano a 0. Qualche rispondente le utilizza. Questi strumenti costituiscono uno dei fronti più innovativi nell'ambito della sicurezza digitale, soprattutto per correlare grandi numeri di informazioni e di log, e per individuare comportamenti di persone e/o di sistemi ICT considerati anomali rispetto ai normali funzionamenti, e cercare così di prevenire deterioramenti

funzionali ed attacchi. La complessità dei moderni sistemi informatici e la produzione di una miriade di segnalazioni non consentono, per essere realmente gestiti e in tempi quasi reali, di una crescente automazione. La gestione manuale non ha ormai più senso, nemmeno nelle realtà di medio-piccole dimensioni.
Il 15,4% dei rispondenti dichiara di avere strumenti per poter attuare un piano di Disaster Recovery, che è l'elemento fondamentale per poter attuare una vera continuità operativa (business continuity) dell'azienda/ente, e le cui modalità di attuazione sono dettagliate nella seguente fig. 9.3-2.

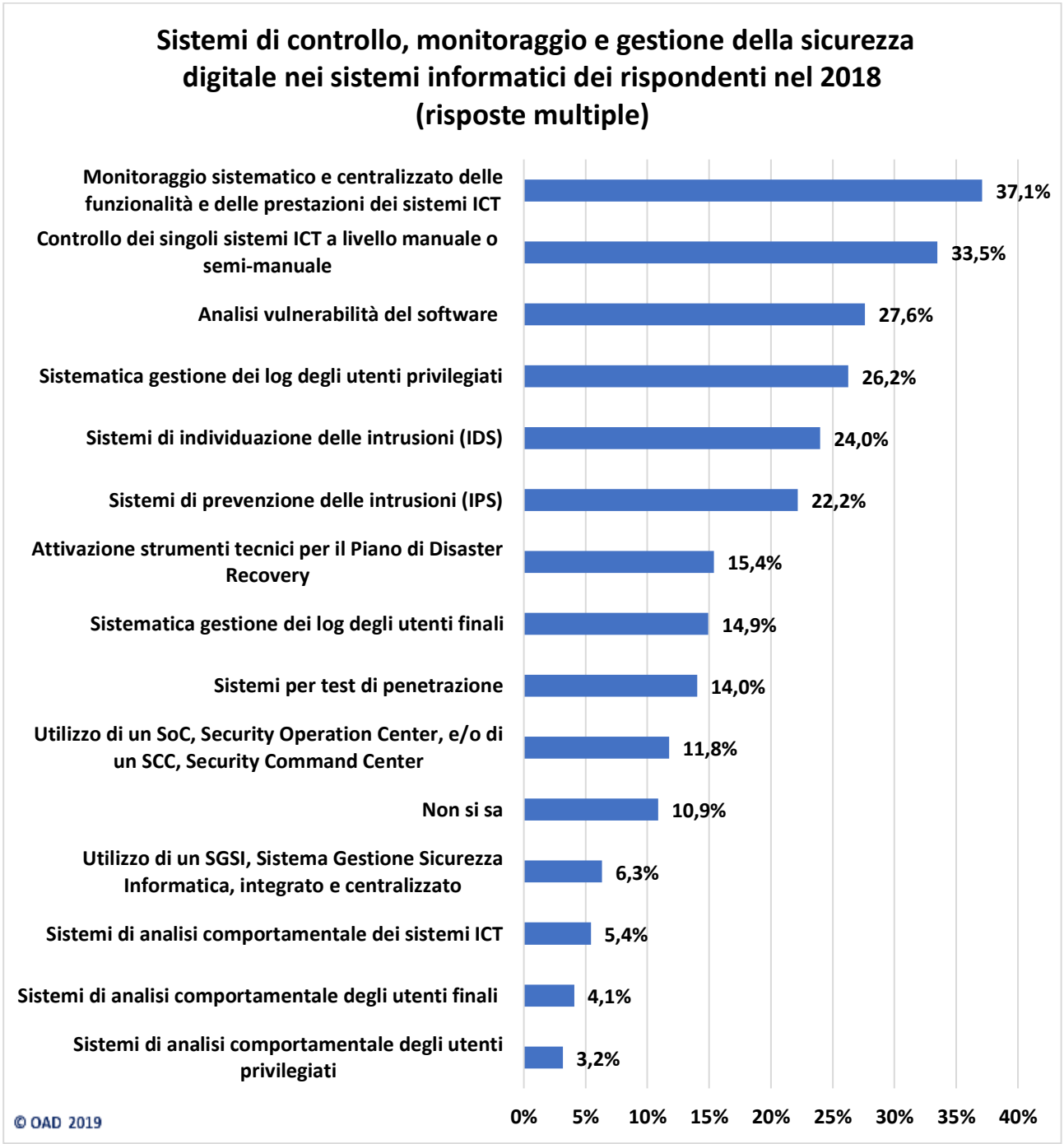

Fig. 9.3-1

È opportuno precisare la differenza tra avere un piano di DR e disporre delle risorse ICT per poterlo attuare, alla bisogna: il piano di DR è un documento, più o meno dettagliato, che specifica come e quando attuare un DR con misure tecniche ed organizzative; invece aver disponibili le misure tecniche significa aver attivato, e quindi pagare, le risorse ICT alternative a quelle del sistema informatico, da attivare qualora quest'ultimo incorresse in un disastro. 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. Per lo stesso bacino di rispondenti del 2019, il 15,4% (fig. 9.3-1) ha le risorse ICT per attuare il proprio paino di DR, cifra che è circa la metà del 29,9% dei rispondenti che ha un piano di DR.
La fig. 10.1-2 mostra, con risposte multiple, inoltre che il 13,1% dei rispondenti ha in corso la definizione di un piano di DR.

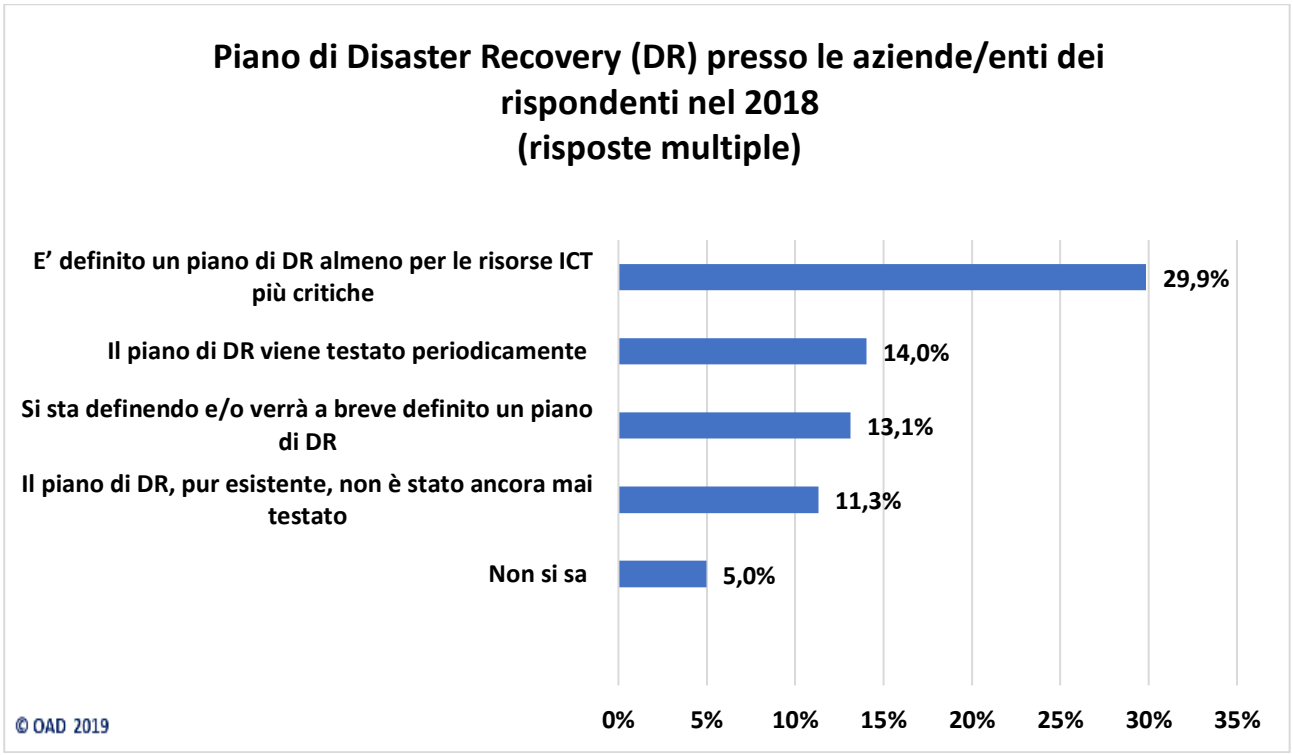

Fig. 9.3-2

Nel complesso i dati emersi evidenziano come il bacino dei rispondenti, pur utilizzando in vari casi specifiche misure e strumenti per la sicurezza digitale, anche sofisticati, come indicato in §9.1, §9.2 e nel presente paragrafo, è ancora carente, in media, nella gestione e nel controllo della stessa. Le basse percentuali sono sicuramente causate da un lato dall'alta quota di piccole e piccolissime organizzazioni tra i rispondenti, dall'altro dalla poca propensione, in Italia in generale, alla prevenzione e al costante e sistematico monitoraggio dei sistemi ICT.

10 Il campione di rispondenti e delle loro aziende/enti emerso dall'indagine

Le risposte avute al questionario OAD 2019 sono state 296, di poco superiori ai 269 dell'indagine precedente, OAD 2018. La cosa positiva è che il numero di risposte complete, ossia di tutte le 116 domande del questionario 2019, è stato superiore a quelle dell'anno precedente.
I potenziali rispondenti sono stati contatti prevalentemente via posta elettronica, segnalazioni sui siti web e sui social network da AIPSI, Malabo e Reportec, oltre che dai Patrocinatori.
Le risposte ricevute sono in numero sufficiente e significativo per poter fornire delle concrete indicazioni sugli attacchi ai sistemi informatici in Italia e su quali sono le principali misure di contrasto messe in atto.

10.1 Ruolo del rispondente nell'azienda/ente

Il bacino di rispondenti, assolutamente anonimi è costituito prevalentemente da CIO e da figure operanti nella struttura dei sistemi informatici, la UOSI, dai fornitori ICT e dai consulenti che gestiscono per l'azienda/ente la sicurezza digitale (interamente o sue parti), fino ai responsabili di massimo livello delle aziende piccole e piccolissime che conoscono e decidono per i loro sistemi informatici e la relativa sicurezza.

La fig. 10.1-1 mostra la ripartizione dei compilatori per ruolo: al primo posto, con il 18,3% sul totale dei rispondenti, sono responsabili del sistema informatico, i CIO, Chief Information Officer, cui seguono con il 17% professionisti esterni alla struttura, anche appartenenti a società specializzate, che espletano come terze parti il ruolo di gestori della sicurezza digitale. Questo dato conferma il fenomeno della terziarizzazione a specialisti/società specializzate nella sicurezza digitale.
Con il medesimo 17% del bacino dei rispondenti si collocano i vertici aziendali (costituiti tipicamente da Proprietario, Partner, Presidente, Amministratore Unico o Delegato, Direttore Generale) soprattutto per la forte incidenza delle piccole e piccolissime aziende, oltre che degli studi professionali (ad esempio di avvocati, anche grazie al Patrocinio di FiiF, il Fondo per l'innovazione del Consiglio Nazionale Forense). Con il 15% il personale interno alla struttura UOSI: quindi tra CIO e suo personale, si arriva a 1/3 esatto dei rispondenti, CISO, Chief Information Security Officer, a parte. I rispondenti con ruolo di responsabile della sicurezza digitale, i CISO, sono solo il 7,2%, e questo è chiaro indicatore di come nelle organizzazioni italiane questo ruolo non è molto presente. Con il 9,7% il CTO, Chief Technology Officer: è una figura di alto livello tipica delle industrie manifatturiere e di quelle ICT che realizzano prodotti e servizi.

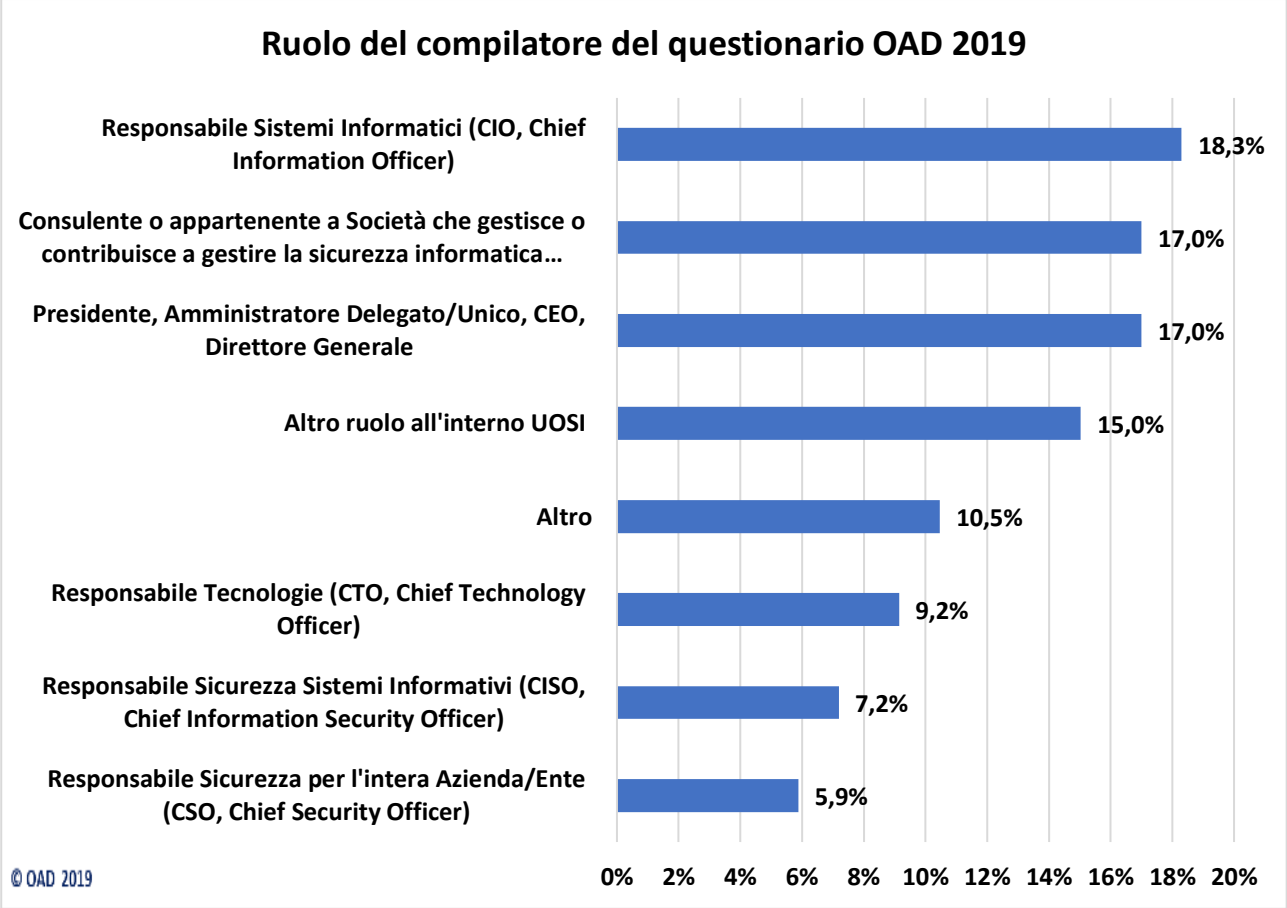

Fig. 10.1-1

All'ultimo posto, con il 5,9%, il CSO, Chief Security Officer, il responsabile della intera sicurezza aziendale. Tale percentuale è ragionevole, dato che questo ruolo è tipico di grandi e grandissime organizzazioni: difficilmente si occupa di sicurezza digitale, anche se in alcune organizzazioni il CISO dipende gerarchicamente dal CSO per una più chiara e netta separazione dei ruoli e delle responsabilità con il personale dell'UOSI, il CIO per primo. Nella voce "Altro" vari rispondenti hanno specificato il loro ruolo: alcuni hanno indicato quelli di IT Manager e di Data Scientist, quello di responsabili commerciali[24], quello di Responsabile della sicurezza sul lavoro (RSPP), quello di responsabile della privacy e della protezione dei dati (DPO), quello di quadro e di impiegato, tralasciando di indicare di quale unità organizzativa.

