Sponsor

AICA

aipsi

BUSINESSe
BE your Security Company

hp

Riesko
Manage your risks

sernet GROUP

Technology Estate

TREND MICRO

Rapporto 2015 OAI

a cura di
Marco R.A. Bozzetti

Osservatorio Attacchi Informatici in Italia

oai

Autorizz. - Trib. Milano n. 432 del 22/11/1980
iscritta al registro degli Operatori di Comunicazione n. 2111

Soiel International
Via Martiri Oscuri, 3 - 20125 Milano
soiel@soiel.it - www.soiel.it

Rapporto
2015 OAI

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 OAI di questa edizione.
Un grazie particolare agli Sponsor, all'editore Soiel International, alla Sirmi con il dott. Cuzari, al Comitato Scientifico OAI, al dott. Francesco Zambon, all'ing. Maurizio Mapelli di AIPSI, ai dott. Antonio Apruzzese e Salvatore La Barbera della Polizia Postale, che hanno contribuito in vario modo alla realizzazione del presente rapporto.

INDICE

1. EXECUTIVE SUMMARY

Il presente Rapporto 2015 OAI, giunto alla quinta edizione, fornisce l'analisi degli attacchi intenzionali ai sistemi informatici di organizzazioni di ogni dimensione e settore merceologico, incluse le Pubbliche Amministrazioni centrali e locali, rilevati nel 2013 e nel 2014. L'analisi si basa sull'elaborazione delle risposte avute dal Questionario 2014 via web nel periodo gennaio-marzo 2015, per un totale di 424 rispondenti. Essendo volontarie le risposte al questionario, il campione emerso non ha stretta 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, basilari anche per la sensibilizzazione sulla sicurezza informatica oltre che come riferimento per l'analisi dei rischi. Inoltre il Rapporto analizza quali sono gli strumenti di prevenzione, protezione e ripristino per contrastare tali attacchi, e come le aziende/enti reagiscono in caso di attacco. Innumerevoli le considerazioni che possono emergere dai dati raccolti, nel seguito si sintetizzano alcuni degli aspetti più significativi, sia allineati con i più recenti rapporti internazionali, sia specifici della realtà italiana.

Il bacino di 424 rispondenti risulta costituito da aziende di servizi (terziario) ed industriali (secondario), si veda fig. A.2, i cui sistemi informatici si collocano mediamente nella fascia medio alta in termini sia di governance ICT sia di strumenti di sicurezza ICT in uso. I trend sugli attacchi emersi con il campione di rispondenti sono sostanzialmente in linea con i quelli internazionali, a parte alcune specificità tipicamente nazionali nel seguito evidenziate.

A livello generale i macro-trend emersi dall'indagine includono i seguenti principali aspetti.

- Gli attacchi nel 2014 sono aumentati sia come numero sia come sofisticazione, ed i più diffusi permangono il "malware", il "social engineering", la saturazione delle risorse (DoS e DDoS) ed il furto dei dispositivi ICT, in particolare di quelli mobili tipo "smartphone" e "tablet" (fig. 4-5); tali risultati sono congruenti coi dati forniti dal Cnaipic-Polizia Postale (Tabella 4).
- Le quattro tipologie di attacchi di cui sopra sono posizionate ai primi quattro posti per diffusione in tutte le indagini OAI (fig. 4-6).
- Tutte le tipologie di attacco considerate (Tabella 1) nel 2014 hanno avuto un incremento di diffusione rispetto al 2013 (Tabella 3), tranne il furto di dispositivi ICT, che comunque rimane un attacco tra i più diffusi in Italia. Il più forte incremento riguarda gli attacchi basati sul ricatto informatico, che può sfruttare codici maligni tipo ransomware, oltre che i sofisticati TA/APT, Targeted Attack/Advanced Persistent Threat.
- Alla base di ogni attacco c'è lo sfruttamento di una o più vulnerabilità tecnica, organizzativa e delle persone, siano essi utenti finali o operatori dei sistemi informatici; le criticità maggiori derivano da problemi organizzativi o delle persone che con le loro azioni, o non azioni, consentono l'attuazione dell'attacco; nella maggior parte dei casi di attacchi riusciti il punto più debole nella catena della sicurezza è rappresentato dall'utente finale.
- Con l'evoluzione tecnologica crescono nuove vulnerabilità tecniche, ad esempio con la virtualizzazione, con il cloud, e con i nuovi sempre più potenti dispositivi mobili. Le vulnerabilità talvolta non sono scoperte e risolte in breve dai fornitori, e rimangono così sfruttabili dagli attaccanti anche per tempi lunghi. Gli aggiornamenti disponibili per ovviare alle vulnerabilità software, le così dette "patch", non sempre vengono tempestivamente installati; 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 dal perdurare della crisi economica.
- Lo sfruttamento delle vulnerabilità tecniche avviene prevalentemente negli ambiti web.
- La vulnerabilità delle persone si basa in primis sulla loro disponibilità e buona fede, 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. Essi facilitano la possibilità di rubare le identità digitali degli utenti ed acquisire informazioni riservate con le quali svolgere attacchi e compiere frodi informatiche. Nel 2014 il fenomeno del furto dell'identità digitale è stato così significativo

da far definire da molti rapporti internazionali il 2014 come l'anno dei "data breach".

A livello più specificatamente italiano, e con riferimento al campione emerso dall'indagine, si evidenzia che:

- il 44,7% del campione ha rilevato attacchi nel 2014, contro un 37,5% nel 2013, con un incremento del 7,2% (fig. 4-1); solo come tendenza indicativa, dati i bacini di rispondenti diversi nelle precedenti indagini OAI, il valore del 2014 risulta il più alto dopo quello del 2008 (fig. 4-2);
- il numero di attacchi e la loro frequenza aumenta prevalentemente per dimensione dell'organizzazione: più le aziende/enti sono grandi e note a livello internazionale, più sono un target appetibile per il cyber crime;
- alcuni o molti attacchi possono non essere stati rilevati dalle aziende/enti, ma i relativamente pochi attacchi in Italia dipendono, a giudizio dell'autore, anche dalla prevalenza in Italia di piccole e piccolissime aziende (Tabella A-1), che non possono essere un primario obiettivo per gli attaccanti;
- l'impatto degli attacchi risulta grave solo in un limitato numero di casi (fig. 4-7); gli attacchi che nel 2014 hanno avuto il maggior e più grave impatto sono stati gli attacchi alla sicurezza fisica, gli accessi non autorizzati ai sistemi ICT ed alle loro applicazioni, gli attacchi alle reti, i TA/APT (fig. 4-8);
- la non gravità della maggior parte degli attacchi subiti è confermata dai veloci tempi di ripristino: il 68,4% dei casi è ripristinato in giornata, e solo il 4,1% dei casi è ripristinato entro un mese (fig. 5-5 e 5-6);
- indipendentemente dalle dimensioni e dal settore merceologico di appartenenza, la maggior parte dei sistemi informatici è tecnicamente aggiornata (fig. A-11), ed una significativa parte del campione dispone di architetture ad alta affidabilità (fig. A-6);
- nonostante la non disponibilità di banda larga in alcune zone d'Italia, quasi i 2/3 dei rispondenti terziarizzano parte o tutto il proprio sistema informatico e/o la sua gestione (fig. A-13); poco meno della metà utilizza soluzioni in cloud (fig. A-14);
- tutti i rispondenti hanno connessioni ad Internet, ed il 63,6% utilizza VPN;
- la consumerizzazione (BYOD) pone problemi per la sicurezza informatica ed il 23,4% dei rispondenti non la consente (fig. A-10);
- le misure di sicurezza e gli strumenti per la sua gestione nel campione dei rispondenti sono più tecniche che organizzative, è più basate su una logica di reazione che di prevenzione;
- le misure tecniche di sicurezza, da quelle fisiche a quelle per la protezione dei dati (da fig. 6-1 a fig. 6-7), sono abbastanza diffuse come strumenti di base e circa 1/3 dei rispondenti utilizza strumenti di livello medio-alto. Le debolezze maggiori emerse riguardano la verifica del codice sicuro per il software messo in produzione, il log degli operatori, le prove dei piani di Disaster Recovery, la protezione delle informazioni;
- sul piano organizzativo della sicurezza informatica, per una buona o comunque non trascurabile percentuale del campione, le aziende/enti sono in media "meno avanzate" che sul piano tecnico;
- aspetti positivi:
  - quasi il 70% dei rispondenti ha definito, pubblicato e gestisce le "policy" sulla sicurezza e le relative procedure organizzative, di riferimento anche per i suoi fornitori, e per il 15% sono in corso di definizione (fig. 6-11);
  - l'auditing informatico viene svolto dal 52% dei rispondenti (fig. 6-22) ed il 56,7% di questi lo effettua in modalità periodica e regolare (fig. 6-24);
- aspetti critici:
  - un ruolo specifico di CISO è definito ed attuato solo dal 38,7% dei rispondenti;
  - l'analisi del rischio informatico è effettuata da circa ¼ dei rispondenti (fig. 6-8) ed è ancor meno diffusa l'assicurazione del rischio residuo con il 19,1% (fig. 6-9);
  - il 43,1% dei rispondenti effettua una analisi del danno subito (fig. 4-9) in seguito ad un attacco, ma è ancora embrionale, o limitata a poche aziende/enti, la sua stima economica;
  - non ancora diffusa la definita e chiara separazione delle responsabilità tra i vari attori della sicurezza ICT, approccio seguito dal 35,3% dei rispondenti (fig. 6-10);
  - gestione degli incidenti e dei problemi gestita dal 31,8%, ed uso dell'help/service desk da parte del 31,2% dei rispondenti (fig. 6-10);
  - uso limitato di best practice quali ITIL e COBIT o standard quali la famiglia ISO 27000 (da fig. 6-13

a fig. 6-19), ed ancor più limitata la loro certificazione a livello aziendale/ente o personale; assai limitata, per lo più alle grandi organizzazioni, la richiesta ai fornitori di seguire almeno sostanzialmente tali best practice e standard o di avere le relative certificazioni;
- limitata richiesta di certificazioni inerenti la sicurezza informatica sia per il personale interno (fig.6-20) sia per il personale dei fornitori (6-21).

Per concludere, il 2014 sarà probabilmente ricordato, a livello mondiale, come l'anno dei data breach, ossia delle violazioni dei dati: tipicamente furti di dati e di identità digitali.
Il 2014 ha confermato che gli attacchi informatici impattano talvolta gravemente sia le aziende/enti che li hanno subiti sia i singoli individui che, direttamente o non, ne sono stati coinvolti: gli impatti hanno riguardato, e riguarderanno soprattutto perdite finanziarie e di reputazione. Le infrastrutture critiche ICT potranno poi essere attaccate per terrorismo. L'Italia fino ad ora non è stata al centro del cyber crime e della cyber war, ma corre un crescente rischio di esserlo nel prossimo futuro.

1EN. EXECUTIVE SUMMARY IN ENGLISH

The present Report 2015 OAI (annual Observatory on Informatics Attacks in Italy), now in its fifth edition, provides an analysis of intentional attacks against informatics systems for organizations of every size and industry sector, including central and local public administrations, detected in 2013 and 2014. The analysis is based on the responses received via web from the questionnaire 2014 in January-March 2015, with a total of 424 respondents. Since the web survey is not based on a specific sample of respondents, the resulting data can not have statistical significance. Given the number of responses and their good distribution in terms of size and industry sector, OAI 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 analyzes what are the tools of prevention, protection and recovery to counteract such attacks, and how companies react in case of attack. Several considerations may emerge from the data collected, in the following we summarize some of the most significant.

The macro-trends that emerged from the survey are listed in the following.

- The attacks in 2014 increased both in number and sophistication; the most common are "malware", "social engineering", saturation of resources (DoS and DDoS) and theft of ICT devices, particularly the mobile one such as "smartphone" and "tablet" (fig. 4-5); these results are consistent with the data provided by CNAIPIC-Postal Police (Table 4).
- These most common attacks are always in the top four for dissemination in all OAI reports (Fig. 4-6).
- All the types of attack considered in 2014 (Table 1) had an increase of diffusion compared to 2013 (Table 3), except for the theft of ICT devices, which still remains an attack among the most popular in Italy. The largest increase is for the blackmail attacks, which can exploit ransomware, and for the sophisticated TA / APT, Targeted Attack / Advanced Persistent Threat.
- 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 most critical result from organizational problems or persons who by their actions, or no action, allowing the implementation of the attack; in most cases of successful attacks the weakest point in the safety chain is represented by the end user.
- With the technological evolution grow new technical vulnerabilities, for example, with virtualization, the cloud, and with the new more powerful mobile devices. The vulnerabilities are sometimes not discovered and resolved in short from suppliers, and remain so exploitable by attackers for long times. Even with updates to address the vulnerability software, the so-called "patch", these are not always promptly installed; the causes may be different, but most often are organizational: in particular the lack of knowledge of the availability of patches and updates, the lack of procedures for software testing, the non-renewal of contracts for software maintenance, perhaps caused by the continuing economical crisis.
- The exploitation of technical vulnerabilities occurs mainly with web sites and their platforms.
- The vulnerability of people, is based primarily on their availability and good faith to help, on their naivety or carelessness, on the lack of knowledge on how to

use ICT tools in a secure way, on the lack of sensitivity and attention to computer security. Amplifiers and facilitators of personal vulnerability are social networks, e-mail, search engines, the more capable USB sticks, collaborative tools. They facilitate the ability to steal the digital identities and to acquire confidential information with which to carry out attacks and make computer fraud. In 2014, the phenomenon of the theft of digital identity has been so significant to define 2014 as the year of "data breach."

Some aspects of the OAI survey are more specifically Italian, and include:

- 44.7% of the sample has detected attacks in 2014, compared to 37.5% in 2013, with an increase of 7.2% (Fig. 4-1); only as indicative trend, given the different basins of respondents in previous OAI surveys, the value of 2014 is the highest since 2008 (Fig. 4-2);
- the number of attacks and their frequency increases mainly for size of the organization: more organizations are big and internationally known, more they are an attractive target for cyber crime;
- some attacks can not be detected, but the reason of the relatively few attacks in Italy depends, in the opinion of the author, mainly by the prevalence in Italy of small and very small companies (Table A-1), which can not be a primary target for attackers;
- the impact of the attack is severe only in a limited number of cases (fig. 4-7); attacks which in 2014 had the largest and most severe impacts were attacks on physical security, unauthorized access to ICT systems and their applications, network attacks, the TA / APT (fig. 4-8);
- the non-seriousness of most of the attacks is confirmed by the fast recovery time: 68.4% of the cases is restored in the day, and only 4.1% of cases within one month (Fig. 5-5 and 5-6);
- regardless of the size and the product sector of the respondents, the majority of computer systems is technically updated (Fig. A-11), and a significant part of the sample has informatics architectures with high reliability (Fig. A-6);
- despite the non-availability of broadband in some parts of Italy, especially outside the big cities, almost 2/3 of respondents outsources part or all of its informatics system and its management (fig. A-13); slightly less than half uses solutions in the cloud (Fig. A-14);
- all respondents have Internet connections, and 63.6% use VPN;
- consumerization (BYOD) poses problems for computer security and 23.4% of the sample did not allow (fig. A-10);
- security measures and ICT governance are more technical than organizational, and they are based more on a reaction approach than a prevention one;
- the technical security measures, from the physical security to the data protection (from Fig. 6-1 to Fig. 6-7), are fairly common as basic tools and about one third of the respondents are using solutions of medium-high level. The major weaknesses emerged concerns the verification of secure code, the log of the operators, the periodic test of the disaster recovery plans, the protection of information;
- for a large or not negligible percentage of the sample, the organizational security is "less advanced" than the technical one;
- positive issues:
  - nearly 70% of respondents defined, published and manages the ICT security "policy" and related organizational procedures; and 15% is developing a security policy (fig. 6-11) ;
  - ICT auditing is carried by 52% of respondents (Fig. 6-22) and 56.7% of those carried out in a periodic way (fig. 6-24);
- critical issues:
  - a specific CISO role is defined and implemented only by 38.7% of respondents;
  - ICT risk analysis carried out by about ¼ of respondents (Fig. 6-8), and even less widespread insurance risk with the remaining 19.1% (Fig. 6-9);
  - 43.1% of respondents carry out an analysis of the damage (Fig. 4-9) after an attack, but it is still embryonic, or limited to a few large companies its economic estimate;
  - A clear separation of duties among the various actors of ICT security is not yet widespread, and this approach is followed by 35.3% of respondents (fig. 6-10);
  - incidents and problems management are carried out by 31.8%, and Help / service desk is used by 31.2% of respondents (fig. 6-10);

- best practices such as ITIL and COBIT or standards such as ISO 27000 family (fig. 6-13 to Fig. 6-19) are very limited, and even more limited their certification at the corporate or personnel level; very limited, mostly to large organizations, the request suppliers to at least substantially follow these best practices and standards, or to have their certifications;
- limited requests for ICT security certificates both for internal staff (fig.6-20) and for the staff of suppliers (6-21).

