OAD
Osservatorio
Attacchi Digitali
in Italia

Rapporto
OAD 2016

a cura di Marco R. A. Bozzetti

in collaborazione con

GOLD PARTNER

SILVER PARTNERS

aipsi sernet Technology Estate TREND MICRO

Indagine effettua da malabo ICT Advisory NEXTVALUE INSIGHTS FOR YOUR BUSINESS

Finito di stampare a Luglio 2016

NEXTVALUE S.r.l.
Viale Bianca Maria 18 - 20129 Milano
Ph. +39 02 8976 3767 | info@nextvalue.it
Partita IVA 03678780960 - Codice Fiscale 03678780960
REA 1693394 Milano

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, alla dott.a Giulia Nebuloni e all'ing. Alfredo Gatti di NEXTVALUE, al dott. Francesco Zambon, all'ing. Maurizio Mapelli di AIPSI, al dott. Salvatore La Barbera della Polizia Postale e delle Comunicazioni, che hanno contribuito in vario modo alla realizzazione del presente rapporto.

INDICE

FIGURE E TABELLE

Perché un Osservatorio Attacchi Digitali in Italia?

di Alfredo Gatti

Da sei anni NEXTVALUE ha incluso tra i propri Insights il tema dell'Information Security Management e della Cyber Security, invitando CSO e CISO di Grandi imprese italiane a condividere le loro esperienze nel ruolo, i loro feedback su investimenti, risorse, difficoltà e a dirci la loro opinione sul grado di resilienza raggiunto dalle rispettive imprese. Ci è sempre mancata la vista complementare, quella di un rilevamento puntuale e di una analisi sui reali attacchi ai sistemi informativi di imprese e enti pubblici italiani. Lo potevamo chiedere noi agli stessi Responsabili dei Sistemi Informativi e della Sicurezza Informatica, ma pensavo che tali dati potessero essere già disponibili grazie a rilevamenti disposti da una qualche entità che si dichiara associazione o iniziativa preposta al riguardo. Purtroppo, dopo qualche infruttuoso tentativo di ricerca e di collaborazione con "i soliti nomi" mi sono dovuto ricredere perché i dati in possesso erano decisamente scarsi e spesso sembravano provenire più da input di vendor che dai reali utilizzatori ...

E a questo punto che l'amico Marco Bozzetti è venuto a propormi di mettere insieme le forze e di trasformare quell'imponente lavoro che lui svolgeva con l'Osservatorio degli Attacchi Informatici in un nuovo progetto di Osservatori Attacchi Digitali (OAD) in cui si indagasse decisamente più a fondo sulle vulnerabilità attribuibili alle tecnologie digitali, così indispensabili nei progetti di innovazione delle imprese. Che cosa poteva offrire NEXTVALUE al progetto? L'esperienza di azienda di ricerca impegnata sui vari fronti della trasformazione digitale delle Grandi Imprese italiane ed europee e, soprattutto, una vasta e attiva business community di CIO come CIONET, ma anche una altrettanto importante community di CSO e CISO di imprese finali. Che cosa chiedere in cambio? Che i risultati fossero disponibili a tutti questi decisori.

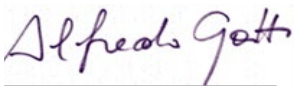
Eccoli qui i risultati. Bozzetti, Malabo e AIPSI hanno fatto un lavoro eccezionale, suffragato dall'elevato e qualificato numero dei rispondenti, dal significativo contributo della Polizia Postale e dal supporto degli Sponsor che hanno creduto nel progetto e lo hanno supportato fin dall'inizio.

L'enorme lavoro ci permette di avere una precisa immagine a tutto tondo di ciò che accade nelle imprese e negli enti pubblici italiani. L'analisi è precisa e circostanziata, per questo può essere ancor più di interesse anche per chi non è un addetto ai lavori; ed è con orgoglio che mi unisco al lancio di questo primo Osservatori Attacchi Digitali in Italia.

Che cosa avverrà dopo? In un mercato dove le tecnologie digitali sono sempre più all'ordine del giorno e sempre più innumerevoli divengono gli oggetti interconnessi l'issue "sicurezza" non ha mai fine e l'interesse delle imprese e degli enti pubblici per conoscere ciò che avviene in caso di attacco sarà ancora più alto, visto il valore delle informazioni in gioco. Ma andiamo per gradi e facciamo nostra fino in fondo l'informazione che ci proviene da questo report.

Buon lavoro!

Alfredo Gatti
Managing Partner di NEXTVALUE
Managing Director di CIONET Italia



1 Executive Summary

L'Osservatorio Attacchi Digitali in Italia, OAD, è il nuovo nome dato alla precedente iniziativa OAI, Osservatorio Attacchi Informatici in Italia, iniziativa giunta ora alla sesta edizione, e che realizza annualmente un Rapporto con l'analisi degli attacchi intenzionali, rilevati nel 2015, ai sistemi informatici di organizzazioni di ogni dimensione e settore merceologico, incluse le Pubbliche Amministrazioni centrali e locali. OAD, sotto l'egida di AIPSI, Capitolo italiano di ISSA, vede dal 2016 per la sua realizzazione la collaborazione tra la società dell'autore, Malabo Srl, e Nextvalue Srl, società di ricerche di mercato e di consulenza nell'ambito ICT.

L'indagine OAD si basa sull'elaborazione delle risposte avute da un questionario via web nei primi mesi del 2016, per un totale di 288 rispondenti. Essendo volontarie le risposte al questionario, il campione emerso non ha valenza statistica, ma, dato il numero di risposte e la buona distribuzione per dimensioni e per settore merceologico, esso fornisce precise e contestuali indicazioni sul fenomeno degli attacchi informatici in Italia: informazioni basilari sia per la sensibilizzazione sulla sicurezza digitale sia per l'analisi dei rischi. Il Rapporto analizza quali sono gli strumenti di prevenzione, protezione e ripristino in uso dei sistemi informatici dei rispondenti per contrastare e limitare tali attacchi, e come essi reagiscono in caso di attacco. Innumerevoli le considerazioni che possono emergere dai dati raccolti, nel seguito si sintetizzano alcuni degli aspetti più significativi.

Il bacino di rispondenti risulta costituito per la maggior parte da aziende di servizi di diversi settori merceologici (terziario), seguite in minor numero da aziende manifatturiere (secondario), e da Pubbliche Amministrazioni. In termini di dimensioni delle aziende/enti dei rispondenti, la maggior parte dei rispondenti, 43,7%, appartiene a strutture fino a 49 dipendenti, il 22,6% a strutture tra 50 e 250 dipendenti (limite italiano per far parte delle PMI, Piccole Medie Imprese), il 33,6% a strutture oltre i 250, equamente distribuite nelle tre classi considerate, 251-1000, 1001-5000, oltre 5001. Il campione emerso risulta quindi abbastanza ben bilanciato tra piccole strutture e quelle medio grandi e grandissime.

I compilatori del questionario sono per il 35.3% responsabili dei sistemi informatici, per il 15,1% personale appartenente all'unità organizzativa dei sistemi informatici, per l'8% responsabili della sicurezza digitale (CISO). Il 24,4% è costituito dal vertice aziendale (proprietario, amministratore delegato, partner, direttore generale), soprattutto per le piccole e le piccolissime imprese.

I trend sugli attacchi emersi con il campione di rispondenti sono sostanzialmente in linea con quelli internazionali, e sintetizzati nei punti seguenti che evidenziano anche alcune specificità tipicamente nazionali.

- Gli attacchi nel 2015 hanno colpito (e/o sono stati rilevati) il 37,6% dei rispondenti, con una quota simile a quella delle precedenti edizioni (pur avendo tale confronto un valore puramente indicativo e non statistico). E' invece aumentato significativamente il numero di attacchi complessivi nell'anno per azienda/ente.
- La percentuale al di sotto del 40% di attacchi subiti e rilevati si conferma stabile dal 2007, anno da cui parte l'indagine OAI-OAD; essa è dovuta, a giudizio dell'autore, soprattutto dalla maggioranza di piccole e piccolissime imprese in Italia, che non costituiscono, singolarmente, un obiettivo di interesse per organizzazioni, spesso internazionali, di cyber criminali. Una seconda causa è sicuramente data dalla non rilevazione, in molti casi, dell'attacco subito, ma questo significa che tale attacco non ha avuto rilevabili impatti sull'azienda/ente, al di là del possibile furto di informazioni.
- Le tipologie di attacchi più diffusi nel 2015 sono il "malware" (78,4%), il "social engineering" (71,9%), il furto dei dispositivi ICT (34%) e la saturazione delle risorse (29,4%). Queste quattro tipologie di attacchi sono in cima alla classifica di tutte le sei edizioni di OAI-OAD, con percentuali diverse ed in posizioni tra loro differenti a seconda degli anni, ma con il malware, che include il ransomware, sempre primo in classifica.
- Nel 2015, come negli anni precedenti, il numero di attacchi e la loro frequenza aumentano prevalentemente per dimensione dell'organizzazione in numero di dipendenti: più le aziende/enti sono grandi e note a livello internazionale, più hanno (o si presume che abbiano) capacità economiche e finanziarie, più rapprasentano un obiettivo appetibile per il cyber crime.
- L'impatto degli attacchi risulta grave solo in un limitato numero di casi, il 14,6%. Gli attacchi che nel 2015 hanno avuto il maggior e più grave impatto sono stati i ricatti ICT, seguiti con quasi 10 punti di distacco dalla saturazione delle risorse, dai malware e dagli TA/APT (Targeted Attacks/Advanced Persistent Threats), tutti con percentuali superiori al 20%.
- La non gravità dell'impatto nella maggior parte degli attacchi subiti è confermata dai veloci tempi di ripristino della situazione ex ante: il 44% dei casi è ripristinato in giornata, e complessivamente circa l'80% dei casi è ripristinato in 3 giorni. Nessun caso ha richiesto più di un mese. Le tipologie di attacco che hanno richiesto più di una settimana per il ripristino vedono al primo posto il malware, grazie anche all'ampia diffusione del ransomware in Italia, seguito dal furto di apparati ICT e dalla saturazione di risorse.
- L'analisi economica dell'impatto dell'attacco subito è effettuata dal

25,9% per tutti gli attacchi e dal 10,2% solo per quelli più gravi. Per i rispondenti che lo hanno segnalato, il più alto costo indicato è di € 70.000.

- Gran parte degli attacchi, malware inclusi, si basano sulle vulnerabilità tecniche dei software e delle architetture. Le vulnerabilità note sono normalmente risolte dai produttori-fornitori, che emettono patch e aggiornamenti dei software; ma questi non sempre vengono tempestivamente installati: solo il 44,5% dei rispondenti aggiorna il software in uso. Le cause possono essere diverse, ma il più delle volte sono organizzative: in particolare, la non conoscenza delle disponibilità di patch, la mancanza di procedure per i test del software, il non rinnovo dei contratti di manutenzione del software, causato in molte realtà anche dal perdurare della crisi economica. Alcune vulnerabilità non sono scoperte e rimediate dai produttori ma, se lo sono dagli attaccanti, questi software divengono oggetto di attacchi che vanno a buon fine anche per tempi lunghi.
- Il comportamento delle persone utenti e/o operatori dei sistemi informatici è la vulnerabilità più critica e diffusa, causa della maggior parte degli attacchi riusciti; essa si basa sulla disponibilità e buona fede delle persone, sulla loro disattenzione o ingenuità, sulla non conoscenza di come usare in maniera sicura gli strumenti ICT, sulla scarsa sensibilità ed attenzione alla sicurezza informatica. Strumenti facilitatori ed amplificatori delle vulnerabilità personali sono i social network, la posta elettronica, i motori di ricerca, le sempre più capaci chiavette USB, gli strumenti collaborativi, l'utilizzo ormai prevalente di sistemi d'utente mobili, quali smartphone e tablet, Essi facilitano la possibilità di rubare le identità digitali degli utenti ed acquisire informazioni riservate con le quali svolgere attacchi e compiere frodi informatiche.
- Per chi usa servizi in cloud, i ¾ dei rispondenti non hanno rilevato attacchi, solo il 3,4% li ha subiti sulle applicazioni (SaaS, Software as a Service), ed il 2,5% sulle infrastutture ICT (IaaS, Infrastructure as a Service); non è stato rilevato alcun attacco sulle PaaS, Platform as a Service. Queste basse percentuali sono un indicatore dell'affidabilità e della sicurezza dei servizi in cloud in uso.
- La motivazione principale per gli attacchi, in particolare di quelli più temuti nel prossimo futuro, è l'ottenere illegali ritorni economici: le stime dei rispondenti sono per il 52,1% per le frodi, per il 51,3% per i ricatti (ma anche per ritorsioni) e per il 28,1% per lo spionaggio, in particolare industriale.
    - La Polizia Postale e delle Comunicazioni nel 2015, nell'ambito del contrasto al "financial cybercrime", ha verificato 16.697 transazioni on line dubbie in 10 gruppi bancari, bloccando € 65.870.825,63 e recuperando € 2.734.269,31.

    - Solo l'1,3% dei rispondenti afferma di aver avuto nel 2015 sottrazioni di denaro sui conti bancari causati da furti di identità digitali: un indicatore che i sistemi informatici delle banche italiane usate dal campione assicurano un buon livello di sicurezza digitale.
- Indipendentemente dalle dimensioni e dal settore merceologico di appartenenza, gli aspetti tecnici ed architetturali dei sistemi informatici sono per la maggior parte allo state dell'arte:
    - il 52, 1% dispone di architetture ad alta affidabilità;
    - il 42,1% ha un Piano di Business Continuity (continuità operativa);
    - i sistemi operativi dei server sono aggiornati alle più recenti versioni: il 68,9% utilizza Windows Server 2012, e il 14,3% l'ultimo rilasciato Windows Server 2016. Il 58,8% usa sistemi operativi "hypervisor" per la virtualizzazione dei server.
- Le misure tecniche per la sicurezza digitale, da quelle fisiche a quelle per la protezione dei dati, sono abbastanza diffuse su tutto il campione emerso. Alcune delle debolezze riscontrate, come percentuale di diffusione, riguardano la verifica del codice sicuro per il software messo in produzione, effettuata dal 16,8%, la sistematica gestione delle patch e delle versioni del software, effettuata da poco più della metà del campione, l'archiviazione criptata delle informazioni critiche, effettuata dal 21,8%, la raccolta e la gestione dei log degli operatori, obbligatoria per la privacy, effettuata da meno della metà dei rispondenti, le prove dei piani di Disaster Recovery effettuate dal 21,% contro un significativo 39,5% che ha un piano di Disaster Recovery.
- Assai positivo che un 15,1% di rispondenti utilizzi sistemi di analisi comportamentale dei sistemi ICT e/o dei loro utenti, uno dei moderni mezzi 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, per una buona o comunque non trascurabile percentuale del campione, risultano "meno avanzate" di quelle tecniche, anche se alcuni aspetti sono positivi e migliorativi, come trend, rispetto a quanto rilevato nelle precedenti edizioni:
    - il 57,4% del campione non ha definito policy sulla sicurezza digitale;
    - la struttura organizzativa per la sicurezza digitale non è formalmente definita per la maggior parte dei rispondenti: il 39,5% ha definito un ruolo preciso per il responsabile della sicurezza digitale (CISO) e nel 18,6% dei casi tale ruolo è informalmente svolto dal responsabile dell'ICT (CIO); solo una minima parte del campione, 3,1%, delega tale ruolo a società e/o professionisti esterni;
    - per ruoli interni inerenti la sicurezza digitale solo il 12,6% richiede specifiche certificazioni, e per il personale esterno di fornitori e

consulenti solo l'11,8%;
- ancora limitato alle strutture dimensionalmente più grandi l'uso sistematico di standard e best practice per la sicurezza digitale ed il suo governo:
  - gli standard della famiglia ISO 27000 sono adottati con certificazioni dal 12,6% dei rispondenti;
  - ITIL è seguito con personale certificato dal 12,6%;
  - COBIT è seguito con certificazioni dal 3,4%;
- l'analisi dei rischi è effettuata dal 23,5% dei rispondenti ma un 20,2% già riassicura il rischio residuo, ed il 13,4% intende farlo nel prossimo futuro;
- l'auditing ICT, interno, esterno e in mix, è svolto dal 45,8% dei rispondenti ed il 65,5% di questi lo effettua in maniera strutturata, periodica e regolare.

Per concludere, la presente indagine conferma i macro trend dei precedenti Rapporti OAI e delle recenti indagini internazionali. La realtà italiana con un grandissimo numero di piccole e piccolissime imprese non fa rientrare il nostro paese tra quelli più colpiti a livello mondiale. Le aziende/enti rispondenti hanno migliorato le misure tecniche ed in parte quelle organizzative, ma gli ultimi attacchi digitali sono più sofisticati, più difficili da individuare e possono impattare talvolta gravemente chi li subisce: gli impatti hanno riguardato, e riguarderanno soprattutto perdite finanziarie e di reputazione. Inoltre, non solo le infrastrutture critiche ICT potranno essere attaccate per terrorismo, ma anche le piccole realtà potranno essere oggetto di attacchi massivi e paralleli, con l'obiettivo, essendo meno protette, di causare un collasso di non breve durata delle attività e dell'economia italiana nel suo complesso. L'Italia fino ad ora non è stata al centro del cyber crime e del cyber war, ma corre un crescente rischio di esserlo nel prossimo futuro, se la sensibilizzazione e la cultura della sicurezza digitale non crescono nel Paese a tutti i livelli.

1 en Executive Summary in English

OAD, Observatory on Digital Attacks in Italy, is the new name for the previous OAI, Observatory on Informatics Attacks in Italy. This initiative, now in its sixth edition, provides an analysis of intentional attacks against informatics systems for organizations of every size and industry sector, including central and local public administrations, and provides an annual report. OAD is promoted by AIPSI, Italian Chapter of ISSA, and is realized by Malabo Srl , the company of the author for ICT advisory, and by Nextvalue Srl, a company active on ICT market research and consulting.

The OAD analysis is based on the responses received via web from an online questionnaire in January-June 2016, with a total of 288 respondents. Since the web survey is not based on a specific sample of respondents, the resulting data cannot have statistical significance. Given the number of responses and their good distribution in terms of size and industry sector, OAD survey provides accurate and contextual information on the phenomenon of cyber-attacks in Italy; it is also useful to raise awareness about computer security as well as to be a reference for risk analysis. In addition, the report analyses what are the tools used by the respondents for the prevention, protection and recovery of the attacks, and how they react in case of attack. Several considerations may emerge from all the data collected, in the following we summarize some of the most significant.

- The OAD Report 2016 considers the attacks detected in 2015.
- The respondents are mostly from companies of the services sectors (tertiary), followed to a lesser number of manufacturing companies (secondary), and public administration. In terms of size of the organizations, the majority of respondents, 43.7%, belongs to structures up to 49 employees, 22.6% in structures between 50 and 250 employees (Italian limit for SMEs, Small and Medium Enterprises), 33.6% more than 250, equally distributed in the considered three classes of 251-1000, 1001-5000, over 5001. The sample is fairly well balanced among SME, large structures and very large ones.
- The compilers of the questionnaire are responsible at the 35.3% of IT systems, for the 15.1% belongs to the organizational unit of computer systems, for the l8% are responsible for the digital security (CISO). The 24.4% belongs to the top management (owner, managing director, partner, general manager), especially for small and micro enterprises.
- The attacks in 2015 hit 37.6% of respondents, with a share similar to that of the previous OAI editions (although this comparison is only indicative and has not statistical value). It is instead significantly increased

the total number of attacks in the year for company / institution.

- A percentage below 40% of the detected attacks has remained stable since 2007. To the author's judgment, this is due especially by the vast majority of small and very small enterprises in Italy, which are not, individually, a target of interest for the cybercrime. A second cause is certainly due to the non-detection of the attacks, but this implies that the attack did not have a strong impact on the company / organization, beyond the possible theft of information.
- The most common types of attacks in 2015 are malware (78.4%), social engineering (71.9%), theft of ICT devices (34%), saturation of resources (29.4 %). These four types of attacks have been always on the top of the list of the attacks for all the OAI-OAD editions, with different percentages and in different positions from each other depending on the year, but with malware, which includes ransomware, always first in the standings.
- In 2015, as in the previous years, the number of attacks and their frequency increases depending mainly on the organization size (as number of employees): an organization more is big and internationally known, more it should have economic and financial capacity, and therefore more it is an attractive target for cyber-crime, and therefore more it is attacked.
- The impact of attacks is severe only in a limited number of cases, 14.6%. Attacks that in 2015 had the largest and most severe impacts were blackmail ICT, followed by denial of services (Dos/Ddos), malware and TA / APT (Targeted Attacks / Advanced Persistent Threats), all with percentages higher than 20%.
- The low severity of the impact in most of the attacks is confirmed by the fast recovery time: the 44% of cases it is restored in a day, and globally about the 80% of cases is restored in three days. No case took more than a month. The types of attack that required more than a week to restore include malware, thanks also to the wide spread of ransomware in Italy, theft of ICT equipment and Dos/Ddos.
- The economic impact of an attack is carried out by 25.9% for all the attacks and by 10.2% only for the most serious. For respondents who have reported, the higher cost of single attack has been estimated about € 70,000.
- The economic impact of an attack is carried out by the 25.9% for all the attacks and by the 10.2% only for the most serious. For respondents who have reported, the highest cost for a single attack has been estimated about € 70,000.
- Normally each attack exploits one or more vulnerabilities, which can be technical, organizational or caused by people, be they end users or operators of computer systems. The known technical vulnerabilities are usually resolved by the producer-suppliers, emitting patches and

software updates, are not always promptly installed. The vulnerabilities are sometimes not discovered and resolved in short from suppliers, and remain so exploitable by attackers for long times.

- The known technical vulnerabilities are usually resolved by the produce, emitting patches and software updates: but only the 44.5% of the respondents updates promptly the software in production. The causes may be different, but most of them are organizational: in particular the lack of knowledge of the availability of patches, lack of procedures for software testing, the non-renewal of software maintenance contracts, that often is caused from the severe economic crisis that still remains in Italy
- The behaviour of ICT users and ICT operators is the most critical and widespread vulnerability, on which the majority of successful attacks are based. Facilitators and amplifiers of personal vulnerability are some instruments such as social networks, e-mail, search engines, collaborative tools, the more powerful USB sticks and the now prevalent use of mobile devices. These tools facilitate the possibility to steal the identities of users and acquire their confidential information with which to carry out attacks and make computer frauds.
- For the user of cloud services, three-quarters of respondents did not detect attacks, only 3.4% have suffered them on applications (SaaS, Software as a Service), and 2.5% on ICT infrastructures (IaaS, Infrastructure as a Service); no attacks on PaaS, Platform as a Service, have been detected. These low percentages are a clear indicator of the reliability and availability of the cloud services in use.
- Three-quarters of the user of cloud services has not detected attacks, only 3.4% have suffered them on applications (SaaS, Software as a Service), and 2.5% on ICT infrastructures (IaaS, Infrastructure as a Service); no attacks on PaaS, Platform as a Service. These low percentages are a clear indicator of the good level of digital security of the cloud services in use.
- The main motivation for the digital attacks (particularly the most feared in the next future) is to get the illegal economic returns: the estimates of respondents are 52.1% for fraud, 51.3% for blackmail and 28.1% for espionage, particularly industrial.
    - During 2015, The Postal and Communications Police of Italy, as part of the fight against “financial cybercrime,” has checked 16,697dubious online transactions in 10 banking groups, blocking € 65,870,825.63 and recovering € 2,734,269.31.
    - Only 1.3% of respondents stated that in 2015 they had a subtraction of money in the bank accounts caused by the theft of digital identity: an indicator that the computer systems used by the sample of Italian banks ensure a good level of digital security.
- Regardless of the size and the product sector of the respondents, a

significant part of the sample utilizes computer systems at the status of the art and technically promptly updated:

- 52.1%, has informatics architectures with high reliability;
- 42.1% has a Business Continuity Plan;
- the operating systems of the servers are mainly of the last versions: the 68.9% uses Windows Server 2012, and the 14.3% uses Windows Server 2016. The 58.8% uses hypervisors for server virtualization.

- The technical measures for digital security, from the physical ones to those for the data protection, are fairly widespread throughout the sample.
  - A significant 15.1% of respondents are using behavioural analysis for ICT systems and users, one of the most advanced tools for preventing functional and technical deterioration of ICT ssytems, and therefore for identifying possible attacks on going.
  - Some of the weaknesses, as a percentage of dissemination, concern the inspection of the software code , performed by 16.8%, the systematic management of patches and versions, performed by just over half of the sample, the encrypted storage of critical information, performed by 21.8%, the management of operator logs, mandatory for privacy, carried out by less than half of the respondents, the periodic test of the Disaster Recovery plans made by the 21% against a 39.5% which published a Disaster Recovery plan.
- The organizational level is less advanced than the technical one for the digital security of the sample, although some aspects are positive and underline some improvements, as trend, compared to the figure recorded in the previous editions:
  - 57.4% of the sample did not set policy on digital security;
  - the organizational structure for digital security is not formally and/or very well defined for most of the respondents: 39.5% defines a clear role for CISO and in the 18.6% of the cases this role is directly performed by the CIO; only a small fraction of the sample, 3.1%, outsources the CISO role to external professionals or companies;
  - for internal roles concerning digital security, only the 12.6% requires specific certifications; for external suppliers and consultants these certifications are required by the 11.8% of the respondents;
  - the systematic use of standards and best practices for digital security and its government is still limited mainly to the largest structures:
    - the standards of the ISO 27000 family are adopted with certifications from 12.6% of respondents;

    - ITIL is followed by certified personnel by the 12.6%;
    - COBIT is followed with certifications by the 3.4%;
- the risk analysis is carried out by the 23.5% of respondents; the 20.2% already assures the residual risk, and the 13.4% intend to do so in the near future;
- the ICT audit, internal, external or mixed, is performed by the 45.8% of respondents; the 65.5% of these performs it in a structured way, periodic and regular.

In conclusion, OAD 2016 confirms the macro-trend of the previous OAI reports and of the recent international surveys. Due to the huge number of small and very small organizations that constitute its economic kernel, Italy now does not fall among the countries most affected by digital attacks. The majority of the respondents have improved the security level of their ICT systems, but the latest digital attacks are more and more sophisticated, more and more difficult to detect and they can seriously impact the attacked companies. mainly for losses in finance and in reputation. Moreover, not only the ICT critical infrastructures should be a target for terrorism, but also small realities may be subject to massive and parallel attacks, with the objective, being these last less protected, to cause a collapse of the whole Italian economy. Until now Italy is not a key target of the cyber-crime and of a terroristic cyber war, but runs a growing risk to be an easy target in the near future if the awareness and the culture of digital security is not growing in the country at every level.

2 Introduzione

L'iniziativa OAD, Osservatorio Attacchi Digitali in Italia, è l'evoluzione della precedente Iniziativa OAI, Osservatorio Attacchi Informatici in Italia, l'unica indagine on line via web in Italia sugli attacchi informatici per tutti i settori merceologici, incluse le Pubbliche Amministrazioni Centrali e Locali. Dall'elaborazione dei dati raccolti viene realizzato un rapporto annuale, che fornisce una specifica e concreta indicazione del fenomeno degli attacchi intenzionali sui sistemi informatici italiani.

Obiettivo primario di OAD è raccogliere ed elaborare le indicazioni sugli attacchi intenzionali rilevati dalle aziende/enti, individuando lo specifico trend del fenomeno in Italia ed essere così di riferimento, autorevole e indipendente, per l'analisi e la gestione dei rischi informatici. Ulteriore e non meno importante obiettivo è quello di aiutare nella diffusione di sensibilità e cultura in materia di sicurezza informatica soprattutto presso i decisori "non tecnici", figure tipicamente ricoperte dai vertici dell'organizzazione che decidono e stabiliscono i budget ed i progetti per la sicurezza informatica.

Il presente Rapporto 2016 fa riferimento agli attacchi informatici rilevati nel corso del 2015. Costituisce la sesta edizione, dopo i precedenti rapporti del 2015 (2014), 2013, 2012, 2011 e del 2009-10, che nel loro insieme coprono gli attacchi rilevati e subiti dal 2007 a fine 2015.

Anche questa edizione, come la precedente, è sponsorizzata da Associazioni ed Aziende del settore. Gli Sponsor del presente rapporto sono l'associazione AIPSI[1] e le aziende dell'offerta ICT[2] F5 Networks, Gruppo Sernet, Technology Estate, Trend Micro, le cui schede di presentazione, con l'approfondimento delle loro attività nel campo della sicurezza informatica, sono inserite in ordine alfabetico nell'Allegato I.

OAD 2016 annovera, oltre alla collaborazione con la Polizia delle Comunicazioni, il patrocinio di AICA (Associazione Italiana Calcolo Automatico), AIPSI (Associazione Italiana Professionisti Sicurezza Informatica), Assintel di Confcommercio (Associazione Nazionale Imprese ICT), Assolombarda di Confindustria, AUSED (Associazione Utilizzatori Sistemi e Tecnologie dell'informazione), CDI (Club Dirigenti Informatica di Torino), CDTI (Club Dirigenti Tecnologie dell'Informazione di Roma), Club per le Tecnologie dell'Informazione Centro, Club per le Tecnologie dell'Informazione Liguria, Club per le Tecnologie dell'Informazione di Milano, FidaInform (la Federazione dei ClubTI Italiani), FTI (Forum per le Tecnologie dell'Informazione), il Capitolo Italiano di IEEE-Computer Society, Inforav (Istituto per lo sviluppo e la gestione avanzata dell'informazione), itSMF Italia (information technology Service Management Forum).

1 AIPSI, Associazione Italiana Professionisti Sicurezza Informatica, (http://www.aipsi.org/) capitolo italiano della mondiale ISSA (https://www.issa.org/)

2 ICT, Information and Communication Technology

Nell'iniziativa OAD il ruolo attivo dei Patrocinatori è determinante per allargare e stimolare il bacino dei possibili risponditori contattati, oltre che per far conoscere e divulgare il rapporto annuale, contribuendo in tal modo anche alla diffusione della cultura sulla sicurezza ICT.
Le precedenti edizioni[3] del Rapporto OAI sono scaricabili gratuitamente dai siti web elencati in nota. Il Rapporto 2016 è scaricabile per 4 mesi dalla sua pubblicazione in esclusiva ai soli interlocutori degli Sponsor cui è stato inviato da questi ultimi l'opportuno codice-coupon. Dopo i quattro mesi dell'esclusiva, il Rapporto 2016 è liberamente scaricabile da chiunque sia interessato, così come i Rapporti dei precedenti anni.

Per la corretta ed effettiva comprensione del Rapporto, si richiede che il lettore abbia delle conoscenze di base di informatica e di sicurezza ICT, dato l'uso di termini tecnici. Per facilitare la lettura, è disponibile nell'Allegato D un glossario degli acronimi e dei termini tecnici specialistici usati.

2.1 LE MOTIVAZIONI DELL'OSSERVATORIO SUGLI ATTACCHI INFORMATICI 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/ 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, (nell'Allegato C.2 un elenco delle principali e più aggiornate fonti), ma difficilmente essi forniscono dati specifici sulla realtà italiana, salvo casi eccezionali.

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

3 I precedenti Rapporti OAI sono scaricabili dal sito web dell'Autore, www.malaboadvisoring.it, dal sito di AIPSI, www.aipsi.org, e dai siti di alcuni Sponsor e Patrocinatori.

- 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 dall'autore con OCI, Osservatorio Criminalità Informatica, di FTI-Sicurforum[4]. 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.

Dato il successo riscosso nelle precedenti edizioni, l'iniziativa OAD continua e si consolida grazie alla collaborazione con NEXTVALUE e con la comunità italiana di CIONET (per approfondimenti si veda http://www.cionet.com/about/cionet-italy/), oltre che grazie alle sponsorizzazioni che consentono di coprire almeno parzialmente i costi vivi, e si posiziona come l'unica indagine indipendente in Italia basata sulle risposte al questionario annuale da parte di chi si occupa, direttamente o indirettamente, della sicurezza ICT nella propria azienda/ente o per terzi.

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

3 Le tipologie di attacco considerate

OAD, come il precedente OAI, è indirizzato alle azioni **deliberate** e **intenzionali** rivolte contro i sistemi informatici e non ai rischi cui i sistemi sono sottoposti per un loro cattivo funzionamento, per un maldestro uso da parte degli utenti e degli operatori, o per fenomeni accidentali esterni.

Come chiaramente specificato nel Questionario OAD posto sul web, 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 un'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.

La tassonomia degli attacchi informatici considerata nel Questionario è riportata nella seguente Tabella 1 (l'ordine non fa riferimento alla criticità o gravità dell'attacco; per la spiegazione dei termini gergali si rimanda al glossario in Allegato E).

Tabella 1 Tipologia degli attacchi considerati

1. **Attacchi fisici**, quali sabotaggi e vandalismi, con distruzione di risorse informatiche e/o di risorse a supporto (es. UPS, alimentatori, condizionatori, ecc.) a livello centrale o periferico.
2. **Furto di apparati informatici,** facilmente occultabili e trasportabili, contenenti dati (unità di rete, Laptop, hard disk, floppy, nastri, Chiavette USB, ecc.)
3. **Furto di informazioni** e loro uso illegale da **dispositivi mobili** (palmari, cellulari, laptop)
4. **Furto di informazioni** e loro uso illegale **da dispositivi non mobili** e da tutte le altre risorse ICT.
5. **Attacchi di Social Engineering e di Phishing** per tentare di ottenere con l'inganno (via telefono, e-mail, chat, ecc.) informazioni riservate quali credenziali di accesso, identità digitale, ecc.
6. **Ricatti sulla continuità operativa e sull'integrità dei dati del sistema informativo** (ad esempio: viene minacciato l'attacco, magari dimostrando la capacità di effettuarlo, ma non è effettuato; spesso il solo ricatto basta per effettuare la frode. Rientra in questa tipologia il ransomware)
7. **Accesso a e uso non autorizzato degli elaboratori, delle applicazioni supportate e delle relative informazioni**
8. **Modifiche non autorizzate ai programmi applicativi e di sistema, alle configurazioni ecc.**
9. **Modifiche non autorizzate ai dati e alle informazioni trattate**
10. **Utilizzo vulnerabilità del codice software**, sia a livello di posto di lavoro che di server: tipici esempi: back-door aperte, SQL injection, buffer overflow, ecc.
11. **Codici maligni (malware)** di varia natura, quali virus, Trojan horses, Rootkit, bots , exploits, sia a livello di posto di lavoro che di server.
12. **Attacchi per la saturazione di risorse ICT** : oltre a DoS (Denial of Service), DDoS (Distributed Denial of Service), si includono in questa classe anche mail bombing, spamming, catene di S. Antonio informatiche, ecc. Anche le botnet possono essere indirizzate a DDoS, ma richiedendo degli agenti (bot) sono considerate malware
13. **Attacchi alle reti, fisse o wireless, e ai DNS** (Domain Name System)
14. **Attacchi mirati (targeted) e APT**, Advanced Persistent Threats, basati su uso contemporaneo e/o persistente di più tecniche sofisticate di attacco.

4 Gli attacchi informatici rilevati

La fig. 4-1 mostra, percentualmente, il numero di attacchi rilevati dai rispondenti nel 2015. Nel 2015 il 62,4% non ha mai subito o rilevato un attacco intenzionale, il 37,6% li ha invece subiti, e tra questi il 9,4% ha subito più di 10 attacchi nell'anno, come dettagliato nella fig. 4-2.

