OAD
Osservatorio
Attacchi Digitali
in Italia

Rapporto 2018 OAD

a cura di M. R. A. Bozzetti

SPONSOR

digiTree inthecyber intelligence & defense advisors par-tec beyond the IT domain Technology Estate

in collaborazione con Polizia Postale e delle Comunicazioni

polizia delle comunicazioni

Indagine effettuata da

aipsi ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

malabo ICT Advisory

Media Partner

Reportec

Ringraziamenti

Si ringraziano tutte le persone che hanno 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 alla dott.ssa Nunzia Ciardi, Direttore della Polizia Postale e delle Comunicazioni, e al dott. La Barbera, Direttore Polizia Postale e delle Comunicazioni Regione Lombardia.

Pubblicato a Novembre 2018 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

Sommario

1. Executive Summary

L'Osservatorio Attacchi Digitali in Italia, OAD arriva nel 2018 al decimo anno di indagini sugli attacchi digitali in Italia. Il Rapporto OAD 2018 è realizzato dall'autore Marco R. A. Bozzetti con la sua società Malabo Srl, sotto l'egida di AIPSI, Capitolo italiano di ISSA, e con la preziosa e fattiva collaborazione dell'editore Reportec Srl e della Polizia Postale e delle Telecomunicazioni, che ha fornito i dati per il capitolo 11 ed il cui Direttore Centrale, dott.ssa Nunzia Ciardi, ha scritto l'interessante prefazione.
Il Rapporto OAD 2018 analizza gli attacchi intenzionali, rilevati nel 2016 e 2017 in Italia, ai sistemi informatici di organizzazioni di ogni dimensione e settore merceologico, incluse le Pubbliche Amministrazioni centrali e locali. Esso si basa sull'elaborazione delle risposte avute da un questionario via web reso liberamente disponibile su Internet nel primo semestre del 2018. 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.
Il bacino di rispondenti emerso per l'indagine 2018 risulta costituito per la maggior parte da aziende appartenenti al settore ICT (36%), da quello dei servizi (13%) che include gli studi professionali, e da quello manifatturiero (13%), cui seguono con percentuali inferiori organizzazioni appartenenti a tutti gli altri settori merceologici (classificati secondo il codice ATECO), cui si aggiungono le Pubbliche Amministrazioni Centrali e Locali. Come dimensioni per numero di dipendenti, circa l'80% appartiene ad organizzazioni fino a 250 persone, di cui il 37,5% a strutture fino a 10 dipendenti. Il campione emerso risulta quindi abbastanza ben bilanciato tra piccole strutture e quelle medio grandi, anche in riferimento alle ultime statistiche ISTAT che per le imprese rileva il 99,91% di PMI, e tra queste il 95,22% fino a 9 dipendenti.
I compilatori del questionario 2018 sono stati 269, di cui il 20% è costituito da persone del vertice aziendale, il 19,22% dai responsabili dei sistemi informatici (CIO), il 17% da personale di terze parti cui è terziarizzata, in tutto o in parte, la gestione del sistema e della sua sicurezza, il 14% da personale appartenente all'unità organizzativa dei sistemi informatici. Solo per un 5,19% i responsabili della sicurezza informatica (CISO), con tale ruolo definito formalmente nell'organigramma.
L'indagine OAD 2018, rispetto alle edizioni precedenti, ha ridefinito la tassonomia degli attacchi digitali, distinguendo chiaramente che cosa si attacca dal come si attacca, ossia con quali tecniche.
Il questionario OAD 2018 per il 2016 ha solo chiesto che cosa è stato attaccato, mentre per il 2017 si sono approfonditi, per ogni tipo di attacco (il che cosa), le tecniche di attacco (il come), la loro frequenza, gli impatti, le motivazioni, il tempo di ripristino. Tra le tipologie di attacco l'indagine ha considerato anche i sistemi di automazione industriale, la robotica, i sistemi IoT, i sistemi basati su blockchain: le risposte raccolte sono indicatrici di come queste tecnologie si stanno estendendo in vari settori, e che siano attaccabili, come qualsiasi altro sistema ICT.

Complessivamente gli attacchi rilevati nel 2016 hanno colpito il 41,57% dei sistemi informatici dei rispondenti, e nel 2017 il 45,32%%. Tali percentuali sono in linea con quelle delle precedenti edizioni (prevalentemente attorno al 40%, pur avendo tale confronto un valore puramente indicativo e non statistico), ed evidenziano come il 2017 sia stato, con il 2008, uno degli anni con più attacchi digitali.
Le tipologie di attacco più diffuse tra i sistemi dei rispondenti sono state:

- nel 2016: gli attacchi alle reti (44,62%), seguono il furto fisico di dispositivi ICT o di loro parti (33,33%) e gli attacchi ai propri sistemi terziarizzati (21,54%);
- • nel 2017: gli attacchi al controllo degli accessi (39,39%), la saturazione delle risorse digitali (29,22%), la distruzione fisica di dispositivi ICT o di loro parti (28,57%).

La tecnica di attacco più diffusa e più usata considerando tutte le tipologie di attacco nel 2017 è quella che usa codici maligni, script e comandi diretti al sistema operativo e/o alle banche dati. Segue, ma con largo distacco, l'uso di agenti autonomi (virus). Seguono con percentuali decrescenti i Toolkit, al terzo porto come diffusione. La raccolta di informazioni, tipicamente tramite social engineering, si posiziona come diffusione al penultimo posto, segno che buona parte degli attacchi nel 2017 è avvenuta soprattutto tramite strumenti tecnici e operando da remoto.
Gli impatti a seguito degli attacchi più gravi sono analizzati per ogni tipologia di attacco, così come le possibili motivazioni degli attaccanti ed i tempi di ripristino a seguito degli attacchi più gravi. Tutti questi approfondimenti cambiano, e talvolta sono specifici per tipologia, ma in linea generale emergono i seguenti punti:

- gli impatti più diffusi includono disservizi e danni con clienti ed utenti, vandalismo, sabotaggio, ulteriore attacco basato sulle informazioni e sulle azioni del primo; la diffusione di quest'ultimo impatto, che risulta anche una delle motivazioni più diffuse, evidenzia che gli attacchi e le tecniche di attacco sono sempre più correlate tra loro;
- le motivazioni più diffuse includono ricatto/ritorsione, frode, utilizzo dell'attacco per compierne ulteriori e più gravi;
- i tempi di ripristino sono per la stragrande maggioranza entro tre giorni dall'attacco, ma 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 gli attacchi al controllo degli accessi, temuti dal 40,40% dei rispondenti, cui seguono, nella fascia del 30%, il furto di informazioni da sistemi mobili e fissi, con i furti sui mobili più temuti che sui fissi (al contrario di quanto occorso nel 2017). Il DoS/DDoS, gli attacchi alle reti e l'uso non autorizzato dei sistemi ICT sono ciascuno temuti dal 20% dei rispondenti. Altre tipologie d'attacco sono temute con percentuali inferiori e decrescenti. Le tecniche di attacco più temute nel prossimo futuro vedono al primo posto, per poco meno la metà dei rispondenti, il malware, gli script ed i command, cui segue con il 45% circa la raccolta di informazioni, tipicamente il social engineering.

L'indagine 2018, e il relativo rapporto finale, rilevano, oltre agli attacchi subiti, le misure di sicurezza che i sistemi informatici dei rispondenti hanno messo in atto, anche per meglio comprendere, almeno in linea generale, quanto le contromisure attivate, tecniche ed organizzative, sono riuscite a prevenire e contrastare gli attacchi rilevati. I sistemi informatici dei rispondenti e le misure di sicurezza che li proteggono, risultano essere, come percentuale di diffusione, nella fascia medio-alta per i sistemi ICT impiegati e per la loro sicurezza digitale, pur con qualche elemento di eccellenza e qualche altro di debolezza soprattutto nell'ottica delle percentuali del bacino di rispondenti emerso:

- il 45,59% dei rispondenti dispone di architetture ad alta affidabilità;
- quasi il 20% ha un Piano di Business Continuity (continuità operativa) ed il 33,84% un piano di Disaster Recovery, ma solo 1/3 di chi ha un piano di DR ha anche predisposto le risorse tecniche per attuarlo;
- i sistemi operativi dei server sono in buona parte aggiornati alle più recenti versioni, ed un 45,59% usa sistemi operativi "hypervisor" per la virtualizzazione dei server;
- poco meno dei ¾ dei rispondenti usano housing, hosting e cloud per una parte o per l'intero sistema informatico;
- per ¼ circa dei rispondenti la gestione del sistema informatico è automatizzata.

Le misure tecniche di base per la sicurezza digitale, da quelle fisiche a quelle per la protezione dei dati, rilevano dati in certi casi contrastanti, ma soprattutto non sono diffuse come dovrebbero su tutto il cam-

pione emerso, con alcune carenze diffuse e gravi, soprattutto per gli obblighi di conformità al regolamento GDPR. Le carenze e debolezze più gravi, come percentuale di diffusione tra i rispondenti, e che non riguardano solo le piccole e piccolissime strutture (anche se la loro prevalenza incide sulle percentuali complessive), includono:

- la mancanza della definizione di una architettura per la sicurezza digitale per i ¾ dei rispondenti;
- le limitate misure di sicurezza fisica per la protezione dei sistemi ICT in locale;
- per il controllo degli accessi, misure per lo più basate sul solo uso di identificatore d'utente e password, ma per meno della metà dei rispondenti; il 37,88% usano Active Directory o LDAP; il 13% circa usano di certificati e di PKI;
- per la sicurezza delle reti, quasi la metà dei sistemi informatici dei rispondenti usa DMZ e firewall, 40% usa VPN, 1/3 usa filtraggi per le URL e ¼ usa IPS/IDS;
- per la sicurezza logica dei singoli sistemi ICT, il 94,46% usa anti-malware ed antivirus, il 34,85% la sistematica gestione delle patch e delle versioni del software, solo il 32% circa i sistemi per l'archiviazione e la gestione dei log degli amministratori di sistema, che è obbligatoria dal 2008 per disposizione del Garante della Privacy;
- come contromisure a livello applicativo, ben il 42,42% di rispondenti dichiara l'uso di firewall applicativi (% alta, qualche rispondente forse ha confuso firewall applicativi con i più diffusi firewall di rete), solo il 16,67% effettua il controllo della sicurezza del codice per il software messo in produzione;
- per la sicurezza dei dati, l'archiviazione sicura dei back up è effettuata da 1/3 dei rispondenti, e da poco meno del 20% l'archiviazione criptata delle informazioni critiche, che dovrebbe estendersi molto per i dati personali-sensibili grazie al GDPR;
- per la gestione e il governo della sicurezza digitale, gli strumenti più diffusi sono il monitoraggio ed il controllo centralizzato delle funzionalità e delle prestazioni dei sistemi ICT con un 27,7%. Di poco superiore al 17% l'uso di strumenti per l'analisi delle vulnerabilità, e con percentuali inferiori al 5% l'utilizzo di sistemi di intelligenza artificiale per la correlazione tra eventi e l'analisi comportamentale dei sistemi ICT e/o dei loro utenti: un positivo indicatore, anche se ancora in fase embrionale, nell'adozione di moderni strumenti per individuare comportamenti anomali di persone e/ o di sistemi, e cercare così di prevenire deterioramenti funzionali, prestazionali ed attacchi.

Le misure organizzative per la sicurezza informatica risultano percentualmente meno avanzate di quelle tecniche:

- più dei ¾ dei rispondenti ha nella propria organizzazione chi espleta il ruolo di responsabile della sicurezza digitale (CISO), ma solo il 30% ha ufficializzato questo ruolo basilare per la sicurezza e la sua gestione;
- per 1/3 circa sono definite e in uso policy e procedure organizzative per la gestione della sicurezza digitale, ma meno del 10% ha definito in esse una chiara separazione dei ruoli;
- un non trascurabile 21,72% delle aziende/enti rispondenti non effettua alcun tipo di formazione e sensibilizzazione sulla sicurezza digitale;
- ancora scarso l'interesse sulle certificazioni professionali per la sicurezza digitale: il 40% circa delle aziende/enti rispondenti non è interessata e non richiede certificazioni né al proprio interno né ai fornitori ICT, ed il 14,65% non sa addirittura rispondere in merito; sono più richieste certificazioni al proprio interno che ai fornitori;
- l'analisi dei rischi è effettuata dal 45,39% dei rispondenti, una percentuale più alta rispetto a quelle rilevate nelle precedenti indagini OAD, dovuta sicuramente agli obblighi GDPR per la privacy: ma in questa ottica la percentuale è ancora assai bassa. Il 12% ha già in essere una assicurazione per i rischi ICT, ed il 10% ha a piano di sottoscriverne una;
- il 42,25% dei rispondenti già effettua auditing per il proprio sistema informatico e la sua sicurezza,

e il 9,15% lo ha a piano a breve. Interessante sottolineare che il 73% delle strutture con meno di 250 dipendenti lo effettua, e di queste circa la metà è costituita da piccolissime organizzazioni con meno di 10 dipendenti.

Molto interessanti i dati forniti dalla Polizia Postale e delle Comunicazioni per il 2016-17, ed analizzate nel capitolo 11 del rapporto, che confermano l'incremento di attacchi nel 2017:

- nell'ambito della protezione delle Infrastrutture Critiche, gli attacchi rilevati sono aumenti del 22,27%, gli allarmi del 369%, le persone denunciate del 7,34%;
- nel contrasto al "financial cybercrime", le transazioni fraudolente bloccate in € sono aumentate di quasi il 30%;
- nel contrasto al cyber terrorismo sono aumentate del 100% sia le persone denunciate che quelle arrestate.

Per concludere, i risultati della presente indagine OAD, che hanno portato alla stesura di un rapporto finale di 200 pagine A4 con circa 150 grafici, confermano sia i trend evidenziati nei precedenti rapporti OAD-OAI, sia gli ultimi rapporti internazionali sulla sicurezza digitale: il 2017 ha visto un forte incremento di attacchi sia di tipo massivo sia di tipo "targeted", sempre più sofisticati e con impatti talvolta assai gravi. 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 gli attacchi massivi costituiscono un rischio imminente e grave, come in parte è già successo con la larga diffusione di ransomware su sistemi non aggiornati e senza un aggiornato e completo back up. Come ben espresso dal Direttore della Polizia Postale e delle Comunicazioni nella sua prefazione "*tra le ragioni che favoriscono la diffusione della minaccia cyber, nei termini endemici attualmente sperimentati, figura la perdurante sottovalutazione degli aspetti legati alla sicurezza informatica, ed il conseguente mancato approntamento di meccanismi adeguati di difesa tecnologica, sia da parte dei singoli cittadini, sia a livello delle piccole o grandi realtà aziendali ed istituzionali del Paese*." Gli obblighi normativi, come ad esempio la conformità al GDPR per la privacy, aiutano a migliorare le misure di sicurezza digitale e a far crescere la consapevolezza sul problema: ma questo non basta se la sensibilizzazione e la cultura della sicurezza digitale, e quindi i relativi budget, non crescono nel Paese a tutti i livelli, in particolare a quelli di vertice dei decisori di aziende/enti e dei politici che legiferano sulla sicurezza digitale.

2. Executive Summary (english)

The Observatory on Digital Attacks in Italy (OAD) arrives in 2018 at the tenth year of surveys on digital attacks in Italy. OAD 2018 has been realized by Marco R.A. Bozzetti with his company Malabo Srl, under the aegis of AIPSI, Italian Chapter of ISSA, and with the precious and effective collaboration of the publisher Reportec Srl and of the Italian Postal Police, who provided data for the report's last chapter and whose Central Director, Nunzia Ciardi, wrote the report's preface.
The 2018 OAD Report analyzes the intentional attacks, detected from 2016 to 2017 in Italy, to the IT systems of organizations of all sizes and sectors, including central and local public administrations. It is based on the elaboration of the answers received from a web questionnaire available online in the first half of 2018. Being free access to the questionnaire on the Internet, the sample emerged does not have strict statistical value, but, given the number of answers and the good distribution by size and by sector of the of respondents, it provides precise and contextual indications on the phenomenon of digital attacks in Italy.
The survey also identifies the prevention, protection and recovery tools used by respondents' IT systems to counteract and limit such attacks.
The respondents are mostly made up of companies belonging to the ICT sector (36%), to the services' sector (13%) and to manufacturing industry (13%), followed by lower percentages of organizations belonging to all the other sectors (classified according to ATECO), to which are added the Central and Local Public Administrations. In terms of number of employees, around 80% belong to organizations of up to 250 people, of whom 37.5% belong to those with up to 10 employees. The sample emerged is therefore well balanced between small and medium-large structures, with reference to the latest ISTAT statistic, for which 99.91% are SMEs, and among these 95.22% up to 9 employees.

The respondents of the 2018 questionnaire are 269, of which 20% consists of top managers, 19.22% CIO, 17% of third-party staff, 14% by personnel belonging to the organizational unit of information systems: only 5.19% of CISO, with this role formally defined in the organization chart. in Italy, this role is mainly performed in part-time among different other roles.
The OAD 2018 survey has redefined the taxonomy of digital attacks, clearly distinguishing the type of the attack (the what), referred to the attack's target, by the techniques for conducting the attack itself (the how).
The 2018 OAD questionnaire, for each type of attack (the what), put questions on the techniques of attack (the how), their frequency, impacts, motivations, recovery time. Among the types of attack the survey also considered industrial automation systems, robotics, IoT systems, blockchain-based systems.
The digital attacks detected in 2016 hit 41.57% of the respondents' IT systems, and in 2017 45.32 %. These percentages are in line with those of the OAD' previous editions (mainly around 40%, although this comparison is purely indicative and non-statistical), and they confirm that 2017 was one of the years with more digital attacks.
The most common types of attacks among the respondents' ICT systems were:

- in 2016: network attacks (44.62%), followed by the physical theft of ICT devices or of their parts (33.33%) and attacks on the outsourced ICT systems (21.54%);
- in 2017: attacks on access control (39.39%), DoS/DDoS (29.22%), physical destruction of ICT devices or of their parts (28.57%).

Considering all the types of attack in 2017, the most used attack technique is the one that uses malware, scripts and OS commands. The use of autonomous agents (viruses) follows, but with a large gap, and with a decreasing percentage the use of toolkits. The collection of information, typically through social engi-

neering, is positioned to the penultimate place, an indicator that most of the attacks in 2017 took place mainly through technical tools and operating remotely.

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 required by the most serious attacks. All these insights change, and sometimes they are specific by type, but in general the following points emerge:

- the most widespread impacts include: a decrease of the level of the service provided to the customers and users, vandalism, sabotage, further attacks based on the information and the actions performed with the previous one; the spread of this last impact, which is also one of the most widespread motivations, shows that attacks are increasingly correlated with each other;
- the most widespread motivations include: blackmail / retaliation, fraud, use of the attack to make further attacks more and more serious;
- recovery times are for the vast majority within three days after the attack, even if in many cases the recovery requires only one day. In the most serious and complex cases, a full recovery can take even longer than a month.

The most feared attacks in the future are related, at least in part, to the most serious attacks suffered in 2017. The first ones are the attacks on access control, feared by 40% of respondents, followed by the theft of information from mobile devices and desktops, feared by 30%. DoS / DDoS, attacks on networks and unauthorized use of ICT systems are each feared by 20% of the respondents. Other types of attack are feared with lower and decreasing percentages. Referring to the attack techniques, the most feared one is malware-scripts-commands for about 50% of the respondents, followed by information gathering, typically through social engineering, for about 45%.

The 2018 survey detects also the security measures that the ICT systems of the respondents have implemented: these can be considered at a medium-high level concerning the ICT technologies, and at a medium-low level concerning the digital security, despite some element of excellence for both these topics:

- 45.59% of respondents utilizes highly reliable architectures;
- almost 20% have a Business Continuity Plan and 33.84% a Disaster Recovery Plan, but only 1/3 of those last have also the availability of the necessary technical infrastructures to deploy the DR when a disaster may occur on the informatic system;
- the operating systems of the servers and of the end user devices are mostly updated to the latest versions, and 45.59% use "hypervisor" operating systems for server virtualization;
- a little less than ¾ of respondents use housing, hosting and cloud for part or for the entire their informatic system;
- for ¼ of respondents the operational management of the IT system is automated.

The basic technical measures for digital security are not as widespread as they should on the whole sample, but they have some widespread and serious shortcomings, above all in the presence of the GDPR regulation. Some weaknesses include:

- for 37% of the respondents, the lack of a digital security architecture;
- the limited physical security measures for the protection of local ICT systems;
- for about 50% of the respondents, the access control systems are mostly based only on user ID-password; 37.88% use Active Directory or LDAP and about 13% use certificates and PKI;
- concerning the network security, almost half of respondent's IT systems use DMZ and firewall, 40% use VPN, 1/3 use URL filtering and ¼ use IPS / IDS;
- concerning the logical security of individual ICT systems, even if 94.46% use anti-malware and antivirus, only 34.85% provides systematic management of patches and software versions, and

only 32% mange the system administrators' logs; this last activity is mandatory since 2008 for a directive of the Italian Privacy Authority;

- concerning security at the application level, even if 42.42% of respondents declare to use application firewalls (very high percentage, some responders may have confused them with the most widespread network firewalls), only 16.67% carry out the security check for the software code;
- concerning data security, safe back-ups are performed by 1/3 of the respondents, and just under 20% perform encryption to store critical information; encryption should extend a lot for protecting personal-sensitive data thanks to GDPR;
- concerning the digital security management and governance, the most common tools used by 27.7% of the respondents are the centralized monitoring and control systems; about 17% of the respondents use tools for the analysis of vulnerabilities; few advanced respondents, lower than 5%, use artificial intelligence systems for the events correlation and for the behavioral analysis of ICT systems and / or of their users.

The organizational measures for computer security in the companies of the respondents are less widespread (as percentages) and mostly less advanced and implemented than the technical ones:

- more than ¾ of respondents have in their organization who performs the basic activity of a CISO, but only 30% have formalized this role, that is essential for security and its management;
- approximately 1/3 have defined and are using organizational policies and procedures for the management of digital security, but less than 10% have defined a clear separation of duties for all the actors of the ICT department;
- 21.72% of responding companies do not carry out any type of training and awareness on digital security;
- there is still little interest in professional certifications on digital security: about 40% of responding companies are not interested and do not require certification either for internal professionals and/or ICT department or for ICT suppliers, and 14.65% of the respondents is not able to answer; for the companies interested, certifications are required more for internal professionals;
- the risk analysis is carried out by 45.39% of the respondents, a higher percentage than those found in previous OAD investigations, certainly due to the GDPR obligations for privacy: but in this context the percentage is still too low. 12% already have insurance coverage for ICT risks, and 10% have plans to subscribe one;
- 42.25% of respondents already perform auditing for their IT system and its security, and 9.15% have a plan for auditing in the next future. It is interesting to underline that auditing is performed by 73% of the structures with less than 250 employees, and of these about half are the very small ones with less than 10 employees.

The Italian Postal Police, which is in Italy the main responsible for the fight against cybercrime, has provided many interesting data on its activities, done both in 2017 and in 2016. These data are analyzed in the last chapter of the report (§11), and they show that:

- for the Critical Infrastructures, the attacks detected increased by 22.27%, the alarms by 369%, the reported persons by 7.34%;
- in contrast to the financial cybercrime, the blocked fraudulent transactions increased (in €) by almost 30%;
- in contrast to cyber terrorism, the reported people and those arrested increased both by 100%.

To conclude, the results of the present OAD survey confirm both the trends highlighted in previous OAD-OAI reports, and the latest international reports on digital security: 2017 saw a sharp increase in both massive and "targeted" attacks, increasingly sophisticated and sometimes with very serious impacts. The

Italian reality, made up of a very large number of SME, does not make our country one of the most attractive for digital criminals; but massive attacks may be an imminent and serious risk, as has already happened with the large spread of ransomware on systems not updated and without a complete back up. As expressed by the Director of the Postal and Communications Police in her preface "*Among the reasons that favor the spread of the cyber threat, in the endemic terms currently tested, figure the ongoing underestimation of aspects related to information security, and the consequent failure to set up an adequate technological defense*." Regulatory obligations, such as compliance with the GDPR for privacy, help to improve digital security measures: but this is not enough, if the awareness and culture of digital security do not grow in the country at all levels, mainly at the level of the top managers and of the politicians who legislate on cybersecurity.

3. Prefazione del Direttore Polizia Postale, dott.ssa Nunzia Ciardi

Lo scenario globale degli attacchi informatici ha ormai da tempo superato i livelli di guardia, favorito, tra l'altro, dalla diffusone capillare di software e strumenti, dal sempre più agevole utilizzo, appositamente studiati per la violazione di reti e sistemi, cui si unisce un deciso aumento nel ricorso a prestazioni criminali (il c.d. *crime as a service*), reperibili su larga scala all'interno dei canali di vendita clandestini, esistenti sul dark web.
Si assiste, soprattutto negli ultimi anni, ad un aumento esponenziale delle violazioni di spazi e sistemi informatici, indotti da motivazioni ancora in larghissima parte riconducibili al cybercrime (in considerazione della elevata mole di profitti illeciti conseguibili con i reati informatici), sebbene degni di assoluto rilievo - specie dal punto di vista qualitativo – siano oggi gli attacchi informatici ispirati da motivazioni di guerra cibernetica (*cyber warfare*) a matrice statuale, nonché gli attacchi mossi da ragioni di attivismo ideologico (*cyber hacktivism*) o peggio, ispirati da matrici fondamentaliste e da scopi terroristici (*cyber terrorism*).

Sovente, tra le ragioni che favoriscono la diffusione della minaccia cyber, nei termini endemici attualmente sperimentati, figura la perdurante sottovalutazione degli aspetti legati alla sicurezza informatica, ed il conseguente mancato approntamento di meccanismi adeguati di difesa tecnologica, sia da parte dei singoli cittadini, sia a livello delle piccole o grandi realtà aziendali ed istituzionali del Paese.
Occorre allora che tutti gli attori, ed in particolare le organizzazioni complesse e le realtà aziendali più strutturate, mantengano un approccio consapevole al problema della sicurezza informatica, dedicando ad essa risorse ed energie che appaiono oggi come un necessario investimento, anziché un inerte costo.
Le Istituzioni, per parte loro, sono chiamate a ripensare i paradigmi di approccio alla prevenzione e repressione della criminalità informatica, indirizzando la propria azione verso la ricerca di modelli sempre più fattivi ed efficaci di partenariato pubblico-privato, capaci di stimolare la cultura del "fare rete" con i soggetti destinatari dell'azione pubblica e con le migliori risorse della ricerca scientifica.
La Polizia Postale e delle Comunicazioni ha da tempo sposato tale prospettiva, declinando in vario modo l'idea del *networking* con i partner istituzionali, in ogni suo settore d'intervento.
Nei settori della protezione delle infrastrutture critiche informatizzate e del contrasto al crimine informatico/finanziario, ad esempio, la Specialità procede secondo un modello convenzionale, che ha permesso l'istituzione di un rapporto diretto e quotidiano tra gli esperti di polizia ed i gestori tecnici dei sistemi IT nevralgici per il Paese (dal sistema delle pubbliche amministrazioni nazionali, ai servizi di approvvigionamento idrico ed energetico, ai trasporti, le telecomunicazioni, la sanità ed sistema finanziario).
Il fronte della collaborazione internazionale vede la Polizia Postale impegnata nello scambio quotidiano con le Unità *cyber* delle principali forze di polizia estere, oltreché nel rapporto con i più importanti provider di servizi e contenuti a livello mondiale.
Lo scopo è quello di alimentare, nel tempo, la cultura di una sicurezza diffusa e condivisa, che possa agire quale virtuoso moltiplicatore delle capacità di risposta, riuscendo ad opporre adeguata resistenza ad una minaccia sempre più multiforme, pervasiva, tentacolare.

Dott.ssa Nunzia Ciardi
Direttore Servizio Polizia Postale e delle Comunicazioni

4. Introduzione al Rapporto OAD 2018

OAD, Osservatorio Attacchi Digitali in Italia, è l'evoluzione del precedente OAI, Osservatorio Attacchi Informatici in Italia[1], e 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 2018 fa riferimento agli attacchi digitali intenzionali rilevati nel corso del 2016 e 2017, e si congiunge logicamente al Rapporto 2016, che considerava gli attacchi del 2015, ed a quelli precedenti del 2015 (2014), 2013, 2012, 2011 e del 2009-10, che nel loro insieme coprono un decennio di indagini sugli attacchi, dal 2007 al 2017.
Vengono considerati due anni dato che l'indagine OAD 2017 era solo focalizzata verticalmente sugli attacchi agli applicativi, e non ha considerato le altre tipologie di attacco per poter fornire una analisi generale come quelle effettuate belle precedenti edizioni.
L'indagine 2018 ed il presente rapporto ritornano ad un'indagine generale per coprire tutte le tipologie di attacco intenzionali a livello di aziende/enti, ma con una diversa e più rigorosa tassonomia degli attacchi, dettagliata nell'Allegato A.1.
In occasione del decennale è stato inoltre realizzato un sito web dedicato unicamente all'iniziativa OAD, www.oadweb.it, che costituisce un completo archivio non solo dei vari rapporti annuali pubblicati, ma anche di tutti gli eventi e delle pubblicazioni, dirette ed indirette, effettuate in merito ai risultati delle indagini OAD e OAI negli anni. In questo sito sono gratuitamente scaricabili tutti i precedenti rapporti OAI ed OAD, e la documentazione prodotta e/o raccolta di articoli e presentazioni in merito.
Il Rapporto OAD 2018 è realizzato dall'autore Marco R. A. Bozzetti con la sua società Malabo Srl, sotto l'egida di AIPSI, Capitolo italiano di ISSA, e con la preziosa e fattiva collaborazione dell'editore Reportec Srl e della Polizia Postale e delle Telecomunicazioni, che ha fornito i dati per il capitolo 11 ed il cui Direttore, dott.ssa Nunzia Ciardi, ha scritto l'interessante prefazione.
Per coprire almeno una parte dei costi, OAD 2018 è stata sponsorizzata dalle aziende dell'offerta ICT DigiTree[2], IntheCyber, Par-Sec, Technology Estate, le cui schede di presentazione, con l'approfondimento delle loro attività nel campo della sicurezza informatica, sono in ordine alfabetico nell'Allegato C.
Come per le edizioni precedenti OAD 2018 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 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.

1 - Il cambio del nome è stato voluto per esplicitare fin dal nome che l'indagine riguarda gli attacchi digitali sia dell'informatica che delle telecomunicazioni e del networking

2 - CT, Information and Communication Technology

Il Rapporto OAD 2018 si basa sull'elaborazione e l'analisi delle risposte avute dal questionario via web reso liberamente disponibile su Internet nel primo semestre del 2018. 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 269 risposte al questionario OAD 2018, costituito da 117 domande con risposte predefinite tra le quali scegliere, è stato prodotto il presente rapporto finale, costituito da 150 pagine A4 e da circa 141figure 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 E un glossario degli acronimi e dei termini tecnici specialistici usati.

4.1 - 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 di AIPSI un Osservatorio Nazionale annuale, le cui caratteristiche metodologiche sono riportate nell'Allegato A, riprendendo l'esperienza passata avuta con OCI,

Osservatorio Criminalità Informatica, di FTI-Sicurforum[3]. L'approccio è simile: l'indagine è svolta in collaborazione con gli esperti degli Sponsor e dei vari enti patrocinatori, la raccolta dei dati avviene elaborando le risposte via web dei vari rispondenti, il rapporto annuale è elaborato in maniera omogenea.

4.2 - Le vulnerabilità ICT causa prima di ogni tipo di attacco digitale intenzionale

Il Global Risk Report[4] del World Economic Forum, pubblicato a gennaio 2018, pone i rischi ICT al terzo posto dei rischi "globali", dopo i disastri naturali e gli eventi climatici estremi. I rischi ICT, nell'ambito dei rischi globali di questo rapporto, sono considerati come conseguenze negative, intenzionali o non intenzionali, dei progressi tecnologici in genere, non solo digitali, che causano o possono causare danni umani, ambientali ed economici.

Rischio, vulnerabilità, attacco, minaccia sono termini di uso comune e diffuso nel trattare la sicurezza digitale, ma non hanno definizioni univoche, nemmeno a livello di standard e best practice, e sono soventi usati in maniera impropria. Per questo motivo si è voluto chiarirli concettualmente, almeno per come sono usati nel presente rapporto: la loro semantica è chiarita nelle definizioni della tabella in fig. 4.2-1.

Termine	Definizione/spiegazione
Minaccia	una possibile fonte di danni
Rischio	possibilità che una minaccia si verifichi
Attacco	effettivo manifestarsi di un rischio
Vulnerabilità	debolezza di una risorsa (ICT) o di un gruppo di risorse (ICT) che possono essere sfruttate da una o più minacce (da ISO 27005)
Misura di contrasto e controllo	misura tecnica ed organizzativa capaci di eliminare o limitare il rischio di una minaccia

Fig. 4.2-1

Tutte le minacce ICT, intenzionali o non, si basano su vulnerabilità che possono essere categorizzate in:

- **Vulnerabilità tecniche** dell'hardware, delle reti e del software in suo, oltre che delle architetture ICT e delle configurazioni dei singoli sistemi ICT;
- **Vulnerabilità delle persone** che includono:
  - Social Engineering e phishing

3 - Per i Rapporti OCI del 1997, 2000 e 2004, pubblicati da Franco Angeli, si veda **http://www.forumti.it/**

4 - **https://www.weforum.org/reports/the-global-risks-report-2018**

    - Utilizzo improprio e/o a rischio dei **social network**, anche a livello aziendale;
- **Vulnerabilità organizzative**, che includono:
    - Mancanza o non utilizzo procedure organizzative
    - Insufficiente o non utilizzo degli standard e delle best practices
    - Mancanza di formazione e sensibilizzazione
    - Mancanza di controlli e monitoraggi sistematici
    - Analisi dei rischi mancante o difettosa
    - Non efficace controllo dei fornitori
    - Limitata o mancante separazione dei ruoli (SoD, Separation of Duties).

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. L'Allegato E.2 fornisce un elenco, non esaustivo, delle principali fonti internazionali con aggiornati elenchi delle vulnerabilità tecniche ICT.

5. Il nuovo approccio per OAD 2018 e la nuova logica per la tassonomia degli attacchi digitali

L'indagine OAD è indirizzata a rilevare le azioni deliberate e intenzionali rivolte contro i sistemi informatici, e non i rischi cui essi sono sottoposti per il loro cattivo funzionamento, per un maldestro uso da parte degli utenti e degli operatori, o per fenomeni accidentali esterni.
Come specificato nel Questionario, per l'indagine OAD sono considerati solo gli attacchi che sono stati effettivamente rilevati, e non è necessario che abbiano creato danni ed impatti negativi all'organizzazione e ai suoi processi.
L'attacco contro un sistema informatico è tale quando si intende violato, con una attività non autorizzata, almeno uno dei requisiti della sicurezza ICT, definita come la "protezione dei requisiti di integrità, disponibilità e confidenzialità" delle informazioni trattate, ossia acquisite, comunicate, archiviate e processate.
Nello specifico:

- integrità è la proprietà dell'informazione di non essere alterabile;
- disponibilità è la proprietà dell'informazione di essere accessibile e utilizzabile quando richiesto dai processi e dagli utenti autorizzati;
- confidenzialità è la proprietà dell'informazione di essere nota solo a chi ne ha il diritto.
- Per le informazioni e i sistemi connessi in rete le esigenze di sicurezza includono anche:
- autenticità, ossia la certezza da parte del destinatario dell'identità del mittente;
- non ripudio, ossia il fatto che il mittente o il destinatario di un messaggio non ne possono negare l'invio o la ricezione.

In OAD 2018, a partire dal questionario, l'impostazione e la logica della classificazione degli attacchi distingue in modo più rigoroso e più chiaro (rispetto ai questionari delle precedenti edizioni, oltre che ai vari rapporti internazionali) il che cosa viene attaccato dal come, ossia con quale tecniche, viene portato l'attacco.
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: un tipico esempio sono gli attacchi fisici ai dispositivi ICT.
Tale nuovo approccio è descritto nell'Allegato A, e per la spiegazione dei termini usati si rimanda al glossario in Allegato B.
La matrice in fig. 5-1 che mappa il che cosa si attacca con il come si attacca, schematizza chiaramente il nuovo approccio seguito per l'indagine 2018 OAD.
Le famiglie di attacchi (che cosa si attacca), indicate nel presente rapporto come tipologie di attacchi, sono rappresentate nella matrice dalle righe, ed includono:

- Distruzione fisica di dispositivi ICT o di loro parti
- Furto fisico di dispositivi ICT o di loro parti
- Furto informazioni da sistemi fissi (PC, server, storage system, …)
- Furto informazioni da sistemi mobili (palmari, smartphone, tablet, ecc.)
- Attacchi all'identificazione, autenticazione e controllo accessi degli utenti e degli operatori
- Attacchi alle reti locali e geografiche, fisse e wireless, e ai DNS
- Uso non autorizzato risorse ICT (dal PC ai server-storage e ai servizi in cloud)
- Modifiche non autorizzate ai programmi applicativi e di sistema, alle configurazioni, ecc.

- Modifiche non autorizzate alle informazioni trattate dai sistemi ICT
- Saturazione risorse digitali (DoS, DDoS)
- Attacchi ai propri sistemi in cloud o in housing/hosting da Fornitori
- Attacchi a dispositivi IoT (Internet of Things) in uso
- Attacchi ai propri sistemi di automazione industriale (DCS, PLC, etc. e/o di robotica
- Attacchi a sistemi e/o servizi usati e basati su blockchain.

Le famiglie di tecniche di attacco (come si attacca) sono le colonne della matrice ed includono:

- Attacco fisico: per distruggere dispositivi ICT, ad esempio come atto vandalico o di terrorismo, include anche il furto di dispositivi ICT o di loro parti (ad esempio l'hard disk)
- Raccolta informazioni: con le quali si possono compiere attacchi, quali ad esempio tecniche di social engineering, phishing, pharming, hoax, scannerizzazioni e ricerche in Internet, ecc.
- Script e programmi maligni quali ransomware, spyware, adware, ecc.
- 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, ecc.)
- Strumenti distribuiti controllati centralmente (da un Command Control) quali botnet
- Utilizzo di due o più delle precedenti tecniche (APT, Advanced Persistent Threat).

In questa edizione sono esaminati gli attacchi alle parti di sistemi informatici terziarizzati in cloud/housing/hosting, vista anche la forte crescita dell'outsourcing, ai sistemi IoT, ai sistemi di automazione industriale e di robotica, che seppure in maniera meno dettagliata erano stati considerati anche nelle precedenti edizioni. Novità assoluta gli attacchi ai sistemi basati su tecniche di blockchain, che iniziano ad essere usati anche in Italia per specifiche funzionalità in alcuni settori.

Nel Capitolo 6 seguente, ogni tipologia di attacco viene esaminata sulla base delle risposte ricevute da chi ha rilevato la specifica tipologia d'attacco, e che riguardano:

- il numero di attacchi di quel tipo nel 2017, se sopra o sotto la soglia di 10 attacchi rilevati nell'anno;
- 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 2017.

6. Gli attacchi digitali rilevati (che cosa viene attaccato)

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

La fig. 6-2 evidenzia se si sono rilevati più o meno di 10 attacchi per anno per azienda/ente, così da indicare della loro numerosità per singola azienda/ente. 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. Dalla figura è interessare evidenziare come nel 2017 sia aumentata la frequenza di attacchi sopra i 10 per singola azienda/ente, e sia diminuita quella sotto tale soglia.

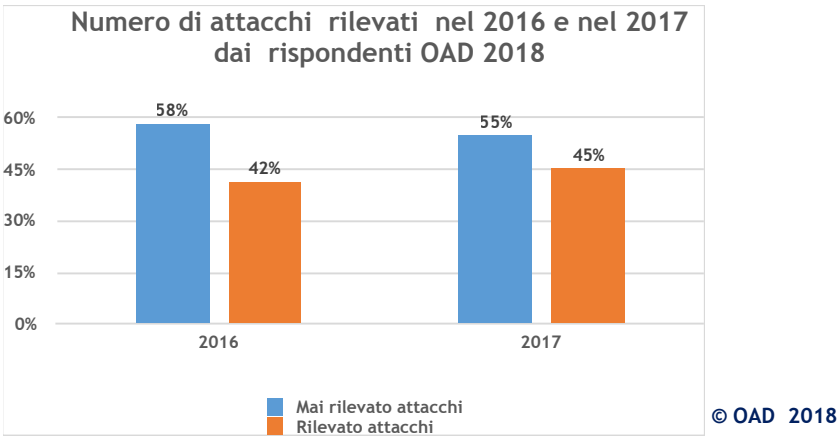

Fig. 6-1

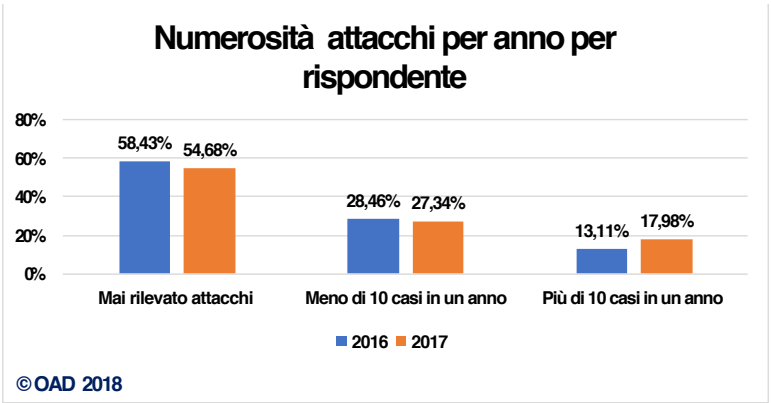

Fig. 6-2

La fig. 6-3 confronta il numero di attacchi rilevati nei diversi Rapporti OAI dal 2007 al 2017. Tale confronto non ha valenza statistica ed è da considerare come trend puramente indicativo, dato che i campioni dei rispondenti nei diversi anni sono diversi come mix e come numero. Nell'arco temporale considerato il 2008 rappresenta l'"annus horribilis" per la quantità di attacchi occorsi, seguito dal 2017.

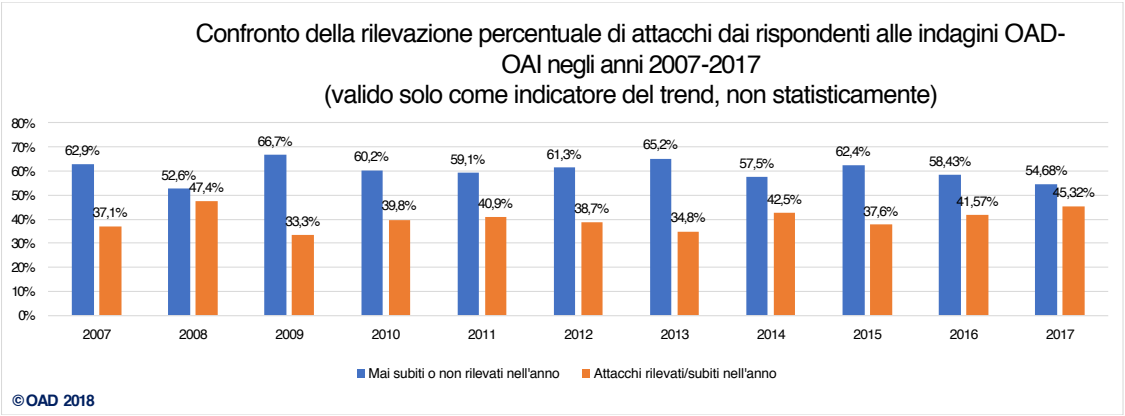

Fig. 6-3

Come anche indicato da numerosi altri rapporti internazionali, a livello mondiale il 2017 ha avuto un incremento del numero di attacchi rispetto agli anni precedenti, oltre che, in molti casi, ad una maggior gravità complessiva degli impatti. La fig. 6-3 mostra un'onda altalenante negli anni della percentuale di attacchi rilevati: cresce poi scende poi risale e così via. Tale onda 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.
Solo come trend indicativo, la figura evidenzia poi che negli ultimi tre anni, dal 2015 in avanti, il numero di aziende/enti che hanno rilevato attacchi è percentualmente sempre cresciuto. Un chiaro indicatore della efficacia e della conseguente criticità degli attacchi portati, e delle misure di sicurezza di contrasto che non si sono rilevate adeguate ed efficaci.
La percentuale 40% per gli attacchi rilevati in Italia nei dici anni di indagini OAD-OAI, pur con campioni diversi di rispondenti, si conferma una media stabile negli anni per il fenomeno attacchi 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 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. Essi non costituisco quindi 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; valgone 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.

Come mostrato nella fig. 6-4, la più recente indagine ISTAT del 2018 evidenza che le microimprese (con meno di dieci addetti) in Italia sono circa 4,2 milioni e rappresentano, il 95% del totale delle unità produttive: impiegano circa 7,8 milioni di addetti, che rappresenta il 47% contro il 29% nella media europea. La stessa figura evidenzia la quota particolarmente modesta di imprese oltre 250 addetti; lo 0,1% delle imprese e il 19% degli addetti. Tale frammentazione comporta una dimensione media di 3,9 addetti per impresa a fronte di una media europea di 6,8 addetti. Il 63,3% delle microimprese è inoltre costituito da imprese individuali, una quota pari a oltre il doppio di quella media europea.

Fig. 6-4 (Fonte ISTAT)

È 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 motivi ideologici o terroristici (per l'analisi delle possibili motivazioni si rimanda ai successivi paragrafi sulle singole tipologie di attacco, da §6.1 a §6.14).

Una sintesi della distribuzione percentuale degli attacchi subiti nel 2017 per dimensione e per fatturato delle aziende/enti dei rispondenti[5] è riportata nella fig. 6-5. Essa mostra come le organizzazioni più attaccate nel 2017 siano, percentualmente, quelle più piccole, sia con pochi attacchi nell'anno sia con attacchi più frequenti, maggiori di 10 attacchi all'anno.

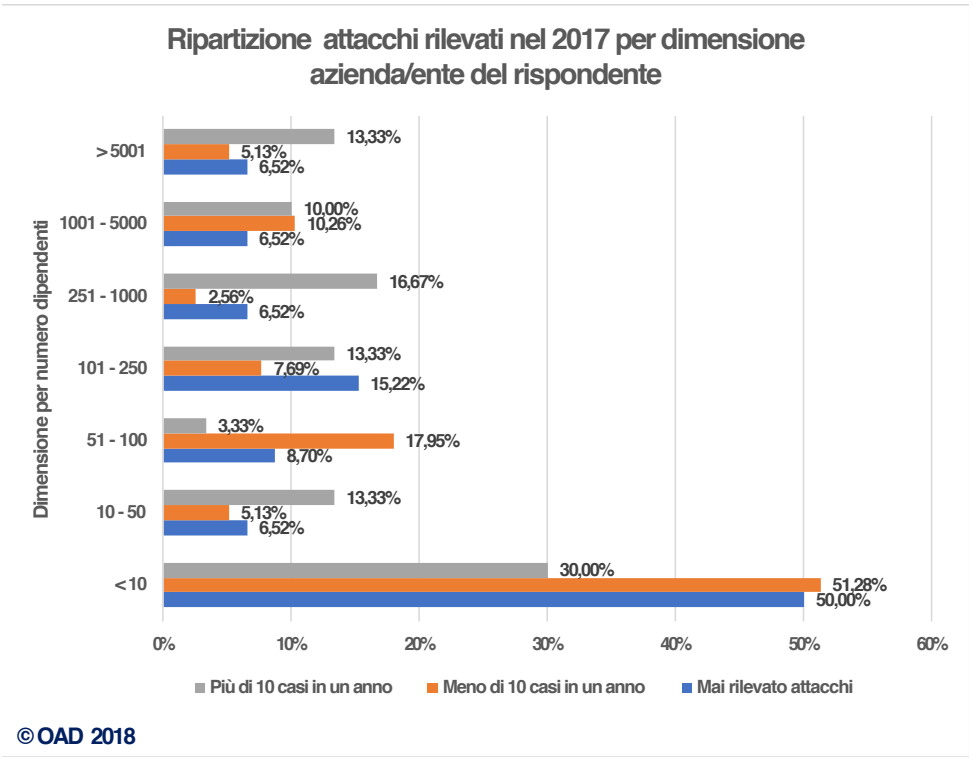

Fig. 6-5

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

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.

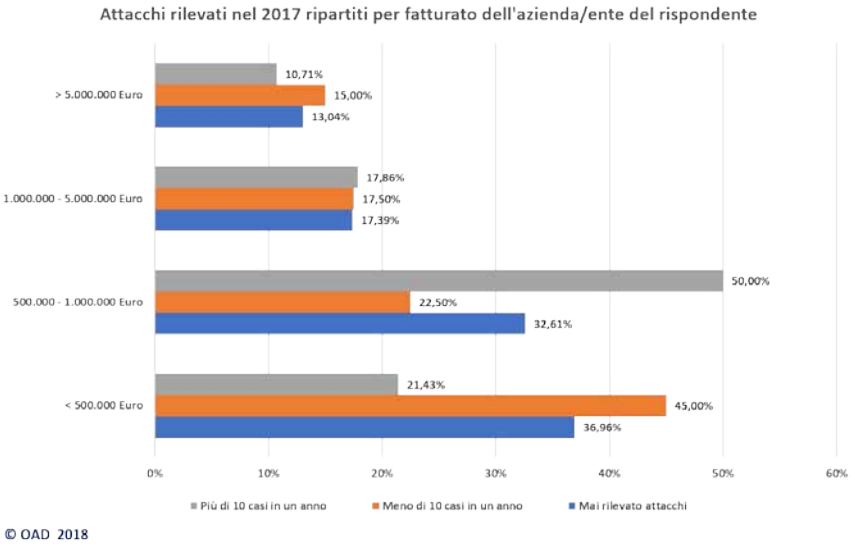

Fig.6-6

Facendo riferimento alle tipologie di attacco, ossia al "che cosa" viene attaccato (si veda Allegato A), tipologie analizzate una per una nei paragrafi seguenti, la fig. 6-7 mostra la diffusione in percentuale degli attacchi rilevati nel 2016 e nel 2017 dal campione dei rispondenti:

- nel 2017: al primo post gli attacchi al controllo degli accessi (39,39%), al secondo posto la saturazione delle risorse digitali (29,22%), al terzo la distruzione fisica di dispositivi ICT o di loro parti (28,57%);
- nel 2016: al primo posto gli attacchi alle reti (44,62%), seguono il furto fisico di dispositivi ICT o di loro parti (33,33%) e gli attacchi ai propri sistemi terziarizzati (21,54%).

Le tipologie di attacchi più diffuse, almeno tra i rispondenti a OAD 2018, nel 2016 e nel 2017 sono allineate con quelle rilevate a livello mondiale e riportate nei principali rapporti internazionali, valori delle percentuali a parte.
Il confronto dei dati tra il 2016 ed il 2017, basati sulle risposte dello stesso bacino di rispondenti, è statisticamente valido e sono da evidenziare le principali variazioni in positivo e negativo tra i due anni:

- maggiori incrementi tra 2016 e 2017: gli attacchi al controllo degli accessi, con un + 32,73%, seguiti dal furto informazioni da sistemi fissi, + 21,08%, e dalla saturazione delle risorse con un +19,99%;
- maggiori decrementi: al primo posto, con un -17,40%, gli attacchi alle reti, cui segue con un -8,88% l'attacco ai propri sistemi terziarizzati e con un -8,04% il furto fisico di dispositivi ICT o di loro parti.

E' interessante osservare come tutti i decrementi maggiori fanno riferimento agli attacchi più diffusi nel 2016: le aziende/enti che hanno subiti tali attacchi hanno subito implementato opportune misure di

sicurezza che sono risultate efficaci già l'anno seguente.
Gli incrementi maggiori di attacchi sono occorsi per tipologie di attacco che hanno avuto forti incrementi anche a livello mondiale, a partire dagli attacchi ai controlli degli accessi.

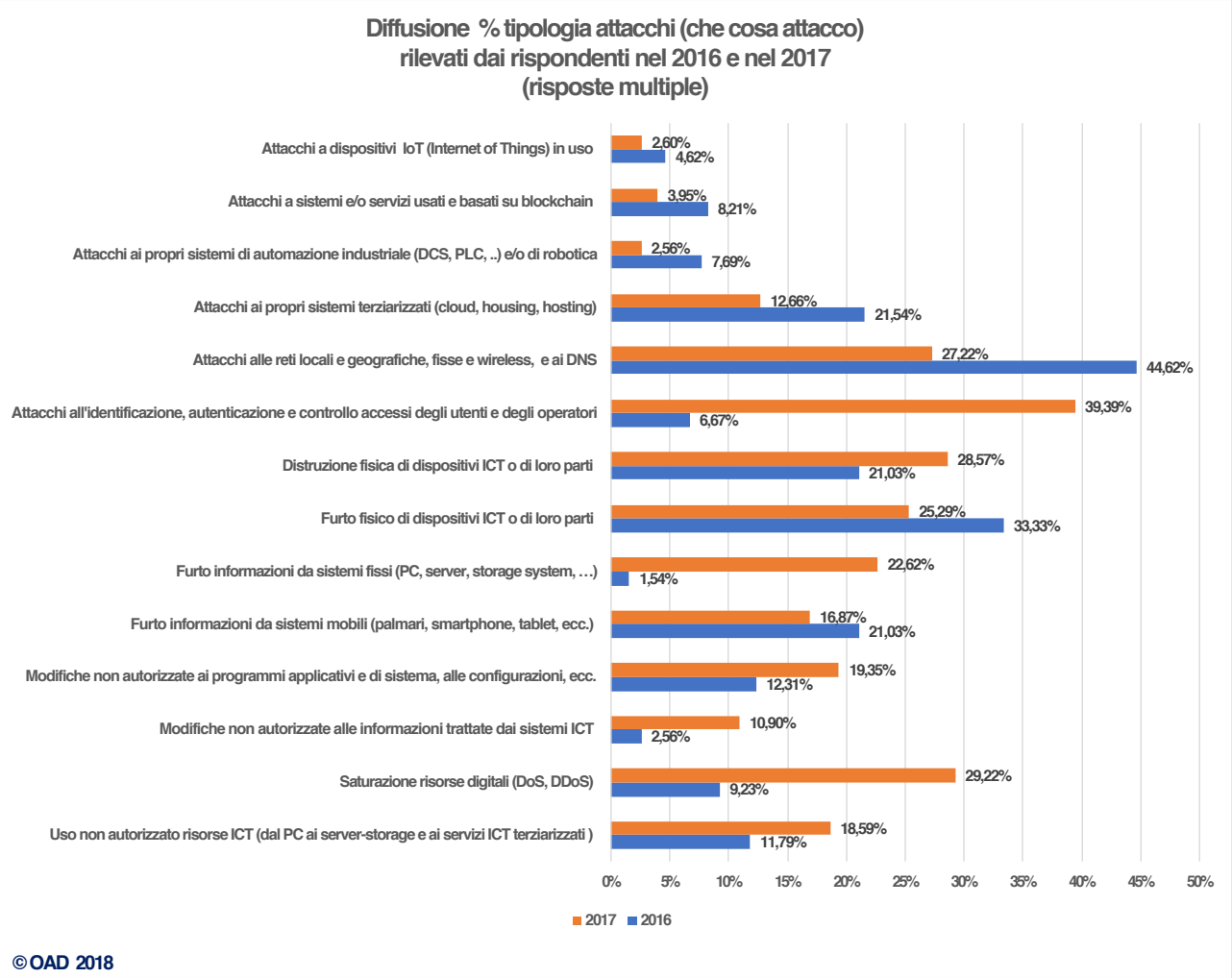

Fig. 6-7

La fig. 6-8 sintetizza, per le varie tipologie di attacco rilevate dai rispondenti nel 2017, le tecniche di attacco usate: come mostra la figura, esse sono state raggruppate in sette "macro" categorie, dettagliate nell'Allegato A.1.1, tra le quali il rispondente poteva scegliere con risposte multiple.
Il valore in % sull'asse orizzontale del grafico è un indice della loro diffusione nel 2017 nell'ambito delle 14 tipologie di attacchi, e non ha uno specifico significato statistico.
Nei paragrafi seguenti del presente capitolo, tipologia per tipologia, vengono riportate le tecniche d'attacco che i rispondenti hanno rilevato o che, a buon senso, hanno stimato rispondendo al questionario.
I moderni attacchi sono il più delle volte polimorfi, usano cioè più tecniche di attacco, sia contemporaneamente, sia in successione cronologica. Ad esempio, viene prima effettuata una raccolta di informazioni, ad esempio tramite social engineering o scannerizzazione di indirizzi IP pubblici, poi con queste informazioni si tenta di accedere alla risorsa ICT target installando malware, o virus o bot; viene poi attuato l'attacco finale che può a sua volta avere obiettivi multipli e contemporanei: rubare informazioni, danneggiare o modificare applicativi, bloccare servizi, ecc .
Al primo posto come più usati per i vari attacchi codici maligni e script, che includono anche i comandi

diretti al sistema operativo e/o alle banche dati (§A.1.1.3): la diffusione in Italia di ransomware negli anni più recenti ha sicuramente contribuito al primo posto di questa categoria. Al secondo posto gli agenti autonomi, ossia i virus, che sono una parte dei codici maligni, ma si differenziano per la loro capacità di diffondersi, come i virus biologici. I Toolkit raggiungono il terzo porto come diffusione, grazie anche ai numerosi software gratuiti messi a disposizione su Internet. Molti di questi strumenti possono essere usati sia per prevenire e contrastare gli attacchi, come le scansioni per la vulnerabilità di un sistema, ma anche per individuare le possibili vulnerabilità dello stesso e da queste partire per un attacco.