10.2 L'azienda/ente del rispondente

La fig. 10.2-1 riporta la tabella con la tassonomia della classificazione di OAD dei settori merceologici: essa fa riferimento alla classificazione ATECO, sulla cui base si sono raggruppati alcune classi e alla quale si sono aggiunte le Pubbliche Amministrazioni Centrali e Locali.
Questa classificazione abbastanza dettagliata, pur con vari raggruppamenti, è stata ritenuta utile per ridurre possibili errori di posizionamento della loro azienda da parte dei rispondenti. Problema che era emerso nei primi anni dell'indagine OAI/OAD.

[24] Appartengono probabilmente a succursali italiane di aziende internazionali con attività in Italia prevalentemente di vendita, e che direttamente si occupano degli o seguono gli aspetti informatici in Italia, e quindi anche della sicurezza digitale

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

Fig. 10.2-1 Tabella dei settori merceologici considerati

La fig. 10.2-2 mostra la ripartizione merceologica delle aziende/enti dei rispondenti secondo la Tabella di cui sopra. Essa evidenzia da un lato che il bacino dei rispondenti emerso con l'indagine del 2019 copre tutti i settori merceologici elencati, ma dall'altro che i rispondenti appartengono per la quota maggiore al settore ICT, con un 25,7%, e al settore manifatturiero, con circa 10 punti percentuali di differenza.
Tra il 9,7 ed il 9,2% si posizionano i rispondenti del settore istruzione, dei servizi professionali e di supporto alle imprese, della sanità e assistenza sociale.
Tutti gli altri settori merceologici hanno avuto dei rispondenti, ma con percentuali dal 5,9% in giù. Come già sottolineato nei capitoli precedente, questi settori hanno avuto troppo pochi rispondenti perché possano essere elaborate rappresentative tendenze settoriali. Per questo motivo nel presente rapporto non sono state elaborate analisi e correlazioni per settori, ma solo per dimensione delle aziende/enti come numero di dipendenti.

La fig. 10.2-3 mostra la ripartizione percentuale delle aziende/enti dei rispondenti per dimensioni, in termini di numero di dipendenti, distinguendo in quattro classi quelle fino a 250 dipendenti, che raggruppano 62,6% dei rispondenti; altre 3 classi per le grandi e grandissime, che complessivamente coprono il rimanente 37,4%.
Interessante notare come le due classi più piccole, fino a 10 e fino a 50 dipendenti, hanno raccolto la medesima e più alta percentuale: 18,7%.
La distribuzione per dimensione delle aziende/enti del campione emerso risulta abbastanza ben bilanciato e rappresentativo delle varie classi considerate in OAD, ed anche in riferimento alle già

citate e più recenti statistiche ISTAT sulle imprese attive (§6 e fig. 6-4), pur con una percentuale ben più alta per le organizzazioni oltre i 250 dipendenti. La Tabella di fig. 10.2-4 confronta, a livello percentuale, la ripartizione ISTAT con quella emersa dal bacino dei rispondenti al questionario 2019 OAD.
Per le Pubbliche Amministrazioni, centrali e locali, non si hanno dati precisi: le stime più autorevoli indicano circa 55.000 enti, con autonomia funzionale e finanziaria, incluse scuole, ASL ed ospedali.

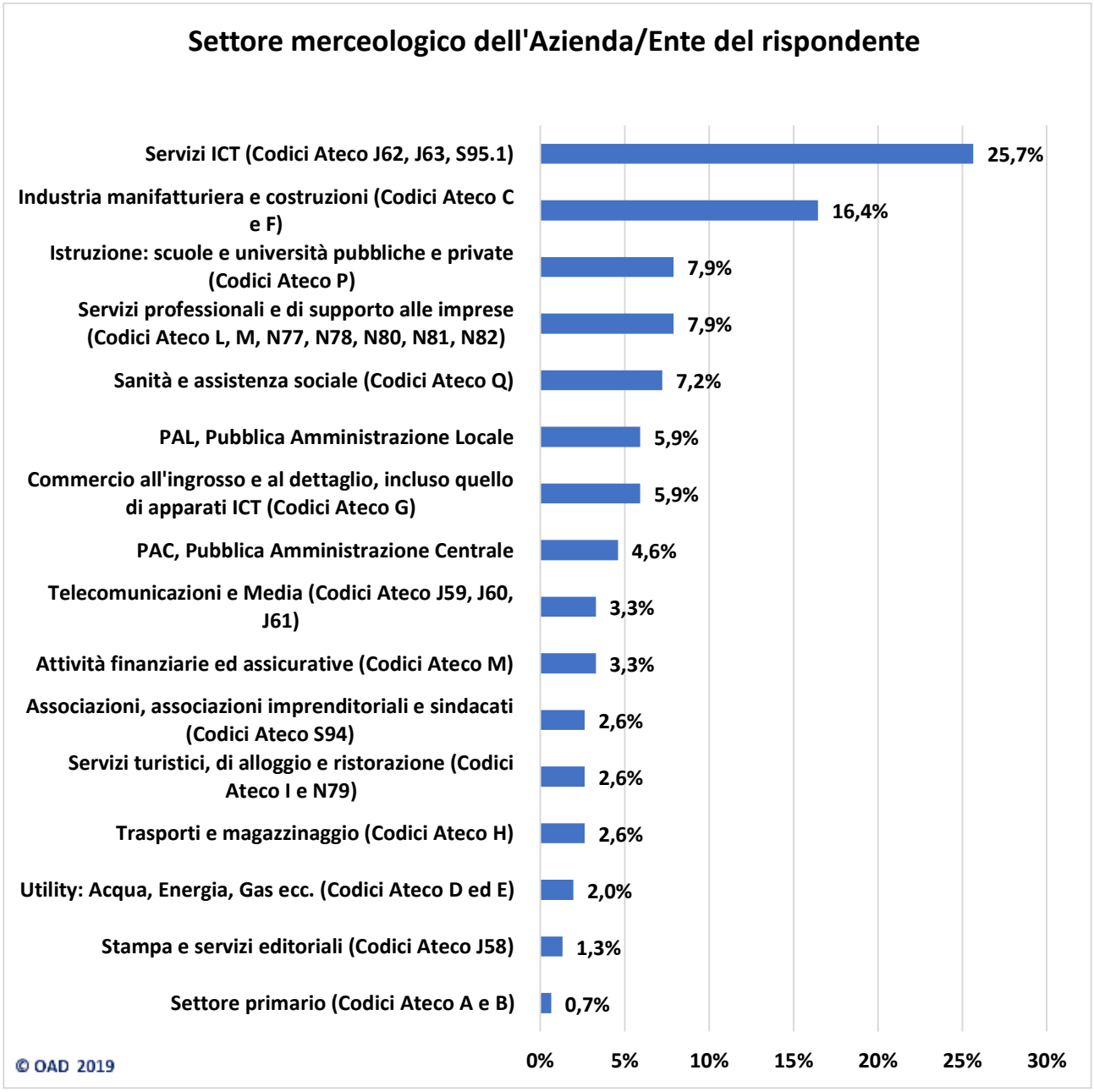

Fig. 10.2-2

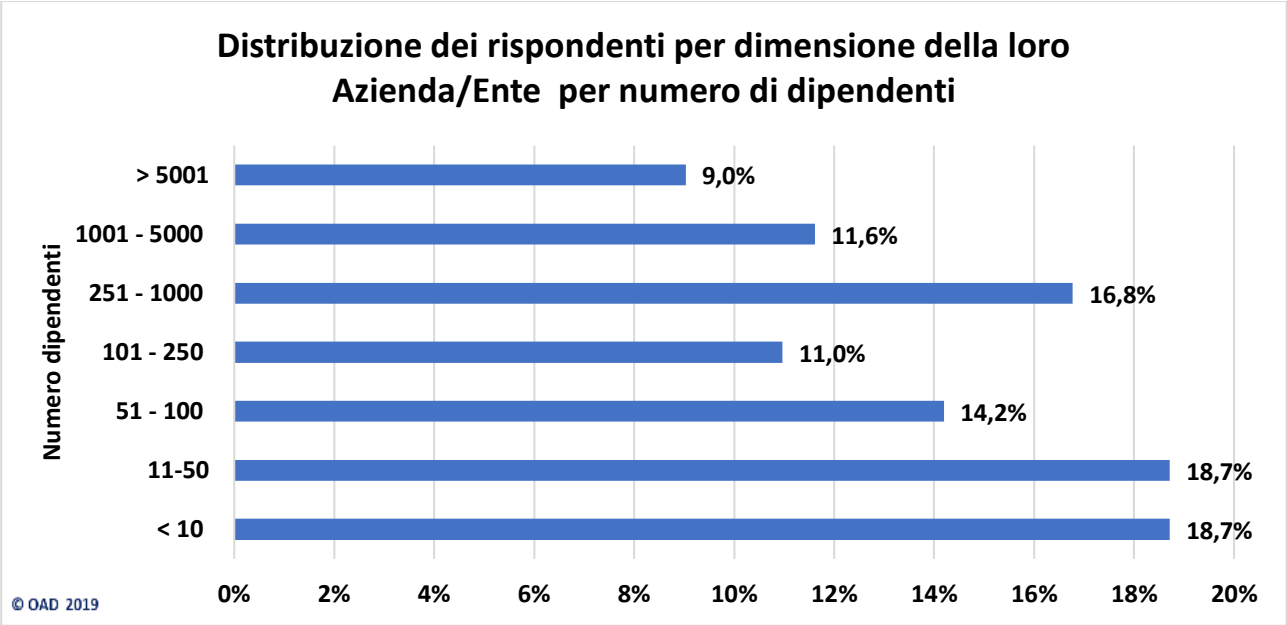

Fig. 10.2-3

Ripartizione ISTAT	Numero dipendenti	% sul totale ISTAT	% rispondenti OAD 2019
< 10	4.179.818	95,05%	18,70%
11-49	191.004	4,34%	18,70%
50-249	22.906	0,52%	25,20%
>250	3.895	0,09%	37,40%
Totale dipendenti ISTAT /rispondenti OAD 2019	4.397.623		296
1-249	4.393.728	99,91%	62,60%

Fig. 10.2-4

La fig. 10.2-5 mostra la ripartizione percentuale delle aziende/enti dei rispondenti per il fatturato annuo nell'ultimo anno disponibile, fatturato suddiviso nelle quattro classi indicate nel questionario e riportate in figura.

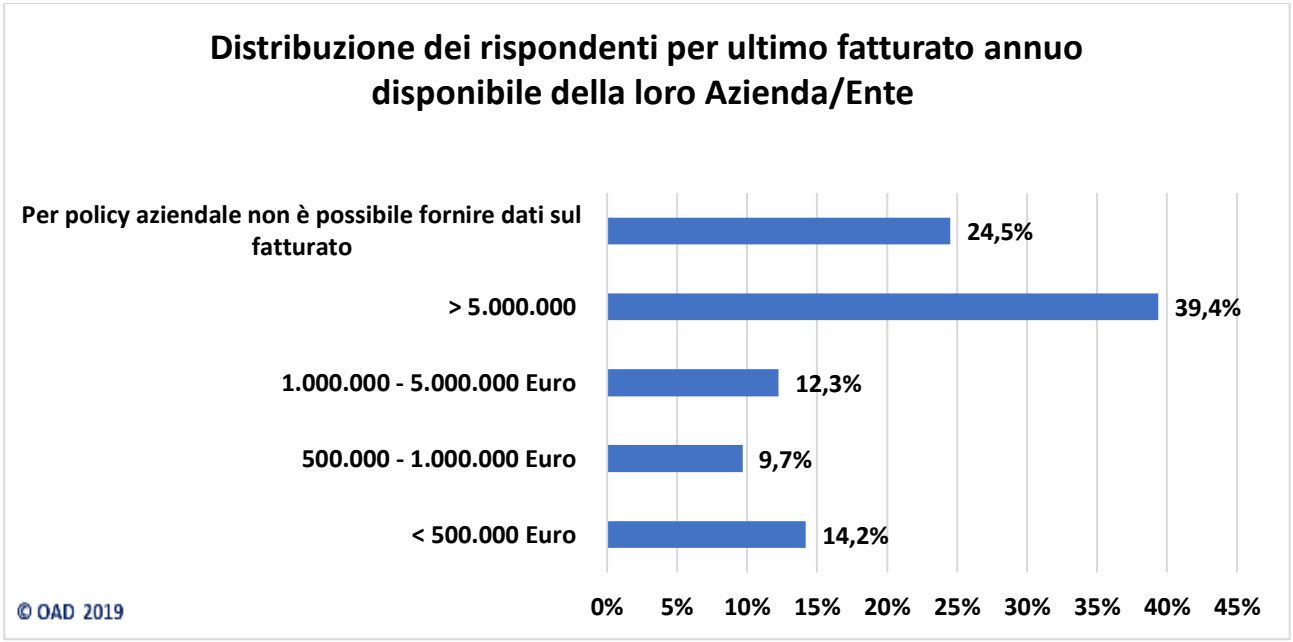

Fig. 10.2-5

Il questionario 2019 prevedeva: fino a € 500.000, da € 500.000 a 1 Milione, da 1 a 5 Milioni €, oltre i 5 Milioni di €.
Il bacino di rispondenti è abbastanza ben bilanciato rispetto alla distribuzione di fatturato annuo, considerando il numero ben maggiore di strutture piccole rispetto alle grandi, e quindi di fatturati piccoli rispetto a quelli grandi. La maggior parte dei rispondenti, 39,4% dichiara che la sua azienda/ente fattura più di 5 Mlni nell'ultimo anno di bilancio. Da sottolineare che quasi ¼ dei rispondenti non ha potuto/voluto fornire la classe di fatturato nella quale rientra la sua azienda/ente, affermando che le policy di riservatezza gli impedivano di indicare una classe di fatturato, pur in una indagine completamente anonima.

La fig. 10.2-6 mostra la distribuzione dell'azienda/ente del dipendente per area geografica di copertura delle attività svolte: la stragrande maggioranza opera in Italia, il 74,5% e di questi il 35,3% nel solo nord Italia, mentre il 25,5% opera a livello internazionale con l'Europa ed il resto del mondo.