Fig. 4-1 Attacchi rilevati nel 2015 dal campione rispondenti OAD 2016

Fig. 4-2 Dettaglio del numero di attacchi subiti nel 2015 dal campione rispondenti OAD 2016 (288)

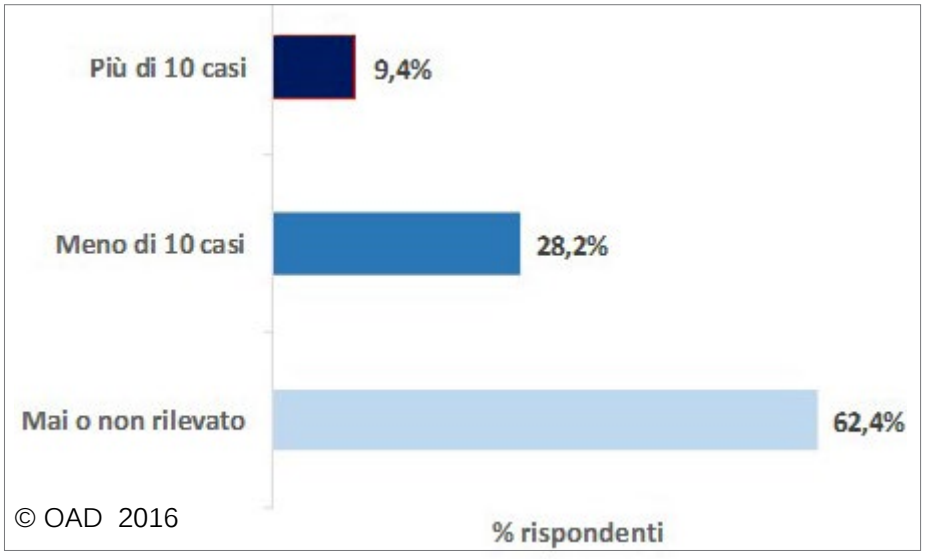
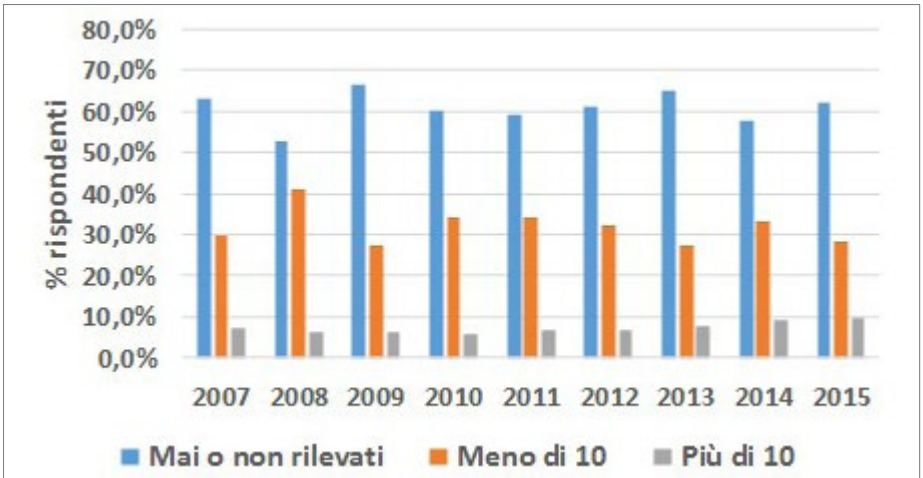
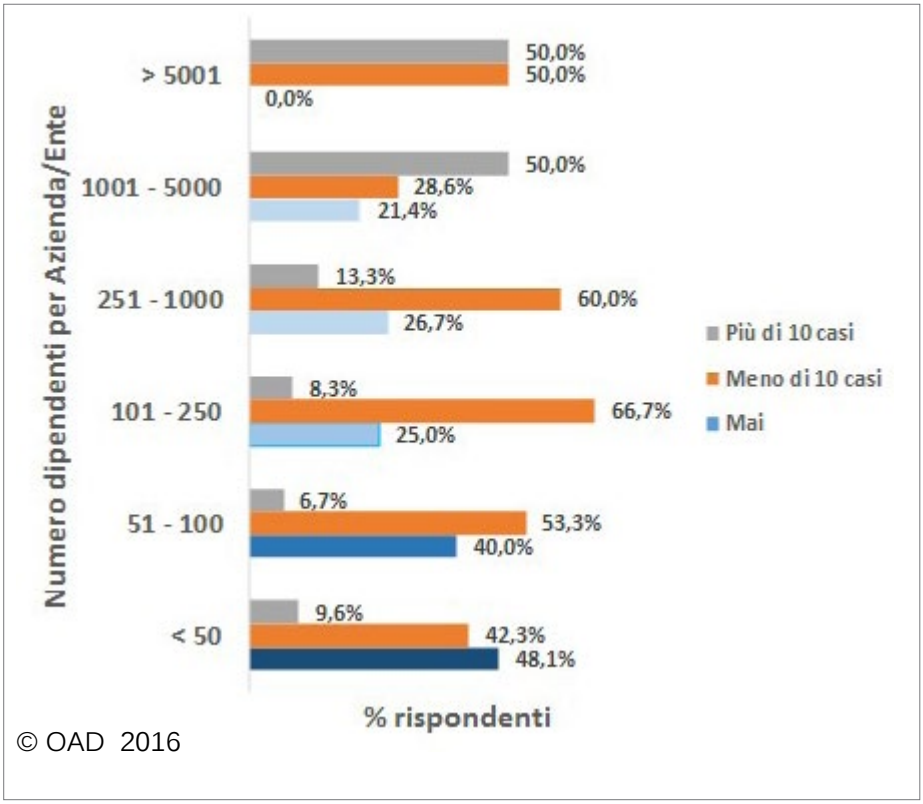


Fig. 4-3 Confronto percentuale degli attacchi rilevati nelle varie edizioni di OAI-OAD.



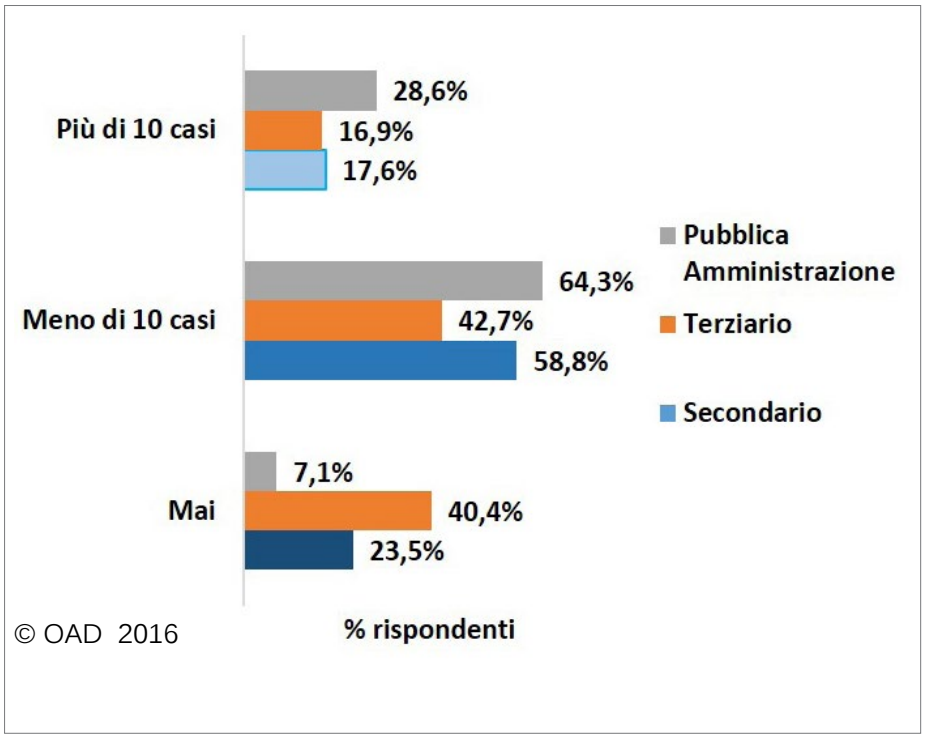
La fig. 4-3 confronta il numero di attacchi rilevati nei diversi Rapporti OAI dal 2007 al 2015, da considerare come trend puramente indicativo, dato che i campioni dei rispondenti nei diversi anni sono diversi come mix e come numero. Tale trend conferma la sostanziale stabilità del fenomeno in Italia, che evidenzia che a subire attacchi è sempre all'incirca il 40% del campione emerso nei vari anni, con una varianza limitata al 4,5%.
Nell'arco temporale considerato e per il campione emerso nelle varie indagini, il 2008 rappresenta l'"annus horribilis" per la quantità e la diffusione di attacchi occorsi, e il 2014 ha evidenziato un picco simile, leggermente ridotto nel 2015. Significativo che nel 2015 si è registrato il valore più alto di attacchi ripetuti nell'intero arco temporale, con un 9,4%.
Il valore 40% per gli attacchi rilevati in Italia nelle precedenti indagini OAI e l'attuale OAD, pur con campioni diversi di rispondenti, si conferma negli anni con oscillazioni relativamente contenute; da alcuni esperti è considerato troppo basso, indice che molti attacchi non sono stati rilevati.
Questo è sicuramente possibile, a livello mondiale si stima addirittura che 2/3 degli attacchi non siano rilevati.
Ma per l'Italia un ulteriore importante elemento da considerare è l'esistenza di poche grandi aziende/enti ed il numero elevatissimo di piccole e piccolissime imprese, come dettagliato nell'Allegato B.1; queste ultime sicuramente non rappresentano un obiettivo di interesse specifico per i cyber criminali.
La convalida di questo assunto è data dall'analisi degli attacchi nel 2015 per dimensione di azienda/ente dei rispondenti, mostrata in fig. 4-4.
Per i dettagli sulle caratteristiche "macro" dell'organizzazione e dei sistemi informatici dei rispondenti si rimanda all'Allegato B.

Fig. 4-4 Percentuale numero di attacchi ripartiti per dimensione di azienda/ente



La figura mostra come, nel campione emerso, gli attacchi aumentino prevalentemente per dimensione dell'organizzazione, indicata dal numero di dipendenti: il "mai" si riduce dalle aziende con meno di 50 dipendenti fino ad azzerarsi per quelle con più di 5000 dipendenti.
Le grandi organizzazioni, nella fascia >5000, sono quelle più note e più appetibili dal cyber crime, e sono anche quelle che hanno la maggior quota di più di 10 attacchi per anno.
La fig. 4-5 mostra il numero di attacchi subiti nei tre macro settori secondario, terziario e Pubblica Amministrazione (PA), sia centrale (PAC) sia locale (PAL), nei quali sono stati accorpati i settori merceologici dei rispondenti, dettagliati nell'Allegato B.1. Come evidenziato nella fig. B-2 del citato allegato, si sono avute zero risposte da aziende del settore primario e relativamente poche, come purtroppo negli anni precedenti, dalla Pubblica Amministrazione, sia centrale sia locale. La maggior parte delle risposte è pervenuta da aziende dei servizi, quindi del terziario, e, seppur con percentuali più basse, da aziende manifatturiere, ossia del secondario.
La figura mostra come i rispondenti del settore terziario siano quelli che subiscono o rilevano meno attacchi rispetto ai rispondenti del settore secondario e delle PA.

Fig. 4-5 Percentuale numero di attacchi ripartiti per macro settore



Questo è dovuto anche ad una buona quota di rispondenti del settore ICT, che si presume abbiano misure di difesa alla stato dell'arte. Ma potrebbe valere anche qui il detto del "ciabattino con le scarpe rotte" !

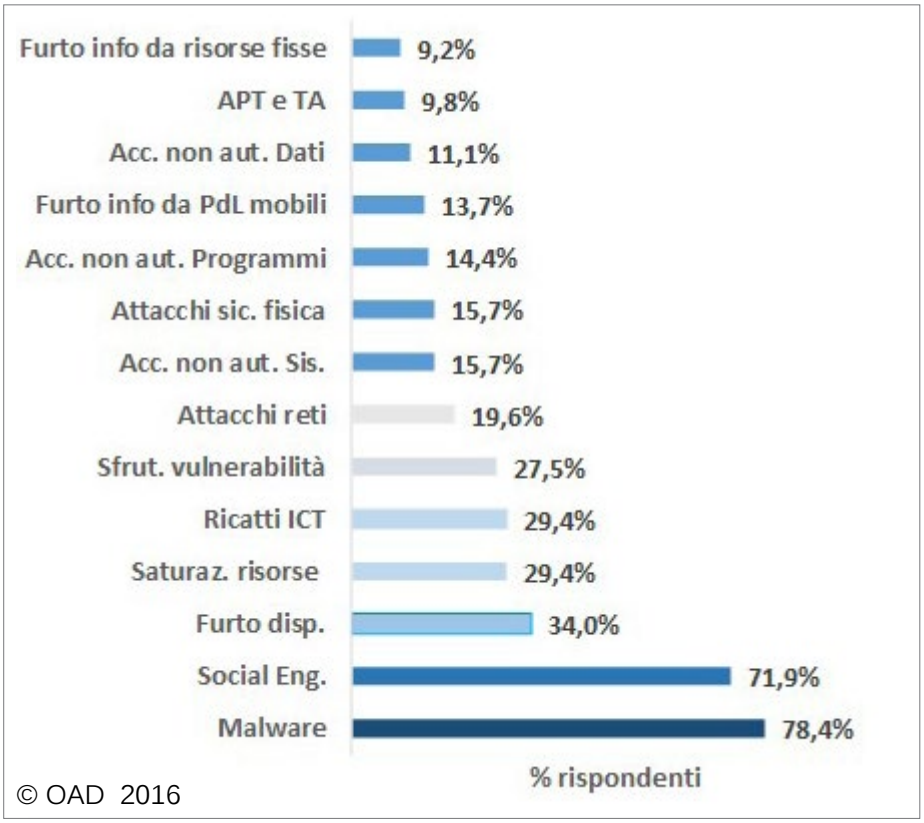
Facendo riferimento alle principali tipologie di attacco elencate nella Tabella 1, la fig. 4-6 mostra la diffusione in percentuale degli attacchi subiti nel 2015 dal campione dei rispondenti.

Anche per questa edizione, come per tutte le precedenti di OAI (si veda a conferma la fig. 4-7 che confronta le diverse rilevazioni negli anni, sempre e solo da considerare come semplice indicatore di taluni trend senza alcun valore statistico dati i bacini diversi di rispondenti), i primi quattro posti di attacchi più diffusi sono sempre occupati dai medesimi tipi di attacchi digitali.

Al primo posto permane il malware con un 78,4%, che include anche i codici maligni "ransomware" e senza contare il picco del 2008. Come indicato nella fig. 4-7, il **malware** è in crescita dal 2009, con un picco nel 2015 dovuto alla diffusione in Italia dei ramsomware. Per approfondimenti sui codici maligni si rimanda a §4.2.1.

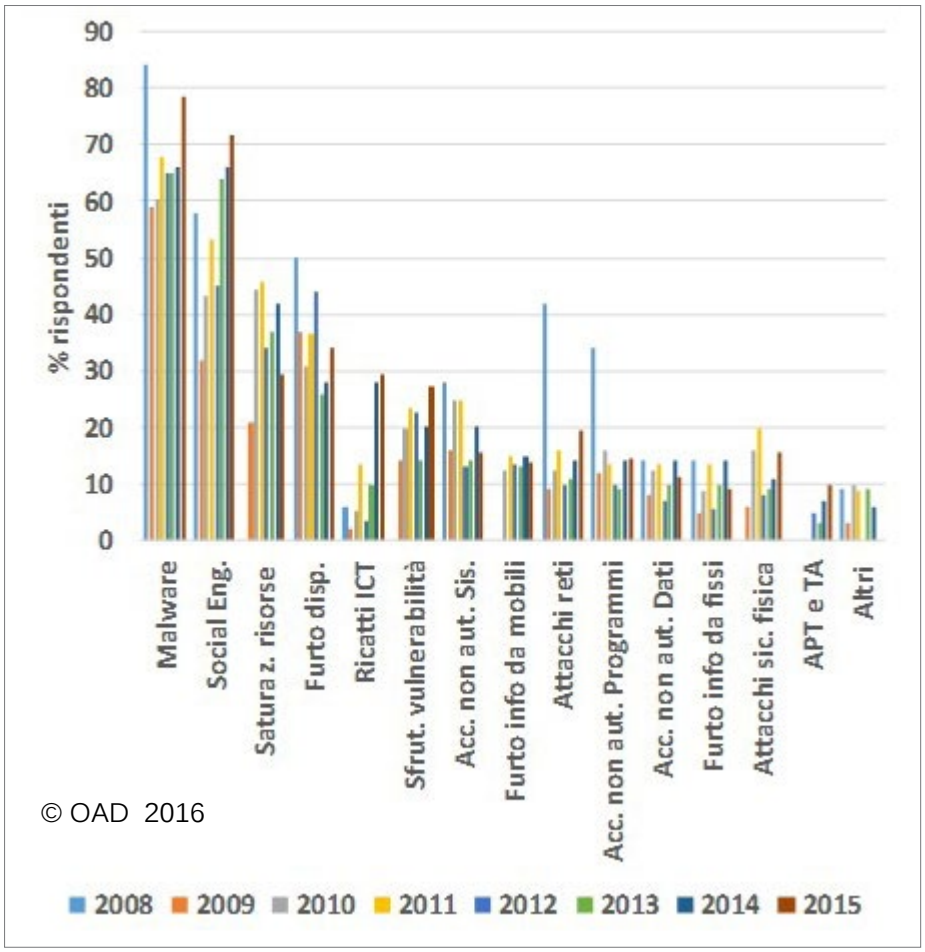
Al secondo posto il **social engineering** con il 71,9%. Questa categoria di attacco sovente costituisce l'inizio di attacchi ben più complessi come APT e TA, ed include il **phishing**, che negli ultimi anni dalla posta elettronica si è esteso agli SMS, alle chat, ai social network.

Fig. 4-6 Ripartizione percentuale per tipologia di attacco (risposte multiple)



Come evidenziato in fig. 4-7, il social engineering ha avuto nel 2015 il picco più elevato, e negli anni precedenti, a partire dal 2009, è stato sempre in crescita come diffusione;
Al terzo posto, con un 34 % fortemente distaccato come percentuale rispetto ai due valori precedenti, il **furto di dispositivi ICT**.
Tale tipologia di attacco era al quarto posto nell'edizione precedente, e si è scambiata il posto con la "saturazione delle risorse ICT".
Questo tipo di furto "fisico" non si limita ai soli sistemi mobili, ma a qualunque dispositivo di piccole dimensioni e non molto pesante, facilmente asportabile ad esempio nascondendolo nella propria borsa, in una tasca, sotto una giacca, un impermeabile o un cappotto; rientrano tra questi dispositivi le periferiche, dalle web cam ai mouse o alle stesse tastiere, i lap top, gli hard disk removibili e le sempre più capaci chiavette USB.
L'esplosione della diffusione di tablet e di smartphone ha ampliato il bacino dei potenziali oggetti ICT rubabili, più per venderli sul "mercato nero" che per carpire le informazioni in essi contenuti.
Al quarto posto la **saturazione delle risorse ICT** (DoS/DDoS), con un 29,4%, insieme ai **ricatti ICT**.

Fig. 4-7 Ripartizione percentuale per tipologia di attacco dal 2008 al 2015 (risposte multiple)



Come evidenziato nella fig. 4-7, nel 2014 e nel 2015 i ricatti ICT hanno avuto un forte incremento percentuale, pur con bacini diversi di rispondenti: questo probabilmente è anche dovuto alla forte diffusione in Italia dei ramsoware, che avrebbero dovuto essere conteggiati solo nei malware, come esplicitamente chiarito nel Questionario sia del 2014 sia del 2015[5].
Nei precedenti Rapporti OAI si era già parlato del "pizzo informatico" come potenziale attacco "di massa", dovuto sia alla crescente diffusione di "ransomware", sia alla verifica, con opportune scansioni da remoto, della debolezza delle protezioni in essere sul sistema ICT obiettivo, e poi minacciando l'azienda/ente di compiere attacchi se non viene pagato il "pizzo" richiesto.
Tutti gli altri tipi di attacchi nel 2015 si attestano come diffusione tra i rispondenti sotto il 20%, e due soli, TA/APT ed il furto di informazioni da dispositivi fissi, al di sotto del 10%.

5 Non è possibile individuare se i rispondenti, in caso di attacco con Crypto Locker o simili, hanno selezionato la risposta nel questionario di malware, di ricatti o di entrambi.

Al settimo posto gli **attacchi alle reti**, con un 19,6%. La tendenza nel tempo è di crescita, pur con qualche oscillazione, derivata principalmente dal crescente uso delle reti mobili, sia locali che geografiche, e dalla loro integrazione con quelle fisse. Tipici attacchi alle reti si basano su DNS spoofing e sullo spoofing dell'indirizzo IP.
All'ottavo posto con identica percentuale del 15,7%, l'**accesso non autorizzato ai sistemi ICT** e gli **attacchi alla sicurezza fisica** dei sistemi ICT e dei locali nei quali si trovano. L'accesso non autorizzato ai sistemi ICT, visti come un tutt'uno, è il primo passo per accedere illegalmente ai programmi software ed ai dati da questi ultimi trattati, dati che solitamente rappresentano il bene digitale da rubare per compiere frodi, tipicamente il furto dell'identità digitale di una persona.
Negli attacchi alla sicurezza fisica rientrano sabotaggi e vandalismi, con distruzione di risorse informatiche e/o di risorse a supporto (es. UPS, alimentatori, condizionatori, ecc.) a livello centrale e/o periferico. Pur se con percentuali basse e tra gli ultimi nella classifica, gli attacchi alla sicurezza fisica sono in crescita dal 2012 ma, come evidenziato nella fig. 4-10, non hanno provocato impatti significativi, mentre nel 2014 essi avevano causato i danni più gravi nel campione dei rispondenti.
A giudizio dell'autore una delle cause degli attacchi fisici è dovuta al relativamente alto numero di di PMI tra i rispondenti, come analizzato nell'Allegato B.1, e questi normalmente hanno limitati meccanismi di protezione e controllo.
Al decimo posto **l'accesso non autorizzato ai programmi software**, con una percentuale del 14,4%, correttamente inferiore al 15,7% dell'accesso all'intero sistema ICT. L'accesso logico ai sistemi ICT ed alle loro applicazioni senza averne i diritti avviene prevalentemente grazie alla conoscenza delle password di chi ne ha i diritti, ed è particolarmente critico quando si scoprono e si usano i diritti di amministratore. Le più semplici e diffuse tecniche per scoprire gli "account" di un utente o di un amministratore sono il "social engineering" e lo "sniffing", relativamente più facile tramite reti wireless. Esiste poi il mercato nero degli "account" su Internet dove, con vari rischi ma a prezzi accessibili, si possono illegalmente comperare liste di "account". Lato utente finale l'accesso ad un sistema per accedere ad una applicazione è di solito trasparente, ossia non visto; l'accesso e l'uso non autorizzato di un sistema, visto come un'unica entità, è quindi considerato più lato operatori e sistemisti, e non lato utenti finali. Anche l'accesso non autorizzato ai dati può avvenire tramite attacchi diretti ai file system e alle banche dati, senza dover passare per l'applicazione che li tratta.
All'undicesimo posto **il furto di informazioni da dispositivi d'utente mobili,** con un 13,7% di diffusione sul campione di rispondenti. Come già evidenziato nei precedenti Rapporti, questo furto può essere correlato sia al furto "fisico" dei dispositivi sia alle numerose vulnerabilità dei sistemi operativi, da

Android a iOS, da Windows Phone a Blackberry, e delle relative applicazioni, chiamate in gergo "app". Tale furto ha come obiettivo una frode, basata il più delle volte sul furto dell'identità digitale.
Al dodicesimo posto si posiziona con un 11,1% **l'accesso non autorizzato ai dati** trattati da programmi software e/o archiviati in file system o banche dati.
Al tredicesimo posto gli **attacchi APT, Advanced Persistent Threats, e TA, Targeted Attacks**, basati su uso contemporaneo e/o persistente di più tecniche sofisticate di attacco, con una diffusione nel campione del 9,8%. TA ed APT costituiscono la frontiera più critica, in quanto si tratta di attacchi condotti da esperti con notevoli risorse a disposizione, e pertanto sono prevalentemente rivolti ad infrastrutture critiche. Tali attacchi sono talvolta vere e proprie azioni di "guerra informatica": esempi[6] ormai ben noti di questi attacchi a livello mondiale, iniziati presumibilmente da fine 2009, sono l'Operazione Aurora, Stuxnet, LuckyCat, DigiNotar, Global Payments Inc., Flame, Anthem, Home Depote, JP Morgan Chase. Pur se di difficile identificazione, APT e TA iniziano ad essere presenti e in crescita dal 2013 anche in Italia, come evidenziato dalla fig. 4-7, e percentualmente raggiungo nel 2015 la diffusione più alta, almeno nel campione dei rispondenti. Pur con tutte le precauzioni più volte sottolineate nel paragonare i dati emersi dai precedenti Rapporti, tale continua crescita è un chiaro indice dell'inasprimento del cyber-crime di alto livello in quest'ultimo periodo. Al quattordicesimo ed ultimo posto per diffusione **il furto di informazioni da dispositivi d'utente fissi,** con il 9,2% nel 2015, che allarga sensibilmente, rispetto alle edizioni precedenti, la differenza tra furto di informazioni dai dispositivi d'utente mobili e quelli fissi. Questo dato si collega con e dipende da quello del furto di dispositivi mobili, e dalla crescente sostituzione dei dispositivi d'utente fissi con quelli mobili. L'andamento storico della diffusione è oscillante, come mostra la fig. 4-7, ma la disponibilità a basso prezzo di hard disk e chiavette con interfaccia USB e capacità dell'ordine dei Tera rende facile copiare tutto il contenuto di un posto di lavoro ed anche di un server o di un storage. Nessuna indicazione per il 2015 come **"Altri"**, per attacchi non includibili nelle tipologie di cui alla Tabella 1.

4.1 GLI IMPATTI DAGLI ATTACCHI SUBITI

Il Questionario OAD, come quello della precedente edizione, ha richiesto, a seguito degli attacchi subiti, quali impatti hanno avuto, se poco o molto significativi. Per non appesantire il questionario, non si è voluto dettagliare il tipo di impatto, ad esempio economico, legale, di immagine, lasciando al compilatore la libertà di rispondere considerando qualitativamente l'intera valenza del termine "impatto" per la sua azienda/ente.
Le risposte avute dai rispondenti che hanno subito rilevato gli attacchi sono sintetizzate nella fig. 4-8, che evidenzia, fatto 100 il numero complessivo

6 Per approfondimenti si rimanda alla vasta documentazione disponibile in Internet; a cura dell'autore alcuni articoli su APT e TA pubblicati nella Rubrica OAI su Office Automation,
scaricabili da http://www.malaboadvisoring.it/index.phpoption=com_content&view=article&id=31&Itemid=50

di attacchi, che solo il 14,6% del totale li ha considerati molto significativi. Facendo riferimento al numero di attacchi subiti dalla singola azienda/ente, la fig. 4-9 dettaglia la valutazione dell'impatto per numero di attacchi subiti nel 2015.

Fig. 4-8 Ripartizione percentuale tra attacchi poco e molto significativi per chi li ha subiti

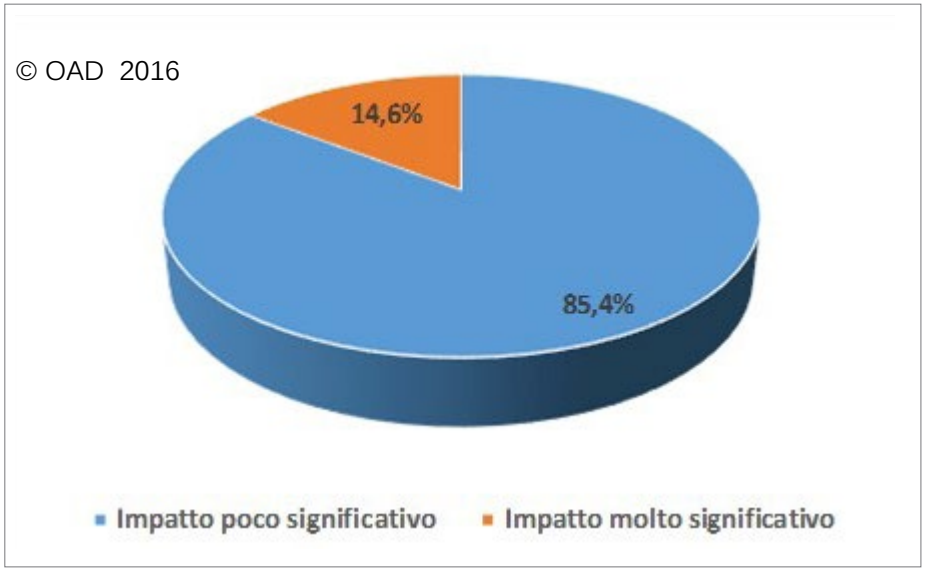
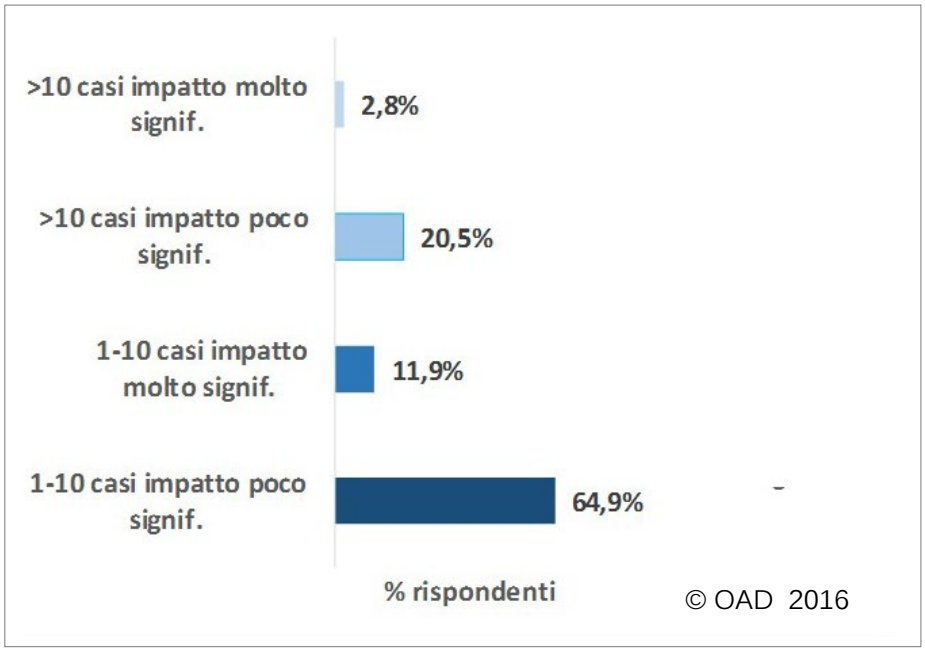


Fig. 4-9 Ripartizione percentuale dell'impatto per numero di attacchi subiti



Si evidenzia come la stragrande maggioranza considera gli impatti subiti poco significativi, indipendentemente da quanti ne ha subiti nell'anno.
La fig. 4-10 classifica le 14 tipologie di attacchi considerati (sui veda Tabella 1) in funzione della valutazione, per ciascuno di essi, di impatti significativi per chi li ha subiti: come facilmente prevedibile, gli impatti più gravi sono attribuiti in primis ai ricatti ICT, seguiti con quasi 10 punti di distacco dalla saturazione delle risorse, dai malware e dagli APT e TA, tutti superiori al 20%, come evidenziato nella fig. 4-10.
La fig. 4-11 correla l'impatto molto significativo dell'attacco con la sua diffusione, nel campione dei rispondenti: emerge che alcuni attacchi relativamente poco diffusi, hanno percentualmente tra i più alti impatti: ricatti ICT, APT e TA.

Fig. 4-10 Tipologia di attacchi con impatti molto significativi sull'azienda/ente (risposte multiple)

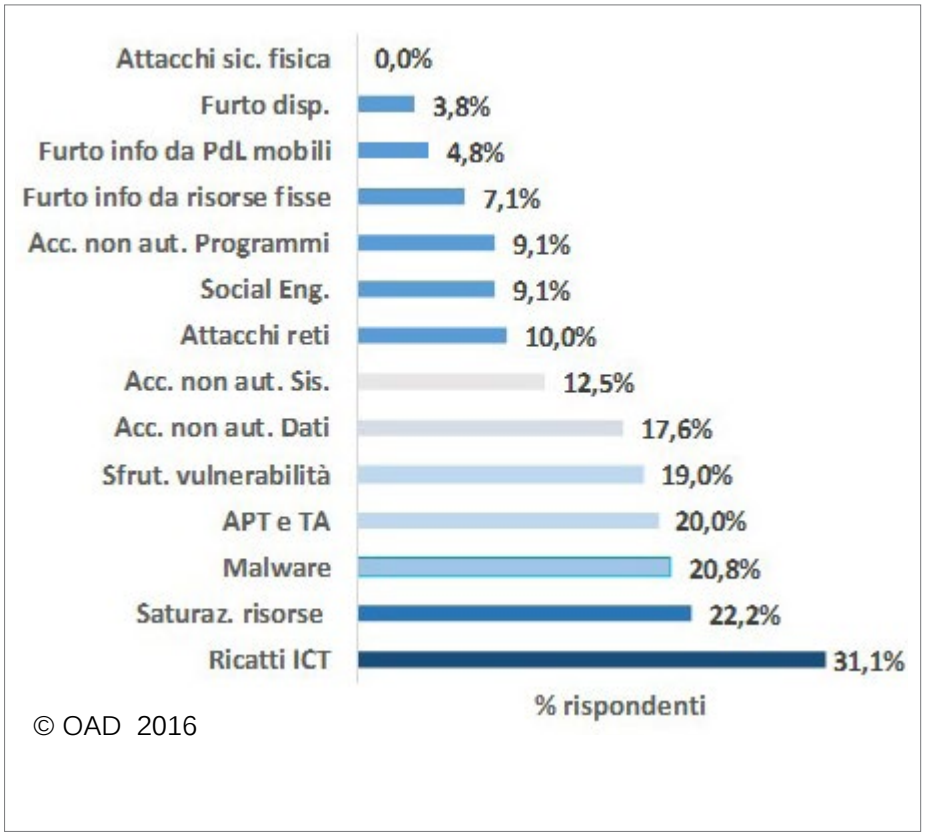
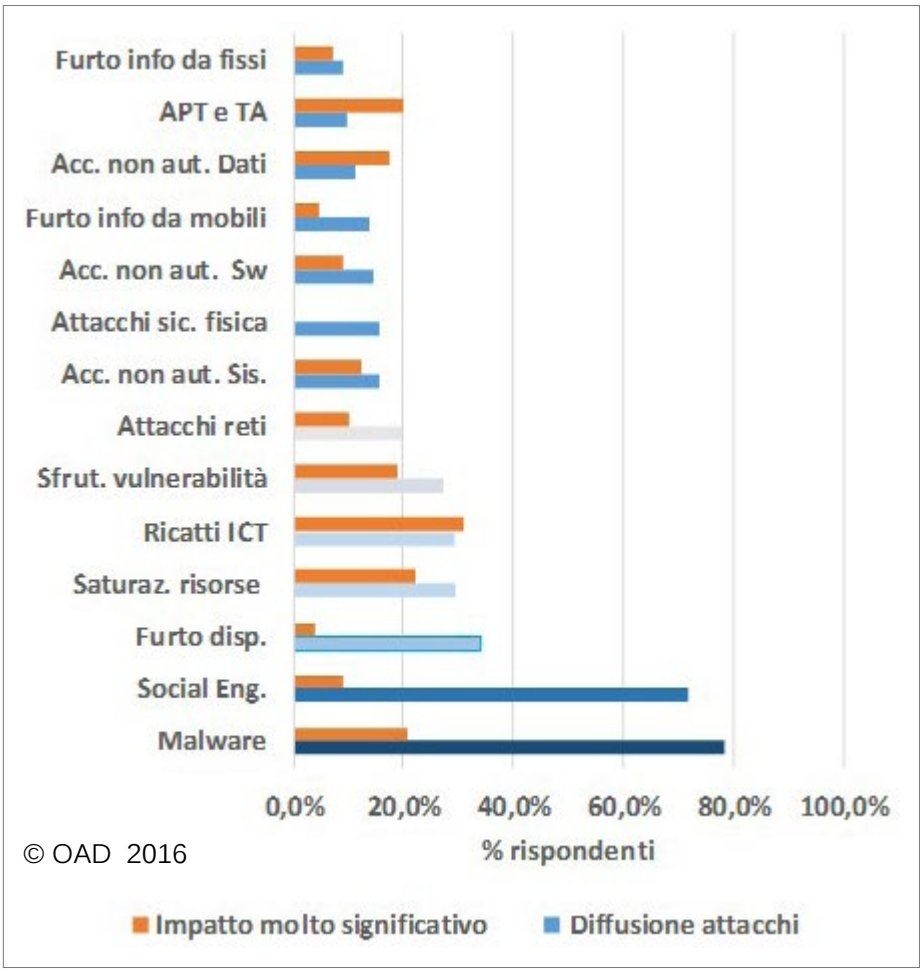


Fig. 4-11 Correlazione tra impatti molto significativi e diffusione degli attacchi (risposte multiple)



4.1.1 L'impatto economico degli attacchi digitali

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, anche per il danno economico è stata lasciata libertà al rispondente di considerarlo e stimarlo secondo le sue abitudini e prassi.

La fig. 4-12 indica che la stima economica di un attacco non è effettuata dal 43,5 % dei rispondenti, che il 25,9% la effettua per tutti gli attacchi subiti, il 10,2% solo per quelli più gravi. Tali dati percentuali sono analoghi a quelli della precedente edizione di OAI. Alcuni dei rispondenti che effettuano la stima economica hanno indicato sia il valore più alto per un singolo attacco, sia il valore complessivo del costo di tutti gli attacchi subiti nel 2015, come riportato nella Tabella 2.