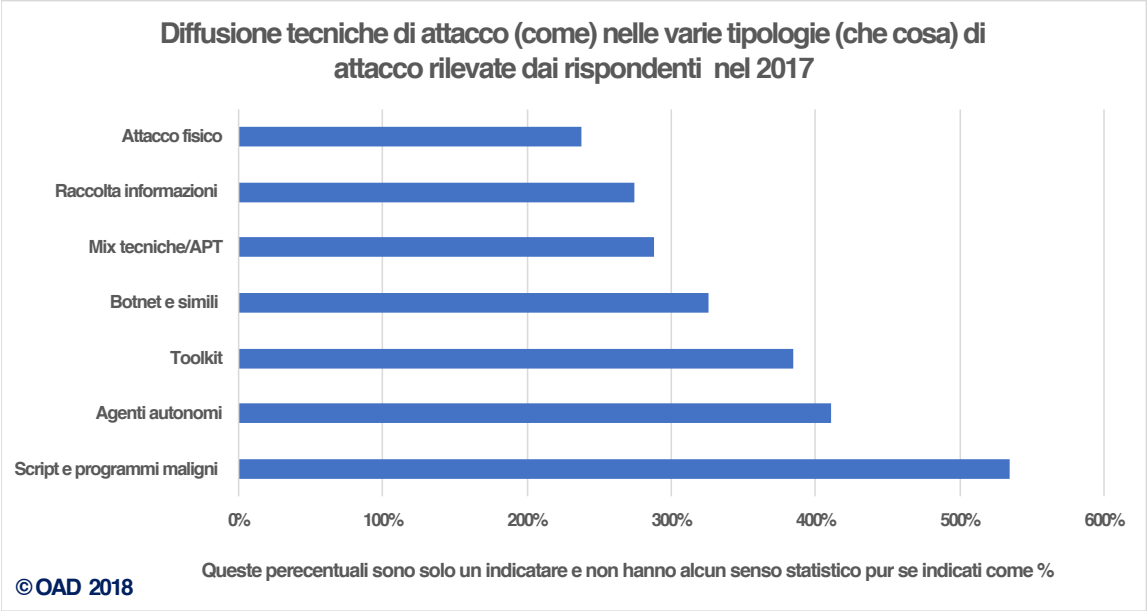

Fig. 6-8

Le botnet sono usate soprattutto per la saturazione delle risorse, un attacco non facile da contrastare se non si hanno specifici accordi e soluzioni preimpostate con il fornitore di rete, e la forte diffusione nel 2017 (con un forte incremento rispetto al 2016) di questa tipologia di attacco spiega la diffusione anche in Italia di botnet. Con una minore diffusione, ma sempre significativa, gli APT, la raccolta di informazioni e gli attacchi fisici.

Le fig. 6-9 e 6-10 mostrano la distribuzione % degli attacchi e della loro numerosità per settore merceologico delle aziende/enti dei rispondenti, rispettivamente negli anni 2017 e 2016.

In §10.2 è dettagliata la tipologia e la numerosità dei rispondenti per settore merceologico, avendo preso a riferimento la classificazione ufficiale ATECO[6].
Purtroppo, e nonostante gli sforzi effettuati nel 2017 e nel 2018 nel cercare di coinvolgere varie associazioni di categoria dei settori merceologici che nel passato meno (o per nulla) avevano fornito rispondenti, anche in questa edizione i settori che più hanno risposto sono le aziende ICT, le società di servizi, che includono anche gli studi professionali, e quelle manifatturiere.
I referenti di alcune aziende/enti non hanno risposto ad alcune delle domande del questionario, trince-

6 - https://www.istat.it/it/files/2011/03/metenorme09_40classificazione_attivita_economiche_2007.pdf

randosi dietro le policy aziendali che impediscono il fornire questo tipo di informazioni classificate come riservate, anche se il questionario è totalmente anonimo.
I settori merceologici Servizi ICT (Codice Ateco J62, J63, S95.1), Servizi professionali (Codici Ateco L, M, N77, N78, N80, N81, N82) e Industria manifatturiera e costruzioni (Codici Ateco C e F) hanno un numero sufficiente di risposte e le indicazioni percentuali loro relative forniscono un indicatore credibile, in termini statistici: tutti gli altri contribuiscono numericamente all'inquadramento generale del fenomeno degli attacchi digitali in Italia, ma sono troppo pochi per poter effettuare specifiche analisi settoriali e considerarli indicatori della situazione degli attacchi digitali del loro settore.
Per questo motivo si è pertanto fatto soprattutto uso di correlazioni con le dimensioni delle aziende/enti, più che con i settori merceologici. Si spera ovviamente di riuscire nei prossimi anni ad allargare la base dei rispondenti a quei settori che ad oggi hanno risposto in misura minimale.

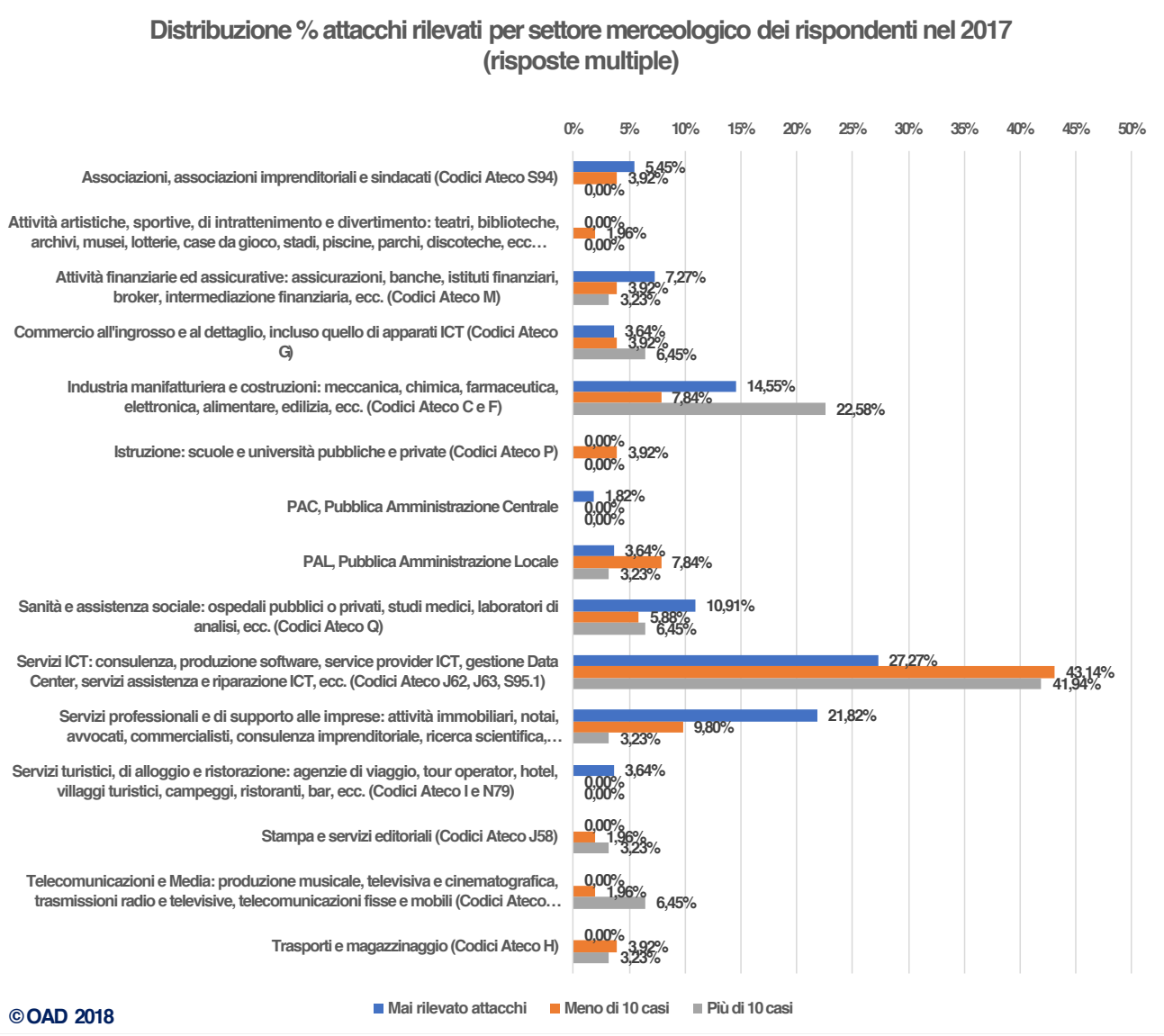

Fig. 6-9

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

- Avendo modificato nel Questionario OAD 2018 la tassonomia degli attacchi, distinguendo il più chiaramente possibile che cosa è attaccato dalle tecniche di attacco, non è più possibile un diretto confronto con i dati delle precedenti edizioni di OAD e OAI, anche se di valore puramente indicativo e non statistico.
- Il furto di dispositivi ICT e di loro parti mantiene un'alta percentuale sia nel 2016 che nel 2017: a giudizio dell'autore questo è soprattutto motivato dalla rivendita al mercato nero di sofisticati e costosi smartphone e tablet.
- Lascia stupiti l'alta % di distruzione fisica di risorse ICT o di loro parti: il questionario chiariva che tali distruzioni, così come tutti gli altri attacchi considerati, dovevano essere intenzionali, e non causati da malfunzionamenti o rotture dovute all'usura o ad un involontario loro cattivo uso. A parere dell'autore alcuni rispondenti hanno considerato come attacchi anche rotture dovute a "naturali" decadimenti dei dispositivi ICT; la fig. 6.1-3 evidenzia comunque una relativamente elevata % di motivazioni del tipo vandalismo, terrorismo, ricatto.
- I tre macrosettori merceologici che hanno avuto più rispondenti, ICT, servizi, manifatturiero, sono anche quelli che evidenziano una maggior percentuale di attacchi subiti.
- Interessante evidenziare come i fornitori ICT, che hanno avuto il maggior numero di rispondenti, sono quelli che hanno rilevato, in %, più attacchi, rispetto agli altri settori merceologici; questo è dovuto, a giudizio dell'autore, principalmente a due fattori concomitanti:
- Queste aziende sono tra i primi obiettivi di attacchi da parte di organizzazioni criminali, dato anche il trend crescente di terziarizzazione, soprattutto con il cloud; si tenga presente che la recente diretta NIS[7] per la strategia e gli organi di supporto alla cybersecurity nazionale, inquadrata in quella europea, considera tra gli enti oggetto della direttiva i fornitori di infrastrutture digitali, di motori di ricerca, di servizi cloud e di piattaforme di commercio elettronico;
- Nella quasi totalità dei casi i fornitori di servizi ICT italiani o operanti in Italia conoscono ed applicano le best practice della sicurezza digitale, e pertanto i loro sistemi informatici, sistematicamente monitorati e controllati, individuano facilmente gli attacchi ed i tentativi di attacco, mentre i sistemi informatici di aziende/enti di altri settori non sono sempre in grado di individuarli, se non dopo molto tempo e/o dopo essersi accorti degli impatti subiti.
- Più furti di informazioni dai dispositivi d'utente fissi (22,62%) che da quelli mobili (16,87%), come dettagliato in §6.3 e §6.4. 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. Il posto di lavoro fisso, invece, 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. Tutto questo spiega l'impennata di furti dai dispositivi fissi. In termini di timori per il futuro, si veda §8, sono più temuti i furti di informazione dai dispositivi mobili.

Un elemento basilare per comprendere la gravità e la criticità di un attacco è l'individuazione del possibile attaccante e delle sue motivazioni.
Per il 2017 il Questionario 2018 OAD ha chiesto ai compilatori di indicare le possibili motivazioni dell'at-

7 - NIS, Network and Information Security. Si veda https://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/cyber-la-nis-entra-in-vigore-litalia-si-rafforza-e-fa-rete-con-lue.htmlhttp://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2018-06-09&atto.codiceRedazionale=18G00092&elenco30giorni=false

tacco (o degli attacchi) più gravi per ogni tipologia d'attacco: le risposte avute sono sintetizzate in grafici nei vari paragrafi da §6.1 a §6.16.
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.

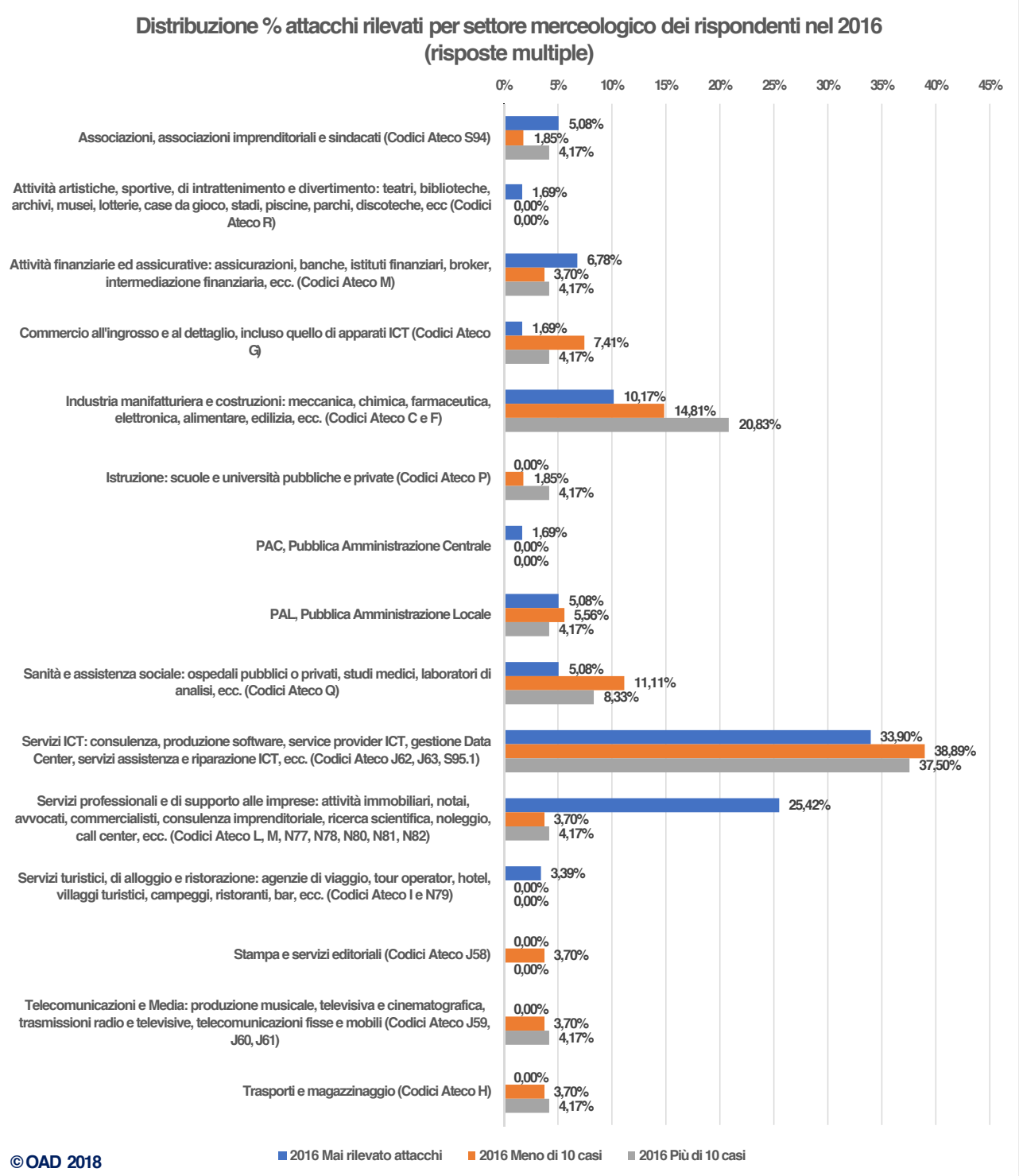

Fig. 6-10

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 mazzate per scassare la loro struttura, rottura delle connessioni e delle parti elettroniche, rottura delle ventole di raffreddamento e della parte di alimentazione, ecc. Nel Questionario OAD 2018, 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 2017: nel complesso il 28,57% dei rispondenti, una percentuale elevata. Lo stesso campione di rispondenti, per il 2016, ha subito tali attacchi (fig. 6-9) per il 21,03%: si è avuta quindi una crescita non trascurabile, pur essendo già percentualmente alto anche il valore del 2016, con lo stesso campione di rispondenti. Il valore emerso , sia per il 2016 che per il 2017, è veramente alto, e l'autore non vorrebbe che alcuni rispondenti abbiano inserito in questa tipologia anche rotture non intenzionali dei dispostivi, ossia dovute a guasti dell'hardware, pur essendo ben precisato nel questionario che gli attacchi da considerare devono essere solo quelli intenzionali.
Un ulteriore errore potrebbe essere stato l'includere nel danneggiamento di un dispositivo anche il suo furto, considerato invece con specifica domanda nel questionario e analizzato nel prossimo paragrafo.

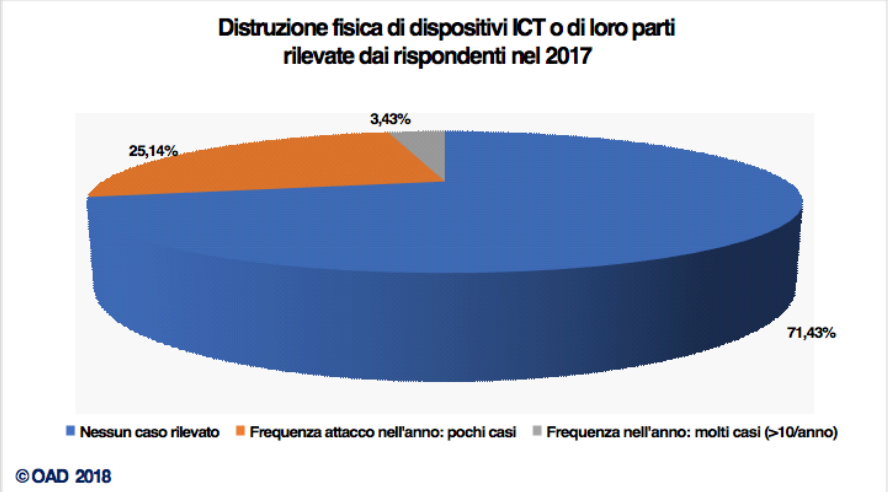

Fig. 6.1-1

La fig. 6.1-2 evidenzia come l'impatto più diffuso tra le aziende/enti dei rispondenti, 60,00%, sia stato la parziale interruzione dei servizi ICT erogati e che circa 1/3 dei rispondenti non abbia avuto impatti, o siano stati irrilevanti.

La fig. 6.1-3 elenca le principali motivazioni dell'attacco: al primo posto la ritorsione e/o il ricatto, al secondo il "non so" del rispondente insieme all'hacktivism, al terzo il vandalismo. Nella voce "altro" i rispondenti hanno indicato motivi riconducibili all'imperizia degli utenti e/o degli operatori, oltre a maldestri tentativi di furto.

La fig. 6.1-4 mostra il tempo di ripristino della situazione ex ante l'attacco nel caso del peggior attacco subito. Il 42% delle aziende/enti dei rispondenti, che hanno subito questo tipo di attacco, ripristina entro un solo giorno, confermando così l'impatto non o poco significativo, e ben il 28% ripristina tra 2 e 3 giorni. Solo in pochi casi si supera la settimana, e in pochissimi il mese.

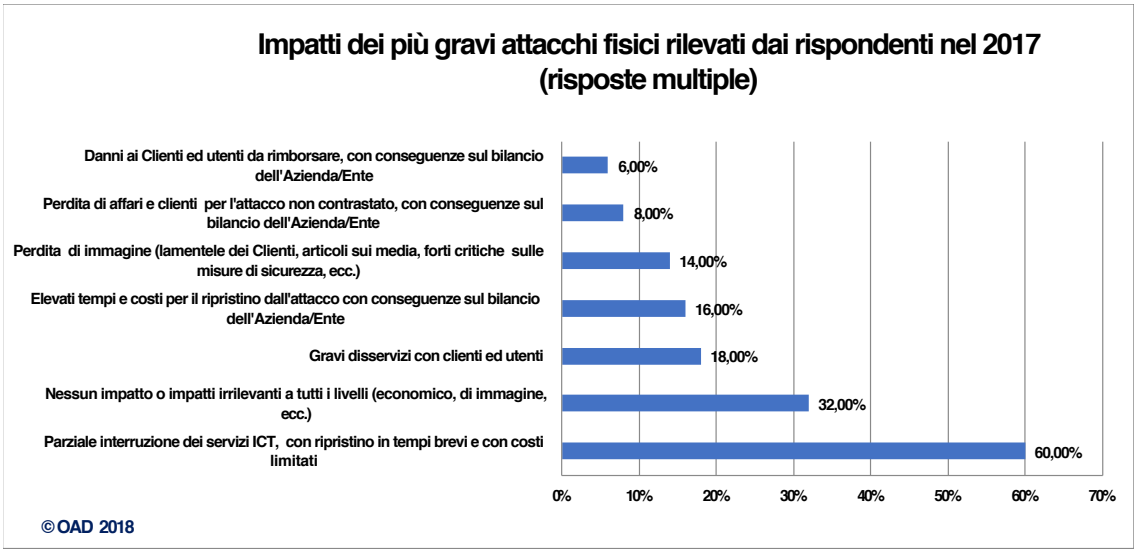

Fig. 6.1-2

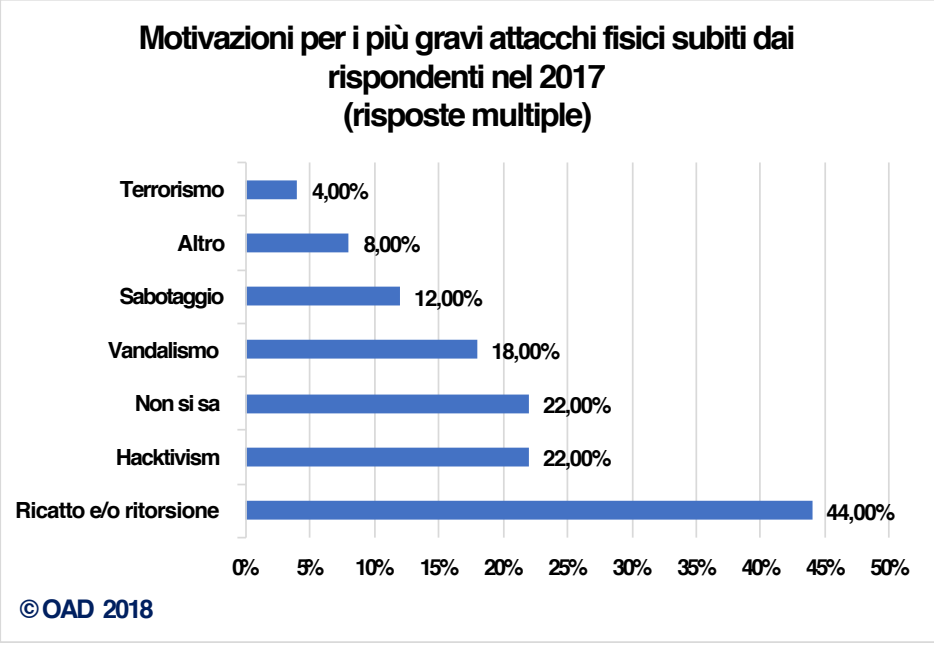

Fig. 6.1-3

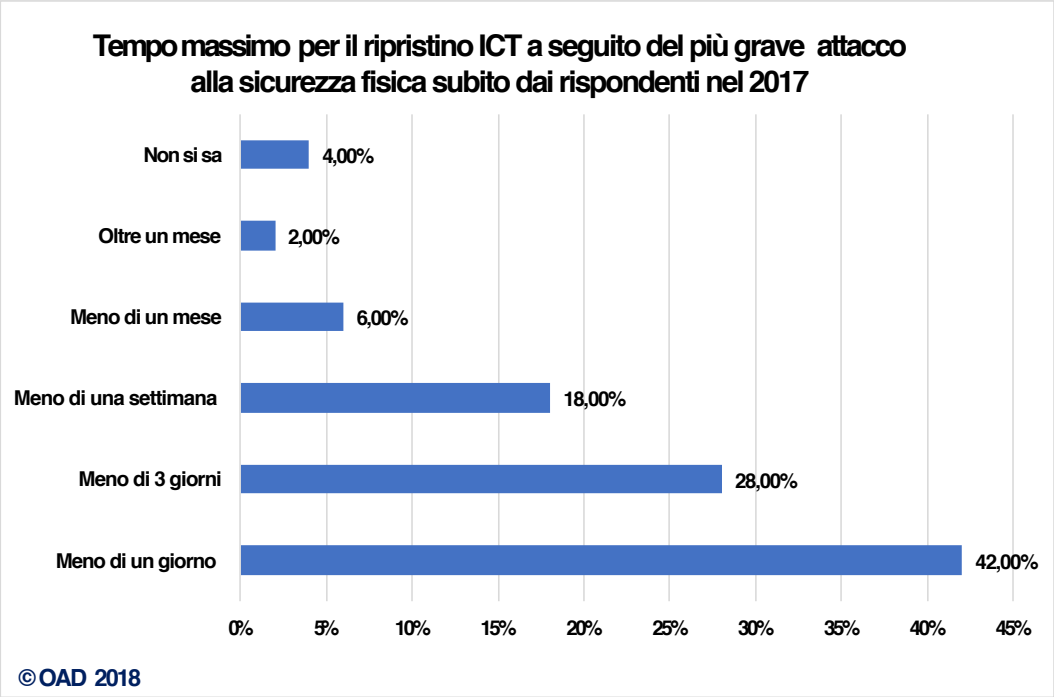

Fig. 6.1-4

6.2 - Furto fisico di dispositivi ICT o di loro parti

Come più volte sottolineato anche nelle precedenti edizioni, una alta percentuale di furti di dispostivi ICT è dovuta prevalentemente al furto di smartphone e di tablet, anche per l'ampio mercato "nero" che si è creato in Italia.

La fig. 6.2-1 evidenzia quanti rispondenti hanno subito un furto di dispositivi ICT nel 2017: nel complesso il 25,29 % dei rispondenti, una percentuale elevata ma in diminuzione rispetto all'anno precedente (33,33%, si veda fig. 6-7).
Anche per il furto di dispositivi ICT o di loro parti, quali ad esempio l'hard disk o delle periferiche del sistema oggetto del furto, la tecnica d'attacco può essere solo l'attacco fisico: per tale motivo nel questionario OAD 2018, per questa tipologia di attacco non sono state riportate le sotto-domande sulle possibili tecniche di attacco usate.

La fig. 6.2-2 mostra gli impatti subiti a seguito del furto di dispostivi ICT: la metà delle aziende/enti rispondenti ha rilevato la parziale interruzione dei servizi ICT erogati e un terzo circa non ha avuto impatti, o sono stati irrilevanti.

La fig. 6.2-3 elenca le principali motivazioni dell'attacco: il 60% dei rispondenti ritiene che il motivo più diffuso sia il valore della risorsa ICT rubata da rivendere, ed il secondo, per il contenuto informativo dell'oggetto rubato: tipicamente dispositivi mobili ed hard disk. Nella voce "altro" i rispondenti hanno indicato motivi riconducibili all'imperizia degli utenti finali e/o privilegiati.

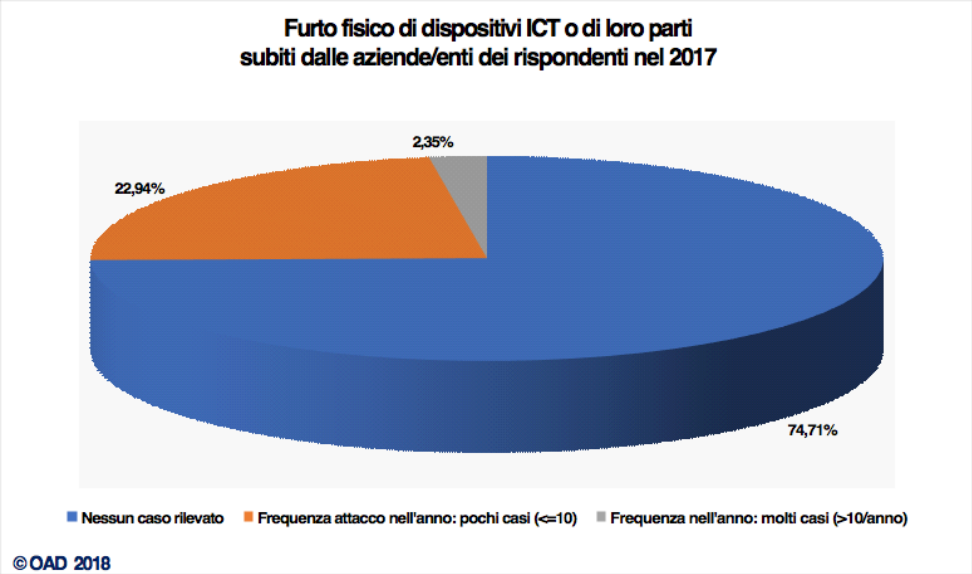

Fig. 6.2-1

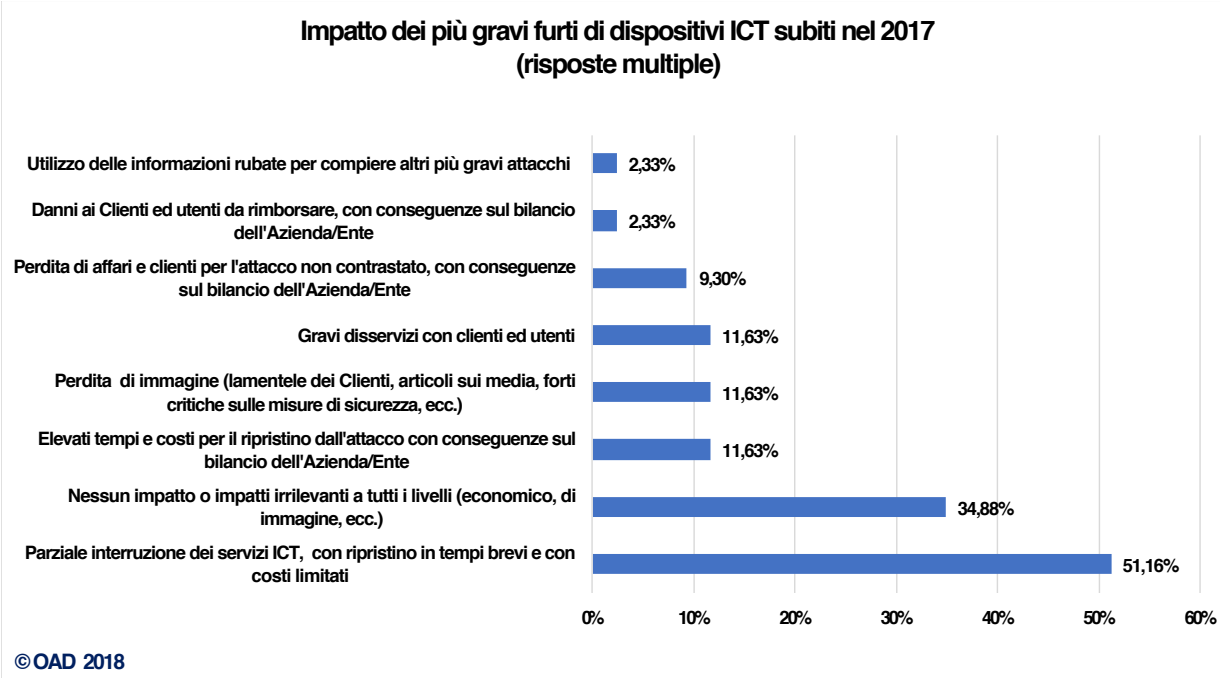

Fig. 6.2-2

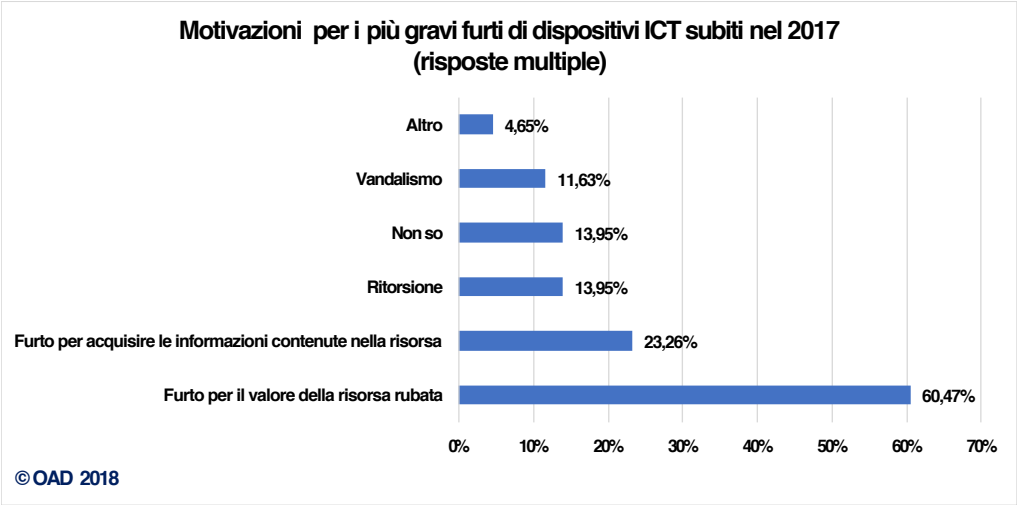

Fig. 6.2-3

La fig. 6.2-4 mostra il tempo di ripristino della situazione ex ante l'attacco nel caso del peggior attacco subito: entro 3 giorni si ripristina complessivamente nel 76,19% dei casi.

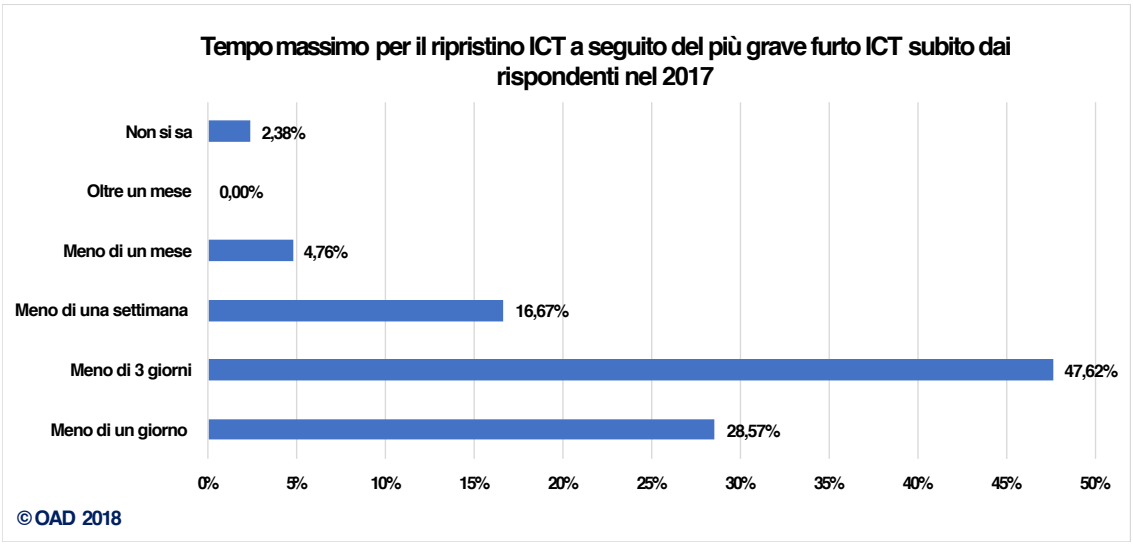

Fig. 6.2-4

6.3 - Furto informazioni da sistemi ICT fissi

I sistemi ICT fissi includono PC e posti di lavoro, server, storage system, unità di rete, e così via. Il furto di informazioni da sistemi fissi implica che l'attaccante sia stato in grado di accedere, senza averne i diritti, ed una volta entrato di acquisire le informazioni, tipicamente archiviate in file o su banche dati, e di copiarle. E' 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, ecc.
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[8] indica: si veda anche §6.9 sugli attacchi alle informazioni e §9.2 sulle misure tecniche di contrasto in atto da parte dei rispondenti.

La fig. 6.3-1 evidenzia quanti rispondenti hanno subito tale tipo di attacco nel 2017: nel complesso il 22,62% dei rispondenti, contro il solo 1,54% nel 2016 (fig. 6-7). Il forte incremento avuto nel 2017 è un ulteriore indicatore di come il 2017 sia stato un anno particolarmente grave per numero e gravità di attacchi digitali. La percentuale rilevata è superiore a quella relativa ai furti di informazioni dai dispositivi d'utente mobili (16,87%), di cui in §6.4. 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. Il posto di lavoro fisso invece, 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. Tutto questo spiega l'impennata di furti dai dispositivi fissi.

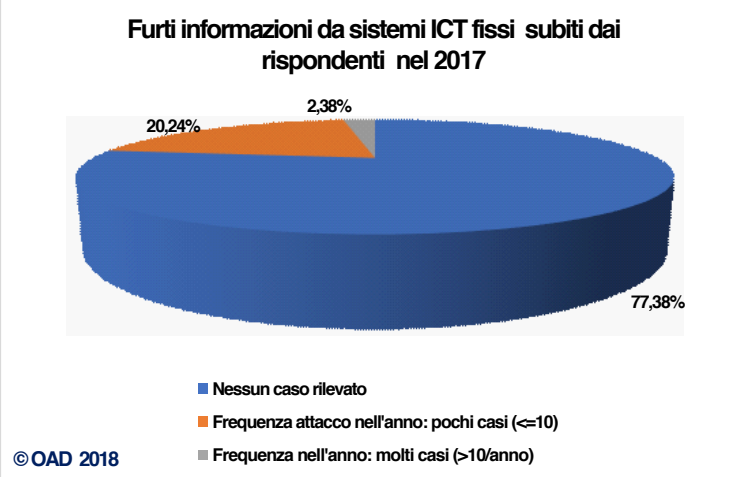

Fig. 6.3-1

La fig. 6.3-2 riporta quali sono state le tecniche d'attacco per il furto di informazioni da sistemi ICT fissi, con risposte multiple. La tecnica più diffusa, secondo 2/3 dei rispondenti, è tramite malware, script e "command"; segue, con poco meno della metà dei rispondenti, la raccolta di informazioni tramite le quali poter rubare le informazioni target. Al terzo posto, sempre con un riguardevole 40% circa, l'uso di agenti autonomi. Al

8 - 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

quarto l'uso di toolkit per poco più del 20%. Le altre tecniche hanno percentuali più basse. Solo il 5,26% dei rispondenti non sa quale tecnica sia stata usata per rubare le informazioni: è una percentuale bassa, inferiore a quella che si sarebbe aspettato l'autore. E questa risposta, come le analoghe altre nei vari punti del questionario, conferma la correttezza delle risposte per la stragrande maggioranza dei rispondenti.

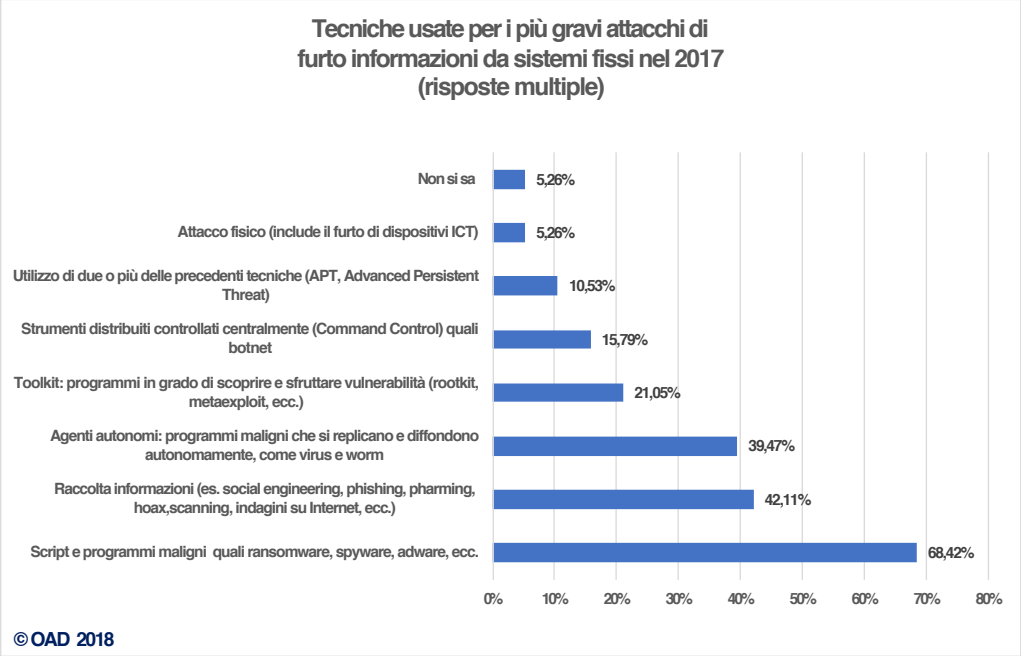

Fig. 6.3-2

L'impatto causato da questi furti di informazioni è illustrato nella Fig. 6.3-3, che per la metà dei rispondenti che hanno rilevato questo attacco non ha causato danni o gli impatti sono stati irrilevanti. Con forte distacco, ~~quasi a metà rispetto~~ il 26,32% dei rispondenti ha subito una parziale interruzione dei servizi ICT, ma di breve durata e di relativamente facile ripristino. Con % che man mano si riducono cresce la gravità dell'impatto subito. Si rammenta che le risposte sono multiple, e che lo stesso attacco di grave impatto può aver causato perdita di immagine sul mercato con conseguente perdita di business, gravi disservizi che hanno causato elevati costi sia per il loro ripristino sia per le eventuali penali da pagare ai clienti, e così via.

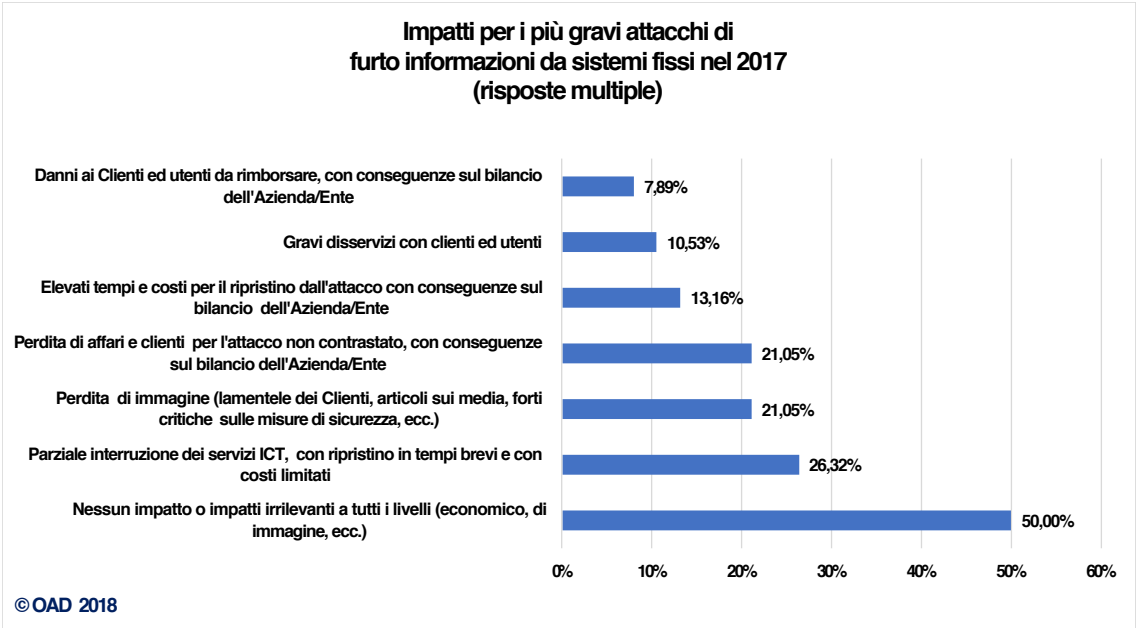

Fig. 6.3-3

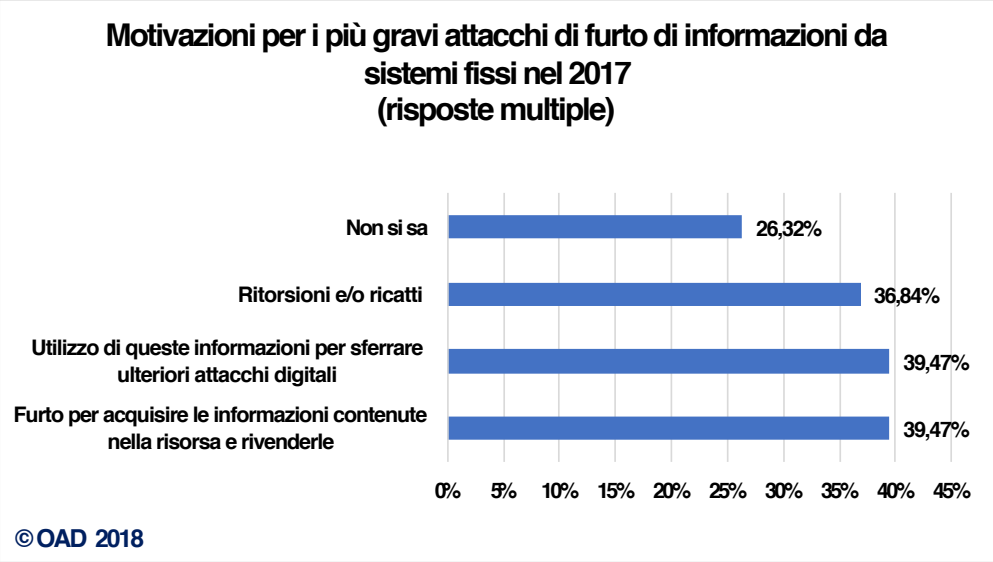

Fig. 6.3-4

Le motivazioni stimate dai rispondenti per i furti di informazione di questo tipo sono riportate nella fig. 6.3-4. Il furto delle informazioni è motivato con la stessa percentuale (39,47%) sia per rivenderle, sia per usarle per sferrare altri attacchi. Una percentuale leggermente inferiore ritiene che tali informazioni siano usate per ritorsioni e/o ricatti.

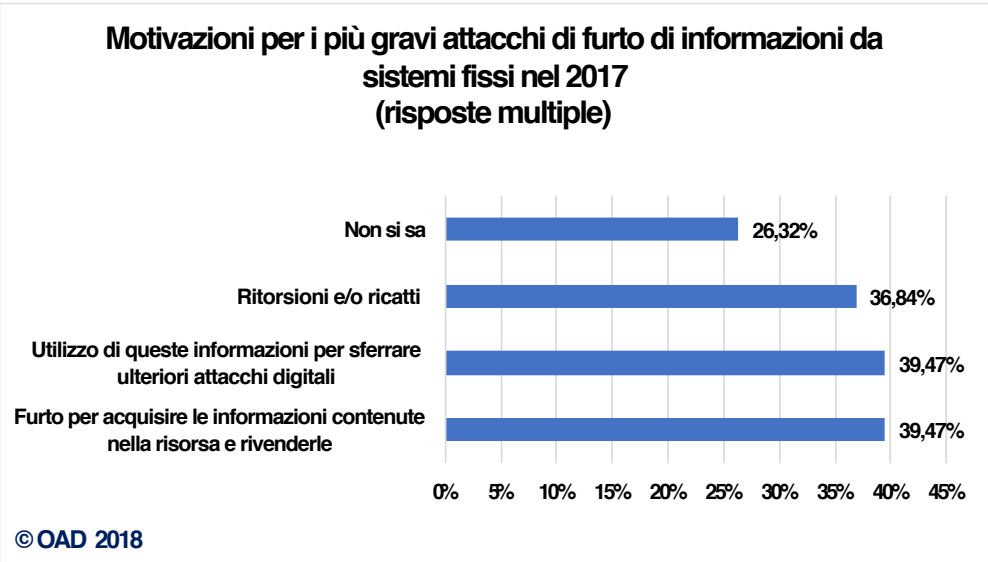

Fig. 6.3-5

6.4 - Furto informazioni da sistemi ICT mobili

Per sistemi ICT mobili si intendono i dispositivi d'utente mobili, che includono tipicamente palmari, smartphone, tablet, ed anche i leggeri laptop di piccole dimensioni. Oltre a questi – di qui la volutamente generica indicazione nel titolo e nel questionario 2018 di "sistemi ICT mobili" – chiavette e gli hard disk removibili con interfaccia USB, che ormai 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 che questi sistemi possono facilmente essere occultati in una tasca, è veramente facile poter copiare interi file system da piccoli server, oltre che da singoli PC.
Come mostrato nella fig. 6.4-1, il 16,87% dei rispondenti ha rilevato attacchi di questo tipo, in diminuzione rispetto al 21,03% del 2016 (fig. 6-7).

La fig. 6.4-2 sulle tecniche usate per portare tale attacco, almeno nel caso più grave, non evidenzia però il furto fisico ("solo" il 14,29% dei rispondenti) al primo posto, bensì l'uso di Script o di programmi maligni, con un 42,86%. Infatti, se sui dispositivi mobili ci sono informazioni appetibili, essi sono protetti, e così il semplice furto non consente di accedere alle informazioni che vi sono contenute; con opportuni script o malware, magari attivati via phishing, è ben più probabile raggiungere le informazioni contenute.

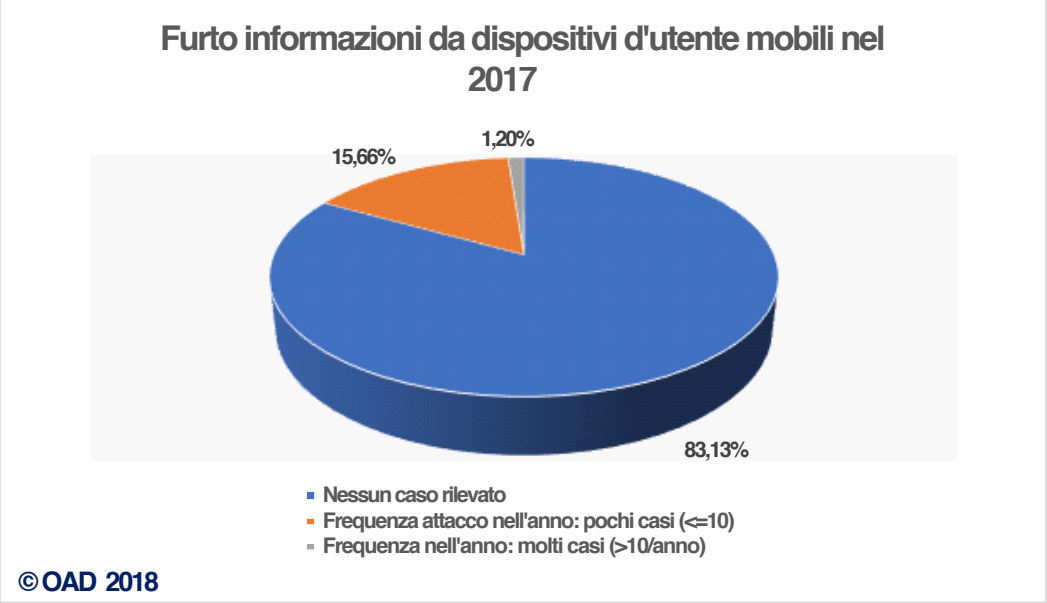

Fig. 6.4-1

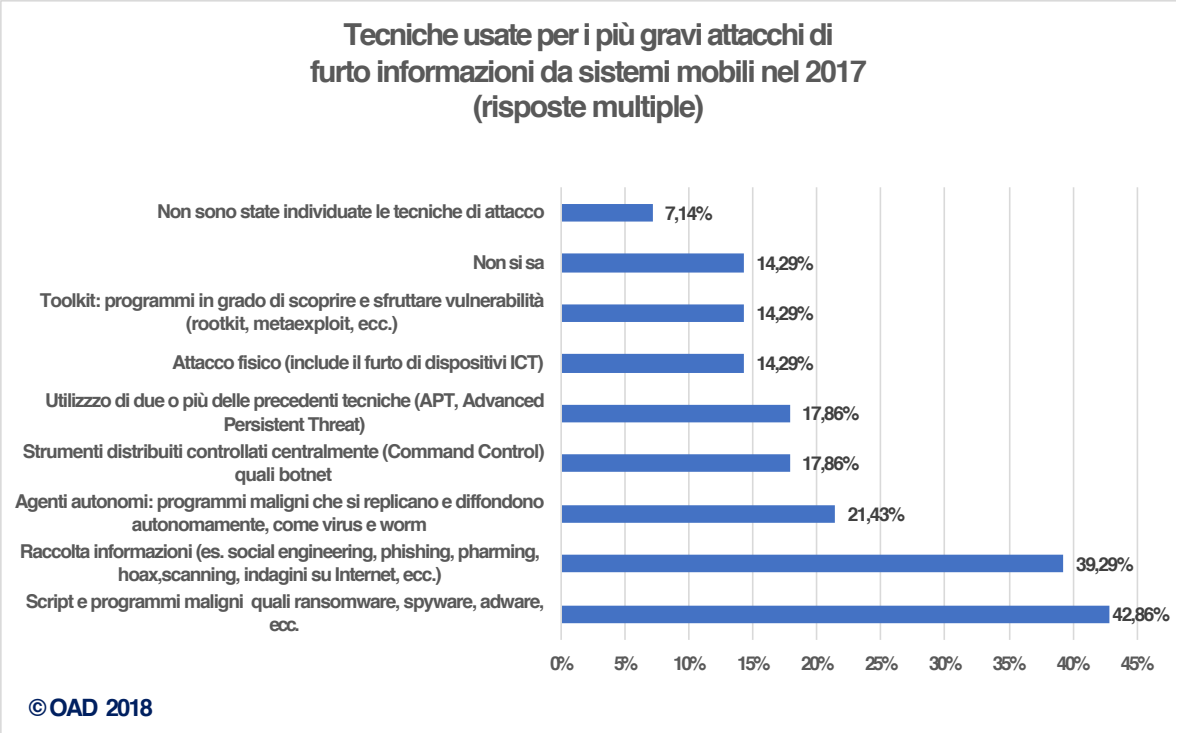

Fig. 6.4-2

Ed infatti al secondo posto si trova la tecnica della raccolta di informazioni, con una percentuale superiore al 39%. L'uso di agenti autonomi replicanti e di bot, oltre che di toolkit, ha percentuali decrescenti ma comunque non trascurabili. Le risposte potevano essere multiple, e come già evidenziato, il furto di informazioni anche su dispostivi d'utente mobili richiede normalmente la concatenazione e/o la contemporaneità di più tecniche.

La fig. 6.4-3 evidenza gli impatti subiti a seguito del più grave attacco di furto di informazioni da sistemi mobili. Più della metà dei rispondenti che hanno subito tale attacco, non ha riscontrato impatti, o solo impatti irrilevanti sul sistema informatico e sul suo funzionamento. Ma il primo impatto dell'elenco riguarda gravi disservizi, con un 28,57%, quindi un forte e critico impatto, che a sua volta può aver causato gli altri impatti elencati, che hanno tutti % decrescenti.