Finally, 2014 will probably be remembered, worldwide, as the year of the data breach, typically for theft of data and digital identities.
The cyber attacks in 2014 confirm that sometimes severely impact both the attacked organizations and individuals who, directly or not, were involved: the impacts mainly concern financial losses and reputation. Critical ICT infrastructures will be more and more a target of terrorism.
Overall, up to now, Italy has suffered cyber crime and cyber war in a limited way, but is running a growing risk in the near future.

2. INTRODUZIONE

L'iniziativa OAI, Osservatorio Attacchi Informatici in Italia, è 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, concreta indicazione del fenomeno degli attacchi intenzionali sui sistemi informatici italiani.
Obiettivo primario di OAI è il recepire ed elaborare le indicazioni sugli attacchi intenzionali rilevati dalle aziende/enti, individuando lo specifico trend del fenomeno in Italia ed essere di riferimento, autorevole e indipendente, per l'analisi e la gestione dei rischi informatici. Ulteriore e non meno importante obiettivo è quello di aiutare nello sviluppo di sensibilità e cultura in materia di sicurezza informatica soprattutto 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 2015 fa riferimento agli attacchi informatici rilevati nel corso del 2014 e del 2013. Costituisce la quinta edizione, dopo i precedenti rapporti del 2013, 2012, 2011 e del 2009-10 che nel loro insieme coprono gli attacchi subiti dal 2007 a fine 2014.
Anche questa edizione, come la precedente, è sponsorizzata da Associazioni ed Aziende del settore. Gli Sponsor del presente rapporto sono le associazioni AICA[1] e AIPSI[2] e le aziende dell'offerta ICT[3] Business-e, HP, Riesko, 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 B.
OAI 2015 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).
Nell'iniziativa OAI il ruolo attivo dei Patrocinatori è significativo 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.
In tale ottica e per creare una certa continuità tra un'edizione e l'altra del Rapporto, l'Editore Soiel International e

[1] AICA, Associazione Italiana Calcolo Automatico (http://www.aicanet.it/)
[2] AIPSI, Associazione Italiana Professionisti Sicurezza Informatica, (http://www.aipsi.org/) capitolo italiano della mondiale ISSA (https://www.issa.org/)
[3] ICT, Information and Communication Technology

l'Autore hanno dato vita ad una Rubrica OAI pubblicata mensilmente sulla rivista Office Automation[4]. L'Autore ha inoltre creato un Gruppo OAI su LinkedIn.
Le precedenti edizioni[5] del Rapporto OAI sono scaricabili gratuitamente dai siti web elencati in nota. L'attuale edizione 2015 è scaricabile per 4 mesi dalla sua pubblicazione in esclusiva ai soli selezionati interlocutori degli Sponsor cui è stato inviato l'opportuno codice-coupon. Dopo i quattro mesi dell'esclusiva, il Rapporto è liberamente scaricabile da tutti gli interessati. 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

Con la pervasiva e crescente diffusione ed utilizzo di tecnologie informatiche e di comunicazione, e in particolare di dispositivi mobili e di sistemi informatici inclusi (embedded) in macchinari di ogni genere ed utilizzo, 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 in ogni settore di attività. Di qui l'importanza della loro affidabilità e disponibilità, senza la quale gli stessi processi, anche i più semplici, non possono ormai essere più espletati e gestiti.
L'evoluzione moderna dei sistemi informativi si è evoluta e consolidata su Internet, sui siti web, sui sistemi mobili, sull'Internet delle cose (IoT, Internet of Think), sui social network, sul crescente uso di terziarizzazione e di cloud computing.
Anche grazie alla diffusione di dispositivi mobili d'utente, che sono ormai dei potenti computer personali, delle reti senza fili (wireless), dei "social networking" e dei servizi ad essi correlati, ad esempio Facebook, YouTube, LinkedIn e Twitter, il confine tra ambiente domestico e ambiente di lavoro è sempre più labile, aiutato in questo dall'uso dello stesso dispositivo d'utente, tipicamente laptop, tablet e smartphone, in entrambi gli ambienti; l'acronimo BYOD, Bring Your Own Device, indica ormai anche in italiano il permesso di usare i propri personali dispositivi ICT mobili anche per il lavoro. Questo fenomeno, indicato con il termine di "consumerizzazione", è ormai molto diffuso ma pone una specifica serie di problemi di sicurezza.
Le tecniche di virtualizzazione consentono di razionalizzare le risorse hardware e gli ambienti applicativi, gestendoli in maniera dinamica, ma a loro volta introducono specifiche vulnerabilità e conseguenti problemi di sicurezza.
Lo sviluppo del software ha compiuto passi significativi, ma ancora è soggetto a gravi vulnerabilità per una non sicura programmazione e per la sovente mancanza di reali ed efficaci controlli; la programmazione a oggetti, gli standard SOA (Service Oriented Architecture) con i web service, le moderne metodiche ed i moderni ambienti di sviluppo software hanno migliorato il livello medio di sicurezza, ma non hanno eliminato le possibili vulnerabilità del codice sviluppato.
La pila dei protocolli TCP/IP e l'ambiente web costituiscono le piattaforme standard de facto e de jure per il trattamento di ogni genere d'informazione, con eterogeneità di sistemi e di funzioni; ma proprio perché così ben conosciute, gli attaccanti trovano più facilmente nuove vulnerabilità e modalità di attacco.
La veloce evoluzione tecnologica, di cui i temi sopra elencati rappresentano solo alcuni degli aspetti più noti, da un lato rende i sistemi informatici sempre più complessi e difficili da gestire, e con crescenti vulnerabilità; d'altra parte per effettuare attacchi deliberati e nocivi sono sovente necessarie competenze ridotte da parte degli attaccanti ed è sempre più facile reperire, anche gratuitamente su Internet, gli strumenti necessari.
Ma quali sono gli attacchi che più sovente affliggono i sistemi informativi italiani? E come si fa a reagire di fronte a tali attacchi? 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

[4] L'archivio degli articoli della Rubrica OAI è disponibile in http://www.malaboadvisoring.it/index.php?option=com_content&view=article&id=31&Itemid=50.
[5] I precedenti Rapporti OAI sono scaricabili dal sito web dell'Autore, www.malaboadvisoring.it, dal sito di AIPSI, www.aipsi.org, da quello dell'Editore Soiel International, www.soiel.it, e dai siti di alcuni Sponsor e Patrocinatori.

sicurezza informatica a livello mondiale, quali HP e Trend Micro (nell'Allegato C.2 un elenco delle principali e più aggiornate fonti). Questi studi forniscono con cadenza periodica informazioni dettagliate per i principali paesi e individuano i principali trend; dati specifici riguardanti l'Italia purtroppo sono raramente presenti, salvo casi eccezionali, e si devono pertanto estrapolare dalle medie europee.

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

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

Sulla stampa a livello nazionale l'occorrenza degli attacchi e lo stato dell'arte ad essi relativo sono prevalentemente trattati o come una notizia sensazionale di richiamo mediatico o come una nota tecnica per specialisti, con termini tecnici difficilmente comprensibili ai non addetti ai lavori.

Il reale livello di sicurezza di un sistema ICT dipende anche da come lo si usa e lo si gestisce, non solo dalle tecnologie impiegate: organizzazione, informazione e coinvolgimento di tutto il personale sono altrettanto importanti, se non di più, dell'installazione corretta di sistemi di sicurezza quali firewall, anti malware, sistemi di identificazione e autenticazione, back-up e così via.

Proprio per colmare un certo vuoto di attenzione e di sensibilizzazione sulla sicurezza informatica in Italia, con la prima edizione del rapporto OAI si decise di rilanciare un Osservatorio Nazionale, ereditando l'esperienza passata avuta con OCI, Osservatorio Criminalità Informatica, di FTI-Sicurforum[6]. Si definì una metodologia di indagine in collaborazione con gli esperti dei vari Enti patrocinatori, per raccogliere sul campo i dati presso un insieme di enti e di imprese (che si spera possa sempre più ampliarsi nel tempo) e per fornire con cadenza annuale e gratuitamente i risultati.

Dato il successo riscosso nelle precedenti edizioni, l'iniziativa OAI continua e si consolida grazie sia all'impegno volontario e professionale di alcuni esperti sia 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.

2.2 ASPETTI METODOLOGICI DELL'INDAGINE OAI

A differenza degli anni precedenti, nel Questionario OAI di fine 2014 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, per consentire così di raccogliere informazioni non note e poter rispondere correttamente alla domande cui non si sa rispondere). Nell'ottica di garantire e migliorare la qualità del Rapporto, con questa edizione è stato inoltre costituito un Comitato Scientifico[7] per la verifica dei contenuti del Questionario e del Rapporto finale.

Il rapporto OAI 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 (Proprietari, così come evidenziato in fig. A-1 dell'Allegato A.

L'Autore, l'Editore Soiel ed i Patrocinatori hanno invitato a compilare il Questionario 2014 le persone con i profili

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

[7] Il Comitato Scientifico OAI è presieduto dal prof. Stefano Zanero del Politecnico di Milano e componente dell'International Board ISSA, ed è costituito dal prof. Roberto Baldoni, Executive Director Cyber Security National Laboratory, dal prof. Cosimo Comella, Garante Privacy - Dirigente Dipartimento risorse tecnologiche, dal prof. Pierluigi Perri, Università di Milano e Studio legale Monducci, Perri & Spedicato, dal prof. Fabio Roli, Dipartimento Ingegneria Elettrica ed Elettronica Università di Cagliari

sopra elencati con messaggi di posta elettronica, utilizzando le loro "mailing list" di clienti, sia lato domanda che lato offerta, di lettori delle riviste, di soci e simpatizzanti delle associazioni patrocinanti. Sono stati inoltre sollecitati i partecipanti a vari "social network" inerenti l'ICT e la sicurezza informatica, ed alcuni dei Patrocinatori e Sponsor hanno pubblicato "banner" e comunicazioni di invito sui loro siti web.
Il Questionario OAI 2014 è rimasto accessibile on line da inizio gennaio a metà marzo 2015, ed anche in questo arco temporale il bacino dei potenziali rispondenti ha ricevuto vari inviti e solleciti.
Nel complesso il numero delle persone contattate si è aggirato attorno a seimila, appartenenti ad un ampio insieme di aziende di ogni dimensione e settore merceologico, inclusi enti pubblici centrali e locali.
L'indagine annuale OAI 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 A, il numero (424) e l'eterogeneità delle aziende/enti dei rispondenti, sia per settore merceologico che per dimensione, è comunque significativo per fornire preziose 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 altre risposte previste o ad evidenziarle se significative.
Nel rapporto in alcuni casi si confrontano i dati attuali con quelli delle precedenti edizioni: i campioni di rispondenti sono diversi, anche per il loro aumento di 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 cinque edizioni, le percentuali variano a secondo 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 statistici e comunque il livello di dettaglio sulle caratteristiche tecniche dei sistemi ICT non consente in alcun modo di poter risalire all'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 e l'Editore garantiscono inoltre la totale riservatezza sulle risposte raccolte, utilizzate solo per la produzione del presente rapporto.

3. LE TIPOLOGIE DI ATTACCO CONSIDERATE

La sicurezza ICT è 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.

L'attacco contro un sistema informatico è tale quando si intende violato almeno uno dei requisiti sopra esposti con una attività non autorizzata.
Si evidenzia dal nome stesso come l'OAI sia indirizzato alle azioni deliberate e intenzionali rivolte contro i sistemi informatici e non ai rischi cui i sistemi sono sottoposti per il loro cattivo funzionamento, per un maldestro uso da parte degli utenti e degli operatori, o per fenomeni accidentali esterni.
Gli attacchi intenzionali possono provenire dall'esterno dell'organizzazione considerata, tipicamente attraverso Internet e/o accessi remoti, oppure dall'interno dell'orga-

nizzazione stessa, o infine, come spesso accade, da una combinazione di personale interno ed esterno. Per approfondimenti sulle logiche, le motivazioni e le tipologie degli attaccanti, oltre che sulle loro competenze e sulla loro cultura, si rimanda all'ampia letteratura in materia, in particolare al recente libro "Sicurezza digitale" dell'Autore e di Francesco Zambon edito da Soiel International[8].
Per il Questionario OAI 2013 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.
La classificazione degli incidenti e degli attacchi per raccogliere i dati sugli attacchi è definita in termini semplici, non troppo tecnici e comprensibili.
La tassonomia degli attacchi informatici considerata nel Questionario 2014 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 D).

4. GLI ATTACCHI INFORMATICI RILEVATI

La fig. 4-1 mostra, percentualmente, il numero di attacchi rilevati dai rispondenti nel 2013 e nel 2014. Nel 2013 il 62,5% non ha mai rilevato un attacco intenzionale, il 37,5% li ha invece subiti e rilevati, e tra questi l'8,6% ha subito più di 10 attacchi nell'anno. Nel 2014 il numero di attacchi rilevati è aumentato del 7,2%, arrivando al 44,7% dei rispondenti, e il 10% ne ha subiti più di 10 nell'anno, anche dello stesso tipo. È importante evidenziare poi la differenza percentuale tra la numerosità di attacchi nell'anno nella stessa azienda/ente: quelli oltre le 10 volte sono assai meno numerose. L'aumento del numero di attacchi nel 2014 è confermato dalle altre indagini sia a livello nazionale che internazionale.
La fig. 4-2 confronta il numero di attacchi rilevati nei diversi Rapporti OAI dal 2008-2015, da considerare come trend puramente indicativo, dato che i campioni emersi in questi anni sono diversi come mix e come numero. Considerando tutti casi, più e meno 10 attacchi nell'anno, si evidenzia che in media ha subito attacchi il 40% del campione emerso dalle indagini nei vari anni, con una varianza limitata al 4,5%. Da questo confronto, anche se puramente indicativo, si traggono alcune considerazioni, riprese a livello internazionale anche da altri rapporti. Nell'arco temporale considerato e per il campione emerso nelle varie indagini, il 2008 rappresenta l'"annus horribilis" per la quantità di attacchi occorsi, ed il 2014 gli si avvicina. Significativo che sia nel 2013 sia nel 2014 si siano registrati i valori più alti di attacchi ripetuti, con un 8,6% ed un 10% rispettivamente. Il valore 40% per gli attacchi rilevati in Italia nelle indagini OAI, 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 e il numero elevatissimo di piccole e piccolissime imprese, come mostrato nella Tabella A-1 dell'Allegato A; queste aziende sicuramente non rappresentano un obiettivo di interesse per i cyber criminali. La convalida di questo assunto è data dall'analisi degli attacchi nel 2014 per dimensione di azienda/ente dei rispondenti, mostrata in fig. 4-3. Per i dettagli sulle caratteristiche "macro" dell'organizzazione e dei sistemi informatici dei rispondenti si rimanda all'Allegato A.

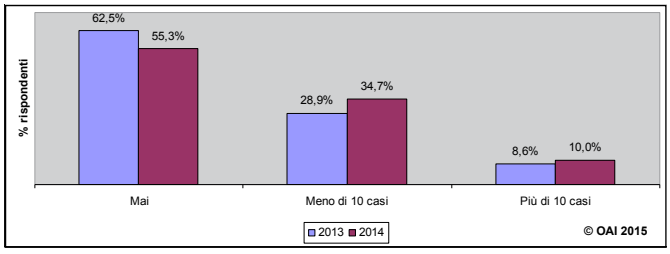

Fig. 4-1 Attacchi rilevati nel 2013 e nel 2014

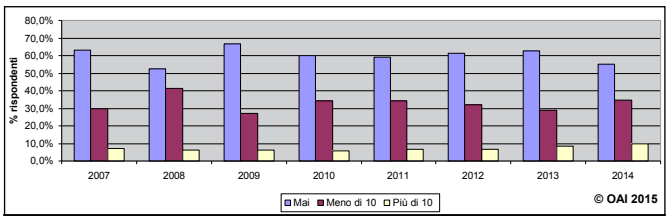

Fig. 4-2 Attacchi rilevati dal 2007 nei vari Rapporti OAI

[8] Si veda http://www.soiel.it/res/libro/id/8/p/libro.html

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. Frodi informatiche tramite uso improprio o manipolazioni non autorizzate e illegali del software applicativo (dal mascheramento dell'identità digitale all'utilizzo di software pirata e/o copie illegali di applicazioni, ecc.).
6. 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.
7. 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).
8. Accesso a e uso non autorizzato degli elaboratori, delle applicazioni supportate e delle relative informazioni.
9. Modifiche non autorizzate ai programmi applicativi e di sistema, alle configurazioni ecc.
10. Modifiche non autorizzate ai dati e alle informazioni trattate.
11. 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.
12. Codici maligni (malware) di varia natura, quali virus, Trojan horses, Rootkit, bots , exploits, sia a livello di posto di lavoro che di server.
13. 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.
14. Attacchi alle reti, fisse o wireless, e ai DNS (Domain Name System).
15. Attacchi mirati (targeted) e APT, Advanced Persistent Threats, basati su uso contemporaneo e/o persistente di più tecniche sofisticate di attacco.