Fig. 4-12 Stima del danno economico degli attacchi subiti

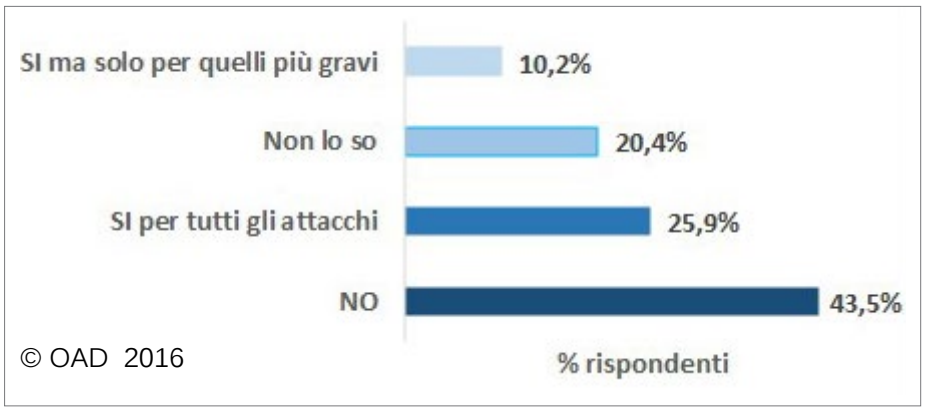


Tabella 2 Valori medi e massimi dei costi economici degli attacchi subiti nel 2015 (Fonte OAD 2016)

Valore medio costo del singolo attacco più grave	3.605,3
Valore più alto del costo del singolo attacco più grave	€ 70.000,00
Valore medio del costo complessivo di tutti gli attacchi subiti nel 2015	€ 6.013,30
Valore più alto del costo complessivo di tutti gli attacchi subiti nel 2015	€ 120.000,00

Diversi i possibili metodi di calcolo, e di qui la forte eterogeneità dei dati forniti dai pochi rispondenti (34 in totale, ma più numerosi delle precedenti edizioni OAI). Dato il basso valore indicato, è ragionevole ipotizzare che i rispondenti hanno fatto riferimento ai soli costi diretti per il ripristino della situazione informatica ex ante, e non considerano altri costi quali l'impatto sul business, la perdita di fatturato e di immagine, e così via.
La recente ricerca del Ponemon Institute, sul costo della violazione dei dati (data breach[7]), effettua anche per l'Italia con il coinvolgimento di 24 aziende/enti italiani di 11 diversi settori merceologici, evidenzia i seguenti aspetti principali:

- Il costo di violazione dei dati per persona continua, in media, a crescere: da € 105 nel 2015 a € 112 nel 2016;
- In Italia determinati settori merceologici hanno costi più elevati, rispetto alla media di cui sopra: in particolare le industrie dei servizi, quelle finanziarie e della sanità. Altri settori hanno un costo decisamente inferiore,

7 Si veda "Ponemon Institute: 2016 Cost of Data Breach Study: Italy" di Giugno 2016 e relativo ad attacchi rilevati nel 2015
8 DLP, Data Loss Prevention

ed includono le pubbliche amministrazioni e l'industria alberghiera;
- La maggior parte delle violazioni dei dati sono causate da criminali informatici per ottenere illegali ritorni economici (si veda anche §4.3 sul Financial Cybercrime): questa tipologia di violazione è la più difficile da identificare ed anche per questo è la più costosa come impatto economico;
- Alcune misure di prevenzione e di protezione riducono il costo della singola violazione, ed includono: l'uso estensivo della crittografia e di meccanismi di DLP[8], i piani di continuità operativa, l'uso di strutture quali il team di gestione degli incidenti e delle emergenze,
- 25% delle violazioni dei dati è causata da difetti dei sistemi ICT, sovente combinata a malfunzionamenti dei processi aziendali ad essi associati;
- Il 29% delle violazioni dei dati è causata dalla negligenza degli operatori ICT e dai fornitori di ICT.

4.2 GLI ATTACCHI ALLE INFRASTRUTTURE CRITICHE ITALIANE: I DATI DALLA POLIZIA POSTALE E E DELLE COMUNICAZIONI E DAL C.N.A.I.P.I.C.

Il C.N.A.I.P.I.C., Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (http://www.poliziadistato.it/articolo/view/23401/), 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 italiane che alla data hanno sottoscritto la convenzione per la protezione informatica con questa struttura sono: ANSA, ENAV, ENI, Ferrovie dello Stato, Intesa Sanpaolo, Poste Italiane, SIA, Snam Rete Gas, Sogei, Telecom, Vodafone. Nell'ambito della collaborazione con OAD, la Polizia Postale ha fornito i dati sulle azioni svolte dal C.N.A.I.P.I.C. nel 2015, riportate nella Tabella 3.

Tabella 3 Statistiche generali attività C.N.A.I.P.I.C. dal 1 gennaio al 30 novembre 2015 (Fonte: Polizia Postale e delle Comunicazioni)

Attacchi rilevati	633
Alert diramati	987
Monitoraggi	13500
Indagini avviate	55
Persone denunciate	44
Persone arrestate	2
Richieste di cooperazione High Tech Crime Network	95

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[9].

4.3 FINANCIAL CYBERCRIME

Considerando che la maggior parte degli attacchi sono effettuati per compiere frodi e far guadagnare economicamente gli attaccanti, nel Questionario 2016 di OAD è stata inserita una nuova specifica domanda, se l'Azienda/Ente ha subito nel 2015 sottrazioni di denaro sui conti bancari causati da furti di identità digitali.

Le risposte avute sono sintetizzate nella fig. 4-13, dove la stragrande maggioranza, più del 92%, dichiara di non aver subito furti sui conti bancari dell'azienda/ente, il 6,5% dichiara di non saperlo, e solo l'1,3% dei rispondenti afferma di aver avuto un furto < € 20.000,00, e nessuno di aver avuto un ammanco superiore a questa cifra.

Questa risposta è un significativo indicatore che i sistemi informatici delle banche italiane hanno buoni livelli di sicurezza e questo genere di frode informatica, basata sul furto delle identità digitali dei clienti, non produce che effetti di poco conto, almeno sul bacino dei rispondenti.

Fig. 4-13 Sottrazioni di denaro sui conti bancari nel 2015 causati da furto di identità digitale

9 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)

4.3.1 Gli attacchi digitali ai servizi di home banking e di monetica: il contrasto dalla Polizia Postale e delle Comunicazioni

La Polizia Postale è da sempre attiva per contrastare questo tipo di crimine informatico, che include anche sul commercio elettronico e sui relativi pagamenti on line.

In questo contesto la Polizia Postale e delle Comunicazioni ha iniziato dal novembre 2013 un progetto chiamato OF2CEN[10], On-Line Fraud Cyber Centre And Expert Network , che coinvolge le principali realtà bancarie italiane rappresentate dall'ABI, l'Associazione bancaria Italiana, oltre che il Gruppo Poste Italiane. Lo scopo del progetto è molteplice, dal raccogliere le segnalazioni di operazioni sospette da parte delle banche, all'analizzare e correlare le varie informazioni ricevute e all' informare le banche in tempo reale sui fenomeni fraudolenti cibernetici.

Tabella 4 Sintesi attività Polizia Postale di contrasto al cyberterrorismo ed ai reati di odio (Fonte: Polizia Postale e delle Comunicazioni)

Spazi web monitorati	
Spazi web (siti, forum, blog, media di informazione, profili twitter e facebook) verificati	11833
Spazi web monitorati	580
Accertamenti in cooperazione con altri Enti	268
Contenuti web oscurati direttamente dal Gestore del Servizio	6612
Contenuti web oscurati su segnalazione della Polizia Postale	23
Segnalazioni ricevute dai cittadini tramite Commissariato di PS On line	
Spazi web segnalati	179
Spazi web riconducibili al terrorismo	71
Atti discriminatori nei confronti delle minoranze	
Segnalazioni	541
Link	192
Denunciati	12
Attività anti terrorismo	
Denunciati	3
Arrestati	0

10 Si veda http://www.poliziadistato.it/articolo/30630/ - https://www.gcsec.org/it/activities/online-fraud-cyber-centre-experts-network-of2cen

Il progetto ha già dato significativi frutti, come l'Operazione Triangle, che ha smascherato una rete internazionale di criminali informatici operanti in Europa, Turchia, Cameron e Nigeria, conclusa con 62 arresti. Questa rete riusciva, con tecniche tipiche del "man in the middle", ad inserirsi nelle transazioni finanziarie tra aziende clienti e fornitori, dirottando i pagamenti su loro conti correnti, con ingenti profitti illegali.
Più in generale, OF2CEN ha visto ad oggi 10 gruppi bancari come "segnalanti" di operazioni on line dubbie, 16697 transazioni on line segnalate, bloccati € 65.870.825,63 e recuperati € 2.734.269,31.
Grazie ai successi ottenuti, il progetto italiano OF2CEN viene ora esportato in Europa con il nome di EU OF2CEN[11] .Il contrasto alle truffe on line si basa soprattutto sulla prevenzione, sul far conoscere e far comprendere a venditori ed acquirenti on line quali sono i pericoli di Internet e come fare per strutturare l'attività del commercio elettronico in maniera sicura, corretta ed efficiente. Forte in questa direzione l'azione di formazione e di sensibilizzazione della Polizia Postale e delle Comunicazioni sia a livello regionale, con incontri presso le organizzazioni imprenditoriali e nelle scuole, sia con una campagna nazionale per gli utenti di Internet chiamata "Una vita da social"[12].

4.4 IL CYBERTERRORISMO ED I CYBER REATI DI ODIO: IL CONTRASTO DALLA POLIZIA POSTALE E DELLE COMUNICAZIONI

Strumenti di informatica ed Internet contribuiscono fortemente al proselitismo ed alla preparazione e al coordinamento di attacchi terroristici. Ma 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. Considerando che le infrastrutture critiche ed i sistemi informatici di grandi aziende/enti hanno normalmente buoni livelli di protezione e di contrasto, e richiedono quindi significative risorse e competenze per poterli attaccare, più pericolosi, a giudizio dell'autore, risultano gli attacchi "massivi", ovvero contemporanei su migliaia di soggetti, tipicamente PMI, studi professionali, esercizi commerciali, i cui sistemi informatici sono, il più delle volte, semplici e non ben protetti e poco sicuri.

4.5 NUOVI E VECCHI ATTACCHI

Reti e sistemi mobili, cloud e servizi ICT terziarizzati, Internet delle cose sono negli ultimi anni le nuove frontiere per gli attacchi digitali, basati al solito sia sulle vulnerabilità dei sistemi ICT e delle loro architetture, sia sulla non conoscenza dei rischi e/o la superficialità degli utenti finali e degli operatori ICT nell'uso degli strumenti informatici.Su tali tematiche OAD 2016 ha posto alcune specifiche domande nel questionario on line, e nel seguito sono riportate e commentate le risposte avute.

11 Si veda http://www.poliziadistato.it/articolo/30663,
12 https://www.commissariatodips.it/vita-da-social.html

4.5.1 Reti e dispositivi d'utente mobili

Sull'uso di reti e di dispositivi d'utente mobili da parte delle aziende/enti dei rispondenti si rimanda all'Allegato B.

In termini di attacchi, la fig. 4-14 evidenzia come, sul totale dei rispondenti, più di 1/3 ha subito nel 2015 il furto di dispositivi ICT, tipicamente di tablet e di smart phone, oltre che di chiavette USB.

Fig. 4-14 Furto di dispositivi ICT, inclusi i dispositivi mobili

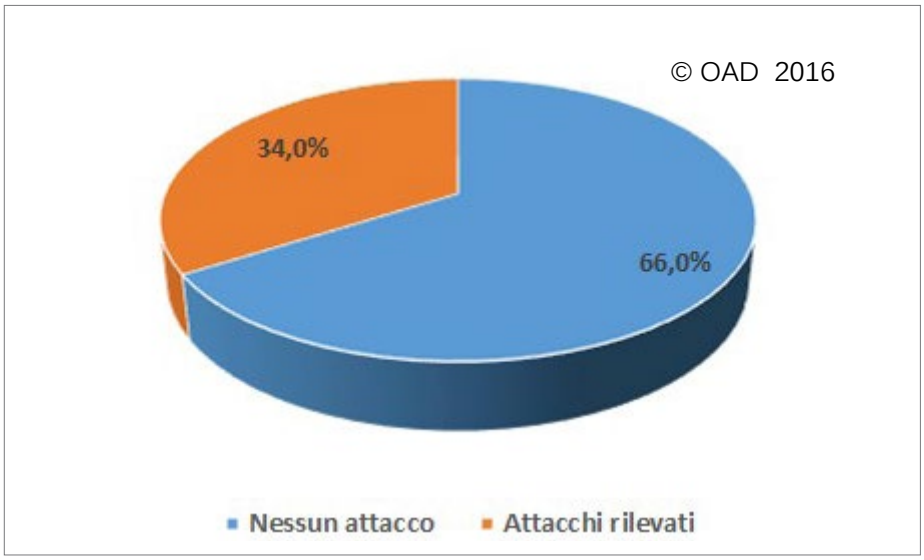


Fig. 4-15 Furto di informazioni da dispositivi mobili nel 2015

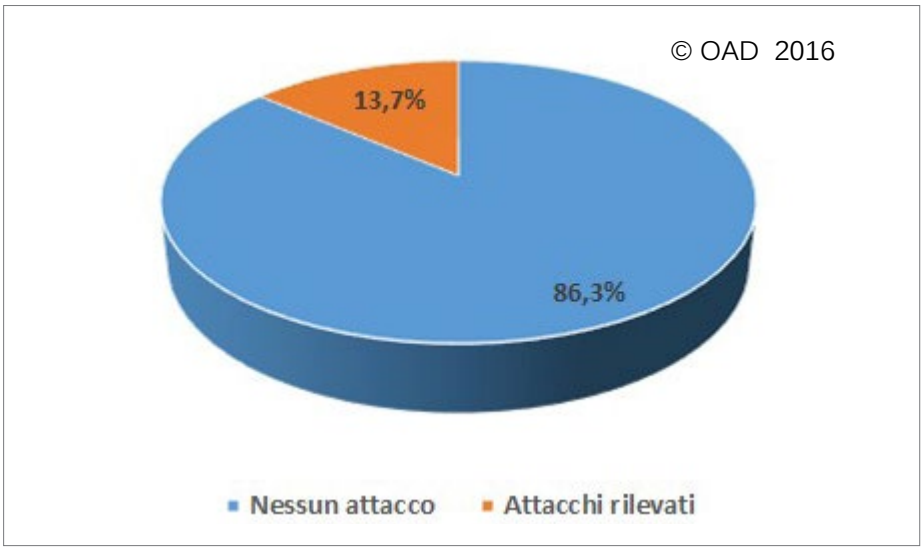
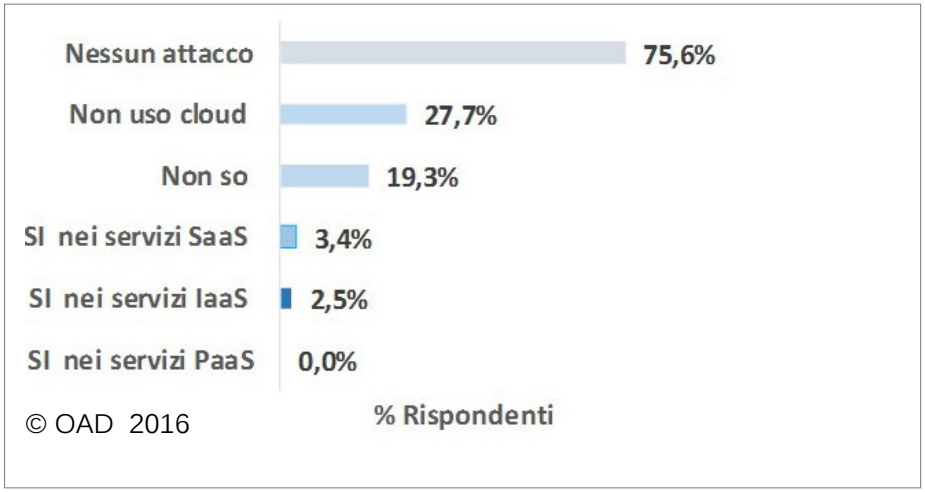


Fig. 4-16 Attacchi subiti nel 2015 ai propri sistemi ICT in cloud qualora siano utilizzati (risposte multiple)



Come già evidenziato in fig. 4-16, questa tipologia di attacco si posiziona al terzo posto come diffusione percentuale.
La fig. 4-15 dettaglia le percentuali di rispondenti che nel 2015 hanno subito furti di informazioni dai dispositivi mobili, sicuramente alcuni di questi a seguito del furto (o della perdita) del dispositivo stesso.
Il valore relativamente basso di 13,7% di chi ha rilevato furti di informazioni da dispositivi mobili conferma che questi sono prevalentemente rubati per rivenderli al mercato "nero".

4.5.2 Servizi ICT terziarizzati in cloud

L'uso di servizi in cloud è in significativa crescita, anche per le PMI, gli studi professionali, l'ambiente turistico ed alberghiero, gli esercizi commerciali.
Il timore di vulnerabilità nella sicurezza digitale aveva inizialmente ostacolato la loro adozione, ma il più delle volte i servizi in cloud hanno livelli di sicurezza ben superiori a quelli implementati ed implementabili sui sistemi informatici, in particolare di aziende/enti di piccole-medie dimensioni.
La fig. 4-16 evidenzia che il 27,7% dei rispondenti non utilizza servizi in cloud. Tra quelli che li usano, i ¾ non hanno rilevato attacchi ai loro servizi ICT in cloud, quelli che li hanno subiti sono in pochi: la percentuale maggiore, il 3,4%, con le applicazioni (SaaS, Software as a Service), a scendere, il 2,5%, con le infrastutture ICT (IaaS, Infrastructure asa a Service); nessun attacco subito dai rispondenti a livello di PaaS, Platform as a Service.
Tali dati confermano l'affidabilità e la sicurezza dei servizi ICT in cloud, che devono comunque essere scelti ed utilizzati con "buon senso", ed in osservanza delle normative sulla privacy.[13.]

13 Come esempio, si rammenta che alla data della stesura del presente Rapporto OAD 2016 l'accordo tra Europa e Stati Uniti sulla privacy, chiamato "harbour", non è più valido, e pertanto dati personali e sensibili non possono essere trattati in cloud con sedi all'infuori dell'Unione Europea e/o che non seguono le norme europee sulla privacy.

I servizi in cloud nel passato hanno avuto una crescita relativamente lenta dovuta proprio alla percezione di problemi di sicurezza.
Le applicazioni ed i dati della mia azienda sono su sistemi di terzi di cui nulla conosco, de gestiti da questi ultimi: al di là del contratto sottoscritto, come posso fidarmi ed essere realmente garantito sulla loro sicurezza?
Al contrario, come già evidenziato precedentemente, i livelli di sicurezza presenti nella maggior parte dei fornitori di cloud sono ben superiori a quelli implementati e/o implementabili nei sistemi informatici, di realtà medio-piccole. Ed il mercato dei servizi in cloud sta crescendo anche per i maggiori livelli di sicurezza fruibili.

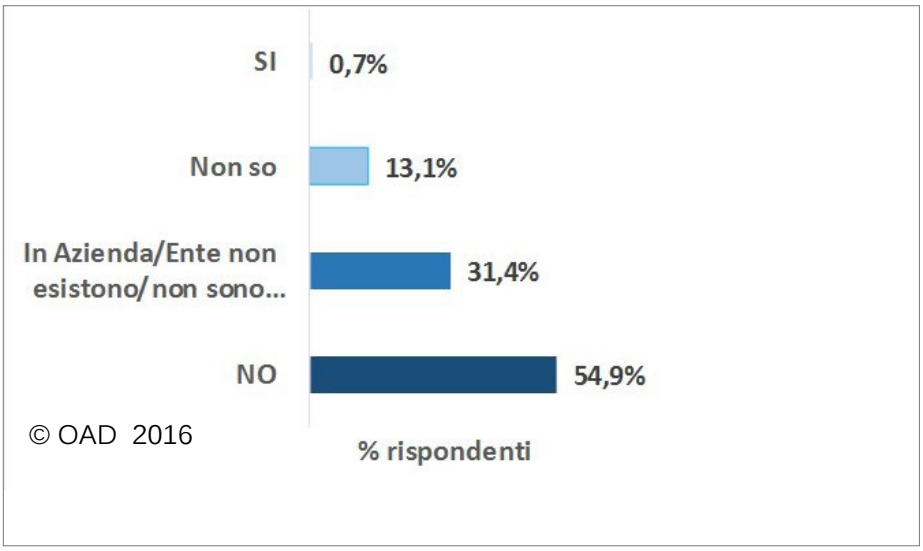
4.5.3 Gli attacchi per l'Internet delle Cose (IoT, Internet of Things)

Internet delle Cose, per brevità indicata nel seguito come IoT, Internet of Things, è il termine usato per indicare 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.
La capacità di comunicare via Internet con la sua pila di protocolli è l'elemento discriminante rispetto ai vari sistemi "embedded", che da anni esistono, dai sistemi di controllo industriali (DCS, Distributed Control System), ai sistemi automatizzati, fino a quelli robotizzati.
Fin dalla fine del 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 Gartner Group in un suo recente studio[14] prevede 20 Miliardi.
Gli IoT sono ormai pervasivi in ambito domestico e lavorativo: sono presenti nella domotica, negli elettrodomestici, nei controlli dei mezzi di trasporto (dalle autovetture agli aerei), nei giochi (es. slot machine), nei sistemi di pagamento, nella logistica e nell'automazione dei magazzini, nell'automazione industriale (DCS[15], PLC[16]), nei controlli delle infrastrutture, in sanità (telecontrolli medici avanzati, sale operatorie robotizzate, e-health), nei contatori smart delle utility (gas, elettricità, acqua), nelle smart city (chioschi e colonne informative, controllo e gestione viabilità, vigilanza urbana con videosorveglianza avanzata, pulizia strade, ecc.), nella stampa 3D, nella telemetria, nelle armi intelligenti, e così via. Gli IoT adottano, oltre alla pila di protocolli TCP/IP, gli standard de facto del mondo ICT mobile e fisso, quali Linux, Windows, Android, iOS, e sono pertanto soggetti allo sfruttamento di tutte le loro tipiche vulnerabilità. In più si deve considerare il problema della loro autenticazione (IoT è un oggetto con software, non una persona) ed il fatto che, in molti casi, gli oggetti sono non presidiati e/o non presidiabili. La raccolta di dati dagli oggetti avviene sovente su storage in cloud, aprendo così il fronte della sicurezza di questo ambiente, oltre che richiedere sempre più sofisticati livelli di integrazione ed interoperabilità con i sistemi informatici.

14 https://www.gartner.com/doc/3277832/forecast-iot-security-worldwide-
15 DCS, Distributed Control System
16 PLC, Programmable Logic Controller

Per la sicurezza IoT non si dovrebbero considerare solo le caratteristiche dell'oggetto e della sua "sicurezza intrinseca", ma anche tutti gli altri aspetti che includono il cloud, le applicazioni mobili (molti oggetti sono basati su OS mobili), le interfacce di rete, il software (è programmato in modo sicuro?), l'uso delle porte USB, la crittografia, le modalità di autenticazione.
La fig. 4-17 evidenzia, sul campione dei rispondenti, che più di 1/3 non utilizza IoT (sommando alla risposta esplicita almeno una parte dei "non so") e che solo lo 0,7% ha rilevato attacchi a questo genere di sistemi.
Una percentuale così bassa non deve trarre in inganno sui rischi potenziali del mondo IoT ed alle sue crescenti connessioni con i più "tradizionali" sistemi informatici dell'azienda/ente: il numero degli oggetti IoT è in fortissima crescita e proporzionalmente cresceranno minacce e vulnerabilità.
Studi già citati nelle precedenti edizioni evidenziavano fin dagli anni scorsi forti vulnerabilità, quali password troppo deboli ed il mantenimento delle password di default pre configurate nel dispositivo (es: password 0000).
Il progetto OWASP[17] sui 10 più usati dispositivi nel mondo IoT ha individuato una media di 25 vulnerabilità per oggetto, che includono privacy, autorizzazioni deboli, mancanza crittografia nelle comunicazioni, interfacce web insicure, software insicuro, insufficiente sicurezza fisica dei dispositivi. Il problema dell'autenticazione di un dispositivo IoT è diffuso e grave: sarebbe necessaria un'autenticazione con un certificato digitale, ma questo farebbe aumentare complessità e costi realizzativi.

Fig. 4-17 Attacchi digitali ai sistemi IoT per le aziende/enti rispondenti che li usano



17 https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

Ulteriori problemi per la sicurezza dei dispositivi IoT sono causati dalla non sistematica installazione delle patch e degli aggiornamenti, e più in generale dalla loro gestione, sovente carente.

4.6 LA SITUAZIONE A LIVELLO EUROPEO SECONDO ENISA

Per meglio inquadrare il fenomeno degli attacchi digitali in Italia nel contesto europeo, come nella precedente edizione si confrontano i dati emersi da OAD 2016 con quelli del più recente rapporto di ENISA Threat Landscape 2015[18]. ENISA, European Network and Information Security Agency, è l'agenzia europea per la sicurezza delle reti e dell'informazione (https://www.enisa.europa.eu/), con il compito di migliorare la sicurezza della Comunità europea, contribuendo allo sviluppo della cultura della sicurezza digitale a beneficio dei cittadini, dei consumatori, delle imprese e delle pubbliche amministrazioni. La fig. 4-18 elenca le principali minacce nel 2015 rilevate da ENISA,, confrontandole con quelle del 2014.
ENISA fa riferimento ad una tassonomia di minacce che logicamente differisce dalla tassonomia degli attacchi considerata da OAD e descritta nella Tabella 1.
La sottostante Tabella 5 cerca di confrontare la classifica ENISA con quella OAD per l'anno 2015. A fianco del nome della minaccia ENISA in parentesi graffa è indicato il nome (o più nomi) della tipologia di attacco OAD logicamente corrispondente. Si nota come in alcuni casi la tipologia ENISA è più dettagliata di quella OAI, in altri casi no. Per facilitare la comprensione della tassonomia
ENISA, è opportuno chiarire il significato di alcuni termini da loro usati:

- Web-based attacks: includono le tecniche per reindirizzare i browser a siti maligni. La corrispondenza con OAD fa riferimento prevalentemente allo sfruttamento di vulnerabilità, al malware ed al social engineering;
- Insider threat: è la minaccia costituita dal personale interno all'azienda/ente che utilizza come utente finale o come operatore i sistemi ICT. Questo personale può svolgere attacchi intenzionali o non con le più varie modalità e tecniche, e per questo motivo nella Tabella 4 si è posto un NS, Non Significativo.
- Analogamente per lo spionaggio cibernetico, Cyber espionage, che può essere effettuato con diverse tecniche di attacco, nella Tabella 4 si è posto un NS, Non Significativo.

La Tabella 5 evidenzia che non è totalmente fattibile e diretto il confronto tra le diverse tipologie usate da ENISA e da OAD, in primo luogo perché fanno riferimento a due temi diversi: la "minaccia" usata da ENISA e l'"attacco" usato da OAD. Dal confronto emerge comunque che il malware è in testa ad entrambe le classifiche.

18 https://www.enisa.europa.eu/publications/etl2015/at.../fullReport

Fig. 4-18 Confronto tra le 15 principali tassonomie di minacce a livello europeo rilevate nel 2014 e nel 2015 dall'annuale Rapporto ENISA (Fonte: ENISA)

Top Threats 2014	Assessed Trends 2014	Top Threats 2015	Assessed Trends 2015	Change in ranking
1. Malicious code: Worms/Trojans	↑	1. Malware	↑	→
2. Web-based attacks	↑	2. Web based attacks	↑	→
3. Web application /Injection attacks	↑	3. Web application attacks	↑	→
4. Botnets	↓	4. Botnets	↓	→
5. Denial of service	↑	5. Denial of service	↑	→
6. Spam	↓	6. Physical damage/theft/loss	⊃	↑
7. Phishing	↑	7. Insider threat (malicious, accidental)	↑	↑
8. Exploit kits	↓	8. Phishing	⊃	↓
9. Data breaches	↑	9. Spam	↓	↓
10. Physical damage/theft /loss	↑	10. Exploit kits	↑	↓
11. Insider threat	⊃	11. Data breaches	⊃	↓
12. Information leakage	↑	12. Identity theft	⊃	↑
13. Identity theft/fraud	↑	13. Information leakage	↑	↓
14. Cyber espionage	↑	14. Ransomware	↑	↑
15. Ransomware/ Rogueware/Scareware	↓	15. Cyber espionage	↑	↓

Legend: Trends: ↓ Declining, ⊃ Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Tabella 5 Confronto tra le classifiche riguardanti l'anno 2015 tra i principali rischi individuati da ENISA e gli attacchi di OAD.

Tassonomia Minacce (Top Threats) ENISA vs Attacchi OAD	Classifica 2016 ENISA	Classifica 2016 OAD
Malicious code: Worms/Trojans {malware}	1	1
Web-based attacks {sfruttamento vulnerabilità}/{malware}/{social engineering}	2	7/1/2
Web application attacks /Injection attacks {sfruttamento vulnerabilità}	3	7
Botnets {malware}	4	1
Denial Of Service {saturazione risorse}	5	4
Spam {saturazione risorse}	9	4
Phishing {social engineering}	8	2
Exploit kits {sfruttamento vulnerabilità}	10	6
Data Breaches {sfruttamento vulnerabilità}	11	6
Physical damage/theft /loss {attacchi sicurezza fisica}/{furto dispositivi}	6	3
Insider threat	7	NS
Information Leakage {Furto di informazioni da mobile e non }	13	11/14
Identity theft/fraud {Furto di informazioni da mobile e non }/accesso non autorizzato host-programmi-dati	12	11/14/8/10/12
Cyber espionage	14	NS
Ransomware {malware}	15	1

5 L'individuazione e la gestione degli attacchi

La fig. 5-1 mostra, la provenienza delle segnalazioni di un attacco (risposte multiple): per il campione dei rispondenti la metà delle segnalazioni arrivano dagli utenti interni del sistema informatico, e con una percentuale di poco inferiore dai sistemi di monitoraggio e controllo e dalla rilevazione diretta dell'impatto, ad esempio il non funzionamento di un sistema o di una applicazione. A decrescere, per circa un terzo dei rispondenti, la segnalazione da parte degli operartori ICT e poi altre opzioni.
Sulla gestione dell'attacco, una volta individuato, due le principali domande poste dal questionario:

- è stato comunicato alle autorità competenti, e se no perché?
- subito l'attacco, in quanto tempo sono state ripristinate le condizioni precedenti?

Nella fig. 5-2 (risposte multiple), quasi il 60% dei rispondenti non lo comunica per le motivazioni dettagliate nella fig. 5-3.
Relativamente basse le percentuali di quelli che lo comunicano: il 15% avvisa le competenti autorità di sicurezza, solitamente la Polizia Postale e delle Comunicazioni, pochi segnalano l'attacco a centri specializzati tipo Cert e nessuno del campione avvisa una Assicurazione, indice che pochi del campione hanno stipulato assicurazioni sul rischio residuo di un attacco, forse anche a causa della complessità e del costo di tali polizze: ed in tempi di crisi. Per un maggior dettaglio si rimanda alla fig. 6-9.

Fig. 5-1 Chi ha segnalato l'attacco (risposte multiple)

Quasi il 12% dichiara di "non sapere": probabilmente nelle loro aziende/enti questa attività è svolta dagli uffici legali o delle pubbliche relazioni o da consulenti esterni, ed il personale più tecnico che opera sulla sicurezza informatica non è informato. La principale motivazione per la non comunicazione, come da fig. 5-3 con risposte multiple, è che l'attacco subito non è risultato "significativo" per chi l'ha subito ed è quindi inutile intraprendere una formale denuncia o interagire coi fornitori o con altri enti: la struttura interna è in grado da sola di gestire l'attacco e le sue conseguenze. Con % molto inferiori, pur avendo risposte multiple, le altre motivazioni, tra le quali si evidenzia la non conoscenza di chi informare e la necessità di seguire le policy. La tutela dell'immagine, come motivazione, ha solo un 3,4%. Un numero non trascurabile di rispondenti ha anche selezionato "Altro", specificando prevalentemente che è inutile/non vale la pena di denunciare l'occorrenza di un attacco. Queste ultime motivazioni sono, a parere dell'autore, da non trascurare: sono un chiaro indice della sfiducia nelle istituzioni e nella giustizia italiane. A seguito di un attacco, oltre alle eventuali segnalazioni di cui alla precedente fig. 5-2, sono intraprese varie azioni, sia tecniche sia organizzative e legali, sintetizzate nella fig. 5-4. La misura intrapresa dal 44,5% dei rispondenti sono gli aggiornamenti per la correzione dei software.
I dati emersi dal campione di rispondenti attuali sono simili, anche se con percentuali diverse, da quelle della passata edizione. Due gli interventi effettuati da più della metà dei rispondenti: l'attivazione di indagini interne (cerchiamo di capire che cosa è successo) e le correzioni del software (patch e/o aggiornamento della versione). Di poco inferiori percentualmente, ma sempre alti, altri due interventi, uno tecnico ed uno organizzativo: l'acquisizione di ulteriori nuovi strumenti di prevenzione e protezione, e l'aggiornamento-miglioramento delle policy in atto.

Fig. 5-2 A chi è stato comunicato l'avvenuto attacco al di fuori dell'azienda/ente (risposte multiple)

Fig. 5-3 Le motivazioni per la non comunicazione all'esterno (risposte multiple)

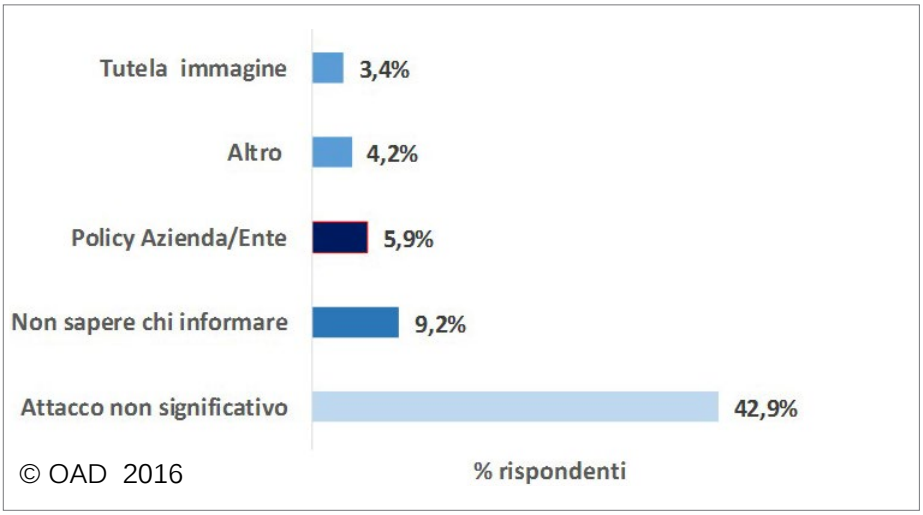
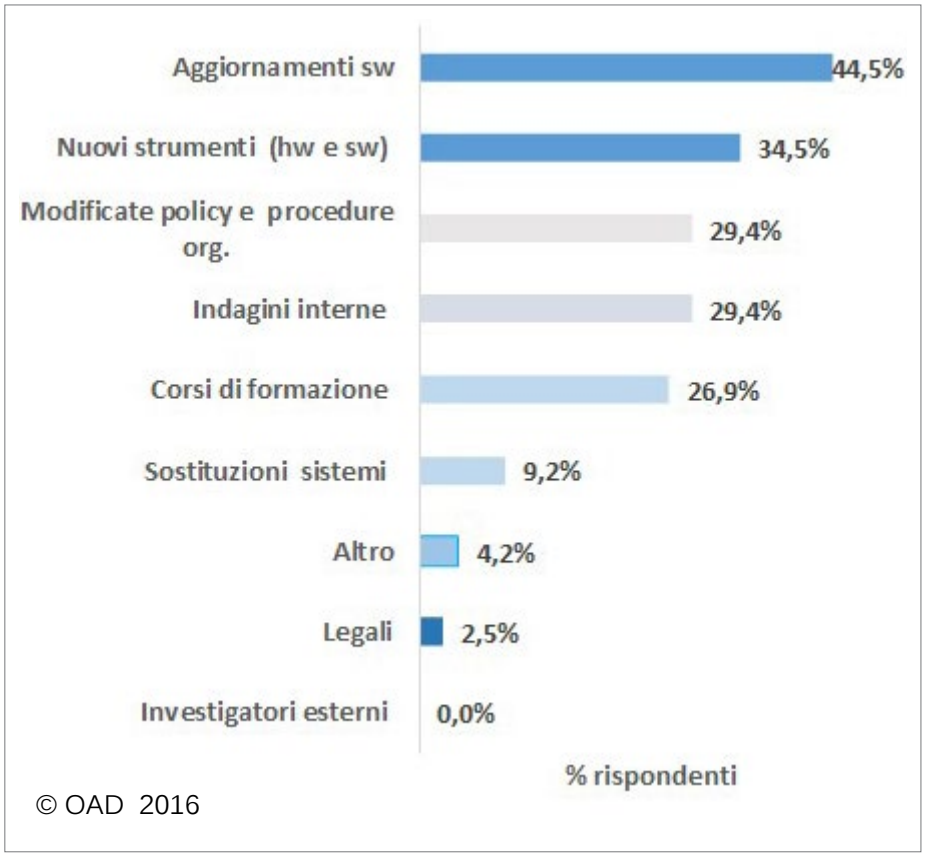


Fig. 5-4 Azioni intraprese dopo un attacco (risposte multiple)



A decrescere poi gli altri interventi, tra cui, con percentuali non trascurabili, il miglioramento della sensibilizzazione ed addestramento del personale tramite corsi e seminari. Queste alte percentuali di adozione da parte dei rispondenti indicano una crescente consapevolezza dell'importanza della sicurezza informatica non solo declinata tecnicamente ma anche organizzativamente. All'ultimo posto il coinvolgimento dei legali (5,38 %), probabile indicazione della scarsa efficacia di tale azione in Italia, tenendo anche conto della ben nota ed inaccettabile durata dei processi sia civili sia penali. Per quanto riguarda i tempi di ripristino a seguito di un attacco, la fig. 5-5 mostra il tempo massimo occorso per il ripristino dei sistemi ICT a seguito di un grave (o il più critico/grave) attacco subito nel 2015. Nella maggior parte dei casi, quasi il 44%, la situazione "ante" è ripresa in meno di un giorno, e complessivamente, in quasi l'80% dei casi, la situazione è ripristinata entro 3 giorni dall'attacco.