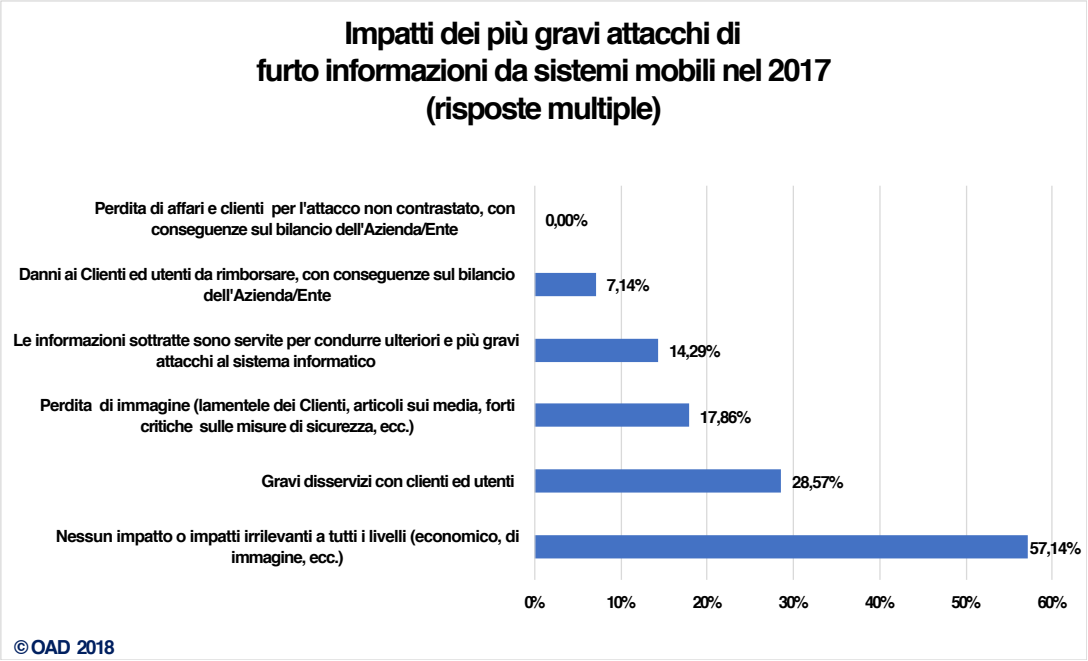

Fig. 6.4-3

Le possibili motivazioni stimate dai rispondenti che hanno subito questo attacco includono al primo posto, con più del 42% dei rispondenti, l'utilizzo delle informazioni rubate per poter sferrare ulteriori attacchi digitali, come mostrato in fig. 6.4-4. Seguono a scalare ritorsioni/ricatti ed il furto per acquisire informazioni da rivendere sul mercato nero.

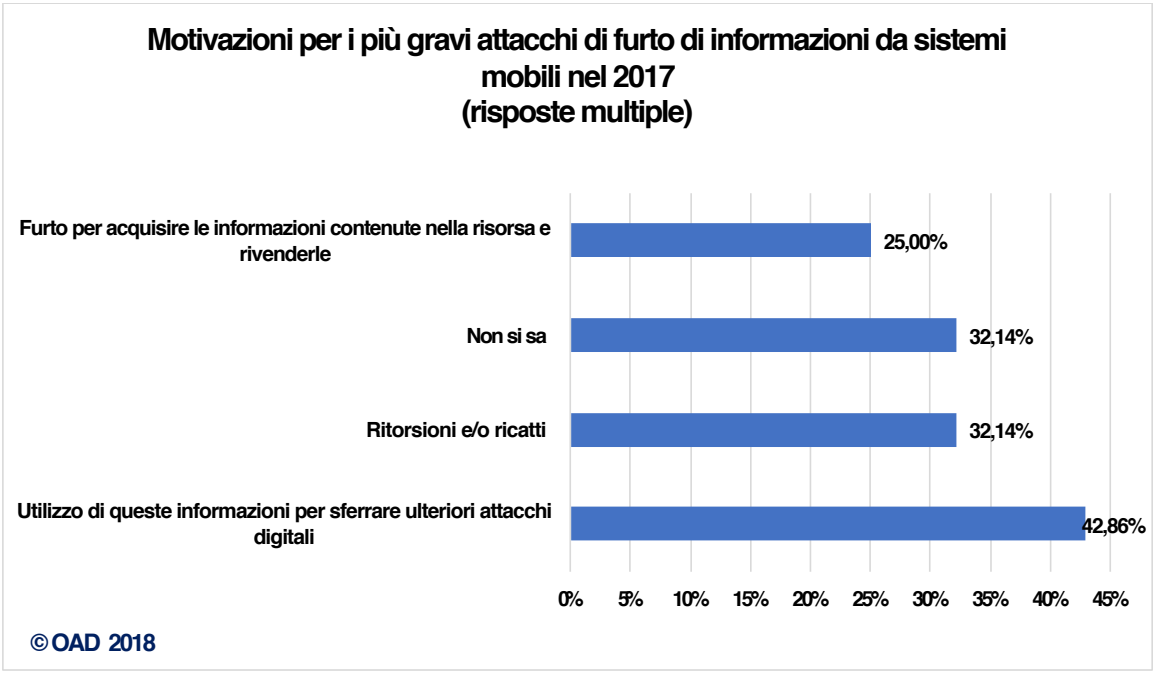

Fig. 6.4-4

La fig. 6.4-5 evidenzia il tempo massimo che è stato speso per il ripristino nel caso più grave di furto di informazioni da sistemi mobili. La criticità di questi furti è ulteriormente evidenziata dai tempi massimi di ripristino: circa i 2/3 dei rispondenti hanno ripristinato il caso peggiore in meno di 3 giorni, ben il 22,22% ci ha messo tra 4 e 7 giorni, ed una piccola %, ma esistente, ha impiegato più di un mese.

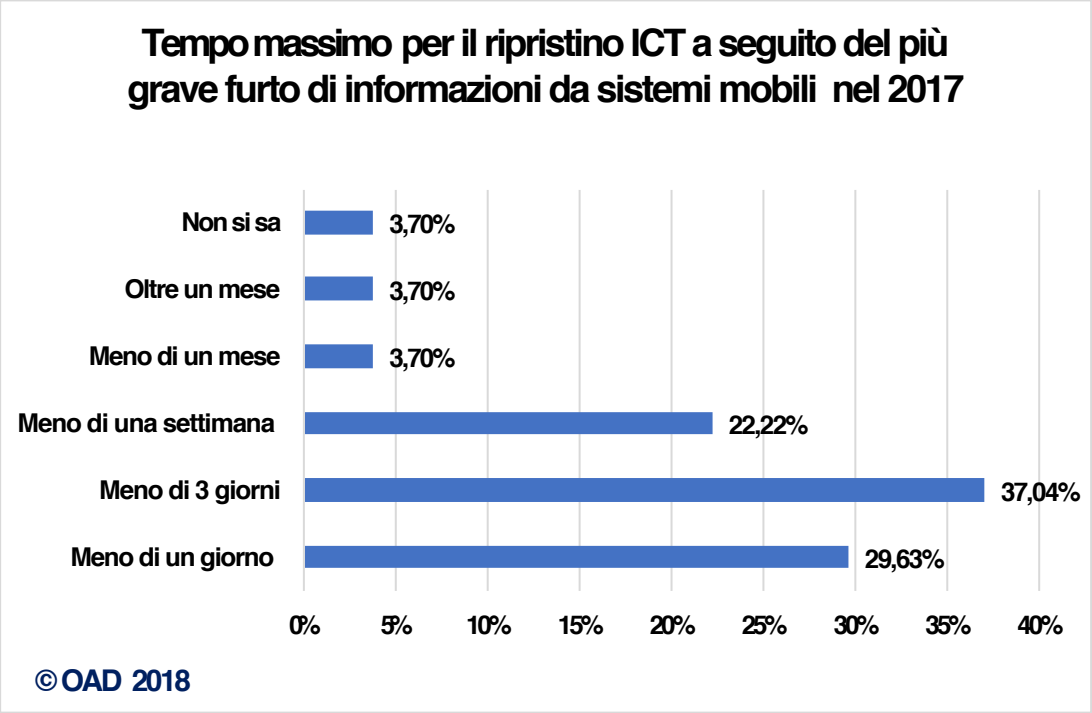

Fig.6.4-5

6.5 - Attacchi all'identificazione, autenticazione e controllo accessi degli utenti e degli operatori

Questa tipologia di attacchi è alla base del furto dell'identità digitale sia a livello di utenti finali sia a livello degli utenti privilegiati. 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.
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 abilità di social engineering o sofisticate tecniche; i dati per accedere all'account sono forniti dallo stesso utente, quando richiede che un suo collega, di cui si fida, lo sostituisca in qualche attività informatica. E' un atteggiamento abbastanza diffuso, ma estremamente rischioso e che dovrebbe essere evitato.
In termini generali si fa riferimento ai tre livelli di identificazione, autenticazione e autorizzazione con la sigla IAA, che verrà usata nel seguito.
Come si evince dalla fig. 6.5-1, il 39,39 % dei rispondenti ha subito attacchi di questo tipo nel 2017, con

un fortissimo aumento rispetto al 6,67% del 2016 (fig. 6-7) per lo stesso bacino di rispondenti. Questo è senza dubbio uno dei principali indicatori, ma non l'unico, del considerevole aumento nel 2017, anche in Italia, degli attacchi informatici.

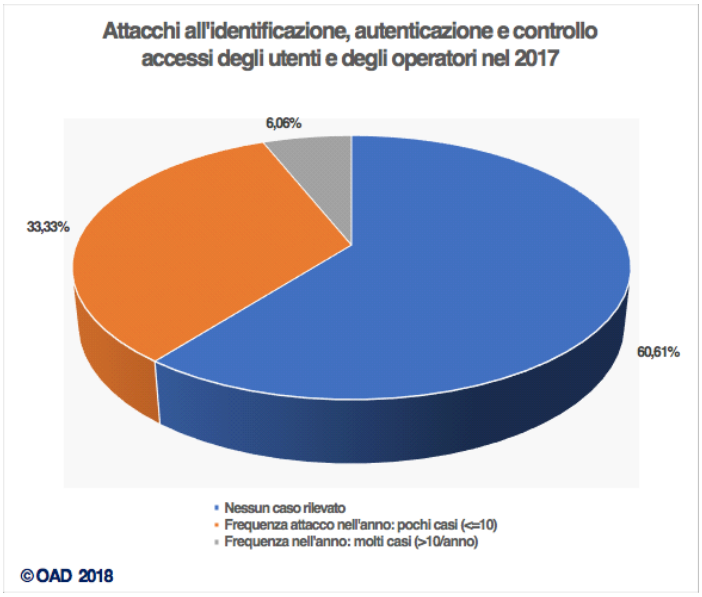

Fig. 6.5-1

La fig. 6.5-2 mostra la distribuzione % delle tecniche di attacco individuate o ipotizzate dai rispondenti che hanno subito questa tipologia d'attacco.
Come per molte altre tipologie d'attacco, al primo posto per il 40% dei rispondenti che hanno rilevato attacchi a IIA, l'uso di script e di programmi maligni; al secondo posto, ma con una % di poco inferiore, la raccolta di informazioni, tipicamente il social engineering. In effetti una delle più grandi vulnerabilità dell'ICT è dato dalle persone, sia utenti finali sia, soprattutto, quelli privilegiati.

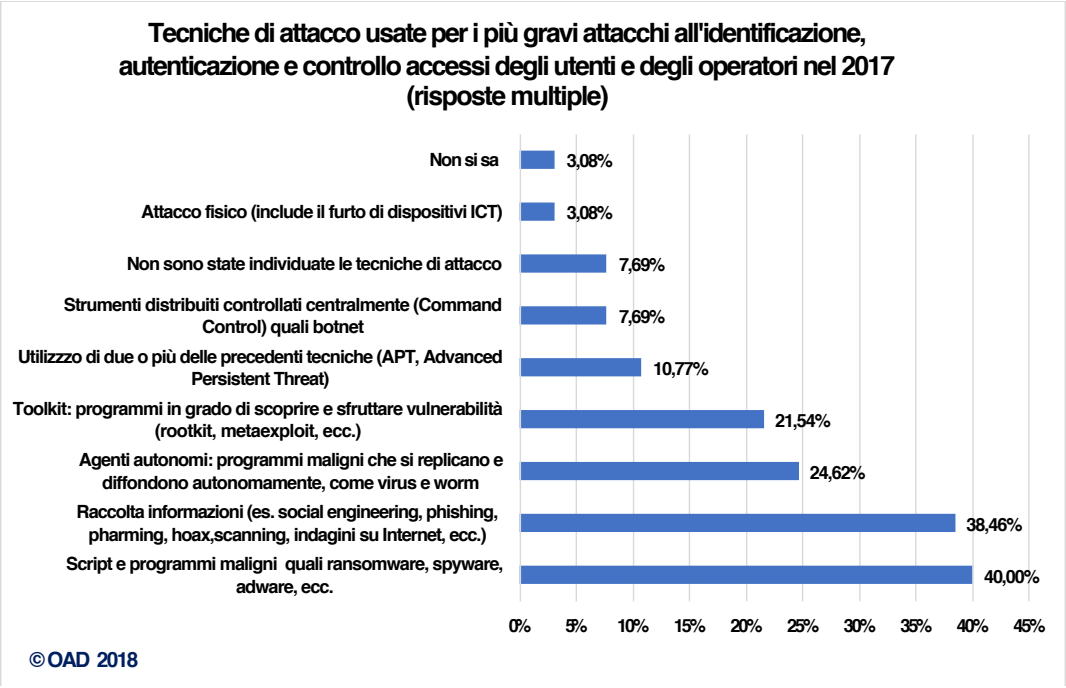

Fig. 6.5-2

La fig. 6.5-3 mostra gli impatti nel caso degli attacchi più gravi ai sistemi di IAAcon risposte multiple: quasi la metà dei rispondenti (46,15%) ha subito una parziale interruzione dei servizi ICT, ma ripristinati in breve tempo e con costi assai limitati, ed il 43,08% afferma di non aver avuto impatti: quindi quasi il 90% dei rispondenti dichiara di aver avuto impatti assai limitati o di non averne avuto. Impatti più gravi riguardano percentuali del 10% o inferiori, a scalare, come indicato nella figura.

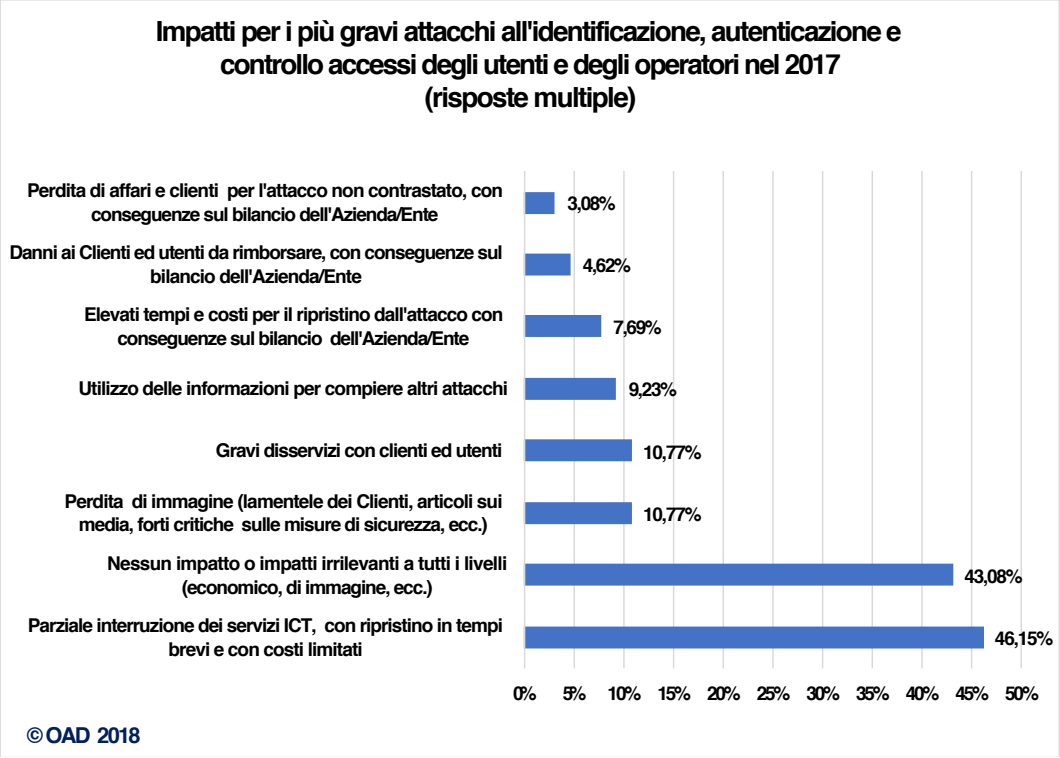

Fig. 6.5-3

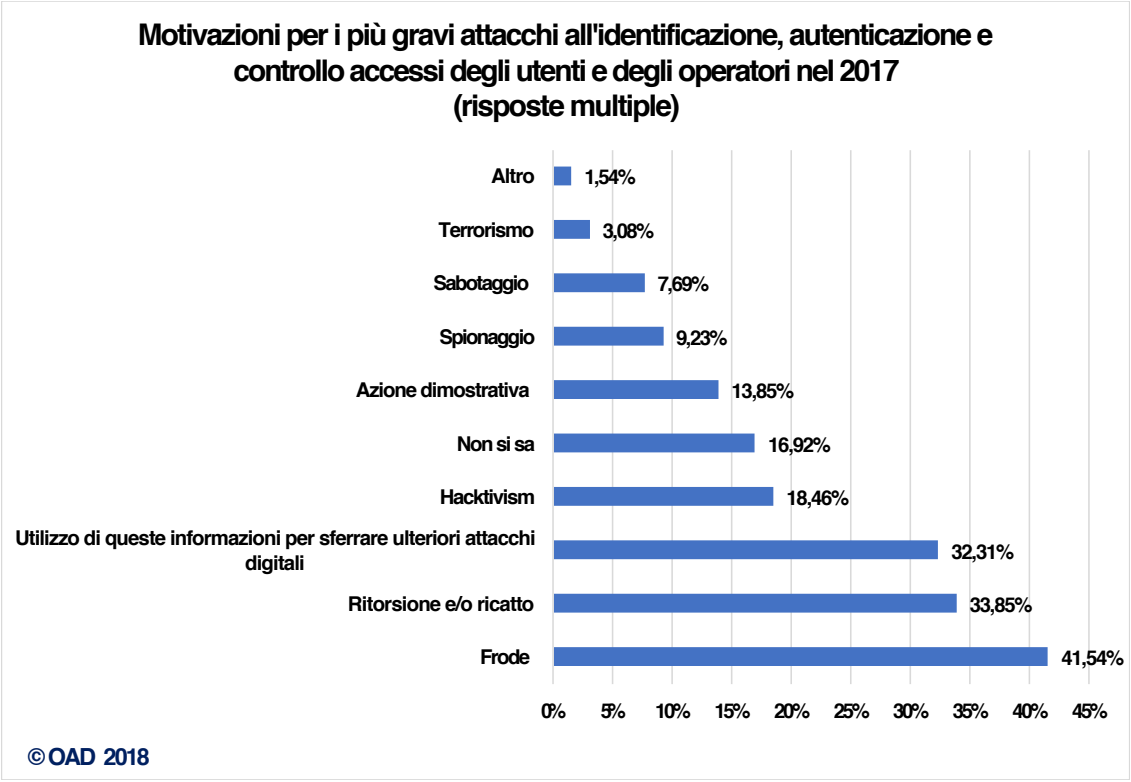

Fig. 6.5-4

La fig. 6.5-4 illustra le motivazioni per l'attacco più grave subito per la tipologia di attacco ai sistemi IAA, con possibilità di risposte multiple: al primo posto la frode, per poco più del 41% dei rispondenti, cui segue la ritorsione/ricatto per quasi il 34%, e per il 32,31% l'utilizzo di queste informazioni, in pratica l'account di un utente finale o privilegiato, per sferrare ulteriori più gravi attacchi. Ci si sarebbe aspettato una % per questa motivazione ben più alta: questo implica che il carpire gli account, per il bacino dei rispondenti, aveva come obiettivo primario delle frodi/ricatti.
Nella voce "altro" alcuni rispondenti hanno specificato che un'ulteriore motivazione è stata "l'ignoranza" degli utenti.

Il tempo massimo richiesto per il ripristino dopo l'attacco più grave all'IAA è stato, per i rispondenti, abbastanza breve: poco meno della metà entro un giorno, e entro 3 giorni complessivamente il 75% dei rispondenti che hanno rilevato questa tipologia di attacco. Solo il 5% ha dovuto impiegare tra una settimana ed un mese, e nessuno ha dovuto superare un mese per ripristinare il tutto.

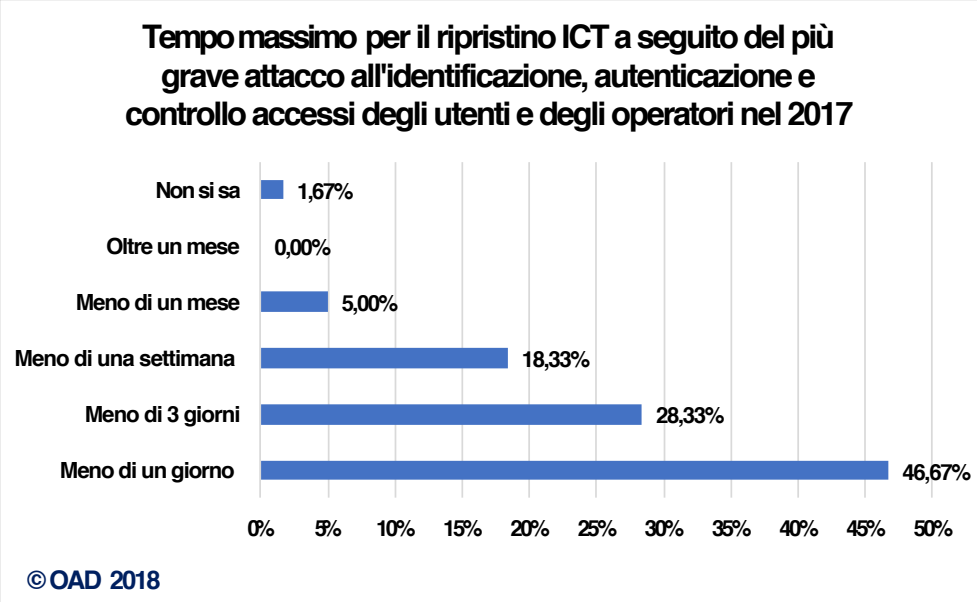

Fig. 6.5-5

6.6 - 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, in pratica WiFi) che geografiche per la telefonia mobile[9],

9 - 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 futuro G5, già in corso di sviluppo anche in Italia . Attualmente in Italia le reti cellulari supportano dal

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 2018 OAD ha raggruppato in un'unica tipologia l'ampia e diversificata famiglia degli attacchi alle reti. 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, lo sniffing del traffico, la saturazione della rete per un attacco DoS/DDoS che ha come obbiettivo un'applicazione web mirata che satura la connessione della rete al server che supporta l'applicazione attaccata (si veda §6.10), 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 ridirizzare il traffico destinato ai server, ad esempio dirottandolo su un server dell'attaccante, ma anche per sferrare attacchi DoS/DDoS. Significativo, ad esempio, che in ottobre del 2016 siano rimasti bloccati per ore, a livello mondiale, vari servizi Internet quali Twitter, Spotify, eBay, Reddit, e visitatissimi giornali on line quali Financial Times e New York Times, dato che è stata bloccata da un attacco DDoS la società statunitense che gestisce i DNS per tutte le famose testate e servizi citati.
La fig. 6.6-1 mostra che il 27,22% dei rispondenti ha rilevato attacchi di reti nel 2017, contro il 44,62% nel 2016 (fig. 6-7), la % più alta tra tutte le tipologie d'attacco in quell'anno. Nel 2016 questa tipologia d'attacchi è risultata al primo posto per diffusione, nel bacino dei rispondenti, e nel 2017, per lo stesso campione, è passata al quarto posto.

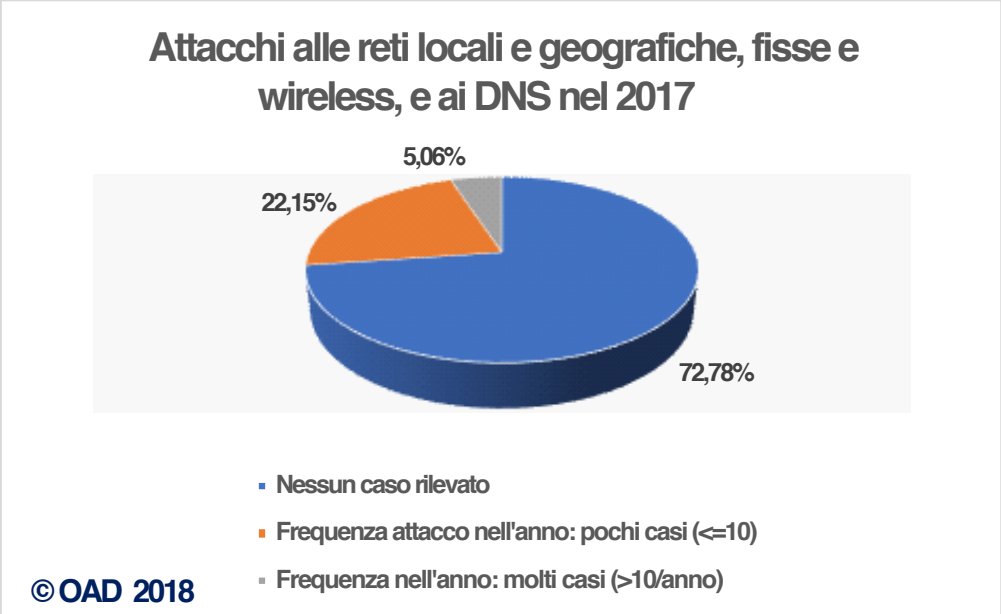

Fig. 6.6-1

La fig. 6.6-2 mostra le tecniche di attacco che i rispondenti che hanno subito questi tipi di attacco ritengono

G2 in avanti, e prevalentemente sono G3. 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.

siano state usate, con risposte multiple: ai primi due posti l'uso di script e codici maligni, e la raccolta di informazioni, entrambe ben superiori al 30%. Seguono poi, con % significativamente decrescenti, l'uso di agenti autonomi, di toolkit, di boot fino all'ultimo posto con il furto di dispositivi, ovviamente in questo caso di rete.

La fig. 6.6-3 mostra gli impatti causati dai più gravi attacchi alle reti: per più del 58% dei rispondenti non si sono avuti impatti o sono stati trascurabili; per circa il 28% l'impatto è stato l'interruzione momentanea dei servizi ICT erogati, ripristinati in breve tempo e con bassi costi.
Conseguenze più gravi con % nettamente inferiori negli altri casi. Nella voce "altro" si è specificato che si sono avuti, a seguito dell'attacco più grave, dei rallentamenti nelle reti.

La fig. 6.6-4 mostra le possibili motivazioni, almeno per i più gravi attacchi alle reti, che i rispondenti ritengono avessero gli attaccanti, con possibili risposte multiple. Con il medesimo 30,23% al primo posto tre motivazioni: poter portare altri attacchi (quindi da remoto), frodi e ritorsioni/ricatti. Segue, con la medesima percentuale 23,26%, l'azione dimostrativa e lo spionaggio, poi con il 18,60% l'hactivism, con il 13,95% sabotaggio e con il 4,65% il terrorismo.

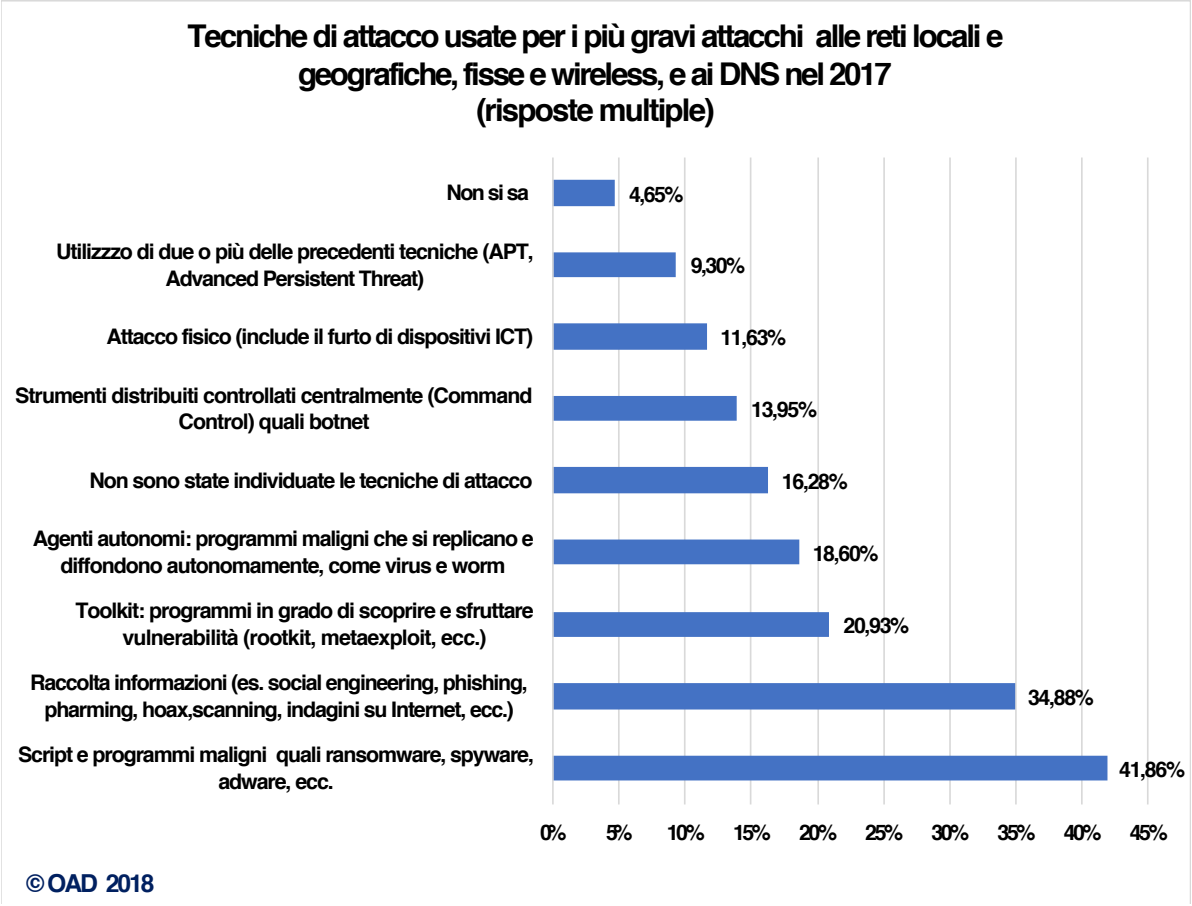

Fig. 6.6-2

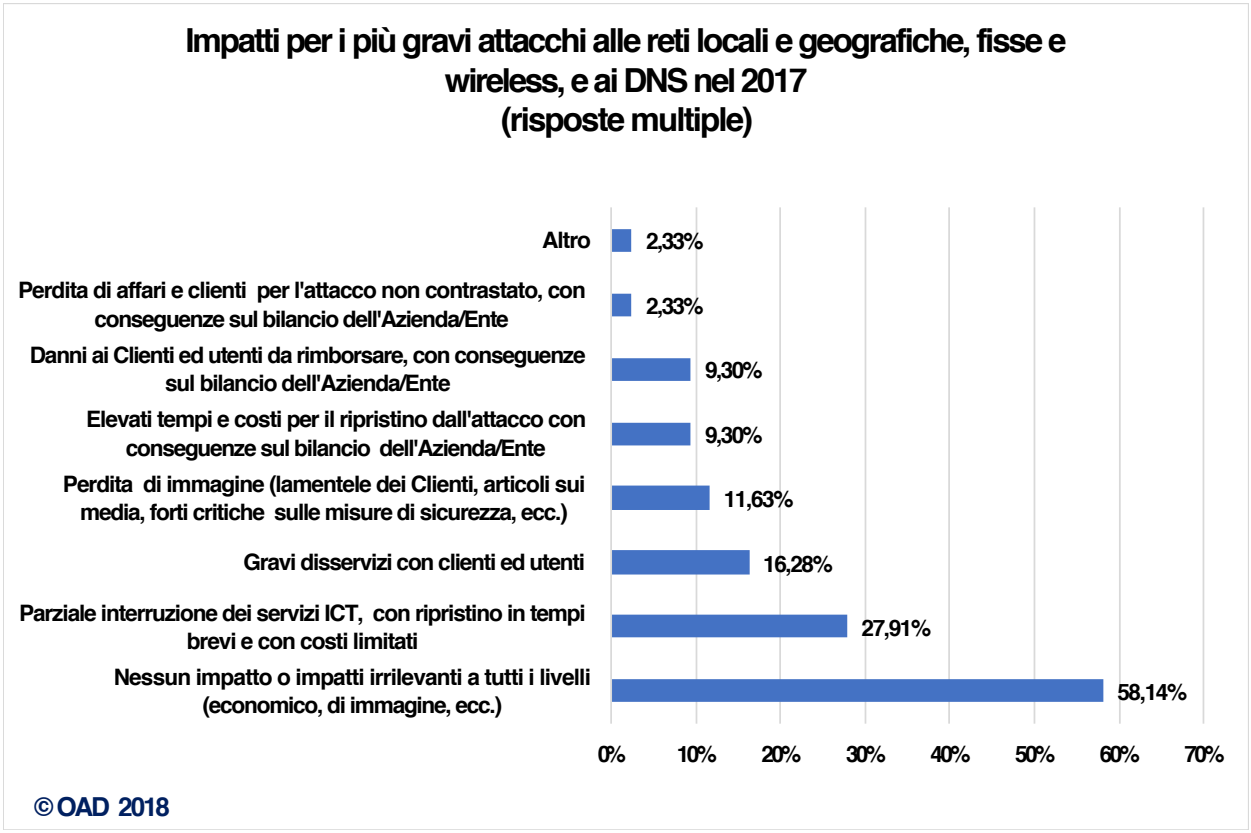

Fig. 6.6-3

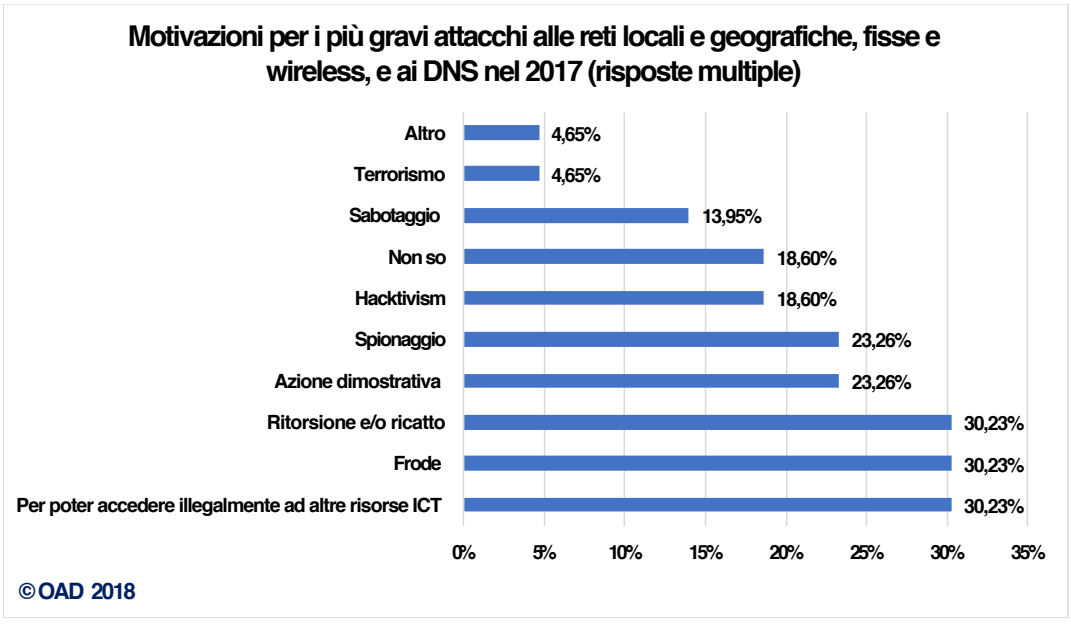

Fig. 6.6-4

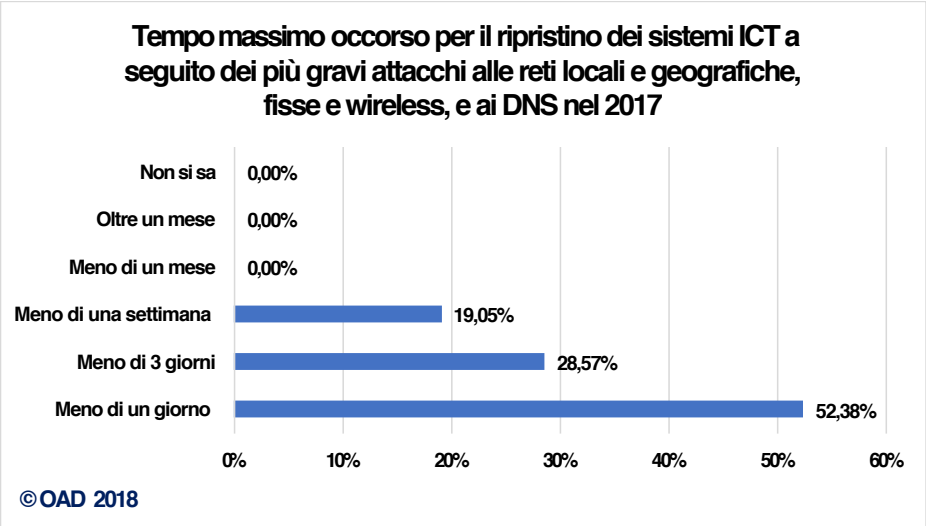

Fig. 6.6-5

I tempi massimi rilevati dai rispondenti per il ripristino, come indicato nella fig. 6.6-5, non superano la settimana, e per quasi l'81% entro tre giorni. Tali tempi così brevi sono dovuti, per le reti geografiche e per le connessioni a queste dei sistemi ICT, dall'intervento del fornitore TLC, e dai suoi strumenti di monitoraggi e controllo in grado di individuare tempestivamente problemi e disfunzioni, e di porvi rimedio in breve. Per le reti locali cablate ci sono meno attacchi, se non da utenti privilegiati interni, e per quelle wireless, se correttamente configurate e con l'uso di protocolli sicuri, gli attacchi possibili sono relativamente pochi e facilmente individuabili.

6.7 - Uso non autorizzato risorse ICT

L'uso non autorizzato, delle risorse ICT del sistema informatico dell'azienda/ente sia on premise, dai PC ai server-storage, sia a quelle in hosting/housing/cloud, per il 2017 è rappresentato nella fig. 6.7-1: poco meno del 20% dei rispondenti lo ha rilevato, rispetto al 11,79% del 2016 (fig. 6-7).
Questa tipologia di attacco avrebbe dovuto avere percentuali ben più alte, dato che è concettualmente propedeutica a tutti i tipi di accessi e modifiche non autorizzate e ai furti di informazioni dai dispositivi d'utente fissi o mobili: e quindi dovrebbe essere la prima in classifica, con percentuali attorno o superiori al 50% per entrambi gli anni. Sicuramente, invece, è stata considerata dai rispondenti come una tipologia a sé stante e non considerata come punto d'ingresso per altre tipologie d'attacco come quelle sopra menzionate.
Nei fatti, è stata quindi considerata come una tipologia d'attacco per l'accesso e l'uso non autorizzato di risorse, ma che non ha comportato furti di informazioni e/o modifiche non autorizzate. E tale interpretazione è confermata sia dalla bassa percentuale rilevata di attacchi di questo tipo, sia dai relativi impatti causati, di cui alla fig. 6.7-3.

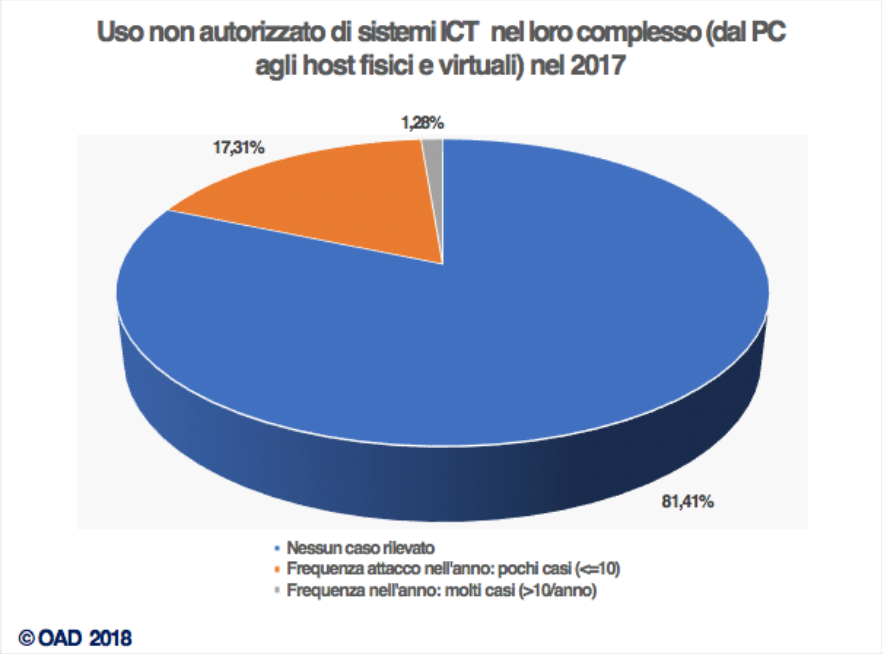

Fig. 6.7-1

La fig. 6.7-2 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 (41,38%) cui segue la cattura illecita di informazioni (24,48%), e con identiche percentuali, l'azione di agenti autonomi e attacchi tipo APT (27,59%). Toolkit e botnet seguono anch'essi alla pari con un 17,24%. Le tecniche per questa tipologia d'attacco sono quindi prevalentemente effettuate tramite strumenti informatici, anche sofisticati, il che denota un livello di competenze tecniche degli attaccanti crescente.

Gli impatti causati da questi attacchi, almeno per il bacino dei rispondenti, sono illustrati nella fig. 6.7-3. Per circa la metà dei rispondenti non si sono avuti impatti o solo impatti trascurabili; per il 27,59% si sono avuti invece gravi disservizi, come è tipico dopo un attacco ad una risorsa ICT. Per il 24,14% ci sono stati disservizi, ma di lieve entità e facilmente e velocemente. Nel complesso, la metà dei rispondenti ha avuto disservizi a seguito di questi attacchi. Tutti gli altri impatti hanno avuto % uguali o simili, anche perché, come sopra già indicato, gli impatti conseguenti ad un attacco sono multipli, e a fronte di disservizi possono esserci anche perdita di immagine, elevati costi di ripristino, danni ai clienti da rimborsare ecc.

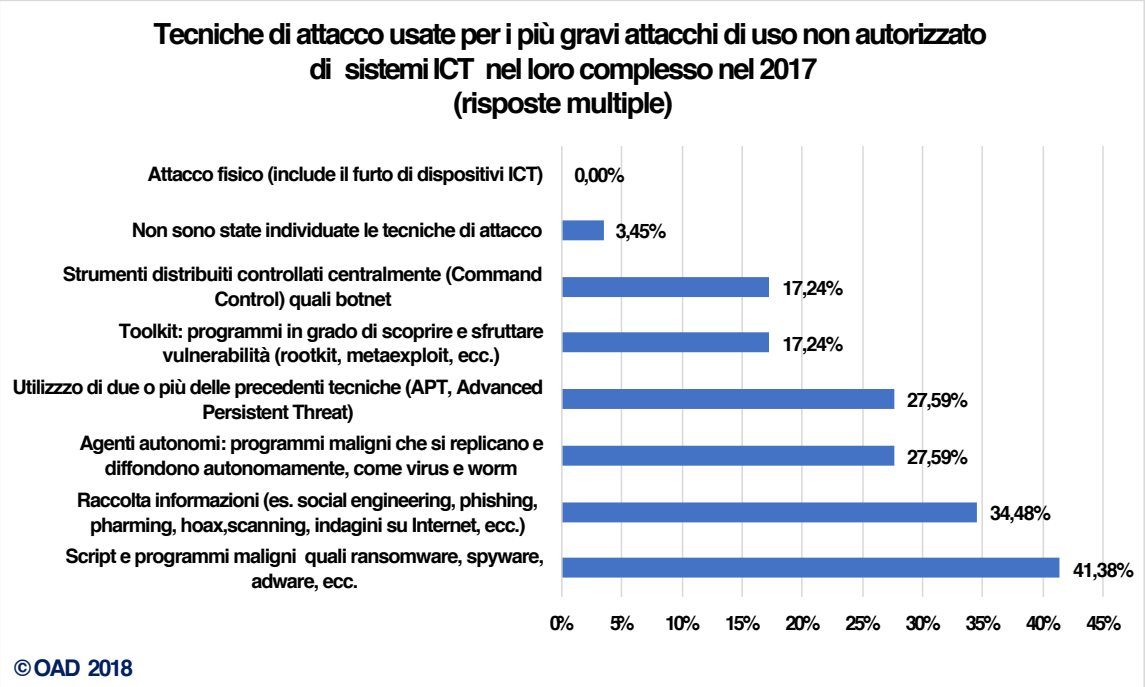

Fig. 6.7-2

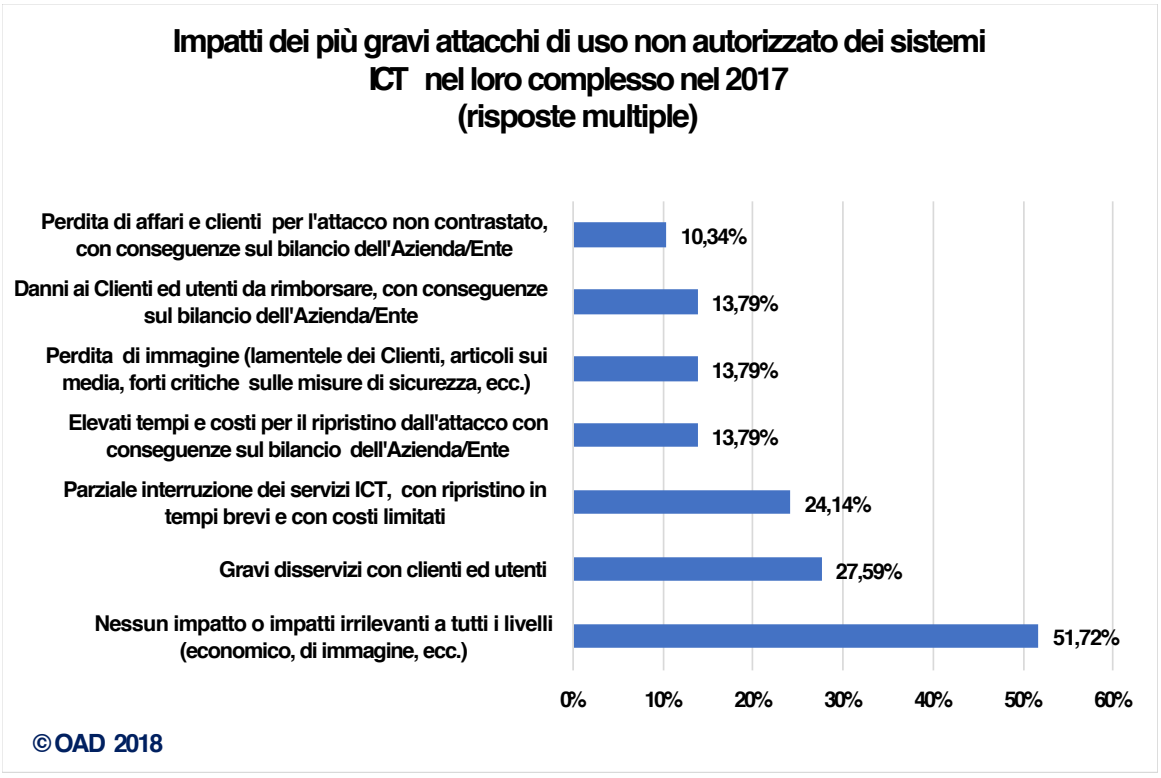

Fig. 6.7-3

La fig. 6.7-4 mostra le probabili motivazioni degli attaccanti: ai primi tre posti, come per la maggior parte delle altre tipologie di attacco, le frodi, i ricatti/estorsioni, la base per altri attacchi. Un significativo 24,14% ritiene che sia spionaggio, e data la maggioranza dei rispondenti dei settori dei servizi e manifatturiero,

tale spionaggio è prevalentemente industriale. Il 20,69% dei rispondenti non sa attribuire plausibili motivazioni, tenendo conto del loro contesto.

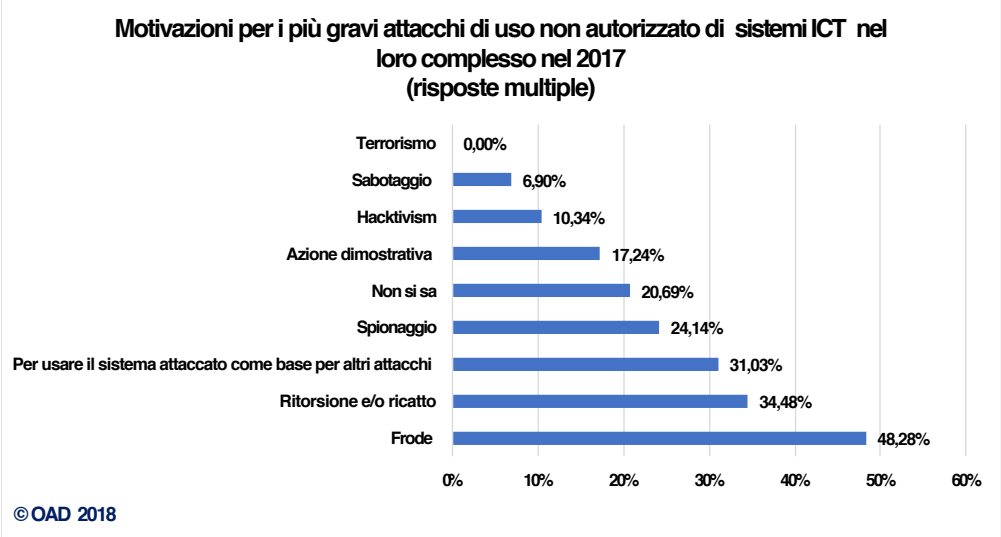

Fig. 6.7-4

I tempi massimi di ripristino dopo aver subito un attacco di questo genere, mostrati in fig. 6.7-5, sono congruenti con gli impatti di cui alla fig. 6.7.3: entro 3 giorni si è avuto il ripristino per quasi il 69% dei rispondenti, e di questi il 24,14% ha ripristinato entro un giorno. Una uguale % ha ripristinato tra il quarto ed il settimo giorno, ed il 3,45% entro il mese. In nessun caso è stato superato un mese.

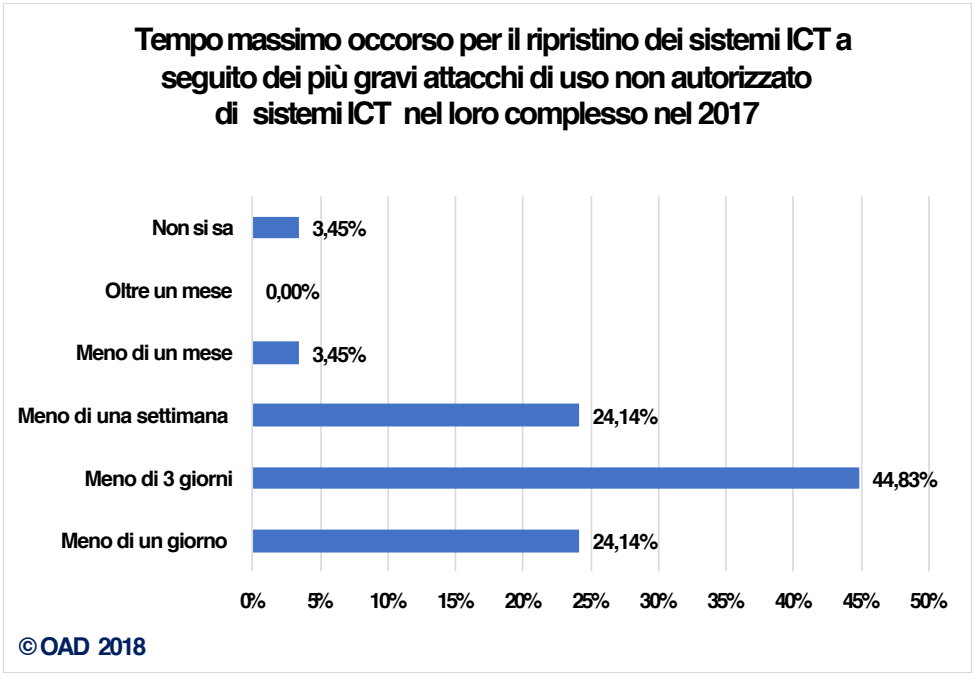

Fig. 6.7-5

6.8 - Modifiche non autorizzate ai programmi applicativi e di sistema, alle configurazioni, etc.

Attaccare i sistemi ICT modificando illecitamente le loro configurazioni, il loro software di base o addirittura il software applicativo richiede o di bypassare i controlli degli accessi, tecnicamente una operazione complessa e difficile ed in certi contesti non fattibile, o di "mascherarsi" da utente privilegiato, rubando identità digitale e diritti d'accesso di tali utenti.
La fig. 6.8.1 mostra come il 19,35% dei rispondenti ha rilevato nel 2018 questo tipo di attacchi, rispetto al 12,31% rilevato nel 2016 dallo stesso bacino di rispondenti. Come per molti altri attacchi, nel 2017 la diffusione di questa tipologia è aumentata di 7 punti, confermando come il 2017 sia stato anche per l'Italia un altro "annus horribilis", dopo il 2008 (si veda fig. 6-3), sia per diffusione degli attacchi digitali sia per crescita della loro sofisticazione e pericolosità.
La criticità riscontrata su questa tipologia di attacco è confermata dalle successive figure.

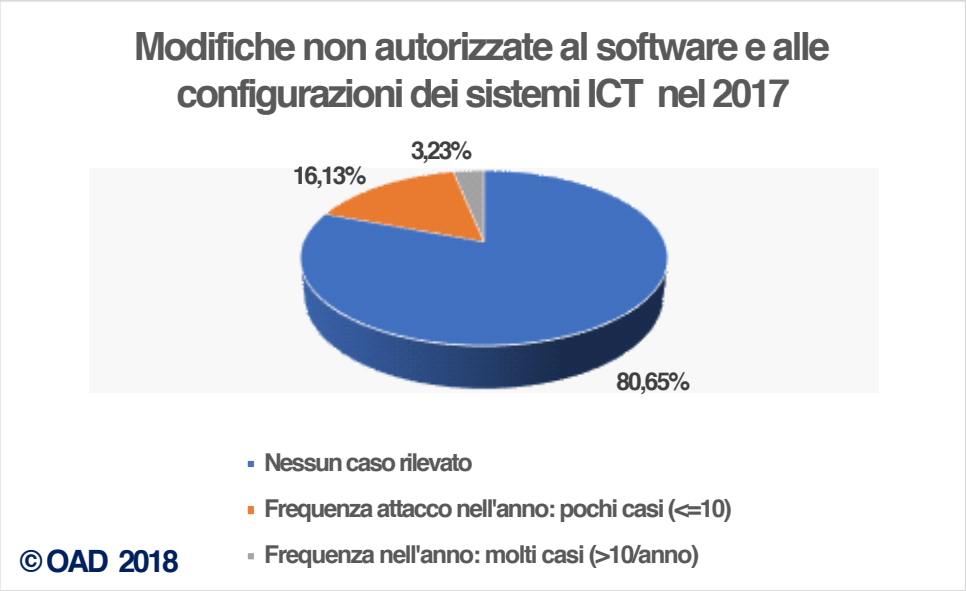

Fig. 6.8-1

Le tecniche usate per condurre questi attacchi sono elencate, con la % della stima dei rispondenti, nella fig. 6.8-2. E' bene evidenziare come ai tre primi posti, per diffusione nel campione emerso dei rispondenti che li hanno subiti, si trovano rispettivamente script e malware, con un elevato 56,67%, cui seguono gli agenti autonomi e poi i toolkit. La raccolta illegittima di informazioni si colloca solo al quarto posto. Gli attacchi subiti si sono quindi basati più su interventi tecnici sui sistemi, piuttosto che al sostituirsi all'utente privilegiato: molto probabilmente sono state tentate da remoto e senza il supporto di una "quinta colonna" all'interno della organizzazione dell'attaccato, o all'interno degli outsourcer ICT di quest'ultimo.