La figura mostra come, nel campione emerso, gli attacchi aumentino prevalentemente per dimensione dell'organizzazione, indicata dal numero di dipendenti, con un picco però per le aziende nella fascia 10-101, con il 13,8%, seguite da quelle nella fascia >5001 con il 10,7% sul totale. Le organizzazioni della fascia 10-101 sono quelle più numerose tra i rispondenti, con il 35,4%, come mostrato in fig. A-3. 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. 4-4 mostra il numero di attacchi subiti nei tre macro settori, primario insieme a secondario, terziario e Pubblica Amministrazione (PA), sia centrale (PAC) che locale

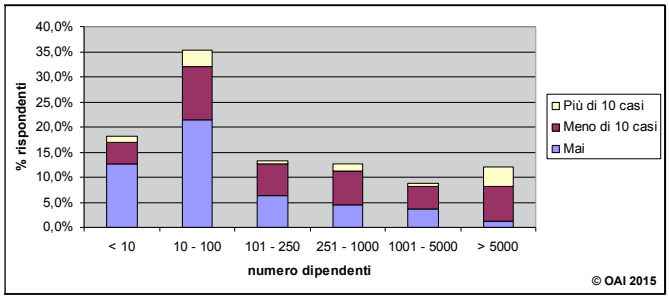

Fig. 4-3 Attacchi 2014 per dimensione dell'azienda/ente

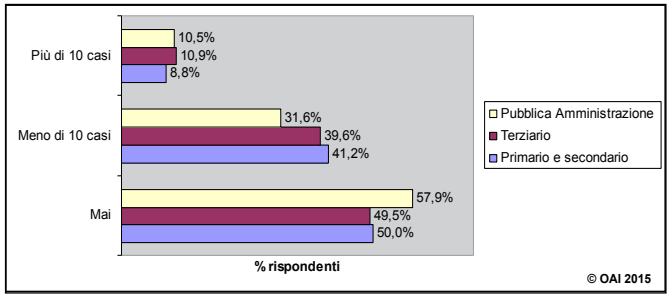

Fig. 4-4 Attacchi 2014 per macro settore

(PAL), nei quali sono stati accorpati i singoli settori merceologici dei rispondenti, dettagliati nella fig. A-2. La maggior parte delle risposte è pervenuta da aziende dei servizi e dell'industria manifatturiera, la PA ha risposto in misura maggiore che negli scorsi anni, ma ancora troppo limitata tenendo conto dell'elevato numero di enti pubblici, soprattutto PAL. Nell'ambito del campione emerso, per il 2014 la PA ha subito/rilevato in percentuale meno attacchi rispetto agli altri due macro settori. Facendo riferimento alle principali tipologie di attacco elencate nella Tabella1, la fig. 4-5 mostra la diffusione in percentuale degli attacchi subiti nel campione dei rispondenti e la Tabella 2 dettaglia la classifica dei tipi di attacchi più diffusi in Italia con le variazioni avute tra il 2013 ed il 2014.
La Tabella evidenzia come solo una tipologia ha avuto un decremento percentuale, quella dei furti di dispositivi ICT. Anche per questa edizione, come per tutte le precedenti di OAI (si veda a conferma la fig. 4-6), i primi quattro posti di attacchi più diffusi sono sempre i medesimi.
In particolare nel 2014:

- al primo posto permane il malware, 67,9%, quasi affiancato dal social engineering con il 67,1%. Il "social engineering" è alla base dei principali attacchi, anche complessi (si veda APT e TA), avvenuti negli ultimi anni, ed include il phishing, che dalla posta elettronica si è esteso agli SMS, alle chat, ai social network. Nel corso degli ultimi anni, come evidenziato in fig. 4-6, il social engineering ha avuto una significativa crescita percentuale. Il malware, dopo il picco del 2008, ha un andamento oscillante, ma sempre da primo in classifica, tra il 60 ed il 68%. Per approfondimenti sui codici maligni si rimanda a §4.2.1;
- al terzo posto la saturazione delle risorse ICT (DoS/DDoS), che era al quarto posto nella scorsa edizione, e che arriva nel 2014 al 42,5%, con un incremento rispetto al 38,8 % del 2013 ed al 34,5% del 2012; anche questo tipo di attacco ha avuto un andamento oscillante negli anni; una forte crescita fino al 2011,

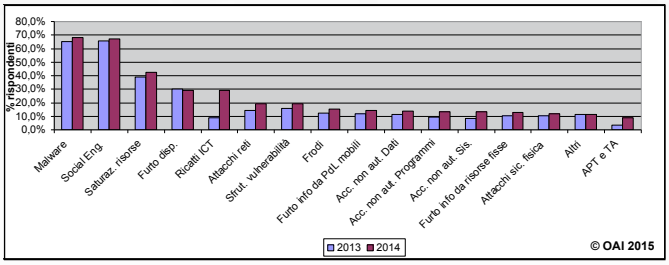

Fig. 4-5 Diffusione tipologia attacchi subiti 2013-2014 (risposte multiple)

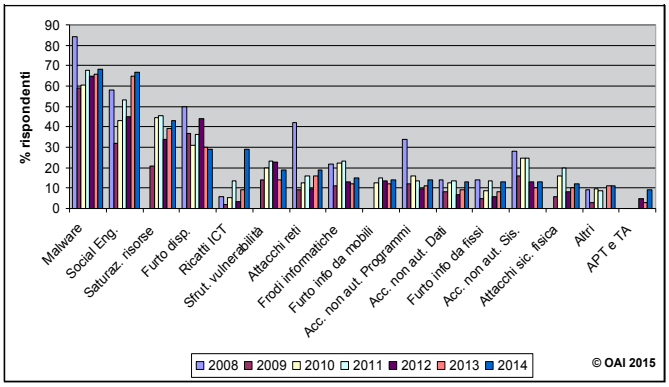

Fig. 4-6 Confronto diffusione attacchi 2008-2014 (risposte multiple)

Classifica	Tipologia attacchi	2013	2014	Variazione
1	Malware	65,1%	67,9%	2,8%
2	Social Eng.	65,8%	67,1%	1,4%
3	Saturaz. risorse	38,8%	42,5%	3,7%
4	Furto disp.	30,3%	29,2%	-1,1%
5	Ricatti ICT	8,7%	28,9%	20,2%
6	Attacchi reti	14,5%	19,2%	4,7%
7	Sfrut. vulnerabilità	15,8%	19,1%	3,3%
8	Frodi	12,4%	15,1%	2,8%
9	Furto info da PdL mobili	11,9%	14,2%	2,3%
10	Acc. non aut. Dati	11,2%	14,0%	2,8%
11	Acc. non aut. Programmi	9,3%	13,4%	4,2%
12	Acc. non aut. Sis.	8,3%	13,4%	5,1%
13	Furto info da risorse fisse	10,5%	12,7%	2,3%
14	Attacchi sic. fisica	10,4%	11,8%	1,4%
15	Altri	11,4%	11,5%	0,1%
16	APT e TA	3,3%	8,9%	5,6%

Tabella 2 Variazione % attacchi subiti tra 2014 e 2013

Classifica	Tipologia attacchi	2013	2014	Variazione
5	Ricatti ICT	8,7%	28,9%	20,2%
16	APT e TA	3,3%	8,9%	5,6%
13	Acc. non aut. Sis.	8,3%	13,4%	5,1%
7	Attacchi reti	14,5%	19,2%	4,7%
10	Acc. non aut. Programmi	9,3%	13,4%	4,2%
3	Saturaz. risorse	38,8%	42,5%	3,7%
6	Sfrut. vulnerabilità	15,8%	19,1%	3,3%
11	Acc. non aut. Dati	11,2%	14,0%	2,8%
2	Malware	65,1%	67,9%	2,8%
8	Frodi	12,4%	15,1%	2,8%
9	Furto info da PdL mobili	11,9%	14,2%	2,3%
12	Furto info da risorse fisse	10,5%	12,7%	2,3%
1	Social Eng.	65,8%	67,1%	1,4%
14	Attacchi sic. fisica	10,4%	11,8%	1,4%
15	Altri	11,4%	11,5%	0,1%
4	Furto disp.	30,3%	29,2%	-1,1%

Tabella 3 Ordinamento attacchi per variazione % tra 2014 e 2013

poi una diminuzione nel 2012, per poi risalire negli ultimi due anni;

- al quarto posto il furto di dispositivi ICT con un 29,2% nel 2014, diminuito rispetto al 30,3% del 2013 ed al 44,4% del 2012. Confrontando i dati in fig. 4-6, il fenomeno del furto di dispositivi si sta riducendo e nel 2014, come evidenziato in Tabella 3, è l'unico ad avere un decremento, pur rimanendo tra i primi quattro come diffusione. 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 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 da rubare, più per venderli sul "mercato nero" che per rubare le informazioni in essi contenuti.

La Tabella 3 elenca i tipi di attacco classificandoli per maggior variazione tra 2013 e 2014: in quest'ultimo anno i ricatti ICT subiscono il più significativo balzo in avanti, raggiungendo il quinto posto della classifica OAI degli attacchi più diffusi in Italia, con il 28,9% dei rispondenti, passando dall'8,7 % del 2013 e dal 4% del 2012. Nei precedenti Rapporti OAI si era già parlato del "pizzo informatico" come potenziale attacco "di massa", ed il 2013-14 sono stati anni con una crescente diffusione di "ransomware", in particolare con il Crypto Locker e suoi simili e derivati[9]. Ulteriori attacchi di questo tipo sono svolti senza malware, ma verificando con opportune scansioni da remoto la 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 2014 si attestano sotto il 20%, ed una sola, TA/APT, al di sotto del 10%.

Al sesto posto per diffusione si attestano gli attacchi alle reti, con il forte incremento del 4,7%. 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. Al settimo posto, con una differenza minima rispetto al precedente (0,1%), gli attacchi basati sullo sfruttamento delle vulnerabilità dei programmi, con un aumento del 3,3% rispetto al 2013, sia a livello di posto di lavoro che di server: tipici esempi back-door aperte, SQL injection, buffer overflow, ecc. Rientrano in questa tipologia di attacchi sulle quelli basati sulle vulnerabilità zero-day, ossia le vulnerabilità che non sono ancora state individuate dalla casa madre (ma dall'attaccante sì) e/o per le quali non è stato ancora pubblicata la "patch" di correzione. Le vulnerabilità del software sono alla base della maggior parte degli attacchi "tecnici", e la loro diffusione, si veda fig. 4-6, è andata aumentando fino al 2012, per poi avere un brusco arresto nel 2013 e riprendere la crescita nel 2014. Questo andamento è indicativo della crescente consapevolezza della necessità di aggiornare sistematicamente patch e versioni del software in uso.

All'ottavo posto le frodi informatiche con un incremento del 2,8% rispetto al 2013. Esse costituiscono il principale obiettivo dei cyber criminali e possono essere realizzate in vari modi e con la combinazione di diverse tipologie di attacco. Tipici esempi includono lo sfruttamento, ovviamente illegale, di conti bancari, di abbonamenti a servizi, da quelli telefonici alle pay-tv, dei pagamenti di sanzioni e di acquisti in rete, e così via. I ricatti informatici rientrano di fatto tra le frodi informatiche, ma per le loro specifiche caratteristiche si è ritenuto opportuno definire una tipologia ad hoc. L'andamento negli anni delle frodi, come diffusione per i diversi campioni OAI emersi, risulta oscillante, ma la tendenza è la loro crescita.

Al nono posto il furto di informazioni da dispositivi d'utente mobili, con un incremento del 2,3% rispetto al 2013. 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 ovvio obiettivo una frode, basata il

[9] 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.

più delle volte sul furto dell'identità digitale. Al decimo, undicesimo e tredicesimo posto si posizionano accessi non autorizzati ai programmi, ai dati da questi trattati ed ai sistemi che li supportano. Queste tipologie di attacchi sono logicamente concatenate tra loro: prima si accede ad un sistema, poi ad una sua applicazione, ed infine ai dati da quest'ultima trattati. 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.
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".
Tutte queste tre tipologie d'attacco hanno subito incrementi significativi tra il 2013 ed il 2014, come mostrato in Tabella 2 e 3. Da un punto di vista storico, come da fig. 4-6, tutti e tre hanno avuto un andamento oscillante ma non trascurabile, data la loro criticità e le gravi conseguenze che possono causare per la consistenza, integrità e correttezza dei dati e delle applicazioni che li trattano.
Al dodicesimo posto per diffusione il furto di informazioni da dispositivi d'utente fissi, con il 12,7% nel 2014 ed un incremento del 2,3% rispetto al 2013. Questa diffusione ha poco più di un punto percentuale (1,4%) di differenza da quella dei dispositivi mobili, ma è un ulteriore indicatore di come il fisso sia sostituito sempre più dal mobile per l'utente finale. L'andamento storico della diffusione è oscillante, 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… ma anche di un server o di un storage. Al quattordicesimo posto come diffusione nel 2014 gli attacchi alla sicurezza fisica dei sistemi ICT e delle infrastrutture a loro supporto, con un 11,8% ed un incremento del 1,4% rispetto al 2013. In questa categoria 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 nell'ultimo triennio e, come illustrato più avanti, sono quelli che hanno causato i più gravi danni nel 2014 nel campione dei rispondenti.
Al penultimo posto, con un 11,5% per il 2014 molto vicino al 11,4% del 2013, gli attacchi indicati come "Altri" che includono gli attacchi che il rispondente non riconosce nella tipologia di Tabella 1. Nel questionario era prevista la possibilità di specificare quale tipo di attacco non classificato era stato subito; non tutti hanno specificato l'attacco, alcuni sono stati collocati dall'autore nelle tipologie predefinite, e quelli rimasti includono:

- attacco ad e-mail di Google Mail, acquisizione delle password di accesso e invio di mail contraffatte (fake) a tutta la rubrica;
- tentato accesso a sistema cloud via ftp;
- un non meglio definito "utilizzo di risorse telefoniche".

All'ultimo posto come diffusione gli attacchi APT, Advanced Persistent Threats, e TA, Targeted Attacks, basati su uso contemporaneo e/o persistente di più tecniche sofisticate di attacco. Nel 2014, con l'8,9%, hanno avuto un forte incremento del 5,6% rispetto al 2013. 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[10] 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, fino

[10] 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

ai recenti Anthem, Home Depote, JP Morgan Chase. Pur se di difficile identificazione, APT e TA iniziano ad essere presenti e in crescita anche in Italia. La relativamente bassa percentuale di diffusione è dovuta, per l'Autore, soprattutto al già citato limitato numero di grande aziende/enti in Italia. Il forte incremento tra 2013 e 2014 è un chiaro indice dell'inasprimento del cyber crime in quest'ultimo periodo.

4.1 GLI IMPATTI DEGLI ATTACCHI RILEVATI

Il Questionario 2014 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. Il risultato, posto a 100 il numero complessivo di attacchi subiti per anno, è sintetizzato nella fig. 4-7. I dati emersi sono percentualmente simili per il 2013 e 2014, ed anche a quanto rilevato, pur con campioni di rispondenti diversi, nelle precedenti edizioni di OAI. La stragrande maggioranza degli attacchi ha avuto impatti poco significativi: quelli occorsi fino a dieci volte per anno, rappresentano circa il 70% del campione; quelli occorsi più di 10 volte nell'anno, il 17% circa del campione.

Gli attacchi con impatti sono percentualmente simili nel 2014 e nel 2013, con un piccolo incremento nel 2014 per gli attacchi con non più di 10 occorrenze per anno.

Nella presente edizione si è voluto analizzare il "forte impatto" anche per tipologia di attacco, ed il risultato è rappresentato nella fig. 4-8.

Dalla figura emerge che nel 2014 è aumentata percentualmente la gravità di tutte le tipologie, a parte il furto di informazioni da dispositivi d'utente sia fissi che mobili.

Come già anticipato, gli attacchi alla sicurezza fisica, pur limitati in termini di diffusione, sono quelli che hanno creato maggiori impatti. Il motivo, a giudizio dell'Autore, è in parte dovuto alla relativa facilità di calcolare il danno economico subito.

Tutti gli altri attacchi rilevati sono stati ritenuti a grave impatto tra il 30 ed il 10% dei rispondenti, a parte 4 che scendono sotto il 10%. Ed è interessante evidenziare che tra questi social engineering e furti di dispositivi ICT, sono tra i primi quattro come diffusione, e che le frodi, che per definizione arrecano danni economici, hanno avuto un impatto grave solo per pochi rispondenti. Il malware, di poco sopra il 10% come grave impatto, è in assoluto il più diffuso, ma non reca "normalmente" gravi danni.