Questi tempi indicano da un lato che gli strumenti di prevenzione, protezione e ripristino sono ora più diffusi e più efficaci, dall'altro che la stragrande maggioranza degli attacchi, almeno per il campione della presente indagine, non ha serie conseguenze, come d'altro canto evidenziato nel precedente § 4.1.

La fig. 5-6 mostra quali sono le tipologie di attacchi che hanno richiesto tempi di ripristino superiori alla settimana: sul podio, come primo classificato con un relativo forte distacco rispetto agli altri due, i codici maligni. Essi quindi possono avere impatti significativi, ed a questo hanno sicuramente contribuito i ransomware. Al secondo posto i furti di dispositivi: tra denunce ed eventuale riacquisto e riconfigurazione del dispositivo può passare facilmente più di una settimana.

Al terzo posto la saturazione di risorse, i Dos/Ddos: l'identificazione dell'attacco ed il conseguente intervento del (o dei) fornitore(i) di TLC con tutte le riconfigurazioni necessarie possono richiedere ben più di una settimana.

E' bene sottolineare come i tre attacchi che possono richiedere più di una settimana rientrano tra le quattro tipologie di attacchi che da sempre sono i più diffusi tra i rispondenti di tutte le indagini OAI-OAD.

Fig. 5-5 Tempo massimo occorso per il ripristino dei sistemi ICT

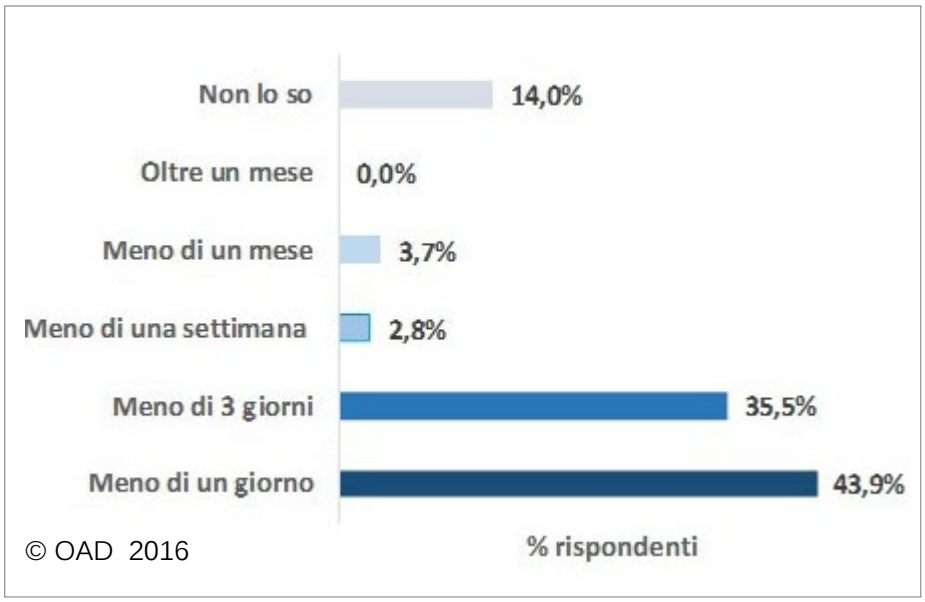
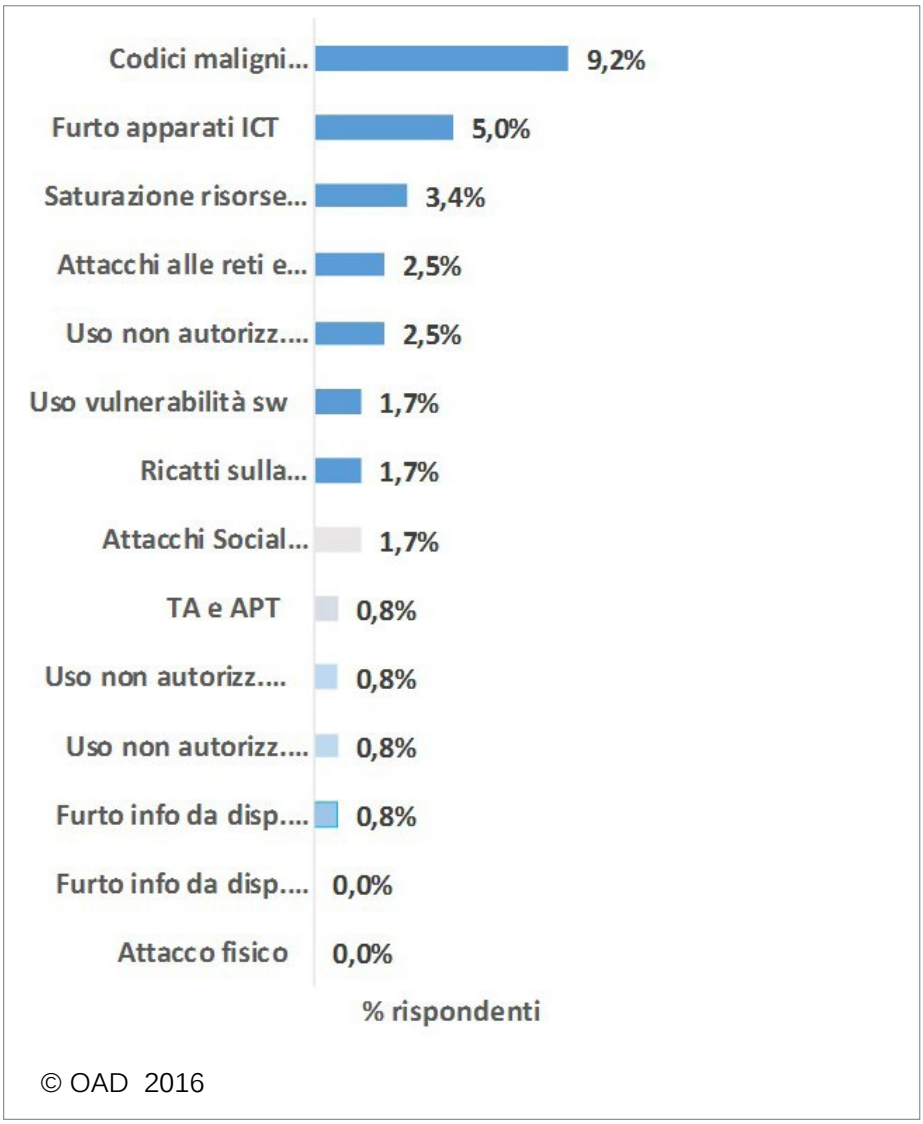


Fig. 5-6 Attacchi che hanno richiesto tempi di ripristino superiori alla settimana (risposte multiple)



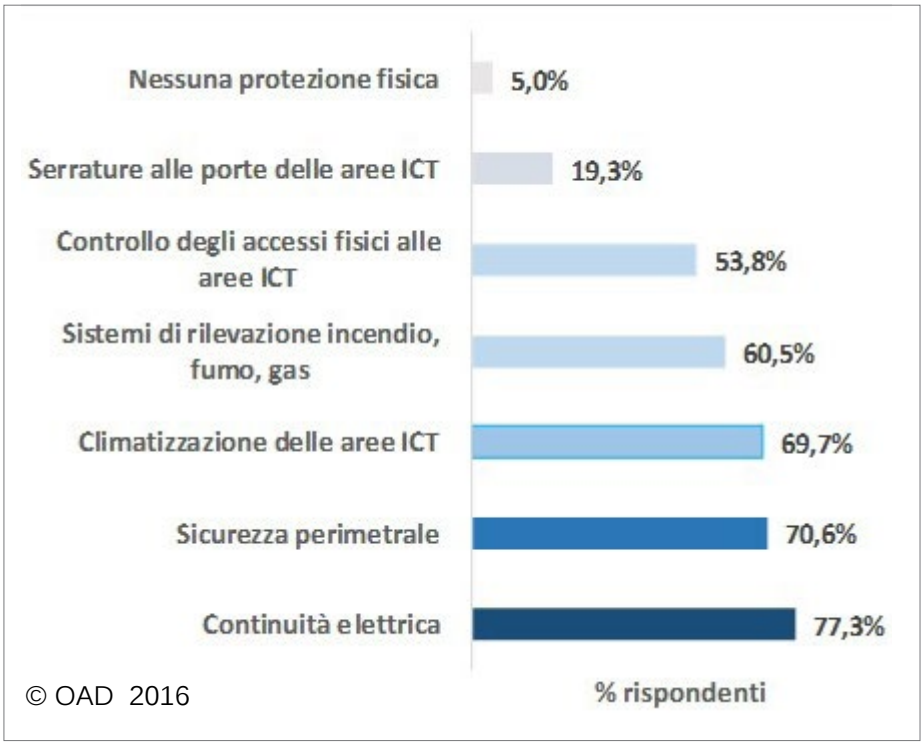
6 Strumenti e misure di sicurezza ICT adottate

Facendo riferimento alle macro caratteristiche dei sistemi informatici e delle aziende/enti dei rispondenti illustrate nell'Allegato B, nel seguito vengono analizzati gli strumenti di sicurezza in uso, a livello sia tecnico sia organizzativo, per poter meglio comprendere come gli attacchi analizzati al §4.

6.1 SICUREZZA FISICA

La fig. 6-1 schematizza le principali misure in uso per la protezione "fisica" dei Data Center, delle "computer room"[19] o di qualsiasi luogo ove sono installate risorse ICT. Gli strumenti più usati, più dei 2/3 dei rispondenti, sono i sistemi per garantire la continuità elettrica, da UPS ad autonomi gruppi di continuità, e quelli di climatizzazione nei locali ove sono concentrate le risorse ICT. Più della metà dispone nei locali del Data Center e/o delle computer room di rilevatori di fumo, gas, umidità, oltre a di sistemi di climatizzazione, A

Fig. 6-1 Strumenti di sicurezza fisica in uso (risposte multiple)



19 Con questo termine si indicano i locali nei quali vengono concentrate le risorse informatiche di un ufficio periferico o di una piccola azienda/ente.

questi si aggiungono protezioni perimetrali passive e attive quali recinzioni antiscavalcamento, inferiate alle finestre e alle porte, sistemi di allarme antintrusione a radar o a micro onde, videosorveglianza.Vengono inoltre effettuati controlli degli accessi delle persone fisiche tramite reception, bussole, lettori di badge, ed altri strumenti, fino al riconoscimento biometrico. Quasi un quinto (1/5) dei rispondenti ha aree dedicate ai sistemi ICT protette solo da porte chiuse a chiave, il il 5% non ha di fatto alcuna misura di sicurezza fisica per i locali ove sono contenuti i sistemi ICT. Questi ultimi due casi sono i tipici casi delle piccole e piccolissime aziende, degli studi professionali, dei piccoli laboratori artigianali. Tale dato è corretto se confrontato con le dimensioni delle organizzazioni per numero di dipendenti (si veda fig. B-4 nell'Allegato B.1)

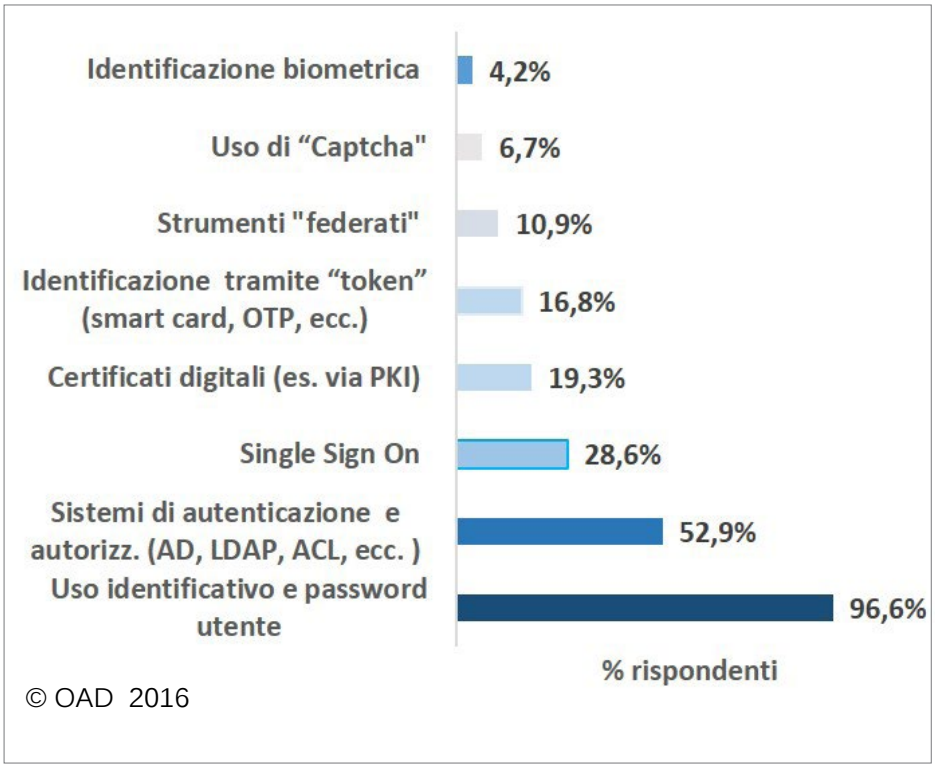
6.2 SICUREZZA LOGICA

Gli strumenti per la sicurezza logica si differenziano in funzione delle unità ICT da proteggere, e si articolano in:

- identificazione, autenticazione, autorizzazione degli utenti;
- protezione delle reti;
- protezione dei sistemi;
- protezione degli applicativi.

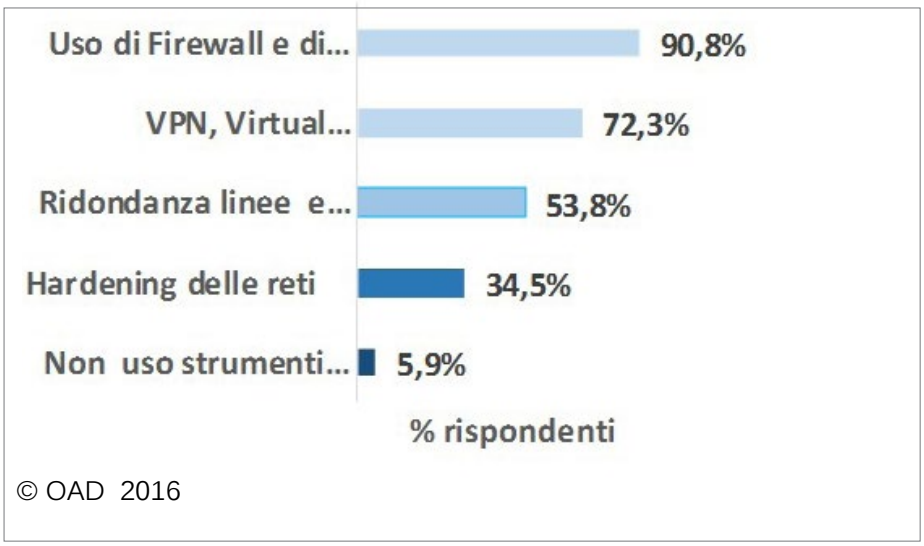
La fig. 6-2 mostra la situazione del campione, con risposte multiple, per gli strumenti di identificazione, autenticazione e controllo degli accessi logici ai sistemi, reti incluse, e alle applicazioni. La classifica degli strumenti più diffusi è uguale a quella della scorsa edizione, con percentuali abbastanza simili, a parte l'identificazione biometrica.
Il mezzo più diffuso, usato dalla quasi totalità dei rispondenti (96,6%) è la consueta coppia identificatore utente – password.
Con una percentuale ben minore, quasi il 53%, sono diffusi gli strumenti di controllo degli accessi dell'utente, che vanno dall' Active Directory di Microsoft all'LDAP, dalle ACL, Access Control List ai Policy Server, e così via.
Al terzo posto le tecniche di SSO, Single Sign One, con una copertura di poco meno del 30%, assai simile a quelle dell'edizione precedente.
Al quarto posto, per circa 1/5 dei rispondenti, l'uso dell'autenticazione forte con certificati digitali, spinta dalla PEC, Posta Elettronica Certificata, e dagli obblighi normativi nelle Pubbliche Amministrazioni per l'uso di piattaforme KPI, Public Key Infrastructure, necessarie per erogare servizi basati sui certificati digitali.
Altri meccanismi di identificazione ed autenticazione, dall'uso di "token" quali chiavi USB, smart card, dispositivi OTP (One Time Password, di crescente diffusione nell'ambito bancario) hanno una diffusione minore nel campione emerso, attorno al 17%.

Fig. 6-2 Misure tecniche di Identificazione, Autenticazione, Autorizzazione (risposte multiple)



Rispetto alle precedenti edizioni, pur con un bacino di rispondenti in parte diverso, si posiziona con un non trascurabile 10,9% l'uso di autenticazioni federate, usate prevalentemente da grandi organizzazioni e dalle strutture italiane di multinazionali.
L'uso di Captcha sulle pagine web per assicurarsi che l'utente sia una persona e non un programma, ha percentuali ancora più basse.
L'identificazione biometrica è ultima nella classifica, come nelle precedenti edizioni, nonostante la crescente diffusione di grafometria negli ambienti bancari, ambienti che hanno però risposto in maniera molto limitata al questionario OAD.
Per la protezione delle proprie reti interne e degli accessi ad Internet e alle reti "pubbliche" , come indicato nella fig. 6-3 con risposte multiple, la quasi totalità dei rispondenti è dotato di dispositivi firewall e di DMZ, DeMilitarized Zone, e più del 72% utilizza soluzioni VPN, Virtual Private Network per proteggere le comunicazioni da remoto.
Più della metà del campione è dotata di soluzioni ridondate sia a livello di collegamenti-reti, sia a livello di sistemi critici: architetture ad alta affidabilità con "mirroring", "clustering", e così via. Più di un terzo ha potenziato il livello di sicurezza delle reti ed una piccola percentuale, il 5,9% non è al

Fig. 6-3 Misure tecniche di protezione delle reti (risposte multiple)



momento dotata di alcuna specifica protezione per le reti: è il caso probabilmente per piccoli e piccolissimi sistemi informatici. La fig. 6-4 fornisce un sintetico quadro, con risposte multiple, della diffusione dei principali strumenti per la protezione logica dei sistemi, in particolare dei server, quadro che è a grandi linee simile a quello delle edizioni passate, soprattutto per i primi tre strumenti più usati.

Al primo posto gli anti-malware, come è ovvio dato che questi sono gli attacchi più diffusi (fig. 4-6 e 4-7): sono usati dalla stragrande maggioranza dei rispondenti (93,3%). Al secondo posto la gestione delle patch e degli aggiornamenti (nella precedente edizione era al quinto posto, ma con una percentuale dello stesso ordine di grandezza). Come per l'anno scorso il dato emerso è preoccupante: quasi la metà dei rispondenti non aggiorna sistematicamente il software di base ed applicativo dei propri sistemi, mantenendo così gravi vulnerabilità sui propri sistemi ICT. Il fenomeno, già emerso nei precedenti rapporti, può avere diverse cause. Tra quelle più probabili, soprattutto nelle piccole organizzazioni, il non rinnovo dei contratti di manutenzione ed aggiornamento del software acquisito, dovuto anche al perdurare della crisi economica e dal conseguente taglio di ogni spesa ritenuta non indispensabile. Ma l'aggiornamento del software è indispensabile, soprattutto per la sicurezza informatica! Poco più della metà dei rispondenti dichiara di disporre di architetture e sistemi ad alta affidabilità, anche grazie a soluzioni cloud ibride. Con una percentuale di poco inferiore, gli strumenti di filtraggio dei contenuti e delle URL, grazie sia alla diffusione dei moderni firewall sia al fatto che il mondo dei web è ormai al centro dei sistemi informatici e quindi della loro sicurezza.

Fig. 6-4 Misure tecniche di protezione dei sistemi ICT (risposte multiple)

E gli strumenti (tipicamente software) di sicurezza End-Point ed i NAC, Network Access Control, usati per controllare "prima dell'accesso" l'identità dell'utente e quanto sia sicuro il dispositivo d'utente da cui chiede l'accesso. Nella voce "Altro" alcuni rispondenti hanno indicato di usare ambienti Linux, al posto di Windows, in quanto ritenuti più sicuri. Sull'uso dei sistemi operativi da parte dei rispondenti, si rimanda all'Allegato B.2.

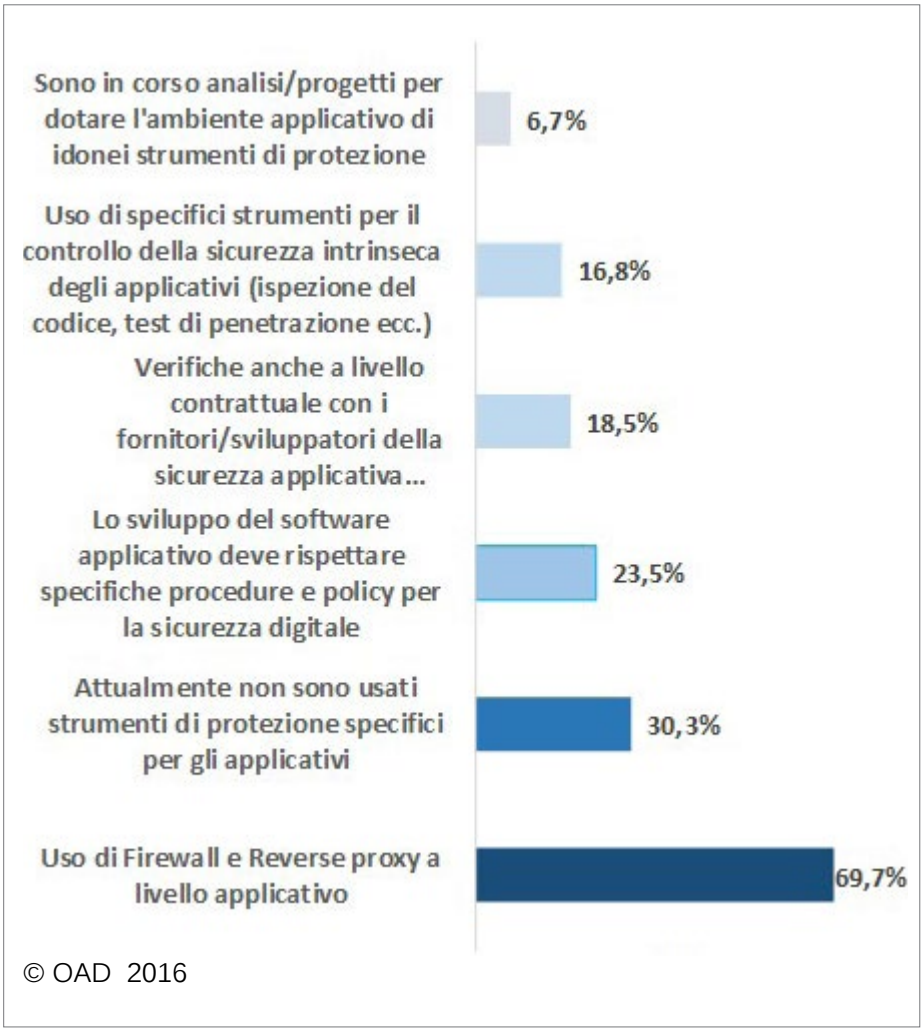
La fig. 6-5 (risposte multiple) sintetizza l'uso di strumenti per la protezione degli applicativi, al di là degli strumenti di controllo degli accessi considerati nella precedente fig. 6-2. Gli strumenti più diffusi, 69,7%, sono i firewall ed i reverse proxy posti a difesa dei server applicativi, dei data base server, e dei sistemi di storage.

Un 30% del campione emerso non usa specifici strumenti di sicurezza per gli applicativi. Un 23,5% sviluppa e/o fa sviluppare software secondo specifiche linee guida per lo sviluppo di codice sicuro. Il controllo che il software sia sicuro, anche con clausole contrattuali in caso di forniture da terze parti, scende ad un 18,5%.

Questo significa che linee guida emesse, magari ben dettagliate, non sempre sono poi verificate ed in questi casi sono un puro invito e/o una precauzione "burocratica", cui non segue alcun effettivo controllo. E l'effettivo controllo con idonei strumenti, quali l'ispezione del codice e i test di penetrazione, scende al 16,8% . Il 6,7% dichiara che sono in corso progetti o analisi di fattibilità per dotarsi di strumenti per la sicurezza applicativa.

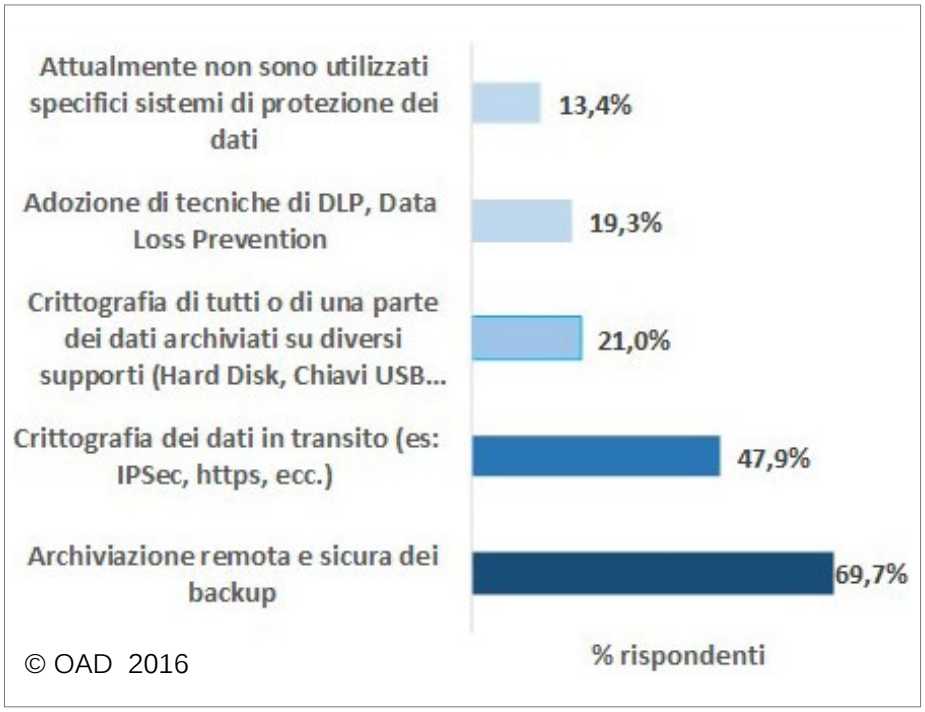
Il problema della sicurezza applicativa è crescente, come indicato anche nella fig. 7-1 sulle principali minacce, dato che la maggior parte degli attacchi più gravi ed impattanti si basa proprio su attacchi agli applicativi, che sono ormai prevalentemente in web.

Fig. 6-5 Strumenti tecnici di sicurezza digitale per gli applicativi (risposte multiple)



Scarsità di specifiche misure di prevenzione e protezione, come indicato dalla fig. 6-5, aggrava la situazione. Per la protezione dei dati, che costituiscono il reale e più importante "asset ICT" dell'azienda/ente, la fig. 6-6 mostra che una buona maggioranza, il 69,7%, utilizza l'archiviazione remota, tipicamente con ISP/ASP (Internet/Application Service Provider) e Fornitori cloud; la tendenza è di replicare in remoto tutti i dati, o quelli più critici, in storage su cloud via IaaS, Infrastructure as a Service. Il secondo strumento più diffuso, usato da circa il 48% del campione, è l'uso della crittografia nella trasmissione dei dati in rete, tipicamente nelle transazioni via web con HTTPS o con FTPS. La crittografia dei dati archiviati, o almeno di quelli più critici, si riduce al 21% dei rispondenti, ed emerge una percentuale di poco inferiore per l'uso di strumenti DLP, Data Loss Prevention. Una percentuale

Fig. 6-6 Misure per la protezione dei dati (risposte multiple)



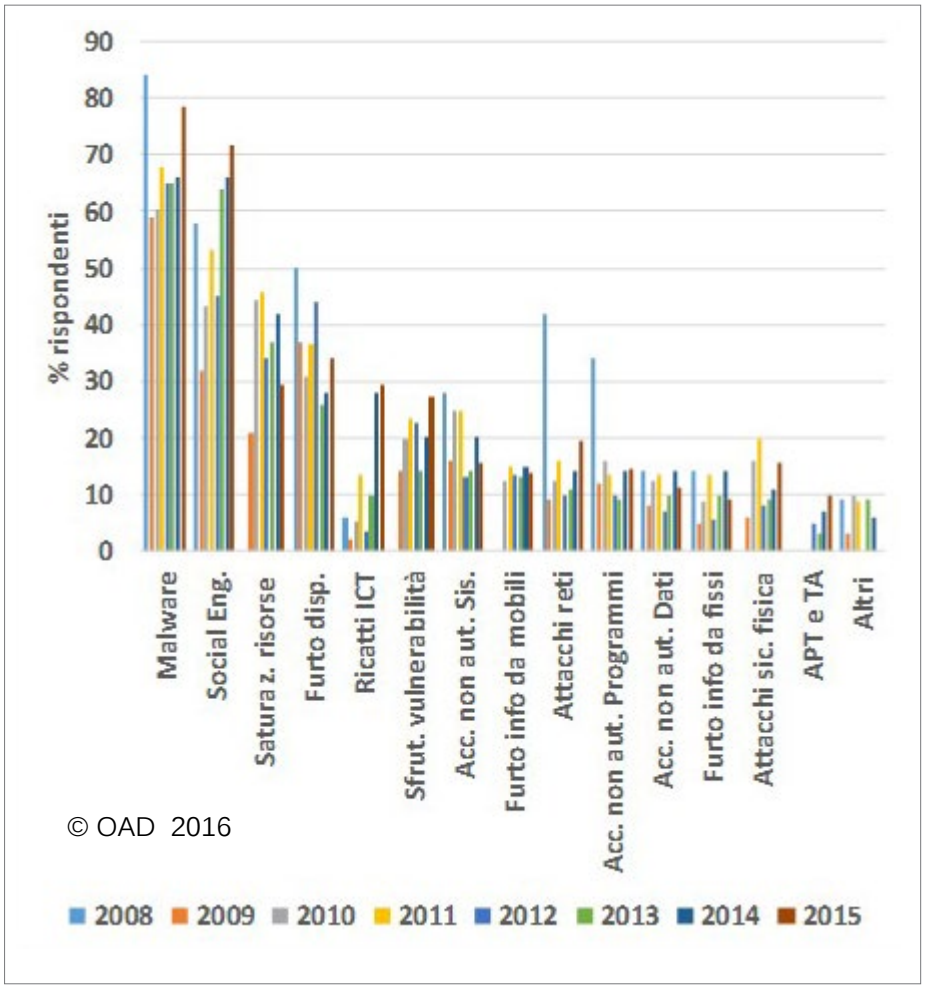
non trascurabile di quasi il 13,4% non usa alcuna specifica tecnica per la protezione dei dati. I dati emersi, simili a quelli delle precedenti edizioni, evidenziano come deve essere fatta ancora molta strada (e molta sensibilizzazione) per la protezione dei dati.
Interessante notare come le percentuali emerse per il 2015 sono molto simili a quelle del 2014, pur con un bacino di rispondenti diverso.

6. 3 GLI STRUMENTI PER LA GESTIONE DELLA SICUREZZA DIGITALE

La fig. 6-7 mostra iprincipali strumenti di gestione della sicurezza ICT utilizzati dall'intero campione e con risposte multiple: la gestione della sicurezza digitale é l'elemento determinante per potere garantire un livello realmente idoneo e proattivo di protezione al sistema informatico. I dati emersi sono simili a quelli delle precedenti edizioni.
Il monitoraggio ed il controllo centralizzato delle funzionalità e delle prestazioni dei sistemi ICT sono in vari modi attuati dal 63% dei rispondenti. Al secondo posto, come diffusione, la gestionedei log degli amministratori ed operatori di sistema, con il 43,7%: pur avendo un peso non trascurabile, ben più della metà dei rispondenti non la effettua, così come invece richiesto Garante della privacy. Il 40,3% opera il controllo e monitoraggio anche o solo a livello del singolo sistema, tipicamente quando si accorge di o gli viene segnalato un malfunzionamento. Anche avendo sistemi di controllo

centralizzati è necessario talvolta effettuare controlli ed interventi locali, ma il più delle volte, soprattutto nei sistemi informativi di piccole e medie dimensioni, la gestione è effettuata solo server per server tramite la consolle del sistema operativo. Un ruolo importante è svolto dai sistemi IPS/IDS, Intrusion Prevention System/ Intrusion Detection System, usati dal 39.5 % dei rispondenti, così come, con la stessa percentuale, i piani di Disaster Recovery, ora facilitati dall'utilizzo del cloud, ma solo il 21,8% effettua periodicamente prove di ripristino emulando situazioni di disastro. Questi dati sono simili, come ordine di grandezza, a quelli rilevati nelle edizioni precedenti, ed evidenziano come in alcuni casi la prevenzione sia più formale e burocratica che effettiva. Il 34,5% effettua il log degli utenti, ed il 21,8% effettua sistematiche analisi delle vulnerabilità (vulnerability assessment) con scansioni delle reti e dei sistemi, ed il 21% effettua prove di attacco (penetration test) per saggiare la tenuta degli strumenti di sicurezza.