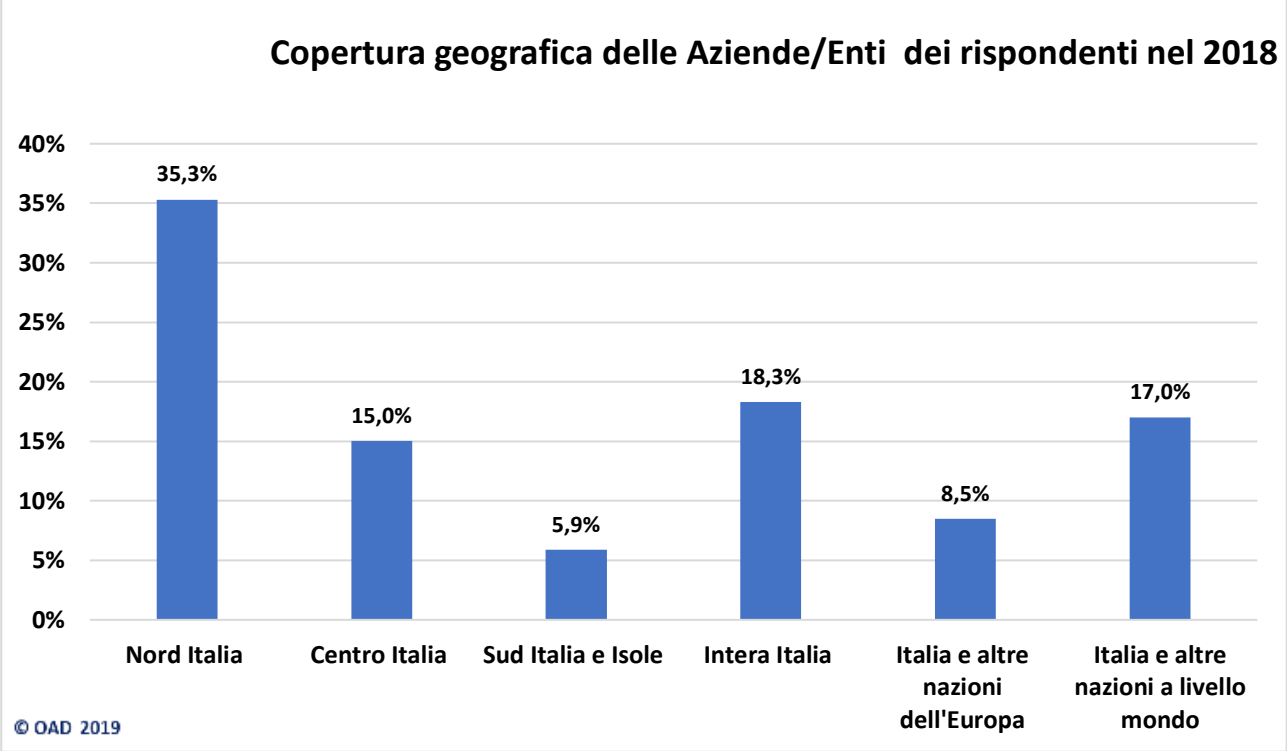

Fig. 10.2-6

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

Come per tutte le precedenti edizioni di OAI-OAD, anche per il 2018 il questionario OAD poneva alcune domande per inquadrare tecnicamente il tipo di sistema informatico dell'azienda/ente del rispondente, iniziando dal livello di affidabilità e disponibilità del sistema informatico nel suo complesso.

La fig. 10.3-1 mostra le risposte, multiple, a questa prima domanda: quasi il 30% dei rispondenti ha posto le risorse ICT più critiche in alta affidabilità al 99%. Quasi il 14% ha un piano di business continuity, e quindi dovrebbe avere anche un piano di DR.
Il 15,8% dei rispondenti dichiara che buona parte dei processi per la gestione del sistema informatico e della sua sicurezza sono automatizzati: questo dato evidenzia come la maggior parte dei sistemi ICT sia ancora "gestita manualmente", unità per unità, ed è una risposta ragionevole, data la percentuale di piccolissime organizzazioni rispondenti. Il 16,3% dei rispondenti afferma che il proprio sistema informatico, in toto o quanto meno le sue parti più critiche, funziona anche in caso di eventi imprevisti.

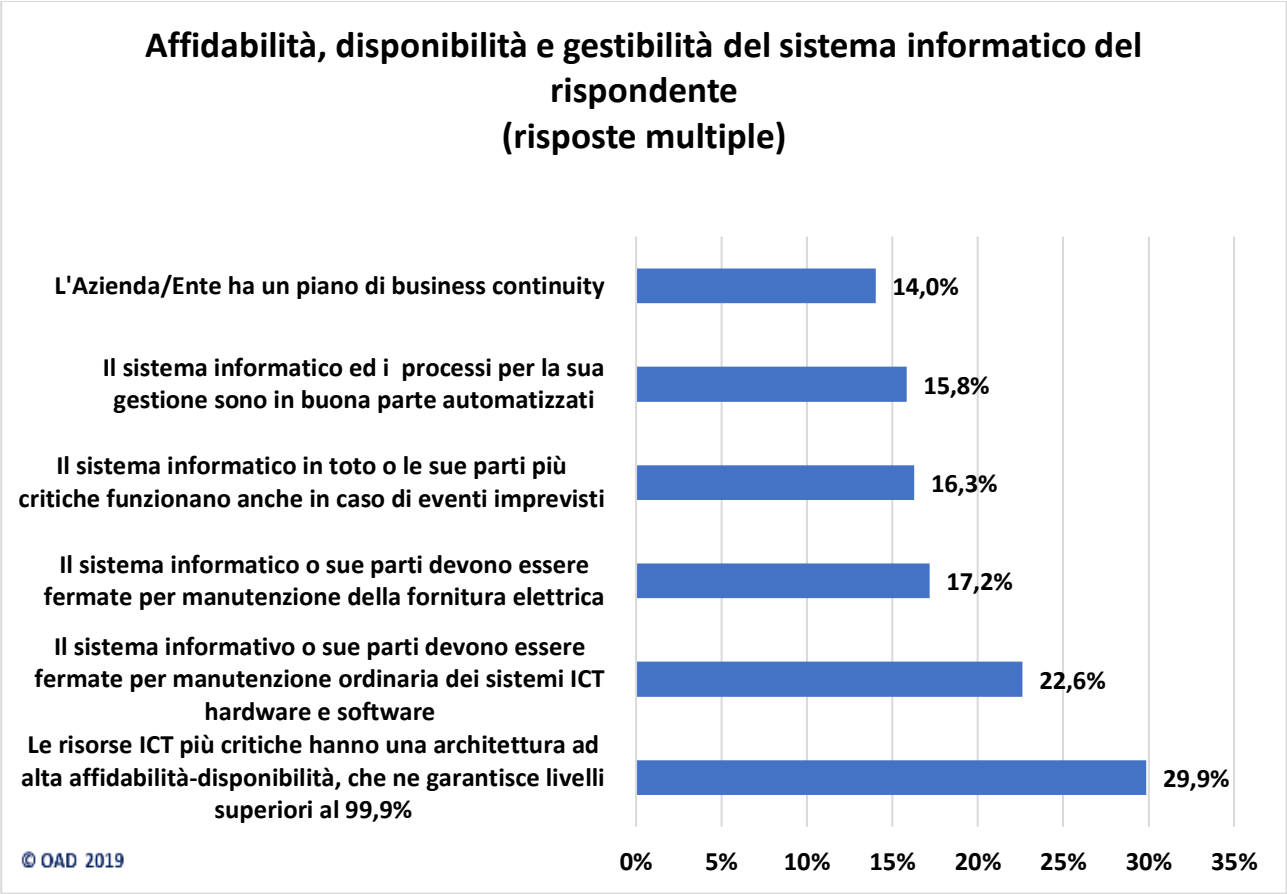

Fig. 10.3-1

La fig. 10.3-2, con risposte multiple, mostra in percentuale il numero di server, sia fisici che virtuali, presenti nei vari ambienti di produzione, di test e di sviluppo del sistema informatico delle aziende/enti di rispondenti. I dati emersi sono congruenti con le percentuali di distribuzione per numero di dipendenti: il 68% dei rispondenti indica fino a 100 server, dimensioni tipiche per il sistema informatico di una medio-piccola organizzazione.

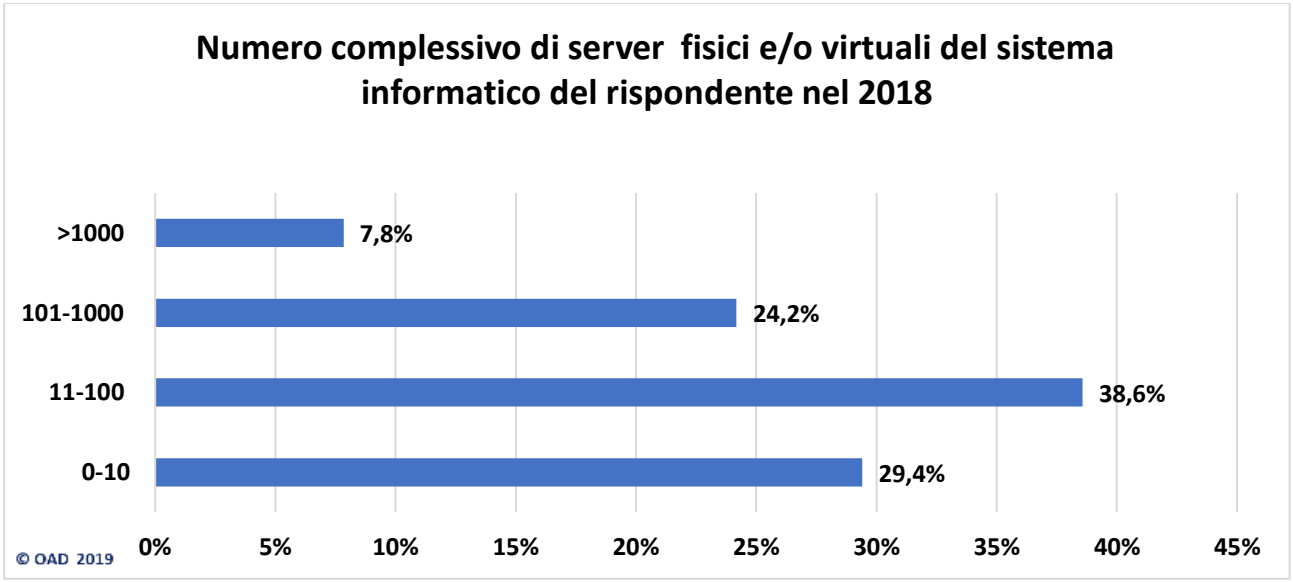

Fig. 10.3-2

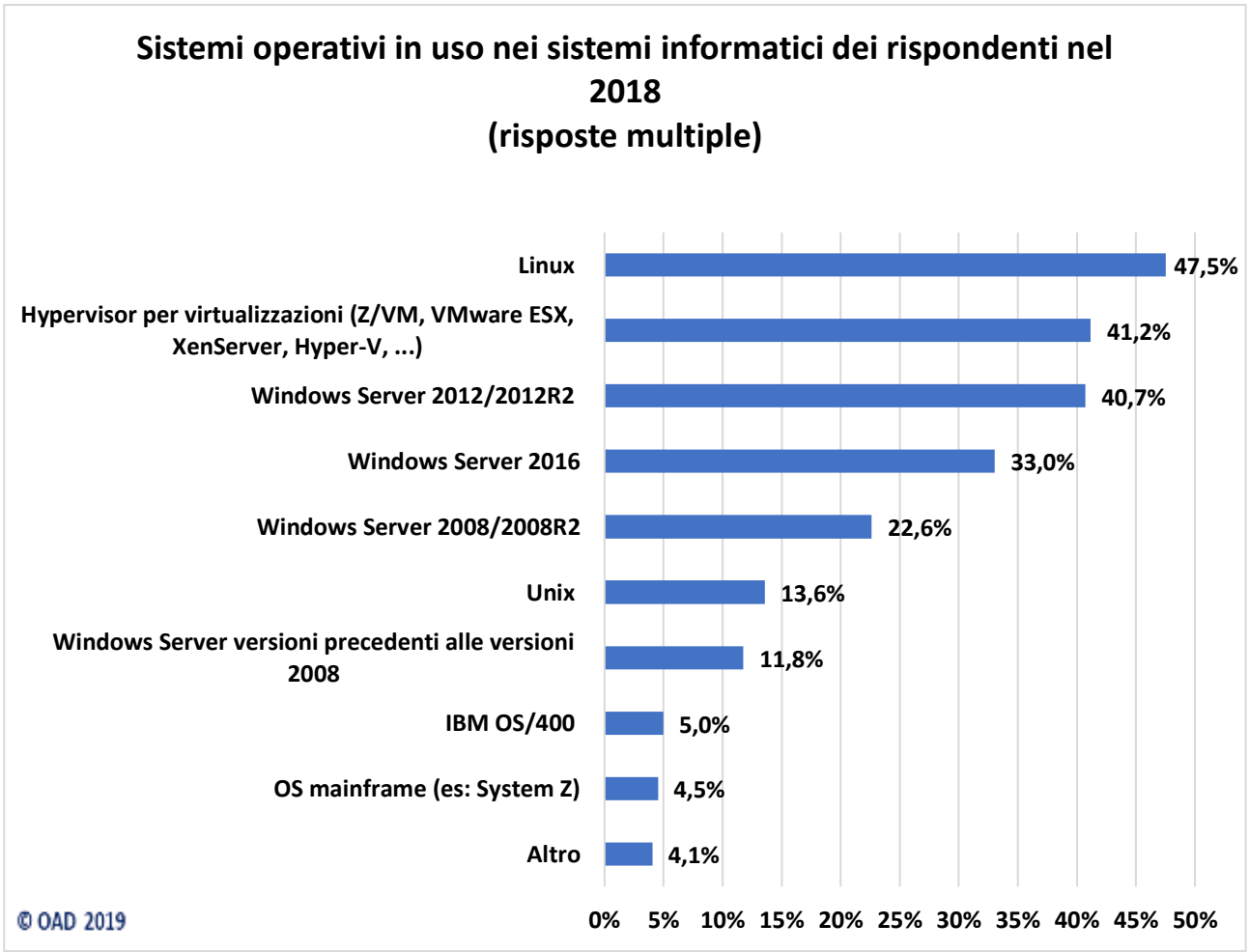

Fig. 10.3-3

La fig. 10.3-3, con risposte multiple, caratterizza i server dei sistemi informatici dei rispondenti per il sistema operativo usato: la figura, con risposte multiple, evidenzia la ripartizione tra l'ambiente Windows di Microsoft, e l'ambiente Linux-Unix e quello degli hypervisor per la virtualizzazione. La prevalenza percentuale dei rispondenti è per le varie versioni di Windows, ed è significativo che quasi la metà dei rispondenti utilizza vari tipi di hypervisor per la virtualizzazione dei server. Una piccola quota del 5% utilizza sistemi IBM AS400, nel passato assai diffusi nelle medie imprese italiane, ed il 4,5% utilizza mainframe con i relativi specifici sistemi operativi. Nella voce "Altro" sono stati indicati l'uso del più recente OS di Windows, il Windows Server STD 2019, l'uso di soli PC senza server, l'uso di sistemi MAC di Apple (a livello PC, non sono server).