La fig. 6.8-3 mostra gli impatti causati da chi ha subito tali attacchi, sempre facendo riferimento ai più gravi, e con risposte multiple. Poco più del 43% non ha avuto impatti, o veramente trascurabili, ma il 50%

circa dei rispondenti ha avuto disservizi, di cui circa la metà gravi. A scendere, percentualmente, gli altri impatti, che il più delle volte si sovrappongono tra loro (risposte multiple) Non trascurabile tra questi un 10,34% di danni ai clienti da rimborsare, con conseguenze sul bilancio dell'azienda/ente.

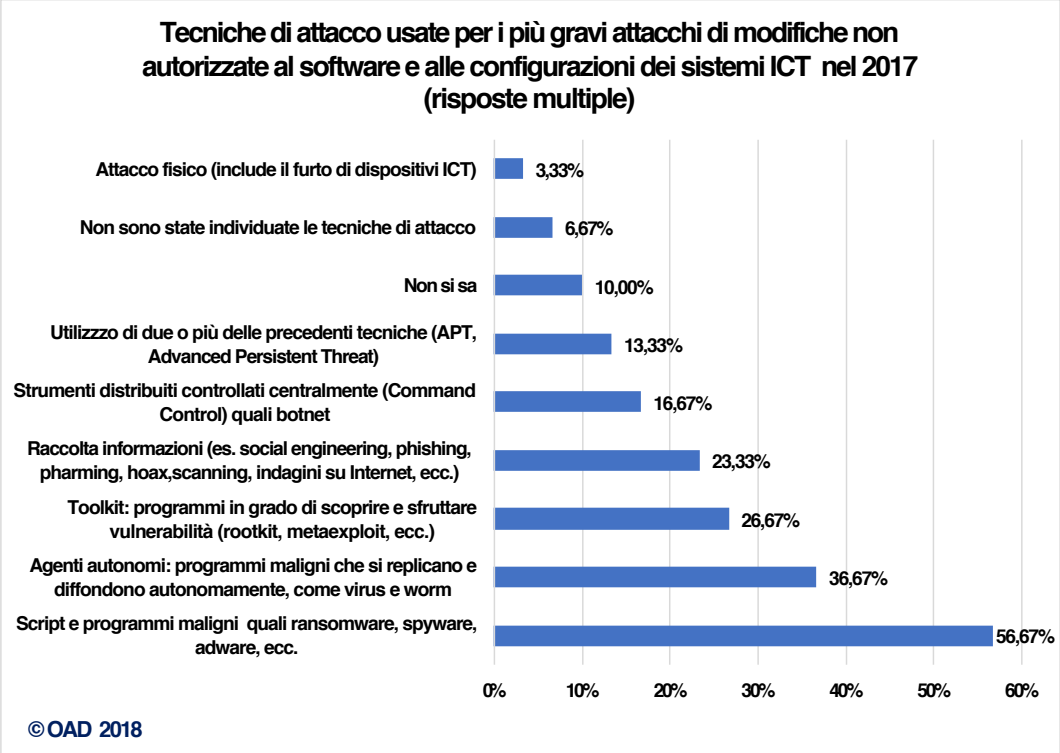

Fig. 6.8-2

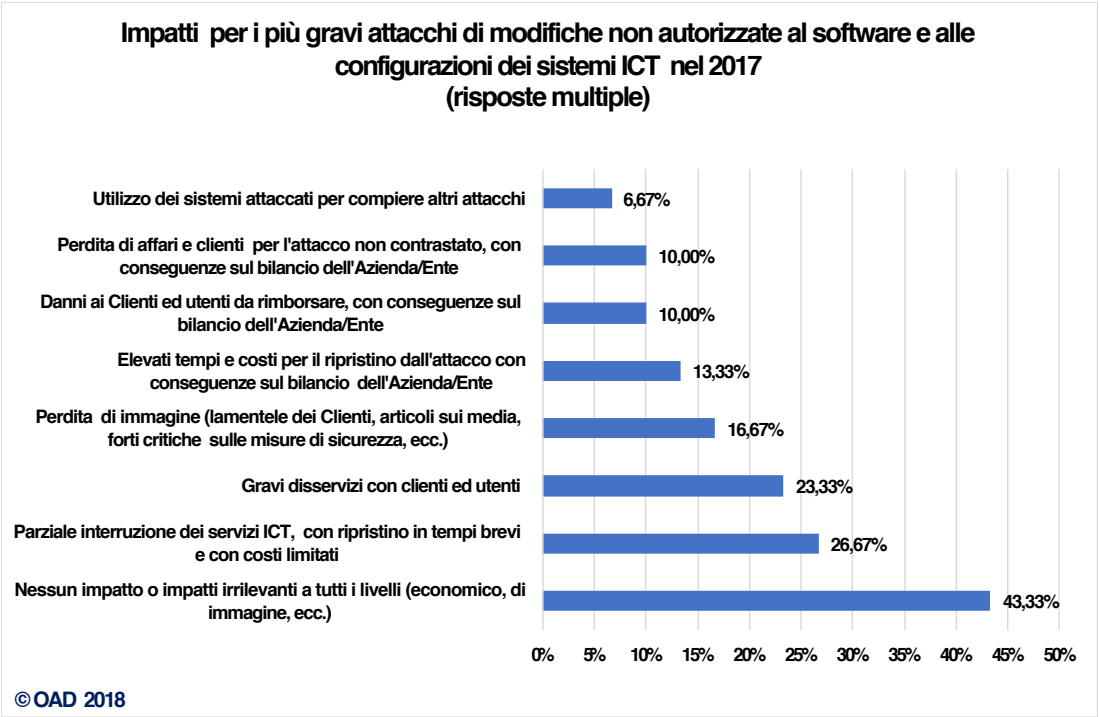

Fig. 6.8-3

Le motivazioni per tali attacchi, con risposte multiple e a giudizio dei rispondenti che li hanno subiti, sono in primo luogo la ritorsione/ricatto (31,03%) e per il 24,14 % l'uso dei sistemi ICT manipolati per sferrare altri attacchi. Segue la frode con circa il 20,69% e di poco inferiori e con identiche % lo spionaggio, prevalentemente industriale, l'azione dimostrativa e l'hacktivism (17,24%). Nella voce "altro" è stata segnalata da alcuni rispondenti l'"ignoranza".

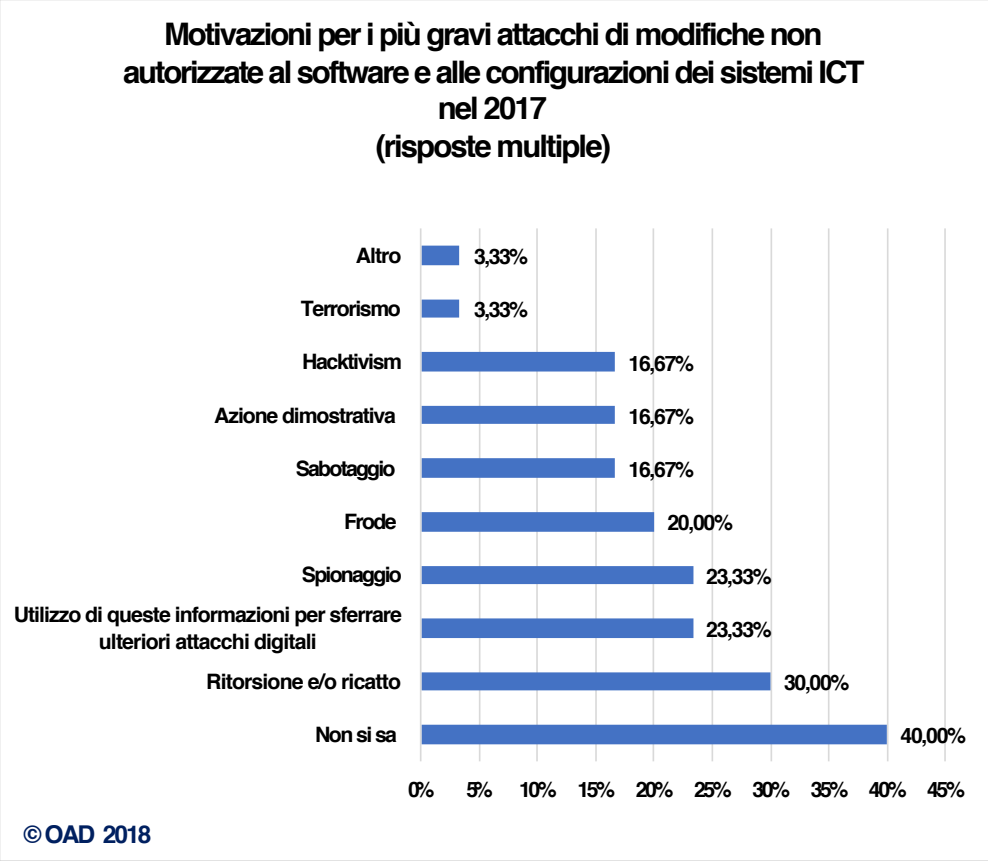

Fig. 6.8-4

Il tempo massimo di ripristino nel caso peggiore di questo tipo d'attacco, come mostrato in fig. 6.8-5, è entro 3 giorni nel 60% dei casi, e in tale percentuale il 36,67% entro il primo giorno. Ma la medesima percentuale, 36,67%, tra 3 giorni ed una settimana, ed una piccola percentuale, ma esistente, sopra il mese.

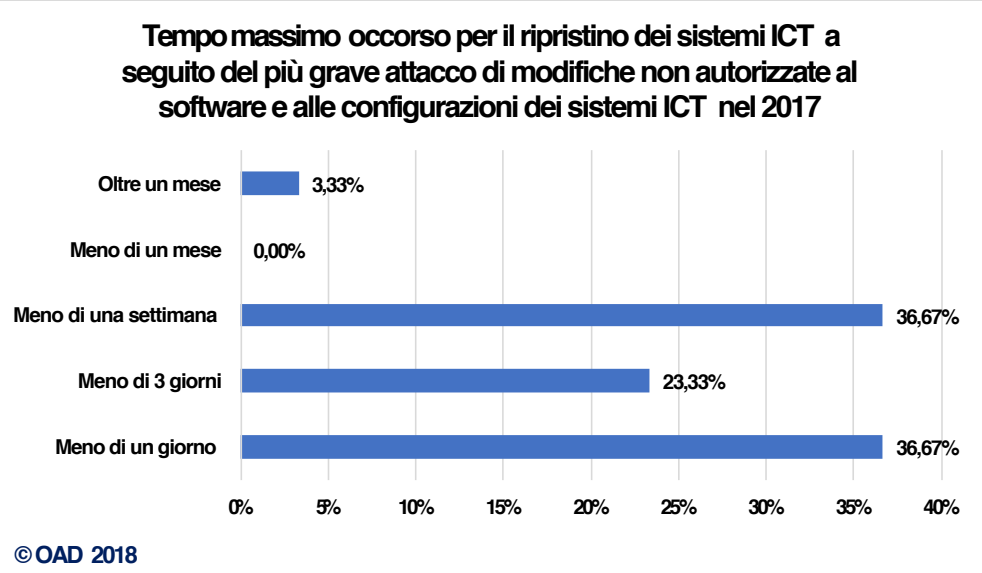

Fig. 6.8-5

6.9 - 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. D'altro canto, un attacco di questo è più facile se si ottengono dettagliate informazioni tecniche e soprattutto se si carpiscono gli account degli utenti privilegiati; ed infatti la fig. 6.9-1 mostra che il 10,9% dei rispondenti ha rilevato questo attacco, percentuale assai più elevata del 2,56% nel 2016 (fig. 6-7), nell'ambito dello stesso campione di rispondenti. Ennesima conferma del forte aumento di attacchi nel 2017 rispetto all'anno precedente.

La fig. 6.9-2 fornisce indicazioni, con risposte multiple, sulle tecniche di attacco congruenti con le considerazioni di cui sopra: con un identico 41,48% i codici maligni/script e la raccolta di informazioni; seguono, anch'esse alla pari con lo stesso 29,41%, gli agenti anonimi ed i toolkit. Con percentuali inferiori al 20% i bot e gli APT.

Fig. 6.9-1

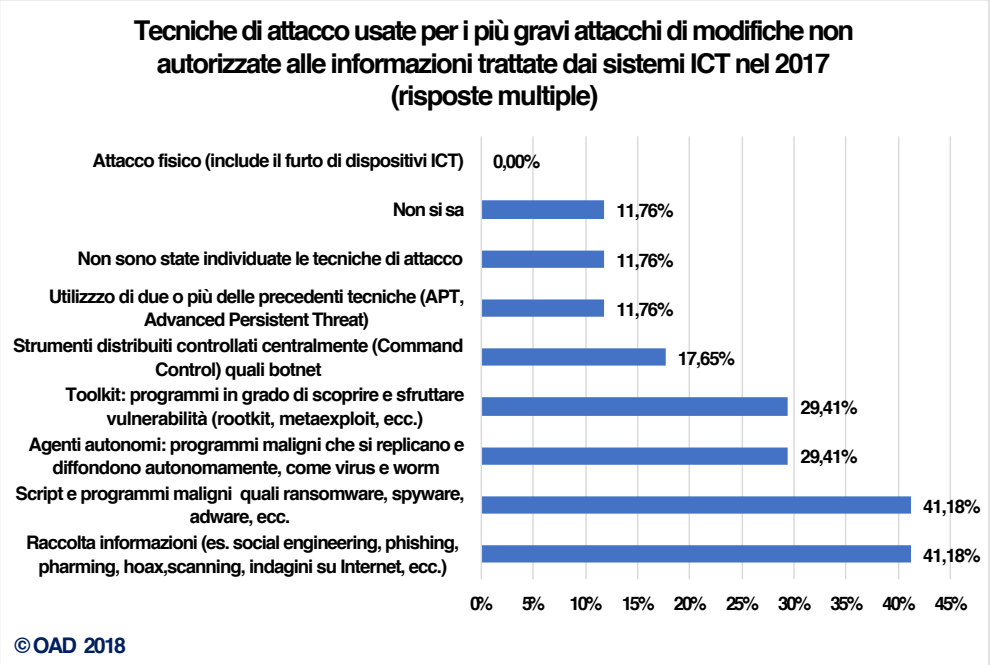

Fig. 6.9-2

La fig. 6.9-3 mostra gli impatti causati dagli attacchi di questo tipo più gravi, sempre con possibilità di risposte multiple. 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.

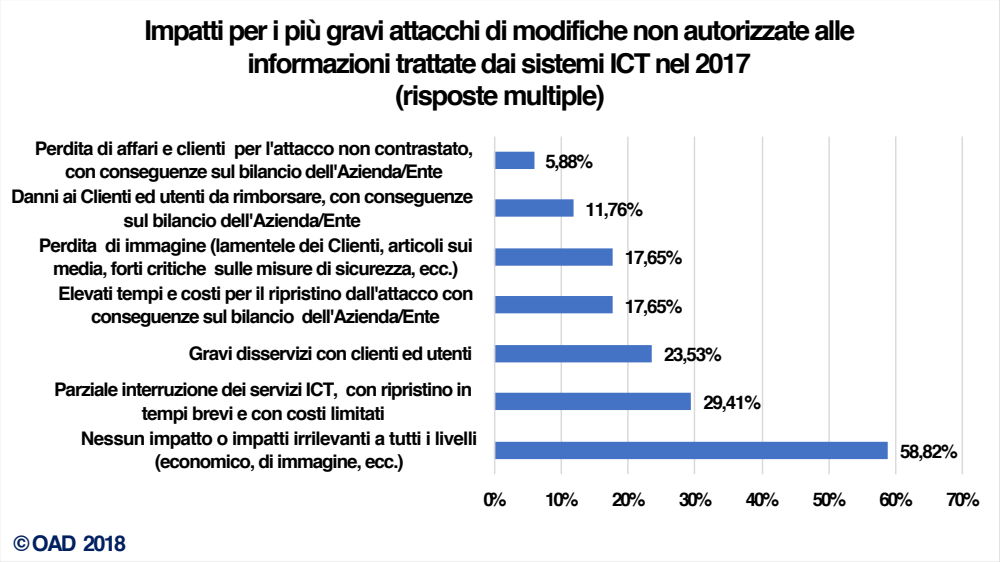

Fig. 6.9-3

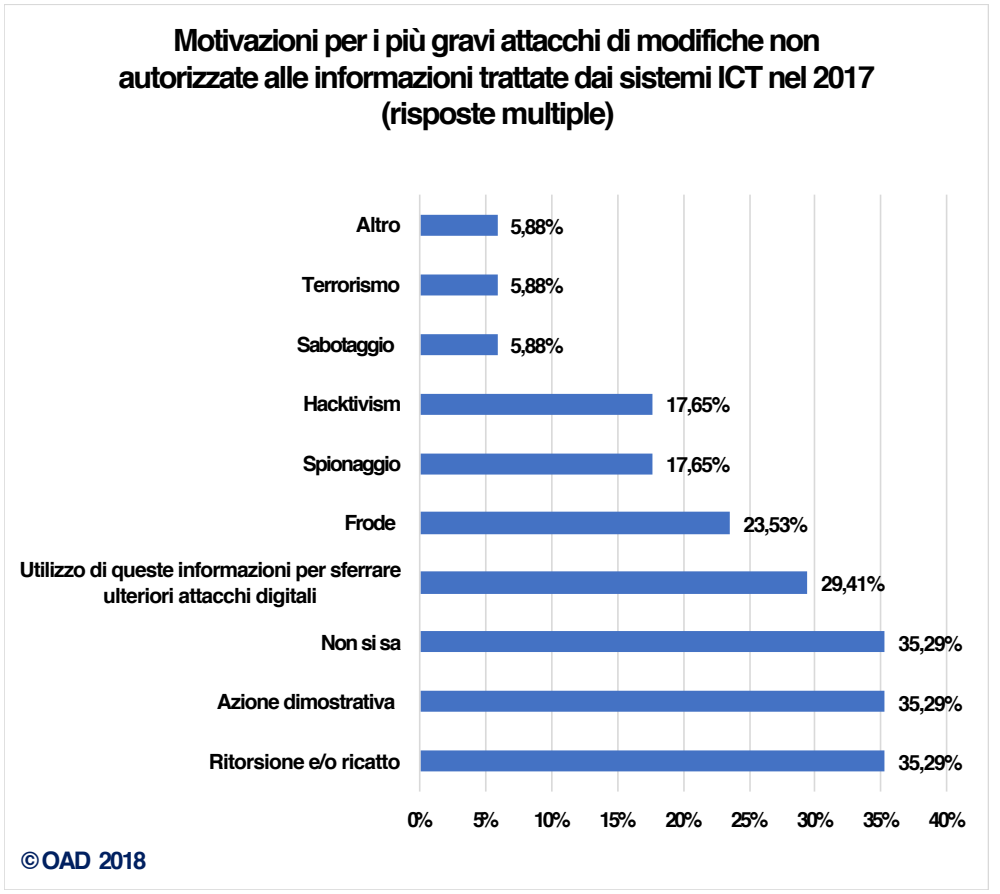

Fig. 6.9-4

La fig. 6.9-4 schematizza le possibili motivazioni per questi attacchi, con risposte multiple: al primo posto la ritorsione/ricatto insieme all'azione dimostrativa con un 35,29%, e con la stessa % i rispondenti che non sanno immaginare le motivazioni degli attaccanti. Con un valore di poco inferiore, il 29,41%, l'utilizzo delle risorse ICT alterate per sferrare altri attacchi. Hactivism e spionaggio con lo stesso 17,65%, e terrorismo e sabotaggio con un 5,88%.
Lascia perplessi una percentuale così alta per l'azione dimostrativa e così bassa per il sabotaggio, per questo tipo di attacco sovente complesso da effettuare.
Con "altro" è indicato risposte soprattutto "ignoranza".
La gravità di questo attacco è in qualche modo ribadita da tempi di ripristino nei casi di attacchi più gravi, come mostrato in fig. 6.9-5: poco meno della metà dei rispondenti riesce a ripristinare entro 3 giorni, per l'altra metà occorrono tra 3 e 7 giorni. Nessuno dei rispondenti ha impiegato da una settimana ad un mese o oltre. Rispetto alle altre tipologie di attacco, la maggior parte dei casi ha richiesto tra i tre ed i sette giorni.

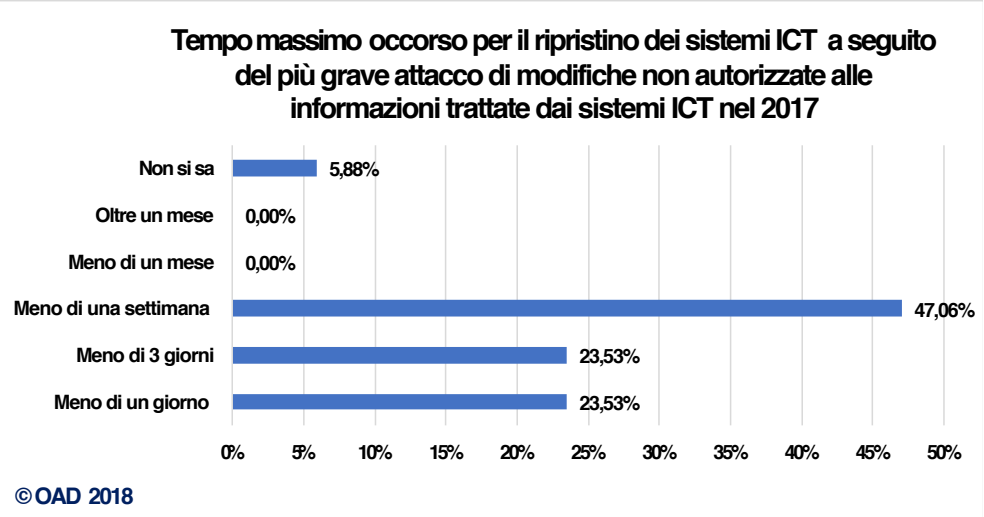

Fig. 6.9-5

6.10 - Saturazione risorse digitali (DoS, DDoS)

La saturazione delle risorse ICT, indicata sovente in Italia con l'acronimo DoS/DDoS, Denial of Service/ Distributed DoS, è un tipo di attacco che nel 2017 ha avuto una forte crescita, come indicato nella fig. 6.10-1: quasi il 30% dei rispondenti ha subito un attacco di questo tipo, contro il 9,23% nel 2016 (fig. 6-7); il numero di attacchi, per l'omogeneo campione di rispondenti, è praticamente più che triplicato.

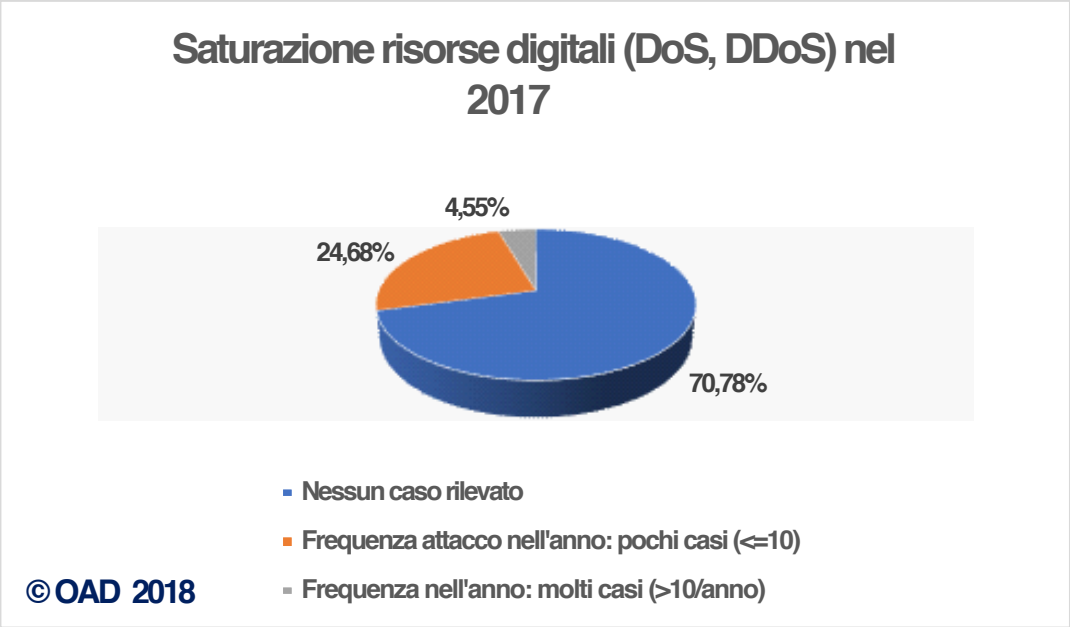

Fig. 6.10-1

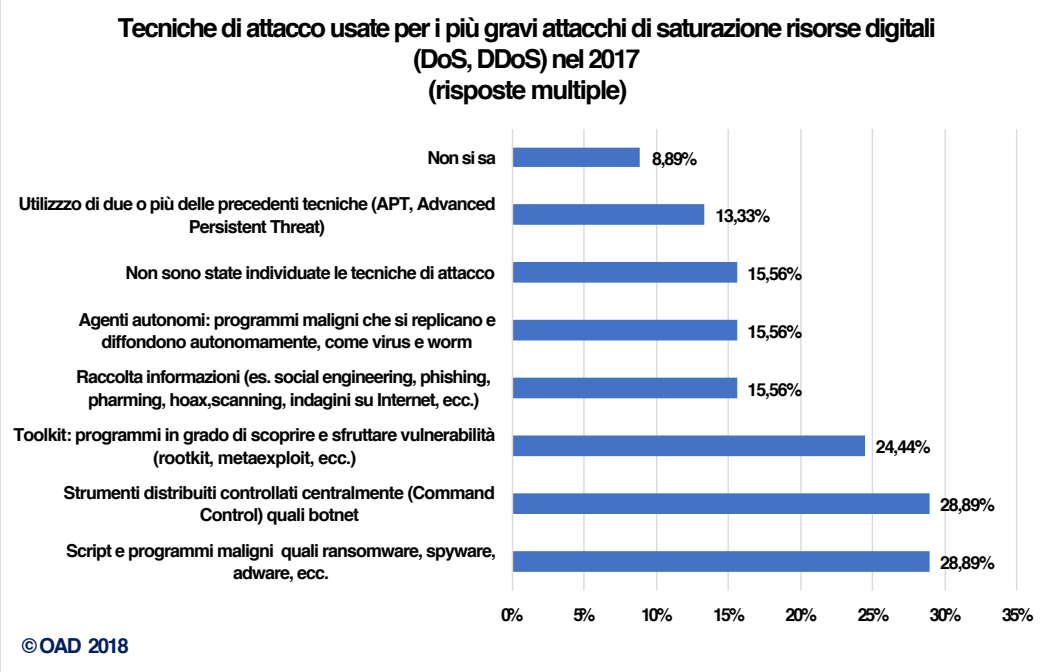

Fig. 6.10-2

Le tecniche usate per portare tali attacchi sono schematizzate, con risposte multiple, nella fig. 60.10-2. Al primo posto con lo stesso 28,89% botnet, che è la modalità più usata per DDoS, e script e codici maligni, dato che gli agent distribuiti sono codici maligni. Seguono i tool con un 24,44%, e con il medesimo 15,56% la raccolta di informazioni e l'uso di agenti autonomi, questi ultimi usati per diffondere in maniera virale sui vari host inconsapevoli il codice maligno dell'agent per sferrare, sotto il comando di un CC nascosto e sovente anonimizzato.
Le implicazioni causate da un DoS/DDoS ai sistemi informatici dei rispondenti che l'hanno subito, e nella maniera più grave, sono in fig. 6.10-3. Come è quasi ovvio per questa tipologia di attacco, più della metà degli attaccati ha avuto disservizi, e di questi il 17,78% gravi. Ma il 53,33% non ha subito alcun reale impatto, o in misura non significativa, il che significa, con molta probabilità, che le loro reti erano protette da attacchi di questo genere, grazie ad accordi coi fornitori di TLC e networking. Oltre alla perdita di immagine (11,11%), seguono tre impatti con lo stesso 8,89%: quasi sicuramente una parte di chi ha avuto gravi disservizi, ha poi subito elevati costi di ripristino, rimborsi dei danni ai clienti, perdita di affari e di clienti.

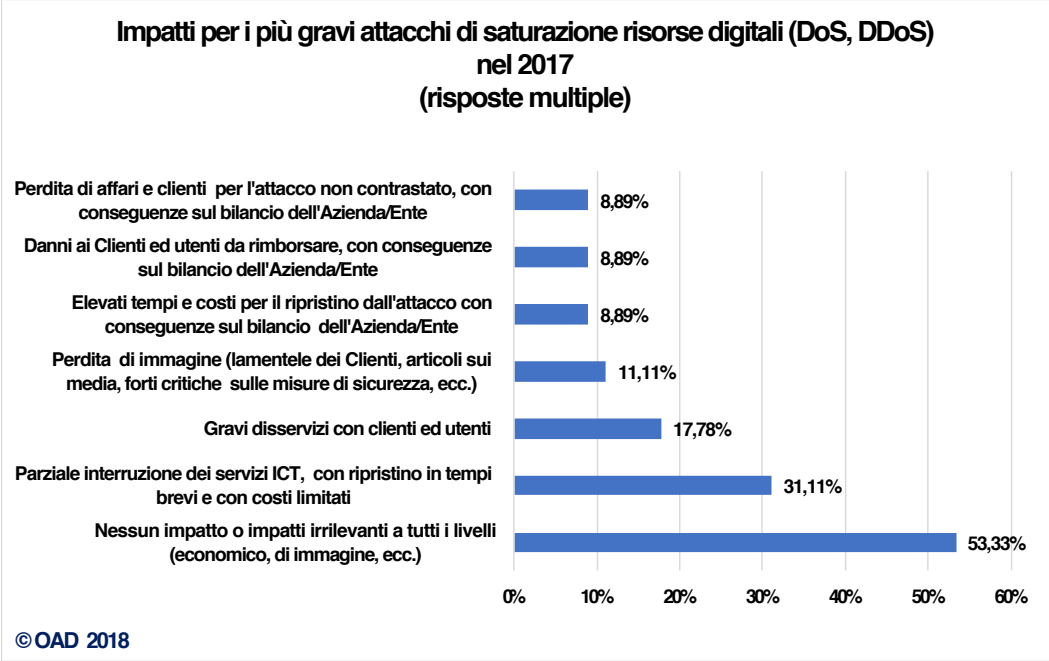

Fig. 6.10-3

La fig. 6.10-4 mostra le motivazioni che, a giudizio dei rispondenti, hanno motivato gli attaccanti. Le risposte sono multiple e quasi 1/3 dei rispondenti ritiene che siano dovute a sabotaggio, che sicuramente è una delle prime motivazioni per un DoS/DDoS. Si sarebbe aspettato con un'alta percentuale la motivazione di ricatto/ritorsione, che invece risulta penultima, con un 15,56%.
Ottengono una % più alta l'azione dimostrativa e l'hactivism, oltre allo spionaggio.
Da sottolineare l'elevato 33,33% 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 53,33% degli attaccati che non ha subito impatti (fig.6.10-3), è confermato dai tempi di ripristino, sempre per gli attacchi più gravi, indicati dalla fig. 3.10-4: ben il 68,89% è stato in grado di ripristinare in un solo giorno, e tra 1 e 3 giorni il 17,78%. Tra 3 e 7 giorni quasi il 9%, e tra una settimana ed un mese il

2,22%. Questi ultimi non avevano sicuramente predisposto le opportune misure coi loro fornitori di reti, e le conseguenze sono anche i tempi indicati. Per la maggior parte delle aziende/enti di medie grandi dimensioni, un blocco di più di 3 giorni può essere letale.

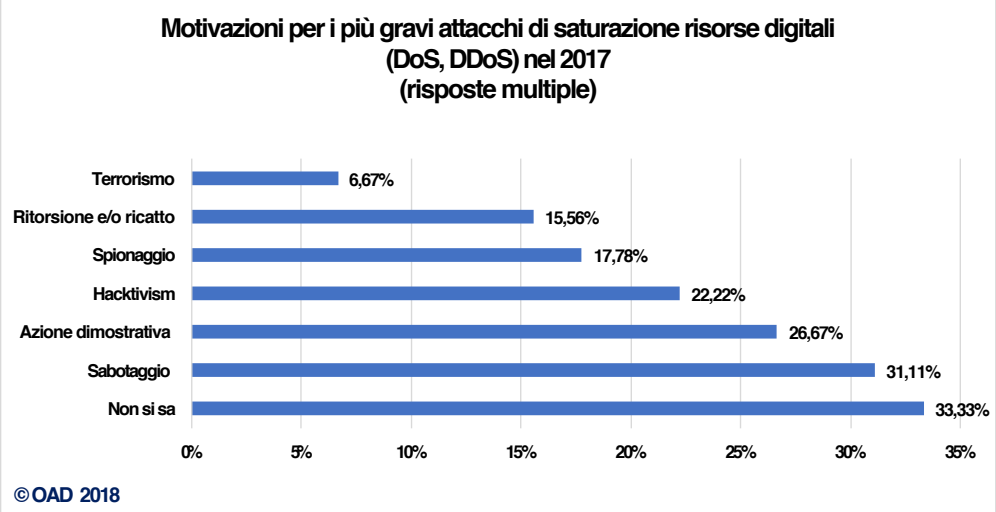

Fig. 6.10-4

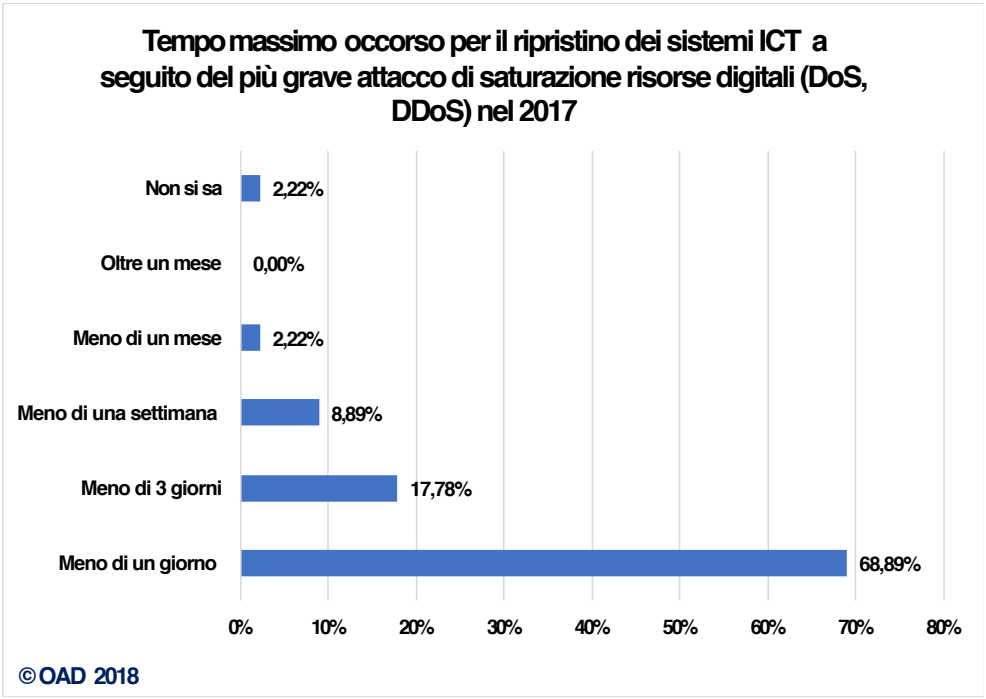

Fig. 6.10-5

6.11 - Attacchi ai propri sistemi in cloud o in housing/ hosting presso fornitori

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, diviene un attacco al sistema informatico o alla sua parte terziarizzata dell'azienda/ente cliente. Gli outsourcer sono medie e grandi imprese, anche a livello internazionale, conosciuti sul mercato e per questo 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.
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 2018 di OAD.

La fig. 6.11-1 indica che hanno rilevato attacchi digitali sui loro sistemi in outsourcing il 29,22% dei rispondenti, rispetto al 9,23% del 2016 (fig. 6-7). Gli attacchi ai sistemi terziarizzati sono quindi aumentati tra 2016 e 2017 di circa il 20%, nell'ambito dello stesso campione di rispondenti: ennesima conferma del forte incremento, anche in Italia, degli attacchi digitali nel 2017.

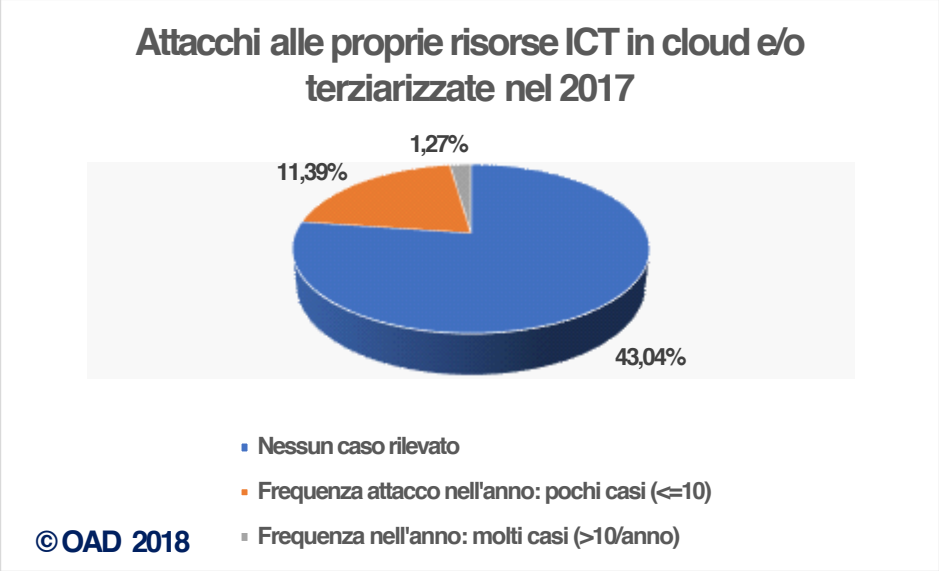

Fig. 6.11-1

Come già considerato in precedenza, la terziarizzazione di sistemi e servizi ICT è in crescita anche in Italia, e gli outsourcer dispongono, nella maggior parte dei casi, di potenti misure tecniche e organizzative di prevenzione e di contrasto agli attacchi digitali, pur offrendo diversi e differenti livelli di sicurezza digitale, a seconda del contratto: chi più paga più ha protezione. Ma d'altro canto gli outsourcer ICT sono un target per attaccanti preparati e con grandi risorse, anche economiche: colpendo e perforando una sola azien-

da possono accedere ad almeno una parte dei clienti di questa, clienti che a loro volto possono essere significativi per l'attaccante.

La fig. 6.11-2 mostra le tecniche probabilmente usate: script e codici maligni hanno la % più alta (40%), cui seguono con % decrescenti gli agenti autonomi e le altre tecniche considerate. Comprensibile ma alta la percentuale dei rispondenti che non sanno quali tecniche sono state usate, dato che il cliente di un outsourcer non è solitamente informato sui dettagli tecnici di una azione così critica e delicata come un attacco digitale che si ripercuote sul cliente stesso. D'altro canto, il rispondente, soprattutto di grandi aziende/enti, può non essere a conoscenza, perché non informato al suo livello, di attacchi di questo genere e di questa importanza.

La fig. 6.11-3 indica gli impatti derivati al cliente rispondente: la metà afferma che non ha avuto impatti, e questa risposta è ragionevole dato che l'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 quasi la metà dei rispondenti (fig. 6.11-5)

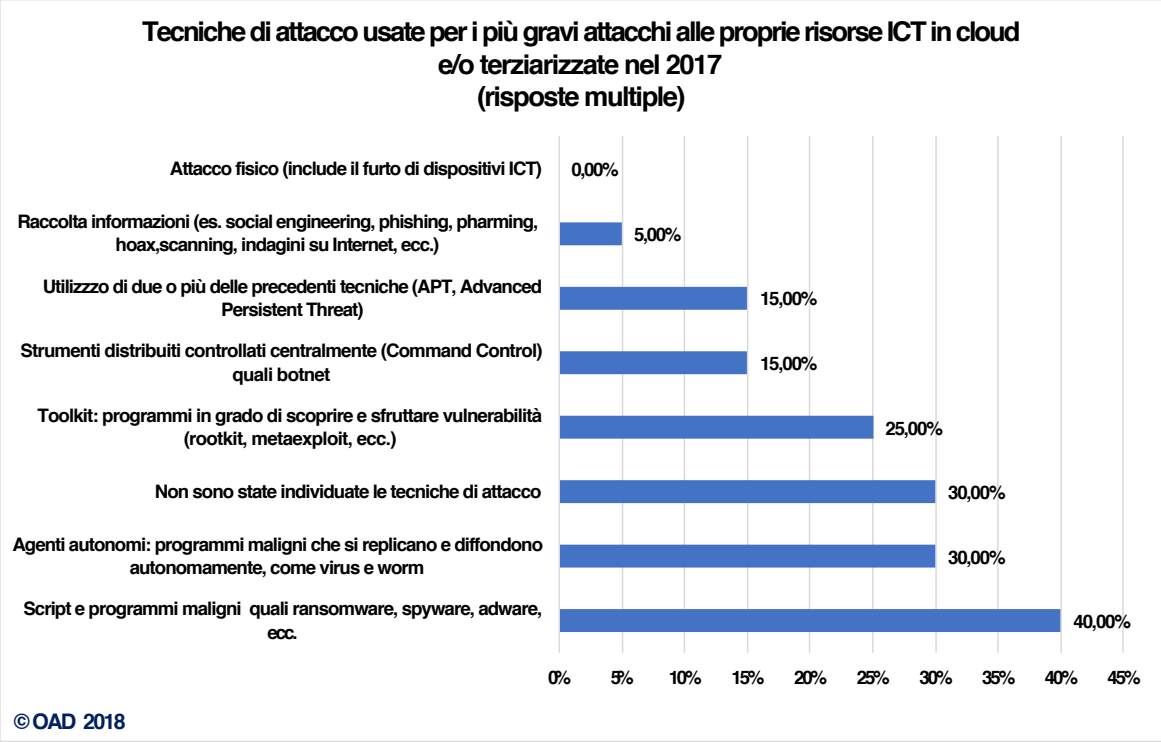

Fig. 6.11-2

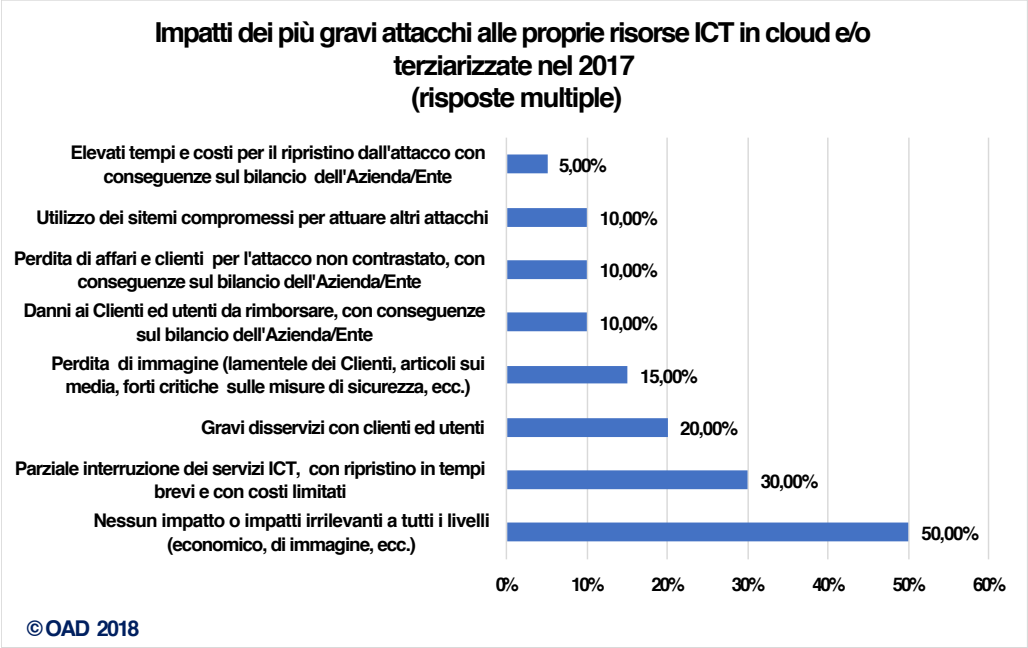

Fig. 6.11-3

Le possibili motivazioni per l'attacco più grave (fig. 6.11-4) non sono note o stimabili dalla metà dei rispondenti. Stranamente la quota più alta, 25%, ipotizza una azione dimostrativa e con lo stesso 15% motivazioni più credibili quali la frode, l'hactivism, ecc. Con percentuali ancora minori ritorsione/ricatto e sabotaggio. Circa il 5% indica anche il terrorismo: percentuale piccola ma esistente, probabilmente indicata da aziende/enti di grandissime dimensioni e ben note, come immagine, sul mercato nazionale e mondiale.

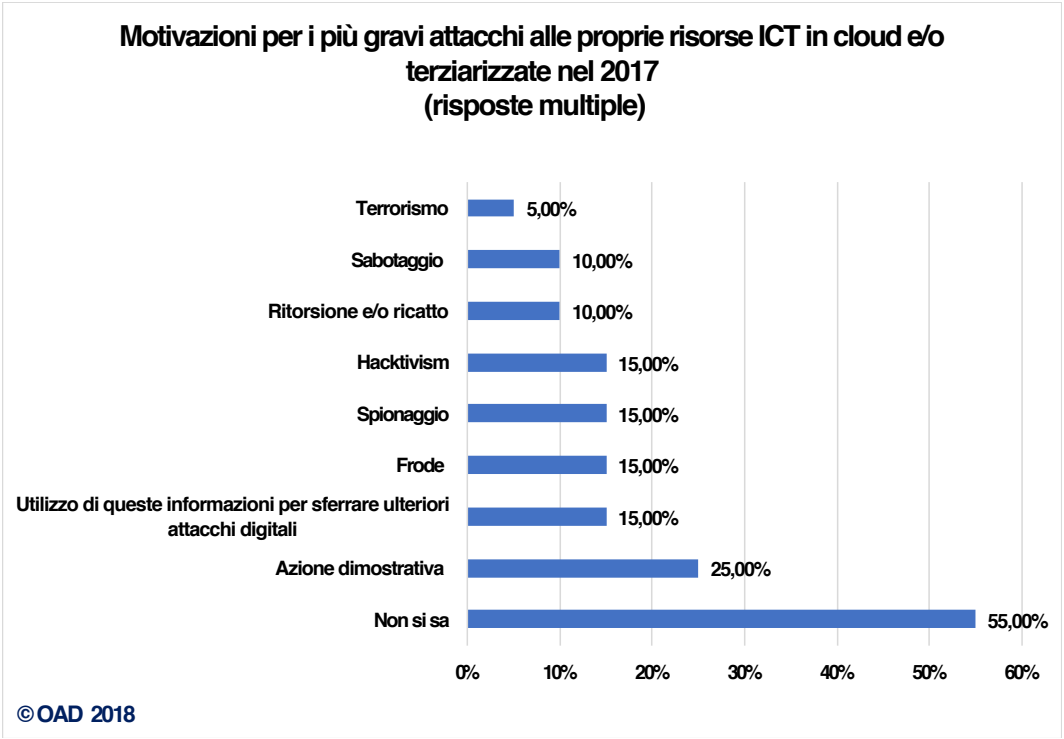

Fig. 6.11-4

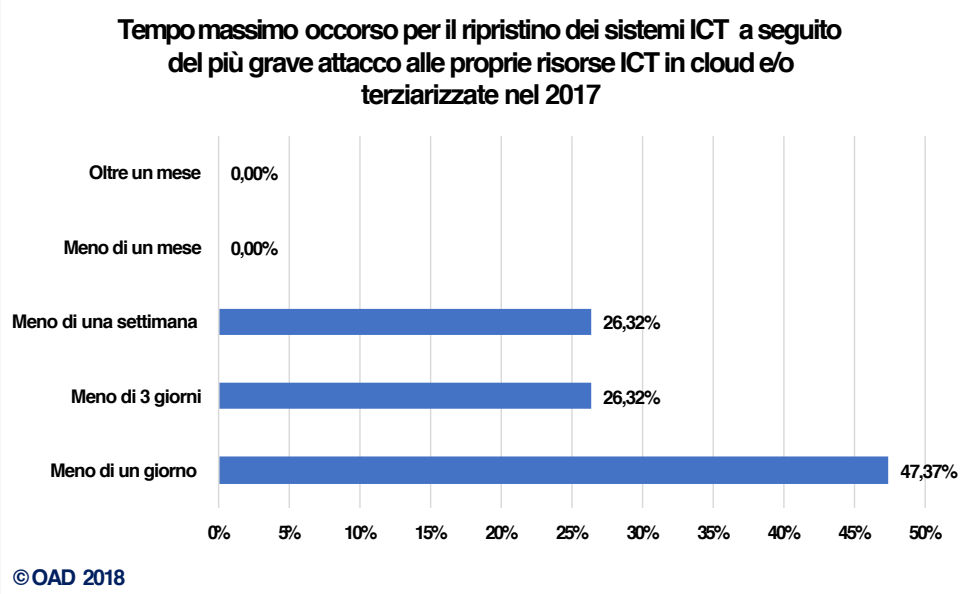

Fig. 6.11-5

Come indicato in fig. 6.11-5, quasi ¾ dei rispondenti che hanno subito questo tipo di attacco hanno avuto un ripristino entro 3 giorni, e di questi ben il 47,37% entro un solo giorno: tempi significativi della efficacia degli outsourcer, confermati dal che in ogni situazione il ripristino sia comunque avvenuto entro una settimana al massimo.

6.12 - Attacchi a dispositivi IoT (Internet of Things) in uso

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 fatto esplodere 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[10] o codici QR[11], 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

10 - Tag RFID

11 - 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.

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.
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 già citato Global Risk Report 2018 del World Economic Forum stima nel 2017 a livello mondiale la presenza di 8,4 Miliardi di dispositivi IoT, a fronte di 7,6 Miliardi di abitanti della terra, e prevede che gli IoT nel 2020, saranno 20,4 Miliardi, quindi quasi triplicati in tre anni con questi ordini di grandezza!
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 2018 inclusa.
La fig. 6.12-1 mostra che il 31,82% dei rispondenti usa dei dispositivi IoT e di questi solo il 2,6% del totale ha rilevato attacchi su di loro. Analizzando e correlando le risposte al questionario OAD 2018, risulta che le aziende che hanno subiti attacchi IoT appartengono ai settori merceologici Trasporti e magazzinaggio (Codici Ateco H), Commercio all'ingrosso e al dettaglio, incluso quello di apparati ICT (Codici Ateco G), Sanità e assistenza sociale: ospedali pubblici o privati, studi medici, laboratori di analisi, ecc. (Codici Ateco Q). Il 2,6% del 2017 è inferiore al valore di 4,62% nel 2016 (fig. 6-7). Questa è una delle poche tipologie di attacchi che hanno subito una riduzione della diffusione di attacchi nel 2017 rispetto al 2016. Questo decremento probabilmente è dovuto al miglioramento delle misure di sicurezza che le aziende/enti dei rispondenti hanno attuato sui sistemi IoT che fin dalla loro nascita e diffusione sono diventati un obiettivo, inizialmente abbastanza facile, di attacchi.

Le tecniche di attacco probabilmente usate per i pur pochi attacchi rilevati dal campione 2018 sono mostrate in fig. 6.12-2. Si invitano i lettori del presente rapporto a considerare come puramente indicative le % in figura, dato che fanno riferimento a troppi pochi casi, seppur reali, subiti dai rispondenti. La % maggiore riguarda l'uso di toolkit, con un 75%. Seguono con la stessa percentuale del 50% tutte le altre tecniche, a parte gli attacchi fisici e la raccolta di informazioni, che non sono state considerate tecniche di attacco usate nei casi rilevati.

L'impatto maggiore causato dagli attacchi più gravi per i rispondenti che li hanno subiti è la perdita di immagine, con un 75%, come mostrato in fig. 6.12-3. Seguono con lo stesso 50% disservizi più o meno gravi e i danni ai clienti da rimborsare. Con il 25 % sono considerati sia nessun impatto rilevante sia la perdita di affari e clienti.

La fig. 6.12-4 mostra le probabili motivazioni degli attaccanti per gli attacchi più gravi: stranamente l'azione dimostrativa, con il 75%, risulta la più diffusa, e la frode non è considerata. Con lo stesso 50% sono invece considerate tutte le altre motivazioni, a parte, e ragionevolmente, l'uso degli IoT attaccati per portare altri attacchi digitali.