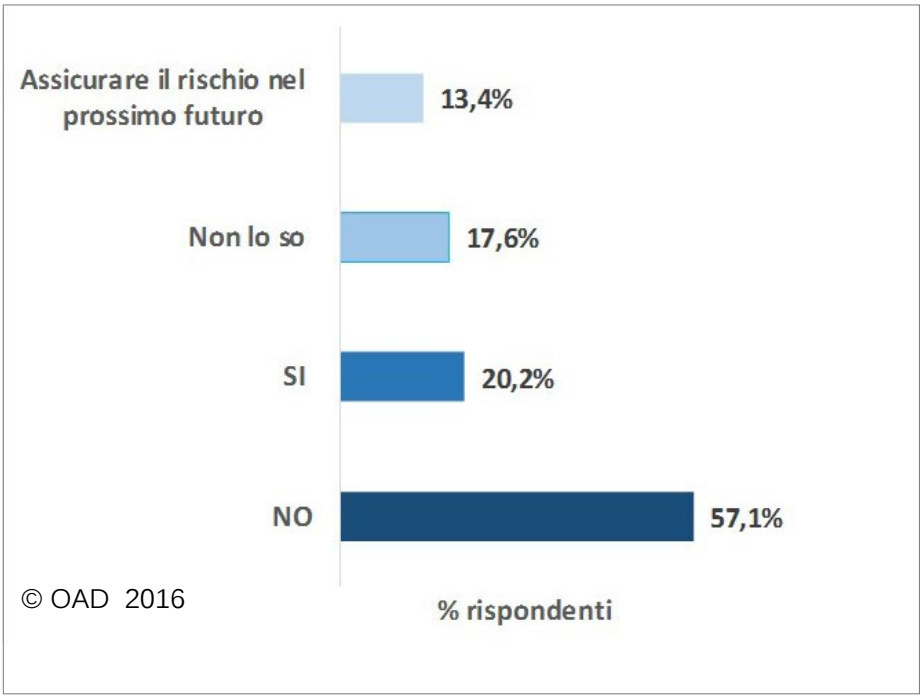
Fig. 6-7 Misure per la gestione della sicurezza digitale (risposte multiple)



Non trascurabile il 15,1% di rispondenti che utilizza sistemi di analisi comportamentale dei sistemi ICT e/o dei loro utenti, uno dei moderni mezzi per individuare comportamenti anomali di persone e/ o di sistemi, e cercare così di prevenire deterioramenti funzionali ed attacchi.
Un aspetto fondamentale nella gestione della sicurezza ICT è la sistematica e periodica analisi e gestione dei rischi. Come evidenziato nella fig. 6-8, poco meno di ¼ dei rispondenti effettuata tale analisi , ed il 14,3% intende effettuarla nel prossimo futuro.
Non trascurabile il 12,6% che afferma di non conoscere se la propria azienda/ente effettui o meno l'analisi dei rischi. Questo dato, oltre a confermare la serietà e la correttezza delle risposte dei rispondenti, indica che l'analisi (e la gestione) dei rischi ICT è effettuata in alcune aziende/enti al di fuori della struttura organizzativa dell'ICT e che il personale di quest'ultima, che in maggioranza ha risposto al questionario OAD, non conosce che cosa fa la sua organizzazione sul tema.
La fig. 6-9 mostra che circa 1/5 dei rispondenti ha già in essere forme assicurative sul rischio informatico, dopo aver implementato quanto opportuno per limitarlo, e che il 13,4% prevede di dotarsene nel prossimo futuro. Anche su questo tema un'importante percentuale di "non sono", 17,6%, comprensibile per le motivazioni già esposte per la precedente figura.

Fig. 6-8 Analisi dei rischi ICT

Fig.6-9 Assicurazione del rischio residuo ICT



6.4 LE MISURE ORGANIZZATIVE

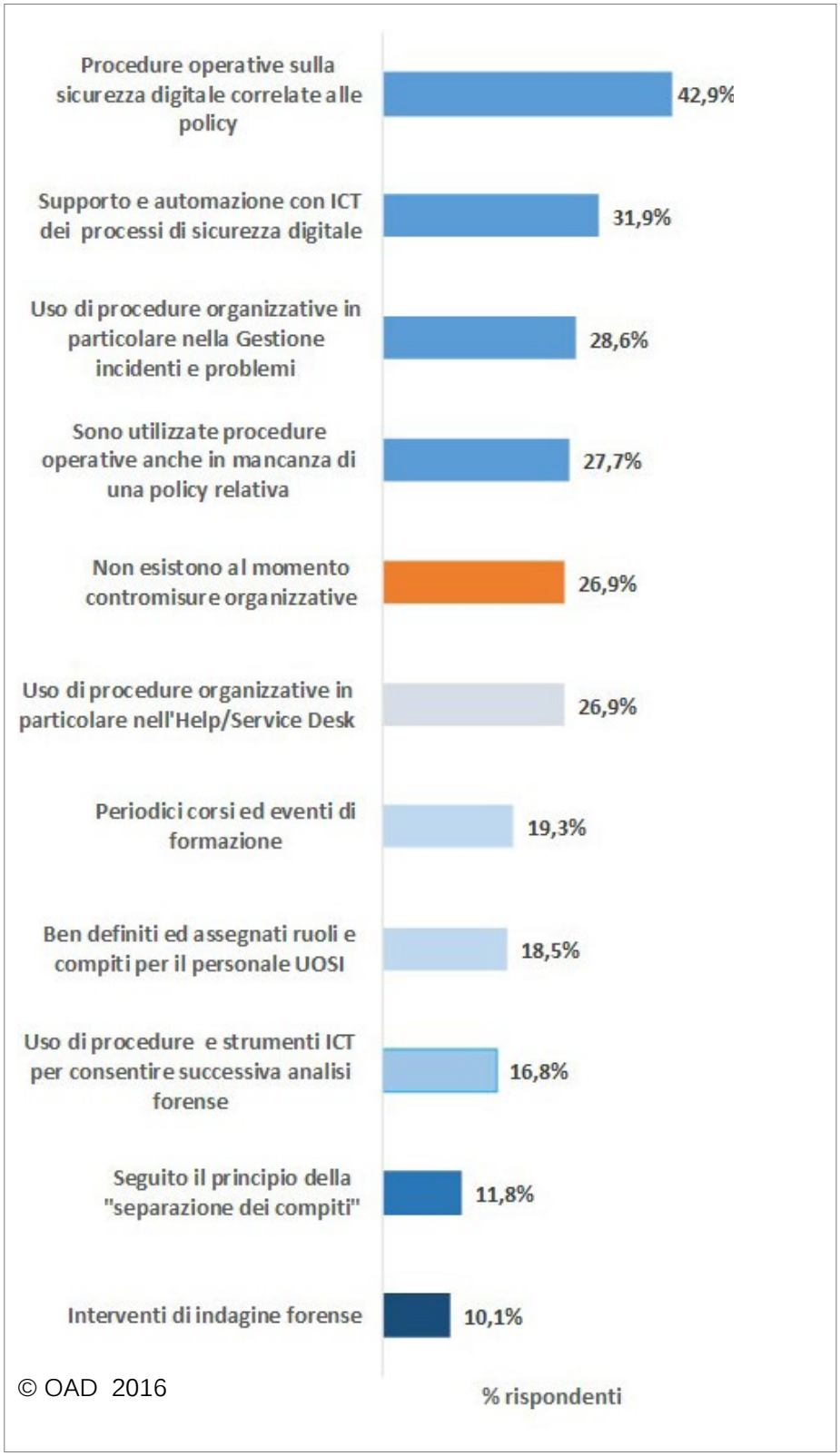
Gli aspetti organizzativi sono determinanti per l'attuazione e la gestione di una effettiva ed efficace sicurezza informatica: aspetti talvolta trascurati, anche perché considerati come troppo burocratici o di interesse solo per le grandi e grandissime organizzazioni. Quanto emerge dalla risposte conferma 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: 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.

La fig. 6-10, con risposte multiple, sintetizza la distribuzione delle principali misure organizzative in uso nel campione dei rispondenti..

Quasi il 43% utilizza procedure organizzative in merito alla sicurezza digitale, definite nell'ottica delle policy emanate. Circa il 42% utilizza strumenti informatici per il supporto e l'automazione, parziale o totale, dei processi per la sicurezza digitale, quali sistemi di work-flow, di correlazione tra gli allarmi, di trouble ticketing, di banche dati e sistemi "smart" a supporto dell'help-desk, ecc. Il 28,6% usa procedure per la gestione di incidenti e problemi, ed il 26,9 per la gestione dell'help desk.

Il dato più preoccupante è che quasi il 27% dichiara di non avere alcuna misura organizzativa per la sicurezza digitale.

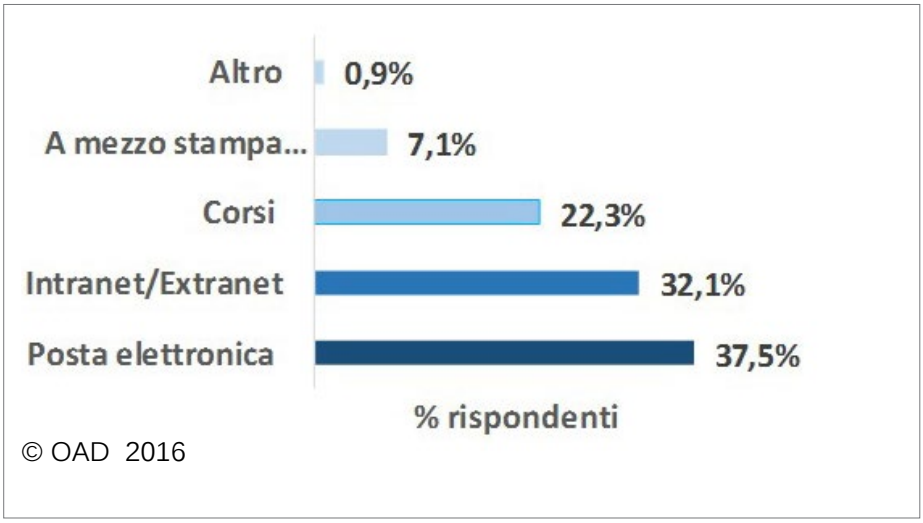
Fig. 6-10 Le principali contromisure organizzative (risposte multiple)



Ma tutti i dati della fig. 6-10 indicano che le misure organizzative nel loro complesso sono, almeno nel campione emerso, ancora troppo poco diffuse e quindi usate, pur essendo l'elemento determinante per l'effettiva attuazione e gestione della sicurezza digitale.
Ed è ancor più preoccupante considerare, come già evidenziato in vari paragrafi del presente Rapporto, che il campione di rispondenti rappresenta una fascia medio alta per il livello di sicurezza digitale nell'ambito delle aziende/enti italiani.
Data l'importanza di una policy per la sicurezza ICT, che logicamente dovrebbe essere un di cui della più generale policy ICT, nel Questionario si sono poste due esplicite domande, la prima sull'esistenza di una policy per la sicurezza, la seconda sulla modalità per la sua comunicazione e diffusione. Le risposte sull'esistenza di una policy sono schematizzate nella fig. 6-11 dove poco più di 1/5 dei rispondenti dichiara di aver definito e comunicato formalmente al proprio interno la policy sulla sicurezza digitale, ma il 57,4% dichiara di non avere una policy per la sicurezza ICT, ed il 21% circa di averla in corso di definizione. Per le aziende/enti che hanno già adottato e in essere "policy" per la sicurezza informatica, la fig. 6-12 mostra, con risposte multiple, quali sono i principali mezzi per la sua comunicazione e diffusione: la prevalenza è via posta elettronica seguita a breve distanza dalla Intranet, cui seguono a decrescere percentualmente l'uso di seminari e corsi, la comunicazione tramite specifiche riunioni e, da ultimo, la comunicazione interna a mezzo stampati. Nella voce "Altro" è stata indicata la comunicazione interna verbale.

Fig. 6-11 Definizione ed uso di una "policy" sulla sicurezza digitale

Fig. 6-12 Comunicazione della policy sulla sicurezza digitale (risposte multiple)



6.4.1 Conformità a standard e a "buone pratiche"

Un concreto ausilio nell'organizzazione della sicurezza digitale 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[20] per la gestione operativa dell'ICT, l'ISO 9001 per la gestione della qualità dei servizi, ecc.[21]

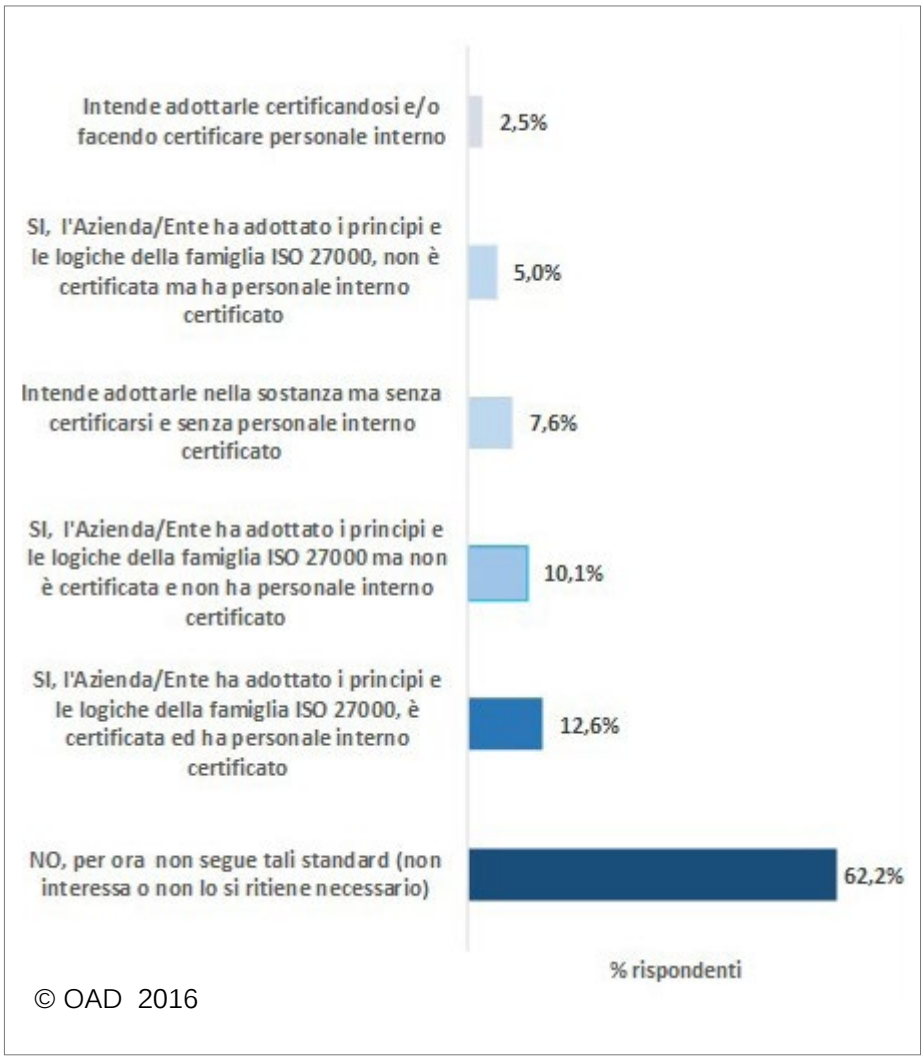
Tali standard e best practice possono essere adottati formalmente, ossia certificandosi, o informalmente all'interno delle proprie strutture, e la loro adozione è in maniera crescente richiesta ai fornitori, sia a livello aziendale sia a livello delle singole persone, perché li seguano nell'erogare i servizi richiesti.

La fig. 6-13 mostra le risposte sull'adozione della famiglia di standard ISO 27000 nell'ambito dell'azienda/ente, normalmente da parte della struttura sistemi informatici. Volutamente, per non appesantire il questionario, non sono state dettagliate domande sui numerosi standard in cui si articola questa famiglia: quelli più seguiti sono tipicamente l'ISO 27001, che definisce i requisiti per un sistema SGSI, e l'ISO 27002, che specifica i controlli operativi sulla sicurezza che dovrebbero essere svolti. La certificazione ad uno di questi standard è normalmente a livello dell'azienda/ente, ma può essere anche a livello della singola persona.

20 ISO 20000 standardizza logiche e processi di ITIL

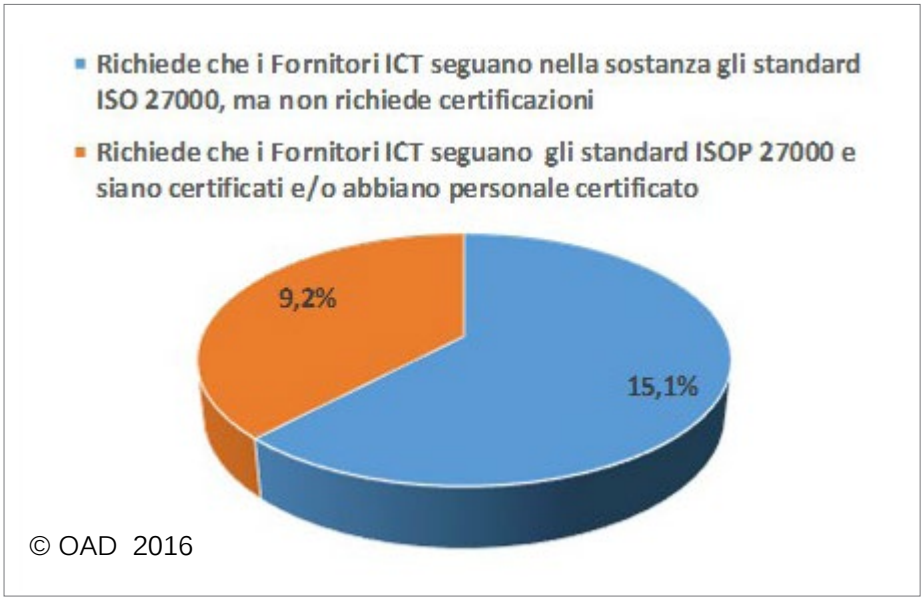
21 Per approfondimenti e confronti tra questi standard e best practice si rimanda al già citato libro di M.R.A. Bozzetti e F. Zambon "Sicurezza Digitale" edito da Soiel International e pubblicato a giugno 2013, ISBN 978 88 908901 0 9.

Fig. 6-13 Adozione standard della famiglia ISO 27000 all'interno dell'azienda/ente



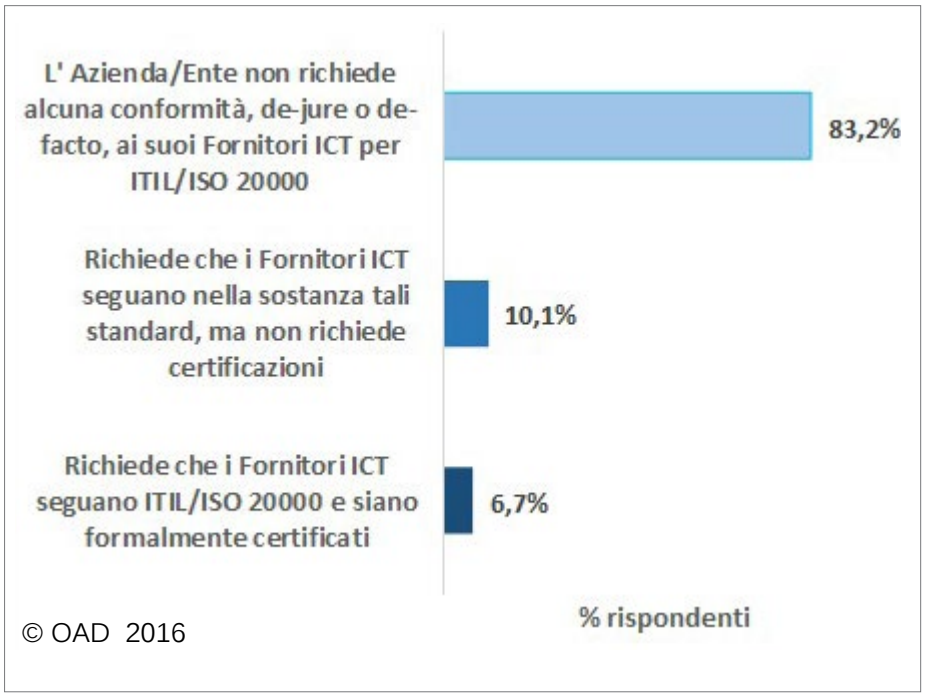
La figura mostra che ben più della metà dei rispondenti, il 62,6%, non è interessata o non ritiene necessario seguire tali standard nel proprio contesto, ed il 12,6% è invece già certificato a livello aziendale: una percentuale molto simile a quella della scorsa edizione, pur tenendo conto che i bacini di rispondenti sono diversi. Il 10,1% già li segue de-facto questi standard pur senza essere certificata, e il 7,6% intende seguirli nel prossimo futuro sempre senza certificazioni. Il 5% del campione non ha certificazioni di questo tipo ma segue de facto tali standard ed ha personale interno certificato. Nel prossimo futuro solo una piccolissima parte del campione, il 2,5%, intende certificarsi o far certificare proprio personale interno.

Fig. 6-14 Richiesta di adozione e di certificazioni della famiglia ISO 27000 lato Fornitori



Come mostrato nella fig. 6-14, solo il 9,2% del campione richiede ai Fornitori certificazioni nell'ambito ISO 27000, e poco più del 15% richiede loro di seguire in pratica tali standard pur senza essere certificati.
Una così bassa percentuale di richieste è senza dubbio un dato allarmante, considerando la forte crescita delle terziarizzazioni, ed è in parte spiegabile dal numero di rispondenti di piccole e medie organizzazioni: essi il più delle volte debbono accettare i contratti dei fornitori (soprattutto di grande 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, e sovente lo è veramente, ed il cliente dà per scontato, di poter usufruire di un elevato livello di servizio.
La certificazione per la best practice ITIL è a livello individuale mentre quella funzionalmente analoga dello standard ISO 20000 è a livello di azienda/ente.
La fig. 6-15 evidenzia che la maggioranza dei rispondenti non è interessata o non ritiene necessaria l'adozione di ITIL, ma un non trascurabile 12,5% del campione già segue le best practice ITIL ed ha proprio personale certificato; un 5,9% segue sostanzialmente queste best practice ma senza certificazioni. Un 11.8% intende seguire ITIL nel prossimo futuro, ma senza certificazioni, e solo un 1,7% dei rispondenti intende seguire ITIL facendo certificare alcune sue persone: questo significa che, del campione emerso, la maggior parte delle aziende/enti interessati già segue queste best

Fig. 6-15 Adozione di ITIL e/o ISO 20000 all'interno dell'azienda/ente



practice con o senza certificazioni, e ben pochi sono quelli che ancora non hanno personale certificato, pur volendo (o dovendo) seguire ITIL. Un 5% è certificato ISO 20000, ed il 2,5% lo farà, probabilmente a causa di obblighi derivanti da normative e/o contratti.

Nei riguardi dei propri fornitori, la fig. 6-16 evidenzia come più del 10% richieda di seguire ITIL/ISO 20000 senza richiedere certificazioni, ed il 6,7% richiede non solo che seguano tali standard, ma che siano anche certificati. L'aspetto più interessante è che aumentano notevolmente queste percentuali rispetto a quelle rilevate nell'edizione precedente (sempre considerando la differenza dei bacini di rispondenti): un indicatore che, seppur molto lentamente, anche in Italia si inizia a richiedere ai Fornitori di seguire consolidati best practice e standard, obbligandoli a certificarsi.

Un'altra importante best practice è il COBIT, fondamentale per una reale "governance" dell'ICT, e quindi anche della sicurezza digitale.

La fig. 6-17 mostra le indicazioni emerse dal campione sull'adozione di COBIT e sulle relative certificazioni, che sono a livello di singola persona. Anche in questo caso la stragrande maggioranza non è interessata o non ritiene necessaria, nel proprio contesto, l'adozione di questa best practice, attualmente alla versione 5. Solo il 5% ha già adottato sostanzialmente COBIT, ma senza personale certificato, ed il 3,4% ha anche personale certificato. Il 6,7% intende adottare COBIT nel prossimo futuro, ma solo 3,4% intende far certificare proprio personale.

Fig. 6-16 Richiesta di conformità e di certificazioni ITIL ed ISO 20000 lato Fornitori

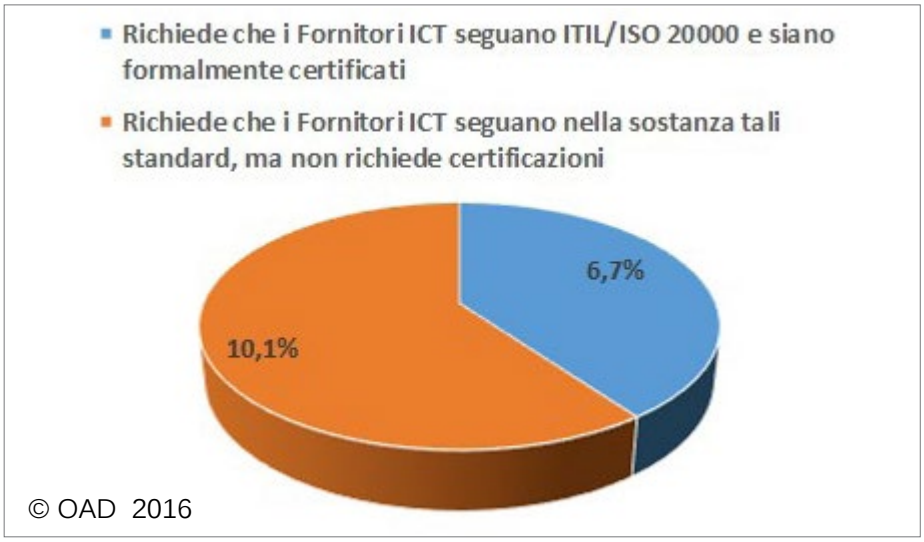
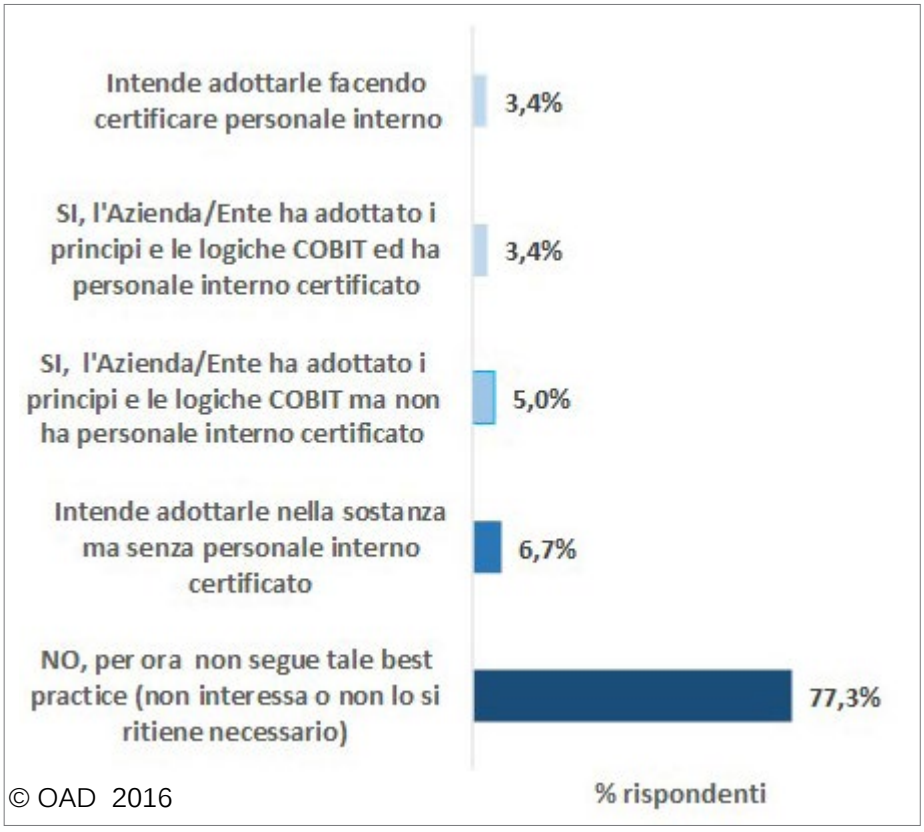


Fig. 6-17 Adozione di COBIT all'interno dell'azienda/ente



Lato Fornitori, la richiesta di seguire sostanzialmente COBIT, ma senza persone certificate è effettuata dal 7,6% del campione, e solo il 4,2% richiede anche personale certificato.
L'adozione di ISO 27000, ITIL e COBIT in Italia è di fatto limitata, seppur in lenta e leggera crescita, sia lato domanda sia lato offerta ICT, e sostanzialmente indipendente dalle dimensioni dell'azienda/ente del campione emerso, che, come dettagliato nell'Allegato A.2, è composto in maniera abbastanza ben bilanciata tra piccole, medie e grandi strutture. La limitazione nell'uso e nella richiesta di metodologie, standard e relative certificazioni riscontrata non è quindi solo causata dalle piccole e piccolissime realtà, ma anche dalla difficoltà nell'adottare metodiche e processi strutturati e trasparenti da parte delle medie e grandi organizzazioni.
Un'ulteriore causa è che tali normative non sono ancora sistematicamente richieste nei capitolati e nelle gare di appalto delle PA, che dovrebbero e potrebbero essere l'elemento trainante.
Un importante tema sulle certificazioni nel contesto, strettamente legatoal sempre vivo tema delle effettive competenze del personale ICT, è la richiesta dell'azienda/ente per il proprio personale interno che si occupa di sicurezza informatica e/o per quello dei suoi fornitori e provider, di avere specifiche qualifiche/certificazioni professionali per la sicurezza ICT quali eCF, EUCIP, CISSP, SSCP, CISA, CISP, OPSA, ecc.
Due leggi italiane in vigore, quella n. 4/2013 sulle "professioni non regolamentate" ed il D. Lgs. n. 13/2013 sulla "certificazione delle competenze" 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 l'UNI 11506, che riprende l'europea eCF[22] sulle competenze e sui profili professionali del settore ICT. In termini generali, e senza far riferimento a specifiche certificazioni nazionali ed internazionali, le fig. 6-19 e 6-20 mostrano percentualmente le richieste di certificazioni sulla sicurezza digitale rispettivamente per il personale interno e per quello dei Fornitori. In entrambi i casi l'81,5% dei rispondenti non richiede certificazioni sulla sicurezza digitale né al personale interno né a quello dei Fornitori.
Il 12,6% già pretende tali certificazioni al proprio personale, ed una percentuale quasi dimezzata, 6,7%, al personale dei Fornitori. In prospettiva, il 5,9% dei rispondenti richiederà queste certificazioni al proprio interno, e l'11,8% lo richiederà nel prossimo futuro ai propri Fornitori.

22 www.ecompetences.eu/it/

Fig. 6-18 Richiesta di conformità e di certificazioni COBIT lato Fornitori

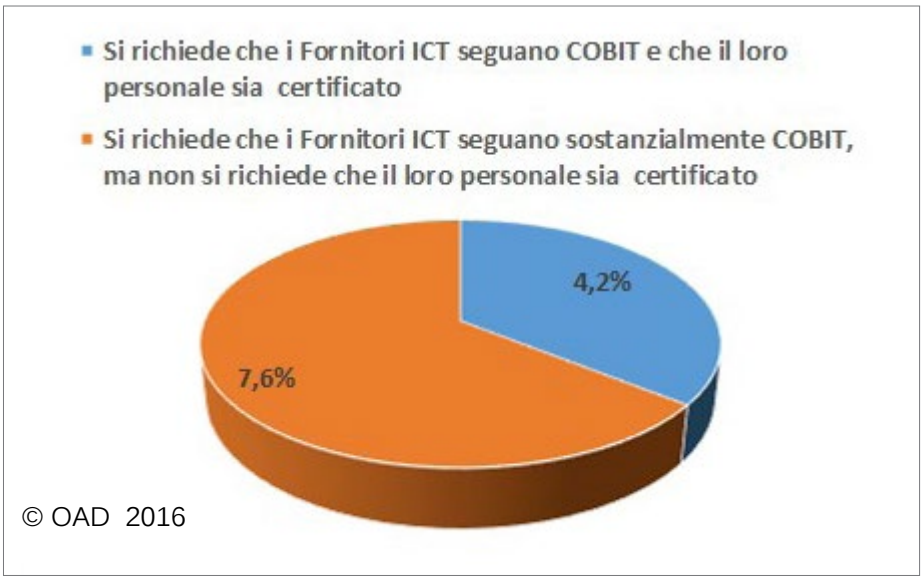


Fig. 6-19 Richiesta di certificazioni al proprio interno

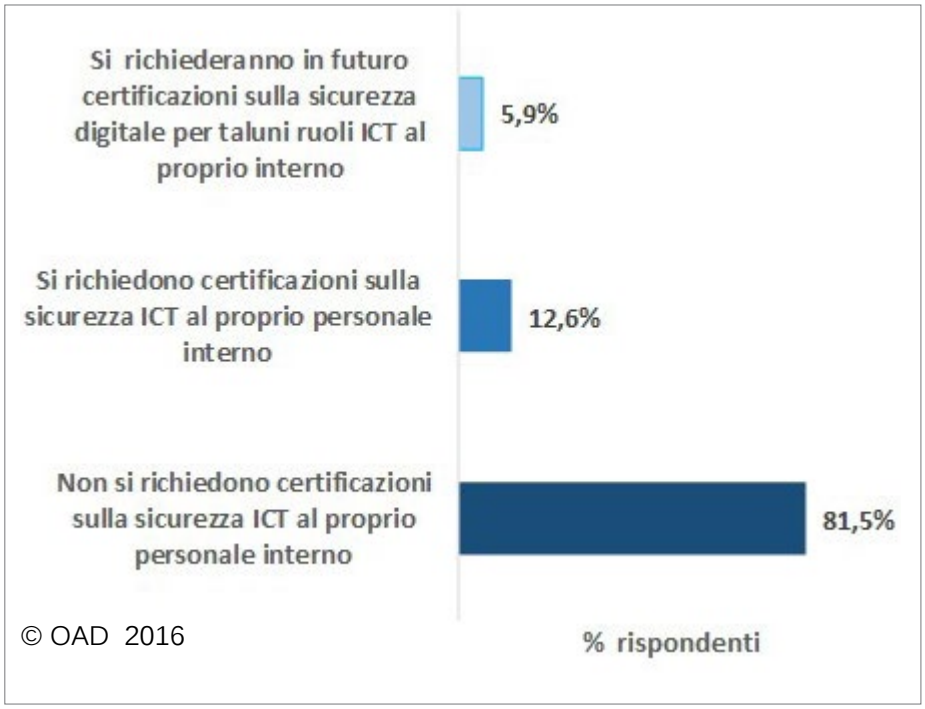
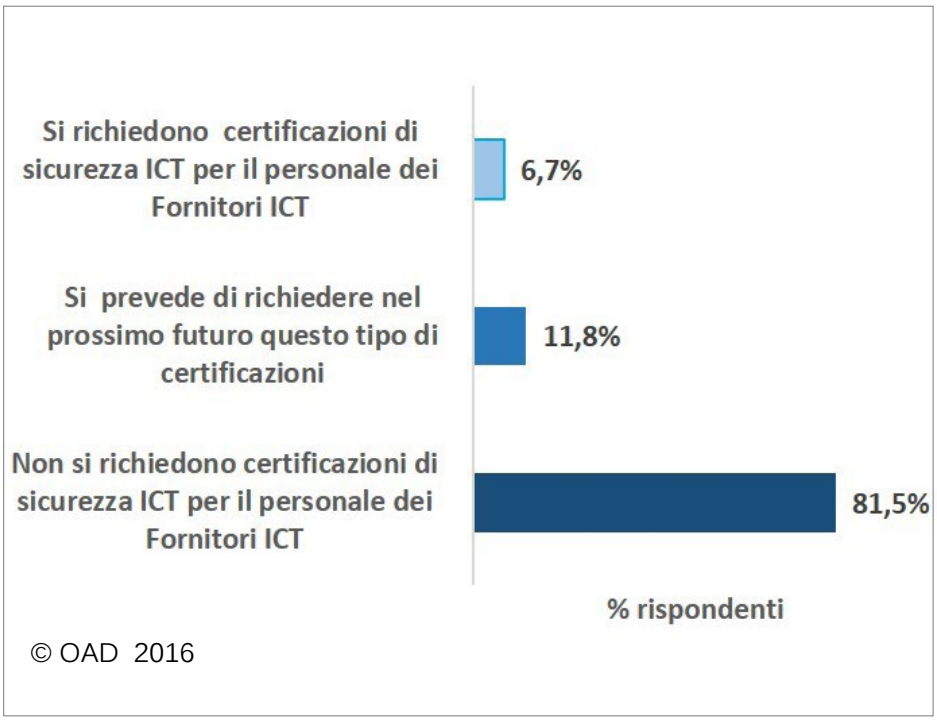


Fig. 6-20 Richiesta al personale dei Fornitori di certificazioni sulla sicurezza digitale



6.4.2 Audit ICT

Nell'ambito della gestione della sicurezza un ruolo importante è giocato dall'auditing dell'ICT. Nell'ambito del campione, come da fig. 6-21, il 45,7% già svolge questo processo pur se in diverse modalità, e il 10,1% intende svolgerlo nel prossimo futuro.
La fig. 6-21 mostra come è svolto l'auditing per chi già lo effettua: il 22,5% lo svolge internamente, un 13,2% lo svolge sia internamente sia esternamente. Il 10,1% lo svolge solo tramite auditor esterni. Come trend emerso è simile a quello dell'edizione precedente: la maggior parte di chi effettua l'auditing lo effettua internamente, in taluni casi con il supporto di esperti esterni.
Confrontando questi dati con quelli precedenti sulle certificazioni, si evidenzia, un grande divario tra l'adozione di audit e l'adozione di metodologie e relative certificazioni sulla sicurezza digitale o più in generale sull'ICT. Le motivazioni sono varie, e possono essere diverse caso per caso, ma secondo l'autore esse includono:

- la forte spinta data da varie leggi e normative che richiedono analisi dei rischi ICT, e che molte aziende/enti fanno svolgere e/o supervisionare da auditor;

- il fatto che logiche e funzioni di auditing sono già presenti nell'azienda/ente per altri settori quali contabilità, controllo di gestione, ecc., e pertanto più facilmente possono essere estese all'ICT.