La fig. 10.3-4 mostra la distribuzione percentuale del numero di posti di lavoro fissi, prevalentemente PC, del sistema informatico dei rispondenti: la maggior parte, il 62,3%, entro i 100 posti fissi, e di questi più di ¼ sotto i 10, come è tipico per le piccolissime organizzazioni.

La fig.10.3-5 mostra l'analoga situazione sui dispositivi d'utente mobili, smartphone e tablet in particolare, di proprietà delle aziende/enti dei rispondenti. Anche per i sistemi mobili, come per i fissi della figura precedente, la percentuale più alta risulta nella fascia 11-100.

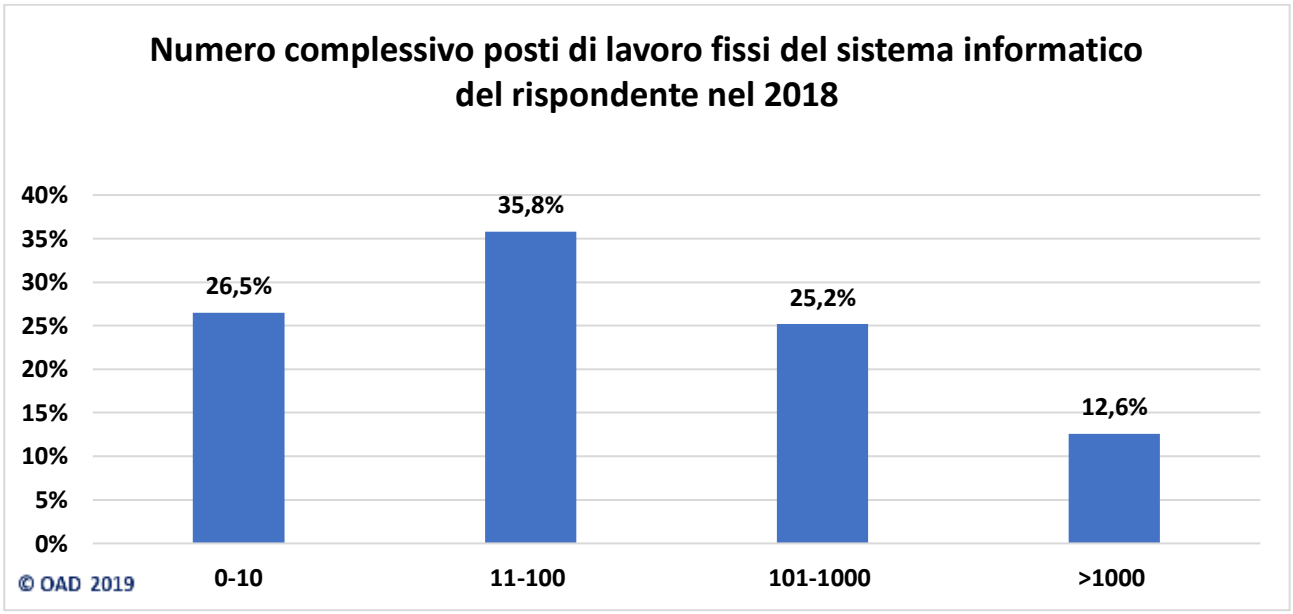

Fig. 10.3-4

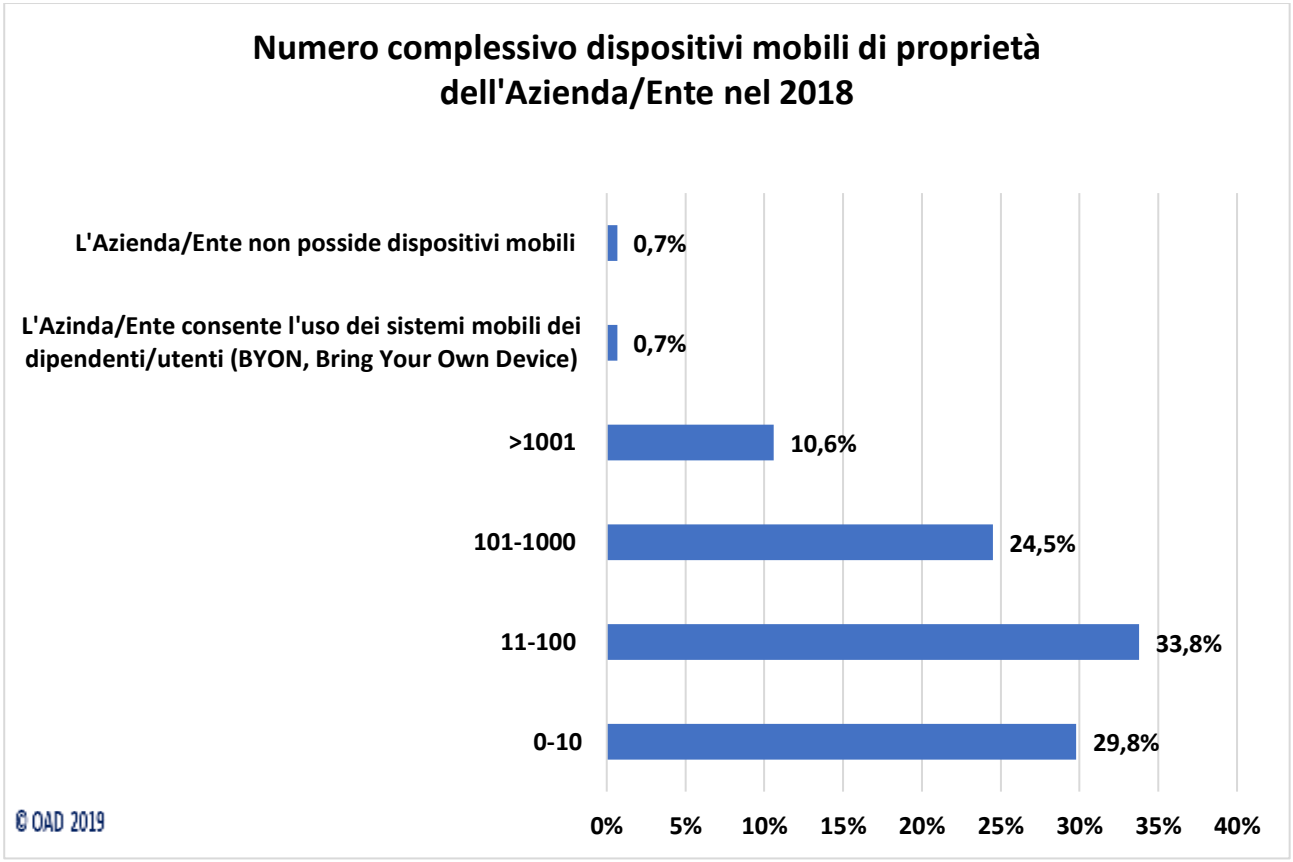

Fig. 10.3-5

Importante e crescente anche in Italia la terziarizzazione dei sistemi ICT, in particolare l'uso di servizi in cloud, oltre che della loro gestione.
La fig.10.3-6, con risposte multiple, mostra la situazione nel bacino emerso dei rispondenti. Significativo evidenziare come solo l'8,6% dei rispondenti non attua alcuna terziarizzazione, rispetto al 40,30% della precedente edizione: la terziarizzazione e l'suo del cloud si vanno imponendo soprattutto per i sistemi informatici delle piccole organizzazioni.

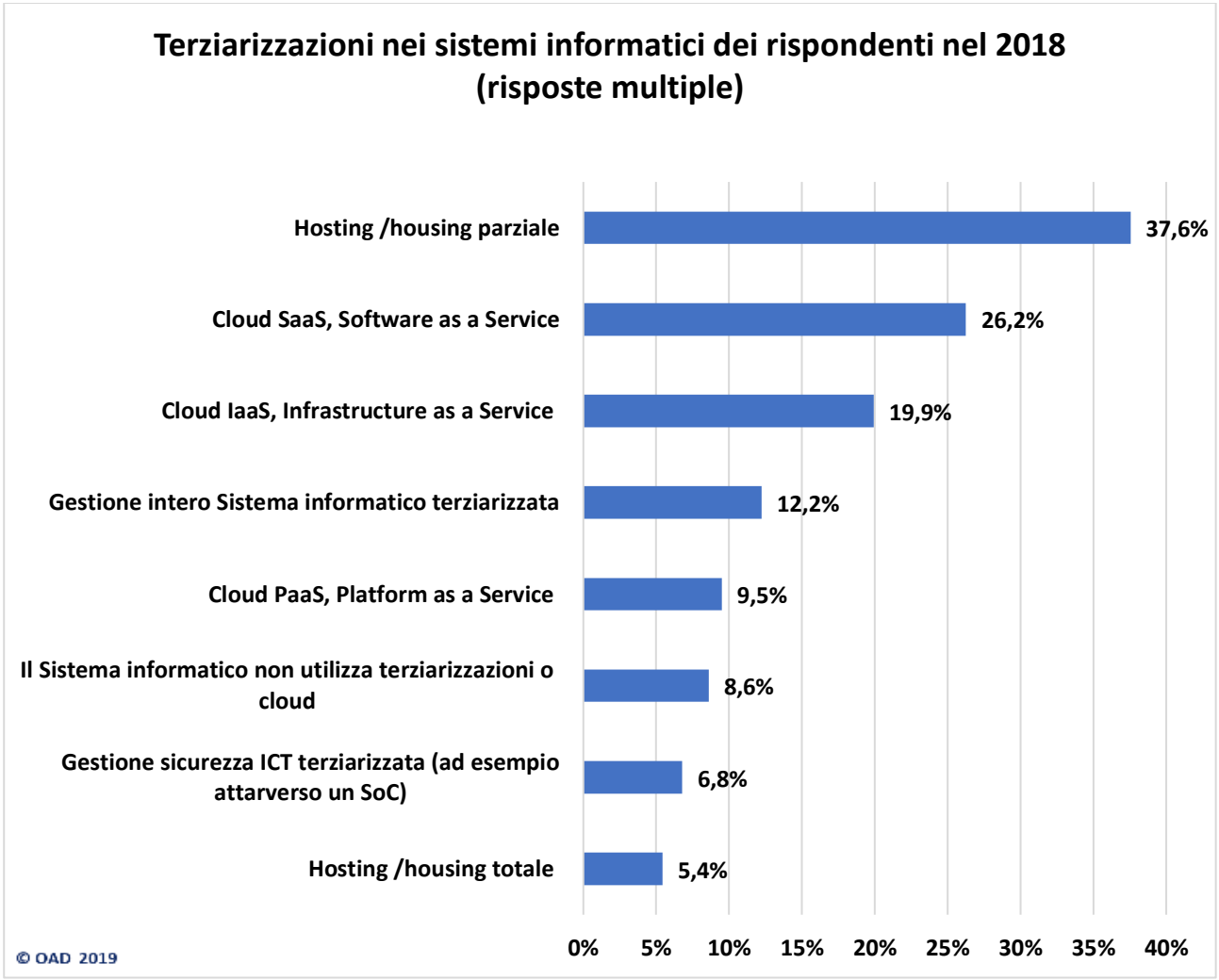

Fig. 10.3-6

Il generico termine OT, Operational Technology, usato anche in italiano, include i vari sistemi di controllo ed automazione industriale e dei processi, quali i sistemi a controllo numerico (CNC), i sistemi SCADA, i Distributed Control System (DCS), gli Industrial Control System (ICS), i Programmable Logic Controlle (PLC), i Programmable Automation Controller (PAC). In OT sono anche inclusi i sistemi robotizzati, gli IoT e gli IIoT.
Questi sistemi non sono utilizzati solo in ambito del controllo di produzione e dei processi continui o non, ma anche nella gestione degli archivi cartacei e dei magazzini, nelle sale operatorie degli ospedali, nei trasporti, nella ricerca e sviluppo, nella logistica
La maggior parte di questi sistemi sono oggi basati sulle più diffuse soluzioni ICT in termini di CPU, di sistemi operativi, di linguaggi di programmazione e tendono in maniera crescente ad interoperare, via Internet e/o reti dedicate, con gli altri ambienti ed applicativi del sistema informatico, mentre negli anni passati erano per lo più usati e gestititi direttamente dai responsabili della produzione e della ricerca, non dal CIO.
Questa tendenza sta ampliando fortemente la superficie di possibile attacco digitale, e tenendo anche conto della numerosità la sicurezza digitale dell'OT di questi dispositivi, essi stanno ponendosi al centro della sicurezza digitale come uno dei problemi critici di cui tenere conto.
Per questi motivi, il questionario OAD 2019, così come quelli degli anni precedenti, ha posto specifiche domande sugli attacchi a questi sistemi, chiedendo anche come essi si integrano nel sistema informatico e come sono gestiti.

La fig. 10.3-7, con risposte multiple, mostra la situazione delle aziende/enti dei rispondenti nell'ambiente OT: solo pochi utilizzano sistemi OT o hanno in corso studi di fattibilità per la loro messa in esercizio. E' da evidenziare come il 4,5% dei rispondenti afferma che i sistemi OT sono collegati al ed interoperano con il sistema informatico. Tra i rispondenti che utilizzano sistemi di automazione, la percentuale più alta, 8,1%, li usa per la logistica ed i magazzini, ed il 7,2 per l'automazione ed il controllo dei processi manifatturieri.