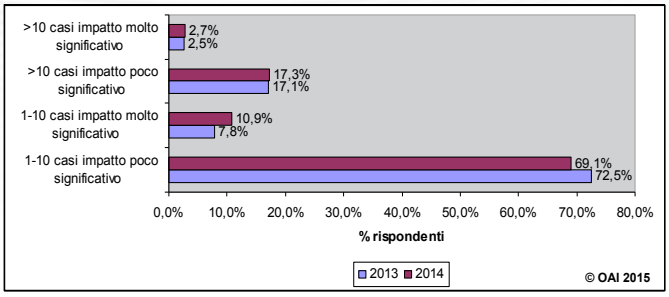

Fig. 4-7 Impatto dell'attacco

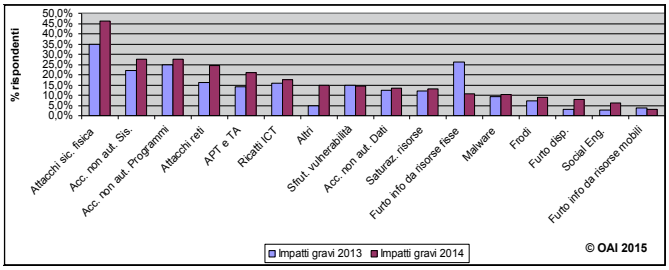

Fig. 4-8 Impatti gravi per tipologia d'attacco nel 2013-14

Sempre in termini di impatto, una domanda specifica chiedeva la stima del danno economico, che, come indicato in fig. 4-9, il 41,5% non effettua ma che, significativamente, il 30% dichiara di farla per tutti gli attacchi subiti, ed il 13,1% solo per quelli più gravi.

I dati percentuali sono abbastanza analoghi a quelli della precedente edizione di OAI.

Un aspetto cruciale di un attacco è l'impatto economico che può causare per il ripristino "ex ante" sia del sistema informatico e dei suoi dati, sia dell'immagine e della repu-

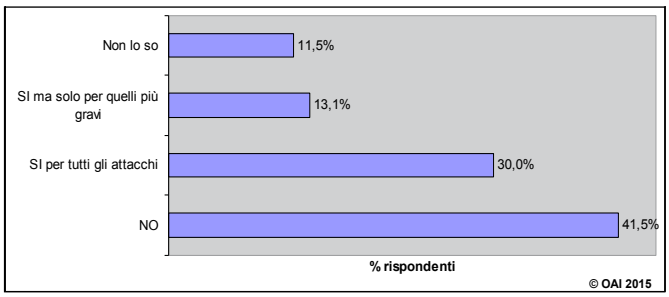

Fig. 4-9 Stima impatto economico dell'attacco subito

tazione sul mercato. Diversi i possibili metodi di calcolo, e di qui la forte eterogeneità delle poche informazioni disponibili, soprattutto a livello italiano.
Pochi rispondenti hanno fornito dati, e questi variano molto; in alcuni casi la risposta non è credibile, contestualizzandola alle altre risposte fornite[11]: eliminati i dati dubbi, la media delle risposte credibili ricevute porta ad un valore medio di € 2.630,00 per attacco, con un minimo di € 400,00 ed un massimo di € 20.000,00. Questi dati sono congruenti con quelli ricevuti nella precedente edizione, sempre puramente indicativi, che variavano da pochi centinaia di Euro a € 70.000,00 per attacco.
Dato il basso valore indicato, è ragionevole ritenere che essi rappresentino i soli costi diretti per il ripristino della situazione informatica ex ante, e non considerino altri costi indiretti e consequenziali, quali l'impatto sul business, la perdita di fatturato e di immagine, ecc.
Specifiche indagini a livello internazionale hanno fornito indicazioni in merito, che comunque devono essere prese con grandi precauzioni per il contesto italiano. Le ricerche più accreditate sono quelle del Ponemon Institute, sponsorizzate da alcuni grandi fornitori di ICT, che forniscono alcuni dati significativi anche se relativi solo a grandi organizzazioni:

- il costo del crimine informatico varia a secondo dell'attacco, del tipo di azienda/ente e delle sue dimensioni in termini di numero di dipendenti: le strutture di dimensioni minori hanno un costo complessivo per anno di $ 1061 per persona utente, quelle di dimensioni maggiori di $ 437[12]; i costi maggiori derivano dagli attacchi perpetrati da attaccanti interni (malicious insider), saturazione delle risorse ed attacchi al web; le aziende/enti con i costi maggiori sono quelle dei settori energetici, utility e finanziarie;
- specifica per l'Italia, seppur svolta su un campione limitato di grandi organizzazioni, è la ricerca sui "data breaches"[13], da cui emerge che il costo per capita medio è aumentato da € 78 nel 2012 a € 102 nel 2014; i costi per capita più alti riguardano aziende "consumer" (es: grandi magazzini, supermercati, ecc.) con € 138 e finanziarie con € 125, quelli più bassi le Pubbliche Amministrazioni con € 55 e le aziende dei servizi con € 50.

4.2 I DATI DALLA POLIZIA POSTALE E DAL CNAIPIC

Il Cnaipic (http://www.poliziadistato.it/articolo/view/23401/) è una struttura della Polizia Postale 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.
Nell'ambito della collaborazione con OAI, la Polizia Postale ha fornito i significativi dati sulle azioni svolte dal Cnaipic nel 2014.
La Tabella 4 mostra il numero di attacchi ai sistemi informatici critici nel 2014.
Le infrastrutture critiche nazionali sono sistemi di grandi e grandissime dimensioni, non certo paragonabili, in media, ai sistemi informatici dei rispondenti OAI, descritti in §A2.2. Ma nonostante tale diversità è significativo che i malware siano anche in questo contesto al primo posto in termini di diffusione. I "defacement" ai siti web, ed in particolare alle loro "home page" sono stati abbastanza numerosi proprie sui siti di pubbliche amministrazioni. Tali attacchi sono considerati in OAI nell'ambito della tipologia "Modifiche non autorizzate ai programmi applicativi e di sistema" (si veda Tabella 1).
La Tabella 5 elenca le principali minacce e vulnerabilità individuate per le infrastrutture critiche, ed i conseguenti allarmi (alert) inviati, insieme a quelli per gli attacchi in atto e in preparazione, mostrati in Tabella 6.
Tale tabella mostra un importante indicatore delle attività di prevenzione, con una media di 3,1 allarmi/giorno per gli attacchi e di 1,1 allarmi/giorno per minacce e vulnerabilità, considerando tutti i 365 giorni di un anno.
La Tabella 7 mostra le conseguenze "giudiziarie" della lot-

[11] In ogni indagine libera via web come quella di OAI ci sono sempre dei "burloni" che sparano risposte e numeri per prendersi gioco o per screditare l'indagine stessa. Ma grazie ai controlli effettuati, tali risposte false sono nella maggior parte dei casi individuate e non considerate
[12] Ponemon Institute: "2014 Global Report on the Cost of Cyber Crime", http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/
[13] Ponemon Institute: "2014 Cost of Data Breach Study: Italy", http://www-01.ibm.com/common/ssi/ShowDoc.wss?docURL=/common/ssi/ecm/se/en/sel03023usen/index.html&lang=en&request_locale=en

Accessi abusivi/dump	**64**
Defacement	**169**
DDoS	**50**
Altri attacchi/malware	**1055**
Totale attacchi rilevati	***1338***

Tabella 4 Cnaipic: Attacchi 2014 alle infrastrutture critiche

Minacce	**148**
Vulnerabilità	**154**
Totale minacce e vulnerabilità rilevate	***302***

Tabella 5 Cnaipic: Minacce e vulnerabilità 2014 rilevate per le infrastrutture critiche

Alert inerenti attacchi informatici	**1135**
Alert inerenti minacce e vulnerabilità	**417**
Totale alert diramati	***1552***

Tabella 6 Cnaipic: Alert diramati 2014 per le infrastrutture critiche

ta per la repressione del crimine informatico. Le indagini per attacchi alle aziende sono più del doppio di quelle per le Pubbliche Amministrazioni, e questo è un chiaro indice di come gli attacchi abbiano motivazioni prevalentemente economiche. Il crimine informatico di alto livello opera a livello internazionale, dato che Internet non ha di fatto confini "nazionali", a parte qualche stato dittatoriale che controlla e blocca, o cerca di bloccare, le comunicazioni. Al contrario gli organi di polizia e la magistratura operano a livello nazionale secondo le leggi di ciascuno

Indagini avviate per attacchi ad enti	**208***
Indagini avviate per attacchi ad aziende	**487***
Persone deferite all' Autorità Giudiziaria	**114***

** Le cifre relative alle attività di P.G. sono riferite a tutto il Servizio Polizia Postale e delle Comunicazioni*

Tabella 7 Polizia Postale: attività 2014 di Polizia Giudiziaria per il cyber crime

Richieste inviate	**45**
Richieste ricevute	**40**
Totale richieste di cooperazione gestite	**85**

Tabella 8 Cooperazione Internazionale Polizia Postale in ambito rete 24/7 High Tech Crime G8 (Convenzione Budapest)

stato, con serie difficoltà per perseguire legalmente il criminale informatico, anche se individuato. Sia per questo motivo sia per poter essere informati sui nuovi attacchi e poter agire sempre più in maniera proattiva e non solo reattiva, è fondamentale l'effettiva ed efficace collaborazione tra i vari organi preposti.
La Tabella 8 mostra il numero di richieste ricevute ed inoltrate tra le polizie nell' ambito del G8, in accordo con la Convenzione di Budapest[14].

4.3 NUOVI E VECCHI ATTACCHI

4.3.1 Vulnerabilità e codici maligni

I codici maligni, o malware, rappresentano e permangono da anni l'attacco più diffuso, nonostante l'uso di antivirus e antispyware sia a livello di dispositivi d'utente sia di server, di sistemi di storage e di rete.

[14] Con Convenzione di Budapest si intende la Convenzione del Consiglio dell'Europa sulla criminalità informatica, fatta 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)

Il termine malware include un vario insieme di programmi sviluppati e diffusi con il solo scopo di provocare danni ai computer sui quali sono attivati: includono i virus, i cavalli di troia (trojan), i worm, i PUP, i "backdoor", gli "adware" e gli "spyware". Per una prima sintetica descrizione di tali termini si rimanda al Glossario nell'Allegato D e per ulteriori approfondimenti al già citato libro "Sicurezza digitale" dell'Autore. Inizialmente creati per PC e server, si sono poi diffusi sui sistemi mobili, in particolare smart phone e tablet, così da creare un vero e proprio problema di "massa" e di porli, in termini di diffusione, sempre al primo posto in tutte le indagini OAI.

Per motivi di lunghezza del questionario e della relativa facilità a rispondere anche da parte di non tecnici, OAI non indaga su quali sono i malware più diffusi, ma numerose indagini internazionali lo fanno, oltre a quella di Fastweb per i suoi clienti in l'Italia[15].

Considerando le più aggiornate indagini (§C.2), i malware si vanno diversificando tra quelli più "generalisti" orientati ai sistemi operativi ed alle piattaforme ICT, e quelli più "specializzati" per specifici settori ed ambienti, ad esempio PoS, home banking, commercio elettronico, SCADA ecc.

Ulteriori fenomeni sui codici maligni, già presenti negli anni precedenti, si sono ulteriormente diffusi e consolidati, ed includono:

- disponibilità di sofisticati strumenti per la creazione di codici maligni, chiamati in gergo DIY[16] Kit (o tool), taluni scaricabili gratuitamente da Internet, che fanno crescere il numero di malware in circolazione;
- anche grazie a questi DIY Kit, facile derivazione di malware diversi da un medesimo "ceppo"; un tipico esempio SpyEye, Citadel, Carberp, Bugat, Shylock, Torpig derivati da Zeus;
- facile modifica e riutilizzo di "vecchi" virus, taluni non più controllati dagli antivirus;
- malware sempre più sofisticati, multipiattaforma (possono operare con diversi sistemi operativi) ed in grado di "nascondersi", eludendo anti-malware e proxy usando la rete anonima TOR[17] e tecniche di "offuscazione" ed elusione;
- sfruttamento delle vulnerabilità della Java Virtual Machine (JVM) e del Java Run Time, richiesti da varie applicazioni;
- controllo e gestione dei malware da remoto tramite server anonimi chiamati C&C, Command &Control, con comunicazioni di norma criptate;
- ampia diffusione di malware sui sistemi mobili, in particolare per quelli con Android;
- alcuni anti-malware inefficaci ed altri addirittura non sicuri (§4.2.1.2).

Nel 2013 e nel 2014 i malware che più hanno fatto parlare di sé includono Shellshock, POODLE, Ghost , FREAK, Zbot, HIMAN. In ambito mobile FakeID e Same Origin Policy (SOP) Bypass.

Uno dei più diffusi è il "vecchio" Conficker worm, in azione da più di 6 anni, ma ampia diffusione anche di Neverquest, Ramnit e Dyre. Tra i malware "generalisti", ripresi anche dalla stampa non tecnica per la loro diffusione ed i loro impatti, il più noto è stato Shellshock[18]: può colpire sistemi Linux, Unix ed Apple OS X che utilizzano una versione della shell di comando Bash dalla versione 4.3 in giù. Suo tramite sono stati effettuati attacchi da remoto, prevalentemente su web server con sistemi operativi Unix/Linux e che operano con script, e tramite servizi quali Secure Shell (SSH) e con protocolli di rete DHCP. Sfruttando le vulnerabilità di Bash[19] nelle versioni non aggiornate, un attaccante può modificare il contenuto del web server, cambiare il codice del sito, rubare i dati dell'utente dal database, cambiare i permessi del sito, installare backdoor e così via. A rischio maggiore sono anche tutti i dispositivi dell'Internet delle Cose (IoT, Internet of of Things), che utilizzano per la maggior parte Linux (si veda §4.2.3).

Grande diffusione di malware per i dispositivi mobili, data la loro diffusione che supera quella dei PC, ed in

[15] Pubblicata nel Rapporto Clusit 2015

[16] DIY, Do It Yourself, traducibile in "fallo da te". Un elenco di DIY Kit, seppur datato, in http://seclists.org/fulldisclosure/2007/Aug/411

[17] TOR, The Onion Router, è un sistema di comunicazione anonima in Internet basato sul protocollo onion router e su tecniche di crittografia: https://www.torproject.org/. Si veda anche: http://threatpost.com/shedding-new-light-on-tor-based-malware/104651

[18] identificato il 24 settembre 2014 e classificato nella banca dati CVE delle vulnerabilità come CVE 2014-7169 e CVE 2014-6271 per il mondo Unix/Linux

particolare per il sistema operativo Android. Meno attaccati gli altri sistemi operativi di riferimento iOS e Mobile Windows. L'uso crescente dei sistemi mobili per acquisti e pagamenti amplia ulteriormente il fenomeno. I più recenti rapporti internazionali sul fenomeno (§C.2) evidenziano come si siano diffusi malware diversi nelle varie nazioni, ma alcuni sono comuni, e tra questi ActSpat, ColdBrother, NotCompatible, ScareMeNot, ScarePackage, SMSCapers, Tornika.
Come già indicato in §4.2 una particolare categoria di codici maligni, chiamati ransomware, consente di bloccare in funzionamento di un PC o di un server, tipicamente criptando il suo file system, e poi richiedono un riscatto per poter avere la chiave di decrittazione. In Italia ha avuto forte diffusione Crypto Locker, ma ne esistono di simili, ad esempio Ransom, Reveton, Crylock, diffusi a livello mondiale. Secondo una indagine Trend Micro[20], nel 2013 l'Italia ha raggiunto il 6° posto come diffusione di ransomware a livello mondiale con il 2,49%, e nel 2014 il 10° con il 1,85%.
A livello di malware "specialistici" particolarmente significativi, anche in Italia, quelli per home banking, commercio elettronico e PoS, Point of Sale. Nei primi due ambiti hanno avuto una forte diffusione i vari derivati da Zeus già citati, diffusione frenata fortemente dal riuscito blocco della rete GameOver Zeus botnet[21]. I PoS malware più diffusi, a livello mondiale, includono BlackPoS, Soraia, Alina, Rdasrv. Secondo la citata indagine Trend Micro, nel 2014 l'Italia è stata seconda a livello mondiale come diffusione.