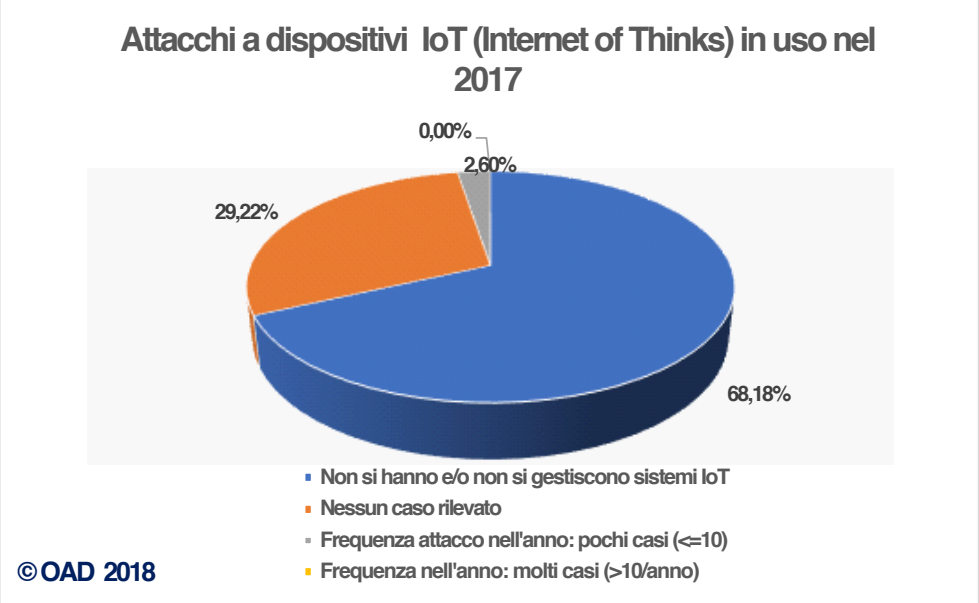

Fig. 6.12-1

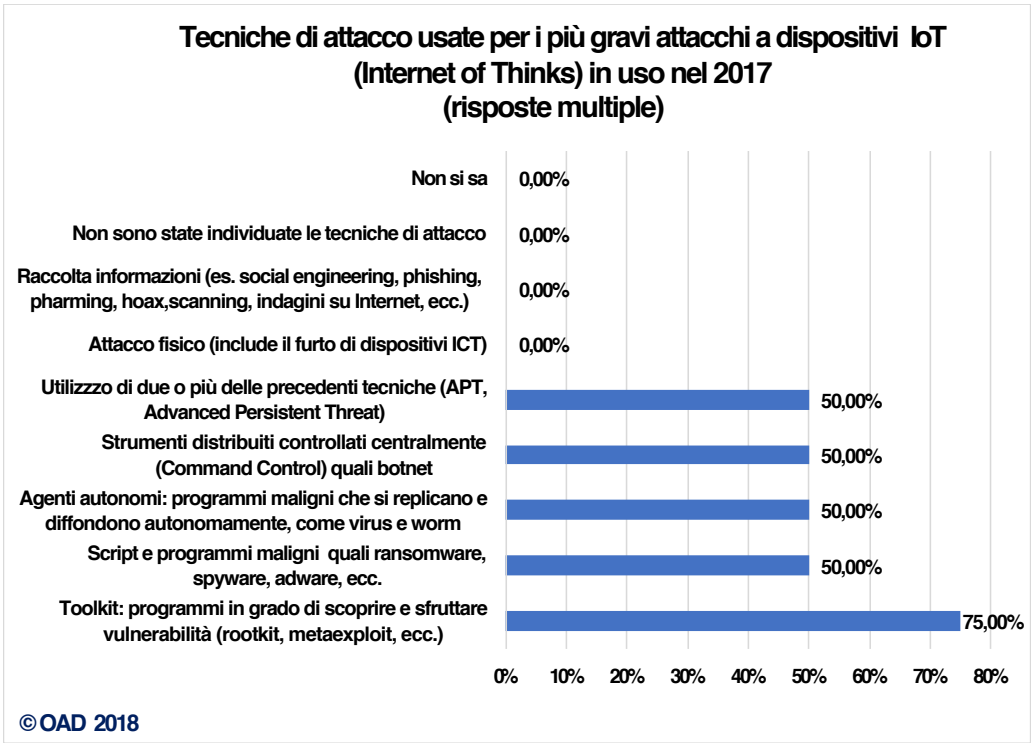

Fig. 6.12-2

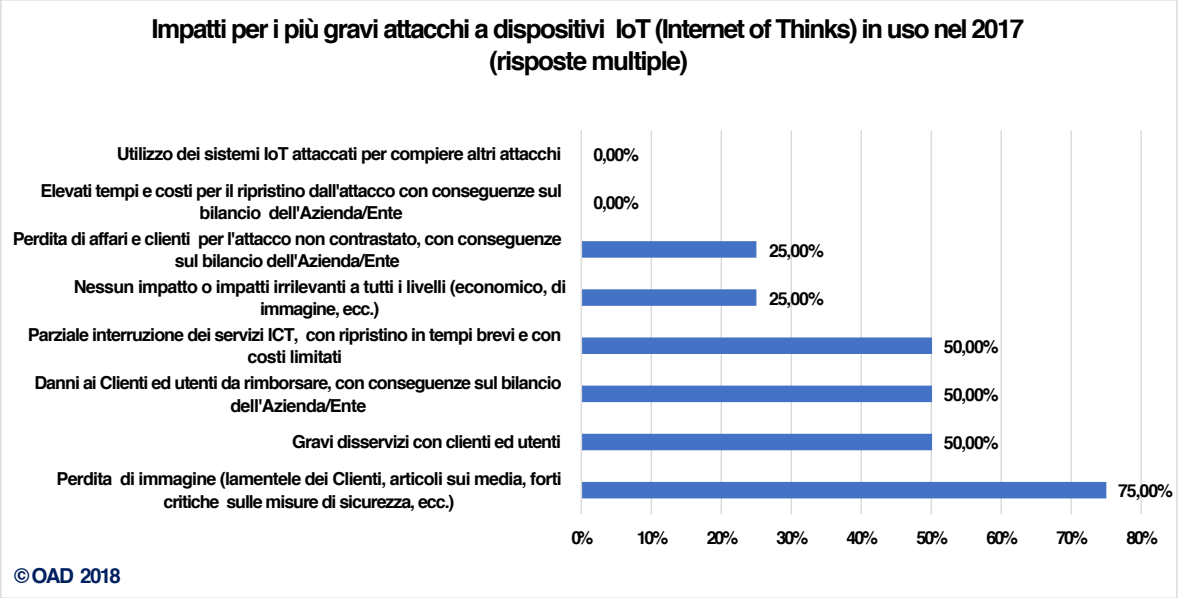

Fig. 6.12-3

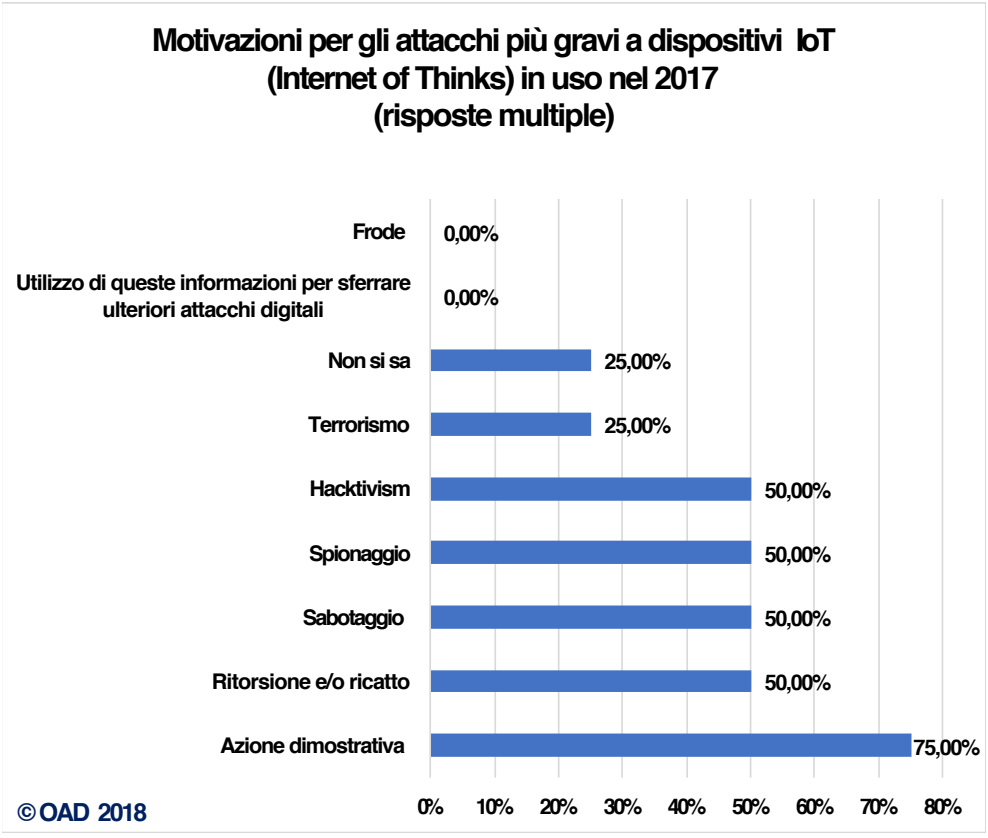

Fig. 6.12-4

La fig.6.12-5 mostra i tempi massimi per il ripristino dopo gli attacchi più gravi rilevati. Interessante evidenziare che in nessun caso il ripristino è potuto avvenire in un giorno o ha richiesto più di un mese: per il 75% dei casi più gravi il ripristino è avvenuto entro una settimana, ed il 25% tra una settimana ed un mese. I tempi indicati sono ragionevoli, tenendo conto che da un lato i dispositivi IoT non sempre sono monitorati e controllati centralmente in maniera continua, dall'altro che alcuni dispositivi sono dislocati in punti non facilmente raggiungibili dalle persone che devono manutenerli.

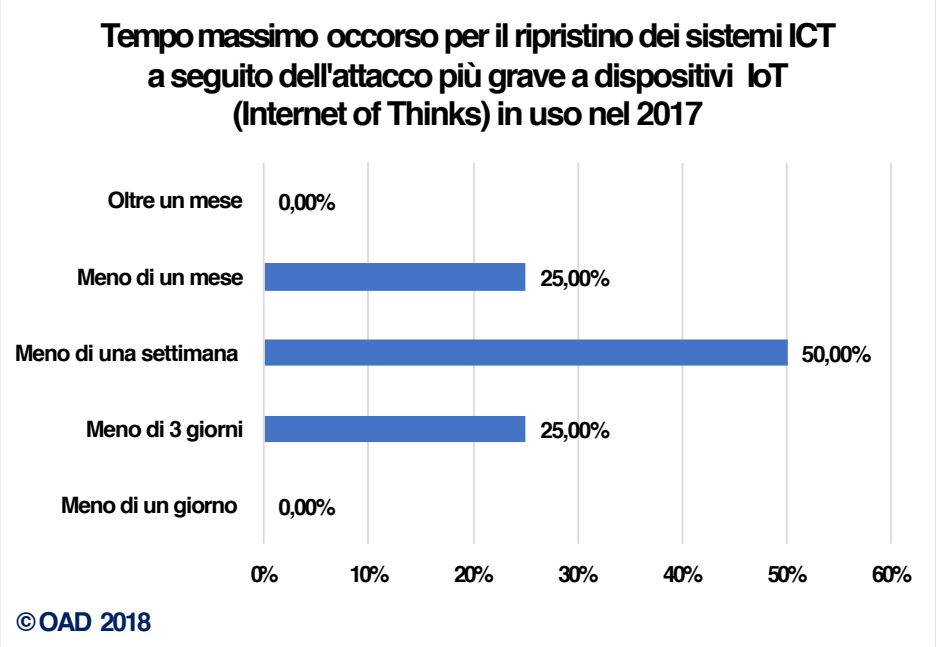

Fig. 6.12.5

6.13 - 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.
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.
La distinzione tra IoT, sistemi di automazione della produzione e sistemi di robotica è sempre più confusa e si differenziano gli apparati, ormai tutti smart e capacci di comunicare, per le loro funzionalità ed i loro utilizzi.

La fig. 6.13-1 mostra che il 26,92% dei rispondenti utilizzano sistemi di automazione/robotica, ma solo il 2,56% ha subito attacchi su di essi. Tale cifra è meno della metà del 8,21% rilevato nel 2016 (fig. 6-7). Correlando e analizzando i dati, emerge che i rispondenti che hanno segnalato attacchi a questi sistemi appartengo ai seguenti settori merceologici: Commercio all'ingrosso e al dettaglio, Pubblica Amministrazione Centrale e Servizi ICT. E' da sottolineare che nessuno dei rispondenti le cui aziende appartengono al settore manifatturiero, ha indicato attacchi digitali ai sistemi di automazione industriale/robotica eventualmente operanti nella sua azienda.

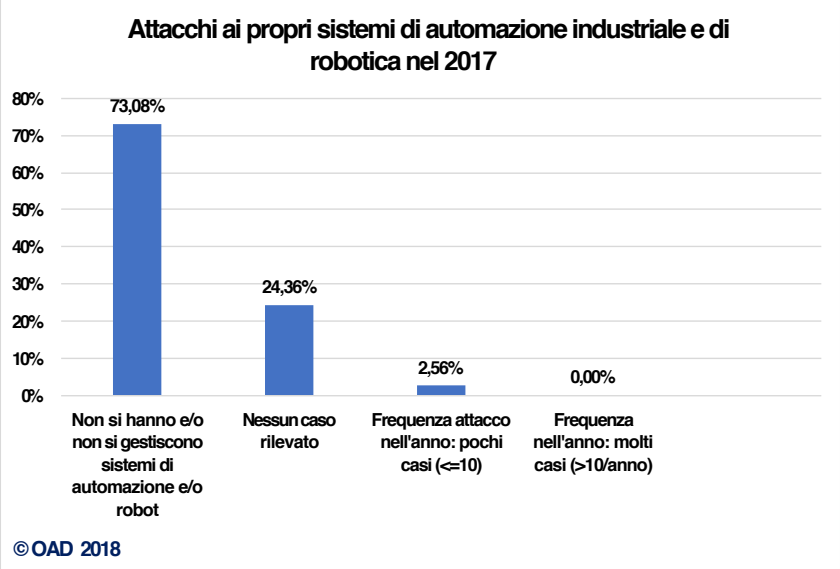

Fig. 6.13-1

La fig. 6.13-2 mostra che le tecniche di attacco più usate secondo i rispondenti che hanno subito tali attacchi sono, con il medesimo 75%, toolkit, botnet e APT. Script e malware, insieme agli agenti autonomi, non sono ai primi posti, come in molte altre tipologie di attacco.

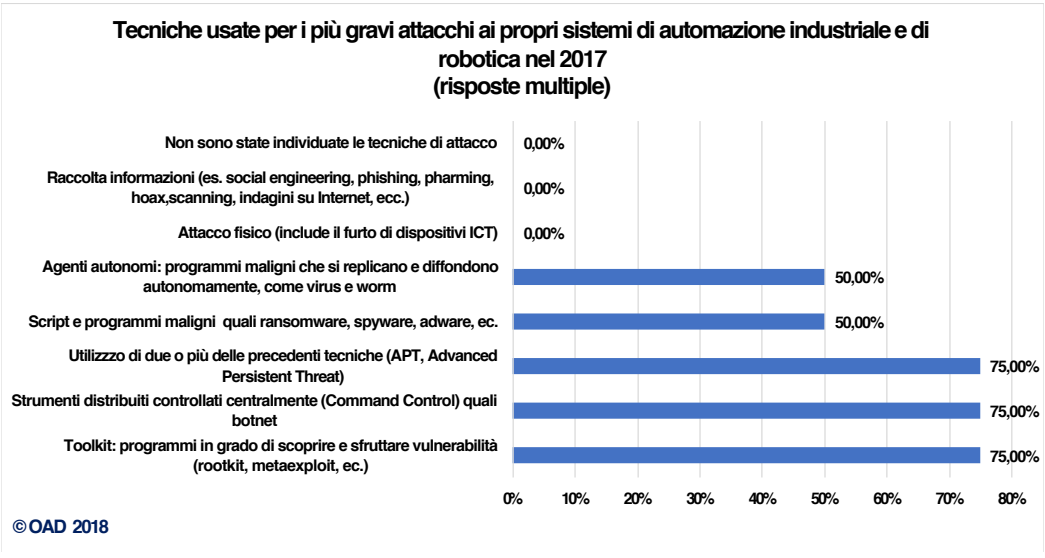

Fig. 6.13-2

La fig. 6.13-3 evidenzia che chi ha subito attacchi gravi ha sempre avuto impatti non trascurabili: per la totalità dei rispondenti ha comportato la perdita di clienti e di affari (100%), cui segue con lo stesso 75%, il danno/i ai clienti da rimborsare e la parziale e non grave interruzione dei servizi ICT forniti. Seguono al 50% la perdita di immagine e gli elevati costi per il ripristino.
Per le possibili motivazioni degli attacchi più gravi non è stato considerato il sabotaggio, invece l'azione dimostrativa è stata quella percentualmente più diffusa, stranamente a giudizio dell'autore, ma i relativamente pochi rispondenti possono rappresentare casi specifici. Tutte le altre motivazioni hanno lo stesso 50% a parte il terrorismo con il 25%.
Il ripristino della situazione ex ante è avvenuto per tutte le aziende/enti che hanno subito l'attacco di questo tipo più grave entro una settimana.

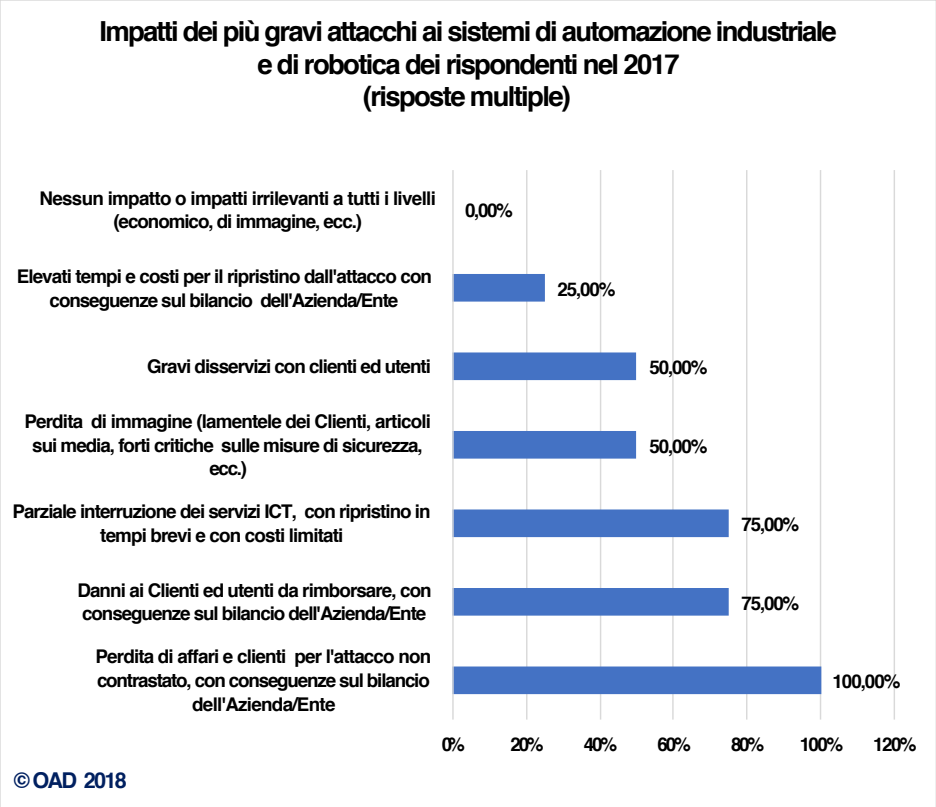

Fig. 6.13-3

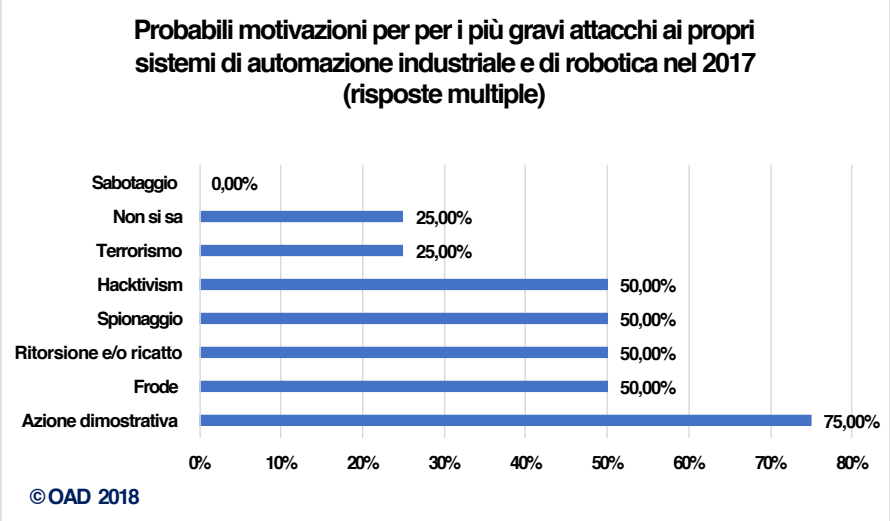

Fig. 6.13-4

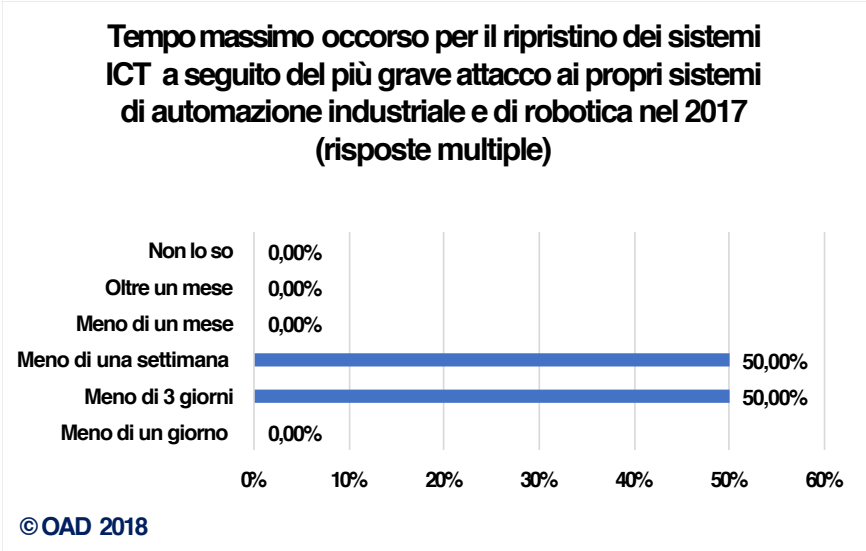

Fig. 6.13-5

Come per gli attacchi ai sistemi IoT, anche in questo caso le indicazioni emerse non sono da considerarsi, con buon senso, come indicatori medi del fenomeno, dato il piccolo numero di rispondenti che hanno rilevato attacchi., ma come specifici e reali casi.

6.14 - Attacchi a sistemi e/o servizi basati su blockchain

La Blockchain è una tecnica introdotta nel 2008 per convalidare le transazioni e la generazione della cripto-valuta bitcoin, con l'obiettivo della libera circolazione della cripto-valuta tra gli utenti, senza o con bassi costi sulle operazioni e soprattutto senza il controllo di un organo centrale regolatore.
Questa tecnica, intrinsecamente sicura "by design", basata sull'elaborazione distribuita ad alta affidabilità (fault tolerance), su consolidate tecniche di moderna crittografia e con consensus 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 inglese, 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 prime soluzioni, per ora per lo più di prova nei loro ambienti digitali .
Dato che anche in Italia varie aziende/enti hanno iniziato a sperimentare o ad usare tecniche di blockchain per specifiche soluzione informatiche, il questionario 2018 ha introdotto 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, e tanto meno nel mondo ICT.
Il 24,34% del campione dei rispondenti dichiara di aver iniziato ad usare questi sistemi (fig. 6.14-1), e solo il 3,95% sul campione totale di chiara di aver subito degli attacchi di questo tipo nel 2017, rispetto al 8,21% nel 2016 (fig. 6-7). Anche in questo caso un decremento degli attacchi, quasi sicuramente dovuto al miglioramento e della messa a punto della soluzione basata sulla blockchain e dal miglioramento del livello di sicurezza implementato.

Nella fig. 6.14-2 le tecniche di attacco probabilmente usate secondo i rispondenti che hanno subito questo tipo di attacco: agenti autonomi e botnet sono quelle che hanno le % maggiori, entrambe sopra il 50%. Seguono poi, tutte con il 33,33%, script-malware, toolkit, APT. Non sono considerati l'attacco fisico e la raccolta di informazioni.

Gli impatti avuti dagli attacchi più gravi (fig. 6.14-3) risentono sicuramente dall'uso prevalentemente prototipale ed embrionale della blockchain, e vedono infatti al primo posto, con lo stesso 66,67%, la perdita di immagine e disservizi di non grave entità; le aziende/enti rispondenti che utilizzano sistemi con questa tecnica sono tutte di medie-grandi dimensioni.

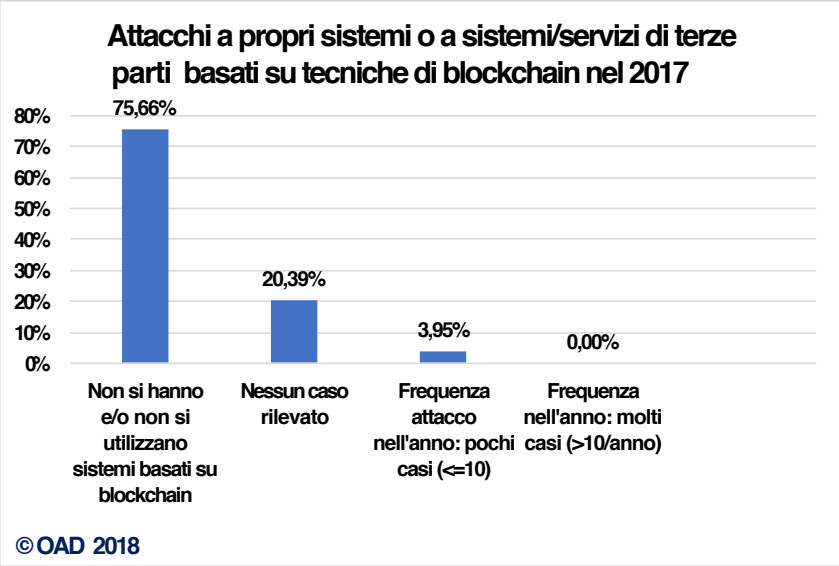

Fig. 6.14-1

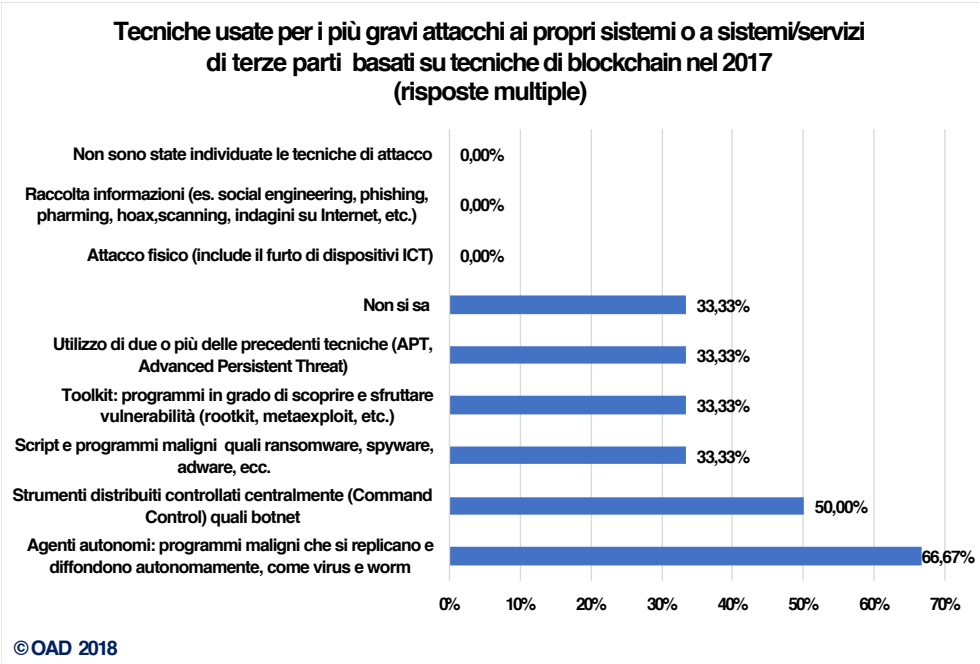

Fig. 6.14-2

Seguono poi, con un 50%, i gravi disservizi e con lo stesso 33,33% danni ai clienti da rimborsare e perdita di affari/clienti.

Le principali possibili motivazioni per i più gravi attacchi subiti di questo tipo (fig. 6.14-4) vedono al primo posto, con un uguale 50%, ritorsione/ricatto e hactivism, seguite da uno stesso 33,33% per frode, azione dimostrativa e spionaggio e da un 16,67% per sabotaggio e terrorismo.

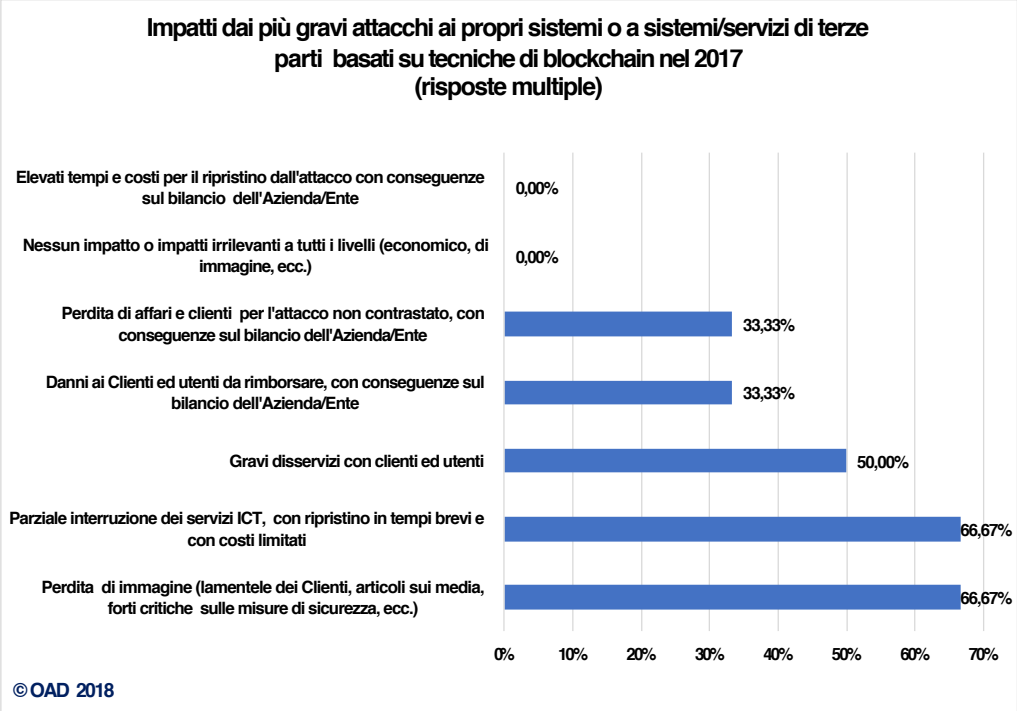

Fig. 6.14-3

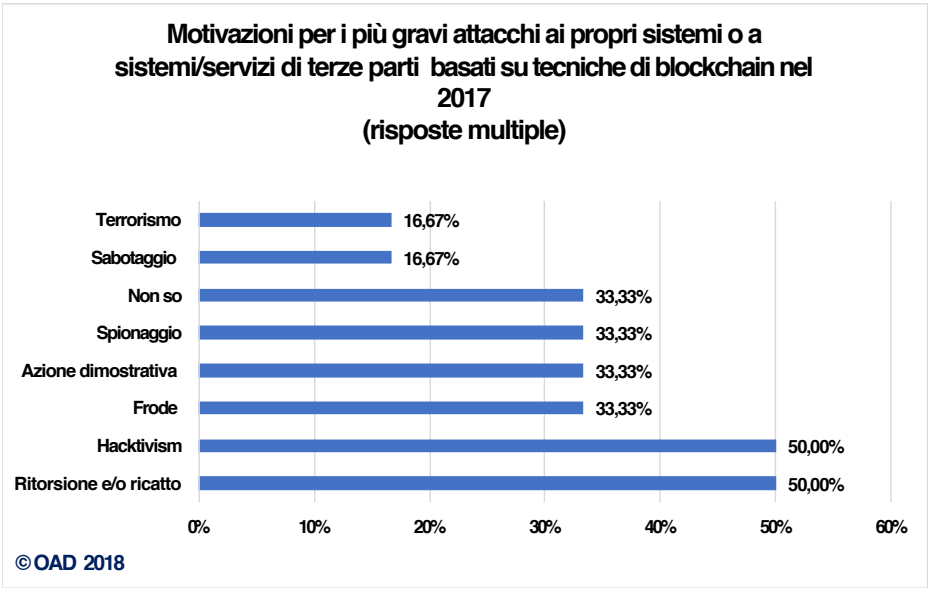

Fig. 6.14-4

I 2/3 dei rispondenti sono riusciti a ripristinare i sistemi entro 3 gg, un altro terzo tra i 3 ed i 7 giorni. Complessivamente nessuno ha dichiarato più di 7 giorni, e questo fatto conferma come i sistemi blockchain abbiano un uso limitato, sperimentale e siano proprio per questo ben controllati.

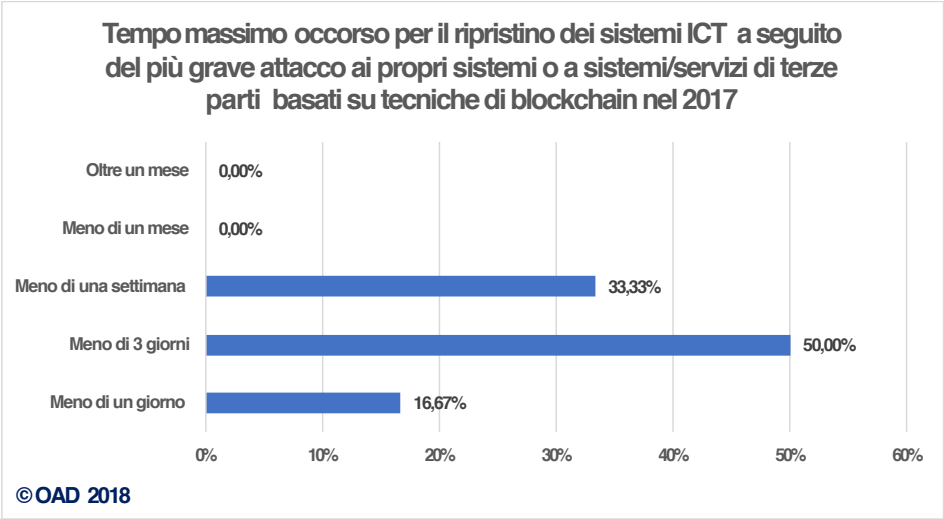
Tempo massimo occorso per il ripristino dei sistemi ICT a seguito del più grave attacco ai propri sistemi o a sistemi/servizi di terze parti basati su tecniche di blockchain nel 2017
Oltre un mese
0,00%
Meno di un mese
0,00%
Meno di una settimana
33,33%
Meno di 3 giorni
50,00%
Meno di un giorno
16,67%
0%
10%
20%
30%
40%
50%
60%
©OAD 2018

Fig. 6.14-5

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

Un insieme delle domande del questionario 2018 era rivolta a comprendere come e da chi vengono rilevati gli attacchi digitali e come sono gestiti.
La fig. 7-1 mostra la provenienza delle segnalazioni di un attacco, con risposte multiple: per il campione dei rispondenti, più della metà delle segnalazioni arriva dagli utenti privilegiati (amministratori di sistema, operatori ICT, ecc.) e per circa il 40% da quelli finali interni. Positivamente, 1/3 arriva anche dai sistemi di monitoraggio e controllo del sistema informatico, percentuale che indica la crescente diffusione e attenzione nell'impiego di strumenti di monitoraggio e controllo del sistema informatico. Segue con circa il 20% la segnalazione da parte degli operatori ICT esterni. Con percentuali decrescenti, seguono l'analisi dei dati del monitoraggio e dei log, 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. Un quarto dei rispondenti non comunica all'esterno per i motivi elencati in fig. 7-3. Un altro 25% lo comunica ai propri fornitori e consulenti, data l'alta percentuale di terziarizzazione, così che gli esperti/addetti ai lavori possano intervenire per capire le ragioni e l'origine dell'attacco, quali contromisure non sono state sufficienti, come migliorare il livello di sicurezza. Il 19,35% lo comunica alle autorità competenti, percentualmente che l'anno prossimo, nella prossima indagine OAD, potrebbe e dovrebbe aumentare dato l'obbligo della denuncia in caso di data breach su dati personali, secondo il regolamento GDPR attivo da maggio 2018. Il 10% circa lo comunica alla sua assicurazione, il che significa che con essa ha assicurato il suo rischio informatico. Tal percentuale è abbastanza alta se confrontata, solo come tendenza, con le analoghe risposte delle precedenti indagini OAI/OAD, positivo segno della cresciuta consapevolezza dei rischi informatici per il business, e della convenienza ad assicurarlo idoneamente. Una percentuale ancora piccola, 6,45%, 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.

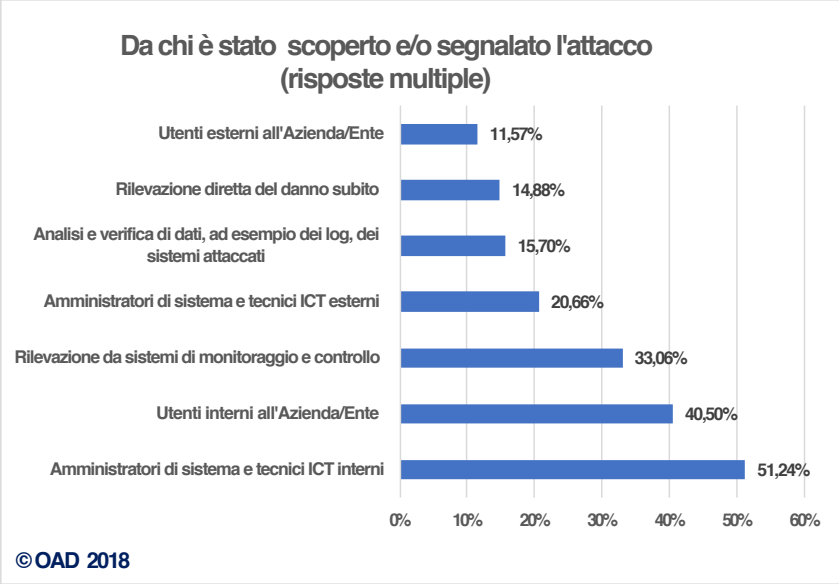

Fig. 7-1

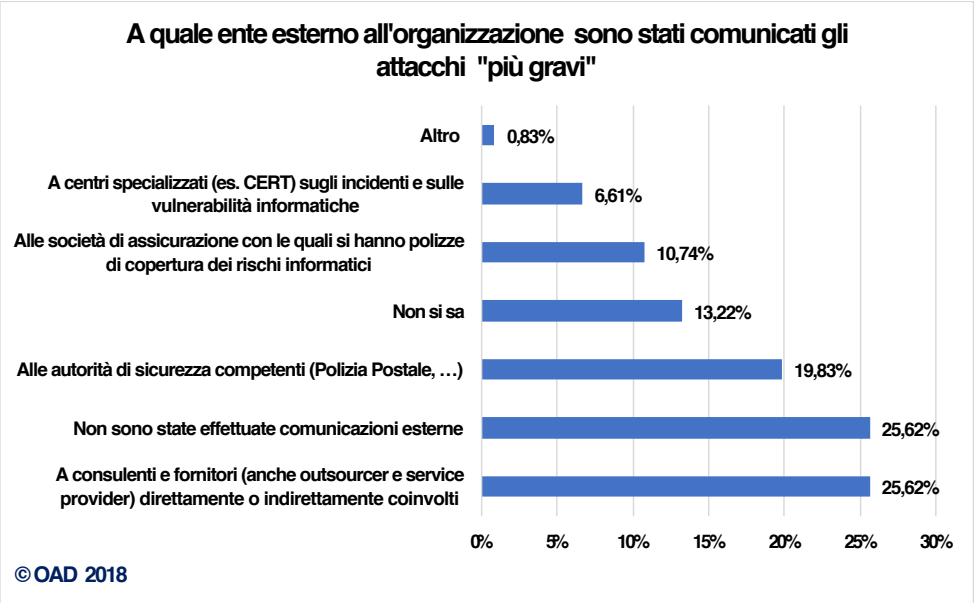

Fig. 7-2

La fig. 7-3 dettaglia, con risposte multiple, le motivazioni per cui non si è comunicato ad esterni l'attacco, da parte dei rispondenti che hanno effettuato tale scelta. Le risposte sono multiple, e per la stragrande maggioranza, la motivazione principale è che l'attacco era troppo poco significativo, quindi, probabilmente, con impatti trascurabili. Al secondo posto, ma a grande distanza con poco meno del 10%, la motivazione è data dalla policy di confidenzialità dell'azienda/ente che non consente l'effettuazione di comunicazioni all'esterno: policy che con il GDPR dovranno essere profondamente modificate. Un 6,67% non lo ha comunicato per non fornire, direttamente o indirettamente, informazioni sulle vulnerabilità e sulle misure di sicurezza digitali in atto.
Un irrisorio 3,23% per la tutela dell'immagine dell'azienda/ente.

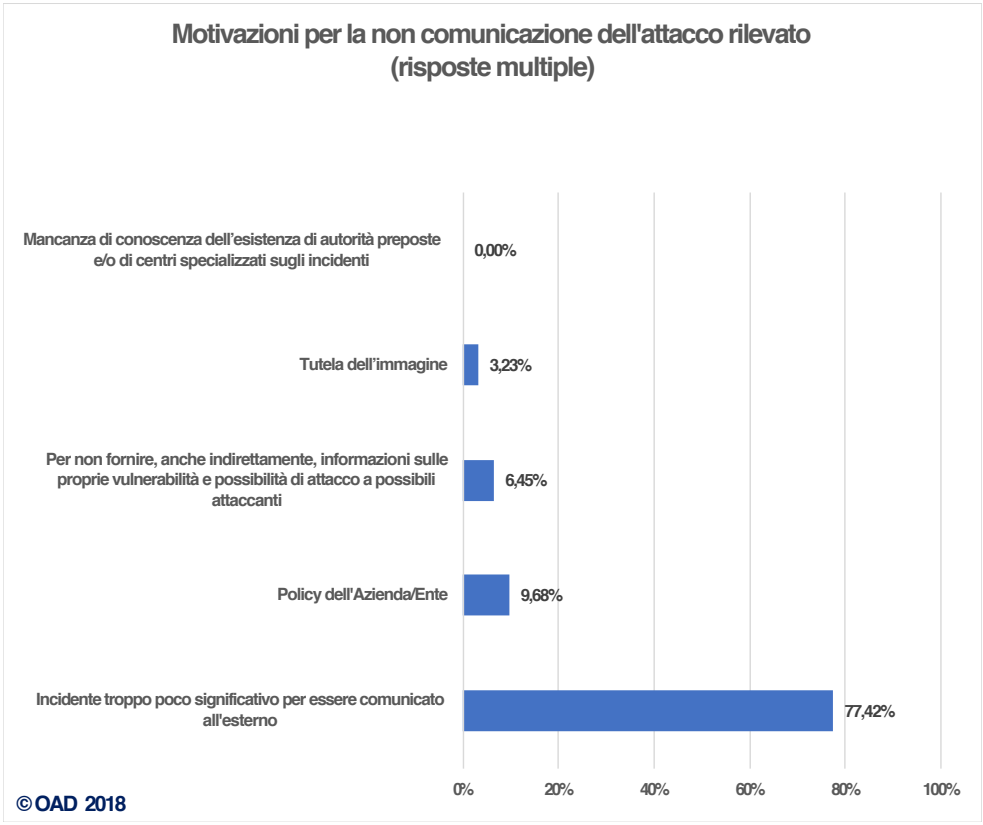

Fig. 7-3

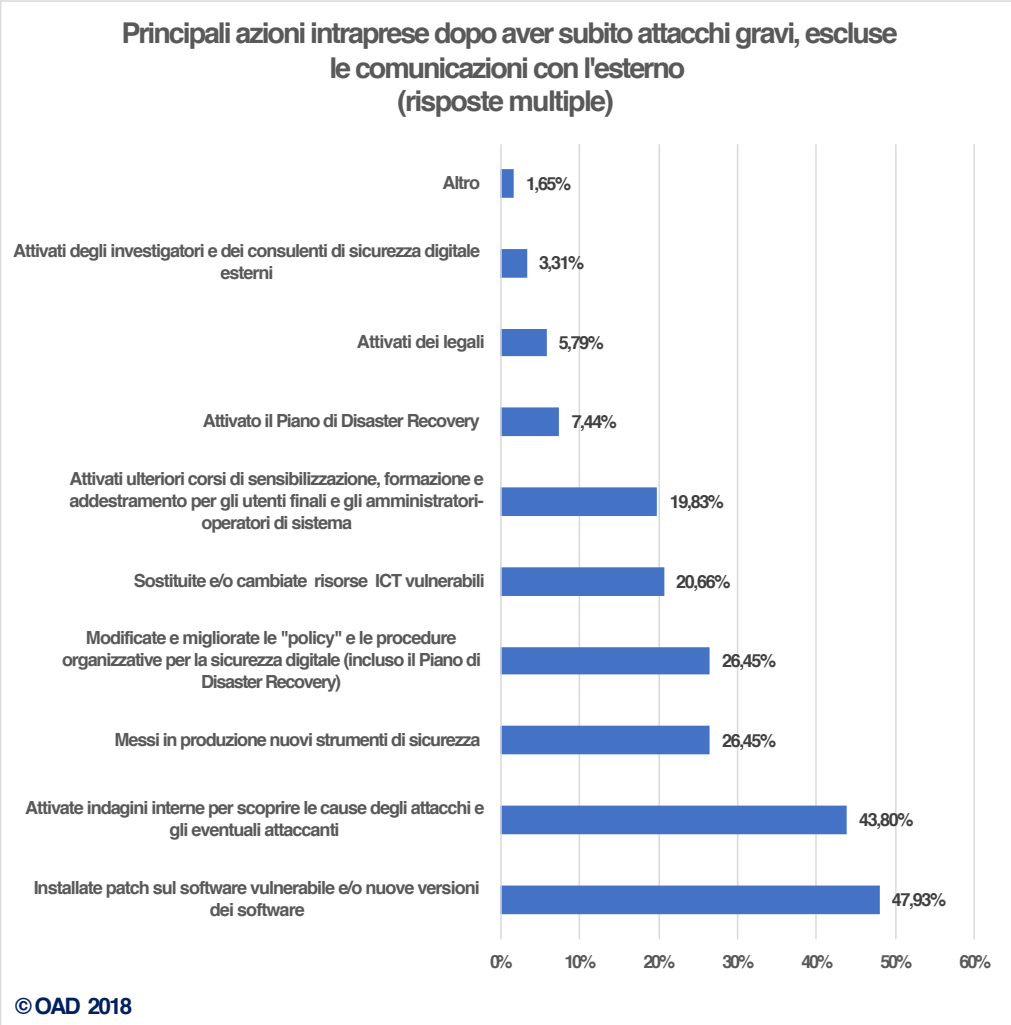

Fig. 7-4

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. In pochi hanno risposto e con valori molti differenti, anche per le diverse loro dimensioni, e pertanto si è preferito non pubblicare alcun valore di riferimento.

Dall'esame delle risposte raccolte tipologia per tipologia, si evidenzia come la maggior parte considera gli impatti subiti poco significativi, indipendentemente da quanti ne ha subiti nell'anno.

La fig. 7.1-1 mostra il confronto delle risposte avute per il 2016 e per il 2017 dallo stesso omogeneo campione di rispondenti, sulla valutazione dell'impatto economico. Il primo significativo dato che emerge è che nel 2016 pochissimi dei rispondenti effettuava un calcolo sul composto economico complessivo di un attacco subito. Nel 2017 invece si è avuto un forte incremento della valutazione, almeno quella complessiva dei costi annuali, passando dal 6,31% al 48,76% dei rispondenti che hanno rilevato attacchi. Questo incremento, soprattutto per la stima dei danni complessivi nell'anno, è un chiaro indicatore che, al crescere degli attacchi digitali e della loro crescente valenza economica di costo, molte aziende/enti hanno iniziato a rilevare il danno economico complessivo su base annua.
Non trascurabile, ma abbastanza simile nei due anni con circa ¼ sul totale, il numero dei rispondenti che non sanno dei costi degli attacchi o non sono in grado di fare delle attendibili stime in merito. Un indicatore che, nonostante i progressi fatti, evidenzia la necessità in Italia di un ulteriore salto "culturale" e di una più profonda ed estesa presa di coscienza sul tema, soprattutto a livello dei vertici di aziende/enti.
La fig. 7.1-2 mette in relazione le risposte avute per l'impatto economico degli attacchi nel 2017 con le dimensioni dell'azienda/ente, dimensioni in termini di numero di dipendenti. I dati emersi sfatano il fatto che solo le strutture di grandi dimensioni sono attente e capaci di rilevare i danni economici: anzi sono proprio le più piccole a stimare tali valori, almeno tra i rispondenti di OAD 2018.

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[12], valuta per le aziende italiane di medie-grandi dimensioni un costo medio per data breach di € 152 per persona dell'azienda/ente attaccato.
A livello mondiale, McKinsey&Company stima l'incremento globale dei costi degli attacchi da $ 345-445 Miliardi nel 2014 a $ 445-600 Miliardi nel 2017.

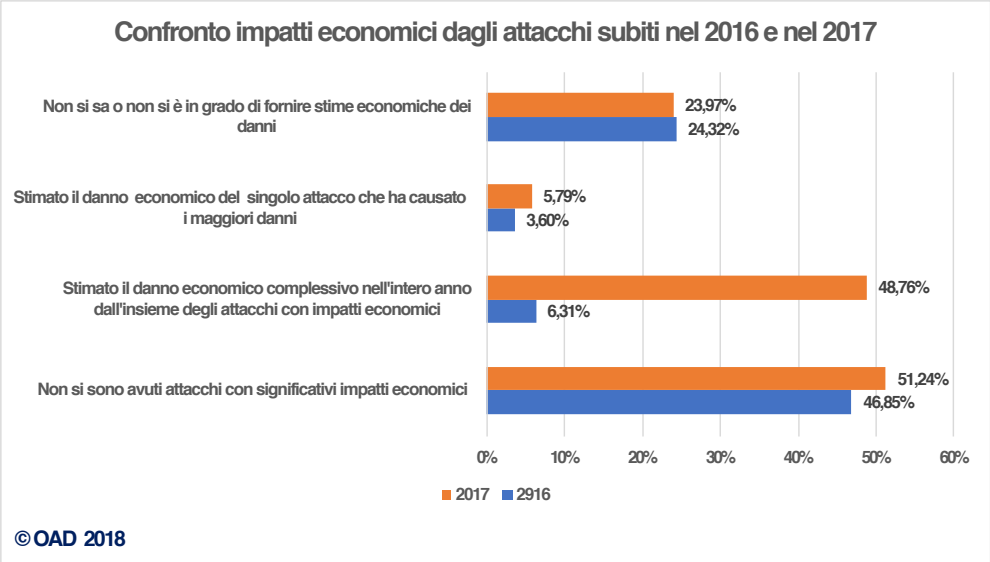

Fig. 7.1-1

12 - 2018 Cost of a Data Breach Study, https://www.ponemon.org/

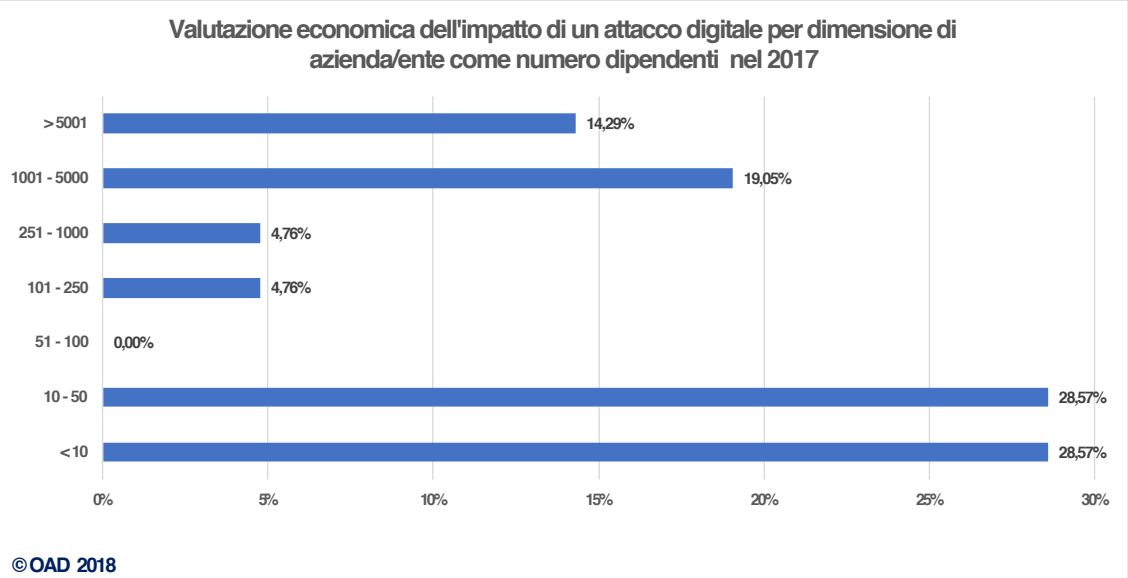
Valutazione economica dell'impatto di un attacco digitale per dimensione di azienda/ente come numero dipendenti nel 2017
> 5001
1001 - 5000
251 - 1000
101 - 250
51 - 100
10 - 50
< 10
14,29%
19,05%
4,76%
4,76%
0,00%
28,57%
28,57%
0%
5%
10%
15%
20%
25%
30%
© OAD 2018

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.

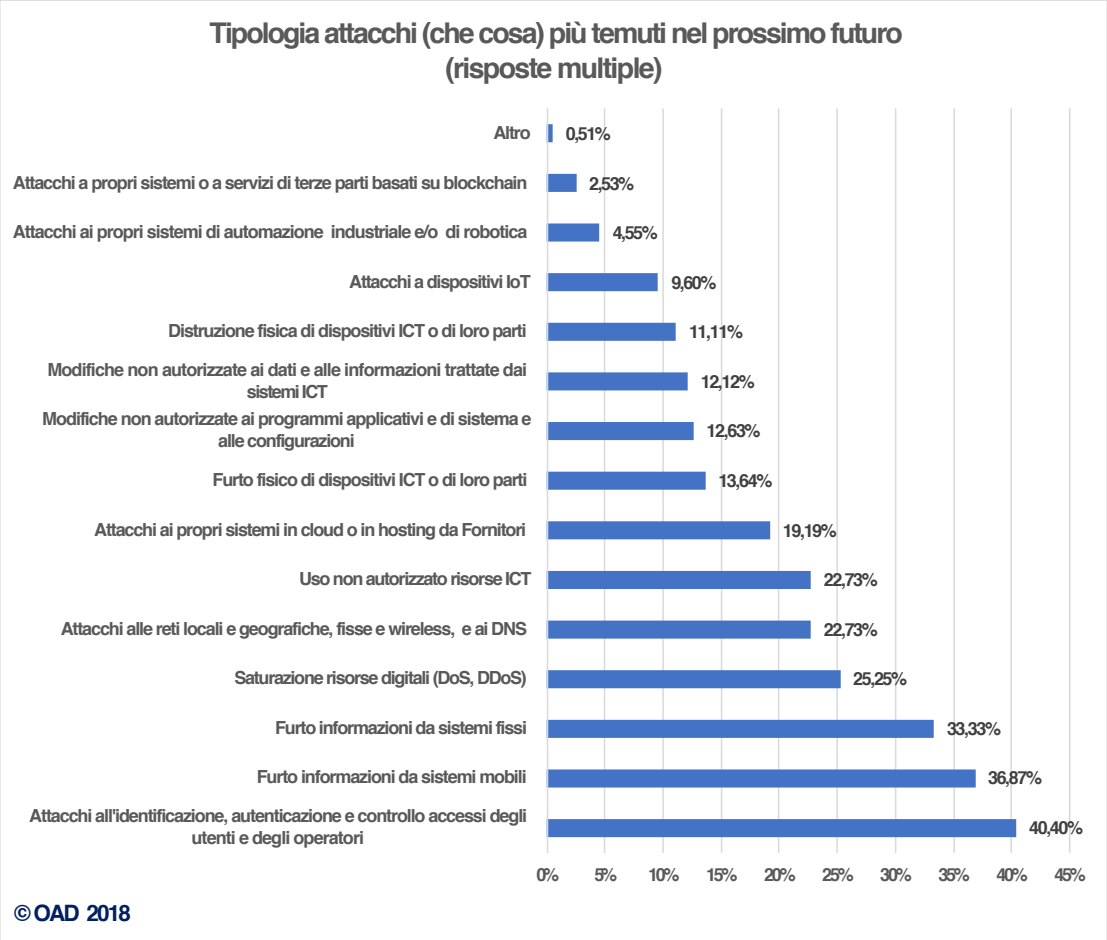

Fig. 8-1

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, il 2017 (si veda fig. 6-7). Al primo posto, con un 40,40% gli attacchi a IAA, cui seguono, nella fascia del 30% e con decrementi tra l'uno e l'altro, il furto di informazioni da sistemi mobili e fissi, con i mobili più temuti dei fissi. Nella fascia del 20%, il DoS/DDoS, gli attacchi alle reti e l'uso non autorizzato dei sistemi ICT. Sotto il 20%, le altre tipologie di attacco temute nel futuro, che diminuiscono man mano in %, come indicato nella

figura. Con il termine "altro" dei rispondenti hanno segnalato, e con ragione, il timore di attacchi ai sistemi VoIP: ormai quasi tutta la telefonia digitale opera sulla pila di protocolli TCP/IP, ossia di Internet, ed i dati di fonia sono integrati e trattati sulle stesse reti locali e geografiche. I PBX VoIP, essendo dei server, possono incorrere nelle stesse vulnerabilità ed attacchi di questi ultimi

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

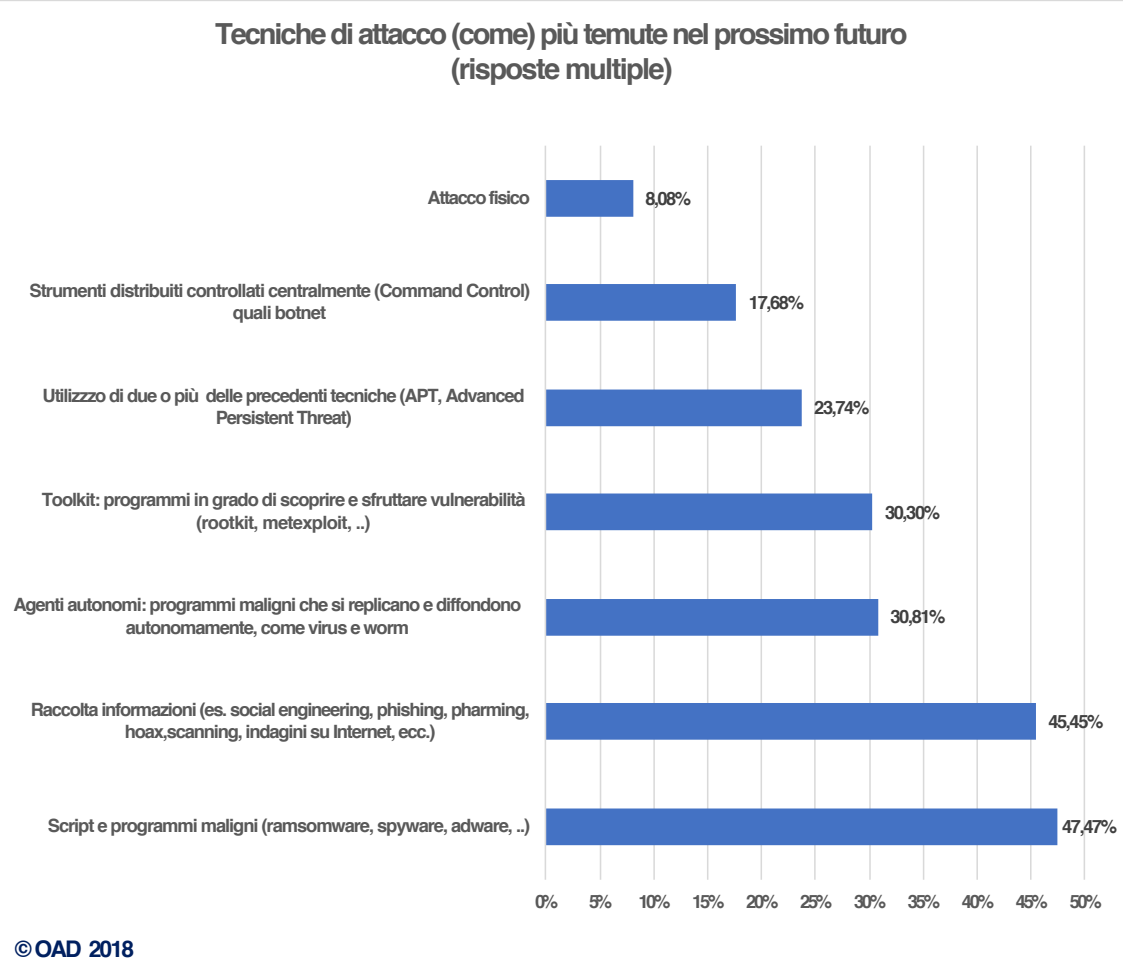

Fig. 8-2

La tecnica di attacco temuta da quasi la metà dei rispondenti è quella degli script-malware, che risulta al primo posto da quella più diffusa nelle varie tipologie di attacchi, come evidenziato in fig. 6.8. La raccolta di informazioni si posiziona al secondo posto, mentre risulta solo al penultimo posto tra quelle rilevate, sempre in fig. 6.8. Gli agenti autonomi sono al terzo posto come temuti, al secondo posto come rilevati, alla pari come % ai Toolkit.
All'ultimo posto l'attacco fisico come tecnica di attacco più temuta, nella stessa posizione come tecnica di attacco rilevata (fig.6.8).
La fig. 8-3 mostra le motivazioni ipotizzate per i futuri attacchi: la frode è la motivazione più probabile per ¾ dei rispondenti. Segue, con una % di quasi la metà della precedente, l'azione dimostrativa. A decrescere le altre possibili motivazioni.