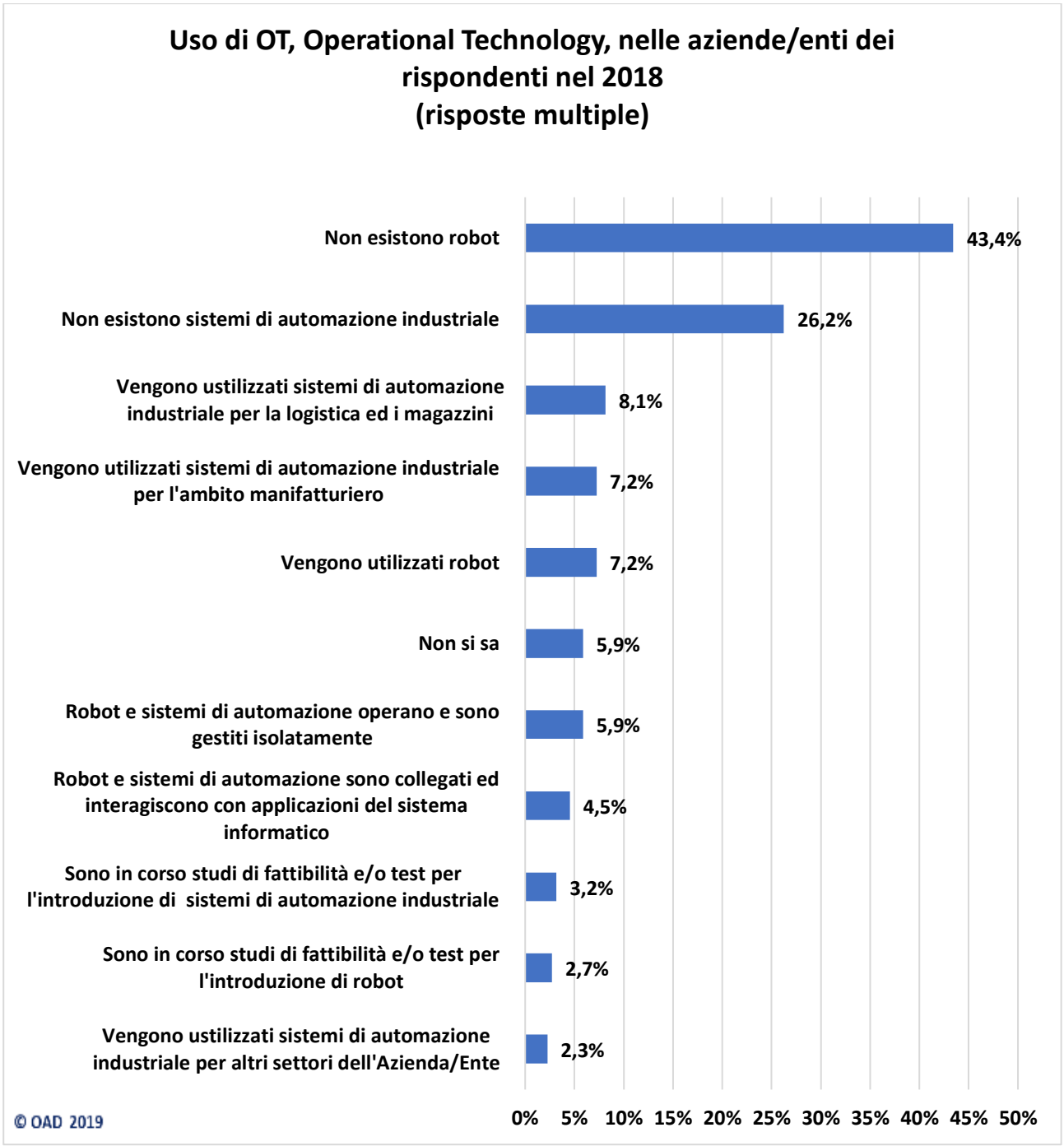

Fig. 10.3-7

Relativamente alta la percentuale dei "Non si sa", che si avvicina al 6%, ma giustificabile; oltre ad essere una conferma della correttezza e serietà dei rispondenti, che avvalora la credibilità delle risposte date, e di conseguenza dell'intero rapporto, questa percentuale è dovuta al già indicato fatto

che i sistemi informatici di controllo della produzione (e/o di processi chimici, nucleari, dei magazzini, ecc.) sono il più delle volte, in Italia, considerati "impianti", totalmente sotto il controllo della produzione, e nemmeno considerati e contabilizzati come sistemi informatici. In tali casi può capitare che il compilatore del questionario non conosca neppure la loro esistenza.

La fig. 10.3-8 con risposte multiple, approfondisce l'uso di sistemi IoT/IIoT dalle risposte ricevute sull'IoT. Interessante notare che il 10% dei rispondenti utilizza IIoT integrati con i sistemi di automazione, e con un medesimo 10% confessa di non sapere nulla in merito: come già sottolineato in altre parti del presente rapporto, la conoscenza di quanto succede nella propria azienda/ente su tale tema dipende dal ruolo del compilare: se non ha un visione ed una informativa generale, ad esempio in quanto specialista nell'UOSI su specifici temi, soprattutto in realtà medio grandi è abbastanza normale che non sappia, o sappia ben poco, di quanto succede in altre divisioni. Per il 3,2% gli IoT/IIoT sono gestititi e controllati, ma sono operanti all'esterno dall'azienda/ente: un esempio è il controllo di territori per Pubbliche Amministrazioni locali quali i comuni. Un altro 3,2% dei rispondenti, che fa parte del mondo ICT, non soli li utilizza, ma li produce e li vende.

Anche per questa edizione, come per la precedente, vengono considerate le tecniche di blockchain, anch'esse soggette ad attacchi (si veda §6.15), pur sapendo che il loro utilizzo, pur crescente, è ancora assai limitato, e soprattutto per il bacino degli attuali rispondenti, come mostrato dalla fig. 10.3-9. Solo il 4,5% dei rispondenti già utilizza, magari solo in via sperimentale, tali tecniche, sia implementate internamente, sia con soluzioni e servizi di terze parti. Il 7,2% dei rispondenti sta effettuando analisi per verificare se iniziare ad usate la blockchain. Le percentuali emerse sono nettamente più basse di quelle emerse nell'indagine dell'anno scorso, e per l'autore queste ultime sono più credibili, tenendo anche conto del tipo di aziende/enti che hanno risposto. Comunque, la blockchain anche in Italia è seriamente considerata per varie applicazioni ed ambiti, e non solo per cripto valute tipo Bitcoin: soprattutto in ambiti chiusi e controllati, la stanno studiando e sperimentando banche ed istituti finanziari, seguiti da logistica e trasporto, sistemi di prenotazione, sistemi di gestione IoT, e così via.

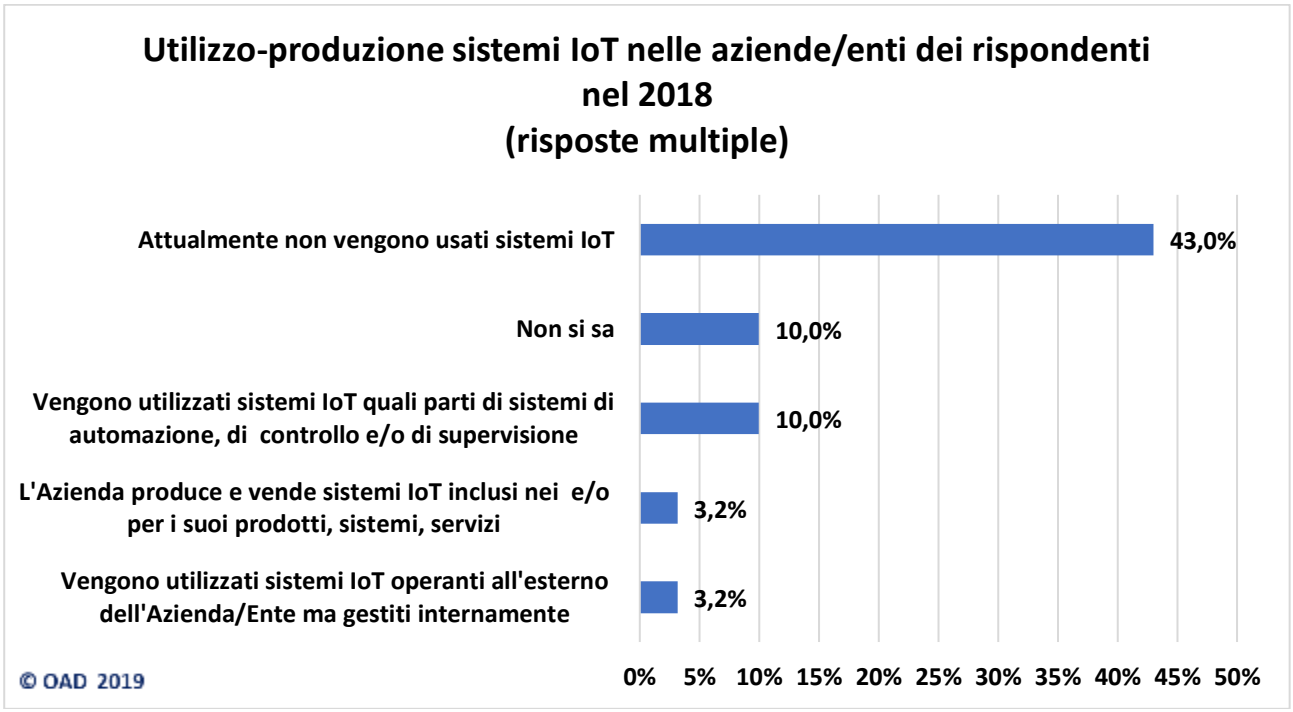

Fig.10.3-8

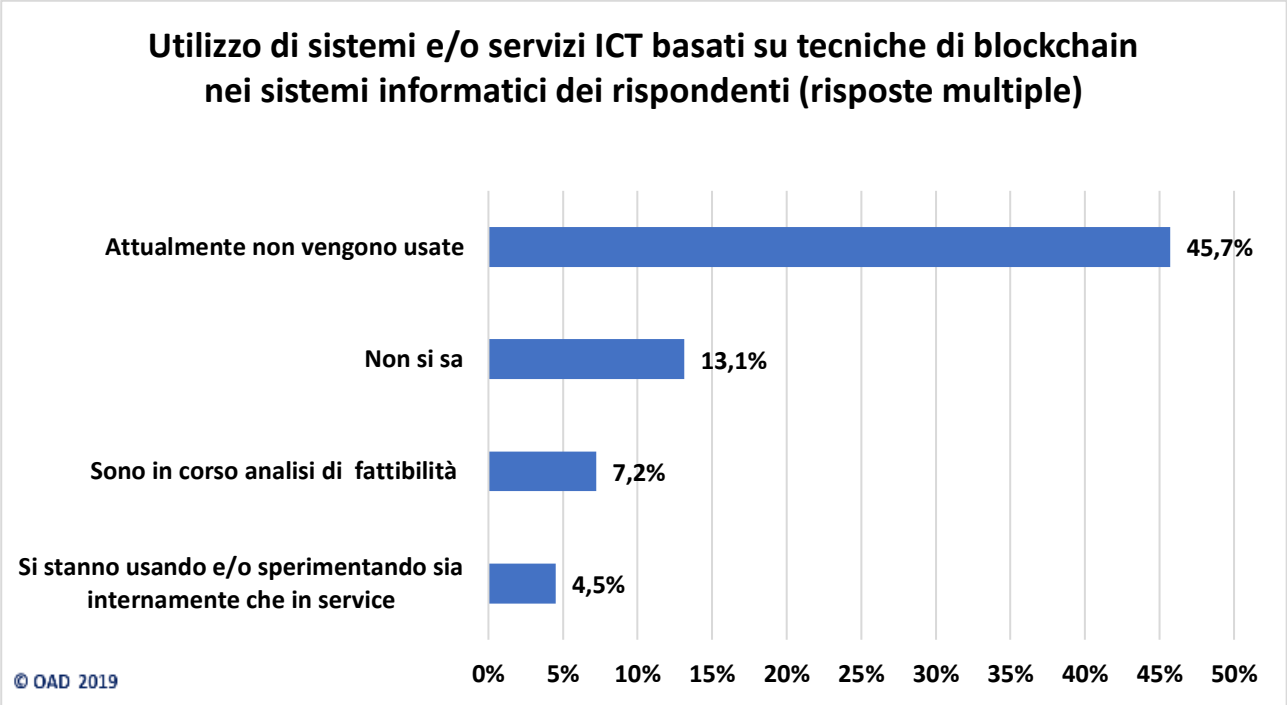
Utilizzo di sistemi e/o servizi ICT basati su tecniche di blockchain nei sistemi informatici dei rispondenti (risposte multiple)
Attualmente non vengono usate
45,7%
Non si sa
13,1%
Sono in corso analisi di fattibilità
7,2%
Si stanno usando e/o sperimentando sia internamente che in service
4,5%
0%
5%
10%
15%
20%
25%
30%
35%
40%
45%
50%
© OAD 2019

Fig. 10.3-9

11 I dati forniti dalla Polizia Postale e delle Comunicazioni

La Polizia Postale e delle Comunicazioni, grazie alla sua responsabile nazionale, il Direttore dott.ssa Nunzia Ciardi, ha fornito come in passato significativi dati sulle azioni svolte in Italia nel 2018 sul fronte del contrasto agli attacchi digitali e ai crimini informatici, facendo in particolare riferimento alle infrastrutture critiche, al crimine digitale (computer crime), in particolare quello finanziario, ai reati contro la persona attraverso reti social ed Internet, al cyber terrorismo.
Il contrasto ai crimini informatici, ora prevalentemente tutti via Internet, si basa soprattutto sulla prevenzione, sul far conoscere e far comprendere a tutti gli utenti, dalle aziende ai singoli cittadini, quali sono 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, e in maniera crescente, in questa direzione, con azioni di formazione e di sensibilizzazione a vari livelli, sia regionali sia per organizzazioni imprenditoriali ed enti, sia infine con campagna nazionali.

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

Il C.N.A.I.P.I.C., Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (https://www.commissariatodips.it/profilo/cnaipic.html /), è una struttura della Polizia Postale e delle Comunicazioni incaricata in via esclusiva della prevenzione e della repressione dei crimini informatici, di matrice comune, organizzata o terroristica, che hanno per obiettivo le infrastrutture informatizzate di natura critica e di rilevanza nazionale.
Le Infrastrutture Critiche includono tipicamente le infrastrutture ICT per la produzione e distribuzione di ogni forma di energia (elettricità, gas, ecc.), per le reti di telecomunicazione, per le reti idriche, per la sanità, per i trasporti (aereo, navale, ferroviario, stradale), per le banche ed i servizi finanziari, per la protezione e la difesa civile e militare, per il supporto degli organi governativi centrali e territoriali.
Per le Infrastrutture Critiche a livello europeo è stata emanata la Direttiva 2008/114/CE[25], per individuare e designare le infrastrutture critiche europee, nonché un approccio per migliorarne la protezione. Essa, pur se focalizzata solo sui settori dell'energia e dei trasporti, ben definisce come infrastruttura critica "*"un elemento, un sistema o parte di questo ubicato negli Stati membri che è essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale dei cittadini ed il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in uno Stato membro a causa dell'impossibilità di mantenere tali funzioni".*
Tale direttiva è stata recepita in Italia con il D.Lgs n. 61 dell'11 aprile 2011[26].