4.3.1.1 Heartbleed

Heartbleed è una vulnerabilità nelle librerie software[22] di crittografia largamente usate per implementare OpenSSL con l'estensione Heartbeat. OpenSSL è il programma opensource per il protocollo di autenticazione e cifratura TSL[23] che consente di crittare i dati in transito tra il browser ed il server web con HTTPS, usato tipicamente per l'home-banking, pagamenti sicuri di e-commerce, ecc. OpenSSL non solo critta i dati in transito, ma protegge lo scambio di password e di certificati elettronici per l'autenticazione degli interlocutori. L'estensione Heartbeat (da cui deriva il nome della vulnerabilità) per i protocolli TLS e DTLS, Datagram TLS, consente di testare e mantenere attiva la comunicazione crittata senza dover rinegoziare ogni volta i parametri ed i certificati relativi. L'estensione è standardizzata con RFC 6520[24] da febbraio 2012, ed è praticamente usata in ogni implementazione di OpenSSL. Dato che i protocolli TSL/SSL costituiscono il cuore della sicurezza delle comunicazioni in Internet, la vulnerabilità Heartbleed è realmente grave e di conseguenza ha avuto vasta eco. OpenSSL è usabile ed è usato non solo per PC e server, con i diversi sistemi operativi, da Windows a Linux e a MAC OS, ma anche su tablet e smartphone con gli specifici sistemi operativi quali Android e iOS. Si stima che OpenSSL versione 1.0.1 sia stata usata, e forse è tutt'ora usata, da circa due terzi dei siti Internet del mondo, e che quindi circa mezzo milioni di siti o più fossero, e forse tuttora lo sono, vulnerabili.
Heartbleed è identificata e classificata nella banca dati delle vulnerabilità come CVE-2014-0160[25] e consente ad un attaccante di catturare informazioni riservate, quali identificativi d'utente, password, certificati elettronici, numeri di carte di credito, che sono scambiati sul collegamento HTTPS. I rischi principali riguardano tipicamente siti web, webmail, social network, sistemi di telefonia IP e server di comunicazione e messaggistica, unità di storage, VPN, firewall e sistemi embedded, tipici dell'Internet delle cose . Ma possono riguardare anche i dispositivi d'utente, PC-tavolette-smartphone, con la versione bacata di OpenSSL.
Il baco nel software permette un attacco di tipo "buffer

[19] Bash è una delle shell di comando (frequentemente usate) per i sistemi operativi Linux, Unix ed Apple OS X. Può anche essere utilizzato per invocare degli script
[20] http://www.trendmicro.it/media/misc/rpt-vulnerabilities-under-attack.pdf
[21] http://www.webnews.it/2014/06/03/fbi-e-microsoft-smantellano-gameover-zeus/
[22] Le librerie di OpenSSL coinvolte con questa vulnerabilità sono d1_both.c e t1_lib.c
[23] TSL, Transport Layer Security, è il protocollo che ha sostituito il precedente SSL, Secure Sockets Layer, tuttora diffuso
[24] http://tools.ietf.org/html/rfc6520
[25] http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160

over-read", che consente di leggere i dati da un buffer di memoria del computer al di là dei confini che dovrebbe avere, leggendo così i dati adiacenti che non dovrebbero e potrebbero essere letti ed usati. I bachi sono stati eliminati con il rilascio della nuova versione OpenSSL, ma tutti gli ambienti, sia server che client, che utilizzano ancora la versione 1.0.1 sono a rischio.

4.3.1.2 Antivirus insicuri

Come mostrato in fig. 4-5 e 4-6 i virus ed i codici maligni costituiscono il più diffuso attacco, ed i software antivirus rappresentano uno dei principali mezzi di contrasto, a loro volta assai diffusi come indicato in fig. 6-4. Non sempre e non tutti i prodotti antivirus e simili sul mercato sono tempestivamente aggiornati ed efficaci, ma soprattutto alcuni non sono sicuri e le loro vulnerabilità (come quelle di ogni software vulnerabile) possono essere sfruttate per portare attacchi.

Una recente indagine[26] tratta delle prestazioni degli antivirus in termini di virus che sono in grado di individuare, soprattutto quelli più recenti e quelli "camuffati". Sono stati esaminati 51 prodotti antivirus in commercio, e si è scoperto che solo una parte, e via via decrescendo come numero, era in grado di individuare i virus ed eventuali loro camuffamenti: addirittura solo 3 su 51 sono riusciti ad individuare Meterpreter shell packed con Veil-Evasion[27]. Ancor più preoccupante il fatto che questa analisi è stata ripetuta, con gli stessi prodotti antivirus ovviamente aggiornati, l'anno successivo in presenza di nuovi virus. Miglioramenti ci sono stati, ma nel complesso circa la metà degli antivirus non è stata capace di individuare nuovi virus e/o quelli opportunamente nascosti.

4.3.2 Il rischio Malvertising

Il termine Malvertising sta per "malicious advertisements", ossia pubblicità malevola, nel senso di pagine web che nascondono un codice maligno o altre tecniche di attacco, come il dirottamento su siti web mascherati e pericolosi. Il rischio malvertising è quello che più cresce ed il meno noto a livello mondiale, anche grazie a leggi diverse nei vari stati e, più in generale, ad una scarsa sorveglianza complessiva sulla pubblicità in Internet. Nel 2014 esso ha avuto una crescita esponenziale, ed è stato la causa di varie frodi e furti d'identità digitale. Secondo un'indagine della californiana RiskIQ[28], nel solo 3 trimestre 2014 negli US sono stati identificati ben 200.000 malvertising, le cui tre più diffuse tecniche di attacco erano: falsi aggiornamenti software (80.000), codici maligni (>70.000), falsi antivirus (quasi 40.000).

4.3.3 Targeted Attack e Advanced Persistent Threat

Negli ultimi anni il trend degli attacchi si è sviluppato su due principali direttrici:

- attacchi massivi relativamente semplici su grandi quantità di interlocutori; tipici esempi il "phishing" e le infezioni virali;
- attacchi mirati (TA, Targeted Attack): sono rivolti ad uno specifico obiettivo, o ad un limitato numero di obbiettivi, e basati sull' uso di più strumenti di attacco; gli APT possono essere considerati un loro sottoinsieme, caratterizzati dall'uso di tecniche di attacco sofisticate, "advanced", e "persistenti". ossia che si inseriscono e si nascondono nei computer, analizzando le possibili vulnerabilità ed sfruttandole con gli strumenti più opportuni. TA e APT rappresentano più una metodica di attacco che una singola tipologia di attacco, e richiedono grandi competenze e risorse per essere realizzate, sconfinando nelle logiche di guerra informatica.

Come evidenziato in Tabella 3, nel 2014 questi attacchi sono cresciuti anche in Italia, ma altri sono i paesi a più alta diffusione: il primo, secondo una recente indagine[29] di Trend Micro, è Taiwan con il 62%, secondo il Giappone con 22%, terzo gli Stati Uniti con un 5%; seguono altri paesi con percentuali dell'1% o inferiori. Sempre la stessa

[26] Ken Munro: "Turning the Tables on Antivirus" , ISSA Journal, Ottobre 2014. Issa Journal è riservata ai Soci ISSA, tra i quali rientrano i Soci AIPSI, capitolo italiano di ISSA

[27] Meterpreter è uno strumento all'interno del Metasploit Framework, uno dei più diffusi meta exploit sul mercato: fornisce il payload avanzato, ossia il run time del malware, estendibile in modo dinamico, che utilizza solo la memoria del sistema e si estende attraverso la rete in fase di esecuzione. Il "reverse shell" richiede inizialmente all'attaccante di porre il suo sistema in ascolto (ossia come listener), cui il sistema target si collega come un client. Gli "exploit" sono programmi che consentono di sfruttare una vulnerabilità. I "meta-exploit" sono strumenti che facilitano la creazione di exploit

[28] http://www.riskiq.com/

indagine indica come la prevalenza di questi attacchi sia indirizzata ai sistemi informatici di pubbliche amministrazioni ed enti governativi (81%), seguita dal settore ICT (4%) e dagli altri settori merceologici con valori percentuali decrescenti.

4.3.3.1 Gli attacchi Watering Hole

Il termine di "watering hole attack", traducibile in" attacco alla pozza d'acqua", fa riferimento agli agguati di animali carnivori alle prede che si dissetano in una pozza d'acqua. Questa è una chiara metafora di un attacco informatico mirato a utenti, le prede, che accedono e navigano in determinati siti web, tipicamente di organizzazioni molto influenti ed autorevoli. Il predatore, sapendo che in quel sito la preda andrà, e probabilmente in determinati giorni, l'aspetta con le proprie armi per... divorarla.
Questo tipo di attacchi, logicamente inclusi tra i TA/APT, si focalizzano su specifiche tipologie di utenti e di programmi, ben noti agli attaccanti. Questi ultimi si concentrano tipicamente su siti web usati per i loro contenuti da un numero di utenti relativamente limitato e dagli interessi specifici: utenti che per la loro posizione e ruolo hanno informazioni riservate e spesso significative capacità economiche, e che pertanto sono di forte interesse per gli attaccanti. Una volta connesso al sito già manipolato dall'attaccante, il browser, il dispositivo dell'utente (dal PC al lap top, dalla tablette allo smartphone) e la sessione con il sito web sono a loro volta attaccati per carpire informazioni dell'utente, tipicamente le sue identità digitali utili a compiere frodi. Acquisite le informazioni, normalmente vengono cancellate le tracce dell'attacco stesso.

4.3.4 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, ai sistemi di controllo industriali (DCS, Distributed Control System), ai sistemi automatizzati, ai sistemi robotizzati. Fin dal 2007-8 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 tra i 30 ed i 50 Miliardi di IoT connessi. 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[30], PLC[31]), 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.
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. Il Rapporto HP 2014 su

[29] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-vulnerabilities-under-attack.pdf
[30] DCS, Distributed Control System
[31] PLC, Programmable Logic Controller

IoT[32] indica che il 70% degli oggetti ha attualmente gravi vulnerabilità, e che l'80% ha password troppo deboli: spesso vengono lasciate quelle di default pre configurate nel dispositivo (es: password 0000 su Bluetooth). Questo rapporto HP si basa sulla recente analisi OWASP[33] sui 10 più usati dispositivi nel mondo IoT, che ha rilevato 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. 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.

4.3.5 La situazione a livello europeo secondo ENISA

L'annuale rapporto ENISA Threat Landscape Report 2014[34] fornisce una classifica delle principali minacce in Europa occorse nel 2014.

La Tabella 9, elenca le principali minacce individuate come più critiche per le aree emergenti dell'ICT: cyber sicurezza fisica, sistemi mobili, cloud computing, infrastrutture critiche, big data, Internet delle cose, virtualizzazione delle reti. reti sociali (social networking).

Nella Tabella la freccia verticale verso l'alto indica una prospettiva di crescita della minaccia, verso il basso una decrescita; la freccia orizzontale indica che la minaccia è stabile. La mancanza di freccia indica che la minaccia non è significativa o pertinente per l'area emergente considerata.

La tipologia di minacce considerate differisce da quelle usate in OAI e riportate in Tabella 1.

La Tabella 10 confronta la classifica ENISA con quella OAI per il 2014. A fianco del nome della minaccia ENISA in parentesi graffa è indicato il nome (o più nomi) della tipologia di attacco OAI 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; era indicato nelle precedenti edizioni come Drive-by Downloads. La cor-

			Aree emergenti						
Classifica ENISA 2014	**Minacce (Top Threats)**	**Attuale Trend**	**Cyber-Physical Systems and CIP**	**Mobile Computing**	**Cloud Computing**	**Trust Infrastr.**	**Big Data**	**Internet delle cose**	**Netw. Virtualisation**
1	*Malicious code: Worms/Trojans*	↑	↑	↑	↑	↑		↑	↑
2	*Web-based attacks*	↑	↑	↑	↑	→		↑	
3	*Web application attacks /Injection attacks*	↑	↑	↑	↑	↑		↑	↑
4	*Botnets*	↙		↑	↑				
5	*Denial Of Service*	↑	↑		→	→		↑	↑
6	*Spam*	↙	↑						
7	*Phishing*	↑		↑		↑	↑	↑	↑
8	*Exploit kits*	↙		↑		↑		↑	
9	*Data Breaches*	↑			↑		↑		↑
10	*Physical damage/theft /loss*	↑	↑	↑		↑	↑	↑	↑
11	*Insider threat*	→	↑		↑		↑	↑	↑
12	*Information Leakage*	↑	↑	↑	↑	↑	↑	↑	↑
13	*Identity theft/fraud*	↑	↑	↑	↑	↑	↑	↑	↑
14	*Cyber espionage*	↑	↑		↑	↑	↑		↑
15	*Ransomware/Rogueware/Scareware*	↙		↑					

Legenda dei trend :

↑	In crescita
→	Stabile
↙	In diminuzione

Tabella 9 Le principali minacce ICT in Europa secondo il Rapporto ENISA 2014

[32] http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en
[33] https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project
[34] https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014

Minacce (Top Threats)	Classifica 2014 ENISA	Classifica 2014 OAI
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	3
Spam {saturazione risorse}	6	3
Phishing {social engineering}	7	2
Exploit kits {sfruttamento vulnerabilità}	8	7
Data Breaches {sfruttamento vulnerabilità}	9	7
Physical damage/theft /loss {attacchi sicurezza fisica}/{furto dispositivi}	10	14
Insider threat	11	NS
Information Leakage {Furto di informazioni da mobile e non}	12	9/13
Identity theft/fraud {Furto di informazioni da mobile e non }/{Frodi informatiche}	13	9/13/8
Cyber espionage	14	8
Ransomware/Rogueware/Scareware {ricatti}	15	5

Tabella 10 Confronto tra le classifiche ENISA ed OAI 2014

rispondenza con OAI 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. Esso può svolgere attacchi intenzionali o non con le più varie modalità e tecniche, e per questo motivo nella Tabella 10 si è posto un NS, Non Significativo.

Dalla Tabella 10 emerge che il confronto è difficile per le diverse tipologie usate da ENISA e da OAI, ed anche dal fatto che il concetto di "minaccia" è diverso e meno tecnico di quello di "attacco": ma emerge che il malware è in testa anche alla classifica europea. La più forte differenza è data dai ricatti e dal ransomware, che in Italia hanno fatto un balzo in avanti significativo rispetto al 2013.

5. L'INDIVIDUAZIONE E LA GESTIONE DEGLI ATTACCHI

La fig. 5-1 mostra, per il campione dei rispondenti, la provenienza delle segnalazioni di un attacco (risposte multiple): le segnalazioni arrivano per il 22,3% dai sistemi di monitoraggio e controllo, ivi inclusi i sistemi di "intrusion prevention" e "detection" (IPS/IDS), e a decrescere dall'analisi dei dati raccolti, dall'evidenza del danno subito, dall'analisi e correlazioni dei dati raccolti. Nessuno dei rispondenti ha indicato segnalazioni di attacchi da utenti esterni o da fornitori, che si accorgono di malfunzionamenti e/o di dati scorretti e li segnalano. I pochi che hanno selezionato anche "Altro" non hanno dettagliato il che cosa. Per questi si può ipotizzare come motivazione che l'azienda faccia parte di una holding internazionale, e che la segnalazione dell'attacco sia arrivata da quest'ul-

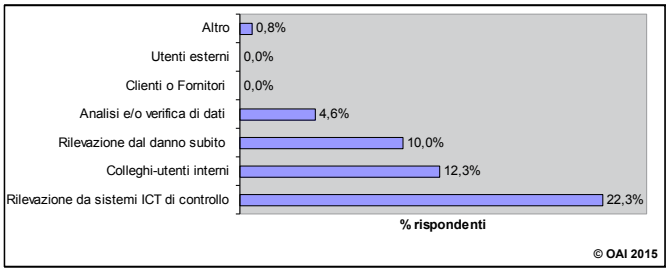

Fig. 5-1 Da chi sono pervenute le segnalazioni degli attacchi (risposte multiple)

[35] si veda http://www.poliziadistato.it/articolo/23393/

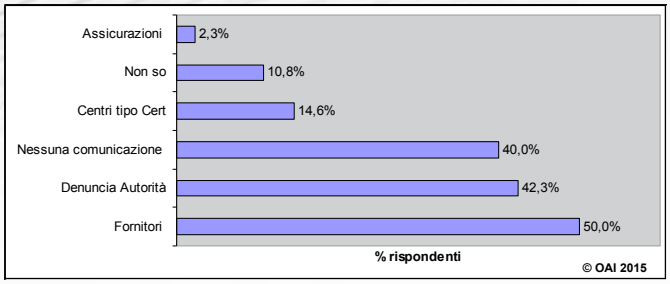

Fig. 5-2 Comunicazione all'esterno dell'avvenuto attacco (risposte multiple)

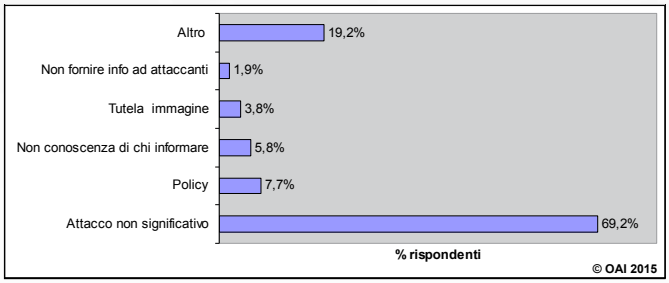

Fig. 5-3 Motivazioni per la "non comunicazione" all'esterno dell'attacco (risposte multiple)

tima. 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), la metà dei rispondenti che hanno subito attacchi lo comunica ai propri Fornitori affinché intervengano ed il 42,3% avvisa le competenti autorità (solitamente la Polizia Postale e delle Comunicazioni[35]) ma sempre un'alta percentuale, il 40%, non lo comunica affatto. Questi dati sono profondamente diversi da quelli emersi nella precedente edizione, dove la maggior parte dei rispondenti non comunicava affatto, e solo il 20% circa lo comunicava alle autorità preposte. Al di là della differenza del mix e del numero di rispondenti tra le due edizioni, questi nuovi dati lasciano presagire un nuovo positivo orientamento culturale sulla sicurezza informatica. Gli attacchi informatici non rappresentano un'infamia professionale e non devono essere nascosti e, pur con l'adeguata riservatezza, è bene siano comunicati alle autorità, che così possono disporre di un più aggiornato e consistente quadro della cyber criminalità sul territorio. Più del 10% 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 sua volta informato. Solo il 2,3% informa l'assicurazione con la quale ha stipulato un contratto: una percentuale stranamente bassa, se confrontata al 19,1% dei rispondenti in fig. 6-9 che dichiarano di avere assicurazioni per il rischio (residuo) informatico.
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 centri: 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 emerge la necessità di seguire le policy. La tutela dell'immagine, come motivazione, ha solo un 3,8% (rispetto al 10% della passata edizione). Un numero non trascurabile di rispondenti ha anche selezionato "Altro", ma senza specificare la motivazione, a parte uno che ha spiegato che, essendo il sistema informatico centralizzato all'estero, questo tipo di comunicazioni è effettuato centralmente dalla holding.
A seguito di un attacco, oltre alle eventuali segnalazioni di cui sopra, sono intraprese varie azioni, sia tecniche sia organizzative e legali, sintetizzate nella fig. 5-4. 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'acquisizio-