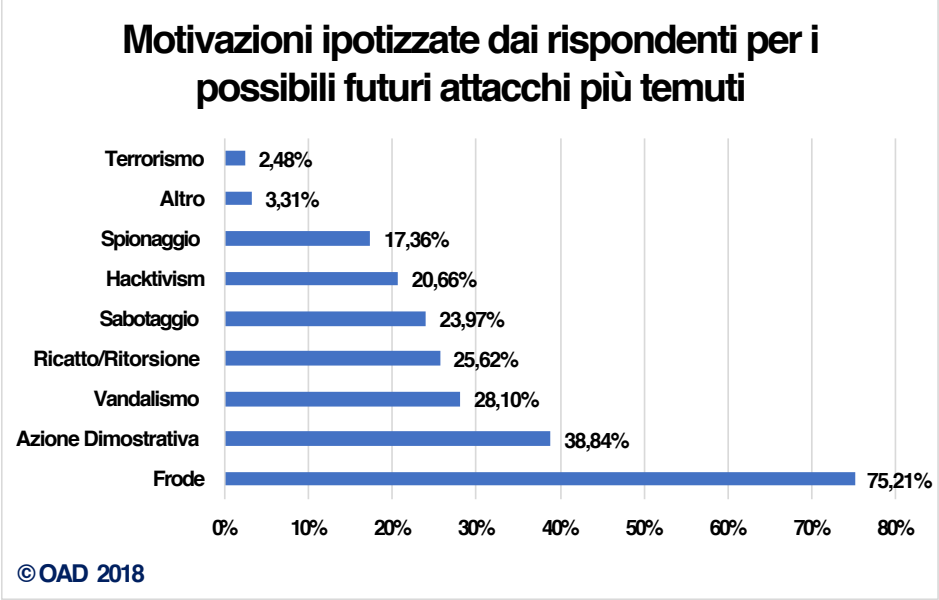
Motivazioni ipotizzate dai rispondenti per i possibili futuri attacchi più temuti
Terrorismo
2,48%
Altro
3,31%
Spionaggio
17,36%
Hacktivism
20,66%
Sabotaggio
23,97%
Ricatto/Ritorsione
25,62%
Vandalismo
28,10%
Azione Dimostrativa
38,84%
Frode
75,21%
0%
10%
20%
30%
40%
50%
60%
70%
80%
©OAD 2018

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 governo sono un mix di misure organizzative e di strumenti tecnici di governo: l'attribuzione di alcune misure in quale sezione, sempre discutibile, è stata effettuata dall'autore nell'ottica di una maggior chiarezza 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, ed 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, ecc.), attività di audit interno e/o esterno.
Il nuovo 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[13], favorisce e favorirà una maggior attenzione su questi aspetti.
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

13 - 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)

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.

9.1.1 - La struttura organizzativa per la sicurezza digitale

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, più di ¾ dei rispondenti hanno nelle loro organizzazioni un simile ruolo, formalizzato (ossia ufficializzato con una lettera di incarico, posizione nell'organigramma e mansionario) oppure no (persone, ufficialmente con altri ruoli che svolgono, in tutto o in parte, le attività tipiche del CISO), all'interno o esternalizzato; un altro indicatore del livello mediamente buono delle aziende/enti dei rispondenti in merito alla sicurezza digitale. Ma per meno di un quarto delle organizzazioni dei rispondenti, il ruolo di CISO non è espletato in alcun modo.
Ma quali sono le aziende/enti nelle quali sembrerebbe che nessuno si occupa di sicurezza digitale? La fig. 9.1.1-2 fornisce una chiara risposta, correlando, sempre in maniera totalmente anonima, chi ha risposto con un "no" totale con il numero di dipendenti della sua azienda/ente. Come è prevedibile, le piccole e medie organizzazioni, sotto i 250 dipendenti, non hanno il ruolo del CISO per il 78,57%; e tra queste le piccolissime non lo hanno nel 50% dei casi: per queste ultime l'autore avrebbe ipotizzato percentuali ancora più alte. Ma anche in grandi e grandissime strutture, pur con basse %, tale ruolo manca. La causa può essere dovuta alla non conoscenza del rispondente di tale ruolo nella sua impresa, ma tale ignoranza per i rispondenti di grandi strutture lascia assai dubbiosi. Di fatto, anche per l'esperienza dell'autore sul campo come consulente direzionale nell'ICT, sovente in Italia manca il ruolo di CISO pure in grandi strutture.

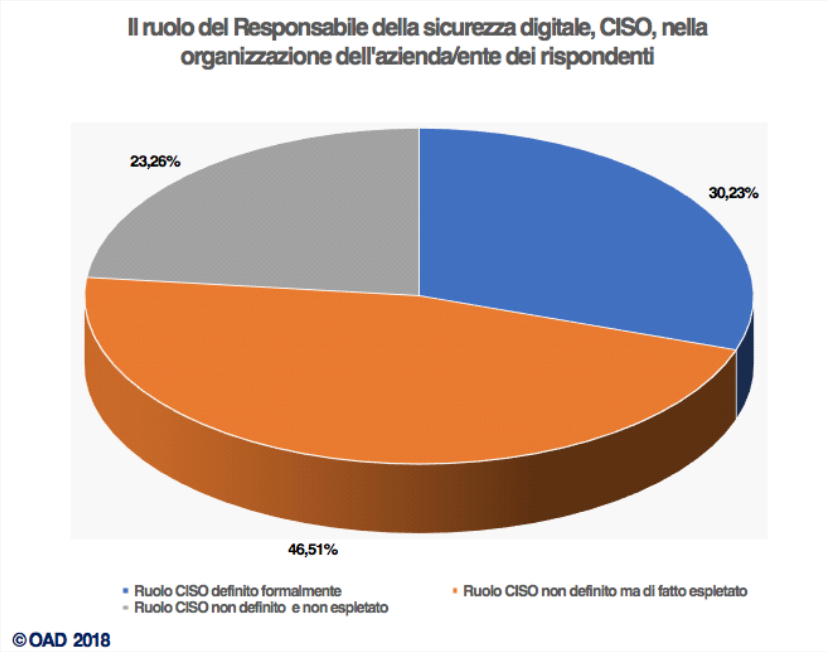

Fig. 9.1.1-1

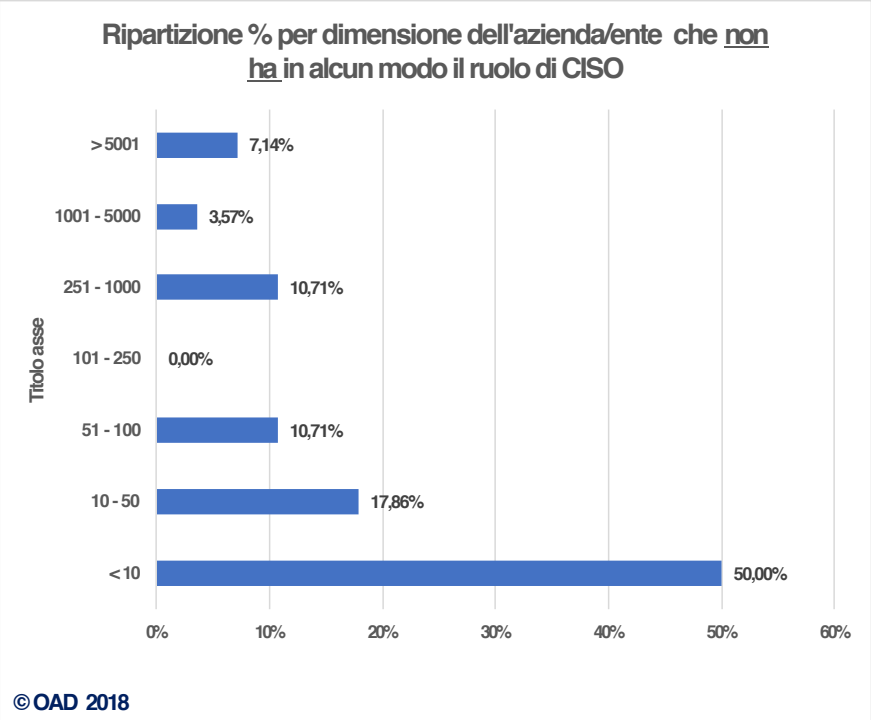

Fig. 9.1.1-2

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.

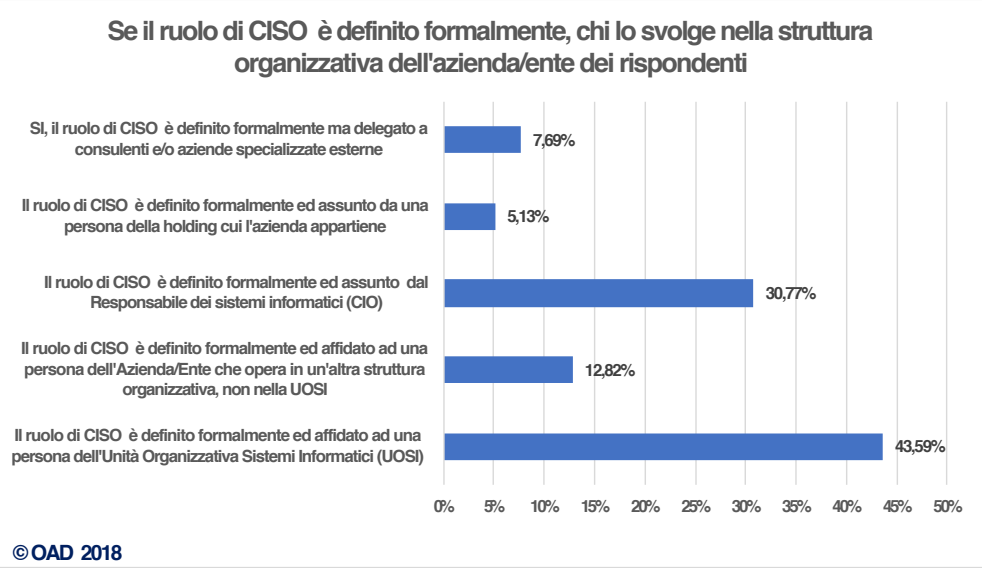

Fig. 9.1.1-3

La maggior parte delle risposte indica che il ruolo è affidato ad una persona della UOSI, e in più del 30% dallo stesso CIO. Quasi il 13% pone il 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 (5,13%). Solo per il 7,69% il ruolo del CISO viene terziarizzato a consulenti o società specializzate. La terziarizzazione del ruolo del CISO sarà probabilmente una tendenza crescente nei prossimi anni, soprattutto per le piccole strutture, ed anche grazie alla pressione legislativa per la conformità al GDPR.
Per le aziende/enti che non hanno formalizzato il ruolo del CISO, la fig. 9.1.1-4 mostra chi di fatto lo espleta: nella maggior parte dei casi il ruolo è de facto assunto dal CIO o da personale della sua struttura UOSI. Nel 21,67% è espletato da personale di altre strutture dell'azienda/ente, non dell'UOSI, e solo nel 6,67% da personale esterno.

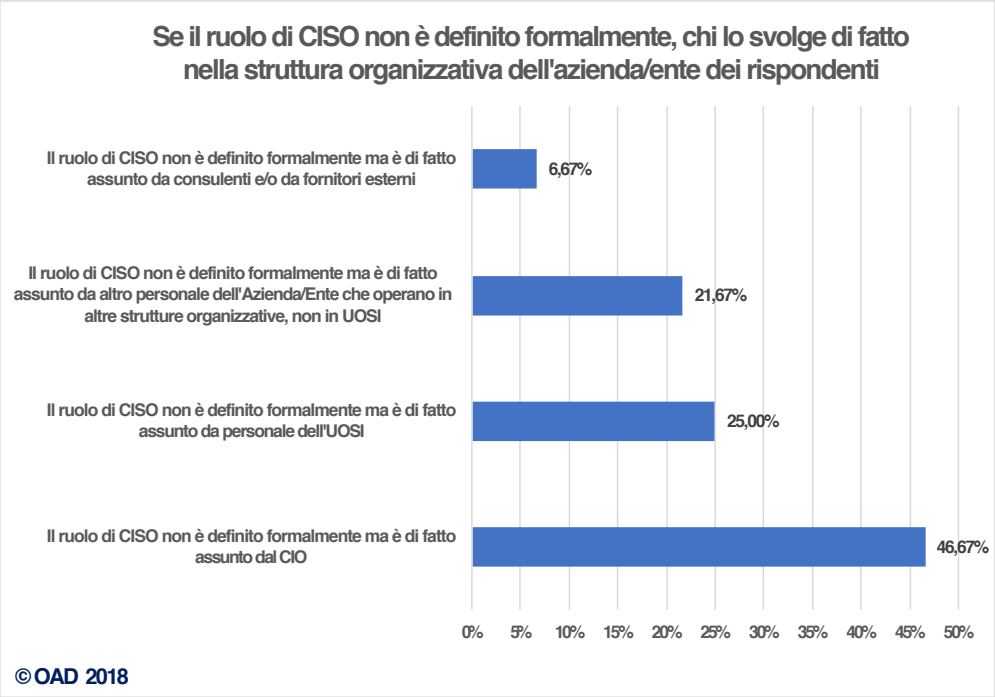

Fig. 9.1.1-4

9.1.2 - Policy e procedure organizzative

La fig. 9.1.2-1 schematizza concettualmente la differenza tra una policy ed una procedura: la prima individua indirizzi e logiche di alto livello, prevalentemente di tipo strategico, fornite dal vertice organizzativo o dal consiglio di amministrazione. Le policy valgono normalmente per più di un anno e difficilmente scendono in dettagli tecnici. Le procedure organizzative forniscono dettagliate istruzioni sia organizzative sia tecniche su come comportarsi per svolgere specifiche attività, qui nell'ambito della sicurezza digitale, e sono rivolte sia alle persone che svolgono determinati ruoli, sia alle strutture organizzative che debbono espletare 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. costituiscono dei manuali d'uso.

Le policy e le procedure organizzative fanno spesso riferimento a normative che occorre rispettare per legge o per 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. Sono inoltre essenziali per dimostrare l'accountability[14], così come richiesto ad esempio dal GDPR, e più in generale da varie leggi e normative (non solo per l'ICT).

Fig. 9.1.2-1

La fig. 9.1.2-2 fornisce una dettagliata indicazione sulla presenza di policy e di quale tipo, ed analogamente la fig. 9.1.2-3 per le procedure organizzative.
Le fig. 9.1.2-4 e 9.1.2-5 correlano le risposte dei rispondenti che hanno dichiarato di non avere policy o procedure con le dimensioni, in termini di dipendenti, delle loro aziende/enti.
Come facilmente prevedibile, la stragrande maggioranza appartiene a piccole imprese, con una forte incidenza di quelle con meno di 10 dipendenti.
Ma alcuni rispondenti, in percentuale pochi, dichiarano che le loro grandi e grandissime aziende non dispongono di policy e di procedure organizzative, e correlando le risposte sono soprattutto queste grandissime ad avere % leggermente più alte.

14 - 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.

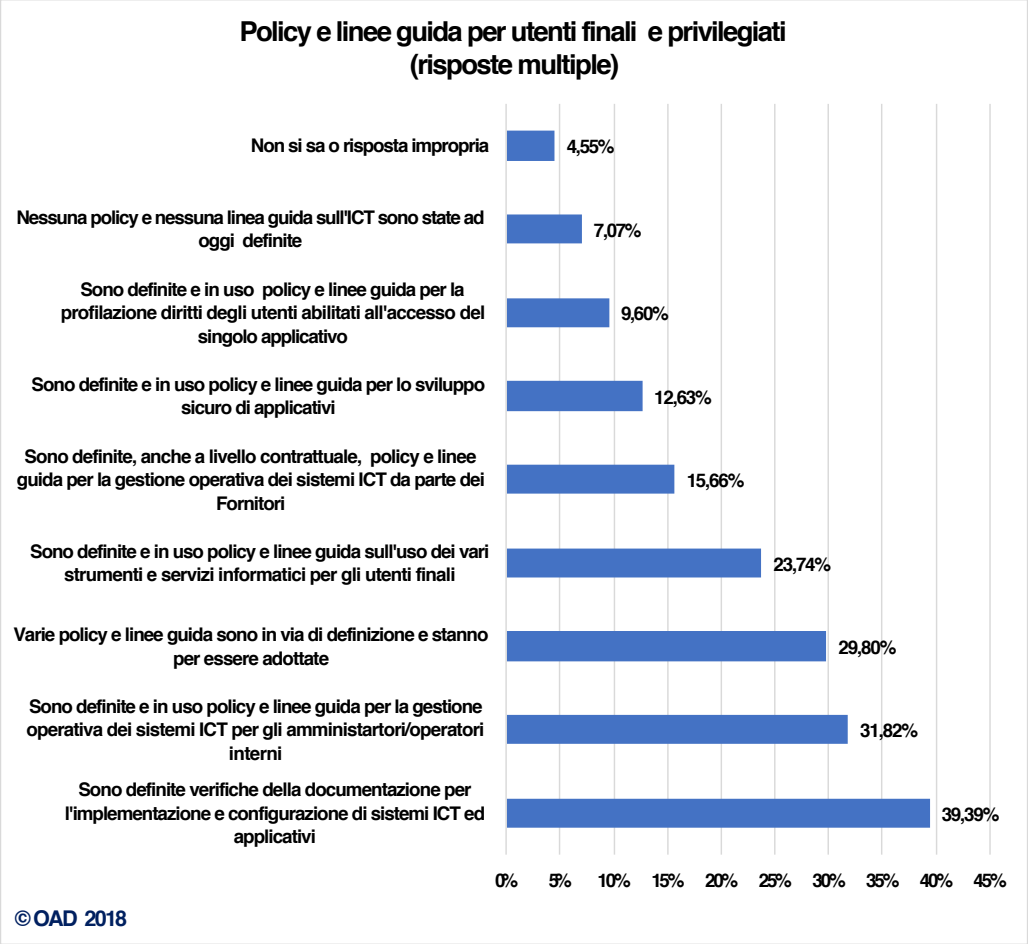

Fig. 9.1.2-2

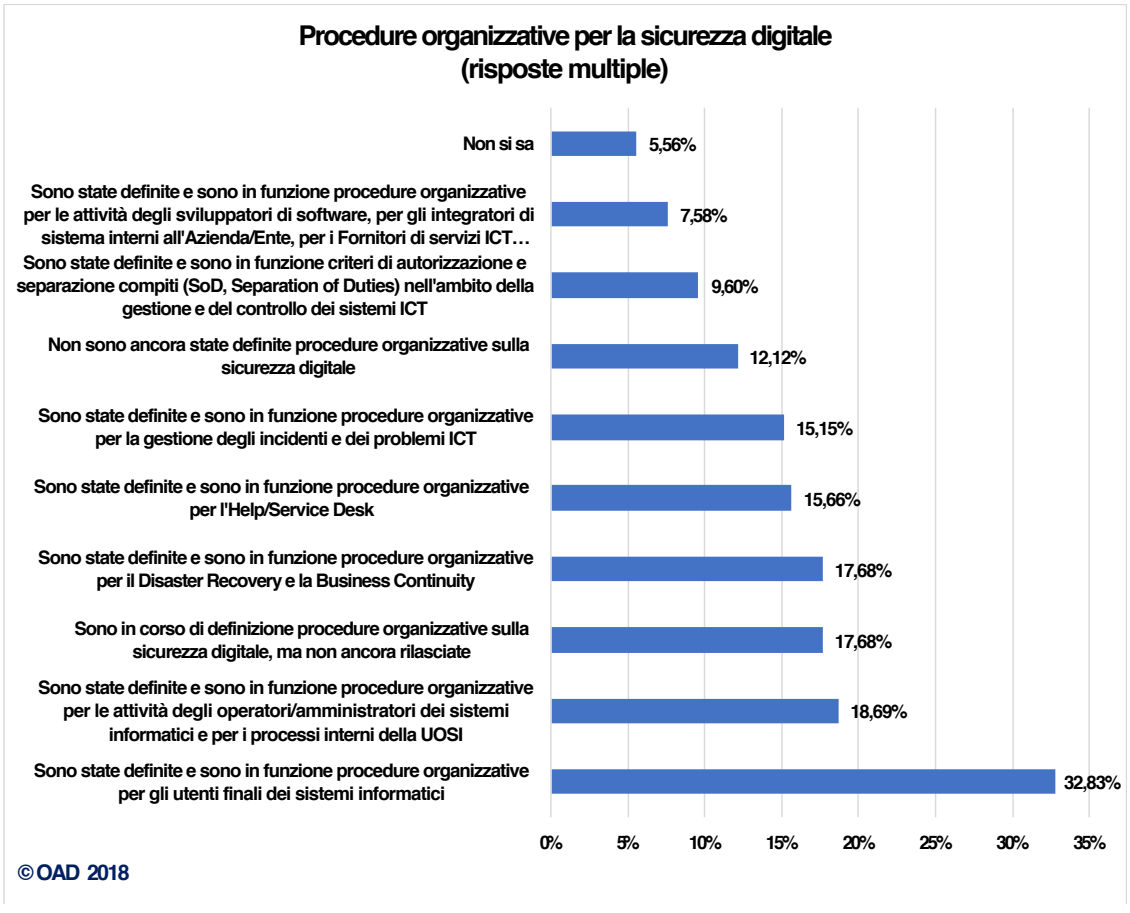

Fig. 9.1.2-3

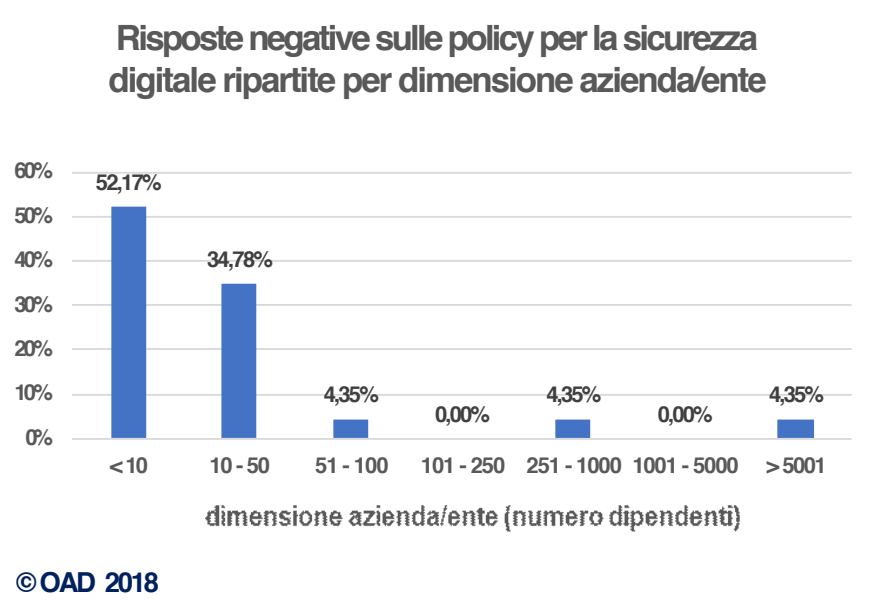

Fig. 9.1.2-4

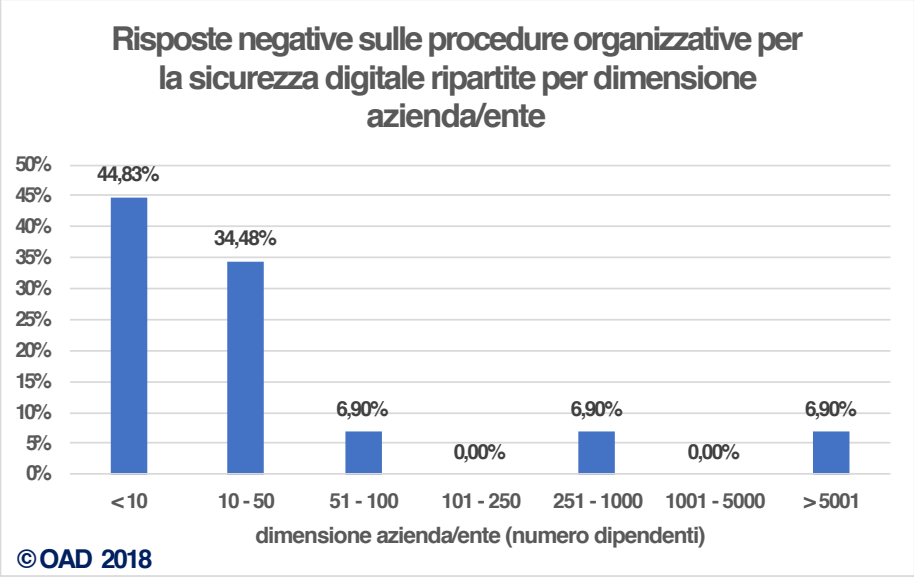

Fig. 9.1.2-5

9.1.3 - Sensibilizzazione, formazione ed addestramento

Come anche evidenziato nella prefazione dal Direttore della Polizia Postale e delle Comunicazioni, la larga diffusione ed efficacia degli attacchi digitali è dovuta anche 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 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 realtà avrebbe bisogno: consapevolezza necessaria per le decisioni da prendere in merito, dal budget da allocare agli interventi tecnici ed organizzativi da effettuare con le opportune priorità.
La fig. 9.1.3-1 mostra che un non trascurabile 21,72% delle aziende/enti rispondenti non effettua alcun tipo di formazione, e che solo un 5,05% non sa rispondere.
Analizzando chi ha selezionato di non effettuare formazione, la fig. 9.1.3-2 mostra che gran parte dei rispondenti del 21,72% appartiene (quasi il 77%) a strutture di piccole-medie dimensioni, mentre il resto appartiene a strutture con più di 250 dipendenti.

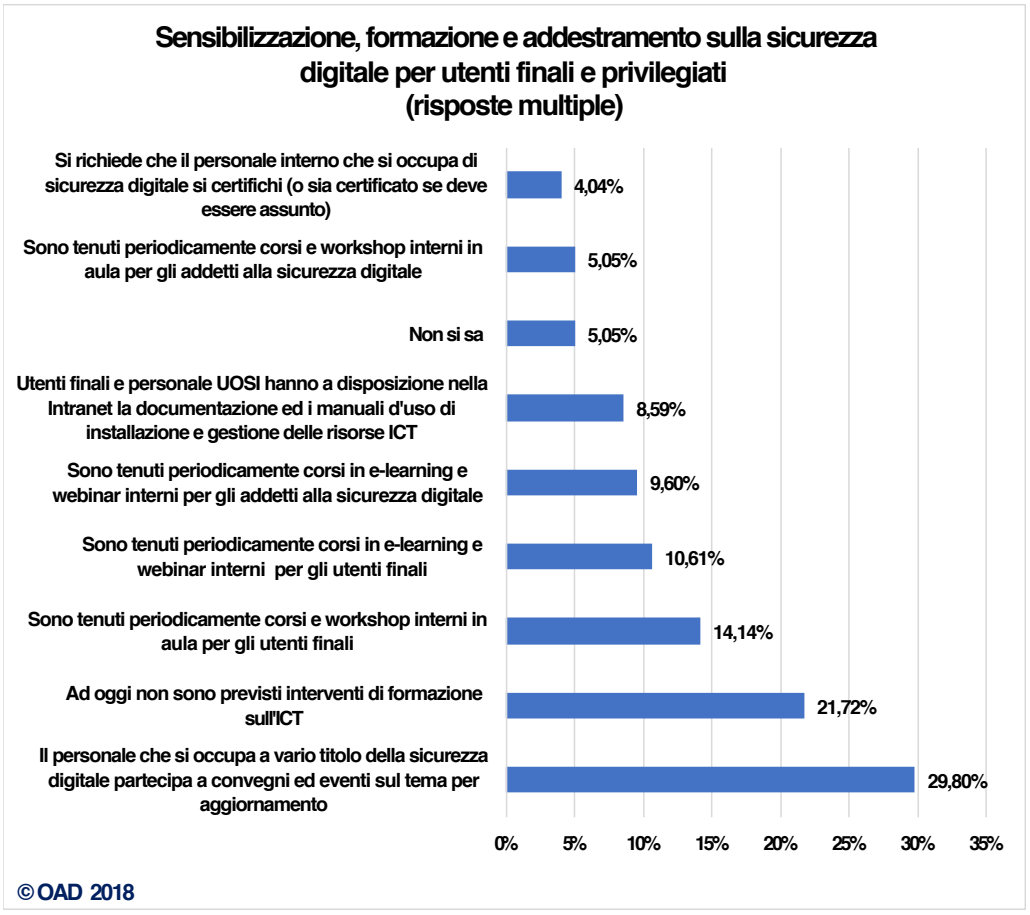

Fig. 9.1.3-1

E di queste ultime, dall'analisi emerge che anche alcune grandi strutture con più di 1000 dipendenti non fanno alcun tipo di formazione sulla sicurezza digitale: esse costituiscono ben il 10% dei rispondenti che non fanno formazione, un ulteriore dato preoccupante per la sicurezza digitale in Italia, che conferma quanto indicato nella prefazione.

Fig. 9.1.3-2

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 adottate 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, il 40% circa dei rispondenti segnala che la propria azienda/ente non è interessata e non richiede certificazioni ed il 14,65% dei rispondenti non sa rispondere sulle certificazioni al proprio interno. Questi due dati sono un segnale di come in Italia le certificazioni, soprattutto per la sicurezza ICT, non siano ancora considerate come uno strumento necessario, anche se non sufficiente, per garantire un minimo livello di garanzia sulle effettive competenze di persone e di aziende.
D'altro canto, però, il 31,31% delle aziende/enti dei rispondenti è già in possesso o sta effettuando certificazioni sulla sicurezza digitale, e di queste circa la metà è certificata ISO 9001 per la qualità totale (che solo marginalmente tratta della scurezza digitale). E' importante evidenziare come quest'ultima percentuale, nel bacino dei rispondenti, sia più alta di circa un punto percentuale del totale delle certificazioni specifiche per la sicurezza. Il motivo è semplice: l'obbligo della certificazione ISO 9001 per aziende/enti che vogliono rispondere a bandi di gara pubblici. 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.

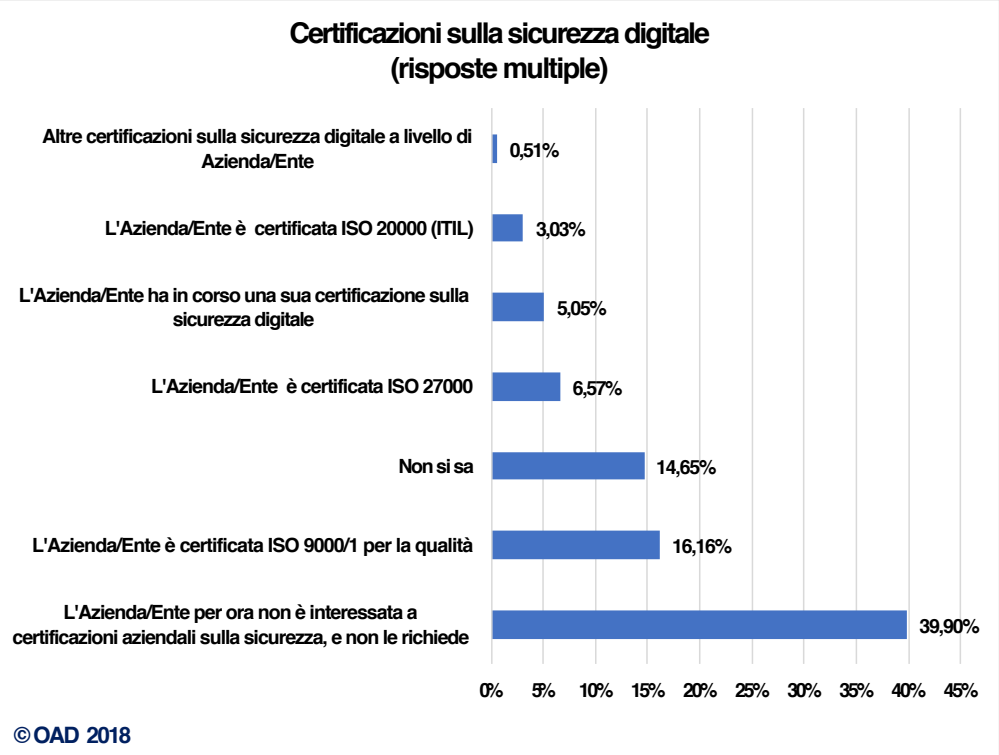

Fig. 9.1.4-1

Il comportamento sulle certificazioni a livello aziendale e a livello individuale, al proprio interno e per i propri fornitori, è dettagliato nelle fig. 9.1.4-2 e 9.1.4-3.
La maggioranza dei rispondenti non richiede certificazioni ma è significativa la differenza percentuale di circa 8 punti a sfavore dei fornitori ICT: per le aziende/enti rispondenti, data la loro prevalente tipologia di settore (fig. 10.2-1), maggiore sul versante dell'offerta che della domanda, è più importante avere proprie certificazioni e proprio personale certificato, piuttosto che quelli del fornitore e del suo personale.

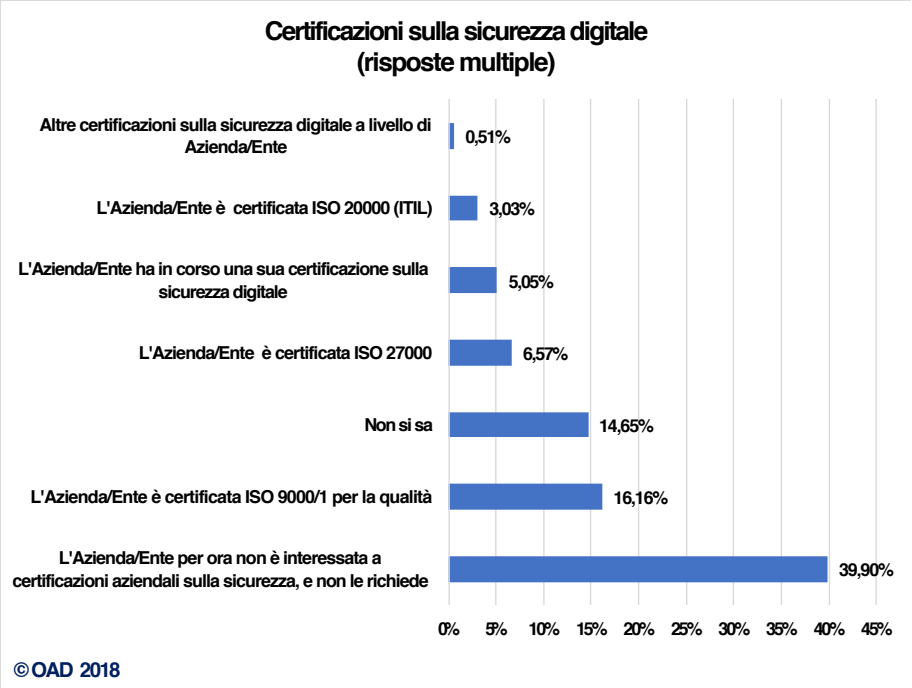

Fig. 9.1.4-2

Da entrambe le figure emerge una % di "non si sa" tra il 12 ed il 14%, non altissima ma comunque preoccupante come indicatore di conoscenza della situazione della propria organizzazione su questo tema, tendendo proprio conto di chi ha risposto al questionario: i rispondenti sono persone o di vertice o coinvolte nei sistemi informatici (si veda §10.1), quindi "del mestiere", e fa specie che non sappiano nulla in merito. Si ritorna al problema della cultura della sicurezza digitale, e più in generale dell'ICT, soprattutto per le persone di vertice, con un preoccupante disinteresse per una più attenta selezione dei fornitori e consulenti ICT in base alle loro effettive capacità e competenze.

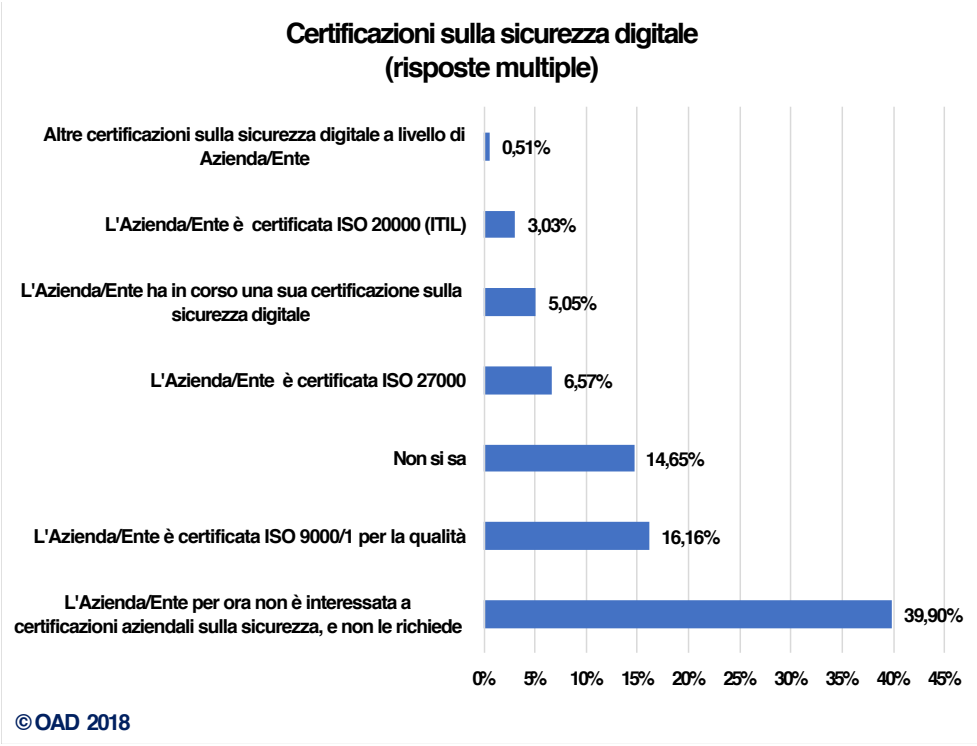

Fig. 9.1.4-3

Non si arriva al 5% per chi richiede certificazioni aziendali o personali ai fornitori ICT, ed è ancor più preoccupante che non si arrivi al 10% per chi intende richiederle nel prossimo futuro, considerando la forte crescita delle terziarizzazioni.
Una così bassa ed allarmante percentuale di richieste è in parte spiegabile dal numero di rispondenti di piccole e medie organizzazioni: essi il più delle volte devono accettare i contratti dei fornitori (soprattutto di grandi strutture e/o stranieri) così come questi ultimi li propongono, e non possono includere specifiche clausole, quali la richiesta di personale certificato. D'altro canto, il livello di sicurezza di molti fornitori è ritenuto assai alto, come normalmente lo è, ed il cliente dà per scontato, di poter usufruire di un elevato livello di servizio.
Comunque, a livello interno dell'organizzazione, già più del 13% delle aziende/enti dei rispondenti richiede per certi ruoli del proprio personale specifiche certificazioni, ed alcuni le hanno già acquisite.
Un'ultima considerazione sull'importanza delle certificazioni ICT, proprio nel settore della sicurezza digitale, e più in generale dell'ICT e delle compliance alle varie normative, data la scarsa competenza e conoscenza da parte del cliente, soprattutto di piccole e piccolissime strutture. Al crescere delle necessità per la sicurezza digitale e per la privacy da parte soprattutto di aziende ed enti senza alcuna esperienza su questi temi, varie aziende e ancor più consulenti si offrono come esperti sia a livello di fornitori/rivenditori di prodotti e servizi per la sicurezza digitale, sia, ed è peggio, come consulenti, anche se non hanno neppur loro competenze professionali in merito, e nemmeno intendono (o possono) acquisirle: devono vendere quello che hanno, prodotti, servizi e pseudo competenza, e spesso lo fanno a prezzi bassissimi, incompatibili ed impensabili per l'effettuazione di un effettivo e qualificato intervento. Alcuni rivenditori tendono ad offrire solo quello che hanno a magazzino (e talvolta anche sistemi totalmente obsoleti tecnicamente), indipendentemente dalla effettiva necessità del cliente. Alcuni consulenti riusano e riciclano schemi e soluzioni, magari scaricati da Internet, senza minimamente contestualizzarli sulla realtà del cliente. Da questi approcci eticamente e professionalmente assai scorretti, derivano i bassi prezzi, ma i risultati il più delle volte sono vere e proprie truffe.
Per una prima scrematura di questi millantatori e truffatori, che rovinano anche il mercato dei corretti venditori e consulenti, la verifica di una loro certificazione può essere una condizione necessaria di selezione. Ma non sufficiente, perché, purtroppo, c'è certificazione e certificazione e non è detto che chi ha molte certificazioni sia anche un buon venditore o consulente che non solo fa gli interessi suoi, come è lecito, ma anche quelli del cliente.

Nel mondo ormai complesso e diversificato delle certificazioni, è bene ricordare che in Italia sono in vigore due leggi, quella n. 4/2013 sulle "professioni non regolamentate" ed il D. Lgs. n. 13/2013 sulla "certificazione delle competenze" che hanno definito le certificazioni personali con valore legale per le figure professionali non regolamentate da Ordini. La prima normativa di riferimento indicata da queste norme è EN 16234-1:2016 (UNI 11506), che riprende la già citata certificazione europea eCF sulle competenze e sui profili professionali dell'ICT.

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. 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, aggiunta di nuove linee di business, cambi a taluni processi, ecc.), sovente esso viene inserito tra gli strumenti per la gestione della sicurezza digitale. Data la sua rilevanza, anche a seguito del GDPR, si è preferito dedicare all'analisi dei rischi un paragrafo a sé stante, nell'ambito delle misure organizzative.

La fig. 9.1.5-1 indica che il 45,39% delle aziende/enti dei rispondenti effettua l'analisi dei rischi in maniera sistematica o quando necessario, e che il 36,17% ha a piano di effettuarla nel prossimo futuro. Queste percentuali sono molto maggiori di quelle rilevate nei precedenti rapporti (pur non essendo confrontabili a livello statistico per la differenza dei bacini dei rispondenti). Un aumento sicuramente favorito dall'obbligo di conformità al GDPR.

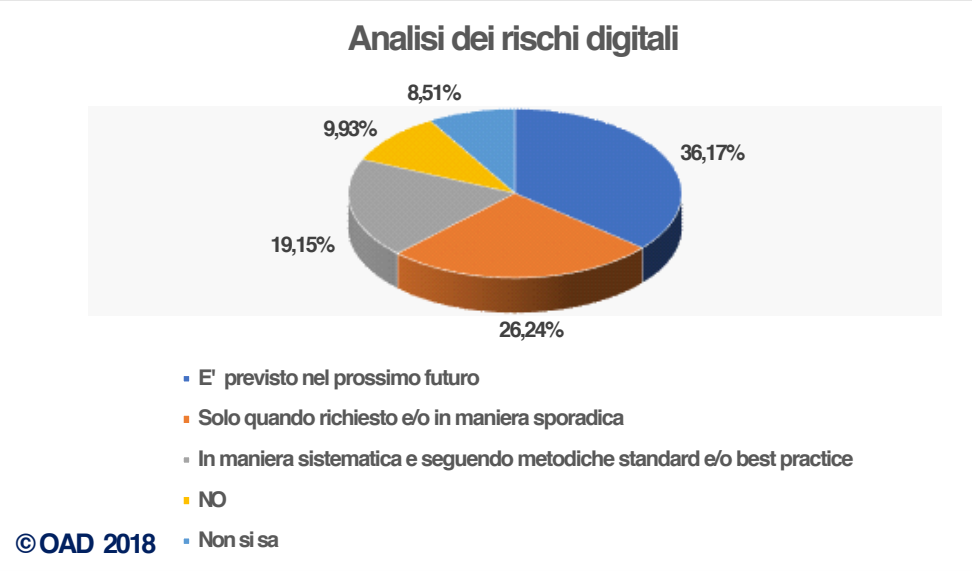

Fig. 9.1.5-1

La fig. 9.1.5-2 evidenzia la sostanziale indipendenza dell'analisi dei rischi dalle dimensioni dell'organizzazione: l'analisi dei rischi, solitamente ritenuta necessaria solo per grandi e grandissime organizzazioni, è effettuata anche da quelle piccole e piccolissime, almeno nell'ambito del bacino dei rispondenti. Occorre puntualizzare la notevole diversità, anche come impegno, tra l'effettuare una analisi dei rischi per piccole o grandi realtà, considerando pure il livello di granularità e dettaglio opportuno. Livello di dettaglio il più delle volte non specificato dalle normative, e ad esempio per il GDPR lasciato alla decisione dei vertici dell'organizzazione e del titolare.

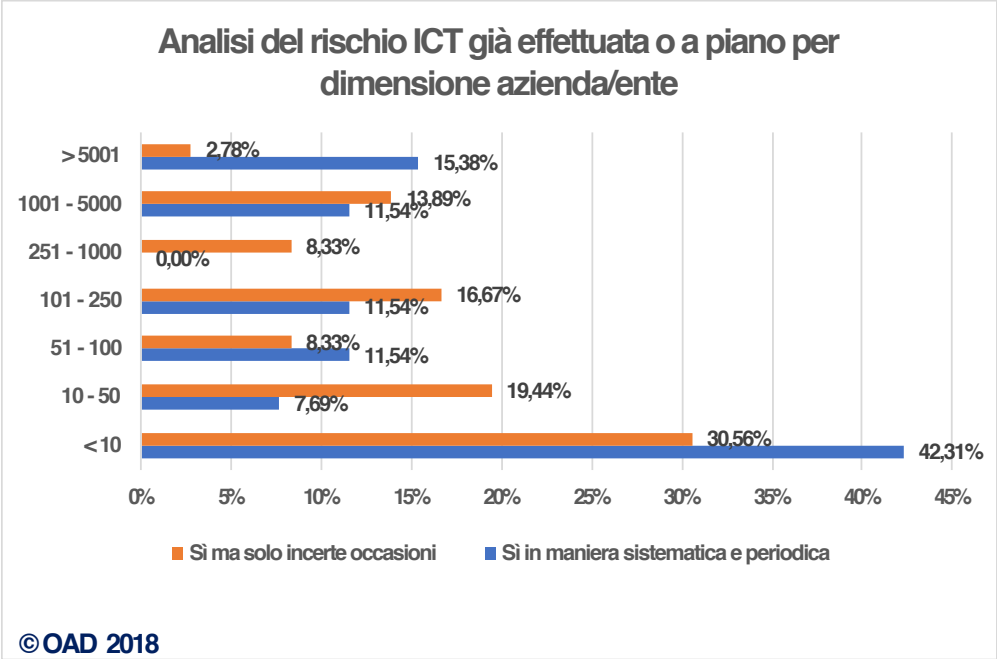

Fig. 9.1.5-2

Il livello di dettaglio dell'analisi dei rischi è determinante quando l'azienda intende assicurare il proprio rischio "residuo", dopo aver implementato le necessarie misure di sicurezza, misure che i tecnici delle assicurazioni ben valutano per individuare il prezzo del premio.

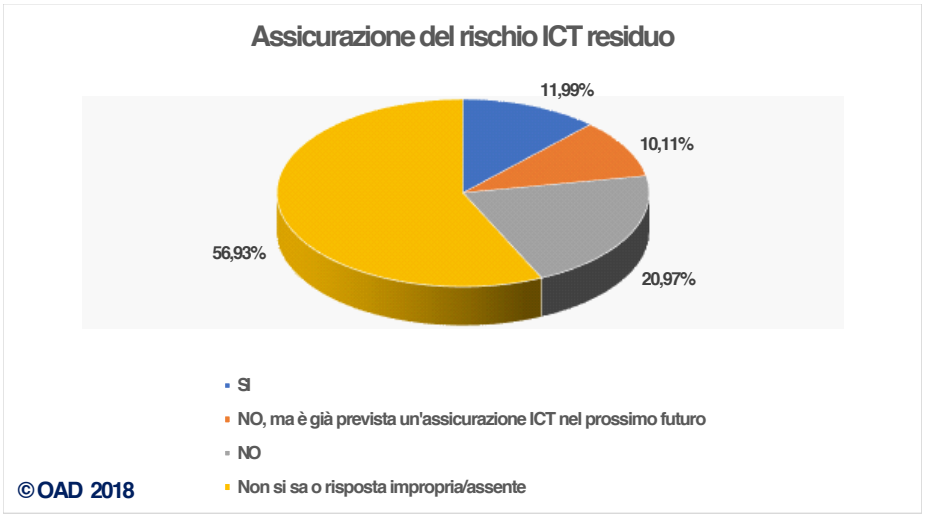

Fig. 9.1.5-3

La fig. 9.1.5-3 mostra che quasi il 12% dei rispondenti ha già in essere una specifica assicurazione per i rischi ICT, mentre il 10% ha a piano di sottoscriverne una.

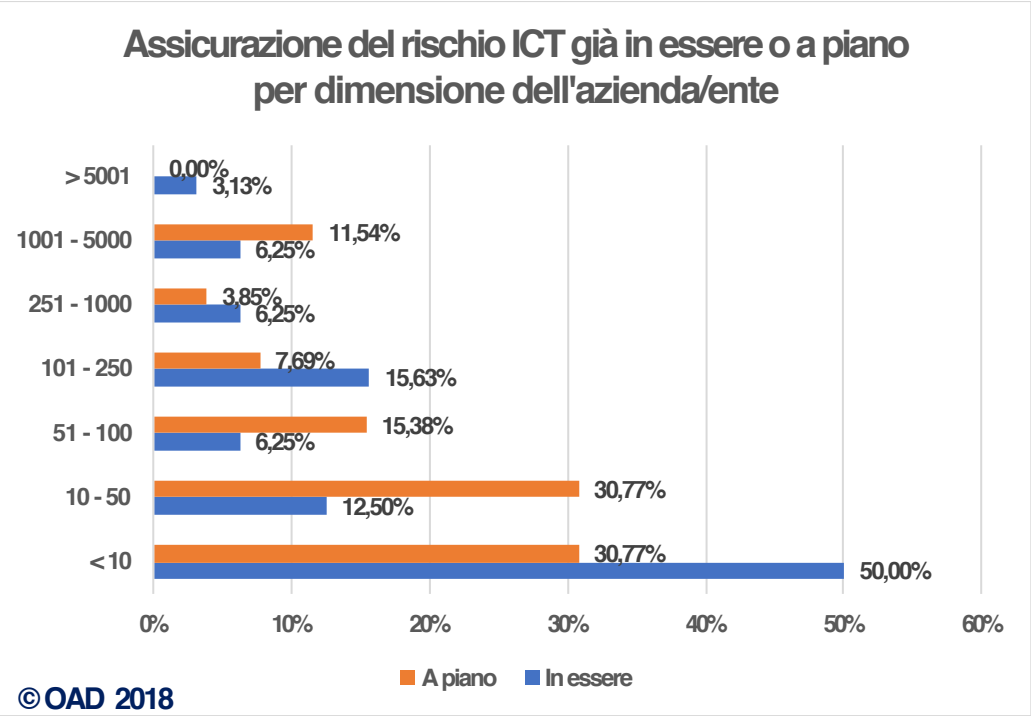

Fig. 9.1.5-4

La fig. 9.1.5-4 mette in relazione le aziende/enti che hanno sottoscritto un'assicurazione del rischio ICT con le loro dimensioni in termini di dipendenti. I dati contraddicono, e alla grande, la comune credenza che le assicurazioni sui rischi ICT siano effettuate, anche per il loro costo, solo da organizzazioni di grandi dimensioni. La figura mostra che proprio le più piccole organizzazioni le hanno adottate, soprattutto nel privato: esse da un alto non hanno grandi capacità finanziarie per far fronte a conteziosi e sanzioni, dall'altro perché è relativamente più facile per loro adottare le misure di sicurezza digitale che un'assicurazione richiede, senza che quest'ultima pretenda premi altissimi, date le piccole dimensioni dei loro sistemi informatici.
Una assicurazione del rischio residuo ICT è inoltre una importante e facile mezzo per contribuire a garantire l'accountability richiesta dal GDPR.

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 42,25% dei rispondenti già effettua auditing per il proprio sistema informatico, e quasi il 9,15% lo ha a piano a breve. Un valore % alto, superiore 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. Una percentuale così alta che non può riguardare solo le grandi organizzazioni: per questo si è analizzata la correlazione tra chi effettua auditing e le sue dimensioni in termini di numero di dipendenti.

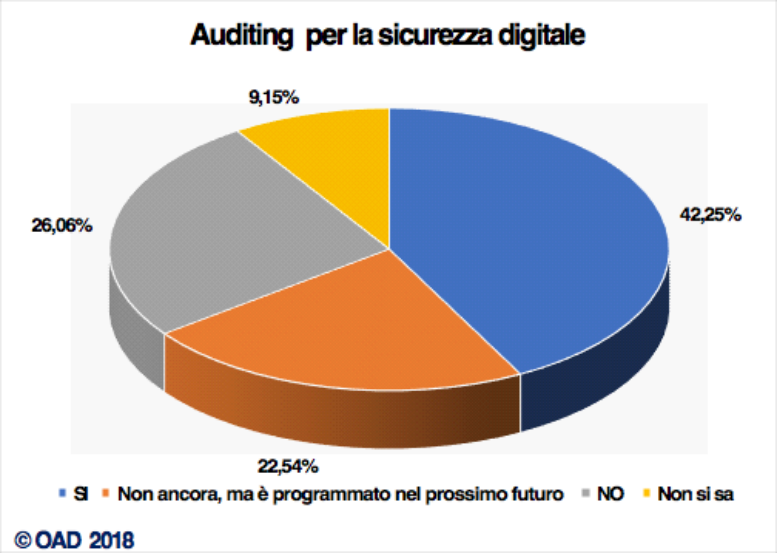

Fig. 9.1.6-1

I risultati sono mostrati nella fig. 9.1.6-2, ed anche per l'auditing, come per l'analisi dei rischi, si sfata la consolidata credenza che venga effettuato solo dalle grandi e grandissimi strutture: lo effettua quasi l'80% delle strutture dei rispondenti con meno di 250 dipendenti, e di questi più della metà dalle piccolissime strutture con meno di 10 dipendenti. Risulta alta anche la percentuale delle piccole-medie organizzazioni che hanno a piano di effettuarlo nel prossimo futuro.