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

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

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

La tabella in fig. 11.1-1 confronta i dati forniti dalla Polizia Postale e delle Comunicazioni inerenti alle attività svolte dal C.N.A.I.P.I.C. nel 2016, 2017 e 2018 sulle infrastrutture critiche italiane.
Varie le considerazioni che si possono fare sull'analisi di questi dati, per quelli del 2016 e 2017 in gran parte effettuate nel precedente Rapporto 2018 OAD.
Il primo dato che emerge è il forte incremento di allarmi diramati, nel 2018 più che raddoppiati rispetto al 2017, e circa 12 volte di più rispetto al 2016: un indicatore incontrovertibile della crescita dei rischi ICT, causato anche dalla più volte citata estensione dell'area potenziale di attacco dovuta anche dall'interoperabilità con ambienti OT ed in particolare IoT/IIoT. Nel 2018 il numero di attacchi alle infrastrutture critiche si è fortemente ridotto, circa la metà, rispetto sia al 2017 che al 2016. Il numero delle indagini è comunque leggermente aumentato, passando dalle 70 nel 2016 alle 74 nel 2018.
Il numero delle persone denunciate è drasticamente diminuito, passando da migliaia a poche unità.
Il numero delle persone arrestate è diminuito da 3 ad 1, anche se la percentuale rispetto alle denunce nel 2018 è fortemente aumentata, date le poche denunce.
Il problema di fondo, già evidenziato e commentato nella scorsa indagine, 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, e nonostante che l'Italia abbia, e da anni, una precisa e severa legislazione, anche a livello penale, sul computer crime, e che ci sia una forza specifica di Polizia, la Polizia Postale, operante sul territorio e con il supporto di unità specializzate dell'Arma dei Carabinieri e della Finanza.
Al di là che queste forze dovrebbero essere potenziate, forse dovrebbero più strettamente collaborare tra loro, le motivazioni di fondo rimangono quelle già indicate nello scorso rapporto.
A personale giudizio dell'autore, varie le cause concomitanti: la prima è la difficoltà nel portare in giudizio il criminale cibernetico, soprattutto se è straniero, con prove incontrovertibili della sua colpevolezza. La prima precauzione di un attaccante è quella di svolgere tutte le azioni nella maniera più anonima possibile, attaccando con agent inseriti su sistemi ICT di ignari possessori a livello mondiale, e cambiando molto velocemente, nell'ordine dei minuti, i sistemi da cui controlla e guida gli attacchi: ed anche questi anonimizzati ed operanti da varie nazioni. In secondo luogo, le leggi sul computer crime differiscono molto nazione per nazione, anche a livello europeo, ed è assai difficile, soprattutto al di fuori della UE, poter effettuare delle rogatorie. In terzo luogo, la problematica del computer crime e la sua pericolosità per ogni attività e per ogni business sono ancora molto sottostimate, soprattutto a livello dei decisori aziendali, delle pubbliche amministrazioni, dei politici e probabilmente anche a livello dei giudici, dei quali ad oggi solo una minoranza ha esperienza e competenze specifiche per trattare tali crimini. Infine, i ben noti e mai risolti problemi della giustizia italiana, che sono soprattutto di tipo organizzativo, e che incidono anche sui reati informatici. Una novità questi ultimi, rispetto a crimini ben più consolidati, ben noti e in taluni casi più gravi, e che passano di fatto in second'ordine.
Per combattere realmente ed efficacemente il crimine digitale è basilare la collaborazione tra le varie polizie ed i governi, iniziando da quelli europei e del mondo occidentale, per la quale la Polizia Postale italiana è attiva e propositiva da anni, promuovendo e partecipando a vari gruppi internazionali. Ad esempio, in ambito C.N.A.I.P.I.C. è attivo il Punto di Contatto Italiano per le emergenze tecnico-operative connesse al verificarsi di episodi di criminalità ICT transnazionale, secondo quando stabilito dalla Convenzione sul Cybercrime di Budapest del 2001[27]. L'ultima riga della tabella in fig. 11.1-1 mostra che le richieste di collaborazione a livello europeo nell'ottica della Convenzione di Budapest sono aumentate nel 2018, data anche la competenza e la capacità dei professionisti del C.N.A.I.P.I.C.

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

11.2 Financial Cyber Crime

Gli attacchi sono prevalentemente per ottenere un illegale guadagno economico, e tutte le transazioni economiche sono un target. La Polizia Postale è da sempre attiva per contrastare questo tipo di crimine informatico, che include anche attacchi sull'ormai diffuso commercio elettronico e sui relativi pagamenti on line.
La tabella in fig. 11.2-1 sintetizza i risultati dell'attività della Polizia Postale e delle Comunicazioni su questo fronte. Per quanto riguarda il blocco delle transazioni fraudolente, il 2018 ha visto un forte incremento del 84,26% rispetto al 2017, e del 139,24% rispetto al 2016. Forte incrementi anche per le somme recuperate: nel 2018 il 944,08% rispetto al 2017.
Non sono stati forniti (nd, non disponibile) i dati sul numero di denunciati e arrestati nel 2018. Per quanto riguarda i dati dei due anni precedenti, vale quanto già evidenziato in §11.1: nonostante tutto il crimine informatico risulta in Italia quasi impunibile.

Financial Cyber Crime	1 gen – 31 dic 2018	1 gen – 31 dic 2017	1 gen – 31 dic 2016
Transazioni Fraudolente Bloccate	**€ 38.400.000,00**	**€ 20.839.576,00**	**€ 16.050.812,50**
Somme Recuperate	**€ 9.000.000,00**	**€ 862.000,00**	**nd**
Arrestati	**nd**	25	25
Denunciati	**nd**	2851	3772

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

Il numero ben maggiore di denunciati e soprattutto di arrestati tra Infrstrutture Critiche e Cyber Crime finanziari è un indice significativo della portata e della diffusione di questo secondo genere di attacchi.

11.3 Cyber Terrorismo

Strumenti di informatica ed Internet contribuiscono fortemente al proselitismo, alla preparazione e al coordinamento di attacchi terroristici. Attacchi solo cibernetici con intento terroristico possono colpire sia infrastrutture critiche sia a livello massivo innumerevoli medie e piccole imprese, così da paralizzare per un certo lasso di tempo l'intera economia del paese oggetto dell'attacco.
La tabella in fig. 11.3-1 fornisce pochi dati ma assai interessanti: sono stati monitorati dalla Polizia Postale nell'anno migliaia di siti web, e sono stati rimossi 250 contenuti.
Non sono stati forniti dati su quanti denunciati e quanti arrestati nell'anno.

Cyber Terrorismo	1 gen – 31 dic 2018
Spazi web monitorati	**36.000**
Contenuti rimossi	**250**

Fig. 11.3-1 Attività di contrasto al cyber terrorismo
(Fonte: Polizia Postale e delle Comunicazioni)

ALLEGATI

Allegato A Aspetti metodologici dell'indagine OAD

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

sommatoria delle risposte avute: la somma finale delle percentuali di ogni singola risposta può essere pertanto superiore o inferiore al 100%
Per le risposte singole ad una data domanda, il denominatore nel calcolo della percentuale è dato dalla somma dei rispondenti: la somma finale delle percentuali di ogni singola risposta è e deve essere 100%.
In molti casi delle domande fanno riferimento ad una specifica risposta di una domanda precedente: ad esempio se si è rilevata una certa tipologia di attacco, quali sono le tecniche con le quali, probabilmente, è stata attuata. Per queste "sotto domande" il valore al denominatore per il calcolo della percentuale è dato dal numero dei rispondenti che hanno selezionato la specifica risposta cui fa poi riferimento la successiva sotto domanda. Nell'esempio di chi ha subito un certo di tipo di attacco, il calcolo delle percentuali sulle tecniche di attacco ha come riferimento il numero di chi ha rilevato quella tipologia (quindi come denominatore nel calcolo della percentuale).
La correlazione tra i dati forniti da domande diverse dal questionario è effettuata tramite pivot del foglio elettronico contenente tutte i record delle risposte, e da questi fogli pivot vengono rielaborati i dati estratti ed eventualmente creati i relativi grafici

Il questionario OAD 2019, rispetto alle precedenti edizioni, è stato concettualmente reimpostato come descritto nel seguente paragrafo §A1. Esso è stato implementato da Malabo Srl basandosi sul software open source Lime Survey nel dominio del sito OAD, https://www.oadweb.it/, realizzato e gestito da Malabo.
Il questionario è rimasto accessibile on line via web da fine giugno ai primi di novembre 2019, con una lunga proroga sulla sua chiusura, dovuta alla cronica difficoltà di far rispondere, e correttamente, al questionario stesso. Nel complesso il numero delle persone contattate è intorno alle quattromila, appartenenti ad un ampio insieme di aziende, enti e studi professionali di ogni dimensione e settore merceologico, inclusi enti pubblici centrali e locali.
Il questionario 2019 era composto da un totale di 116 domande, molte delle quali, le sotto-domande specifiche per ogni tipo di attacco, venivano automaticamente saltate se il rispondente indicava di non aver rilevato quel tipo di attacco. Questa logica implementativa del questionario online ha permesso di ridurre significativamente i tempi per completare l'intero questionario.

A.1 La tassonomia degli attacchi digitali per OAD 2019

L'edizione 2019 ha ripreso la logica della precedente edizione del 2018, migliorando alcune definizioni e portando da 14 a 15 le tipologie di attacco considerate.
La classificazione degli attacchi distingue in modo più rigoroso e più chiaro 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.
Da OAD 2018 si è deciso di distinguere il più chiaramente possibile il target dell'attacco, ossia che cosa si attacca, dalle tecniche usate (sovente una loro combinazione), queste ultime raggruppate in 7 voci, approfondite nel paragrafo successivo §A.1.1.
Le 15 tipologie di attacco (il che cosa attacco) sono:

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

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

Nel testo del presente Rapporto 2019 OAD la tassonomia del che cosa viene attaccato è prevalentemente indicata come “tipologia attacchi”; le principali modalità di attacco, ossia il come, come “tecniche di attacco”.
L’indagine 2019 di OAD fa riferimento agli attacchi intenzionali rilevati nel 2018. Per ogni tipo di attacco (il che cosa) è stata creata una sezione specifica, con gruppi di sotto domande che includono, se l'attacco è stato rilevato (in caso contrario questa parte viene automaticamente saltata):

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

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

Facendo riferimento principalmente alle tassonomie sviluppate da CERT[28] e da Sandia[29], si sono categorizzate le tecniche di attacco sotto riportate per poter descrivere e richiedere nel Questionario 2019 OAD in modo sistematico quali sono (o quali si pensa possano essere state) le tecniche usate dall'attaccante per portare l’attacco rilevato.

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

A.1.1.1 Attacco fisico

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

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

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

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

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

A.1.1.2 Raccolta malevola e non autorizzata di informazioni

Per attaccare un sistema ICT sono utili, in taluni casi indispensabili, informazioni sia dirette sulla sua posizione, sul suo funzionamento, sulla sua configurazione, sulle misure di sicurezza di cui dispone, sugli account degli utenti sia indirette, come i nomi dei suoi utenti e dei suoi gestori, indirizzi fisici e digitali, numeri di telefono, contatti anche via rete con dipendenti potenzialmente infedeli o ingenui ecc. Innumerevoli le tecniche per carpire, direttamente o indirettamente, le informazioni che servono per attuare poi un attacco digitale. Alcune sono "manuali" e consentono di interagire con le persone che trattano con il sistema informatico e con il loro ambiente di lavoro: ad esempio recuperare informazioni dai cestini dei rifiuti o richiedere in maniera subdola informazioni sia de visu sia per telefono (anche questo è social engineering). Altre tecniche per raccogliere informazioni sono informatiche ed includono social engineering, phishing, pharming, hoax, scam, data entry in server trappola, scannerizzazioni e ricerche in Internet, ecc.

A.1.1.3 Script e programmi maligni

Gli script sono semplici programmi software scritti in un linguaggio interpretato facile da utilizzare, senza interfaccia grafica, che svolgono funzioni molto specifiche ed accessorie, ed in grado di interfacciarsi con altri programmi più complessi per svolgere operazioni più sofisticate. Gli script sono sovente usati per personalizzare la configurazione automatica del sistema, per rendere più dinamica una pagina web, per fornire comandi al sistema operativo (tipico dei così detti "script shell") ed al data base, pe personalizzare e rendere "smart" documenti Microsoft Office o simili (es. Libre Office). Esempi di linguaggi di scripting includono Bash, AppleScript, JavaScript, Perl, Python, PHP, VBScript.

Programmi in script sono usati per attacchi digitali, e quelli più semplici richiedono un intervento umano per farli giungere sul sistema bersaglio (ad esempio l'apertura di un allegato in posta elettronica o lo sfruttamento di un buffer overflow presente in una applicazione); quelli più sofisticati sono in grado di attaccare senza bisogno di interventi della vittima.

Con linguaggi più complessi e sofisticati, come C, C++, C#, Java, si possono realizzare programmi d'attacco più complessi e sofisticati, chiamati genericamente malware o codici maligni. Essi sono caratterizzati da un qualche meccanismo con il quale riescono a raggiungere il bersaglio, ed in base sono classificati con specifici nomi, e da un "payload", una parte che esegue l'azione di attacco.

La classificazione per funzioni e capacità dei malware include troian horse, ransonware, spyware, adware (si veda il Glossario in Allegato B per una sintetica spiegazione di questi termini). Occorre sottolineare che la sofisticazione oggi raggiunta da molti codici maligni rende difficile una esatta classificazione, dato che essi sono in grado di svolgere diverse funzioni anche alternative tra loro, il così detto polimorfismo.

Nella categoria "script e programmi maligni" è stata inclusa anche quella così detta di "command", ossia di comandi al sistema operativo o al DBMS che quando vengono eseguiti hanno conseguenze dannose per il sistema. Si tratta tipicamente di comandi malformati che controlli inadeguati consentono di mandare in esecuzione. La tipica conseguenza è l'esecuzione di un comando che altrimenti non sarebbe stato autorizzato. Il comando può modificare i diritti di accesso al sistema, consentire di interrogare, modificare, distruggere informazioni. L'attaccante in questi casi ha solo attivato una sessione Telnet con il bersaglio o, nel caso di "SQL injection" solo scritto pochi caratteri in un form web. Un esempio di comando al DB è il XSS (Cross Site Scripting).

A.1.1.4 Agenti autonomi

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

A.1.1.5 Toolkit

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

A.1.1.6 Botnet e simili

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

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

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

Allegato B Glossario dei principali termini ed acronimi sugli attacchi informatici

Glossario degli acronimi e dei termini tecnici usati e/o da considerare nella lettura del Rapporto OAD 2018.

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

- Botnet: per la sicurezza ICT questo termine indica un insieme di computer, chiamati “zombi”, che a loro insaputa hanno agenti (programmi) malevoli dai quali partono attacchi distribuiti, tipicamente DDOS.
- Buffer overflow: consiste nel sovra-scrivere in un buffer o in uno stack del programma dati o istruzioni con i quali il programma stesso può comportarsi in maniera diversa dal previsto, fornire dati errati, bloccare il sistema operativo, ecc.
- BYOD, Bring Your Own Device: policy aziendale che consente l'utilizzo di dispositivi mobili di proprietà dell'utente anche nell'ambito dei sistemi dell'azienda/ente. Il fenomeno è chiamato anche consumerizzazione.
- Captcha, Completely Automated PublicTuring test to tell Computers and Humans Apart: l'acronimo indica una famiglia di test costituita da una o più domande e risposte per assicurarsi che l'utente sia un essere umano e non un programma software.
- 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.
- Churn rate: tasso di abbandono a favore della concorrenza, tipicamente dopo un attacco.
- CIO, Chief Information Officer: il responsabile dell’intero sistema informatico.
- CISA, ISACA Certified Information Systems Auditor di ISACA.
- CISO, Chief Information Security Officer: il responsabile della sicurezza digitale dell’intero sistema informatico.
- CISSP, Certified Information Systems Security Professional.
- Cluster: insieme di computer e/o di schede (es lame di un sistema blade) cooperanti per aumentare l'affidabilità complessiva del sistema; il termine è anche usato per identificare un insieme contiguo di settori in un disco rigido.
- Cnaipic, Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche.
- Consumerizzazione: vedi BYOD
- CSO, Chief Security Officer; responsabile della sicurezza dell’intera azienda/ente, prevalentemente per la sicurezza fisica di edifici e del personale. In alcune organizzazioni il CISO riporta a questa figura.
- CSSLP, Certified Secure Software Lifecycle Professional.
- CTO, Chief Technology Officer: è il direttore tecnico di più alto livello, tipicamente per aziende che producono prodotti e servizi. In talune organizzazioni il CIO riporta a questa figura.
- DAC, Discretionary Access Control.
- Darknet: sistema usato in Internet per monitorare la rete e possibili attaccanti, con funzionalità simili a quelle di un honeypot.
- Dark web: siti web che si raggiungono via Internet ma attraverso specifici software, configurazioni e accessi autorizzativi, e non sono indicizzati, e quindi ritrovabili, dai motori di ricerca. Molti dark web contengono informazioni criminali, dalla pedopornografia a strumenti informatici di attacco e da account e identità digitali rubate.
- Data Breach: letteralmente “violazione dei dati”, spesso è usato come sinonimo di furto di identità digitale. Tecnicamente è usato per indicare l’accesso a banche dati o a file system contenenti identità digitali o informazioni a quest’ultime correlate.
- Data Center, Centro Dati: si veda CED
- DB, Data Base: banca dati.
- DBMS, Data Base Management System.
- DCS, Distributed Control System.
- Deadlock: un caso particolare di “race condition”, consiste nella condizione in cui due o più processi non sono più in grado di proseguire perché ciascuno aspetta il risultato di una operazione che dovrebbe essere eseguita dall'altro.
- Deamon: software di base operante in back-ground in un ambiente multi-tasking.