Un altro dato positivo emerge dall'analisi di quando è svolto l'auditing, come dettagliato nella fig. 6-22: per i 2/3 di chi lo effettua è ormai diventato un processo sistematico, ben strutturato e regolare, svolto con cadenze periodiche, tipicamente annuali. Quasi il 26% lo effettua in maniera "irregolare", ossia non pianificato periodicamente, ma quando ritenuto necessario, e l'8,6% lo effettua solo a seguito di incidenti o di attacchi gravi. Queste percentuali evidenziano come l'auditing ICT, almeno per il campione di rispondenti, è un processo maturo, svolto in maniera periodica e sistematica.

Fig. 6-21 Attività di auditing ICT

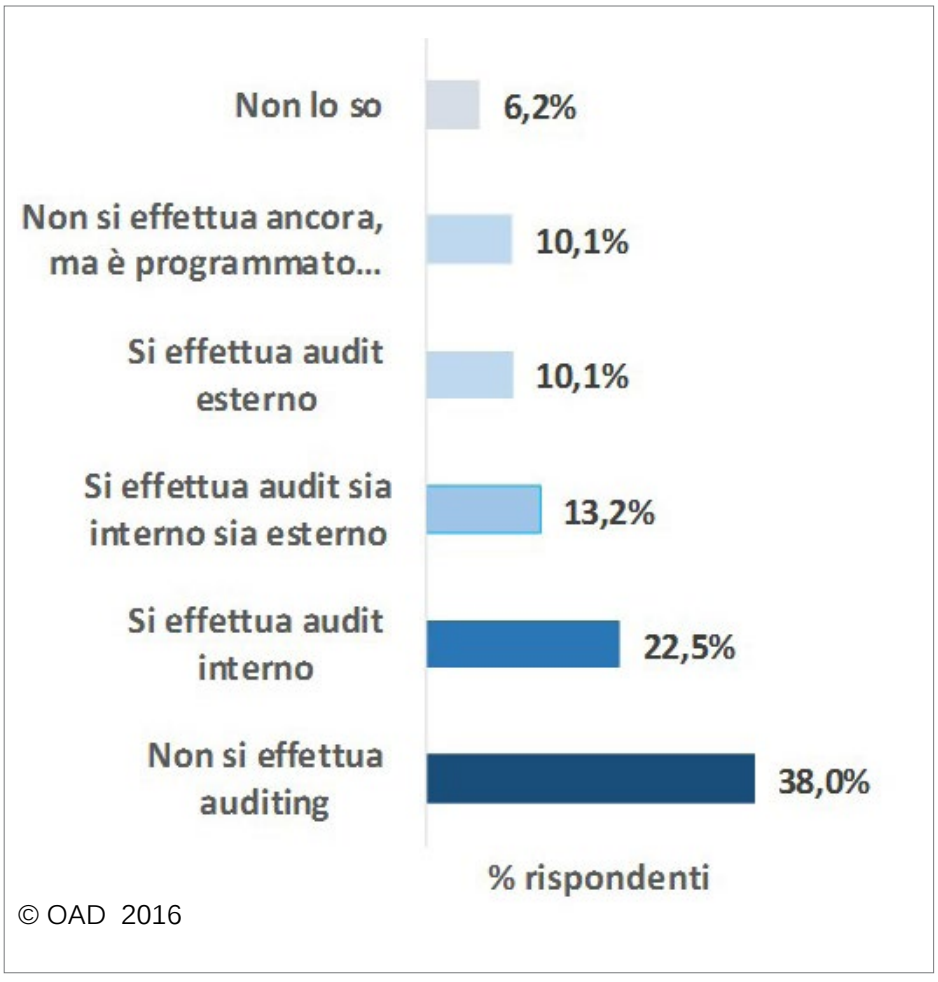
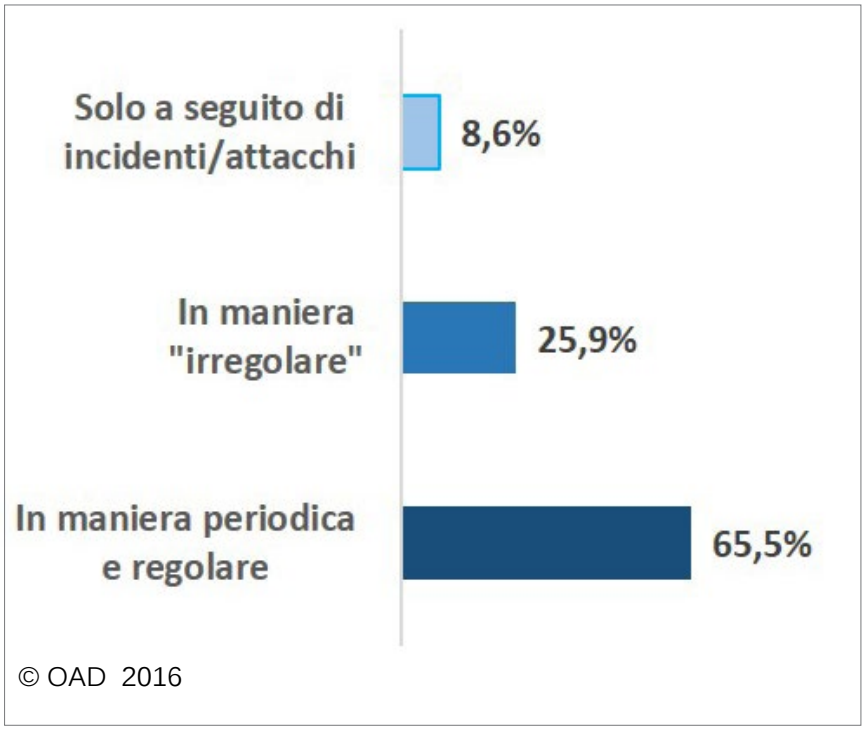


Fig. 6-22 Quando viene effettuato l'auditing

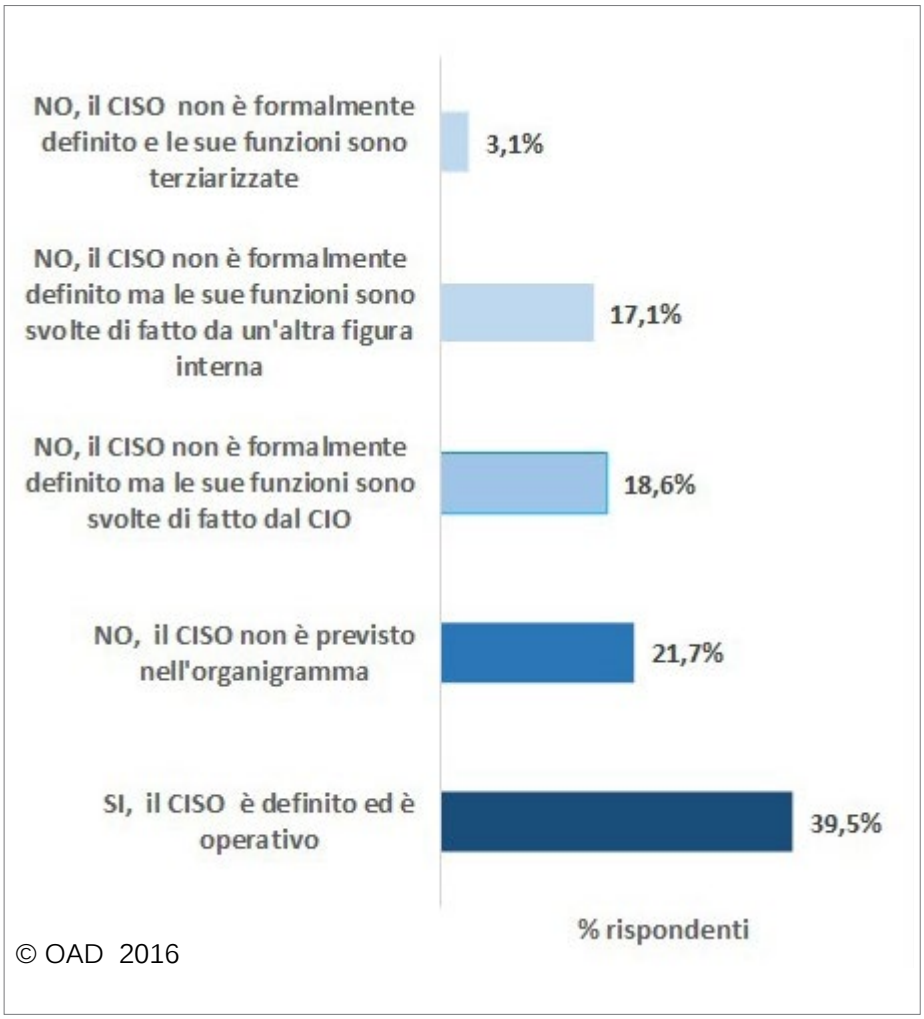


6.4.3 La struttura organizzativa interna per la sicurezza ICT

La struttura organizzativa interna all'azienda/ente per la sicurezza ICT è un altro significativo indicatore di come viene percepito il problema della sicurezza digitale e di come viene governato.
Considerando il mix di competenze tecniche, organizzative e manageriali di un simile ruolo, in inglese chiamato CISO, Chief Information Security Officer.
Come evidenziato nella fig. 6-23, il 39,5% ha definito un ruolo di "responsabile della sicurezza informatica", in inglese chiamato CISO, Chief Information Security Officer, all'interno della propria organizzazione, mentre il 21,7% non prevede tale ruolo.
Per il 18,6% tale ruolo, pur non definito formalmente, è in pratica attuato dal responsabile dei sistemi informatici (CIO), e per il 17,1 % è svolto di fatto da altri ruoli, soventi apicali, quali il responsabile dell'intera azienda/ente (CEO), il responsabile della sicurezza aziendale (CSO), dall'ufficio legale, ecc. Solo una minima parte del campione, 3,1% delega tale ruolo all'esterno a società e/o professionisti di comprovata esperienza.
Emerge chiaramente come le aziende/enti preferiscano di gran lunga gestire all'interno il ruolo di CISO, soprattutto per poter gestire all'interno i sempre più critici problemi legati alla sicurezza digitale.

Ed un valore percentuale così basso per la terziarizzazione di tale ruolo è un indicatore della difficoltà, almeno come percezione, di trovare persone e società veramente affidabili, qualificate e competenti in materia: il tema si riaggancia anche al problema delle certificazioni precedentemente affrontato.
Per le aziende/enti che hanno un ruolo, formalmente definito o no, di CISO al proprio interno, i ¾ circa lo hanno inserito nella struttura organizzativa dei sistemi informatici,chiamata in questo rapporto con l'acronimo UOSI, Unità Organizzativa Sistemi Informatici[23], ed ¼ in altre strutture dell'organizzazione.

Fig. 6-23 Esistenza del ruolo di responsabile della sicurezza digitale (CISO)



23 Il termine UOSI è usato per non connotare il livello gerarchico di questa struttura. Nella realtà italiana sono ancora pochi i casi in cui l'UOSI è una Direzione di primo livello, il cui CIO fa parte del "board". Anche in grandi e grandissime organizzazioni l'UOSI si posiziona a livelli più bassi, e può dipendere dalla Direzione Risorse Umane, dalla Direzione Amministrativa, dalla Direzione Strategie, e così via.

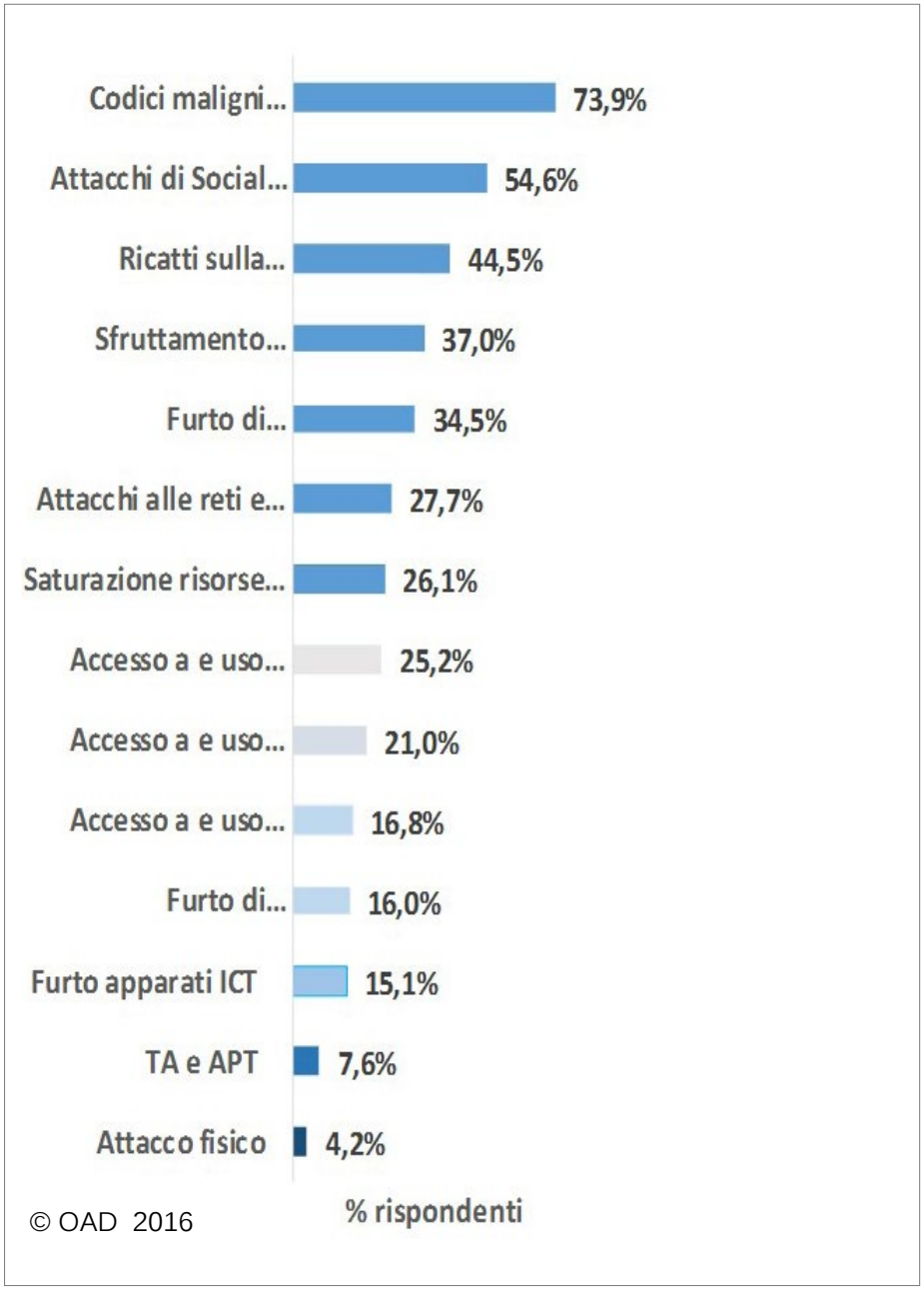
Fig. 6-24 Posizionamento organizzativo CISO

7 Gli attacchi più temuti nel futuro e le probabili motivazioni

La fig. 7-1, con risposte multiple, mostra quali sono gli attacchi ritenuti più pericolosi, e quindi più temuti nel prossimo futuro, indipendentemente da quelli eventualmente subiti e facendo sempre riferimento alla medesima tassonomia di attacchi definita nella Tabella 1. Anche in questo caso, come per le domande su "impatto poco o molto significativo" di cui al §4, non si è volutamente specificato cosa si intende e quali sono i criteri per considerare un attacco più " pericoloso", così da rendere più agile e semplice il questionario. Ciascun rispondente ha quindi selezionato i tipi di attacco ritenuti a suo giudizio più pericolosi per la propria azienda/ente da un punto di vista di impatto sul business, di impatto economico, di immagine, e così via, e/o da un mix di questi criteri.
Ai primi posti, come è ragionevole aspettarsi, alcuni degli attacchi più diffusi, tra quelli elencati in fig. 4-6 e tra quelli di maggior impatto, elencati in fig. 4-10.
Interessante evidenziare come in fondo alla classifica siano posizionati gli attacchi fisici ed i sofisticati TA e APT. Mentre per i primi è facile individuare alcune delle principali motivazioni, quali la facilità di individuazione dell'attacco, la relativa facilità di attuazione delle misure di protezione, per la seconda risulta, almeno per l'autore, più difficile. Come dettagliato nell'Allegato B.1, i rispondenti non sono solo piccole o medie aziende/enti, che potrebbero ritenersi al di fuori dei possibili target ma anche grandi e grandissime che, al contrario, potrebbero essere un preciso target, per questi tipi di sofisticati attacchi. Dimensioni e potenziale target non sono state forse correlate e considerate dai rispondenti, e quelli delle strutture più grandi hanno forse sotto sistemato il rischio che potrebbero correre. Probabilmente alcuni ritengono che il nome della loro azienda/ente non sia sufficientemente conosciuto a livello internazionale, e/o che abbiano misure di prevenzione e di protezione ritenute adeguate.

La fig. 7-2, con risposte multiple, evidenzia quali sono le probabili motivazioni degli attaccanti. Come nella precedente edizione, al primo posto per più della metà dei rispondenti, il 52,1%, è la frode informatica, che permette lauti guadagni illegali con bassi rischi di essere scoperti e puniti.
Al secondo posto il ricatto o ritorsione, cui sicuramente ha contribuito la diffusione in Italia dei ransomware, con un 51,3%.

Fig. 7-1 Gli attacchi ritenuti più pericolosi nel prossimo futuro (risposte multiple)



Nella fascia tra il 30 ed il 40%, il vandalismo e l'hacktivism, che rimangono "storicamente" diffuse motivazioni in ambito italiano.
Nella fascia tra il 20 ed il 30% tre voci, con percentuali decrescenti: il sabotaggio (non facilmente distinguibile dal vandalismo) l'azione dimostrativa, che include anche gli attacchi del così detto "ethical hacking", e lo spionaggio, in particolare quello industriale: quest'ultimo un problema crescente soprattutto per il "made in Italy" e la concorrenza sleale dai paesi stranieri.
All'ultimo posto, con la bassa percentuale del 6,7%, il terrorismo. Un valore così basso è dato sicuramente dal fatto che la maggior parte dei rispondenti appartiene ad aziende di ogni dimensione ma i cui brand non sono ritenuti così noti e di riferimento per essere degli obiettivi terroristici. La motivazione terroristica, nonostante i recenti e crescenti attacchi jihadisti, preoccupa prevalentemente alcune Pubbliche Amministrazioni ed alcune aziende di grande visibilità internazionale.

Fig. 7-2 Le motivazioni per i futuri attacchi secondo i rispondenti (risposte multiple)

A Allegato A Aspetti metodologici dell'indagine OAD

Dalla edizione 2015 è stato modificato l'ordine delle domande, iniziando da quelle relative agli attacchi informatici rilevati e lasciando alla fine quelle relative al tipo di azienda/ente del rispondente, al suo ruolo, alle macro caratteristiche del sistema informatico ed agli strumenti tecnici ed organizzativi di sicurezza informatica in uso. Il motivo principale è dovuto al fatto che alcuni rispondenti non completano il questionario, sia perché non sanno rispondere a talune domande (anche se il questionario on line consente di metterlo in attesa, salvando quanto già inserito, e riprenderlo quando si desidera, permettendo così di raccogliere informazioni non note e poter rispondere correttamente alle domande cui non si sa rispondere direttamente).

Il Rapporto OAD si basa sull'elaborazione delle risposte al questionario ricevute da CIO (Chief Information Officer), CSO (Chief Security Officer), CISO (Chief Information Security Officer), esperti di terze parti che gestiscono la sicurezza informatica, responsabili di vertice (tipicamente i proprietari e gli amministratori delle piccole medie imprese), così come evidenziato in fig. B-1 dell'Allegato B.

AIPSI, l'azienda dell'autore Malabo, NEXTVALUE ed i Patrocinatori hanno invitato, con specifiche pagine sui loro siti web e con messaggi di posta elettronica, a compilare il Questionario dell'attuale edizione tutte le persone con i profili sopra elencati delle loro "mailing list" sia lato domanda sia lato offerta ICT. Sono stati inoltre sollecitati i partecipanti a vari "social network" inerenti l'ICT e la sicurezza digitale, oltre ai partecipanti ai vari eventi sulla sicurezza digitale tenuti dall'Autore, da AIPSI e da alcuni dei Patrocinatori.

Il Questionario OAD è rimasto accessibile on line via web da inizio gennaio ai primi di giugno 2016, e in questo arco temporale i rispondenti ha ricevuto vari inviti e solleciti.

Il Questionario si articola in 65 domande, con 3 o più possibili risposte pre impostate e da selezionare con un click. In alcuni casi la risposta "Altro" consente l'inserimento di testo per poter specificare la risposta da fornire, se non riconducibile a quelle pre impostate.

Nel complesso il numero delle persone contattate si è aggirato attorno ai quattro mila, appartenenti ad un ampio insieme di aziende di ogni dimensione e settore merceologico, inclusi enti pubblici centrali e locali. L'indagine annuale OAD non ha (e non può e non vuole avere) valore strettamente statistico, basandosi su libere risposte via web-Internet da parte di un

campione di rispondenti non predefinito che partecipa su base volontaria. Come descritto nell'Allegato B, il numero e l'eterogeneità delle aziende/enti dei rispondenti, sia per settore merceologico sia per dimensione, è comunque significativo e sufficiente per fornire attendibili indicazioni sul fenomeno degli attacchi in Italia e sulle sue tendenze: indicazioni specifiche che nessun altro rapporto fornisce per l'Italia basandosi su una simile indagine.

Nei casi di risposte non chiare o errate, l'Autore non le ha considerate o le ha corrette, così come ha provveduto a verificare i dettagli delle risposte con "Altro" ed eventualmente a conteggiarle nelle risposte previste o ad evidenziarle nel Rapporto se significative.

Nel Rapporto 2016 OAD in alcuni casi si confrontano i dati emersi dalla attuale indagine con quelli delle precedenti edizioni: i campioni di rispondenti sono diversi, anche per il loro numero, ma dal punto di vista del mix e a livello qualitativo e indicativo sono confrontabili. In tali confronti si deve comunque considerare che, oltre ai campioni diversi nelle sei edizioni di OAI-OAD, le percentuali variano in funzione del numero di rispondenti, risposta per risposta, e nel caso di risposte multiple.

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 di tipo statistico e comunque il livello di dettaglio sulle caratteristiche tecniche dei sistemi ICT non consente in alcun modo di poter risalire alla azienda/ente rispondente.

Per garantire un ulteriore livello di protezione ed evitare l'inoltro di più questionari compilati dalla stessa persona, il questionario, una volta completato e salvato, non può più essere modificato, e dallo stesso posto di lavoro non è più possibile compilare una seconda volta il questionario.

L'Autore, AIPSI, Malabo e Nextvalue garantiscono inoltre la totale riservatezza sulle risposte raccolte, utilizzate solo per l'indagine OAD 2016, la produzione del presente Rapporto e l'eventuale presentazione di OAD in eventi.

B Allegato B Il campione emerso dall'indagine

Le risposte avute sono state 288 un numero di risposte ricevute sono comunque sufficiente e significativo a fornire delle concrete indicazioni sugli attacchi ai sistemi informatici in Italia.

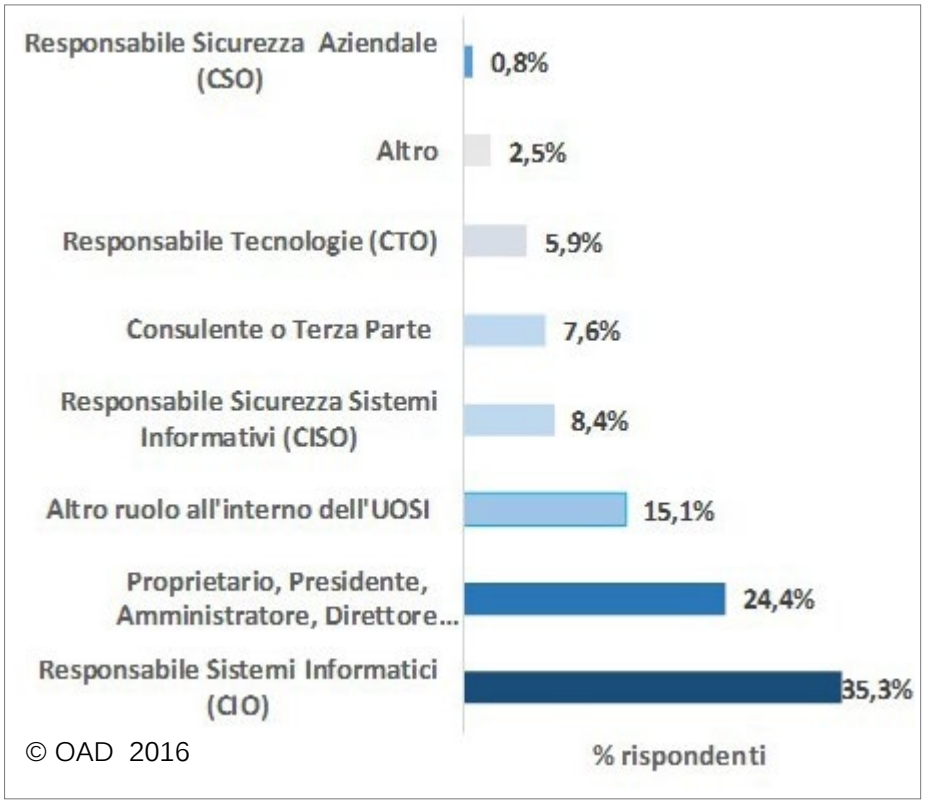
B.1 Chi ha risposto: ruolo e tipo di azienda/ente

Il bacino di utenza contattato è costituito prevalentemente da CIO, CSO, CISO e da altre figure, dai fornitori ed i consulenti, che gestiscono per l'azienda/ente la sicurezza informatica, fino ai responsabili di massimo livello delle aziende piccole e piccolissime (proprietari, presidenti e amministratori) che direttamente o indirettamente conoscono e decidono per i loro sistemi informatici e la relativa sicurezza.

La fig. B-1 mostra la ripartizione dei compilatori per ruolo: al primo posto, come percentuale sul totale dei rispondenti, sono i responsabili dei sistemi informativi (CIO), al secondo posto i vertici dell'azienda/ente (Proprietario, Partner, Presidente, Amministratore Unico o Delegato, Direttore Generale), al terzo posto il personale interno che, a tempo pieno o no, opera sulla sicurezza ICT e che tipicamente è inserito nella struttura UOSI, al quarto posto i responsabili della sicurezza informatica (CISO), che dovrebbero essere i rispondenti tipici del questionario OAD. Tale classifica, ed in particolare il basso valore dell'8,4% per il ruolo di CISO, è un chiaro indicatore di come tale ruolo sia ancora raro negli organigrammi anche di aziende di medie e grandi dimensioni. Inoltre, per le strutture italiane di multinazionali con quartier generale all'estero, il CISO è normalmente operante nel quartier generale. Il secondo posto di un rispondente del vertice aziendale è un chiaro indicatore che, soprattutto nelle piccole imprese, la sicurezza digitale, è gestita proprio dal vertice, magari con l'ausilio di consulenti e/o Fornitori.

In alcuni organizzazioni il responsabile delle tecnologie (CTO, Chief Technology Officer) guida anche l'ICT. All'ultimo posto, con una bassissima percentuale dell'1%, il ruolo di responsabile della sicurezza aziendale (CSO): tale valore è ragionevole, dato che difficilmente il CSO si occupa di sicurezza digitale, anche se in qualche organizzazione (ma poche) il CISO appartiene alla sua struttura organizzativa. Nella voce "Altro" alcuni rispondenti hanno specificato per il loro ruolo quello di "responsabili commerciali". Appartengono probabilmente a succursali italiane di aziende internazionali con attività in Italia prevalentemente di vendita, che direttamente si occupano degli aspetti informatici in Italia, e quindi anche della sicurezza digitale.

Fig. B-1 Ruolo dei rispondenti

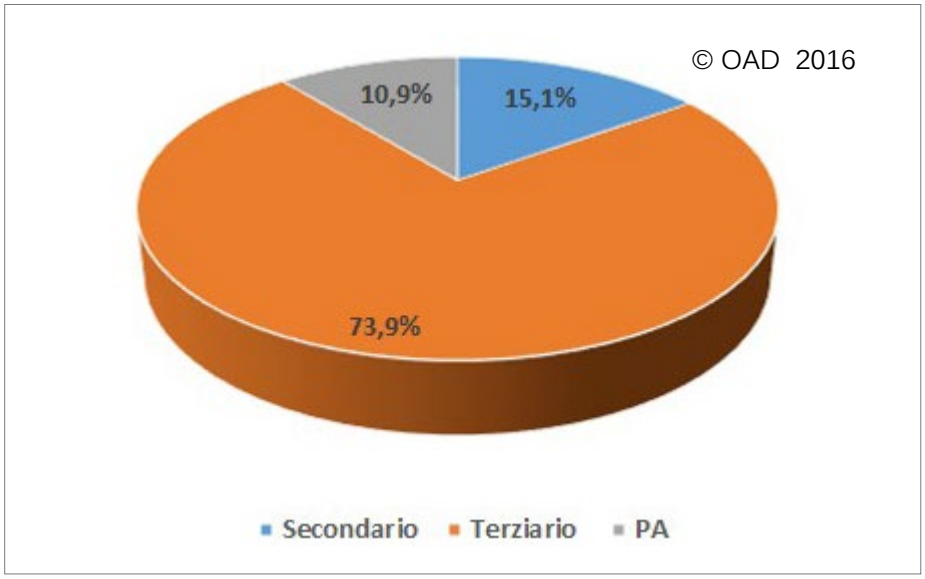


La Fig. B-2 schematizza i macro-settori cui appartengono le aziende/enti dei rispondenti. La stragrande maggioranza appartiene al terziario, e con percentuali molto inferiori gli appartenenti al settore secondario, che include l'industria manifatturiera e delle costruzioni, ed ancora più basse le percentuali dei rispondenti delle Pubbliche Amministrazioni, sia locali sia centrali. Purtroppo non si è avuta alcuna risposta da aziende del settore primario, che include agricoltura, allevamento, pesca, estrazione, causa il non coinvolgimento di fatto delle loro Associazioni di categoria (si cercherà di rimediare nelle prossime edizioni di OAD).

Il dettaglio di appartenenza dei compilatori per i settori merceologici di appartenenza delle loro aziende/enti è dettagliato nella fig. B-3, che fa stretto riferimento, come per la precedente edizione, alla classificazione ATECO, in modo da ridurre possibili errori di posizionamento da parte dei rispondenti. La classificazione ATECO, cui si sono aggiunte le Pubbliche Amministrazioni Centrali e Locali, è riportata nella Tabella 5.

La fig. B-3 evidenzia al primo posto i Servizi ICT, seguiti dall'industria manifatturiera e delle costruzioni (settore secondario).

Fig. B-2 Macro-settori merceologici delle aziende/enti dei rispondenti



Non ci sono stati risposte dal macro settore primario, oltre che dai settori di attività sportive, ricreative ed artistiche, dai trasporti e magazzinaggio.
Pochi anche dal settore dei servizi turistici, alloggio e ristorazione, dall'Istruzione, dagli ambienti bancari ed assicurativi, dalle Pubbliche Amministrazioni. Come indicato dalla fig. B-2, il Rapporto OAD 2016 risulta significativo, come numero di risposte, soprattutto per il macro-settore del terziario. Per le prossime edizioni OAD dovrà meglio coinvolgere i settori merceologici non o troppo poco rappresentati come numeri di risposte al questionario rispetto alle loro dimensioni in Italia, cercando ad esempio di meglio attivare tramite AIPSI e Nextvalue relazioni con le specifiche associazioni di categoria.
La fig. B-4 mostra la ripartizione percentuale delle aziende/enti dei rispondenti per dimensioni, in termini di numero di dipendenti. La ripartizione è stata pensata in tre classi fino a 250 dipendenti, limite dimensionale perché un'azienda rientri nelle PMI, Piccole Medie Imprese, ed in altre 3 classi per rappresentare le grandi e grandissime aziende/enti. La maggior parte dei rispondenti, 43,7%, appartiene a strutture fino a 49 dipendenti. Le altri classi hanno ciascuna una percentuale tra il 10,1 ed il 12,6%. Il campione emerso risulta quindi abbastanza ben bilanciato tra piccole stretture e quelle medio grandi e grandissime. Una conferma viene considerando le più recenti indagini CGIA di Mestre su dati Infocamere – Movimprese del 2012 (gli analoghi ultimi dati ISTAT pubblici risalgono ad un anno prima), per le quali:

- le aziende fino a 49 addetti risultavano essere 5.246.179;
- quelle da 50 fino a 249 risultavano 25.359;
- quelle oltre i 250 risultavano 3.977.