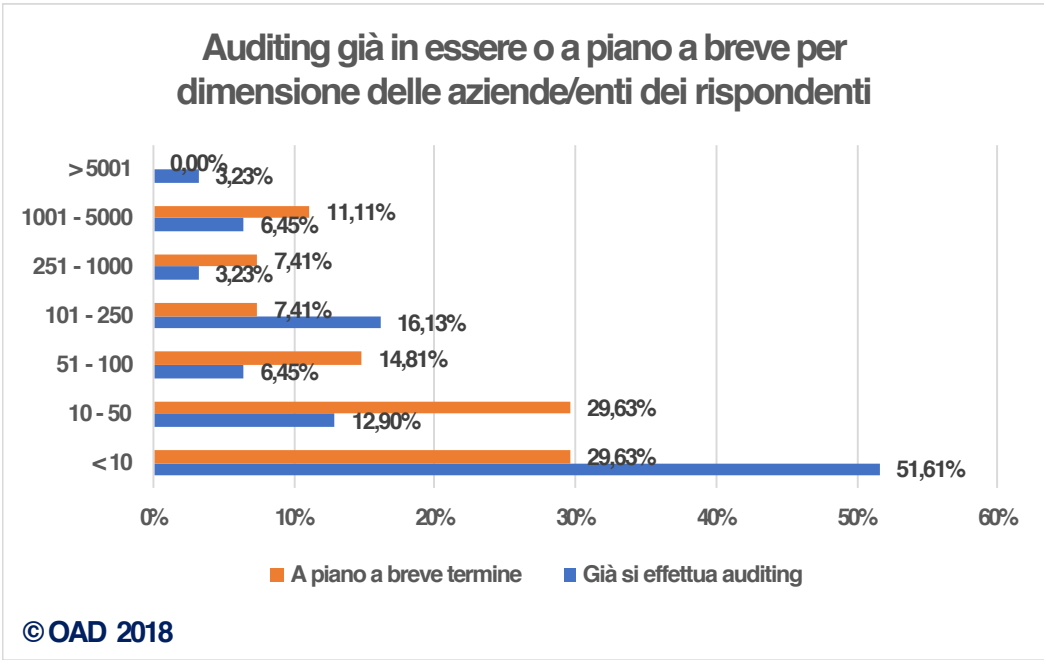

Fig. 9.1.6-2

Per chi già effettua l'auditing sui suoi sistemi informatici, la fig. 9.1.6-3 mostra da chi esso viene effettuato tra personale interno o esterno o da un mix dei due.

Fig. 9.1.6-3

Sempre per chi già effettua l'auditing sui sistemi informatici, la fig. 10.1.6-4 mostra le modalità di effettuazione: la maggioranza, 56,76%, lo effettua in maniera sistematica e periodica o come un processo continuo, come dovrebbe essere, probabilmente anche per poter rinnovare e mantenere le certificazioni quali ad esempio ISO 9001 e ISO 27000 a livello azienda/ente (o per sue specifiche direzioni). Il restante lo effettua in maniera sporadica, ad esempio su richiesta della proprietà/consiglio di amministrazione, oppure dei revisori dei conti, o a seguito di incidenti al sistema informatico.

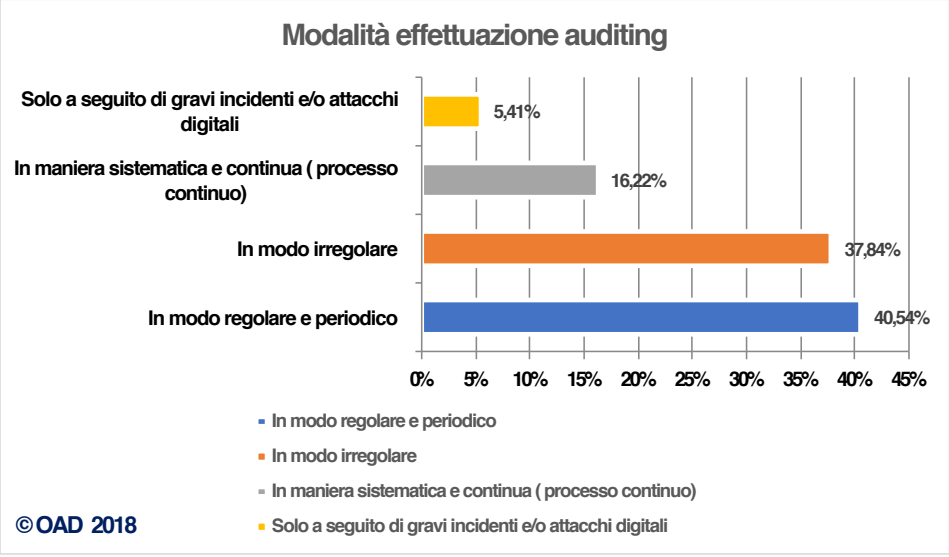

Fig. 9.1.6-4

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 2018 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 capitolo riporta ed analizza nel seguito le risposte avute dai rispondenti in questo stesso ordine logico di raggruppamento delle contromisure attuate o da attuare.

La prima domanda del questionario OAD 2018 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 tecniche 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 un quarto circa dei rispondenti non ha definito alcuna architettura e che un altro quarto circa (sfrondando le risposte molteplici) l'ha definita, pur in modalità diverse: tra queste modalità, in particolare, circa l'8% ha definito una architettura di sicurezza ma che non tiene conto della terziarizzazione di parti del suo sistema informatico.
Come più volte sottolineato, il bacino di rispondenti emersi con l'indagine OAD 2018 si può collocare nella fascia medio alta per livello di sicurezza digitale, pur con una forte percentuale di piccole e piccolissime organizzazioni: ma questi dati indicano come ancora troppo pochi seguano una security by design partendo dal disegno di una architettura con un buon bilanciamento delle varie misure di sicurezza applicate: e la sicurezza digitale è come una catena, tanto forte quanto il suo anello più debole. Solo il 7,58% dei rispondenti ha una architettura ad alta affidabilità con ridondanza delle varie risorse ICT più critiche, e solo il 9,6% basa tale architettura su standard e best practice.

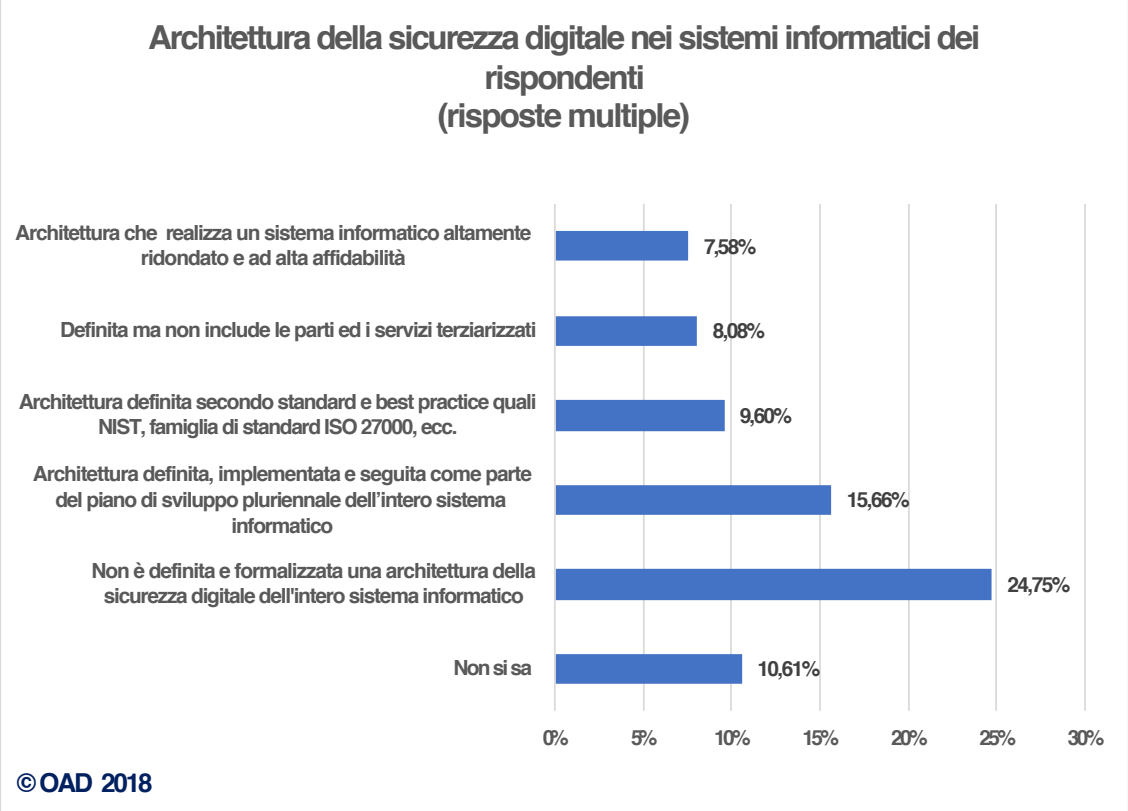

Fig. 9.2-1

Di nuovo un problema di cultura e di competenza, vera, sulla sicurezza digitale, anche da parte dei fornitori e dei consulenti, che in alcuni casi (comunque sempre troppi a giudizio dell'autore) si comportano proprio da truffatori nei confronti dei clienti non competenti in ICT (si veda anche §9.1.4) e sulla sua sicurezza.

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" e in qualsiasi luogo dell'azienda/ente ove si possono trovare. Gli strumenti più usati dal campione emerso sono i sistemi per garantire la continuità elettrica (41,41%), da UPS ad autonomi gruppi di continuità, cui seguono i sistemi di climatizzazione nei locali ove sono concentrate le risorse ICT, e a scalare in percentuale i vari sistemi rilevatori di fumo, gas, umidità, protezioni perimetrali passive e attive, recinzioni anti-scavalcamento, inferiate alle finestre e alle porte, sistemi di allarme antintrusione a radar o a micro onde, videosorveglianza.
Per il 28,28% vengono effettuati controlli degli accessi delle persone fisiche al loro ricevimento (reception) tramite iscrizione in un registro, bussole, lettori di badge, ed altri strumenti, fino al riconoscimento biometrico. Il 26,26% dei sistemi informatici dei rispondenti ha aree dedicate ai sistemi ICT protette solo da porte chiuse a chiave, ed il 12% circa non ha di fatto alcuna misura di sicurezza fisica per i locali ove sono contenuti i sistemi ICT. Con "altro" alcuni rispondenti indicano che, essendo il loro sistema informatico totalmente terziarizzato e in cloud, le misure di sicurezza fisica sono quelle fornite dai Data Center dei fornitori.
Nel complesso le percentuali emerse sulle protezioni fisiche descrivono ambienti fisici relativamente sicuri considerando anche l'incidenza, nelle risposte, della forte quota, l'80% circa, di rispondenti di aziende/

enti di piccole-medie dimensioni, e tra queste ben il 60% è con meno di 50 dipendenti (si vedano fig. B1-2 e B1-3). Tipicamente queste piccole strutture hanno piccoli sistemi informatici, considerati come delle "ICT commodity" e come tali gestite: la parte del sistema informatico locale (on premise) ha poche misure di sicurezza, soprattutto di tipo fisico.

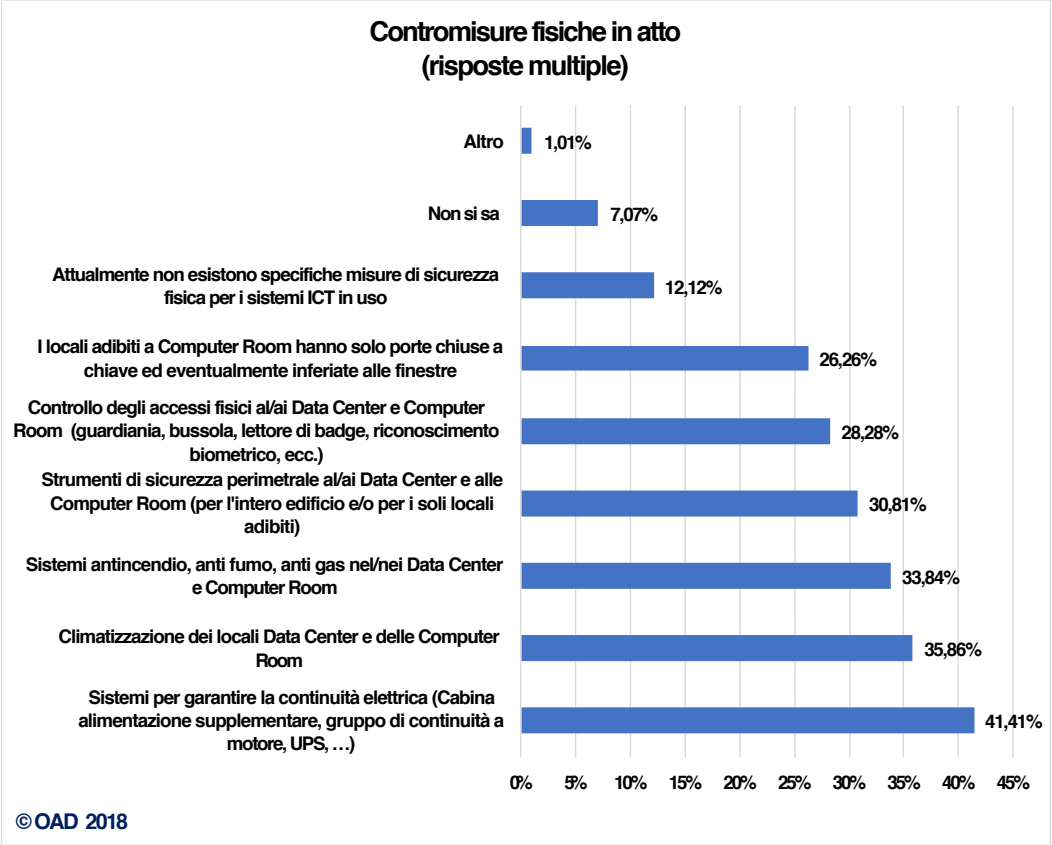

Fig. 9.2-2

Con "altro" alcuni rispondenti hanno specificato che tutto il loro sistema informatico è in cloud, ed il fornitore eroga tutti gli idonei livelli di sicurezza fisica.

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 2017 il più diffuso insieme di attacchi è stato proprio all'ambiente IAA.

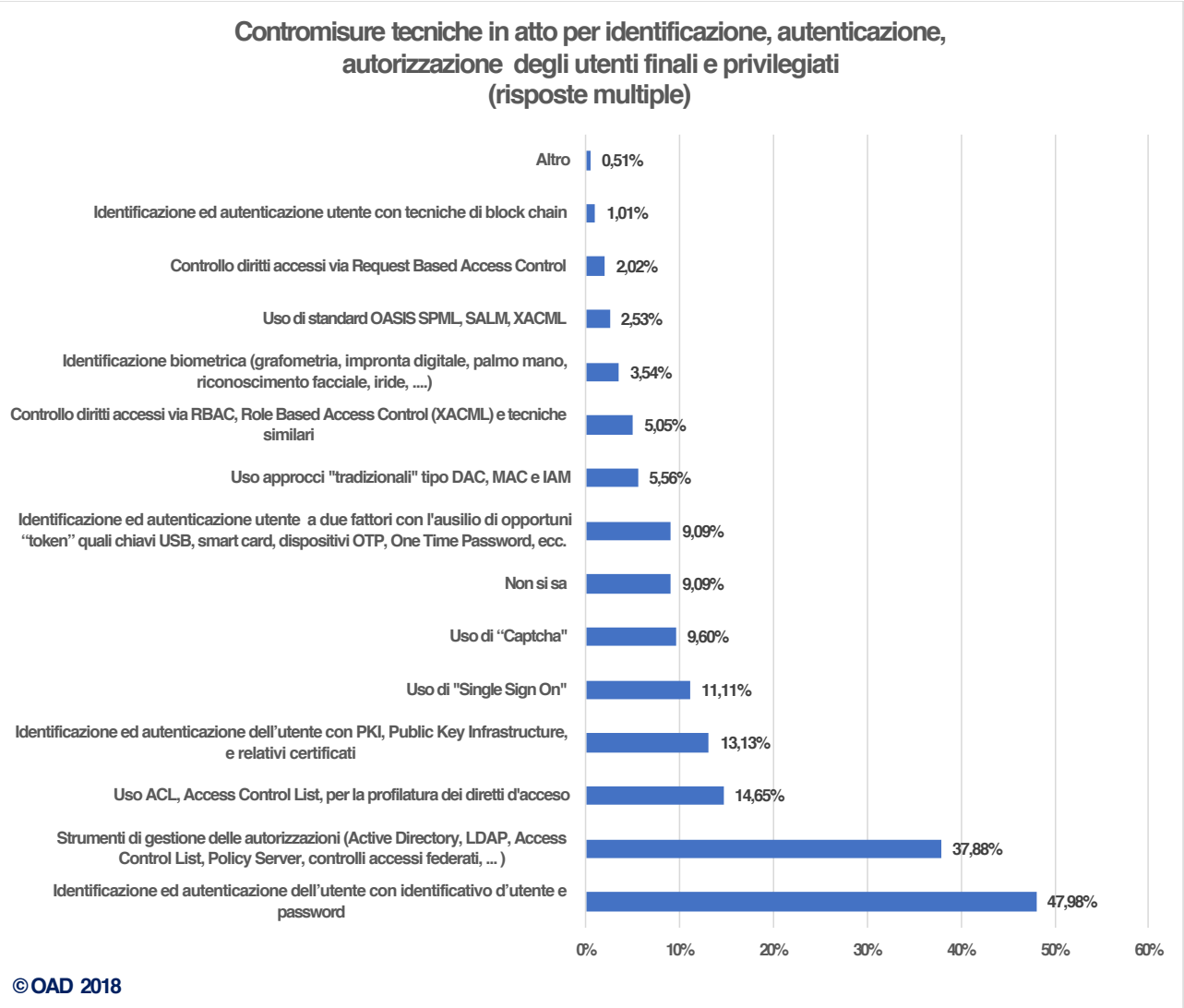

Fig. 9.2-3

La fig. 9.2-3, con risposte multiple, riporta le misure di IAA indicate dai rispondenti: poco meno della metà dei rispondenti fa uso del consueto "account" costituito dalla coppia identificatore utente e password, cui segue, con un 37,88%, l'uso di strumenti di gestione e controllo degli accessi quali i diffusi Active Directory di Microsoft e l'LDAP. Con percentuali assai inferiori, 14,65%, l'uso di elenchi degli utenti abilitati, le ACL, Access Control List, e con un 13,13% l'uso dell'autenticazione forte con certificati digitali, spinta in Italia soprattutto dalla PEC, Posta Elettronica Certificata, e dallo SPID, il sistema unico di login che nella sua forma più forte di autenticazione usa i certificati digitali. L'uso di PKI e certificati è richiesto anche dalle normative delle 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 2018. Come mai? A giudizio dell'autore, molti fattori hanno fino ad oggi contribuito alla non diffusione delle varie tecniche basate sui certificati. Da un lato la complessità organizzativa, una certa difficoltà d'uso per l'utente finale comune (nato "non digitale"), il costo per avere ed utilizzare certificati digitali (ad esempio via smart card con relativo lettore o chiavetta USB), gli unici ad avere validità legale in Italia. Dall'altro, forse, la non cono-

scenza, da parte di molti dei rispondenti, dell'obbligatorietà dell'uso della PEC, obbligatoria da tempo non solo per le Pubbliche Amministrazioni ma anche per le imprese ed i professionisti[15]. Probabile l'ulteriore analoga non conoscenza di SPID. A tutto questo si aggiunge poi l'alta percentuale di piccole e piccolissime organizzazioni rispondenti (si veda §10.2), alcune delle quali, probabilmente, non sono ancora al corrente, dopo sei anni, di tale obbligatorietà; infine, purtroppo, le troppo poche Pubbliche Amministrazioni che hanno risposto al questionario OAD 2018.
Ritornando alla fig. 9.2-3, a decrescere l'uso di SSO, Single Sign One, di Captcha, dell'identificazione ed autenticazione a due fattori, con l'uso, oltre a user-id e password, di un token fisico-logico, ad esempio una chiavetta USB, una smart card, il cellulare per la ricezione di una OTP, One Time Password, assai diffusa per l'home ed il corporate banking.
Seguono le risposte a domande specifiche sulle modalità di autorizzazione, che sono spesso poco conosciute anche dagli addetti ai lavori, all'identificazione biometrica (disponibile soprattutto sui moderni smartphone ma probabilmente nemmeno usata dai proprietari di questi dispositivi), ed infine l'uso di tecniche di autenticazione basate sulla blockchain (è un tipo di PKI per questi aspetti), che iniziano ad essere usate, oltre che per le cripto valute, anche per altri specifici contesti informatici (si rimanda a§6.14). Poche le risposte, dato l'uso ancora embrionale, ma iniziano ad esserci.

Nell'ambito delle contromisure per le reti, la fig. 9.2-4, con risposte multiple, evidenzia che quasi la metà dei rispondenti è dotata di dispositivi firewall e di DMZ, DeMilitarized Zone. Al secondo posto, con circa il 40%, l'uso di VPN, Virtual Private Network, per proteggere le comunicazioni da remoto. Segue, con poco più del 36%, 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 6%, 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 specifici strumenti di monitoraggio e di controllo del comportamento in rete di utenti e programmi.

15 - Si veda la Legge 221/2012 che si affianca alla precedente Legge 2/2009.

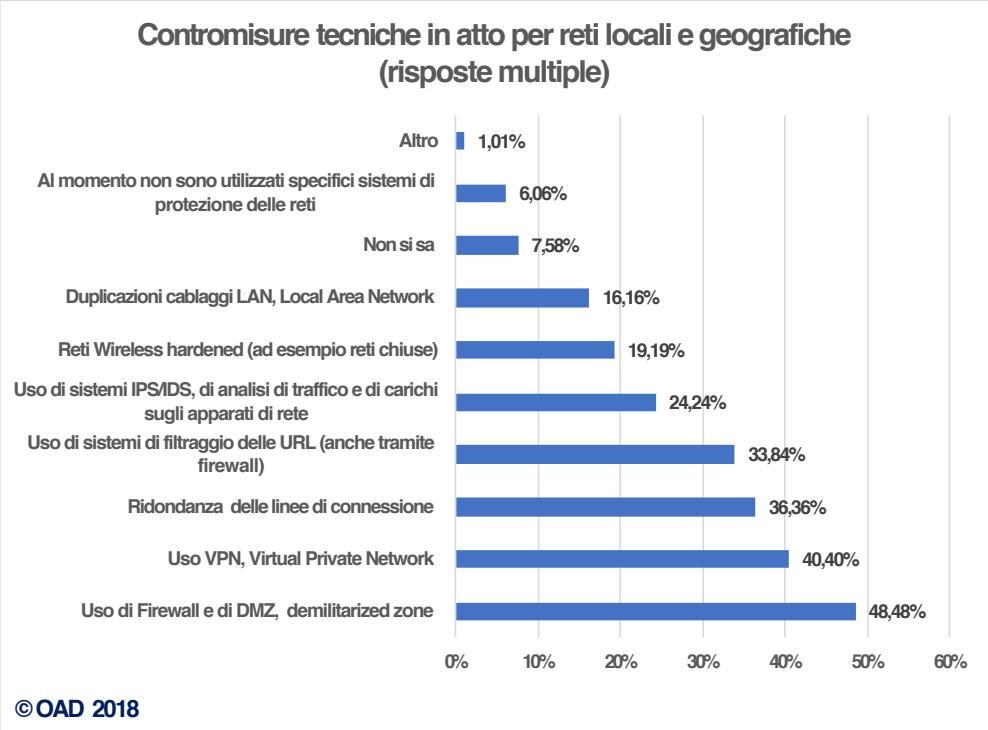

Fig. 9.2-4

Fig. 9.2-5

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, ecc. I sistemi anti-malware sono praticamente usati da tutti (94,46%), seguono a scalare, ma ben sotto la metà dei rispondenti, la virtualizzazione dei sistemi, la gestione delle versioni e delle patch. Non trascurabile la percentuale di rispondenti, 34,34%, 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. Solo qualche sistema ICT dell'intero sistema informatico, visto che, come indicato nella fig. 9.2.1, le architetture complessivamente considerate "ad alta affidabilità" sono dichiarate solo dal 7,58% dei rispondenti.
Quasi 1/3 dei rispondenti raccoglie e gestisce i log degli accessi ai sistemi ICT degli amministratori di sistema: una percentuale molto bassa, dato l'obbligatorietà fin dal 2008 per la disposizione del Garante della Privacy[16], obbligatorietà che continua anche con il GDPR.

Nelle contromisure a livello applicativo, con risposte multiple, emerge l'alta percentuale, 42,42% di rispondenti che dichiarano l'uso di firewall applicativi (FWA), come mostrato in fig. 9.2-6. I FWA sono una buona soluzione per la protezione degli applicativi, ma abbastanza costosa e non semplice da ben configurare, adottata in architetture di sicurezza sofisticate, con segmentazione e "deep security": una così alta percentuale, superiore anche a quella dei FW in fig. 9.2-3, lascia perplesso l'autore, che non vorrebbe che qualche rispondente abbia confuso i firewall di rete con quelli applicativi. Con una percentuale ben minore, 16,67%, 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. Normalmente questo tipo di misure si applicano agli applicativi (o parti di essi) sviluppati ad hoc, e non ai pacchetti di software acquisiti (ad esempio i prodotti Microsoft per PC e per server, gli ERP commerciali, ecc.); ma sarebbe bene effettuare periodicamente dei controlli anche su prodotti applicativi commerciali, soprattutto se non aggiornati con le ultime release.
Sicuramente dovuta all'alta quota di rispondenti di piccole e piccolissime organizzazioni, che tipicamente acquistano applicazioni già presenti sul mercato, anche la bassa (8%) quota di clausole contrattuali sullo sviluppo sicuro di software coi fornitori.

16 - https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1577499

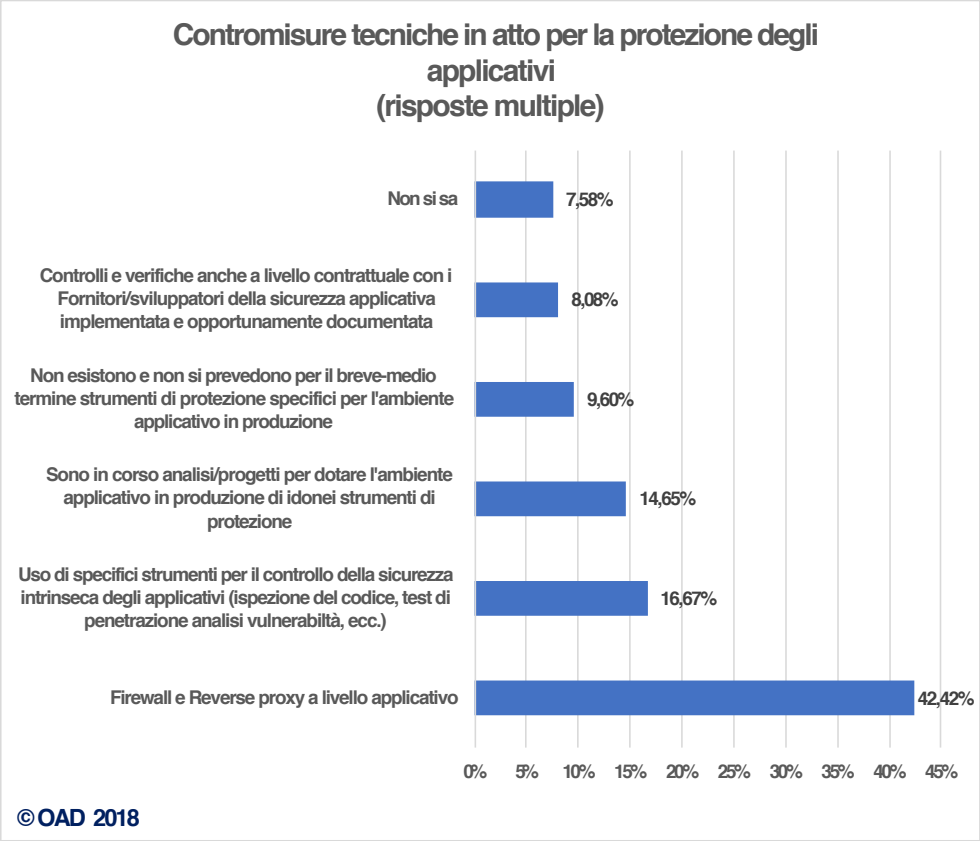

Fig. 9.2-6

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, come nelle edizioni precedenti di OAD-OAD, l'archiviazione sicura dei back up, anche con uso di servizi in cloud (32,32%): i 2/3 rimanenti fanno back up non sicuri, o addirittura non li fanno?

Il secondo strumento più diffuso, con un solo punto percentuale in meno rispetto al precedente, è 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 all'analisi dei rischi digitali sia alla corretta e contestualizzata scelta delle misure di sicurezza. Relativamente basse le percentuali di strumenti per la crittografia dei dati, sia quelli in transito su Internet dei dati (HTTPS, FTPS, VPN, ecc.) con un 26,26%, sia per quelli, più critici, da archiviare, con un 19,7%.

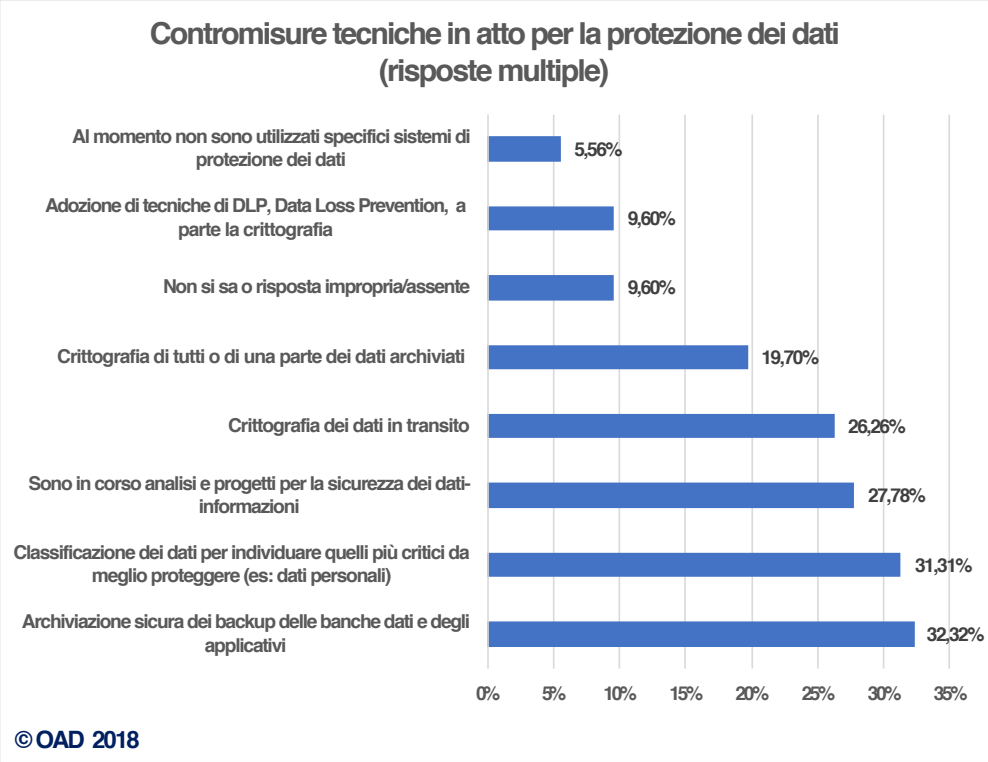

Fig. 9.2-7

Queste percentuali risultano basse nonostante la forte spinta alla crittografia data dal GDPR; ma per quasi il 28% dei rispondenti sono già a piano progetti per una miglior difesa dei dati. Nettamente inferiore la percentuale per l'uso di altri strumenti DLP, Data Loss Prevention, con un 9,6%. Nel complesso, positivamente bassa al 5,56%, la percentuale dei rispondenti che dichiarano che, per ora, non hanno in esercizio specifici strumenti di protezione per i dati.

9.3 - Misure per il governo della sicurezza digitale

Come già anticipato, vari strumenti per la "governance" 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, analizzate in §9.2. L'autore ha voluto evidenziare in un capitolo a sé stante tali strumenti per evidenziarne l'importanza: strumenti determinanti per potere garantire un livello realmente idoneo e proattivo di protezione al sistema informatico nel suo complesso.
Le misure e gli strumenti che sono stati fatti rientrare nell'ambito del governo della sicurezza digitale, e che sono un di cui del più generale governo 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 e di 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 gli strumenti di analisi delle vulnerabilità e di penetrazione (per i penetration test), i sistemi di analisi e di gestione dei

rischi, i sistemi ed i piani per il Disaster Recovery (DR).
La fig. 9.3-1 mostra la diffusione, in %, dei principali strumenti di gestione della sicurezza ICT utilizzati dall'intero campione dei rispondenti, con risposte multiple. Il monitoraggio ed il controllo centralizzato delle funzionalità e delle prestazioni dei sistemi ICT sono gli strumenti più diffusi, cui segue con 2 punti percentuali di differenza il controllo "in locale" anche o solo a livello dei singoli sistemi, tipicamente quando si accorge di o gli viene segnalato un malfunzionamento. dei singoli sistemi.

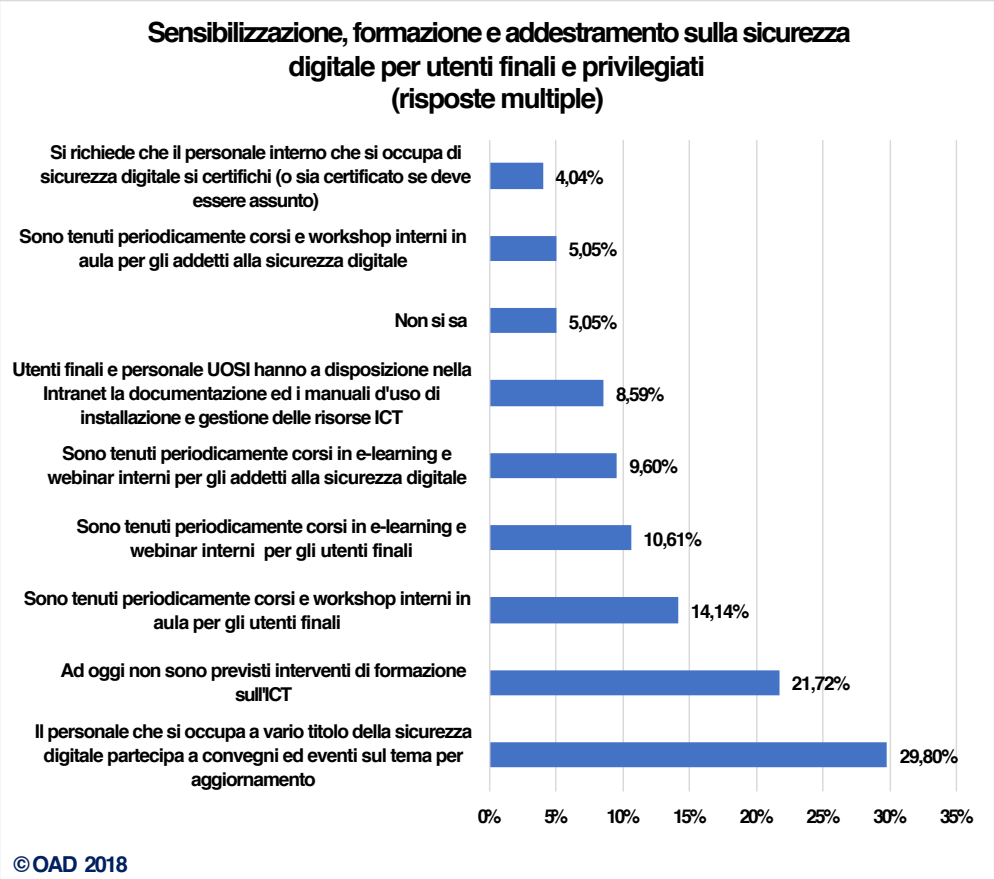

Fig. 9.1.3-1

Al terzo e quarto posto, con un solo punto percentuale di differenza, l'uso di IDS e IPS: data la complessità nell'uso efficace di tali sistemi, la percentuale emersa è relativamente alta. Così come risulta relativamente alta la percentuale, 18% dei rispondenti, sull'uso di sistemi di gestione dei log degli utenti finali, che non è molto distante dal 23,74% nell'uso di sistemi per la gestione dei log degli amministratori di sistema (utenti privilegiati): solo che la prima non è obbligatoria, ma la seconda lo è per la privacy, e fin dal 2008.
Strumenti basati sull'intelligenza artificiale e su sistemi che auto apprendo nel tempo, le learning machine, iniziano a comparire, ma in Italia e nel bacino dei rispondenti ancora in modo embrionale: essi costituiscono la frontiera più innovativa nell'ambito della sicurezza digitale, soprattutto per individuare comportamenti anomali di persone e/o di sistemi, e cercare così di prevenire deterioramenti funzionali ed attacchi. Sono ancora rari nella realtà ICT italiana, ma iniziano ad esserci e ad essere usati.
Strumenti per l'analisi di vulnerabilità sono usati da poco più del 17% dei rispondenti, ma solo l'8,59%,

ossia la metà, usa strumenti per effettuare penetration test. Per approfondimenti sulle risposte avute sul tema dell'analisi e gestioni dei rischi si rimanda a §9.1.5.
Poco più dell'11% dei rispondenti dichiara di avere strumenti per poter attuare il piano di Disaster Recovery, che è l'elemento fondamentale per poter attuare una vera continuità operativa (business continuity) dell'azienda/ente. La fig. 9.3-2, che dettaglia con maggiori particolari come le aziende/enti dei rispondenti affrontano un DR, evidenzia che più di 1/3 dei rispondenti ha un piano di DR.
E' opportuno precisare la differenza tra avere un piano di DR e disporre delle risorse alternative 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. In pratica, come evidenziato dai dati sul DR nelle due figure, solo 1/3 di chi ha un piano di DR ha anche predisposto le risorse tecniche per attuarlo.

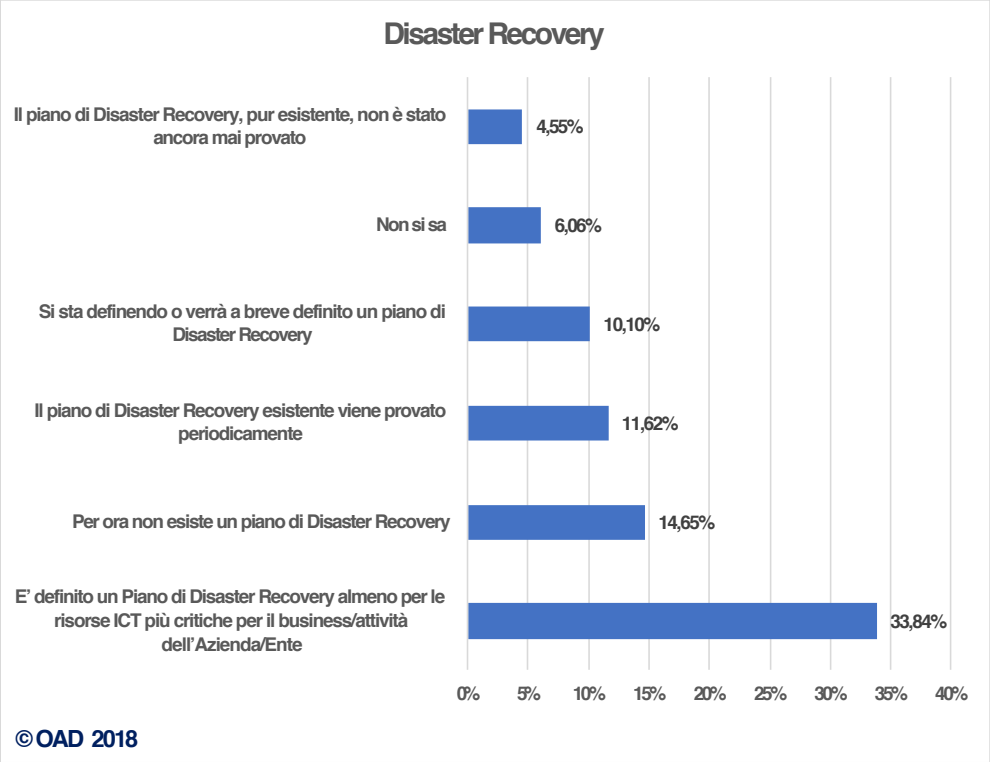

Fig. 9.3-2

Nel complesso i dati emersi evidenziano come il bacino dei rispondenti, pur utilizzando in vari casi specifiche misure e strumenti di sicurezza, anche sofisticati, come indicato in §9.1 e §9.2, 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 (anche a livello individuale, dall'auto al PC).

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

Le risposte avute al questionario OAD 2018 sono state 269.
I potenziali rispondenti sono stati contatti prevalentemente via posta elettronica 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 utenza contattato è costituito prevalentemente da CIO e da figure operanti in 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, come percentuale sul totale dei rispondenti, sono 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) nel bacino complessivo dei rispondenti (fig. 10.1-2 e 3). Con una % di pochissimo inferiore i responsabili dei sistemi informativi (CIO) e al terzo posto, con un 17%, le terze parti, consulenti e fornitori specializzati, cui le aziende/enti delegano, in toto o in parte, la gestione delle misure di sicurezza. Con il 14% il personale interno alla struttura UOSI e con un 12,59% il CTO: è una figura di alto livello tipica delle industrie manifatturiere e di quelle ICT che realizzano prodotti e servizi. Questa relativamente alta percentuale è data dall'alto numero di rispondenti dei settori manifatturiero ed ICT. Solo con un 5,19% i responsabili della sicurezza informatica (CISO), con tale ruolo definito nell'organigramma, e che dovrebbero essere i tipici rispondenti del questionario OAD.

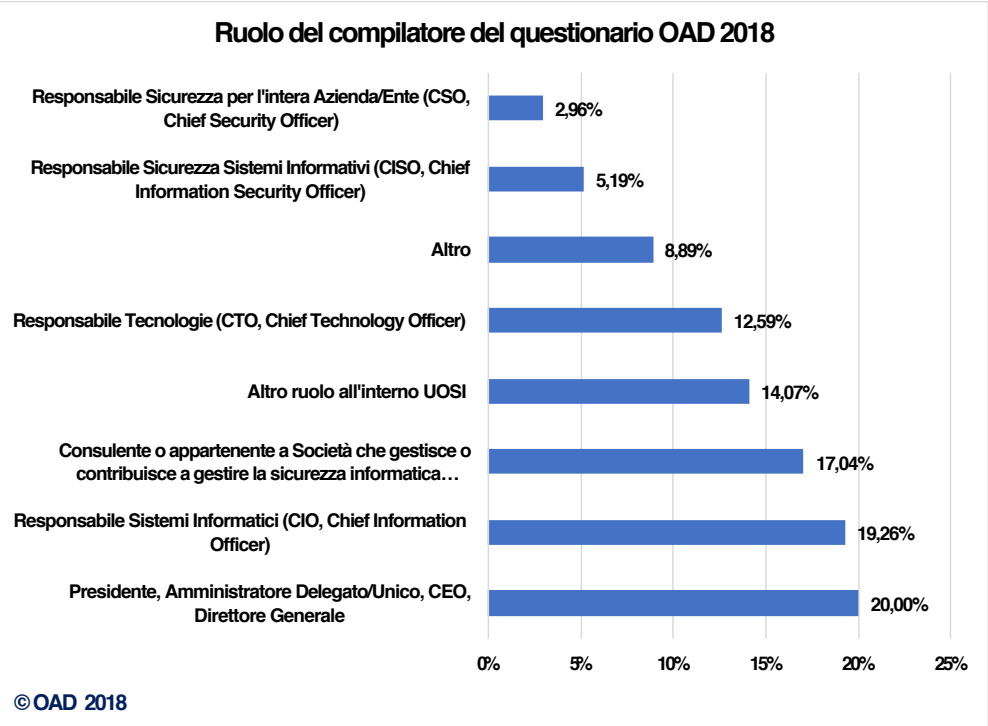

Fig. 10.1-1

La bassa percentuale di CISO rispondenti è un indicatore di come questo ruolo manchi in gran parte delle aziende/enti in Italia, anche nelle organizzazioni di grandi dimensioni. Inoltre, per le strutture italiane di multinazionali con quartier generale all'estero, il CISO è normalmente operante nel quartier generale. All'ultimo posto, con circa il 3%, il CSO, 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" alcuni rispondenti hanno specificato per il loro ruolo quello di responsabili commerciali[17], quello di riferente ICT in altre direzioni e business unit dell'azienda/ente, quello di referente della qualità, quello di responsabile della privacy, per alcuni enti sanitari quello di tecnico di radiologia.

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.
La fig. 10.2-2 mostra la ripartizione merceologica delle aziende/enti dei rispondenti secondo questa classificazione, ritenuta utile per ridurre possibili errori di posizionamento della loro azienda da parte dei rispondenti.

17 - 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, ecc. (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, ecc (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, ecc. (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, ecc. (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, ecc. (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

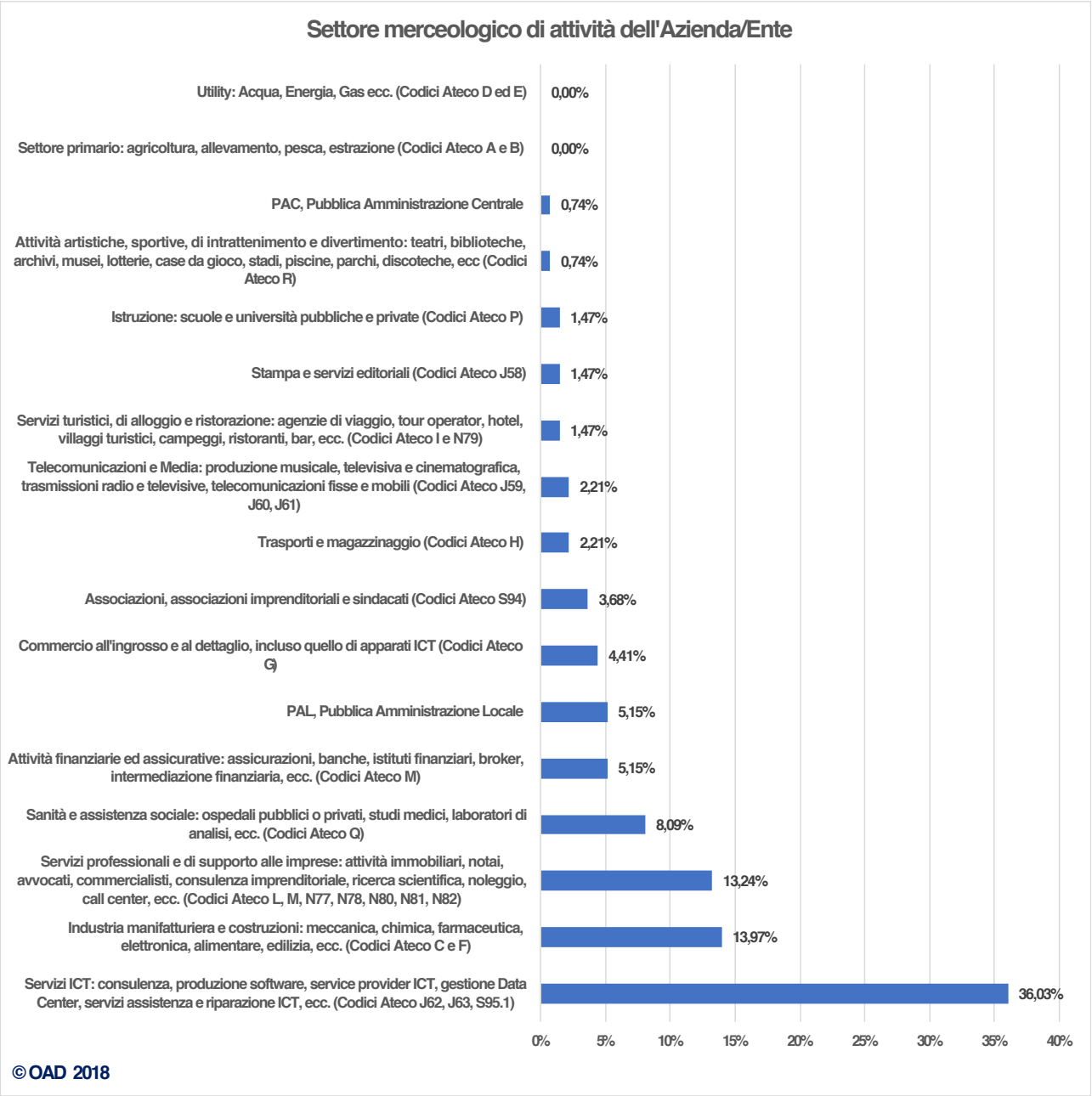

Fig. 10.2-2

Questa fig. 10.2-2 evidenzia come la maggior parte delle aziende dei rispondenti appartenga al settore ICT, il 36% circa, cui seguono con poco più del 13% ciascuno, l'industria manifatturiera e costruzioni insieme ai servizi professionali e di supporto alle imprese; quest'ultimo settore include professionisti come avvocati e commercialisti. Al quarto posto, con un 8%, la sanità e assistenza sociale. Tutti gli altri settori merceologici hanno avuto dei rispondenti, ma con percentuali dal 5% in giù, troppo basse per poter effettuare analisi per e correlazioni per questi settori.
In questa edizione sono totalmente mancati rispondenti per il settore primario e per quello delle utility.

La fig. 10.2-3 mostra la ripartizione percentuale delle aziende/enti dei rispondenti per dimensioni, in termi-

ni di numero di dipendenti, distinguendo in quattro classi quelle fino a 250 dipendenti, che raggruppano quasi l'80% dei rispondenti; altre 3 classi per le grandi e grandissime. La maggior parte, 37,5%, appartiene a strutture fino a 10 dipendenti, spesso indicate nel testo del presente Rapporto come "piccolissime". La distribuzione per dimensione delle aziende/enti del campione emerso risulta abbastanza ben bilanciato e rappresentativo delle varie classi considerate in riferimento alle già citate e più recenti statistiche ISTAT (§6 e fig. 6-4) sulle imprese attive, che forniscono il numero di imprese attive per dimensioni:

- Fino a 9 dipendenti: 4.180.870
- Da 10 a 49: 184.098
- Da 50 a 249: 22.156
- 250 e più: 3.787.

Per le Pubbliche Amministrazioni, centrali e locali, la stima è di più di 55.000 enti, con autonomia funzionale e finanziaria, incluse scuole, ASL ed ospedali.

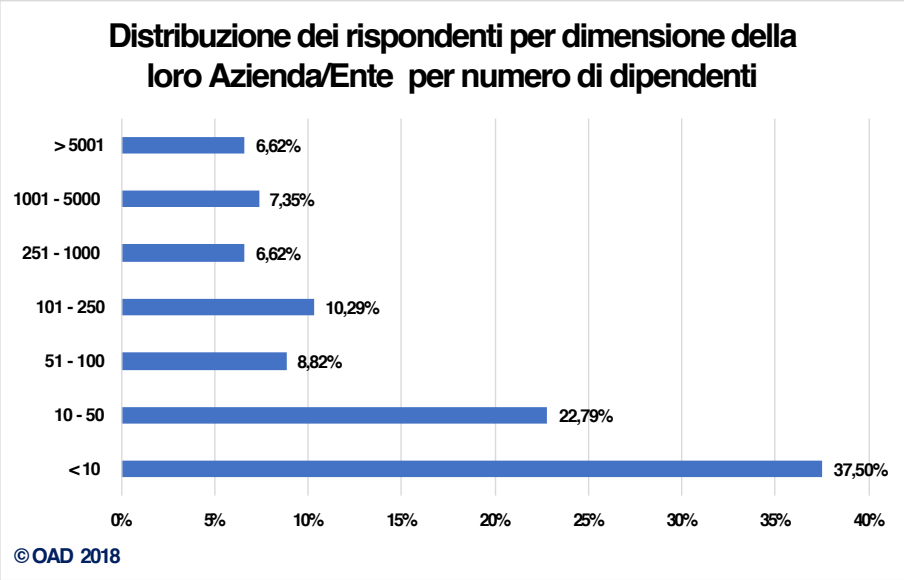

Fig. 10.2-3

La fig. 10.2-4 mostra la ripartizione percentuale delle aziende/enti dei rispondenti per il fatturato annuo nell'ultimo anno disponibile.

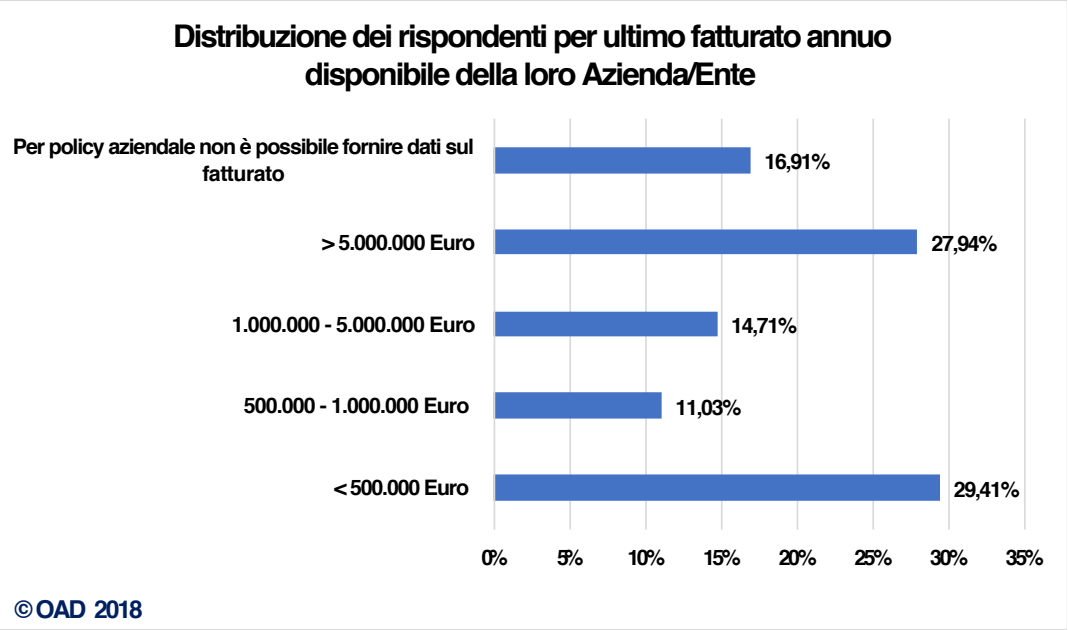

Fig. 10.2-4

Il questionario 2018 prevedeva quattro classi di fatturato: 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 anche 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. Da sottolineare che un numero non piccolo di rispondenti non ha fornito una risposta sulla classe di fatturato cui appartiene la sua azienda/ente, affermando che le policy di riservatezza dell'azienda gli impedivano anche di indicare una classe di fatturato.

La fig. 10.2-5 mostra la distribuzione dell'azienda/ente del dipendente per area geografica di copertura: la stragrande maggioranza opera in Italia, e di questi il 30% circa nel solo nord Italia e poco meno del 15% copre l'intera Italia.

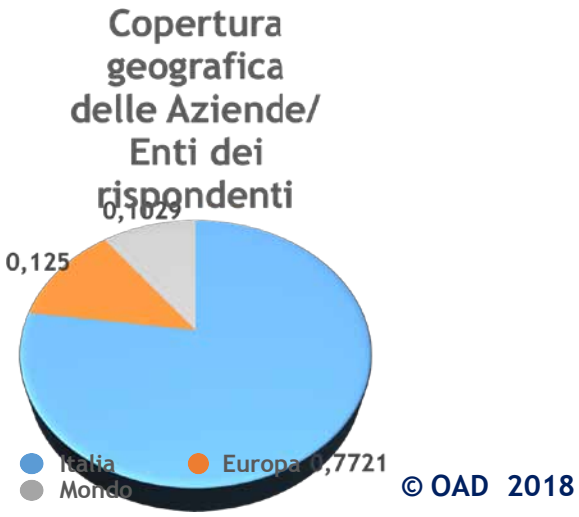

Fig. 10.2-5

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 a questa prima domanda: e se alcuni dei rispondenti non hanno millantato credito, poco mendo della metà dei rispondenti ha posto le risorse ICT più critiche in alta affidabilità al 99%. Quasi il 20% ha un piano di business continuity, e quindi deve avere anche un piano di DR: questa percentuale è congruente con le risposte avute per il DR, si veda fig. 9.3-2.
Un quarto dei rispondenti dichiara che buona parte dei processi per la gestione del sistema informatico e della sua sicurezza sono automatizzati: da un lato questo dato evidenzia come la maggior parte dei sistemi ICT sia ancora "gestita manualmente", unità per unità, ed è comunque una risposta ragionevole, data l'alta percentuale di piccolissime organizzazioni rispondenti; d'altro è un indicatore che le organizzazioni più grandi rispondenti appartengono alla fascia medio alta in termini di governance e di sicurezza del sistema informatico. Sempre ¼ circa 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, ma una percentuale leggermente maggiore, ma una percentuale leggermente maggiore deve arrestarlo, o arrestare sue parti per poter effettuare manutenzione ordinaria dell'hardware e/o del software. Il 21,32% deve fermare l'intero sistema informatico o sue parti per manutenzione della fornitura elettrica.