- Defacing o defacement: in inglese significa deturpare, e nel gergo della sicurezza informatica indica un attacco ad un sito web per modificarlo o distruggerlo; spesso con tale attacco viene modificata solo la home-page a scopo dimostrativo.
- Denial of service (DOS) e Distributed Denial of service (DDOS): attacco per saturare sistemi e servizi ed impedire la loro disponibilità.
- Dialer: programma software che connette il sistema ad Internet, ad una rete o ad un computer remoto tramite linea telefonica (PSTN o ISDN); può essere utilizzato per attacchi e frodi.
- DLP, Data Loss Prevention: sistemi e tecniche per prevenire la perdita e/o il furto di dati nel corso del loro trattamento, archiviazione inclusa.
- DMZ, DeMilitarized Zone: isola del sistema informatico costituita da sottoreti locali, fisiche o virtuali, ove sono allocati i server esposti ad Internet.
- DNS, Domain Name System: sistema gerarchico di nomi (naming) di host su Internet che vengono associati al loro indirizzo IP di identificazione nella rete.
- Drive-by Downloads: attacchi causati dallo scaricare (anche inconsapevolmente) codici maligni o programmi malevoli.
- Drones, Droni: vedi bots.
- ECDL, European Computer Driving Licence: ideata, realizzata e gestita da AICA, ora al 20° anno di vita, è il patentino europeo di conoscenza di vari aspetti dell'ICT soprattutto nell'ottica dell'utente finale.
- eCF, European Competence Framework: quadro europeo standardizzato sulle competenze digitali e sui ruoli ICT che espletano professionalmente tali competenze.
- FTP, File Transfer Protocol: protocollo per il trasferimento di file.
- FTPs, FTP sicuro con la criptazione dei dati durante la trasmissione
- Exploit: attacco ad una risorsa ICT utilizzando sue vulnerabilità.
- Extranet: Intranet accessibile anche da utenti esterni all'azienda/ente.
- Ethical hacking: attività di provare attacchi ai fini di scoprire bachi e vulnerabilità dei programmi, e porvi rimedio con opportune patch/fix.
- Eucip, European Certification of Informatics Professionals: è ora sostituito da eCF.
- Fix: correzione di un programma software, usato spesso come sinonimo di patch.
- Flash threats: tipi di virus in grado di diffondersi molto velocemente.
- Form: in informatica indica il campo generato da una applicazione visibile su una schermata, nel quale l'utente deve inserire dei caratteri per interagire con l'applicazione stessa; è l'elemento base per l'interfaccia tra utente e applicazione per l'inserimento dei dati (data entry).
- FTPS, File Transfer Protocol Secure: per il trasferimento di file crittati
- FW, FireWall generuico, normalmente di rete.
- FWA, FireWall Applicativo.
- Hactivism:termne derivato dalla combinazione di hack e di activism, indica un uso sovversivo dell'ICT per promuovere un'ideologia politica/religiosa e la sua agenda o un cambiamento sociale.
- Hijacking: tipico attacco in rete "dell'uomo in mezzo" tra due interlocutori, che si maschera per uno dei due e prende il controllo della comunicazione. In ambito web, questo termine è usato per indicare un attacco ove: le richieste di pagine a un web vengo dirottate su un web falso (via DNS), sono intercettati validi account di e-mail e poi attaccati questi ultimi (flooding).
- Hoax: in italiana bufala o burla, indica la segnalazione di falsi virus; rientra tra le tecniche di social engineering.
- Honeynet: è una rete di honeypot.
- Honeypot: sistema "trappola" su Internet per farvi accedere con opportune esche possibili attaccanti e poterli individuare.
- Hosting: servizio che "ospita" risorse logiche ICT del Cliente su hardware del fornitore del servizio.

- Housing: concessione in locazione di uno spazio fisico, normalmente in un Data Center già attrezzato, ove riporre, funzionanti, le risorse ICT di proprietà del Cliente.
- HTTPS, HyperText Transfer Protocol Secure: protocollo sicuro per le transazioni crittate tra browser e sito web, e viceversa.
- IAA, Identificazione - Autenticazione – Autorizzazione: per il controllo degli accessi ai sistemi ICT.
- IaaS, Infrastructure as a Service.
- IAM, Identity & Access Management.
- Information Leakage: diffusione-dispersione non autorizzata di informazioni.
- Intranet: rete e server operanti in http/https ed accessibili solo ad utenti interni ad una data azienda/ente.
- IoT, Internet of Things (Internet delle Cose): componenti/sistemi intelligenti ed interoperanti su Internet.
- IIoT, Industrial IoT.
- ISACA, Information Systems Audit and Control Association.
- Key Logger: sistema di tracciamento dei tasti premuti sulla tastiera per poter carpire informazioni quali codici, chiavi, password.
- Kerberos: metodo sicuro per autenticare la richiesta di un servizio, basato su crittografia simmetrica. Utilizzato da Active Directory.
- 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.
- MAC, Mandatory Access Control.
- MAC: codice indirizzo assegnato in modo univoco ad ogni scheda di rete.
- MAC flooding: tecnica di attacco ad uno switch per bloccarne il corretto funzionamento**.**
- MAC Media Access Control: sub strato del livello datalink del modello ISO/OSI.
- Malicious insider : attaccante interno all'organizzazione cui viene portato l'attacco.
- Malvertising, contrazione di "malicious advertisements": pubblicità malevola, con pagine web che nascondono un codice maligno o altre tecniche di attacco, come il dirottamento su siti web mascherati e fraudolenti.
- Malware: termine generico che indica qualsiasi tipo di programma di attacco.
- Mirroring: termine inglese per indicare la replica e la sincronizzazione di dati su due o più dischi.
- NAC, Network Access Control: termine usato con più significati, che complessivamente indica un approccio architetturale ed un insieme di soluzioni per unificare e potenziare le misure di sicurezza a livello del punto di accesso dell'utente al sistema informativo.
- NIS, Network and Information Security: normativa europea per armonizzare la sicurezza digitale dei vari paesi.
- OASIS: Consorzio di aziende ICT no profit che fornisce norme implementative per alcuni standard, tra i quali la SOA e la sua sicurezza (SALM SPML, XACML).
- OSA, Open Security Architecture.
- OT, Operational Technology.
- OTP, One Time Password: dispositivo che genera password da usarsi una sola volta per sessione/transazione.
- Outsourcer: fornitore dei servizi di terziarizzazione.
- PaaS, Platform as a Service.
- PAC, Pubblica Amministrazione Centrale

- PAL, Pubblica Amministrazione Locale
- Payload: è il “carico utile” di informazioni all’interno di un programma, di un protocollo, ecc.; tipicamente è il codice maligno da attivare sul sistema attaccato dopo esservi penetrati.
- PEC, Posta Elettronica Certificata.
- Pharming: attacco per carpire informazioni riservate di un utente basato sulla manipolazione dei server DNS o dei registri del sistema operativo del PC dell’utente.
- Phishing: attacco di social engineering per carpire informazioni riservate di un utente, basato sull’invio di un falso messaggio in posta elettronica che fa riferimento ad un ente primario, che richiede di collegarsi ad un server (trappola) per controllo ed aggiornamento dei dati.
- Ping of death: invio di pacchetti di ping di grandi dimensioni (ICMP echo request), che blocca la pila di protocolli TCP/IP: è un tipo di attacco DoS/DDoS.
- PLC, Programmable Logic Controller.
- PMI, Piccole e Medie Imprese: sotto i 250 dipendenti.
- Port scanner: programma che esplora una fascia di indirizzi IP sulla rete per verificare quali porte, a livello superiore, sono accessibili e quali vulnerabilità eventualmente presentano. È uno strumento di controllo della sicurezza, ma è anche uno strumento propedeutico ad un attacco.
- PUP, Potentially Unwanted Programs: programma che l’utente consente di installare sui suoi sistemi ma che, a sua insaputa, contengono codici maligni o modificano il livello di sicurezza del sistema. Tipici esempi: adware, dialer, sniffer, port scanner.
- QR, Quick Response: è un codice a barre bidimensionale, ossia a matrice, che è impiegato per memorizzare informazioni generalmente destinate a essere lette tramite uno smartphone.
- Race condition: indica le situazioni derivanti da condivisione di una risorsa comune, ad esempio un file o un dato, ed in cui il risultato viene a dipendere dall'ordine in cui vengono effettuate le operazioni.
- Ransomware: codice maligno che restringe e/o blocca i diritti d'accesso e tramite il quale viene chiesto un riscatto (ransom) per far funzionare correttamente il sistema.
- RBAC, Request Based Access Control.
- RBAC, Role Based Access Control.
- RFID, Radio-Frequency Identification: tecnologia per l'identificazione e/o memorizzazione automatica di informazioni inerenti oggetti, animali o persone, basata su un tag intelligente identificativo dell’entità oggetto dell’identificazione ed un dispositivo in grado di riconoscere l’entità se in sua prossimità, scambiando in radio frequenza delle informazioni.
- Ricatto: significa che l'attacco perpetrato viene poi usato per ricattare l'attaccato perché paghi per non subirne di altri, magari più perniciosi. Il malware ransomware ha come tipica motivazione il ricatto, che è un tipo della più generale frode informatica.
- Ritorsione: significa che l'attacco è stato portato come "vendetta" verso torti subiti, o come tali ritenuti: tipico il caso di un dipendente cui è stata negata una sua richiesta, o di ex dipendente licenziato. L'attaccante intende "colpire" con un attacco digitale l'Azienda/Ente che ritiene "colpevole" dei (presunti) torti subiti.
- Rogueware: falso antivirus. E' a sua volta un codice maligno che infetta il sistema.
- Rootkit: Programma software di attacco che consente di prendere il completo controllo di un sistema, alla radice come indica il termine.
- SaaS, Software as a Service.
- SALM, Security Assertion Markup Language.
- 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.
- 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.
- SGSI, Sistema Gestione Sicurezza Informatica.
- SIEM, Security Information and Event Management: sistemi e servizi per la gestione in tempo reale di informazioni ed allarmi generati dalle risorse ICT di un sistema informativo, inclusi i log.
- Sinkhole: metodo per reindirizzare specifico traffico Internet per motive di sicurezza, tipicamente per analizzarlo, per individuare attività anomale o per sventare attacchi. Può essere realizzato tramite darknet o honeynet.
- Sistema Informatico: insieme dei sistemi e dei servizi ICT, dalle reti ai server ed agli applicativi, anche terziarizzati e in cloud, organizzato in una specifica architettura e che una azienda/ente usa a supporto delle proprie attività. Il sistema informatico può includere anche i dispositivi d'utente fissi e mobili (PC, smartphone, tablet, etc.), i sistemi di automazione e controllo industriale (DCS, PLC, robot, ecc.) ed i dispositivi IoT.
- SOA, Service Oriented Architecture.
- SOC, Security Operation Centre.
- Social Engineering (ingegneria sociale): con questo termine vengono considerate tutte le modalità di carpire informazioni, quali l'user-id e la password, per accedere illegalmente ad una risorsa informatica. In generale si intende lo studio del comportamento individuale di una persona al fine di carpire informazioni.
- Sniffing-snooping: tecniche mirate a leggere il contenuto (pay load) dei pacchetti in rete, sia LAN che WAN.
- Smart city: città "intelligente" largamente dotata di infrastrutture e soluzioni ICT sia per i suoi abitanti e per interagire con loro, sia per migliorare il controllo del territorio, della sua sicurezza, dell'ambiente, della viabilità, ecc.
- Smart grid: grid è la rete elettrica di distribuzione di energia, che affiancata da una rete informatica che la gestisce diviene smart
- Smurf: tipo di attacco per la saturazione di una risorsa, avendo una banda trasmissiva limitata. Si usano tipicamente pacchetti ICMP Echo Request in broadcast, che fanno generare a loro volta ICMP Echo Replay.
- Spamming: invio di posta elettronica "indesiderata" all'utente.
- SPID, Sistema Pubblico di Identità Digitale: è attualmente usato per accedere on line ai servizi digitali delle Pubbliche Amministrazioni.
- SPML, Service Provisioning Markup Language.
- 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 ieaniane
- SYN Flooding: invio di un gran numero di pacchetti SYN a un sistema per intasarlo.
- TA, Targeted Attacks: attacchi mirati, talvolta persistenti, effettuati con più strumenti anche contemporaneamente; rientrano in questa categoria APT e Watering Hole.
- TLC, Telecomunicazioni.
- Trojan Horse (cavallo di Troia): codice maligno che realizza azioni indesiderate o non note all'utente. I virus fanno parte di questa categoria.
- TOR, The Onion Router: sistema di comunicazione anonima in Internet basato sul protocollo onion router e su tecniche di crittografia.

- Trouble ticketing: processo e sistema informatico di supporto per la gestione delle richieste e delle segnalazioni da parte degli utenti; tipicamente in uso per help-desk e contact center.
- UOSI, Unità Organizzativa Sistemi Informatici.
- URL, Uniform Resource Locator: sequenza di carattere che identifica in maniera nome univoca una risorsa ICT in rete; esempio: www.oadweb.it.
- Utente finale: utente di un sistema d'utente e/o di una o più applicazioni con i diritti di accesso relativi al suo ruolo, ma non di tipo privilegiato.
- Utente privilegiato: operatori, manutentori ed amministratori di sistema di un sistema informatico, che hanno i più elevati diritti per poter accedere e gestire le risorse ICT del sistema informatico sulle quali debbono operare. Rientrano in questa categoria anche gli sviluppatori di software. Gli attuali trend di forte terziarizzazione di queste funzioni portano a personale esterno dei fornitori dell'azienda/ente cliente tali diritti, con la necessità di maggiori controlli su di loro per assicurarsi l'adeguate livello di sicurezza digitale.
- VoIP, Voice over IP.
- VPN,Virtual Private Network: rete virtuale creata tramite Internet per realizzare una rete "privata" e sicura per i soli utenti abilitati.
- XACML, eXstensible Access Control Markup Language.
- XSS, Cross - site scripting: una vulnerabilità di un sito web che consente di inserire a livello "client" dei codici maligni via "script", ad esempio JavaScript, ed HTML per modificare le pagine web che l'utente vede.
- Watering Hole: famiglia di attacchi che rientrano nella categoria dei Targeted Attack. Il termine, traducibile in" attacco alla pozza d'acqua", fa riferimento agli agguati di animali carnivori alle prede che si dissetano in una pozza d'acqua. La metafora è usata per attacchi mirati a siti web specialistici, ad esempio di finanza, di politica, di strategie, ecc., cui una persona o un'azienda target accede periodicamente.
- Worm: un tipo di virus che non necessita di un file eseguibile per attivarsi e diffondersi, dato che modifica il sistema operativo del sistema attaccato in modo da essere eseguito automaticamente e tentare di replicarsi sfruttando per lo più Internet.
- Zero-day attack: attacchi basati su vulnerabilità a cui non è ancora stato trovato rimedio.
- Zombies, zombi: vedi bots.