Tabella 5 I settori merceologici considerati nel Questionario OAD

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. B-3 Settore merceologico delle aziende/enti dei rispondenti

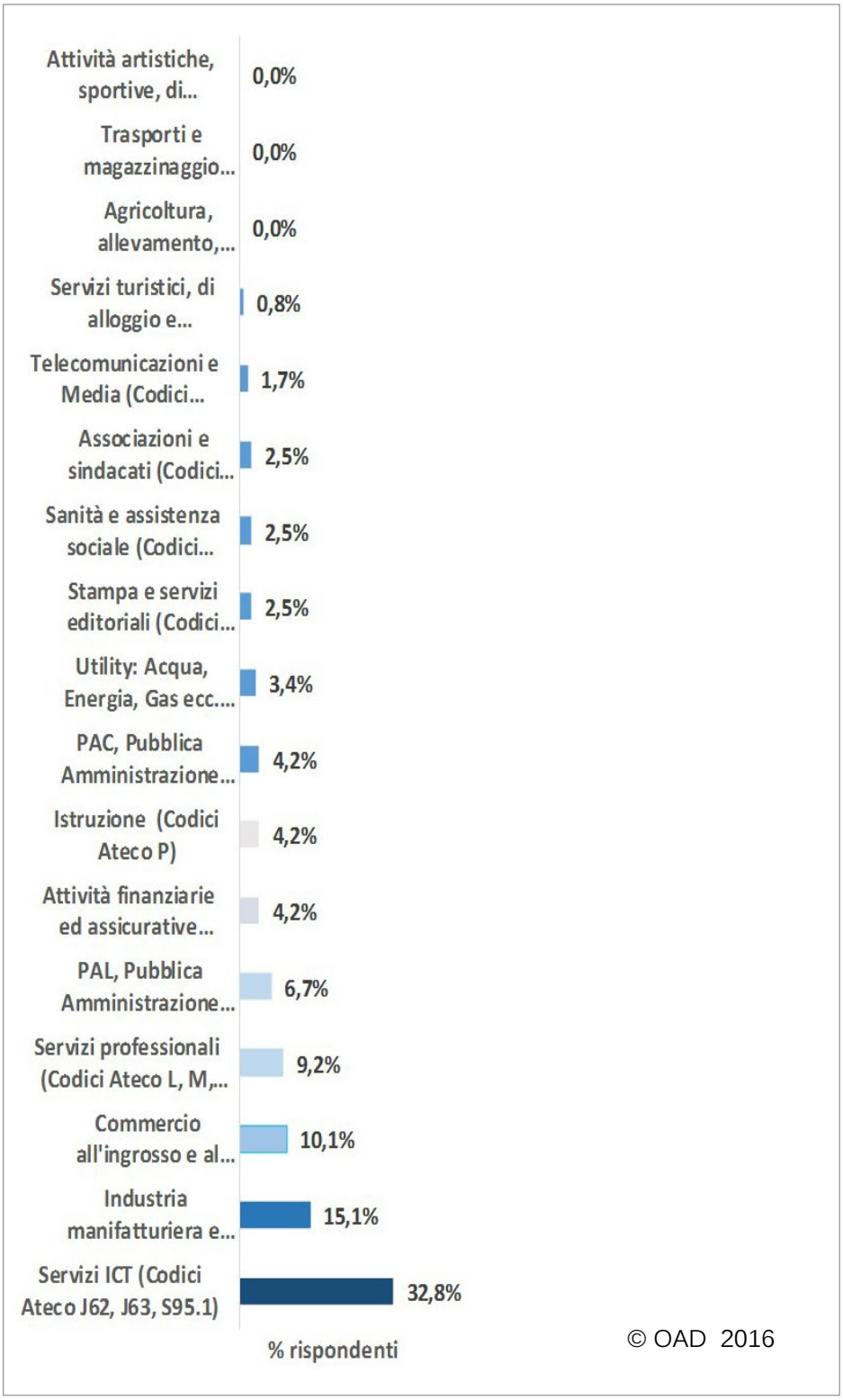
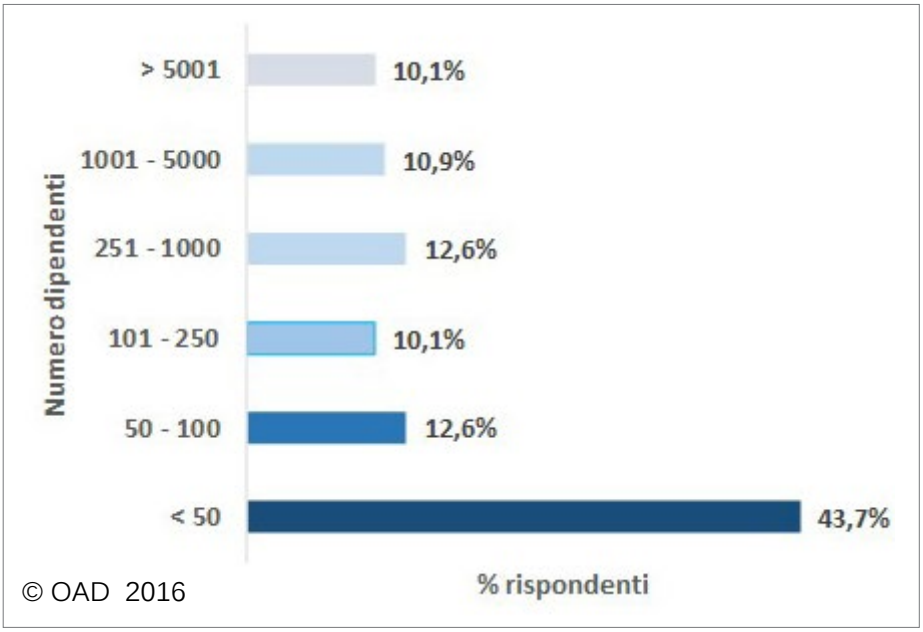


Fig. B-4 Dimensioni aziende/enti dei rispondenti per numero di dipendenti



L'area geografica di copertura dell'azienda/ente è, per il campione raccolto, prevalentemente in Italia, ma il 2,5% opera a livello europeo ed il 17,6% a livello mondiale, come dettagliato nella fig. B-5.
Interessante notare come la percentuale di aziende che operano a livello europeo sia molto inferiore a quella a livello mondiale. Per le aziende dei rispondenti probabilmente operare in Europa risulta più difficile e/o meno redditizio che operare in paesi extra europei.
Complessivamente, più del 20% dei rispondenti opera in aziende attive fuori dall'Italia: un dato significativo sul campione emerso.
Nella fig. B-6 i rispondenti dell'area solo nazionale sono dettagliati per copertura nelle singole aree Nord-Centro-Sud e Isole o sull'intero territorio. Più della metà opera solo al Nord, il 31,6% opera sull'intero territorio nazionale e, a decrescere, il 10,5% solo nel Centro e il 3,2% solo nel Sud-Isole.
Per gli aspetti organizzativi sulla gestione della sicurezza informatica si rimanda a §6.4

Fig. B-5 Copertura geografica delle aziende/enti dei rispondenti

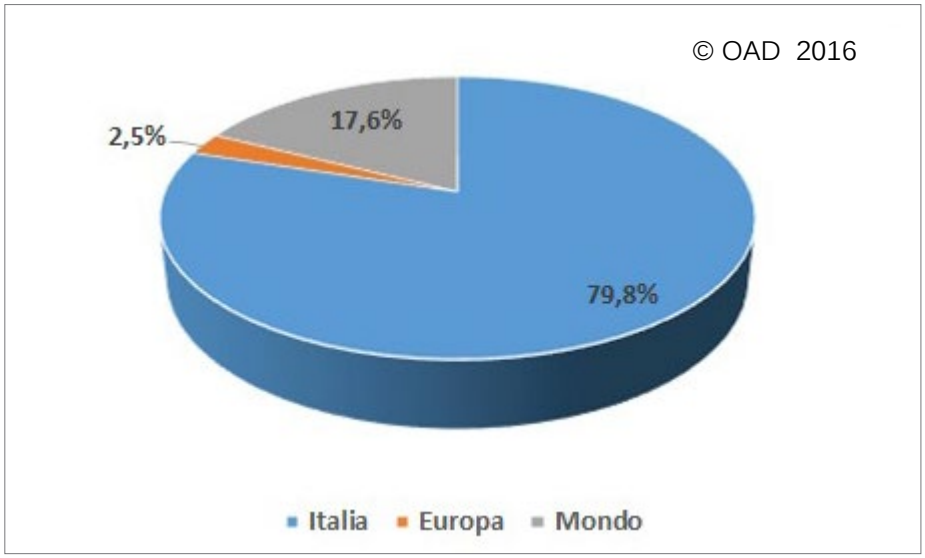
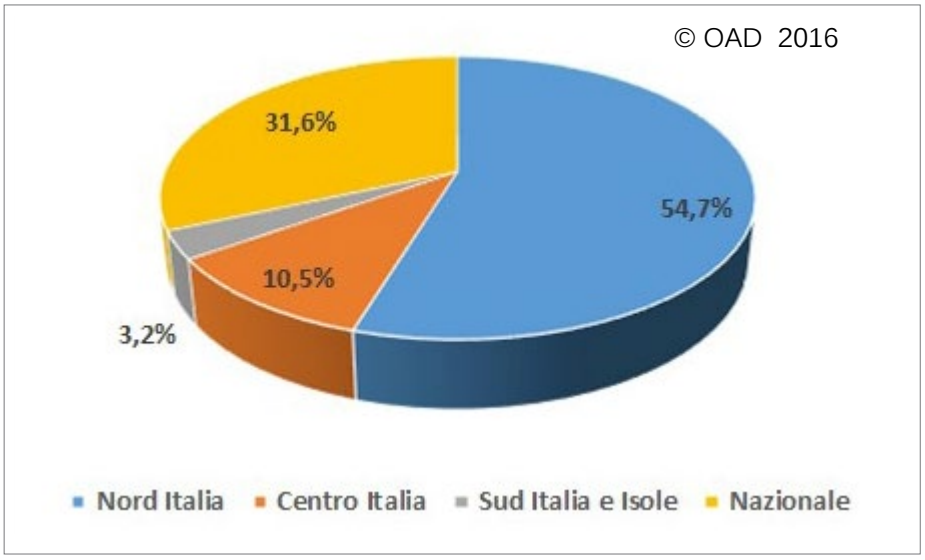


Fig. B-6 Dettaglio copertura geografica in Italia delle aziende/enti dei rispondenti



B.2 Macro caratteristiche dei sistemi informatici del campione emerso dall'indagine

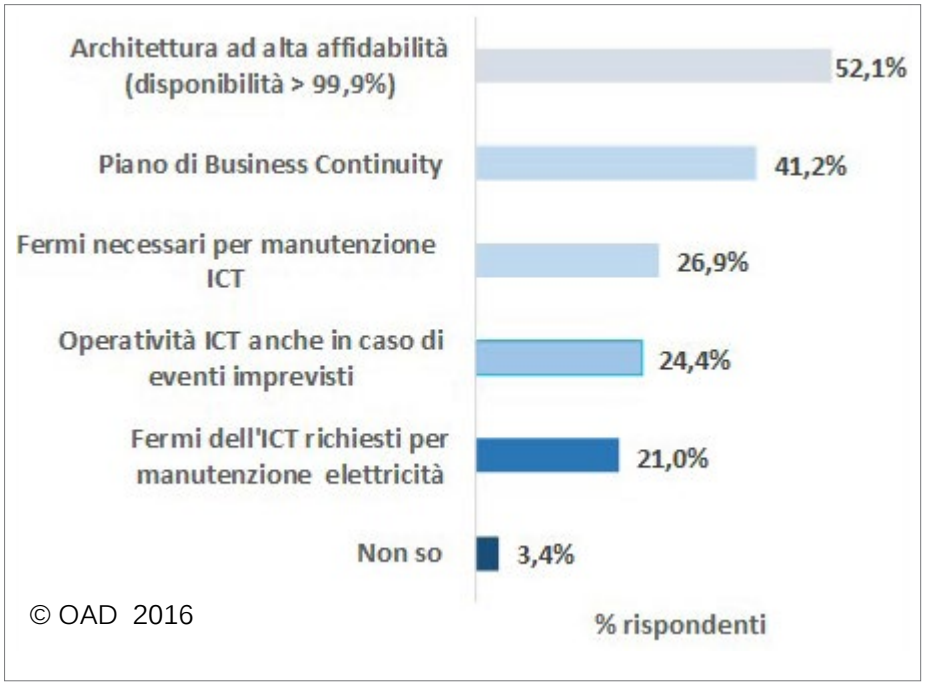
Per comprendere su quali sistemi informatici del campione gli attacchi digitali abbiano o non abbiano avuto successo, il questionario poneva alcune domande per rilevare le caratteristiche tecniche più significative, oltre alle domande sulle misure di sicurezza adottate, di cui al Capitolo 6.

La prima domanda sui sistemi informatici dei rispondenti, con risposte multiple, riguarda la loro affidabilità e disponibilità, e le risposte sono mostrate nella fig.B-7.

Più della metà (52,1%) dei rispondenti dichiara di disporre di architetture ad alta affidabilità, almeno nell'ambito delle applicazioni più critiche per il business, ed il 42,1% di avere un Piano di Business Continuity (continuità operativa).

Quasi ¼ dei rispondenti afferma che il proprio sistema informatico, in toto o quanto meno le sue parti più critiche, funzionano anche in caso di eventi imprevisti, ma una percentuale leggermente maggiore, 26,9%, deve fermare l'intero sistema informatico o sue parti per poter effettuare manutenzione ordinaria dell'hardware e/o del software, ed il 21% che deve fermare l'intero sistema informatico o sue parti per manutenzione della fornitura elettrica.

Fig. B-7 Livello di affidabilità del sistema informatico e/o di sue parti (risposte multiple)



La fig. B-8 mostra in percentuale il numero di server, sia fisici che virtuali, presenti nei vari ambienti di produzione, di test e di sviluppo. I dati sono percentualmente simili a quelli raccolti nelle precedenti edizioni: la stragrande maggioranza dei sistemi ha al massimo fino a 100 server (fisici e/o virtuali), con il 35,3% del totale che arriva solo a 10, come è tipico per strutture di piccole dimensioni.
La fig. B-9 mostra le percentuali del numero di posti di lavoro fissi (PdL) per sistema informatico: la maggior parte, quasi 1/3 dei rispondenti, ha tra 11 e 100 Pdl, ed il 28,6% ne ha al massimo fino a 10. Quasi il 60 % dei rispondenti ha fino a 100 PdL, il 20,2% tra 101 e 1000 PdL, ed il 18,5% oltre i mille.
Questi dati sul numero di server e di PdL sono congruenti con le dimensioni di aziende/enti rispondenti, di cui alla fig. B-4. e confermano il buon bilanciamento tra organizzazioni di diverse dimensioni. La fig. B-10 mostra le percentuali del numero di PC Laptop mobili di proprietà dall'azienda/ente forniti ai dipendenti. Interessante notare che 0,8% dei rispondenti non possiede PC laptop mobili.
La diffusione maggiore in percentuale è data dalla fascia tra 10-100, confermando quanto rilevato nelle figure precedenti. In termini di sicurezza i dispositivi mobili, in particolare smatphone e tablet, giocano un ruolo crescente e critico, data la loro esplosiva diffusione, oltre che per il fenomeno della "consumerizzazione". I dispositivi mobili, tablet e smartphone in primis, di fatto rappresentano l'attuale era "post PC" e per questo motivo dal Rapporto OAI 2012 sono stati considerati e analizzati nell'indagine OAI-OAD.

Fig. B-8 Numero di server fisici e virtuali per sistema informatico

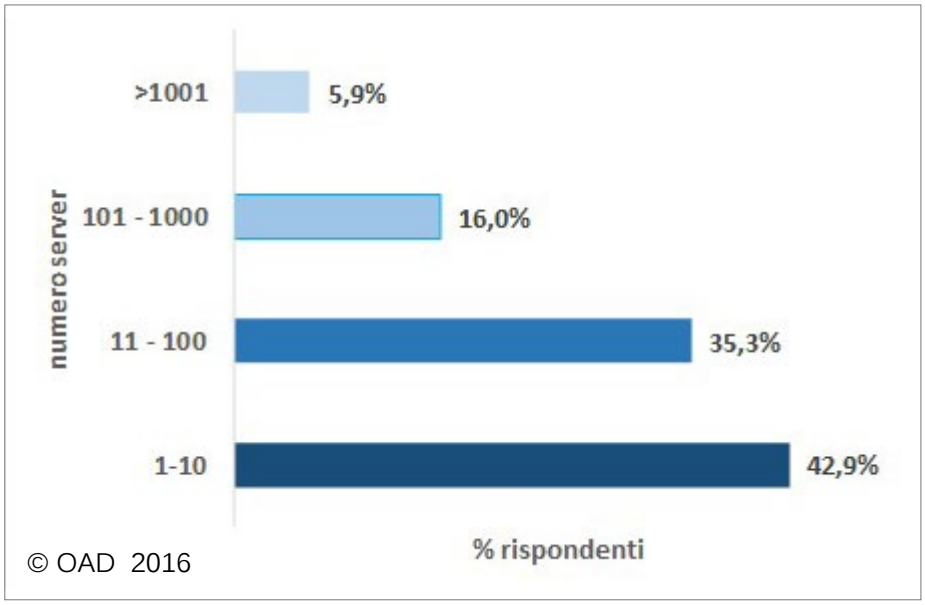


Fig. B-9 Numero di posti di lavoro fissi per sistema informatico

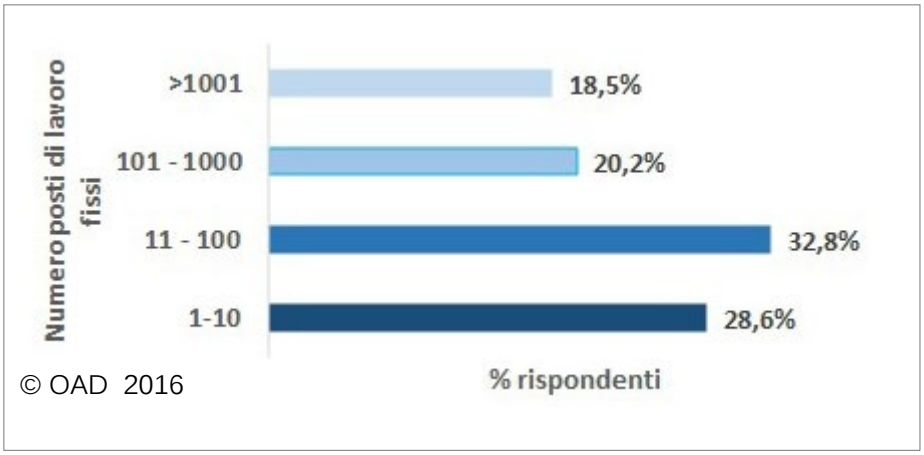
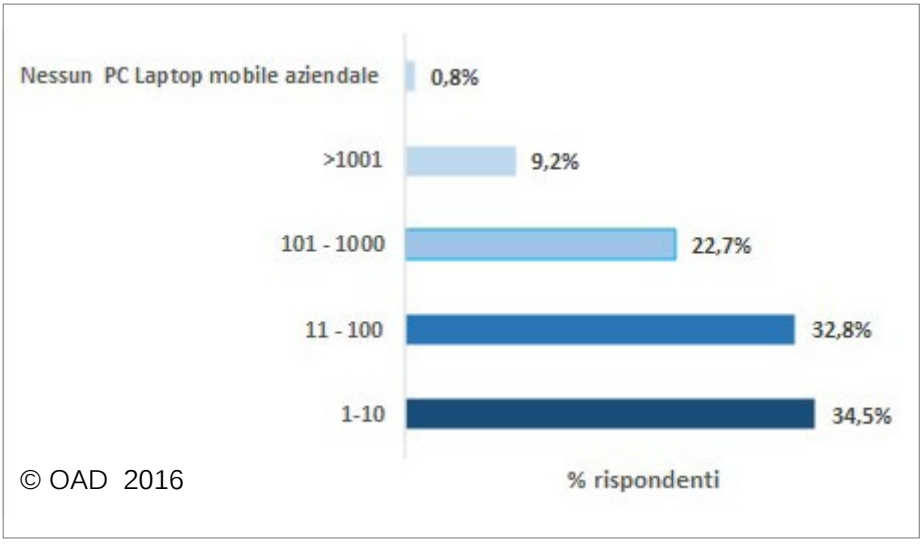


Fig. B-10 Numero PC laptop mobili di proprietà dell'Azienda/Ente



La fig. B-11 mostra le percentuali del numero di tablet di proprietà dall'azienda/ente, tipicamente forniti alle persone di vertice e a quelle che hanno una elevata mobilità.
Da sottolineare l'elevato numero di aziende/enti, 17,6%, che non utilizza tablet di proprietà. Le percentuali rilevate sono congruenti con quelle relative al numero di dipendenti ed al numero di dispositivi fissi e mobili.
La fig. B-12 riporta la distribuzione in percentuale del numero di smartphone per azienda/ente rispondente, anch'essa congruente con gli altri dati del campione. Per i dispositivi mobili le figure da B-10 a B-12 mostrano che alcune poche aziende/enti non ne forniscono ai dipendenti.
Il motivo, al di là della possibile non necessità, deriva principalmente dal rischio percepito per il loro possibile uso anche per motivi non lavorativi e dal conseguente problema di come garantire l'idoneo livello di sicurezza digitale per questi dispositivi d'utente.
Le fig. B-13 e 14 schematizzano come viene affrontato dal campione dei rispondenti il fenomeno della "consumerizzazione", spesso indicato con l'acronimo inglese BYON, Bring Your Own Device, che consente all'utente finale di utilizzare i propri dispositivi mobili per attività sia personali che di lavoro.

Fig. B-11 Numero di dispositivi mobili Tablet di proprietà dell'Azienda/Ente

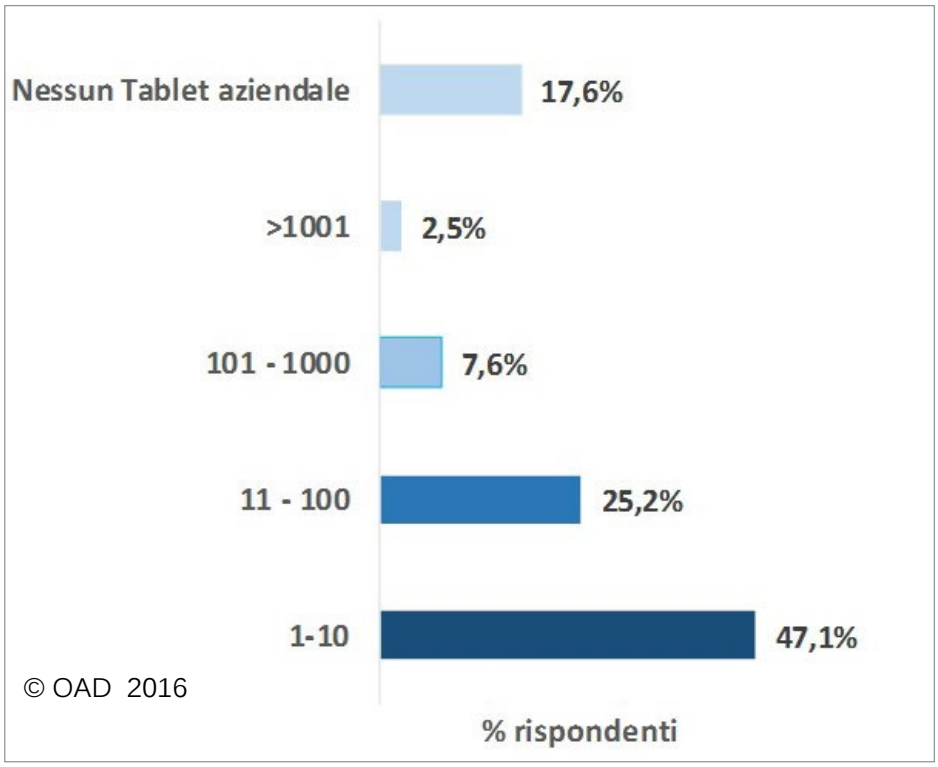
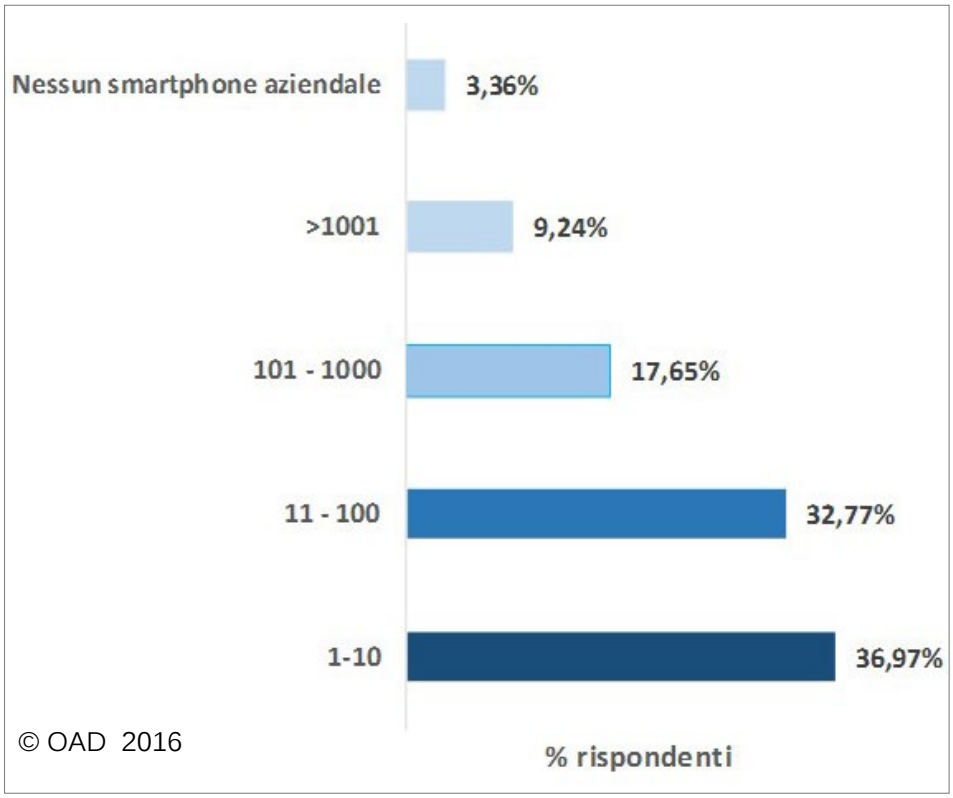
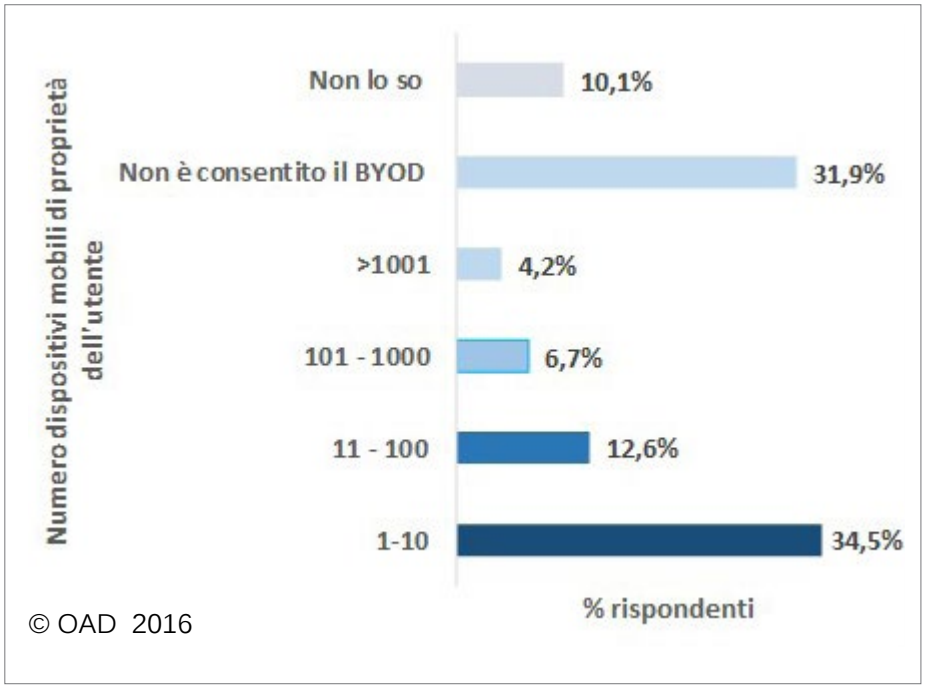


Fig. B-12 Numero di Smartphone di proprietà dell'Azienda/Ente



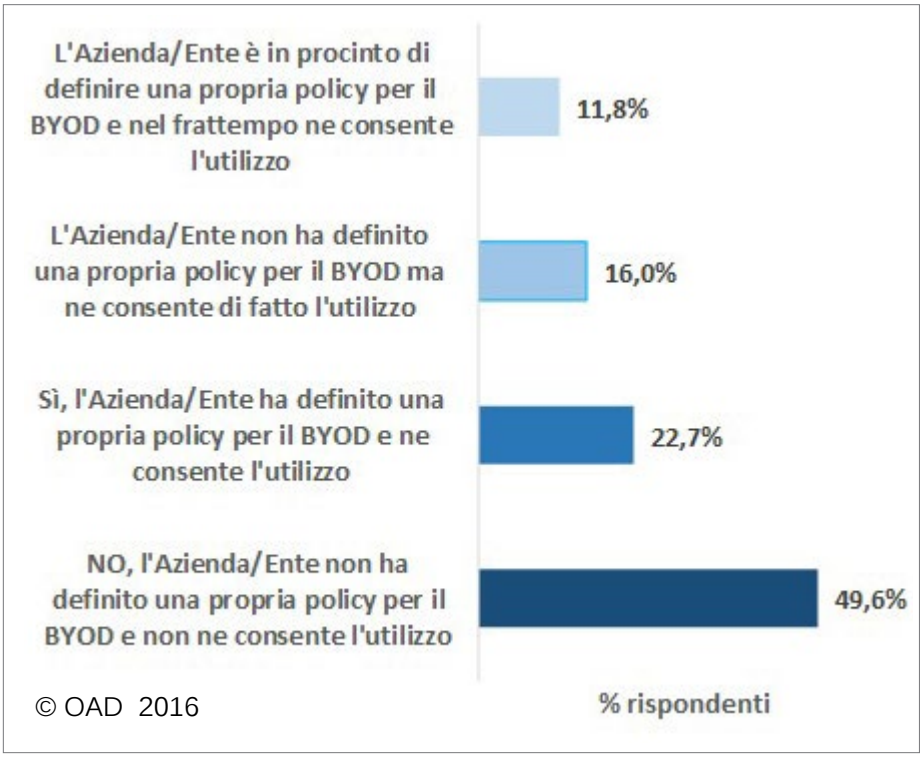
La fig. B-13 illustra il numero di **dispositivi mobili di proprietà dell'utente finale** usati anche per attività di lavoro, e quindi con collegamenti ai sistemi informatici dell'azienda/ente.
I dati emersi meritano alcune considerazioni. In quasi 1/3 delle aziende/enti dei rispondenti non è consentito il BYOD, ed una percentuale non bassa, il 10,1% dichiara di non sapere se e quanti sono i dispositivi degli utenti in BYOD.
Il motivo di questo secondo dato è che talvolta i dispositivi mobili, in particolare gli smartphone, non sono gestiti dalla UOSI ma dalle singole direzioni/unità di business, e le persone di UOSI, che costituiscono la maggior parte dei rispondenti, possono ignorare le dimensioni di questo fenomeno.
Se questo fosse vero, come è molto probabile, è un indicatore che il BYOD, se consentito, non viene governato opportunamente con i conseguenti gravi rischi per la sicurezza digitale.
Le risposte tipo "non so" sono un importante riscontro della correttezza dei compilatori che non "inventano" dati che non conoscono, ed ammettono di ignorare talune situazioni che non gestiscono: sincerità e correttezza che confermano la serietà e l'autorevolezza dei dati raccolti.

Fig. B-13 Numero di dispositivi mobili di proprietà dell'utente finale utilizzabili nell'ambito del sistema informatico dell'azienda/ente



La fig. B-14 dettaglia come viene gestito, se viene gestito, il fenomeno BYOD, che si sta diffondendo, inconsapevolmente o no, in Italia, anche perché voluto in pratica dai vertici delle organizzazioni.
Nel rispondere a questa domanda i rispondenti sembrano essere stati più restrittivi rispetto alla domanda di cui alla fig. B-13: in quest'ultima il divieto d'uso del BYOD è del 31,9%, cui si potrebbe aggiungere una quota parte del "non lo so", ma ora la percentuale sale quasi al 50%.
La piccola incongruenza di questa differenza, che l'autore non ha voluto forzatamente correggere, è probabilmente dovuta al fatto che il rispondente, nel ragionare sulle diverse risposte sulle policy per il BYOD, è stato più restrittivo.
Il dato più interessante è che più di 1/5 dei rispondenti, il 22,7%, ha definito delle precise policy sull'argomento, ed ha quindi attivato specifici strumenti di sicurezza per consentire il BYOD.
La fig. B-15, con risposte multiple, mostra la diffusione dei principali sistemi operativi (OS) per server in uso nei sistemi informatici dei rispondenti. Si evidenzia come gli OS Microsoft Windows nelle loro varie versioni, siano i sistemi più diffusi tra i rispondenti, cui seguono gli OS Linux insieme a quelli Unix, anch'essi nelle varie versioni.

Fig. B-14 Policy per il BYOD delle aziende/enti dei rispondenti

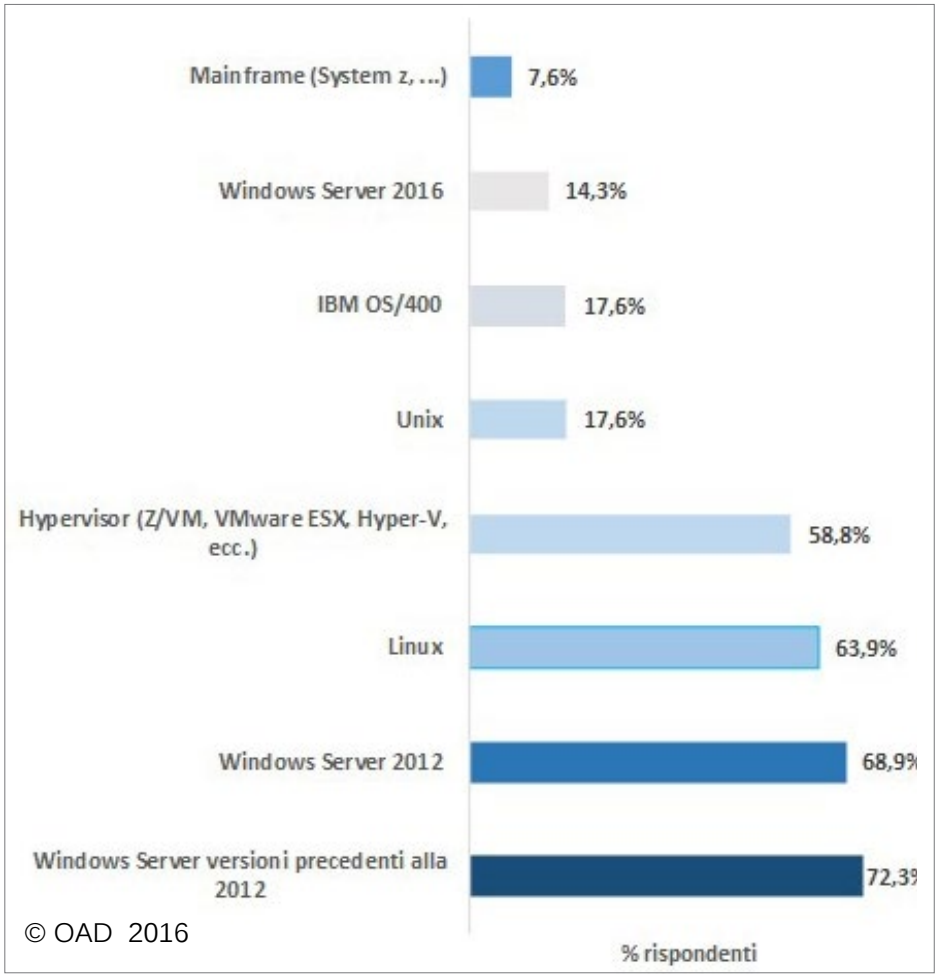


Windows, Linux-Unix sono usati contemporaneamente nella maggior parte dei sistemi informatici, soprattutto quelli di medie e grandi dimensioni, facilitati anche dalla diffusione dei sistemi virtualizzati, utilizzati da quasi il 60% dei rispondenti. In ambito Windows è da sottolineare l'ampia diffusione della versione 2012, con il 68,9%. Ovviamente ancor più diffuse le precedenti versioni dell'OS Windows Server, quali 2008, 2003 e forse anche 2000, incluse nella voce "Windows Server pre 2012", che arrivano al 72,3%. Assai interessante è il 14,3% dell'ultimo OS Windows, il 2016: la piccola differenza tra l'installato pre e dopo la versione 2012 è un chiaro segno che gli OS Windows sono aggiornati abbastanza tempestivamente. I sistemi Linux coprono quasi il 64% del campione con un 56,3%, molto superiore al 17,6% degli OS Unix proprietari. Un notevole risultato per i sistemi opensource. Ampia diffusione, 58,8%, degli OS "hypervisor" per la virtualizzazione dei server, che includono prodotti quali Z/VM, VMWare, ESX, XenServer, Hyper-V, anche grazie alla crescente diffusione di soluzioni in cloud o comunque terziarizzate in hosting.

I sistemi AS 400, storicamente diffusi nelle PMI di fascia medio-alta, con il loro OS 400, mantengono in Italia una quota interessante del 17,6%, pari a quella dei sistemi Unix.

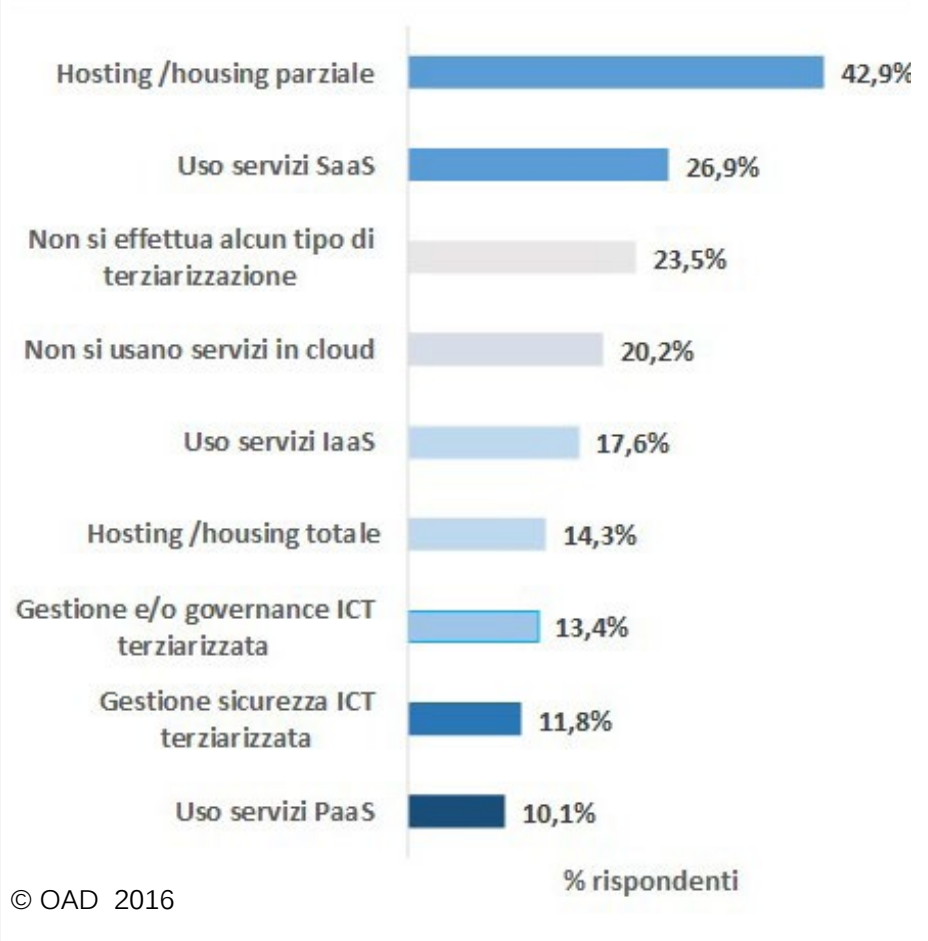
Gli OS per mainframe, come l'IBM System z e supercomputer, costituiscono una nicchia attorno al 7,6%, tipicamente come "host" centrali di grandi organizzazioni quali industrie a livello internazionale, banche, assicurazioni e PAC. I dati raccolti evidenziano come i sistemi informatici del campione rispondente siano aggiornati, indice che tale campione appartiene in media ad una fascia "alta", in termini di maturità nel governo dell'ICT; e come questo mercato sia ormai dominato da due grandi famiglie di prodotti, i sistemi operativi Windows ed i sistemi operativi Linux-Unix, cui si stanno aggiungendo gli hypervisor.
La fig. B-16, con risposte multiple, sintetizza l'uso della terziarizzazione dell'ICT, incluse le soluzioni in cloud. La figura mostra che circa 1/5 dei rispondenti non utilizza servizi in cloud, e che il 23,5%, quasi ¼ dei rispondenti, non effettua alcun tipo di terziarizzazione.