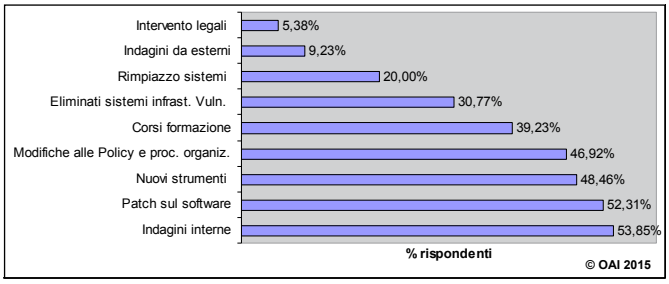

Fig. 5-4 Azioni dopo un attacco (risposte multiple)

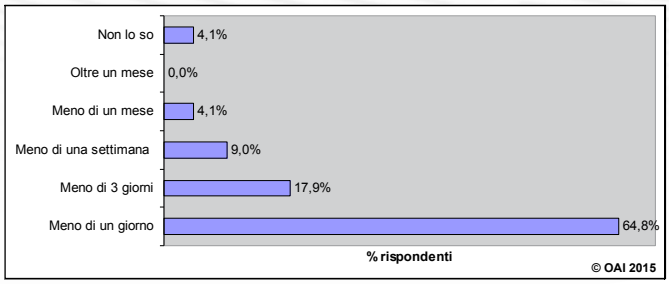

Fig. 5-5 Tempi medi di ripristino dopo un attacco

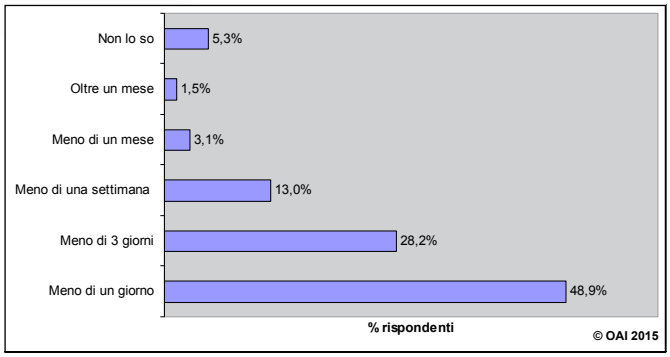

Fig. 5-6 Tempi massimi di ripristino (caso peggiore nell'anno)

ne di ulteriori nuovi strumenti di prevenzione e protezione, e l'aggiornamento-miglioramento delle policy in atto. A decrescere poi gli altri interventi, tra cui, con percentuali non trascurabili, il miglioramento della sensibilizzazione e l'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 forse conto anche della durata dei processi.

Per quanto riguarda i tempi di ripristino a seguito di un attacco, la fig. 5-5 mostra, per i tempi medi, che nella maggior parte dei casi la situazione "ante" è ripresa in meno di un giorno, e complessivamente in quasi l'83% dei casi la situazione è ripristinata entro 3 giorni dall'attacco.

Gli attacchi più gravi possono richiedere ben più tempo, ma tutti sono stati risolti entro un mese dall'occorrenza. Questi dati sono confermati dai tempi "massimi" occorsi nei casi peggiori di ripristino, illustrati nella fig. 5-6. Anche nei casi peggiori, la metà circa viene ripristinata entro 1 giorno, e solo il 1,5% richiede oltre il mese. Come evidenziato anche nella passata edizione, questi tempi indicano da un lato che gli strumenti di prevenzione, protezione e ripristino sono ora più diffusi e più efficaci (si veda §6), 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 e dalle fig. 4-7 e 4-8.

Gli attacchi segnalati che hanno richiesto i tempi di ripristino più lunghi includono:

- attacchi DNS continuativi
- virus diffuso via allegato email
- ripristino totale del laptop
- furto di un access point wifi
- ripristino telefonia
- attacco al sito Internet sfruttando una vulnerabilità di un componente del CMS[36]
- DoS e DDoS
- CriptoLocker
- CBT-Locker
- KeyLock
- perdita di informazioni dal sito web aziendale.

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 A, il seguente capitolo illustra la tipologia di strumenti di sicurezza in uso, a livello sia tecnico sia organizzativo, per poter meglio comprendere e valutare gli attacchi rilevati ed i relativi impatti.

6.1 SICUREZZA FISICA

La fig. 6-1 schematizza le principali misure in uso per la protezione "fisica" dei Data Center, delle "computer room"[37] o di qualsiasi luogo ove sono installate risorse

[36] CMS, Content Management System

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

ICT. Gli strumenti più usati (> 70%) 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 che di 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. Una percentuale leggermente inferiore, ma significativa, effettua controlli degli accessi delle persone fisiche tramite reception, bussole, lettori di badge, ed altri strumenti, fino al riconoscimento biometrico. Quasi un ¼ dei rispondenti non ha di fatto alcuna misura di sicurezza fisica dei locali ove sono contenuti i sistemi ICT, a parte la loro chiusura con serrature sulle porte di accesso è il tipico caso delle piccolissime aziende, degli studi professionali, dei piccoli laboratori artigianali. Tale dato è corretto se confrontato con le dimensioni delle organizzazioni (si veda fig. A-3 nell'Allegato A.1). Nella voce "Altro" alcuni rispondenti hanno riportato la separazione "fisica" in locali diversi, anche geograficamente, dei sistemi ridondati contenenti dati critici. Quelli che hanno tutti i servizi ICT terziarizzati o in cloud, utilizzano le misure di sicurezza fisica dei Fornitori.

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, ed 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, 81,5%, è la consueta coppia identificatore utente - password, assieme agli strumenti di controllo degli accessi dell'utente, 71,7%: strumenti che vanno dall' Active Directory di Microsoft all'LDAP, usato prevalentemente negli ambienti Linux/Unix, dalle ACL, Access Control List ai Policy Server, e così via. Grazie alla spinta della PEC, Posta Elettronica Certificata, oltre all'uso delle CRS, Carta Regionale dei Servizi e nelle Pubbliche Amministrazioni, i certificati digitali raggiungono il 3° posto, con 1/3 circa dei rispondenti che li adottano. Le piattaforme PKI, Public Key Infrastructure, sono necessarie per erogare servizi basati sui certificati digitali. Le tecniche di SSO, Single Sign One, crescono con una copertura del 30%. Altri meccanismi considerati, dall'uso di "token" quali chiavi USB, smart card, dispositivi OTP (One Time Password, di crescente diffusione nell'ambito bancario) fino all'uso di Captcha sulle pagine web per assicurarsi che l'utente sia una persona e non un programma, hanno percentuali più basse ma non trascurabili. L'identificazione biometrica nell'attuale indagine ha avuto un valore percentuale molto basso, 1,7%, considerando le percentuali delle precedenti edizioni (6,3%, 6,2% ,2,52%).
Il motivo, secondo l'autore, è dato dal campione di rispondenti, prevalentemente in ambito industriale e dei servizi, e con una ancor troppo limitata partecipazione di banche, assicurazioni ed istituti finanziari. Sono soprattutto questi ultimi che in Italia hanno o stanno iniziando ad usare tecniche biometriche soprattutto per l'uso della grafometria che permette la digitalizzazione e la gestione totalmente informatica dei documenti firmati.

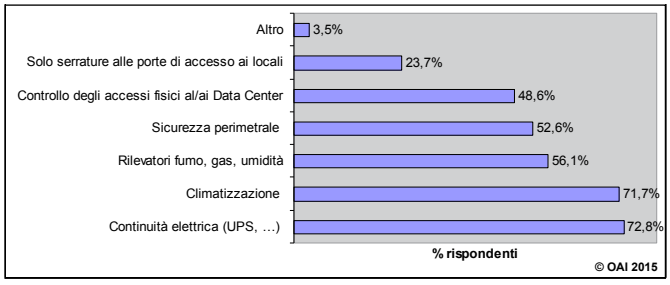

Fig. 6-1 Strumenti sicurezza "fisica" in uso (risposte multiple)

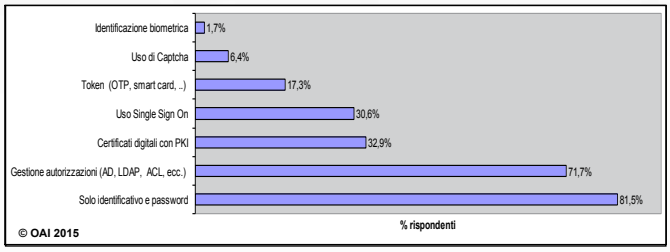

Fig. 6-2 Strumenti per l'identificazione, l'autenticazione e l'autorizzazione (risposte multiple)

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, più dei 3/4 dei rispondenti è dotato di dispositivi firewall e di DMZ, DeMilitarized Zone, e quasi il 65,9% dichiara di utilizzare 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", ecc.
Il 38,7%, rispetto al 27,5%, della passata indagine, ha potenziato il livello di sicurezza delle reti wireless, che possono presentare serie vulnerabilità se non correttamente protette. Una piccola percentuale, il 5,2% (rispetto al precedente 8,5%), non è al momento dotata di alcuna specifica protezione per le reti: è il caso probabilmente per piccoli e piccolissimi sistemi informatici.
Nella voce "Altro" sono state segnalate reti geografiche "dedicate".
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

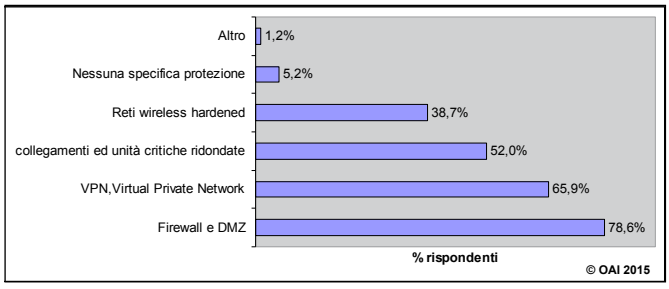

Fig. 6-3 Strumenti sicurezza logica in uso per le reti (risposte multiple)

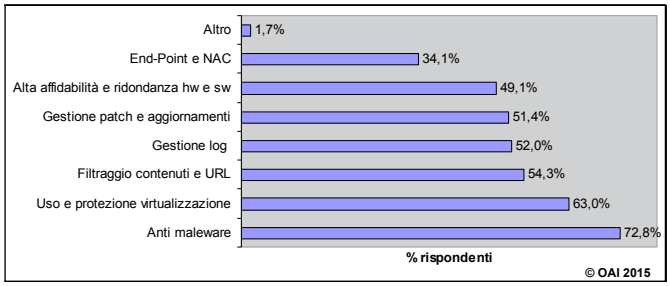

Fig. 6-4 Strumenti sicurezza logica in uso per i sistemi (risposte multiple)

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. 4-5 e 4-6): sono usati nel 2014 dal 72,8% dei rispondenti, rispetto al 70,4%, 80,2%, 97% e 95% delle scorse edizioni dell'OAI. Le differenze percentuali negli anni dipendono, come più volte sottolineato, dal differente bacino di rispondenti, ma il dato che può sconcertare è che non tutti usano software antimalware, in particolare anti virus, anti spyware, ecc. Nelle due ultime edizioni OAI più di 1/4 dei rispondenti non usava questi software di protezione. In effetti alcuni esperti di sicurezza ICT preferiscono non usare antivirus e simili, in particolare in ambito Linux, poiché ritengono che penalizzino le prestazioni dei sistemi più che proteggerli, e che comunque, in caso di attacco da malware, siano necessari interventi specifici da parte di specialisti. Al secondo posto gli strumenti di protezione degli ambienti virtualizzati, con un 63%, significativo indice della loro diffusione, in linea con le caratteristiche dei sistemi informatici di cui all'Allegato A.2. Al terzo posto gli strumenti di filtraggio dei contenuti e delle URL, usati dal 54,3% del campione: una posizione raggiunta sia grazie 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. Il 52% gestisce i log, e sicuramente questa forte diffusione deriva anche dall'obbligo di essere conformi alla normativa sugli amministratori di sistema per la privacy. La gestione delle patch e degli aggiornamenti si posiziona al quinto posto con un 51,4%. Un dato preoccupante: quasi la metà dei rispondenti non aggiorna sistematicamente con le opportune patch 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, dovuto anche dal 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! Quasi la metà dei rispondenti, 49,1%, dichiara di disporre di architetture e sistemi ad alta affidabilità, Un terzo del campione, 34,1%, utilizza strumenti (tipicamente software) di sicurezza End-Point ed i NAC, Network Access Control. Tale percentuale conferma

l'attenzione a controllare "prima dell'accesso" l'identità dell'utente e quanto sia sicuro il dispositivo d'utente da cui chiede l'accesso, tenendo anche conto della diffusione dei sistemi mobili e del fenomeno del BYOD che richiede specifici controlli ed attenzione (si veda anche fig. A-10 e §A.2). I pochi che hanno selezionato "Altro" non hanno indicato quali altri strumenti utilizzano.

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 ed illustrati nella precedente fig. 6-2. Gli strumenti più diffusi, 61,3%, sono i firewall ed i reverse proxy posti a difesa dei server applicativi, dei data base server, e dei sistemi di storage. Al secondo posto si posizionano le linee guida per lo sviluppo di codice software sicuro, normalmente fornite agli sviluppatori interni e/o esterni; in quest'ultimo caso fanno spesso parte del contratto per lo sviluppo. Ma l'effettivo controllo che il software risultante sia realmente sicuro scende ad un 17,9%. Questo significa che quasi la metà delle linee guida emesse, magari ben dettagliate, rimane un puro invito o una precauzione "burocratica", cui non segue alcun effettivo controllo. Poco più di 1/5 non dispone al momento di strumenti per la sicurezza applicativa, e l'8% dichiara che sono in corso progetti o analisi di fattibilità per dotarsi di strumenti per la sicurezza applicativa. I pochi che hanno segnalato anche "Altro" non hanno specificato quali ulteriori strumenti utilizzino.

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 56,6%, 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.

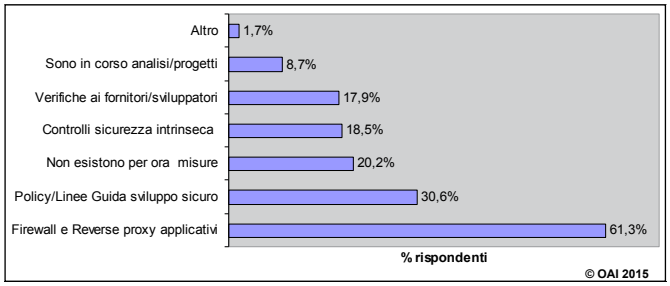

Fig. 6-5 Strumenti in uso per la sicurezza logica degli applicativi (risposte multiple)

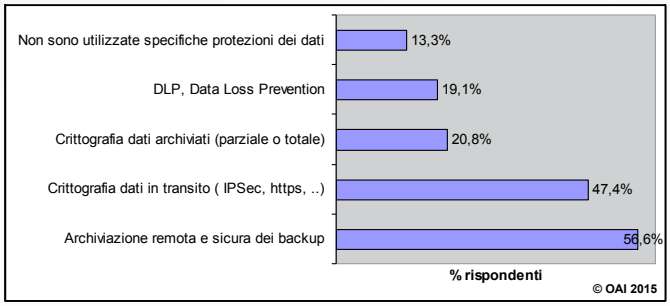

Fig. 6-6 Strumenti in uso per la sicurezza logica delle informazioni (risposte multiple)

Un secondo strumento 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 si riduce al 20,8% dei rispondenti, e con una percentuale di poco inferiore l'uso di strumenti DLP, Data Loss Prevention. Una percentuale non trascurabile di quasi il 13,3% 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. Ed i data breach del 2014 confermano che il problema non è solo italiano.