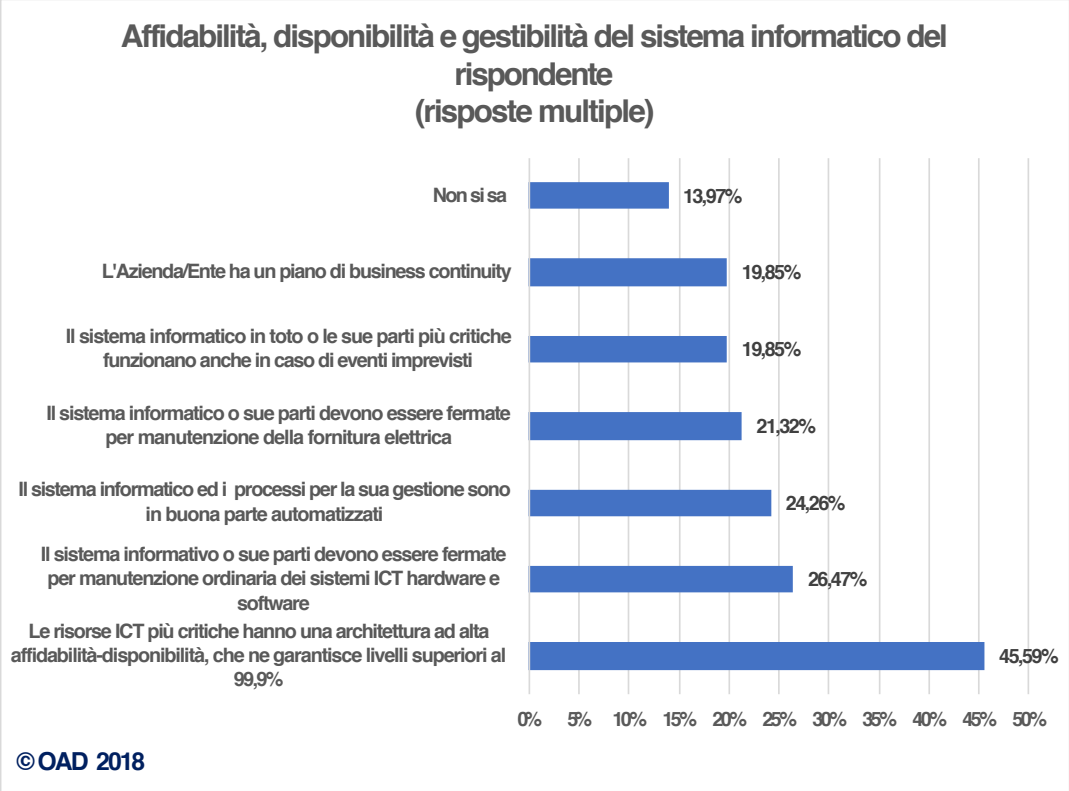

Fig. 10.3-1

La fig. 10.3-2 mostra in percentuale il numero di server, sia fisici che virtuali, presenti nei vari ambienti di produzione, di test e di sviluppo. I dati emersi sono congruenti con le percentuali di distribuzione delle aziende/enti di rispondenti per numero di dipendenti: più della metà rientra nella classe fino a 10 server, tipica configurazione di sistemi informatici delle piccole e piccolissime organizzazioni.

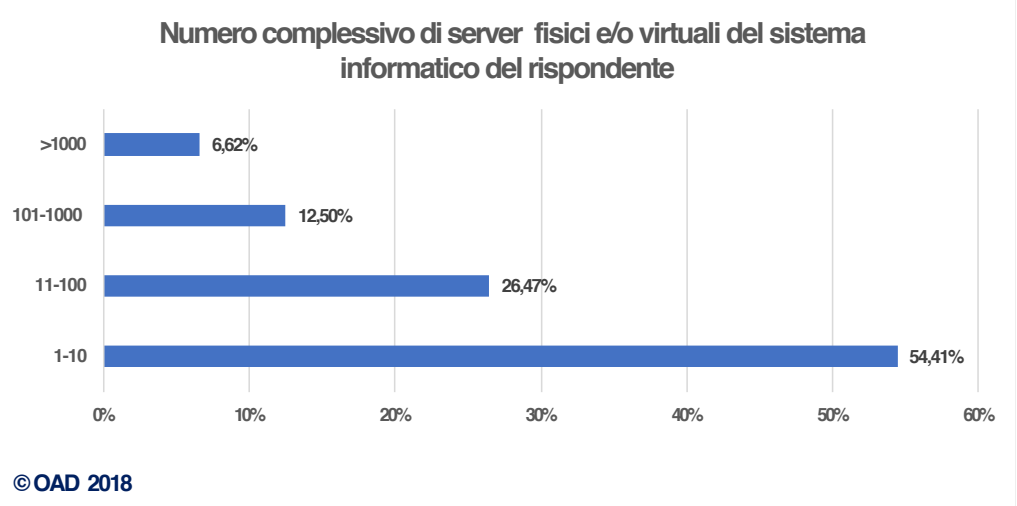

Fig. 10.3-2

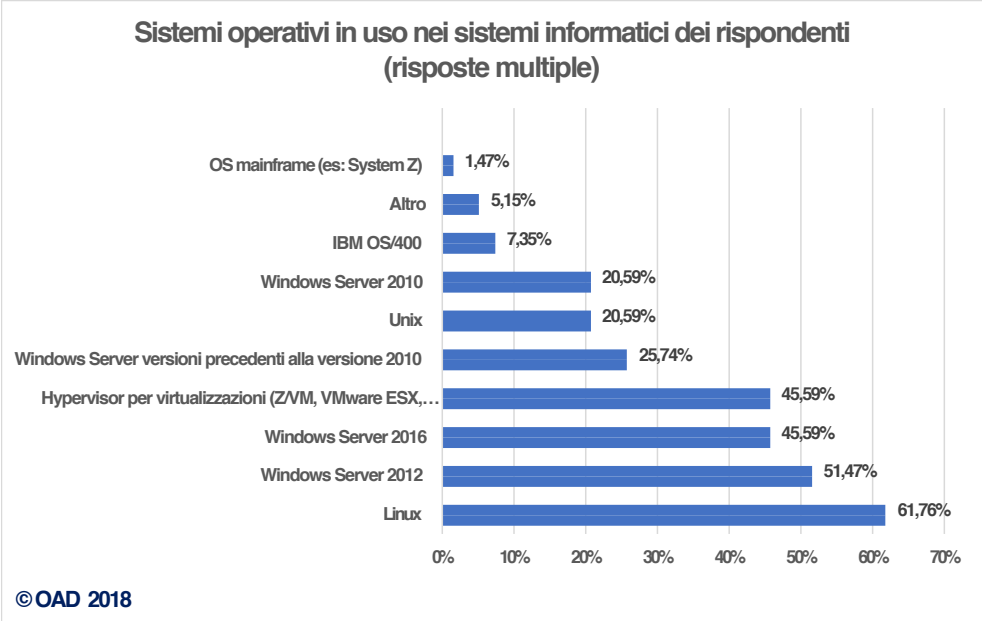

Fig. 10.3-3

La fig. 10.3-3 caratterizza questi server per il sistema operativo: la figura evidenzia la prevalente ripartizione tra l'ambiente Windows di Microsoft, proprietario, e l'ambiente open source di Linux. Significativo che poco meno di 1/3 dei rispondenti utilizza vari tipi di hypervisor per la virtualizzazione dei server. Una piccola quota del 7,35% utilizza sistemi IBM AS400, assai diffusi nelle medie imprese italiane, soprattutto nel passato, e nella voce "altro" sono stati indicati soprattutto sistemi MAC di Apple, diffusi negli studi professionali italiani.

La fig. 10.3-4 mostra la distribuzione percentuale del numero di posti di lavoro fissi, prevalentemente PC, per sistema informatico dei rispondenti: la maggior parte entro i 10 posti lavori, al crescere le percentuali diminuisco: esse sono congruenti con la distribuzione delle aziende/enti per numero di dipendenti, dove il 37,5% è entro i 10 dipendenti.

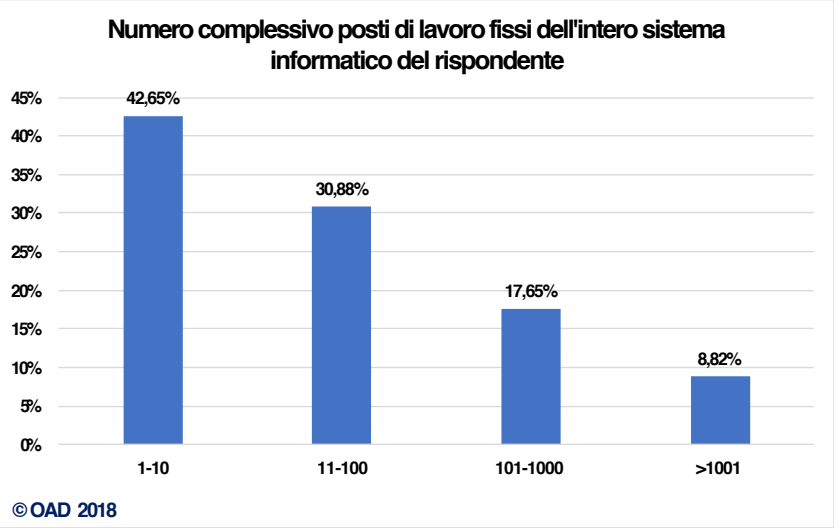

Fig. 10.3-4

La fig.10.3-5 traccia la situazione sui dispositivi d'utente mobili, smartphone e tablet in particolare, di proprietà delle aziende/enti dei rispondenti. La distribuzione % è proporzionale, come per i precedenti grafici, al numero di dipendenti. Interessante evidenziare come poco più del 2% delle aziende/enti non fornisce dispositivi d'utente mobili ai dipendenti, non avendoli di proprietà.

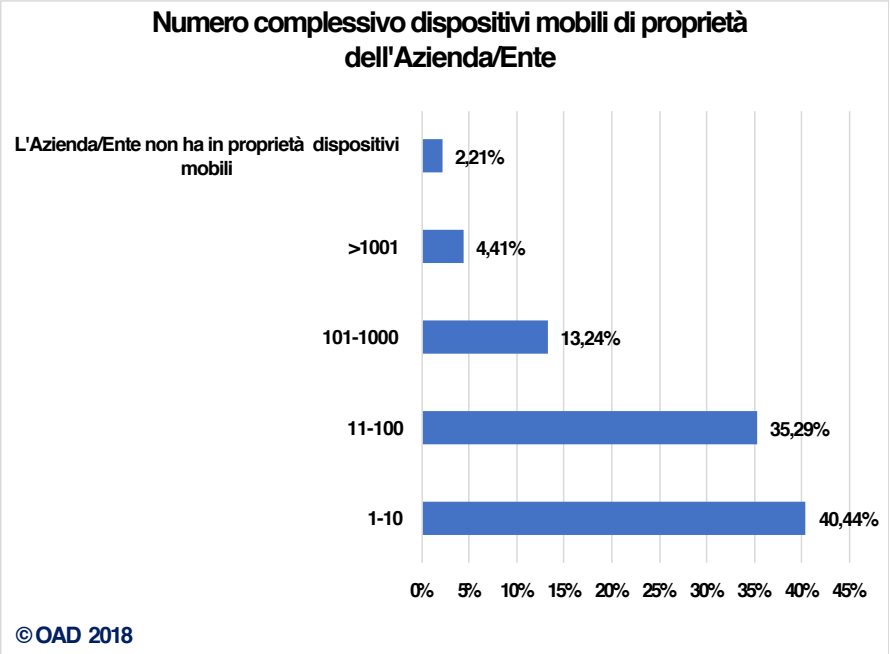

Fig. 10.3-5

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 mostra la situazione nel bacino emerso dei rispondenti. Il 40,30% dei rispondenti non attua alcuna terziarizzazione, mentre quasi 1/3 utilizza per una parte dei suoi sistemi housing e/o hosting. Percentuali inferiori nell'utilizzo di servizi in cloud, i più usati dei quali sono IaaS, cui seguono, decrescendo in %, SaaS e PaaS. Interessante evidenziare che poco più del 8% dei rispondenti ha già terziarizzato la gestione del proprio sistema informatico e della sua sicurezza.

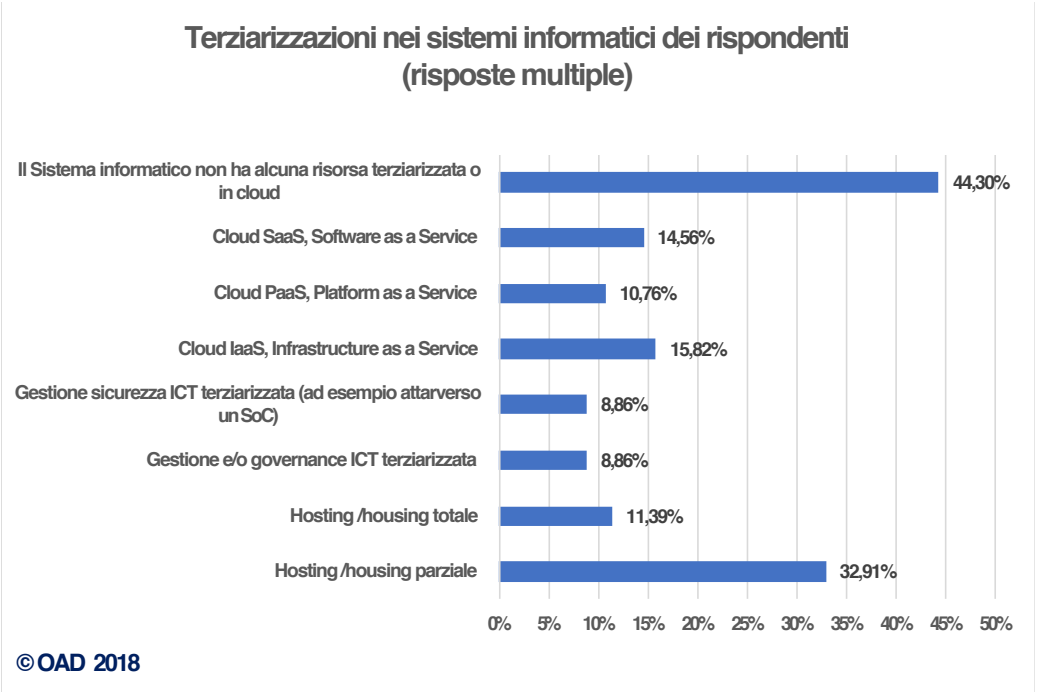

Fig. 10.3-6

Molte aziende italiane, soprattutto del settore manifatturiero e delle utility, ma anche Pubbliche Amministrazioni, per il controllo del territorio e delle smart city, utilizzano sistemi di automazione, di robotica e sistemi IoT. Sistemi di automazione industriale e IoT sono tutti oggigiorno basati sull'ICT e che al loro interno hanno una o più CPU spesso dello stesso tipo di quelle in uso nei PC, e quindi come ultime attaccabili. Anche a seguito dei famosi attacchi STUXNET[18] ai sistemi di controllo delle centrali nucleari iraniane, e ad altri simili, che non hanno però avuto il medesimo clamore mediatico, la sicurezza digitale per questi ambienti è divenuta un problema crescente, ed ha assunto particolare rilievo per i sistemi di automazione e controllo dei processi produttivi e di robotica, oltre che dell'IoT. Per questo motivo il questionario OAD 2018, 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, sintetizza le risposte ricevute su automazione del controllo industriale e sulla robotica, che oggi è sempre più applicata in diversi campi oltre a quello dell'automazione industriale, come ad esempio nella gestione degli archivi cartacei e dei magazzini, nelle sale operatorie degli ospedali, nei trasporti, nella logistica. Congruentemente con la fig. 6.13-1, i rispondenti che non hanno robot ed automazione industriale sono complessivamente circa il 73%: di questi il 58,97% non utilizza robot ed 1/3 non utilizza sistemi di controllo ed automazione industriali (risposte multiple).

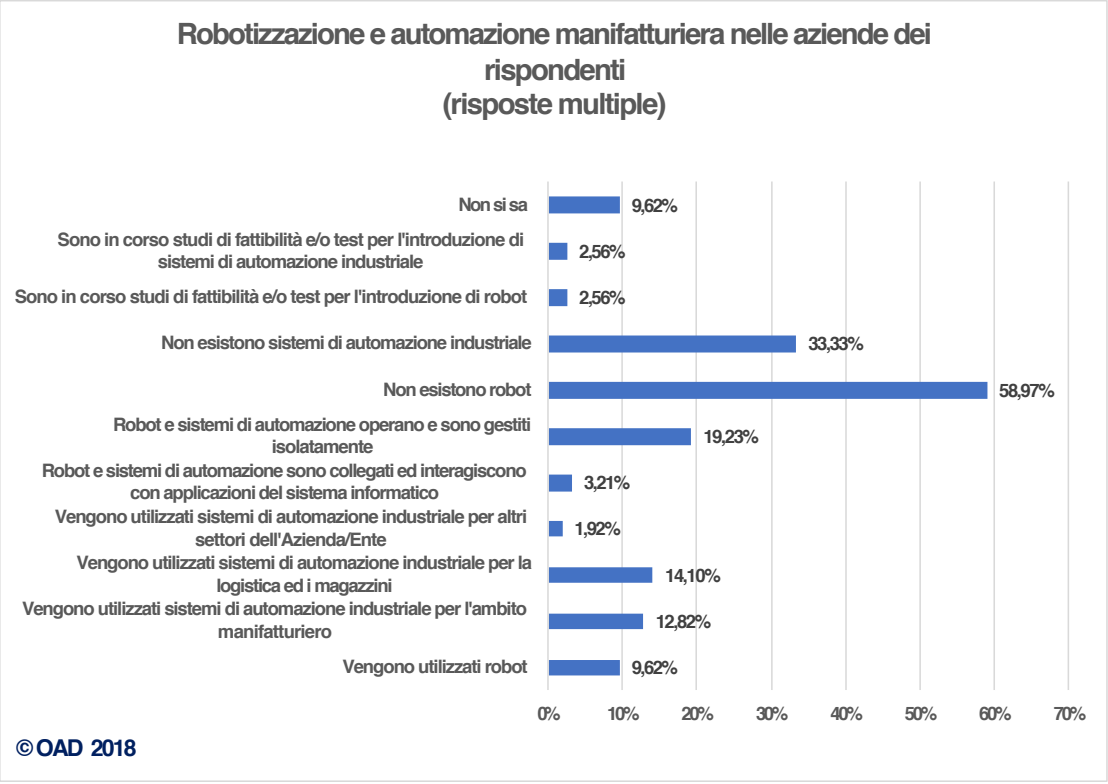

Fig. 10.3-7

18 - Uno dei primi attacchi conosciuti di tipo APT sferrati dal governo USA con quello israeliano nel 2006 contro l'Iran, e basato su un sofisticato malware che attaccava i sistemi PLC di controllo e gestione delle centrifughe delle centrali atomiche.

Molte aziende italiane, soprattutto del settore manifatturiero e delle utility, ma anche Pubbliche Amministrazioni, per il controllo del territorio e delle smart city, utilizzano sistemi di automazione, di robotica e sistemi IoT. Sistemi di automazione industriale e IoT sono tutti oggigiorno basati sull'ICT e che al loro interno hanno una o più CPU spesso dello stesso tipo di quelle in uso nei PC, e quindi come ultime attaccabili. Anche a seguito dei famosi attacchi STUXNET ai sistemi di controllo delle centrali nucleari iraniane, e ad altri simili, che non hanno però avuto il medesimo clamore mediatico, la sicurezza digitale per questi ambienti è divenuta un problema crescente, ed ha assunto particolare rilievo per i sistemi di automazione e controllo dei processi produttivi e di robotica, oltre che dell'IoT. Per questo motivo il questionario OAD 2018, 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, sintetizza le risposte ricevute su automazione del controllo industriale e sulla robotica, che oggi è sempre più applicata in diversi campi oltre a quello dell'automazione industriale, come ad esempio nella gestione degli archivi cartacei e dei magazzini, nelle sale operatorie degli ospedali, nei trasporti, nella logistica. Congruentemente con la fig. 6.13-1, i rispondenti che non hanno robot ed automazione industriale sono complessivamente circa il 73%: di questi il 58,97% non utilizza robot ed 1/3 non utilizza sistemi di controllo ed automazione industriali (risposte multiple).

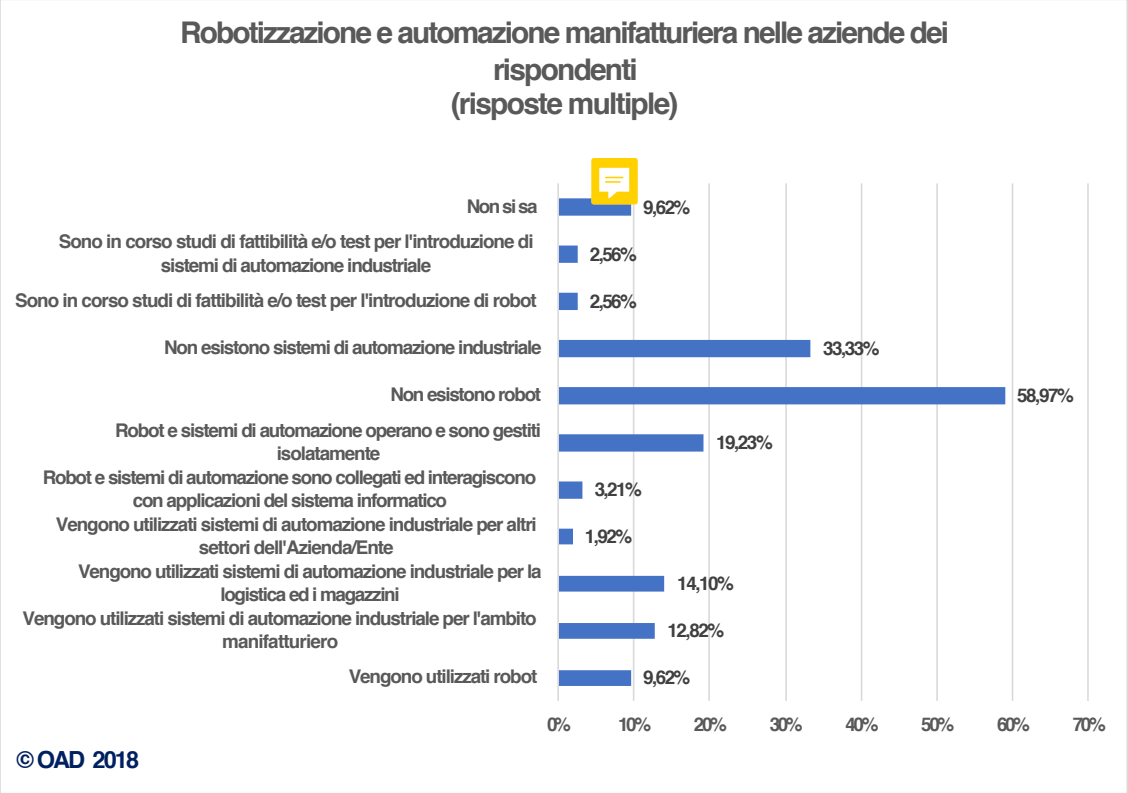

Fig. 10.3-7

Il questionario poneva domande specifiche sull'uso dell'automazione industriale e dei robot, e sulla loro interoperabilità con il sistema informatico aziendale: le poche risposte raccolte sono evidenziate in figura. Relativamente alta la percentuale dei "non si sa", che si avvicina al 10%, ma giustificabile e una conferma della correttezza e serietà dei rispondenti, che avvalora la credibilità delle risposte date, e di conseguenza dell'intero rapporto: tale percentuale alta trova la sua spiegazione in quanto i sistemi informatici di con-

trollo della produzione (e/o di processi chimici, nucleari, dei magazzini, ecc.) sono sovente 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, operante in UOSI, non conosca neppure la loro esistenza.
La fig. 10.3-8 mostra la ripartizione per settore merceologico dei rispondenti che hanno dichiarato di disporre di sistemi di automazione industriale e di robotica. Data la maggioranza di rispondenti del settore ICT, la maggior % è di questo settore. Al secondo posto, quasi ovviamente, i rispondenti del settore manifatturiero. Percentuali non trascurabili per commercio all'ingrosso e trasporti, dato che molta automazione e robotica è applicata nella logistica e nel magazzinaggio.

La fig. 10.3-9 con risposte multiple, sintetizza le risposte ricevute sull'IoT, congruenti con quanto rilevato sugli attacchi in §6.12. La maggioranza dei rispondenti, 68,18% non usa, gestisce o produce sistemi IoT. Per il restante che li usa, il 14,29% li usa all'interno dei propri sistemi di automazione industriale, il 11,69 li gestisce, ma gli IoT sono operanti all'esterno dall'azienda/ente: tipico il caso per il controllo di territori. Interessante che quasi il 6% dei rispondenti, appartenenti a fornitori di ICT, li produce anche. Per i "non si sa" valgono le medesime considerazioni per la precedente figura.

Per la prima volta nella storia decennale dell'indagine OAD-OAI, per l'edizione 2018 vengono considerate le tecniche di blockchain, considerate anche come un possibile specifico target di attacco, e come tale classificate come una specifica tipologia di attacco (si veda §6.14). Sono tecnologie usate, almeno in Italia, ancora in logica prevalentemente sperimentale, come la fig. 10.3-10 mostra, con risposte multiple. In maniera congruente con la fig. 6.14-1, il 24,34 dei rispondenti già utilizza e/o sperimenta queste tecniche: una percentuale abbastanza alta, ma con più del 13% di tutti i rispondenti, quindi più della metà di chi la usa, che afferma di sperimentare queste tecniche sia tecnicamente che funzionalmente per verificare se usarle oppure no. Poco meno del 5% del totale dei rispondenti sta usando servizi ICT basati su blockchain forniti dall'esterno; quasi il 4% del totale sta facendo analisi e studi di fattibilità. L'autore si sarebbe aspettato percentuali più basse: la blockchain è invece già seriamente considerata per varie applicazioni ed ambiti: in primis banche ed istituti finanziari, seguiti da logistica e trasporto, sistemi di prenotazione, sistemi di gestione IoT, e così via.

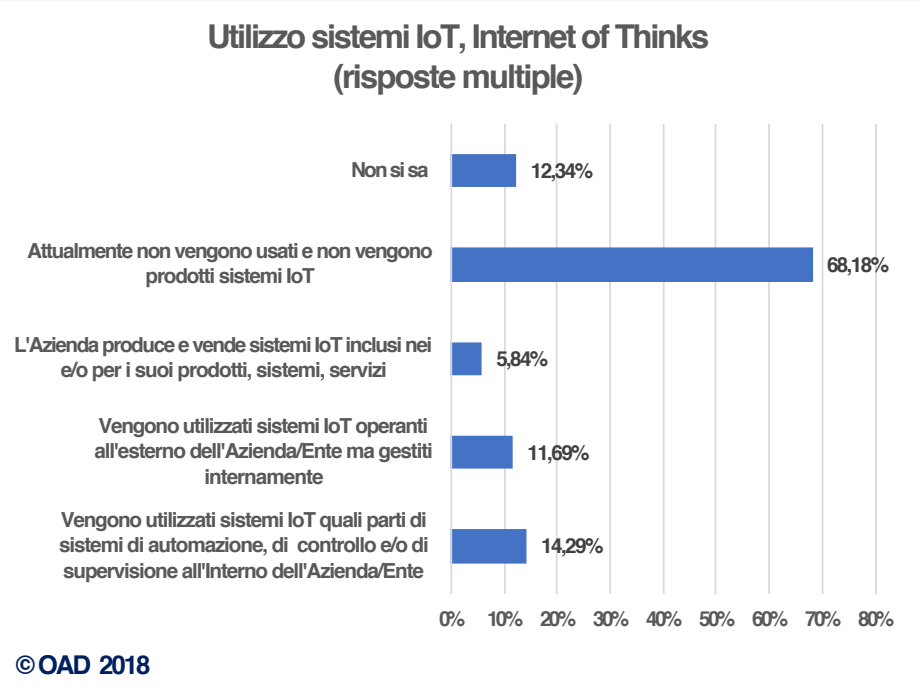

Fig. 10.3-8

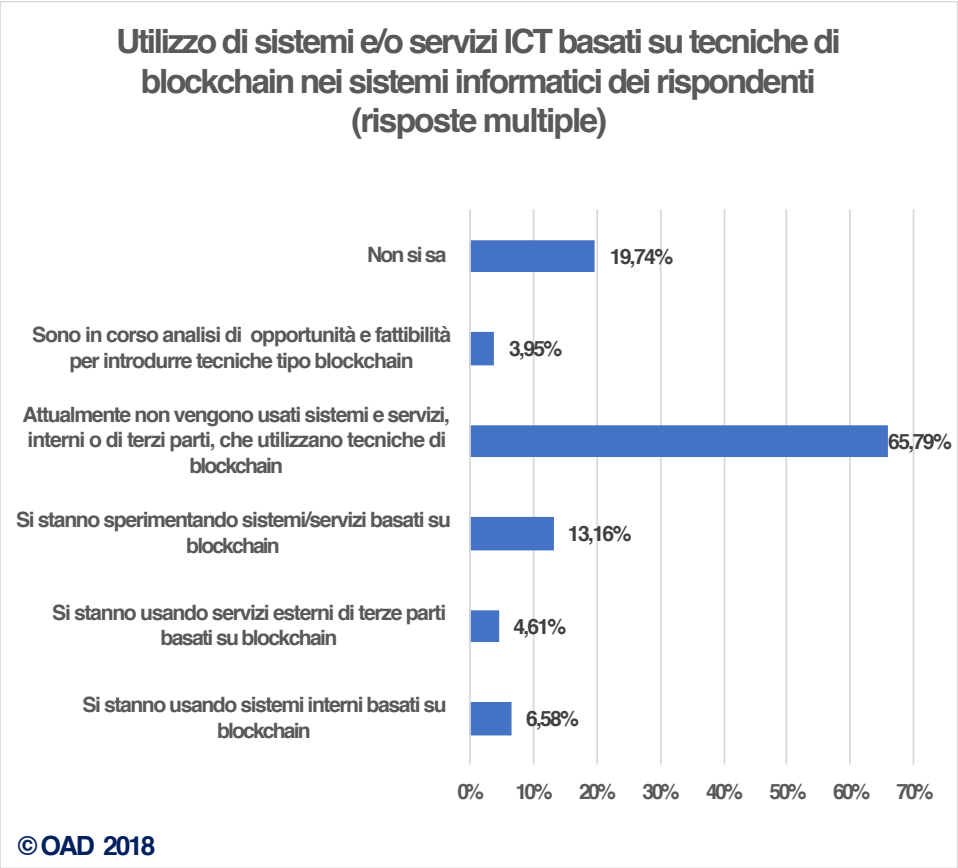
Utilizzo di sistemi e/o servizi ICT basati su tecniche di blockchain nei sistemi informatici dei rispondenti (risposte multiple)
Non si sa
19,74%
Sono in corso analisi di opportunità e fattibilità per introdurre tecniche tipo blockchain
3,95%
Attualmente non vengono usati sistemi e servizi, interni o di terzi parti, che utilizzano tecniche di blockchain
65,79%
Si stanno sperimentando sistemi/servizi basati su blockchain
13,16%
Si stanno usando servizi esterni di terze parti basati su blockchain
4,61%
Si stanno usando sistemi interni basati su blockchain
6,58%
0%
10%
20%
30%
40%
50%
60%
70%
© OAD 2018

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 2016 e nel 2017 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, alla pedopornografia on-line, 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[19], 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[20].

La tabella in fig. 11.1-1 confronta i dati forniti dalla Polizia Postale e delle Telecomunicazioni inerenti alle attività svolte dal C.N.A.I.P.I.C. I dati confermano come il 2017 sia stato un anno ben peggiore rispetto al 2016 sul fronte degli attacchi anche alle infrastrutture critiche: aumentati del 22,27% per quelli rilevati,

19 - https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32008L0114

20 - http://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2011-05-04&atto.codiceRedazionale=011G0101&elenco30giorni=false

e con ben il 369% di incremento di allarmi. Anche le denunce e le perquisizioni sono aumentate, ma gli arresti sono rimasti pari a 3 individui per anno.
Questo numero merita un commento, tenendo conto del numero sia degli attacchi rilevati, sia delle denunce. La prima considerazione è che, vedendo questi numeri, sembrerebbe che il cyber crime "paghi", rimanendo 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. Ma come mai? 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, se esistono, differiscono molto nazione per nazione, 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 sottostimate, come anche sottolineato dal Direttore della Polizia Postale nella Prefazione al presente rapporto: e questo 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.
L'analisi di altri dati di fig. 9.1-1 avvallano le considerazioni di cui sopra. Le percentuali di indagini avviate su attacchi rilevati sono, per il 2017 e 2016, rispettivamente del 6,98% e del 8,29%, ed analogamente le percentuali di persone arrestate su persone denunciate sono del 0,23% e del 0,24%.

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[21]. L'ultima riga della tabella in fig. 9.1-1 mostra che le richieste di collaborazione a livello europeo nell'ottica della Convenzione di Budapest sono leggermente diminuite, ma permangono un elevato impegno per il C.N.A.I.P.I.C.

21 - 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)

Protezione strutture critiche	1 gen – 31 dic 2017	1 gen – 31 dic 2016	Differenza %
Attacchi rilevati	1032	844	**22,27%**
Alert diramati	31524	6721	**369,04%**
Indagini avviate	72	70	**2,86%**
Persone arrestate	3	3	**0,00%**
Persone denunciate	1316	1226	**7,34%**
Perquisizioni	73	58	**25,86%**
Richiesta di cooperazione internazionale in ambito Rete 24/7 High Tech Crime G8 (Convenzione Budapest)	83	85	**-2,35%**

Fig. 9.1-1 Attività per la protezione delle Infrastrutture Critiche (Fonte: Polizia Postale e delle Comunicazioni)

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. 9.2-1 sintetizza i risultati dell'attività della Polizia Postale e delle Comunicazioni su questo fronte, con il blocco nel 2017 di quasi 21 Mlni di € di transazioni fraudolente, con un incremento di circa il 30% rispetto all'anno precedente. Analogamente a quanto evidenziato in §9.1 per le Infrastrutture Critiche, le percentuali di arresti rispetto al numero di denunciati sono, per il 2017 e 2016, rispettivamente del 0,88% e del 0,66%. Valori bassi, le cui cause sono principalmente quelle evidenziate per le Infrastrutture Critiche.

Financial Cyber Crime	1 gen – 31 dic 2017	1 gen – 31 dic 2016	Differenza %
Transazioni Fraudolente Bloccate in €	€ 20.839.576,00	€ 16.050.812,50	**29,84%**
Somme Recuperate	€ 862.000,00	=	
Arrestati	25	25	**0,00%**
Denunciati	2851	3772	**-24,42%**

Fig. 9.2-1 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.
Nell'ambito del contrasto ai cyber crime finanziari, è importante segnalare il "Progetto antifrode" internazionale, iniziato a novembre 2013: OF2CEN (On-Line Fraud Cyber Centre And Expert Network)[22], finanziato

22 - https://www.gcsec.org/it/news-events/online-fraud-cyber-centre-expert-network-of2cen

dall'Unione europea e gestito dalla Polizia Postale e delle Comunicazioni. E' costituito da una piattaforma informatica in cui far confluire tutte le segnalazioni provenienti da banche e Forze di polizia su transazioni sospette che avvengono in Rete, in modo da poter analizzare e condividere in tempo reale ogni informazione e bloccare così le operazioni illegali. Nel solo 2017, grazie a Eu-of2cen, sono state bloccate transazioni, frutto di frodi telematiche commesse attraverso sofisticati strumenti informatici, per oltre 22 milioni di euro e recuperata una somma pari a 900 mila euro.

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. 9.3-1 fornisce pochi dati assai interessanti: in primo luogo che il cyberterrorismo esiste anche sul territorio italiano, che nel 2017 è di fatto raddoppiato, e che la Polizia Postale e delle Comunicazioni lo contrasta.

Cyber Terrorismo	1 gen – 31 dic 2017	1 gen – 31 dic 2016	Differenza %
Arrestati	4	2	**100,00%**
Denunciati	18	9	**100,00%**

Fig. 9.3-1 Attività di contrasto al cyber terrorismo
(Fonte: Polizia Postale e delle Comunicazioni)

Le percentuali di arresti rispetto al numero di denunciati sono uguali nei due anni considerati, pur con il raddoppio di numeri, pari al 22,22%. Quest'ultimo numero ben diverso rispetto alle percentuali, per analogo rapporto, per le Infrastrutture Critiche e per il cyber crime finanziario dello zero virgola qualche decimale: un indicatore che l'ambito giudiziario è maggiormente pronto e capace di reprimere questo tipo di grave reato.

11.4 - Pedopornografia On-Line (C.N.C.P.O.)

La pedopornografia informatizzata esula dagli obiettivi dell'indagine OAD, focalizzata agli attacchi ad aziende ed enti pubblici.
La legge 6 febbraio 2006 n. 38 affida al C.N.C.P.O., Centro Nazionale per il Contrasto Della Pedopornografia On-line, ossia sulla rete Internet, la lotta a questo grave crimine.
Questo Centro è istituito presso la Polizia Postale e delle Comunicazioni e si occupa di prevenzione e repressione di questi reati: le attività svolte ed i risultati ottenuti sono sintetizzati nella tabella in fig. 9.4-1.

Pedopornografia	1 gen – 31 dic 2017	1 gen – 31 dic 2016	Differenza %
Arrestati	55	52	**5,77%**
Denunciati	596	467	**27,62%**
Monitoraggi	28560	22398	**27,51%**
Siti presenti in black list	2077	1972	**5,32%**

Fig. 9.2-1 Attività di contrasto alla pedopornografia on-line
(Fonte: Polizia Postale e delle Comunicazioni)

Anche in questo settore, considerando le percentuali di arresti rispetto al numero di denunciati pari a 9,23% nel 2017 e a 11,13% nel 2016, l'ambito giudiziario risulta più efficace rispetto ai cyber crimini finanziari e vero le infrastrutture critiche. Come per il cyber terrorismo, è relativamente più semplice individuare questi tipi di reato, ed è notevole l'impegno della Polizia Postale: nell'ordine delle decine di migliaia i siti web monitorati e nell'ordine di 2000 i siti oscurati (black list) nel 2016 e nel 2017.

11.5 - Commissariato di P.S. On line

Da più di dieci anni la Polizia di Stato ha realizzato il Commissariato di P.S. on line (si veda https://www.commissariatodips.it/profilo/commissariato-di-ps-on-line.html), gestito dalla Polizia Postale e delle Comunicazioni, per ricevere informazioni o fare segnalazioni di reati che avvengono su Internet:, hacking, phishing, e-commerce, bancomat e carte di credito, spamming, pedofilia online, diritto d'autore, telefonia. Negli anni, questa idea e la sua implementazione ha ricevuto numerosi premi e riconoscimenti a livello internazionale.
La tabella in fig. 9.5-1 sintetizza per il 2016 ed il 2017 le principali attività svolte.

Commissariato di P.S. On Line	1 gen – 31 dic 2017	1 gen – 31 dic 2016	Differenza %
Richiesta informazioni	16737	17374	**-3,67%**
Segnalazioni	18053	19492	**-7,38%**
Denunce	8784	8355	**5,13%**

Fig. 9.5-1 Attività del Commissariato di P.S. on line
(Fonte: Polizia Postale e delle Comunicazioni)

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 tra cui selezionare, posto on line su un sito web accessibile vai 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 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 quindi 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 quindi 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, l'azienda dell'autore Malabo Srl, ed i Patrocinatori coinvolti, invitano ogni anno 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 prevista 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 2018, 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 nuovo sito OAD, **https://www.oadweb.it/**, realizzato sempre da Malabo nel decimo avversario di indagini OAI-OAD.
Il questionario è rimasto accessibile on line via web da febbraio agli inizi di settembre 2018, di fatto con una proroga sulla chiusura del questionario di più di cinque mesi solari, dovuta alla difficoltà di far rispondere, e correttamente al questionario. Nel complesso il numero delle persone contattate è sicuramente maggiore di 5000 ai tremila, 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 2018 era composto da un totale di 114 domande, molte delle quali, le sotto-domande specifiche per ogni tipo di attacco, venivano automaticamente saltate se il rispondente rispondeva di non aver rilevato quel tipo di attacco. Questa logica implementativa del questionario on line ha permesso di ridurre significativamente i tempi per completare l'intero questionario.

A.1 La nuova tassonomia degli attacchi digitali per OAD 2018

Nell'edizione 2018, a partire dal questionario, l'impostazione e la logica della classificazione degli attacchi distingue in modo più rigoroso e più chiaro (rispetto ai questionari delle precedenti edizioni, oltre che ai vari rapporti internazionali) 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.
Con 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), raggruppate in 7 voci, approfondite

tecnicamente nel paragrafo successivo §5.1.
Si è quindi creata una matrice che mappa il che cosa attacco ed il come lo attacco, il cui schema è riportato nella seguente fig. 5-1 (per la spiegazione dei termini gergali si rimanda al glossario in Allegato E): in colonna le tecniche di attacco sopra elencate, per riga il che cosa attacco, le 14 tipologie ossia:

- Distruzione fisica di dispositivi ICT o di loro parti
- Furto fisico di dispositivi ICT o di loro parti
- Furto informazioni da sistemi fissi (PC, server, storage system, …)
- Furto informazioni da sistemi mobili (palmari, smartphone, tablet, ecc.)
- Attacchi all'identificazione, autenticazione e controllo accessi degli utenti e degli operatori
- Attacchi alle reti locali e geografiche, fisse e wireless, e ai DNS
- Uso non autorizzato risorse ICT (dal PC ai server-storage e ai servizi in cloud)
- Modifiche non autorizzate ai programmi applicativi e di sistema, alle configurazioni, ecc.
- Modifiche non autorizzate alle informazioni trattate dai sistemi ICT
- Saturazione risorse digitali (DoS, DDoS)
- Attacchi ai propri sistemi in cloud o in housing/hosting da Fornitori
- Attacchi a dispositivi IoT (Internet of Things) in uso
- Attacchi ai propri sistemi di automazione industriale (DCS, PLC, etc. e/o di robotica
- Attacchi a sistemi e/o servizi usati e basati su blockchain

E' importante evidenziare come in questa edizione vengono considerati anche gli attacchi alle parti di sistemi informatici terziarizzati in cloud/housing/hosting, data la forte crescita dell'outsourcing, ai sistemi IoT, ai sistemi di automazione industriale e di robotica, che erano stati considerati anche nelle precedenti edizioni, seppure in maniera meno dettagliata. Novità assoluta gli attacchi ai sistemi basati su blockchain, che iniziano a1d essere usati anche in Italia per specifiche funzionalità in alcuni settori.

Che cosa è attaccato	**Come (tecniche attaccco)**						
	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)
Distruzione fisica di dispositivi ICT o di loro parti							
Furto fisico di dispositivi ICT o di loro parti							
Furto informazioni da sistemi fissi (PC, server, storage system, …)							
Furto informazioni da sistemi mobili (palmari, smartphone, tablet, ecc.)							
Attacchi all'identificazione, autenticazione e controllo accessi degli utenti e degli operatori							
Attacchi alle reti locali e geografiche, fisse e wireless, e ai DNS							
Uso non autorizzato risorse ICT (dal PC ai server-storage e ai servizi in cloud)							
Modifiche non autorizzate ai programmi applicativi e di sistema, alle configurazioni, ecc.							
Modifiche non autorizzate alle informazioni trattate dai sistemi ICT							
Saturazione risorse digitali (DoS, DDoS)							
Attacchi ai propri sistemi in cloud o in hosting presso Fornitori							
Attacchi a dispositivi IoT (Internet of Thinks) in uso							
Attacchi ai propri sistemi di automazione (DCS, PLC, ..) e di robotica							
Attacchi a sistemi e/o servizi basati su blockchain							

Fig.A.1-1 Matrice tassonomia attacchi

Nel testo del presente Rapporto 2018 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 2018 di OAD fa riferimento agli attacchi rilevati nel 2016 e nel 2017: per non appesantire troppo il numero di domande, per il 2016 viene richiesto solo che cosa è stato attaccato. Per l'anno 2017, per ogni tipo di attacco (il che cosa, asse verticale matrice) nel Questionario 2018 è stata creata una sezione specifica, con gruppi di sotto domande che includono, se l'attacco è stato rilevato:

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

Ogni tipologia d'accatto viene esaminata con le risposte alle sotto-domande sopra elencate nei sotto-paragrafi di §6, dal $6.1 al §6.14.

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

Facendo riferimento principalmente alle tassonomie sviluppate da CERT[23] e da Sandia[24], si sono categorizzate le tecniche di attacco sotto riportate per poter descrivere e richiedere nel Questionario 2018 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, e tra queste, con un taglio tecnico-manageriale al volume sulla sicurezza digitale pubblicato dall'autore nel 2013[25].

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 rotte o 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 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

23 - Per CERT/CC si veda **https://www.sei.cmu.edu/about/divisions/cert/index.cfm**, per il sito italiano: https://www.certnazionale.it/

24 - https://www.sandia.gov/

25 - Marco Bozzetti, Francesco Zambon: "Sicurezza Digitale – Una guida per governare un sistema informatico sicuro", edito e pubblicato da Soiel International Srl a giugno 2013, ISBN 978-88-908901-0-9

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 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 F 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 APT, Advanced Persistent Threat

APT è una tecnica di attacco sofisticata e complessa, basata a sua volta su diverse tecniche operanti contemporaneamente e capaci di scoprire e sfruttare diverse vulnerabilità sul sistema ICT attaccato. 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 certe 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.
- 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.
- IoT, Internet of Things (Internet delle Cose): componenti/sistemi intelligenti ed interoperanti su Internet.
- 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.
- 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

Digitree

Disruptive Technologies for Secure Smart Workers

Digitree è distributore per l'Italia e l'Europa dell'est di soluzioni per la sicurezza informatica. Soluzioni semplici ma di alto livello, che consentano di allargare i tradizionali perimetri di sicurezza, tenendo conto delle esigenze dettate da mobilità e BYOD, e che non comprendano soltanto tecnologia e software, ma capaci di agire anche sull'elemento umano per renderlo l'estrema linea di difesa della sua sicurezza digitale. DigiTree si rivolge a qualunque tipo di pubblico, dall'impresa famigliare alla grande corporate, offrendo soluzioni scalabili e adatte a qualunque tipo di budget.

Protezione dati

Le soluzioni per la protezione di storage (SPYRUS, SafeToGo) permettono di utilizzare la più robusta crittografia hardware automatica, senza doversi preoccupare di noiosi settaggi software o di possibili vulnerabilità. Si accede con la password e i dati sono in chiaro, pronti per poterci lavorare sopra. Si toglie il dispositivo e il motore crittografico interno cifra i i dati rendendoli inaccessibili in caso di furto o smarrimento del dispositivo. Inoltre, tali soluzioni consentono anche di gestire da remoto i dispositivi USB da una console centralizzata che permette agli amministratori di sistema di effettuare tutta una serie di azioni di inventory, audit e controllo su di essi.

Protezione delle connessioni remote

ISL Online, il software di desktop remoto certificato ISO 27001, è stato progettato fin dall'inizio tenendo presente in primo luogo la sicurezza, e le sue eccezionali caratteristiche di sicurezza vengono continuamente aggiornate e sottoposte a penetration test sia interni che indipendenti. Oltre alla versione cloud, ISL Online può inoltre essere ospitato sui server aziendali o configurato come private cloud, per una garanzia di sicurezza e privacy ancora maggiore.

Ingegneria Sociale

DigiTree propone la piattaforma KnowBe4, il nuovo approccio alla formazione sulla security awareness che combina moduli di formazione tradizionale a giochi, video, live demo e quant'altro, mettendo a disposizione tutto un repertorio di poster, newsletter ed altro materiale da poter utilizzare per creare una cultura aziendale consapevole dei rischi derivanti dall'ingegneria sociale (social engineering, phishing, etc.). Inoltre, accanto alla formazione, la stessa piattaforma consente di pianificare campagne di phishing simulato da svolgere con regolarità nel corso dell'anno per costruire un vero e proprio 'firewall umano' a difesa dell'asset informativo aziendale.

Gestione delle Infrastrutture e dei Database

La creazione di un piano per ottenere la compliance con il nuovo GDPR – e riuscire a mantenerla – richiede che si sappia esattamente che cosa ci sia, ad oggi, nel proprio data center, in che modo gli hardware, i software ed i servizi che esso supporta interagiscono tra di loro, e quali sono le dipendenze tra ciascuno di essi. Device42, il rivoluzionario strumento di gestione dei data center e delle infrastrutture ICT, permette di ottenere un quadro completo delle infrastrutture, compresi tutti i database, le applicazioni che li utilizzano e le relazioni tra di esse. E grazie alla sua funzione di auto-discovery permette di ottenere aggiornamenti periodici ed automatici della situazione degli asset.

Servizi GDPR Compliance

Oltre all'offerta di soluzioni software e hardware, grazie alla collaborazione con legali esperti professionisti del settore offriamo servizi personalizzati Servizi IT Legal & GDPR Compliance, a partire da Audit, Risk Assessment e Risk Management, per tutte le attività e le procedure necessarie per prevenire e/o limitari i rischi, semplificare i processi, aggiornare e monitorare tutte le misure tecnico-organizzative e legali dirette al conseguimento di obiettivi di miglioramento e sviluppo del business, di risultato e di immagine.

Per maggiori informazioni visitate: **www.digitree.it**

IntheCyber

InTheCyber Group – Intelligence & Defense Advisors, realtà nata nel 2008 come "Maglan Europe", joint-venture con l'omonima azienda israeliana, da cui si separa a fine 2015, è focalizzata nel supportare aziende ed istituzioni a verificare la reale efficacia delle misure di difesa da attacchi informatici e cyber, per poi guidare in un percorso virtuoso verso il presidio continuativo della Cyber Security e della sua Governance.
Gli esperti di ITC hanno competenze esclusive al servizio dei Clienti secondo un approccio olistico volto alla Difesa a 360° e sono organizzati in 3 Team:
White Team: verifica il livello di compliance alle differenti normative/standard cui il Cliente deve/vuole aderire (GDPR, NIS, NIST, ISO27001) tramite assessment, gap-analysis e consulenza, integrando poi con servizi di executive advisoring e training.
Red Team: sviluppa l'approccio offensivo, tramite vulnerability assessment e simulazioni di attacco dai penetration test verso applicazioni, sistemi, infrastrutture, IoT e ambienti SCADA, sino alle operazioni di spionaggio industriale computerizzato passando per le esercitazioni di social engineering e di empowerment dei team di difesa dei Clienti. Il Red Team si configura poi come Testing Hub per i produttori di tecnologie HW&SW.
Blue Team: verifica le architetture implementate, definisce le misure di hardening sino a prendere in carico le piattaforme di Security del Cliente con il servizio di Detection & Response attivo nell'identificazione rapida delle minacce e nel loro blocco sul nascere.
Gli InTheCyber R&D Labs studiano le evoluzioni tecniche nelle modalità di attacco da parte di hackers, organizzazioni criminali ed entità di spionaggio avanzato. Gli stessi Labs sviluppano tools e servizi di Intelligence a supporto governativo.

InTheCyber, consapevole della strategicità della Difesa Cyber per il Paese ha contribuito alla nascita delle European Center for Advanced Cyber Security (EUCACS) e promuove dal 2010 assieme ad altri enti ed associazioni la Conferenza Nazionale sulla Cyber Warfare, Cyber Warfare Conference (CWC), che si tiene ogni 6 mesi a Roma e Milano.
La CWC riunisce rappresentanti di governo, forze armate, servizi d'Intelligence, imprese, finanza, mondo accademico ed ha come obiettivo quello di accrescere la consapevolezza sulla minaccia Cyber per il Paese e sulla necessità di una stretta collaborazione e condivisione di informazioni per la Sicurezza Nazionale.

Per maggiori informazioni visitate: **http://www.inthecyber.com/it/**

Par-tec

Par-Tec S.p.A. è un software & infrastructure system integrator specializzato nella fornitura di servizi professionali altamente qualificati e nella progettazione di soluzioni innovative cross-market e personalizzate.
Con gli oltre 15 anni di esperienza delle business unit di Roma e Milano, offriamo consolidate competenze negli ambiti dell'Infrastruttura IT, della Business Intelligence, delle Soluzioni Verticali dedicate al mercato finanziario e dell'Educational.
Il nostro team di circa 150 professionisti è costantemente impegnato nella ricerca del migliore equilibrio tra innovazione, comprensione delle esigenze, business efficiency e scalabilità delle soluzioni.

Tra le aree di specializzazione maggiormente in crescita troviamo:

IT Infrastructure & Cloud Computing. Come Red Hat Premier Business Partner - il primo in Italia ad ottenere la specializzazione sul Cloud Infrastructure - disponiamo delle competenze tecniche richieste per supportare le Large Enterprise e le Pubbliche Amministrazioni nel complesso processo di trasformazione del datacenter, in particolare mediante l'adozione dello stack di tecnologie cloud di Red Hat e l'eventuale integrazione di altri progetti e prodotti open source.

DevOps e architetture a microservizi. I nostri esperti stanno supportando importanti realtà italiane nella delicata transizione verso le nuove metodologie emergenti in ambito DevOps, tra cui la Continuous Integration (CI) e il Continuous Delivery (CD) associati allo sviluppo di microservizi basati su container Docker e l'automazione del cloud effettuata mediante strumenti come Ansible.

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 sulle misure minime e sugli standard di sicurezza, 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. Tutti 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**

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 ques'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

FTI

Forum per la Tecnologia dell'Informazione, è una libera associazione apolitica senza scopi di lucro che opera nei settori dell'informatica, delle telecomunicazioni, della multimedialità.
http://www.forumti.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
- 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
- I vari Rapporti annuali OAI e OAD: https://www.oadweb.it/it/main-it/rapporti-e-relativi-convegni.html

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[26]: 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.

26 - CVSS è un sistema di valutazione delle vulnerabilità, che attribuisce a ciascuna un punteggio numerico che riflette la sua gravità. 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". E' 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 qualsiasi tipo di sistema operativo e/o applicativo.
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 (www.sla-watch.com), *GOSI*, per la gestione operativa in parte automatizzata di un sistema informativo 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.sla-watch.com, 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 e della 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 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.
- Rappresentanza dei Soci professionisti dell'Information Security, nell'ambito delle recenti normative italiane stabilite dal D.Lgs. 4/2013 sulle professioni non regolamentate (in preparazione).
- Networking con altri professionisti del settore.
- Possibilità di costituire gruppi di lavoro per ricerche e condivisione informazioni su tematiche d'interesse comune.
- Possibilità di redigere articoli per conto di AIPSI/ISSA e loro pubblicazione nel sito web AIPSI.
- Pubblicazione e ricerca di curricula per agevolare la domanda/offerta di competenze e di professionalità.
- Accesso al materiale riservato ai soci sul sito web di ISSA e di AIPSI.
- Visibilità nazionale ed internazionale grazie al riconoscimento di ISSA nel mondo.
- Possibilità di partecipare come oratore a seminari e conferenze per conto di AIPSI/ISSA.

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


AICA

aipsi

ASSOCIAZIONE ITALIANA
SISTEMI INFORMATIVI IN SANITÀ

ASSOCIAZIONE
SPECIALISTI
SISTEMI
INFORMATIVI

ASSINTEL
ASSOCIAZIONE NAZIONALE
IMPRESE ICT

ASSOLOMBARDA

ASE

CRS
CENTRO RICERCHE
SULLA SCRITTURA
handwriting research center

Club Dirigenti di Informatica

CDTI

CTI
er
CLUB

ti
Liguria
ti

ClubTi

FIDA
INFORM

FTI
FORUM per la
TECNOLOGIA della
INFORMAZIONE

Grafobiometristi
italiani associati

IEEE computer society
Italy
Chapter

Inforav
Istituto per lo sviluppo e la gestione
avanzata dell'informazione