Fig. B-15 I sistemi Operativi in uso (risposte multiple)



La maggior parte dei rispondenti, con quasi il 43%, effettua hosting o housing di parte dei propri sistemi ICT, ed un 14,3% ha l'intero proprio sistema informatico in hosting/housing. Il 37,7% dei rispondenti non terziarizza affatto, ed il 47,4% utilizza un housing/hosting parziale dei propri sistemi ICT. L'housing/hosting totale è effettuato dal 13,6% e con percentuali ancora inferiori viene terziarizzata la gestione e la sicurezza dei sistemi informatici.
Nell'uso del cloud il SaaS ha la quota maggiore con quasi il 27% dei rispondenti, mentre il PaaS ha la quota minore su ogni tipo di terziarizzazione.
Non trascurabile, anche se ancora limitata, la quota di chi terziarizza la gestione della sicurezza digitale, con un 11,8%.
Come per le precedenti edizioni, in termini di trend, confrontando i dati su hosting/housing e su cloud, si evince che la prima è più utilizzata dai rispondenti rispetto al cloud.

Fig. B-16 Terziarizzazione dei servizi ICT (risposte multiple)



Come già emerso nel precedente rapporto, oltre che da altri recenti rapporti e guide [24] sul cloud, è in atto nelle aziende/enti in Italia un chiaro cambio di mentalità e di percezione nel passare a forme di "sourcing", ma sussiste ancora una certa riluttanza nell'uso del cloud, dovuta ai timori sulla sicurezza effettivamente erogata ed ultimamente anche alla rottura tra Unione Europea e Stati Uniti del precedente accordo sulla privacy, chiamato "Safe Harbour Privacy Principles" [25]. La non validità al momento di questo accordo rende la maggior parte dei servizi ICT in cloud (o terziarizzati) erogati da società statunitensi non più conformi alle norme europee, e quindi italiane, sulla privacy: se trattano dati personali, come nella maggior parte dei casi avviene, tali servizi sono al momento "illegali" , e quindi non più utilizzabili pena sanzioni anche penali. Vista la diffusione dei servizi in cloud erogati da società statunitensi, le autorità europee, incluse quelle italiane (dal Garante alla magistratura ed alla Polizia Postale), chiudono entrambi gli occhi e non procedono, nella speranza che venga definito un nuovo accordo[26] che risolva il non piccolo problema. Molte aziende italiane, soprattutto del settore manifatturiero e delle utility, ma anche PAL per il controllo del territorio e delle smart city, utilizzano sistemi di automazione, di robotica e componenti intelligenti ed interoperanti, chiamati Internet delle cose, conosciuti con l'acronimo IoT, Internet of Things. Sistemi e componenti tutti oggigiorno basati su, o con all'interno, tecnologie informatiche, e come tali attaccabili. Per la sicurezza informatica, soprattutto dopo gli attacchi STUXNET ai sistemi di controllo delle centrali nucleari iraniane[27], hanno assunto particolare rilievo i sistemi di controllo dei processi produttivi e di robotica, oltre che dell'IoT, i cui attacchi in Italia sono discussi in §4.5.3. Come mostrato nella fig. B-17, la maggior parte del campione, 76,5%, non ha e/o non usa questo tipo di sistemi. Per chi ne dispone, il 11,8% ha sistemi di automazione, controllo e/o robotica, il 7,6% ha specifici sistemi tipo SCADA ed il 5,9% usa sistema IoT. Quasi il 6% dei compilatori ha ammesso di non avere informazioni su tali sistemi. Talvolta nelle grandi aziende italiane i sistemi informatici di controllo della produzione (e/o di processi chimici, nucleari, dei magazzini, ecc.) sono considerati "impianti", sotto il controllo della produzione, nemmeno contabilizzati come sistemi informatici. In tali casi può capitare che il compilatore del questionario, nella maggior parte dei casi il CIO o un suo collaboratore nell'UOSI, non conosca neppure la loro esistenza. Come già indicato per i sistemi mobili, questa percentuale di "non so" è una conferma della correttezza e serietà dei rispondenti, che avvalora la credibilità delle risposte date, e di conseguenza dei dati del Rapporto.

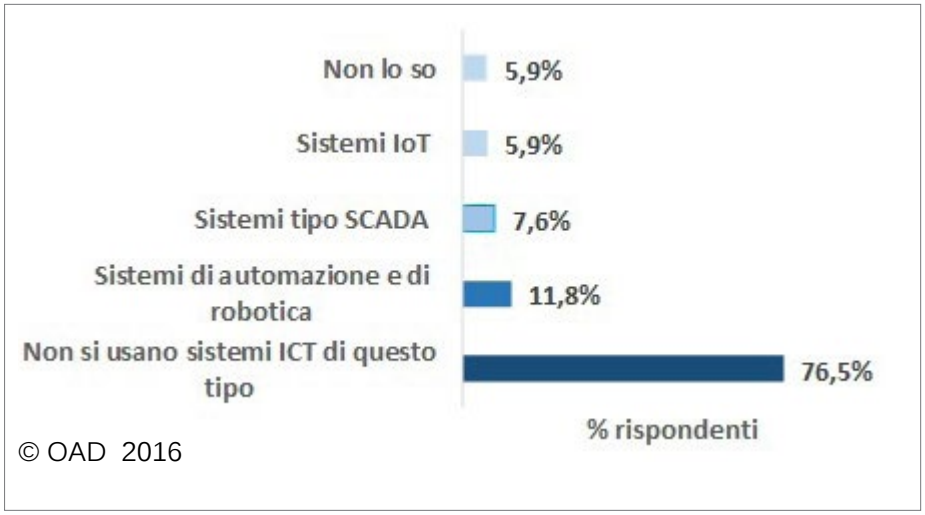
24 Si vedano i Rapporti annuali di Assinform ed Assintel, e quelli trimestrali di Sirmi. Per un inquadramento tecnico e di mercato per non tecnici si veda "Guida al cloud - Nella Nuvola la stella cometa per il Manager" dell'Autore, pubblicata da Soiel per Seeweb a novembre 2012, in gran parte ancora attuale e scaricabile da http://www.malaboadvisoring.it/

25 Si veda anche http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

26 https://www.fas.org/sgp/crs/misc/R44257.pdf

27 Per approfondimenti si vedano gli articoli dell'Autore "Attacchi ai sistemi di controllo industriale e alle infrastrutture" su Office Automation n. 11 novembre 2010, p. 88-89, scaricabile da http://www.malaboadvisoring.it/index.php?option=com_content&view=article&id=31&Itemid=50 e "DataGate" su Office Automation n. 12 dicembre 2013

Fig. B-17 Utilizzo di sistemi di automazione dei processi, di robotica, di IoT (risposte multiple)



C Allegato C
Profili Sponsor

C.1 AIPSI

AIPSI, Associazione Italiana Professionisti Sicurezza Informatica, è il capitolo italiano di ISSA®, l'organizzazione internazionale no-profit di professionisti ed esperti praticanti. Con l'attiva partecipazione dei singoli soci e dei relativi capitoli in tutto il mondo, AIPSI, in qualità di capitolo di ISSA, è parte della più grande associazione non-profit di professionisti della sicurezza che ne vanta oltre 10000 a livello mondiale. L'organizzazione di forum e di seminari di approfondimento e di trasferimento di conoscenze, la redazione di documenti e pubblicazioni, la formazione per le certificazioni europee ECF per la sicurezza informatica, oltre all'interazione fra i vari professionisti della sicurezza contribuiscono concretamente ad incrementare le competenze e la crescita professionale dei Soci, oltre che promuovere più in generale la cultura della sicurezza ICT e della sua gestione in Italia. L'appartenenza al contesto internazionale ISSA, permette ai soci AIPSI, di interagire con gli altri capitoli europei, americani e del resto del mondo. Il comitato direttivo di AIPSI e di ISSA International è costituito da rappresentanti influenti nell'ambito della sicurezza con rappresentanze che provengono da alcune delle principali aziende della domanda e dell'offerta e da consulenti con competenze anche in ambito legale. ISSA è focalizzata nel mantenere la sua posizione di "Global voice of Information Security".

Benefici per i Soci

- Ricevimento di ISSA Journal, la rivista mensile di ISSA.
- Accesso/ricevimento newsletter di ISSA e newsletter italiana di AIPSI.
- Partecipazione ai webinar ISSA.
- Trasferimento di conoscenza e formazione continua sulla sicurezza per l'aggiornamento e la crescita professionale dei Soci.
- Rappresentanza dei Soci professionisti dell'Information Security, nell'ambito delle recenti normative italiane stabilite dal D.Lgs. 4/2013 sulle professioni non regolamentate.
- Corsi per le certificazioni professionali per le competenze sulla sicurezza, in particolare per eCF.
- Networking con altri professionisti del settore.
- Possibilità di costituire gruppi di lavoro per ricerche e condivisione informazioni su tematiche d'interesse comune.
- Accesso e sconti a seminari, conferenze, training a carattere nazionale e internazionale.
- Pubblicazione di articoli e contenuti nel sito web AIPSI.
- Possibilità di redigere articoli per conto di AIPSI/ISSA.
- Pubblicazione e ricerca di curricula vitae per agevolare la domanda/offerta di competenze e di professionalità.
- Accesso al materiale riservato ai soci sul sito web ISSA.
- Visibilità nazionale ed internazionale grazie al riconoscimento di ISSA nel mondo.
- Possibilità di partecipare a seminari e conferenze come operatore per conto di AIPSI/ISSA.

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

C.2 F5

F5 Networks – chi siamo

F5 Networks offre soluzioni per il mondo applicativo, aiutando le organizzazioni a scalare con semplicità i deployment cloud, data center, di telecomunicazioni e il Software-defined networking (SDN), per offrire con successo applicazioni a chiunque, ovunque e in qualunque momento.
Le soluzioni F5 ampliano il raggio d'azione dell'IT attraverso un framework aperto ed estensibile e un ricco ecosistema di partner che include le aziende leader nella tecnologia e nell'orchestrazione.
Le più grandi organizzazioni, i service provider, le amministrazioni pubbliche si affidano a F5 per essere al passo con le tendenze in ambito cloud, security e mobility.

- **Sicurezza delle applicazioni:** F5 aiuta le organizzazioni a ridurre al minimo i rischi e salvaguardare le proprie reti, le applicazioni, le proprietà intellettuali e gli utenti dalle minacce alla sicurezza provenienti sia dall'esterno della rete, sia dagli utenti interni inconsapevoli e da quelli che operano da mobile utilizzando reti pubbliche non protette.
- **Abilitatore del Cloud:** Grazie al supporto delle piattaforme cloud di player come Amazon, VMware e Microsoft , F5 offre la flessibilità che consente alle aziende di adottare il modello d'infrastruttura che meglio risponde alle proprie esigenze.
- **Ottimizzazione delle prestazioni della rete e delle applicazioni:** Le applicazioni enterprise migliori risultano inutili se non sono disponibili, affidabili in grado di offrire le prestazioni che gli utenti si aspettano. F5 comprende la logica applicativa nella sua profondità e utilizza questa conoscenza per ottimizzare le prestazioni della rete e delle applicazioni.
- **Servizi applicativi:** Tutte le applicazioni hanno bisogno di servizi che ne garantiscano la sicurezza, le prestazioni e la disponibilità, ma spesso solo le applicazioni mission-critical ne sono fornite. Con F5 Software-Defined Application Services, non è più necessario scegliere quali applicazioni ottimizzare e proteggere ma è possibile fornire servizi essenziali a tutte le applicazioni ovunque esse risiedano.
- **Tecnologie abilitanti e supporto nel mondo**: Le soluzioni F5 includono una serie di tecnologie di supporto per la visibilità globale sulla rete e sulle applicazioni, la flessibilità e il controllo, che consentono di estendere le operazioni dal data center al cloud. Queste tecnologie consentono di distribuire anche a tempi da record le applicazioni aziendali dei principali vendor come IBM, Microsoft, Oracle e VMware, massimizzando il ROI. F5 è nota anche per i suoi servizi di supporto completi, con clienti che indicano come grado di soddisfazione "9 su 10". DevCentral, la comunità tecnica online di F5, conta 240.000 architetti di rete, professionisti della sicurezza, e sviluppatori di applicazioni che supportano i clienti con know-how tecnico necessario sul codice, nelle configurazioni e nelle discussioni tecniche, fornendo white paper, video e articoli a firma.

Per maggiori informazioni, visitate il sito www.f5.com

C.3 Gruppo Sernet

La missione del Gruppo Sernet (www.sernet.it) è assistere il Management aziendale nei processi critici che lo mettono in relazione con gli altri Stakeholders. Sernet Group presenta, tra gli oltre 350 clienti attivi, alcune tra le più prestigiose aziende italiane.
Le metodologie utilizzate fanno riferimento a best practices e standard internazionali. Settori economici dei clienti Sernet: Telco, Utilities, Media, Industrial Products, Consumer Products, Insurance, Banking, ICT Services, Chemicals, Pharmaceuticals, Contact Center, Food & Beverage, Hospitality, GDO, Public Sector.

Aree di business del Gruppo Sernet:

ICT Governance & Security

- Progetti di ICT Governance e ICT Risk Assessment, con adozione dei più accreditati standard internazionali (CobiT5, ISO 31010, ISO 27005, etc).
- Preparazione alla certificazione ISO 27001 (Sicurezza delle informazioni).
- Preparazione alla Certificazione ISO 20000 (IT Service Management).
- Progetti di Business Continuity, con adozione dello standard ISO 22301.
- Assessment e preparazione alla certificazione PCI-DSS.

Risk e Compliance

Valutazione e governo dei rischi aziendali, progetti per il controllo e mitigazione dei rischi di business, di continuitàoperativa e compliance (D.Lgs 231, Direttive ISVAP e Banca d'Italia, Privacy, Safety, etc).

Certified Management Systems & Corporate Social Responsibility (CSR)

- Sistemi certificati: Quality Management System-ISO 9001, Health and Safety-OHSAS 18001, Environment-ISO 14001, Social Accountability-SA 8000, Energy Management System-ISO 50001.
- CSR: Ethic Code, Sustainability, Environmental Balance Sheet, Intangible Assets, Green Compliance.
- Execution & Corporate Reorganization: progetti di riorganizzazione, reindustrializzazione e ricollocamento; miglioramento dei processi direzionali e operativi.
- Energy: progettazione e realizzazione di soluzioni per il risparmio energetico e l'utilizzo di fonti rinnovabili in campo industriale.
- Riqualificazione Energetica: riqualificazioni energetiche in campo residenziale e terziario, per Enti pubblici e privati, sostenibili dal punto di vista tecnico, economico, sociale, energetico ed ambientale.

Per maggiori informazioni: www.sernet.it

C.4 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 basate sui prodotti SIGNificant della Xyzmo, creando la SIGNificant Suite, totalmente in italiano, che consente l'uso della grafometria non solo per l'identificazione biometrica dei firmatari, ma anche per la gestione documentale dei documenti firmati e l'associazione della grafometria alla firma digitale per la totale validità legale del documento elettronico in Italia.

I componenti della suite includono il SIGNificant Server, il SIGNificant Server Web Signing Interface, il SIGNificant Client, il SIGNificant Biometric Server. Essi registrano la firma autografa di una persona registrando i parametri biometrici quali pressione, accelerazione, velocità, ritmo e movimenti in aria, e incorporano le firme nel documento elettronico. 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 portate di medie e piccole aziende/enti con un elevato numero di documenti firmati e/o con la necessità di una identificazione biometrica dei firmatari.

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

C.5 Trend Micro

Dal 1988, anno della sua fondazione, Trend Micro sviluppa soluzioni di sicurezza innovative che rendono il mondo sicuro affinché aziende e privati possano scambiarsi informazioni digitali.
La Società: Quotata alla Borsa di Tokyo, ha attualmente 5.137 dipendenti e sedi in tutto il mondo, di cui due in Italia a Milano e Roma. Trend Micro è il maggior fornitore di protezione indipendente, riconosciuto dagli analisti del settore per essere leader nel mercato della sicurezza per i server, della sicurezza della virtualizzazione e della protezione dei contenuti per piccole imprese.
Management: Eva Chen, CEO e Co-fondatore, Mahendra Negi, COO&CFO, Steve Chang, Presidente e Fondatore.
Proteggiamo il viaggio verso il Cloud: Con oltre 26 anni di esperienza, Trend Micro è leader nel mercato della sicurezza server grazie a soluzioni di protezione dati client, server e cloud base di massima qualità che bloccano le minacce più velocemente e proteggono i dati in ambienti fisici, virtualizzati e cloud. La capacità di fornire protezione "dal cloud", con la tecnologia leader di settore Trend MicroTM Smart Protection Network™, e sicurezza "per il cloud", con le tecnologie di server, data storage e criptazione, rende Trend Micro la scelta ideale per proteggere il viaggio del sistema informativo verso il Cloud.
Focalizzazione sulle esigenze dei Clienti: Trend Micro mette al centro le specifiche necessità dei clienti con una vasta gamma di soluzioni e servizi cloud-based che garantiscono massima sicurezza, flessibilità e prestazioni con la minima complessità. Trend Micro ha un'ampia selezione di software, appliance gateway virtuali e offerte SaaS per utenti domestici, piccole imprese e aziende. Trend Micro rende sicuri i dati critici dall'endpoint al cloud grazie a sistemi di protezione dati completi, come la data loss prevention, la criptazione, il back up e il ripristino file.
Protezione personalizzata: Trend Micro attraverso una strategia di Custom Defense progetta su misura soluzioni per ogni azienda e offre i prodotti di maggior avanguardia per la protezione della sicurezza in ogni campo, dal mobile agli apparecchi virtuali, ai router, alle soluzioni integrate di terze parti, oltre ai server fisici, virtuali o cloud. Le partnership con leader come VMware, IBM, Dell e Microsoft garantiscono l'integrazione in Trend Micro di soluzioni aggiuntive, per ottenere il massimo dagli investimenti nella sicurezza informatica.
Smart Protection Network: Trend MicroTM Smart Protection Network™ consente di bloccare le minacce "in the cloud", garantendo una protezione proattiva più veloce di qualsiasi altro fornitore e nel 2014 ha neutralizzato 65 miliardi di minacce.
Intelligence e assistenza globali: Attraverso i TrendLabs, con oltre 1.200 esperti Trend Micro offre intelligence puntuale contro le minacce, assistenza e supporto ai clienti.

Per ulteriori informazioni: www.trendmicro.it

D Allegato D Riferimenti e fonti

D.1 Dall'OCI all'OAI: un po' di storia ... e di attualità

- FTI: "La sicurezza nei sistemi informativi – Una guida per l'utente", 1995, Pellicani Editore.
- 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.
- E. Molteni, F. Faenzi: "La sicurezza dei sistemi informativi: teoria e pratica a confronto", 2003, Mondadori informatica
- M. R. A. Bozzetti, R. Massotti, P. Pozzi (a cura di): "Crimine virtuale, minaccia reale", 2004, Franco Angeli
- E. Molteni, R. Ferraris: " Qualcuno ci spia - spyware nel tuo PC", 2005, Hoepli Editore
- 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.
- S. Zanero. "Wireless Malware Propagation: A Reality Check". IEEE Security and Privacy, vol. 7, no. 5, pp. 70-74, September/October, 2009.
- 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
- M. R. A. Bozzetti: Rubrica mensile OAI nella rivista Office Automation, l'archivio degli articoli è scaricabile da http://www.malaboadvisoring.it/index.php?option=com_content&view=article&id=31&Itemid=50
- M. Carminati, R. Caron, I. Epifani, F. Maggi, S. Zanero. "BankSealer: A Decision Support System for Online Banking Fraud Analysis and Investigation". Computers & Security, Elsevier, Vol. 53, pp. 175-186, 2015.

D.2 Le principali fonti sugli attacchi e sulle vulnerabilità

L' elenco non ha alcuna pretesa di essere esaustivo e completo.

- ABILAB - Centrale d'allarme per attacchi informatici: www.abilab.it per l'ambito bancario, accessibile solo agli iscritti;
- CERT-CC, Computer Emergency Response Team - Coordination Centre: http://www.cert.org/certcc.html fornisce uno dei più completi ed aggiornati sistemi di segnalazioni d'allarme, rapporti sulle vulnerabilità; a livello US cura la banca dati sulle i
- CIS-Sapienza: "Cyber Security Report 2015", http://www.cybersecurityframework.it/
- Clusit (www.clusit.it): "Rapporto annuale sulla sicurezza ICT in Italia", interessanti considerazioni sull' elaborazione di dati provenienti da ricerche di terzi (Fastweb) e da altri rapporti
- ENISA, European Union Agency for Network and Information Security: http://www.enisa.europa.eu/
- First, Forum for Incident Response and Security Team: http://www.first.org/ fornisce in particolare il CVSS, Common Vulnerability Scoring System;
- GARR-Cert: www.cert.garr.it fornisce i principali security alert per gli aderenti al Garr, la rete telematica tra Università italiane;
- 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): http://www.ic3.gov/default.aspx fornisce, oltre alla possibilità di denunciare negli US attacchi Informatici, informazioni sugli attacchi stessi e sui trend in atto per i crimini informatici;
- Polizia Postale e Commissariato Pubblica Sicurezza online: per il sito della Polizia Postale si veda http://www.poliziadistato.it/articolo/23393/, per il Commissariato Pubblica Sicurezza online http://www.commissariatodips.it/, utile anche per le denunce on line su reati informatici;
- SANS Institute (www.sans.org): fornisce sistematicamente segnalazioni su vari tipi di attacco e di vulnerabilità;
- Security Intelligence della Trend-Micro http://us.trendmicro.com/us/trendwatch/current-threat-activity/index.html fornisce segnalazioni e trend sugli attacchi; interessante l'"enciclopedia" degli attacchi in http://about-threats.trendmicro.com/us/threatencyclopedia#malware
- Total Defense: http://www.totaldefense.com/global-security-advisor.aspx fornisce avvisi su vulnerabilità e malware;
- Micro Trend: "Threat Reports and Security Predictions", http://www.trendmicro.com/us/security-intelligence/research-and-analysis/threat-reports/;
- World Economic Forum: annuale "Global Risk", che include anche considerazioni sui rischi informatici e di cyberwar; http://www.weforum.org/issues/global-risks.

E Allegato E
Glossario dei principali termini ed acronimi sugli attacchi informatici

- **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.
- **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.

- **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
- **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-scivere 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
- **Churn rate:** tasso di abbandono a favore della concorrenza, tipicamente dopo un attacco
- **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
- **Darknet:** sistema usato in Internet per monitorare la rete e possibili attaccanti, con funzionalità simili a quelle di un honeypot.
- **Data Braech:** 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.
- **Deadlock:** un caso particolare di "race condition", consiste nella con-

dizione 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 mylti-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.
- **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:** vedi bots
- **Exploit:** attacco ad una risorsa informatica basandosi su una sua vulnerabilità
- **Ethical hacking:** attività di provare attacchi ai fini di scoprire bachi e vulnerabilità dei programmi, e porvi rimedio con opportune patch/fix.
- **Fix:** correzione di un programma software, usato spesso come sinonimo di patch
- **Flash threats:** tipi di virus in grado di diffondersi molto velocemente
- **FTPS, File Transfer Protocol Secure:** per il trasferimento di file crittati
- **Hijacking:** tipico attacco in rete "dell□uomo in mezzo" tra due interlocutori, che si maschera per uno dei due e prende il controllo della comunicazione. In ambito web, questo termine è usato per indicare un attacco ove: le richieste di pagine a un web vengo dirottate su un web falso (via DNS), sono intercettati validi account di e-mail e poi attaccati questi ultimi (flooding)
- **Hoax:** in italiano bufala o burla, indica la segnalazione di falsi virus; rientra tra le tecniche di social engineering.
- **Honeynet:** 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.
- **IaaS, Infrastructure as a Service.**
- **Information Leakage:** diffusione-dispersione non autorizzata di informazioni.
- **IoT, Internet of Things:** Internet delle Cose.
- **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.
- **Malicious insider:** attaccante interno all'organizzazione cui viene portato l'attacco.
- **Malvertising, "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.
- **OTP, One Time Password:** dispositivo che genera password da usarsi una sola volta per sessione/transazione.
- **PaaS, Platform as a Service**
- **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 riser-

vate 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.
- **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:** programme 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.
- **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.
- **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.**
- **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.
- **SCC,** Security Command Centre.
- **Scareware**: software d'attacco che finge di prevenire falsi allarmi, e diffonde notizie su falsi malware o attacch**i.**
- **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
- **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.
- **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 i 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.
- **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.
- **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 injection:** tecnica di inserimento di codice in un programma che sfrutta delle vulnerabilità sul database con interfaccia SQL che viene usata dall□applicazione.
- **SSO,** Single Sign On: autenticazione unica per avere accesso a diversi sistemi e programmi.
- **Stealth:** registrazione invisibile
- **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.
- T**rojan 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
- **VPN,Virtual Private Network:** rete virtuale creata tramite Internet per realizzare una rete "private" e sicura per i soli utenti abilitati di un'azienda/ente.
- **XSS, Cross - site scripting:** una vulnerabilità di un sito web che consente di inserire a livello "client" dei codici maligni via "script", ad esem-

pio 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 attach:** attacchi basati su vulnerabilità a cui non è ancora stato trovato rimedio
- **Zombies:** vedi bots.

F Allegato F Profilo dell'Autore

Marco Rodolfo Alessandro Bozzetti, ingegnere elettronico laureato al Politecnico di Milano, è amministratore unico di Malabo Srl, società di consulenza e servizi sull'ICT ed ideatore e curatore di OAD, Osservatorio Attacchi Digitali in Italia. Attraverso la sua società Marco conduce interventi consulenziali lato sia domanda sia offerta ICT ed offre alcuni servizi on line a supporto dei suoi interventi consulenziali. I suoi campi di intervento includono la governance ICT, la sicurezza informatica, il disegno di architetture ICT, la razionalizzazione e la gestione del sistema informativo, la definizione di strategie ICT, l'assessment delle tecnologie, delle competenze e dei ruoli ICT, l'innovazione tramite l'ICT, la riorganizzazione di strutture e processi, il supporto alla compliance alle varie normative, dalla privacy alla safety.
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 a livello "corporate" dell'intero Gruppo ENI.
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, nel Consiglio Direttivo di FIDAInform, socio fondatore e componente del Comitato Scientifico dell'FTI, socio del ClubTI di Milano, di AIPSI. È certificato ITIL v3 ed EUCIP Professional Certificate "Security Adviser".
E' "assessor" e commissario d'esame per le certificazioni eCF.
Ha pubblicato articoli e libri sull'evoluzione tecnologica, la sicurezza, gli scenari e gli impatti dell'ICT.

G Allegato G Malabo Srl

Malabo Srl opera nell'ambito della consulenza e dell'erogazione di servizi ICT, basandosi su una rete consolidata di esperti "senior" e di società ultra specializzate, per clienti lato sia offerta sia domanda ICT.
Malabo dispone di un piccolo laboratorio sperimentale costituito da due server dual Xeon quad core con VMWare ESXi con storage condiviso sui quali installare e testare qualsiasi tipo di sistema operativo e/o applicativo.

La consulenza

Lato domanda l'intervento principale è di aiutare il cliente nell'uso efficace ed efficiente dell'ICT in modo da creare per lui un effettivo e misurabile valore; lo stesso obiettivo si applica per le aziende dell'offerta ICT, per le quali gli interventi spaziano da quelli per il miglior uso dell'ICT, a quelli più strategici per una reale crescita, per incrementare immagine e guadagni, per meglio posizionarsi sul mercato italiano e internazionale. Gli interventi sui sistemi informatici includono la loro razionalizzazione, la riduzione dei costi, la gestione operativa, la definizione e gestione dell' ICT Enterprise Architecture anche con terziarizzazioni e cloud, l'ICT governance, la sicurezza diitale, l'analisi e la gestione dei rischi. A livello organizzativo gli interventi includono l'assessment delle competenze e dei ruoli del personale ICT con riferimento agli standard europei EUCIP/eCF ed all'italiano UNI 11506, la riorganizzazione dei processi ICT con intelligente e contestuale riferimento a ITIL e a COBIT, l'effettivo allineamento tra sistema informatico e business, la gestione delle compliance e delle certificazioni.

I servizi

I servizi che Malabo eroga on line via web includono:

- SLA Watch: è un insieme di servizi "pay per use" per il monitoraggio da remoto delle funzionalità e delle prestazioni di ogni risorsa ICT indirizzabile via Internet di un sistema informatico.
- ICT Inventory: individua automaticamente tutte le risorse fisiche e logiche ICT, con i loro componenti, di un sistema informativo, creando una banca dati centralizzata.
- ICT TT, Trouble Ticketing system: consente la centralizzazione di tutte le segnalazioni e le richieste degli utenti, tracciando puntualmente il

loro ciclo di vita e rendendolo visibile a ciascun utente.

- GOSI, Gestione Operativa Sistema Informatico: integra i servizi sopra elencati viene supportata anche da interventi in loco, con una contestuale applicazione delle buone pratiche ITIL e COBIT.
- Sistema analisi e gestione rischi ICT: disponibile anche in cloud, è basato sui più consolidati standard e best practice (ISO 27001-2-5, NIST 800, Octave Allegro)
- Kit autovalutazione del ritorno economico e dell'analisi del valore di un sistema informatico: può essere usato sia a livello di sistemi o di parti di sistemi già in produzione (post) sia a livello di analisi di fattibilità (ante).
- Kit per la stesura guidata del DPS, Documento Programmatico Sicurezza (normativa privacy) e del DVR, Documento Valutazione Rischi (normativa sicurezza sul lavoro).

Per maggiori informazioni: www.malaboadvisoring.it

H Allegato H
NEXTVALUE Srl

I nostri Clienti sono i principali operatori dell'Information Technology, dei Digital Media e Investitori che operano in modo focalizzato in questi mercati. Essi ci riconoscono il valore aggiunto di saper approfondire ed interpretare la strategia e l'esperienza delle loro imprese nel difficile percorso di trasformazione digitale e di mettere a loro disposizione programmi, insight, contenuti e risorse online per affrontare il cammino con successo.
La nostra missione è di condividere i loro obiettivi di business, di creare per loro una migliore customer experience, di creare opportunità in un contesto di engagement con i decisori dei loro clienti e di progressiva formazione di relazioni di fiducia con essi. Il nostro asset più importante sono le esclusive community di CIO (CIONET Italia è la più importante business community internazionale di Chief Information Officer di aziende Top e Grandi), Direttori IT, CISO e CSO, Head of Digital e Head of eCommerce dei maggiori spender. E' un asset con un ROI molto alto, che remunera l'elevata reputazione e credibilità di programmi quali gli INSIGHTS, i Digital Waves, i WORKSHOP, il Companies to Watch. Tutti i nostri servizi si basano sul processo di crowdsourcing a cui partecipano i membri delle business community e che non produrrebbe risultato se alla base non ci fossero riconosciuti la comprovata indipendenza di giudizio, l'esperienza e la competenza necessaria sui temi dell'innovazione, la capacità di fare, la rigorosa trasparenza, l'elevato standard qualitativo e la piena adesione ai valori etici, ovvero gli elementi distintivi della nostra cultura d'impresa.

Per maggiori informazioni: www.nextvalue.it

I Allegato I Note

1- AIPSI, Associazione Italiana Professionisti Sicurezza Informatica, (http://www.aipsi.org/) capitolo italiano della mondiale ISSA (https://www.issa.org/)
2 - ICT, Information and Communication Technology
3 - I precedenti Rapporti OAI sono scaricabili dal sito web dell'Autore, www.malaboadvisoring.it, dal sito di AIPSI, www.aipsi.org, e dai siti di alcuni Sponsor e Patrocinatori.
4 - Per i Rapporti OCI del 1997, 2000 e 2004, pubblicati da Franco Angeli, si veda http://www.forumti.it/
5 - Non è possibile individuare se i rispondenti, in caso di attacco con Crypto Locker o simili, hanno selezionato la risposta nel questionario di malware, di ricatti o di entrambi.
6 - Per approfondimenti si rimanda alla vasta documentazione disponibile in Internet; a cura dell'autore alcuni articoli su APT e TA pubblicati nella Rubrica OAI su Office Automation, scaricabili da http://www.malaboadvisoring.it/index.php?option=com_content&view=article&id=31&Itemid=50
7 - Si veda "Ponemon Institute: 2016 Cost of Data Breach Study: Italy" di Giugno 2016 e relativo ad attacchi rilevati nel 2015
8 - DLP, Data Loss Prevention
9 - 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)
10 - Si veda http://www.poliziadistato.it/articolo/30630/, https://www.gcsec.org/it/activities/online-fraud-cyber-centre-experts-network-of2cen
11 - Si veda http://www.poliziadistato.it/articolo/30663,
12 - https://www.commissariatodips.it/vita-da-social.html
13 - Come esempio, si rammenta che alla data della stesura del presente Rapporto OAD 2016 l'accordo tra Europa e Stati Uniti sulla privacy, chiamato "harbour", non è più valido, e pertanto dati personali e sensibili non possono essere trattati in cloud con sedi all'infuori dell'Unione Europea e/o che non seguono le norme europee sulla privacy.
14 - https://www.gartner.com/doc/3277832/forecast-iot-security-worldwide-
15 - DCS, Distributed Control System
16 - PLC, Programmable Logic Controller

17 - https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project
18 - https://www.enisa.europa.eu/publications/etl2015/at.../fullReport
19 - Con questo termine si indicano i locali nei quali vengono concentrate le risorse informatiche di un ufficio periferico o di una piccola azienda/ente.
20 - ISO 20000 standardizza logiche e processi di ITIL
21 - Per approfondimenti e confronti tra questi standard e best practice si rimanda al già citato libro di M.R.A. Bozzetti e F. Zambon "Sicurezza Digitale" edito da Soiel International e pubblicato a giugno 2013, ISBN 978 88 908901 0 9.
22 - www.ecompetences.eu/it/
23 - Il termine UOSI è usato per non connotare il livello gerarchico di questa struttura. Nella realtà italiana sono ancora pochi i casi in cui l'UOSI è una Direzione di primo livello, il cui CIO fa parte del "board". Anche in grandi e grandissime organizzazioni l'UOSI si posiziona a livelli più bassi, e può dipendere dalla Direzione Risorse Umane, dalla Direzione Amministrativa, dalla Direzione Strategie, e così via.

PATROCINATORI

AICA

aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

ASSINTEL
ASSOCIAZIONE NAZIONALE IMPRESE ICT

ASSOLOMBARDA
Confindustria Milano Monza e Brianza

AIEA
Associazione Utilizzatori Sistemi E tecnologie Dell'informazione

CDI
Club Dirigenti di Informatica

CDTI

ti Liguria

CTI er Club

ti

ClubTI
Club per le tecnologie dell'informazione

FIDA
INFORM

FTI
FORUM per la TECNOLOGIA della INFORMAZIONE

IEEE computer society
Italy Chapter

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

itSMF
ITALIA