6.3 GLI STRUMENTI PER LA GESTIONE DELLA SICUREZZA DIGITALE

La fig. 6-7 mostra i principali strumenti di gestione della sicurezza ICT utilizzati in percentuale sull'intero campione e con risposte multiple: la gestione della sicurezza informatica é l'elemento determinante per potere garantire un livello realmente idoneo e proattivo di protezione al si-

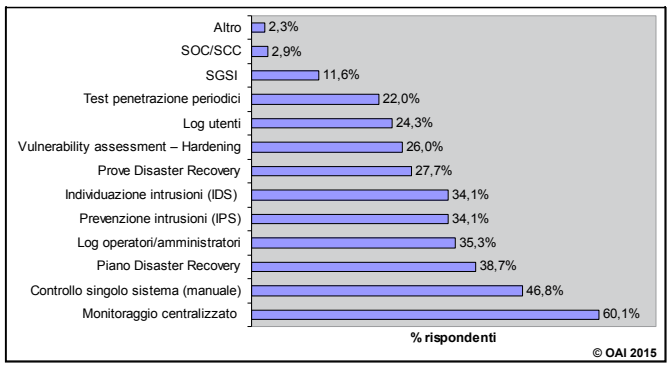

Fig. 6-7 Strumenti in uso per la gestione della sicurezza ICT (risposte multiple)

stema informatico. I dati emersi sono simili a quelli delle precedenti edizioni.
Il monitoraggio e il controllo centralizzato delle funzionalità e delle prestazioni dei sistemi ICT sono in vari modi attuati dal 60,1% dei rispondenti. Il 46,8% 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.
I piani di Disaster Recovery, ora facilitati dall'utilizzo del cloud, sono effettuati dal 38,7% del campione, ma solo il 27,7% 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.
La gestione dei log degli amministratori ed operatori di sistema, con il 35,3%, ha un peso non trascurabile, ma quasi i 2/3 dei rispondenti non la effettua, così come invece richiesto dalla normativa per la privacy. Il 24,3% effettua il log degli utenti, ed i due dati sono a grandi linee congruenti con il valore di 52% emerso come strumento di difesa dei sistemi (fig. 6-4). Si deve tener conto che molti strumenti di difesa possono svolgere anche funzioni di gestione, a secondo delle modalità del loro utilizzo (ed anche funzioni di attacco). Come strumenti per la gestione della sicurezza un ruolo importante è dato dai sistemi IPS/IDS, Intrusion Prevention System/Intrusion Detection System, entrambi usati da più di 1/3 dei rispondenti. Più di ¼ di loro effettua sistematiche analisi delle vulnerabilità (vulnerability assessment) con scansioni delle reti e dei sistemi, ed il 22% effettua prove di attacco (penetration test) per saggiare la tenuta degli strumenti di sicurezza in essere. Percentuali decisamente inferiori per l'utilizzo di sistemi integrati e centralizzati per gestire la sicurezza ICT (SGSI, Sistema Gestione Sicurezza Informatica), e per SOC, Security Operation Center, o SCC, Security Command Center. Queste sono soluzioni tipiche per grandi realtà di fornitori, in particolare di telecomunicazioni e di servizi ICT, che vengono anche offerte in sourcing per realtà più piccole. Un aspetto fondamentale nella gestione della sicurezza ICT è la sistematica e periodica analisi dei rischi. Come evidenziato nella fig. 6-8, solo un ¼ circa dei rispondenti afferma che tale analisi viene effettuata, ma un 22% (rispetto al 9,8% della scorsa edizione) intende effettuare l'analisi dei rischi nel prossimo futuro.
La fig. 6-9 mostra che il 19,1 % dei rispondenti ha già in essere forme assicurative sul rischio informatico, e che il 5,2% prevede di dotarsene nel prossimo futuro.

6.4 LE MISURE ORGANIZZATIVE

Gli aspetti organizzativi sono determinanti per la realizzazione di una effettiva ed efficace sicurezza informatica: aspetti talvolta trascurati, anche perché considerati da alcuni 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 informatica 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 hanno dato e stanno dando i loro frutti.
La fig. 6-10, con risposte multiple, mostra il quadro delle principali misure organizzative in uso.

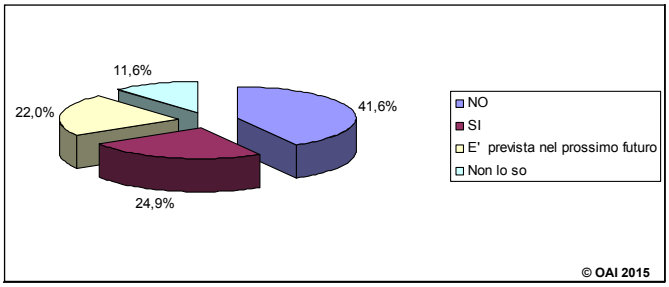

Fig. 6-8 Effettuazione analisi dei rischi ICT

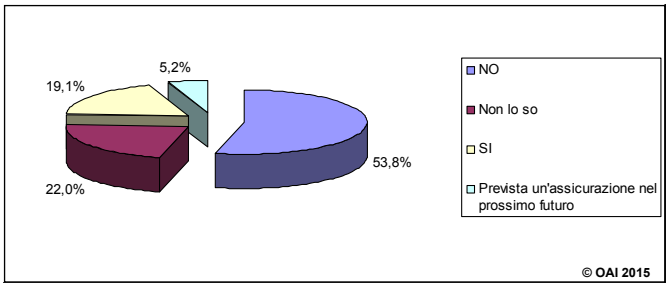

Fig. 6-9 Assicurazione rischio residuo

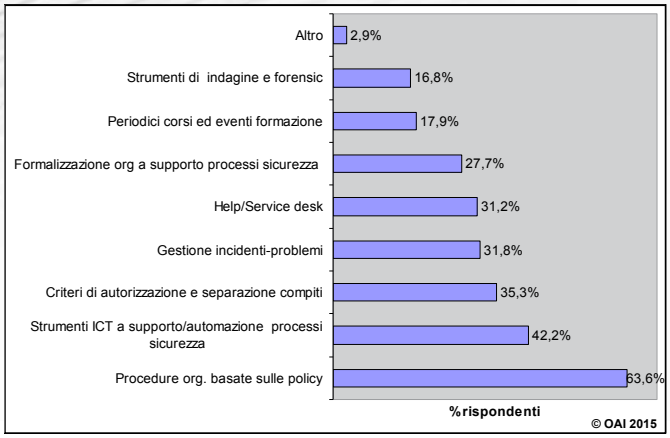

Fig. 6-10 Principali contromisure organizzative (risposte multiple)

Il 63,62% utilizza procedure organizzative in merito alla sicurezza informatica, definite nell'ottica delle policy emanate. Il 42,2% (rispetto al 31,6% della scorsa edizione) utilizza strumenti informatici per il supporto e l'automazione, parziale o totale, dei processi per la sicurezza ICT, quali sistemi di work-flow, di correlazione tra gli allarmi, di trouble ticketing, banche dati e sistemi "smart" a supporto dell'help-desk, ecc. Il 35,3% ha definito ed usa criteri di autorizzazione nell'uso delle risorse ICT in funzione dei ruoli e dei compiti delle varie figure, tenendo conto della necessità di ben separare le singole responsabilità, indicata spesso con l'acronimo inglese SoD, Separation of Duties. Con percentuali molto simili attorno al 31% vengono usate specifiche procedure per la gestione degli incidenti, dei problemi e dell'help desk. Il 27,7% ha formalmente definito attività, procedure e ruoli a supporto dei processi di sicurezza ICT: l'aspetto "formale" indica che sono (o stanno per essere) certificati ISO 27000, COBIT e/o ITIL. Meno di 1/5 attua periodici corsi ed eventi per la sensibilizzazione, formazione e addestramento di utenti e di specialisti ed il non trascurabile 16,8% ha ed utilizza strumenti di indagine e di "analisi forensic". Con la risposta "Altro" è stata specificata la misura organizzativa di impedire l'accesso al Data Center/Computer room dalle 17 alle 8 del giorno dopo.

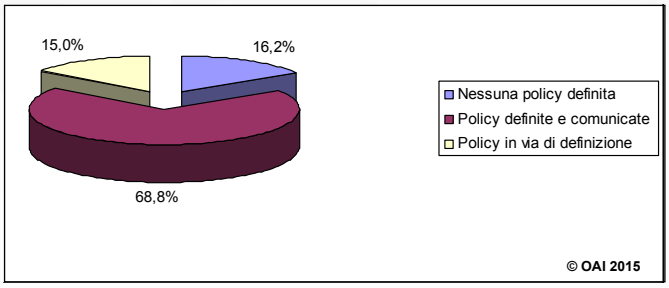

Fig. 6-11 Esistenza policy sulla sicurezza informatica

Data l'importanza di una policy sulla sicurezza ICT, che logicamente dovrebbe essere un di cui della più generale policy ICT, nel Questionario 2014 si sono volutamente poste due esplicite domande sulla sua presenza. La risposta è mostrata nella fig. 6-11, dove ben il 68,8% dichiara di avere una policy per la sicurezza ICT, ed il 15% di avere la policy in corso di definizione. Questi dati sono nella sostanza congruenti con quelli della fig. 6-10.
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.

6.4.1 Conformità a standard e a "buone pratiche"

Un concreto ausilio nell'organizzazione della sicurezza ICT può venire da 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 v3 e l'ISO 20000[38] per la gestione operativa dell'ICT, l'ISO 9001 per la gestione della qualità dei servizi, ecc[39].
Tali standard e best practice possono essere adottati formalmente, ossia certificandosi, o informalmente all'interno delle proprie strutture, e possono essere richiesti ai forni-

[38] ISO 20000 standardizza logiche e processi di ITIL
[39] 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 .

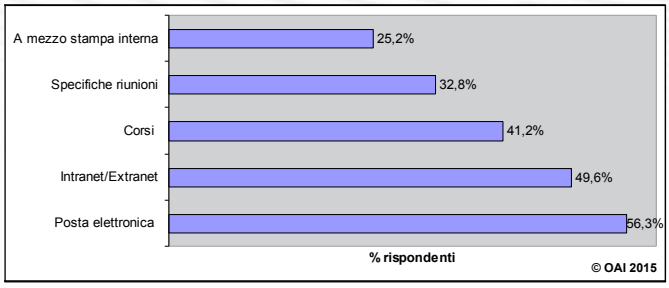

Fig. 6-12 Comunicazione e diffusione delle policy (risposte multiple)

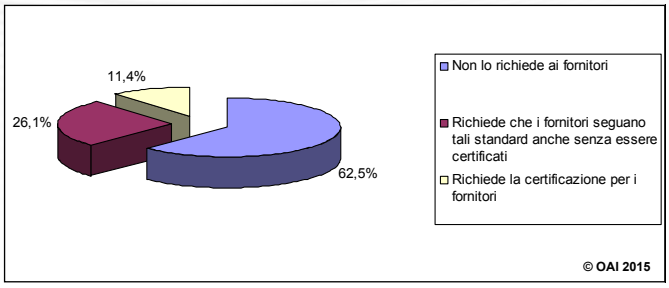

Fig. 6-14 Conformità dei Fornitori alla famiglia ISO 27000

tori e ai provider 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 su tutti gli standard di 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 che dovrebbero essere svolti. La certificazione ad uno di questi standard è normalmente a livello dell'azienda/ente, ma può essere fornita a livello della singola persona. La figura mostra che il 37,6%, non è interessato o non ritiene necessario seguire tali standard nel proprio contesto, ma il 26,5% già li segue de-facto pur senza essere certificata, e che in tale ottica il 14,5% intende seguirli nel prossimo futuro. Il 12% è già certificato, rispetto al 6,6% della scorsa edizione, ed il 9,4 intende farlo. Come mostrato nella fig. 6-14, l'11,4% del campione richiede ai propri fornitori la certificazione nell'ambito ISO 27000, mentre il 26,1% (contro il 13,2% della scorsa edizione) richiede loro di seguire in pratica tali standard pur senza essere certificati.

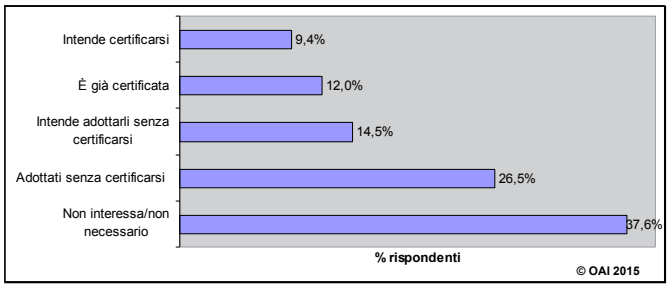

Fig. 6-13 Adozione standard famiglia ISO 27000

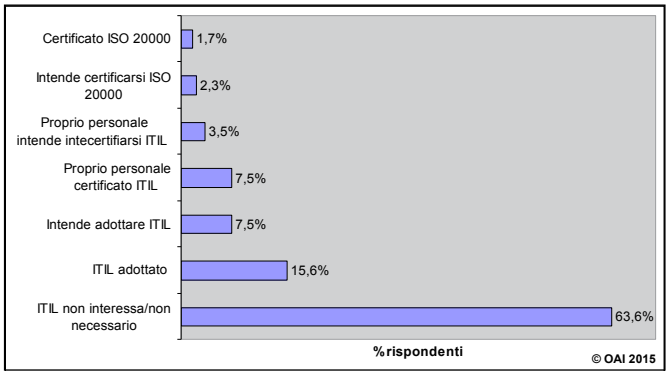

Fig. 6-15 Adozione ITIL ed ISO 20000 (risposte multiple)

La certificazione per la best practice ITIL è a livello individuale mentre quella per lo 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. Un 7,5% intende seguire ITIL nel prossimo futuro, con la medesima percentuale personale interno è certificato e per il 3,5% dei rispondenti alcune persone si certificheranno. Solo l'1,7% è certificato ISO 20000, ed il 2,3% lo farà, tipicamente a causa di obblighi derivanti da normative e/o contratti.

Nei riguardi dei propri fornitori, la fig. 6-16 evidenzia le richieste del campione: la maggior parte non lo richiede, ed in percentuale sono gli stessi rispondenti non interessati ad ITIL. Solo il 2,3% già richiede che i fornitori seguano nei loro processi ITIL, ed il 7,5% lo richiederà nel prossimo futuro. Il 2,9% richiede che il personale dei fornitori sia certificato ITIL. Una piccola percentuale richiede la certificazione ISO 20000, per i motivi sopra indicati.

La fig. 6-17 fornisce le indicazioni del 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

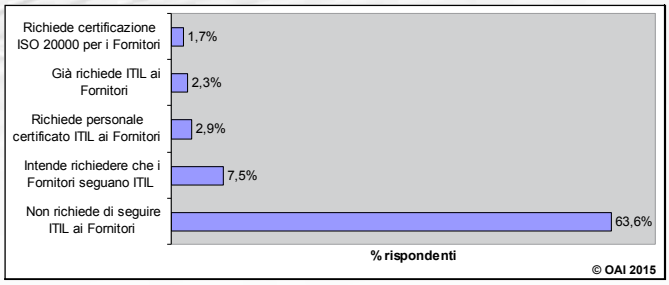

Fig. 6-16 Conformità dei Fornitori a ITIL e a ISO 20000 (risposte multiple)

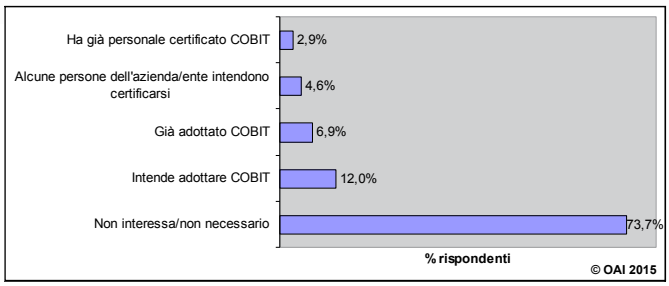

Fig. 6-17 Adozione COBIT (risposte multiple)

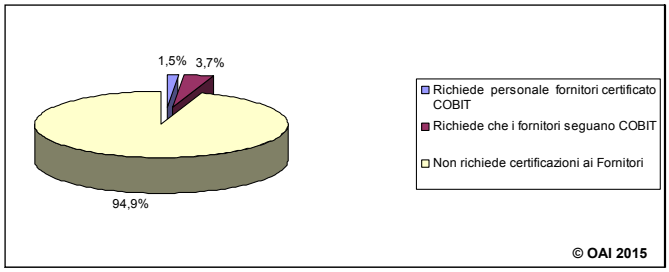

Fig. 6-18 Conformità dei Fornitori a COBIT

practice. Solo il 6,9% ha già adottato COBIT, ed il 12% intende adottarlo nel prossimo futuro.
Ancora più basse le percentuali rilevate per la richiesta ai fornitori di seguire COBIT o di avere figure certificate, come mostrato nella fig. 6-18.
L'adozione di ISO 27000, ITIL e COBIT in Italia è ancora limitata, anche se il campione emerso, come dettagliato nell'Allegato A.2, è composto solo per il 18,4% di aziende/enti fino a 10 dipendenti, ed il 32,9% è composto da aziende/enti con più di 250 dipendenti. La limitazione 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 grandi strutture. Un'ulteriore causa è che tali normative non sono ancora sistematicamente richieste nei capitolati e nelle gare di appalto. Alcune aziende/enti devono essere certificate e/o seguire specifiche normative settoriali che hanno impatti sulla sicurezza e sulla gestione del sistema informatico. Tipici esempi la normativa statunitense Sox[40] se si è quotati negli Stati Uniti, le normative Consob per le società quotate in Borsa, lo standard PCI-DSS per il trattamento dei dati delle carte di credito, le normative per le società dei settori medicinali ed alimentari (ben nota in Italia la HACCP, Hazard Analysis and Critical Control Points per prevenire i pericoli di contaminazione alimentare anche nei negozi), Basilea 2-3 e le norme della Banca d'Italia per le banche, le norme ISVAP per le assicurazioni, le normative sul D.Lgs 231/2001 per la responsabilità amministrativa delle persone giuridiche, la Legge 262/2005 per prevenire l'abuso di mercato con la diffusione di informazioni riservate, e così via.