Allegato C Profili Sponsor

Advansys

Advansys Spa è un system integrator che offre consulenza, sevizi ICT, e soluzione software personalizzate per far crescere le potenzialità di piccole, medie e grandi aziende. I principali fattori di competitività di Advansys sono la flessibilità, la rapidità decisionale, l'uso di nuove tecnologie ICT. Advansys ha avuto modo di sviluppare negli anni progetti importanti per i Clienti con cui ha operato. Professionalità, rispetto dei tempi, pianificazione e risultati in linea con le aspettative sono gli elementi di successo che Advansys è riuscita a introdurre in ogni occasione. La capacità di attivare team qualificati e motivati in tempi rapidi costituisce un ulteriore elemento di successo.

Le principali aree di intervento includono:

- consulenza specialistica, che include anche cyber security
- sistemi direzionali e di rendicontazione: Knowledge Management, Compliance e Regulatory Management, Gestione budget e costi di commessa, Controllo movimenti fondi e transazioni bancarie, Controllo processi d'acquisto
- servizi per l'efficienza di mercato: Facility Management, Application Maintenance, Application Testing, Help Desk, Application Management
- progetti e prodotti per l'innovazione: recentemente anche soluzioni basate su blockchain.

Advansys opera con vari Partner e su differenti piattaforme tecnologiche, tra le quali:

- Enterprise Content Management: Oracle Portal, Open CMS, Liferay, DotNetNuke, Umbraco, WorkTogether
- Document Composition & Management: Ecrion, Documentum, Arxivar, WorkTogether
- Business Process Management: Redhat Jboss, BPM/BRMS, Arxivar, WorkTogether
- Business Intelligence: Pentaho, Jasper, Elasticsearch.

Per maggiori informazioni visitate: https://www.advansys.it/

Par-Tec

A 20 anni dalla sua fondazione, **Par-Tec** è la sintesi delle competenze e delle culture del Gruppo. Considerato uno dei system integrator più attivi della scena open source italiana, realizza soluzioni innovative e personalizzate ed offre servizi professionali di alto profilo rivolti a Large Enterprise, PMI e alla PA.

Infrastruttura IT, cloud enablement, applicazioni verticali per il mercato finanziario, industria 4.0, business intelligence, compliance e formazione sono solo alcune delle aree governate dai nostri **centri di competenza** distribuiti tra **Milano** e **Roma**.

Il **Gruppo Par-Tec** è una realtà che comprende oltre 200 professionisti e include anche:

- **Swing**, specializzata nella fornitura di servizi e consulenza IT in materia di conformità alle normative di Banca d'Italia per il mercato degli intermediari finanziari.
- **Fine Tuning - Consulenza Integrata**, esperta nello sviluppo di applicazioni web-based e nell'integrazione di soluzioni di social & web intelligence e digital analytics.
- **Faberbee**, una startup focalizzata sulla ricerca & sviluppo e sull'implementazione di soluzioni basate su tecnologie Blockchain e Distributed Ledger.
- **Lightstreamer**, che sviluppa l'omonimo prodotto per il real-time data push adottato con successo da importanti realtà in tutto il mondo.

Tra le aree di specializzazione maggiormente in crescita troviamo:

IT Infrastructure & Cloud Computing. Il nostro Cloud & DevOps Competence Center guida e assiste numerose aziende private e organizzazioni pubbliche italiane nel delicato processo di adozione di metodologie, competenze e tecnologie in ambito cloud, tra cui IaaS, PaaS, cloud automation, application containerization e ingegnerizzazione di servizi SaaS.

Privacy Compliance & GDPR. La nostra offerta in ambito Sicurezza comprende l'erogazione di consulenze su aspetti normativi ed organizzativi, la formazione a distanza e in aula, l'integrazione delle tecnologie volte a limitare (o annullare) l'impatto di eventuali incidenti o data breach. Oltre ad essere certificata ISO 27001, Par-Tec può vantare la presenza di un ISO 27001 Lead Auditor, un ICT Security Trainer ed un Data Protection Officer (DPO) certificato.

Educational. Questa business line riunisce l'intera offerta costituita da soluzioni e contenuti per la formazione a distanza e in aula rivolti ad una platea eterogenea che comprende il personale amministrativo, i tecnici e il management aziendale. Il catalogo include una serie di corsi erogabili in modalità e-learning, in aula - anche presso la sede del cliente - e in modalità ibrida, caratterizzata dalla combinazione di contenuti teorici fruibili mediante piattaforma web ed esercitazioni in aula guidate da un docente qualificato. I corsi prevedono degli assessment intermedi e finali volti a verificare quanto appreso, ed il successivo rilascio degli attestati di partecipazione e superamento.

Par-Tec Control Center. Il PCC - una shared control room comprendente differenti competenze e livelli di specializzazione - è la risposta al crescente bisogno di flessibilità nelle attività di monitoraggio, gestione e troubleshooting delle piattaforme di erogazione dei servizi IT e dei processi di business. Il Cliente può scegliere quali servizi includere tra Service Desk e Problem Management o richiedere orari e livelli di servizio personalizzati.

Per maggiori informazioni visitate https://www.par-tec.it

Qintesi

Con oltre 230 dipendenti Qintesi eroga servizi di Management Consulting e di System Integration, offrendo ai Clienti soluzioni innovative.
Qintesi è Gold Partner SAP con la qualifica di “Service Partner” e “Build Partner”; ha ottenuto differenti riconoscimenti da parte di SAP fra cui sei Solution Authorization e una Build Authorization, oltre a ben dieci certificazioni SAP REX, tra cui due di Industry – Insurance ed Engineering & Construction - e, tra le prime in Italia e a livello EMEA, su SAP S4/HANA, SAP HANA e SAP Real Estate Management. Ha realizzato alcuni tra i primi progetti a livello europeo di migrazione a SAP S/4HANA su piattaforma Google Cloud Platform. Comprende inoltre la Service Line dedicata “Management & Consulting”, per offrire al mercato servizi professionali idonei a supportare le imprese nei loro percorsi di crescita.
Il Gruppo è costituito da Qintesi SpA, la capogruppo, player di riferimento nel panorama italiano dei system integrator, che supporta i Clienti nei processi di Digital Transformation attraverso l’utilizzo di sistemi ERP, Business Intelligence ed Advanced Analytics; dalla controllata Qintesi Technology & Services, che disegna e realizza avanzate infrastrutture tecnologiche, gestisce servizi di maintenance, di outsourcing amministrativo e provisioning di servizi esterni; dalla collegata BF Partners, che opera in particolare nei settori retail/GDO, affiancando a SAP applicativi per il facility management come Infocad o sistemi evoluti per la gestione commerciale e dalla 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.
Il Gruppo copre in maniera sinergica molteplici settori di mercato, grazie alle sue solide competenze in particolare in area finance & treasury, controlling, compliance & risk, sourcing & procurement, manufacturing.
Per quanto riguarda la tematica della Cyber Security, Qintesi continua ad investire nello sviluppo e nell’implementazione di soluzioni basate sulla piattaforma applicativa SAP, in particolare nelle seguenti linee di servizio:

- Data Discovery e Data lineage
- Data Segregation
- Data Security Assessment
- Data Masking & Data Scrambling
- Data Logging & Data Monitor
- Data Archiving

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.

Per maggiori informazioni visitate: https://www.qintesi.com/

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 visitate: http://www.technologyestate.eu/

Allegato D Profilo Patrocinatori

AICA

Associazione Italiana per l'Informatica e il Calcolo Automatico, è l'associazione italiana senza scopo di lucro di cultori e professionisti ICT per lo sviluppo e la diffusione delle conoscenze digitali. Tra le varie sue iniziative, ha realizzato a livello europeo l' ECDL e l'eCF (UNI EN 16234-1:2016): per quest'ultimo è accreditata come ente certificatore.
https://www.aicanet.it/

A.I.S.I.S.

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

https://www.aisis.it/

ASSI-Bologna

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

www.assi-bo.it

Assintel

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

Assolombarda

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

AUSED

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

www.aused.org

Centro Ricerche sulla Scrittura

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

www.centroricerchesullascrittura.it

Club Dirigenti di informatica Torino

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

http://www.clubdi.org/

Club Dirigenti Tecnologie dell'Informazione di Roma

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

https://cdtiroma.ning.com/

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

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

http://www.clubtier.org/

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

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

https://www.clubticentro.it/

Club per le Tecnologie dell'Informazione di Milano

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

http://www.clubtimilano.net/

Club per le Tecnologie dell'Informazione della Liguria

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

http://www.ctiliguria.it/

FIDAInform

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

http://www.fidainform.it/

FiiF

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

http://www.fiif.it

GIA

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

http://www.grafobiometristi.it/

IEEE Computer Society - Capitolo Italiano

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

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

Inforav

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

Allegato E Riferimenti e fonti

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

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

E.2 Le principali fonti sugli attacchi e sulle vulnerabilità

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

- ABILAB - Centrale d'allarme per attacchi informatici per l'ambito bancario, accessibile solo agli iscritti: www.abilab.it
- CERT-CC, Computer Emergency Response Team - Coordination Centre: fornisce uno dei più completi ed aggiornati sistemi di segnalazioni d'allarme e di rapporti sulle vulnerabilità: http://www.cert.org/certcc.html
- CERT-PA, Cert per le Pubbliche Amministrazioni italiane: https://www.cert-pa.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[30]: http://www.first.org/
- GARR-Cert fornisce i principali security alert per gli aderenti al Garr, la rete telematica tra le università italiane: www.cert.garr.it
- Internet Crime Complaint Center (IC3) è una partnership tra FBI (Federal Bureau of Investigation), il National White Collar Crime Center (NW3C) e il Bureau of Justice Assistance (BJA), e fornisce, oltre alla possibilità di denunciare negli US attacchi digitali, informazioni sugli attacchi stessi e sui trend in atto per i crimini digitali: http://www.ic3.gov/default.aspx
- NVD, National Vulnerability Database, è l'archivio statunitense di informazioni sulla vulnerabilità standardizzate e gestibili in maniera automatizzata con il protocollo SPAC: https://nvd.nist.gov/
- OECD, Organisation for Economic Co-operation and Development, produce rapporti sui rischi e gli attacchi digitali che impattano sull'economia delle nazioni in Europa: http://www.oecd.org/sti/ieconomy/security.htm
- OWASP, Open Web Application Security Project, progetto open source per la sicurezza delle applicazioni web, fornisce vari rapporti e linee guida sul tema, tra cui, periodicamente, le "top ten", le vulnerabilità ed i rischi più critici per le applicazioni web: https://www.owasp.org/
- SANS Institute fornisce sistematicamente segnalazioni su vari tipi di attacchi e di vulnerabilità, oltre all'aggiornato elenco 20 prioritari controlli di sicurezza per le norme Federali US FISMA: www.sans.org
- Sistema di informazione per la sicurezza della Repubblica Italiana, insieme di organi e autorità che hanno il compito di assicurare le attività di informazione per la sicurezza, allo scopo di salvaguardare la Repubblica da ogni pericolo e minaccia proveniente sia dall'interno sia dall'esterno del Paese, inclusa la sicurezza digitale: http://www.sicurezzanazionale.gov.it/
- WASC, Web Application Security Consortium, effettua vari progetti indipendenti sulla sicurezza digitale per le applicazioni web, e fornisce il WASC Threat Classification Online, simile a OSWAP: http://www.webappsec.org/,
- World Economic Forum, realizza un annuale rapporto sui rischi globali, che includono anche i rischi ICT e le cyberwar; http://www.weforum.org/issues/global-risks**.**

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

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

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

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

Allegato G Malabo Srl

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

Oltre alla sicurezza digitale, i tipici interventi consulenziali di Malabo includono:

- a carattere prevalentemente tecnico: la razionalizzazione del sistema informatico in essere per la riduzione dei costi ed il parallelo miglioramento dei livelli di servizio, l'automazione dei principali processi ICT (riferimenti "contestualizzati" a ITIL, COBIT, standard ISO e ad altre consolidate best practice internazionali), il piano di sviluppo del sistema informatico con la definizione e gestione dell'ICT Enterprise Architecture, eventuali terziarizzazioni ed uso di cloud, l'impostazione e la supervisione di progetti ICT, la selezione di software, l'analisi dei trend tecnologici e del mercato dell'ICT, l'analisi e la gestione dei rischi ICT, la gestione di progetti ICT (project management);
- a carattere prevalentemente organizzativo e manageriale: l'ICT governance, l'allineamento dell'ICT alle esigenze del business, la riorganizzazione dell'unità organizzativa Sistemi informativi e dei suoi processi, l'analisi del valore dell'ICT per l'azienda e per il suo business, l'analisi-assessment delle competenze ICT, la gestione della conformità a normative (es. privacy) e delle certificazioni (sia dell'intera azienda che di sue parti, oltre che del personale ICT), l'uso dell'ICT sia per la riorganizzazione di processi sia per l'innovazione dei prodotti/servizi dell'azienda/ente. Per le aziende dell'offerta ICT, in particolare di piccole e medie dimensioni, analisi ed interventi per aiutare pragmaticamente l'azienda a crescere, per incrementare immagine e guadagni, per meglio farsi conoscere e meglio posizionarsi sul mercato italiano ed internazionale.

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. Grazie al cloud e al proprio laboratorio ICT, Malabo è in grado sia di provare software per verificarne funzionalità, facilità d'uso e sicurezza, sia di fornire ai propri Clienti alcuni servizi personalizzati via Internet, che il più delle volte derivano dagli interventi consulenziali svolti. Esempi di tali servizi includono ***SLA Watch*** per il monitoraggio ed il controllo delle prestazioni delle risorse ICT da remoto, ***GOSI***, per la gestione operativa in parte automatizzata di un sistema informatico di medie dimensioni, ***ARkit*** per l'analisi e la gestione dei rischi ICT, ***ANVA***, per l'analisi del valore dell'ICT.
I principali vantaggi competitivi di Malabo, percepiti dai suoi Clienti, includono l'effettiva, consolidata esperienza e l'aggiornata competenza dei Partner, da cui deriva la semplicità, la velocità e l'economicità dell'intervento, la contestualizzazione dell'intervento sulla realtà del Cliente con la realizzazione di soluzioni su misura e di effettivo trasferimento di conoscenza, il riferimento agli standard e alle best practice internazionali, l'utilizzo di strumenti informatici di supporto, i servizi on line e la formazione.

Per maggiori informazioni: www.malaboadvisoring.it, www.oadweb.it

Allegato H Reportec

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

Per maggiori informazioni: www.reportec.it

Allegato I AIPSI, Capitolo italiano della mondiale ISSA

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

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

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

Pagina intenzionalmente vuota

OAD
Osservatorio
Attacchi Digitali
in Italia

Patrocinatori OAD 2019