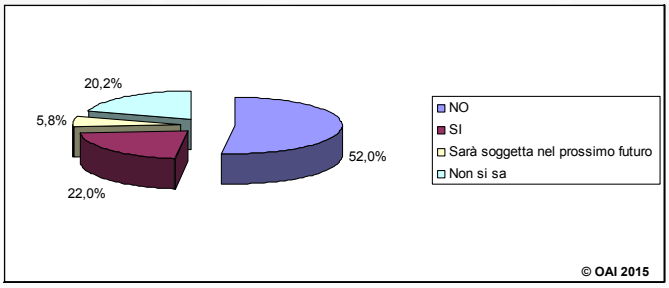

Fig. 6-19 Conformità ad altri standard o normative di settore

In termini molto generali, e senza far riferimento a specifiche norme, la fig. 6-19 mostra che il 22% dei rispondenti deve far fronte a questi ulteriori obblighi, essendo nei settori sopra indicati, ed il 5,8% lo sarà nel prossimo futuro.
Un importante tema ed indicatore di maturità sulla sicurezza 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 quali eCF, EUCIP, CISSP, SSCP, CISA, CISP, OPSA, ecc. Due decreti italia-

[40] Sox è l'acronimo per indicare il Sarbanes–Oxley Act del 2002, la legge federale statunitense che stabilisce un insieme di norme per la correttezza e la trasparenza dei bilanci delle aziende quotate in borsa

ni, il D.Lgs. 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 sulle competenze professionali del settore ICT.
In termini generali, e senza far riferimento a specifiche certificazioni nazionali ed internazionali, la fig. 6-20 mostra che per la stragrande maggioranza dei rispondenti, l'88,4%, queste certificazioni sulla sicurezza ICT non sono richieste all'interno dell'azienda/ente, e che solo il 3,3% intende richiederle nel prossimo futuro. A livello Fornitori la richiesta di queste certificazioni aumenta, come mostrato in fig. 6-21: il 24,4% già le richiede, ed il 10,3% intende richiederle. Questo è un indicatore che conferma il trend di terziarizzare le competenze più specialistiche, e per queste richiedere che il personale sia certificato.

6.4.2 Audit ICT

Nell'ambito della gestione della sicurezza un ruolo importante è giocato dall'auditing dell'ICT, e su questo tema il campione emerso, come da fig. 6-22, per il 52% già svolge questo processo, e l'11% intende svolgerlo. Il grande divario tra quanto emerso sulle certificazioni, di cui al paragrafo precedente, e l'auditing è probabilmente dovuto al fatto che quest'ultima è già presente nell'azienda/ente per altri settori (contabilità, controllo di gestione, ecc.) e più facilmente può (in taluni casi deve) essere estesa all'ICT. La fig. 6-23 evidenzia da chi è svolto l'auditing: per poco meno della metà del campione è svolto internamente, per il 24,4% è svolto esternamente e per un 27,8% è svolto sia internamente che esternamente. La fig. 6-24 indica quando è svolto: il 56,7% lo effettua con periodicità regolare, ad esempio annuale. Il 26,7% lo effettua in maniera "irregolare", ossia non pianificato periodicamente, ma quando ritenuto necessario, il 15,6% lo svolge in maniera continuativa, nell'ambito di un processo ben strutturato e di miglioramento continuo dell'ICT. Una

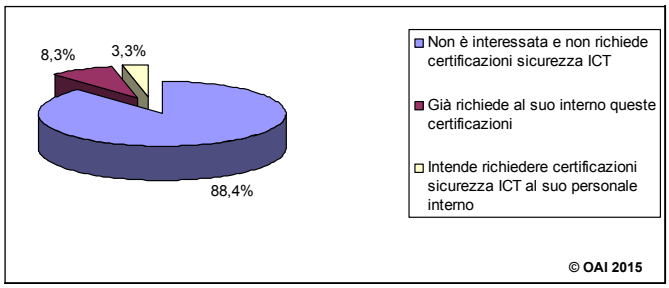

Fig. 6-20 Richiesta al personale interno di specifiche certificazioni/qualificazioni sulla sicurezza informatica

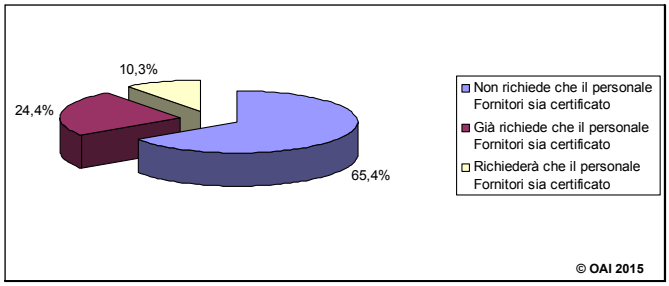

Fig. 6-21 Richiesta al personale fornitori di specifiche certificazioni sulla sicurezza informatica

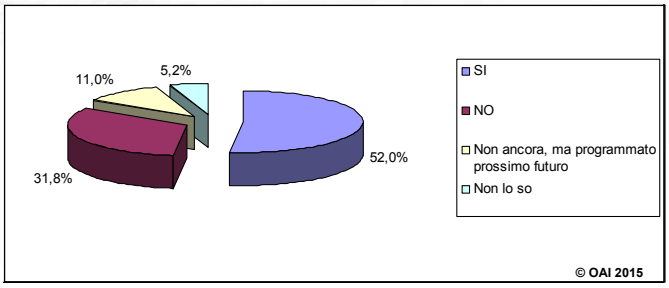

Fig. 6-22 Attività di auditing ICT

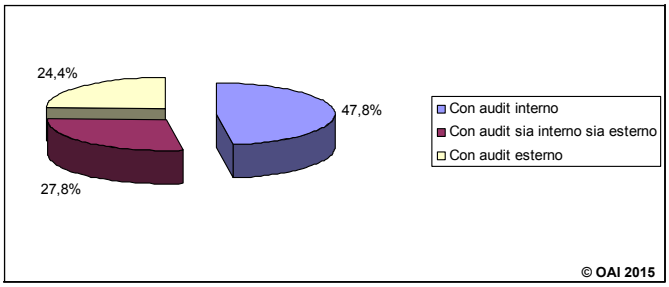

Fig. 6-23 Da chi è effettuato l'auditing ICT

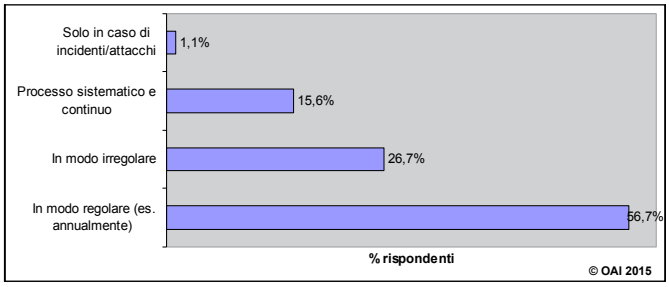

Fig. 6-24 Quando è effettuato l'auditing ICT

percentuale quasi irrisoria, l'1,1%, lo effettua solo a seguito di incidenti o di attacchi gravi. Da queste percentuali emerge che l'auditing ICT, almeno per questo campione di rispondenti, è un processo maturo, svolto in maniera periodica e sistematica.

6.4.3 La struttura organizzativa interna per la sicurezza ICT

La struttura organizzativa interna all'azienda/ente per la sicurezza ICT è un'altra componente fondamentale per ottenere e mantenere il livello di sicurezza idoneo, ed impatta sui vari processi e sulle procedure organizzative (anche per le certificazioni): nelle piccole organizzazioni talvolta tale ruolo non è previsto e quando necessario il vertice della struttura ricorre in maniera estemporanea, spesso in emergenza, a società e tecnici esterni.
Come evidenziato nella fig. 6-25, il 38,7% ha definito un ruolo di "responsabile della sicurezza informatica", in inglese CISO, Chief Information Security Officer; l'8,7% non lo ha ancora definito o ufficializzato, ma è in procinto di farlo.
Poco più della metà, il 52%, non ha per ora alcun responsabile esplicitamente definito ed in carica.
Quando questo ruolo è definito, formalmente o non, può essere allocato in diverse strutture, come mostrato nella fig. 6-26: per il 57,8% dei rispondenti sotto la struttura del responsabile dei sistemi informativi, il CIO (indicata con l'acronimo UOSI, Unità Organizzativa Sistemi Informatici); per il 21,9% nell'ambito della struttura del responsabile della sicurezza aziendale, il CSO, per il 12,5% in altre strutture dell'azienda/ente, quali ad esempio l'ufficio legale, l'organizzazione-personale, l'amministrazione-finanza-controllo. Infine per il 7,8% sono terziarizzate a professionisti o società specializzate.

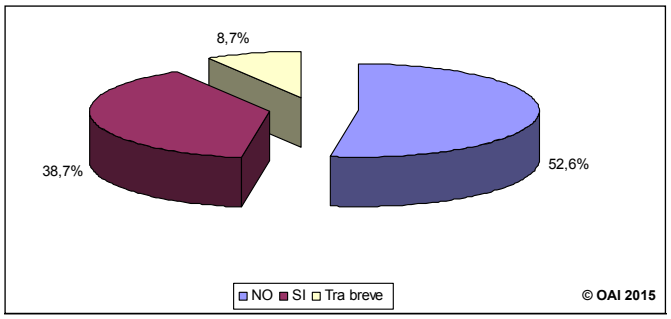

Fig. 6-25 Esistenza ruolo responsabile sicurezza informatica (CISO)

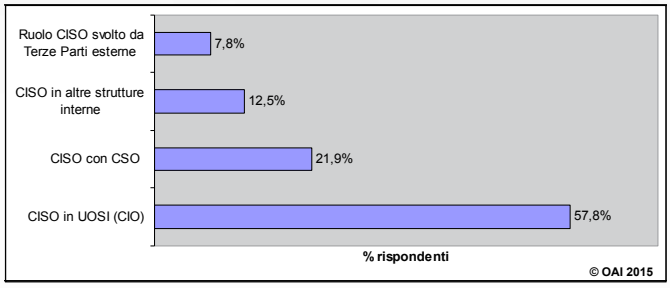

Fig. 6-26 Posizionamento organizzativo CISO

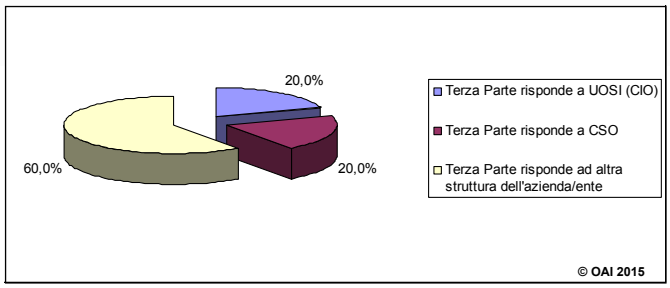

Fig. 6-27 A chi risponde il ruolo di CISO terziarizzato

Qualora questo ruolo fosse terziarizzato, da chi dipende lato azienda/ente cliente? La fig. 6-27 mostra che solo per il 20% dei rispondenti che terziarizzano la controparte è il CIO o il CSO, per il 60% è un'altra struttura aziendale, quale ad esempio l'ufficio acquisti o le altre sopra indicate.

7. GLI ATTACCHI PIÙ TEMUTI NEL FUTURO

La fig. 7-1, con risposte multiple, mostra quali sono gli attacchi ritenuti più probabili e più temuti nel prossimo futuro, tendenzialmente nel 2015 ed oltre, indipendente-

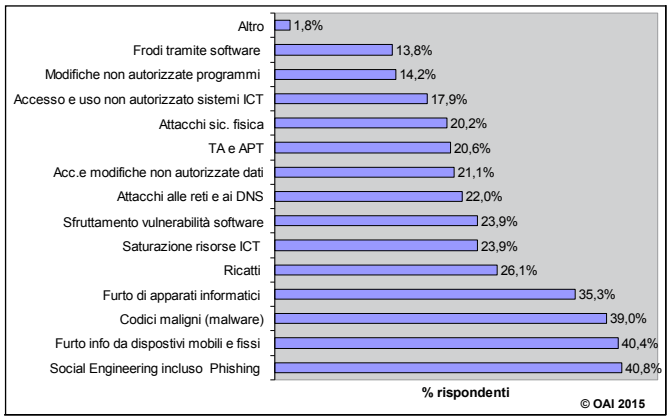

Fig. 7-1 Attacchi maggiormente temuti nel futuro (risposte multiple)

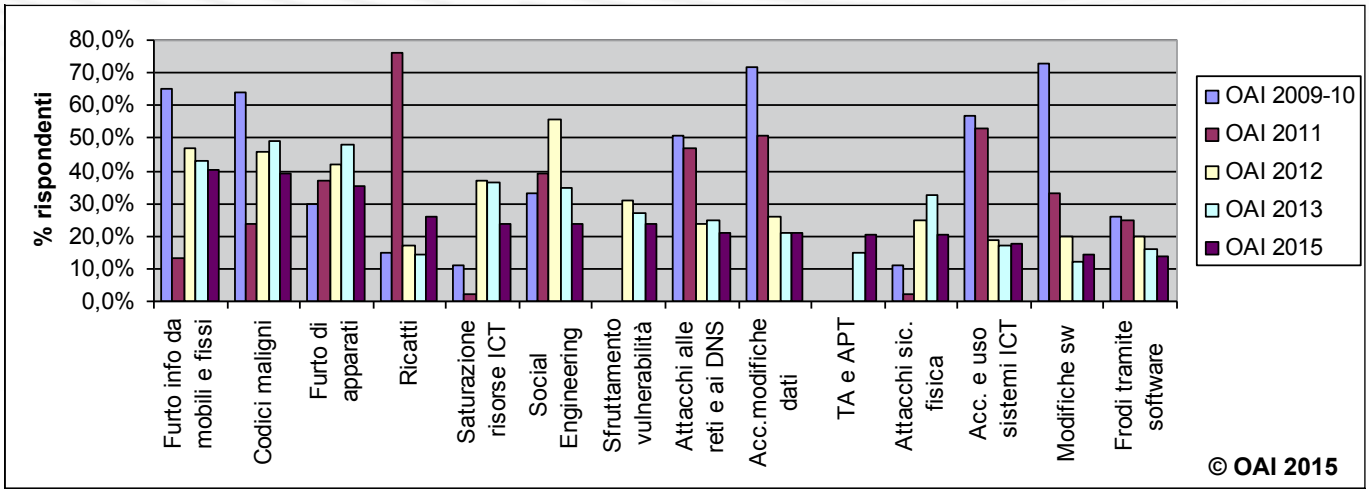

Fig. 7-2 Confronto tra gli attacchi "temuti nel futuro" nei vari Rapporti OAI

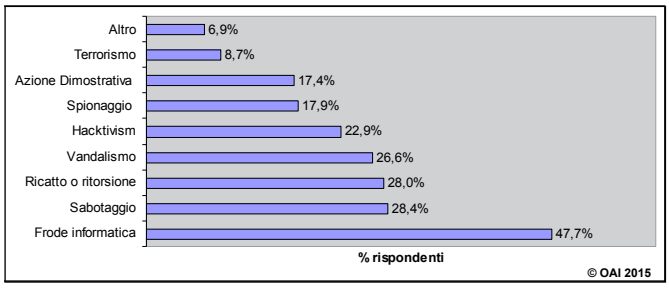

Fig. 7-3 Possibili motivazioni per i futuri attacchi temuti (risposte multiple)

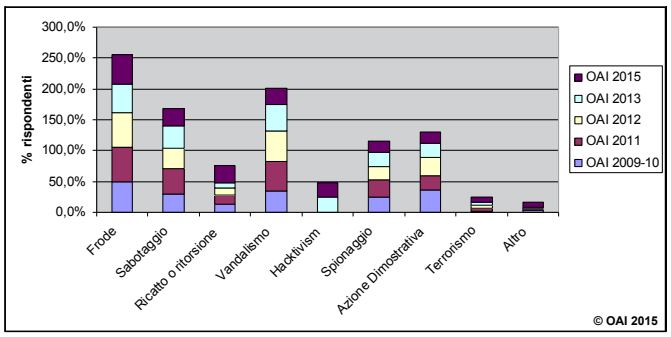

Fig. 7-4 Confronto complessivo delle motivazioni per gli "attacchi temuti nel futuro" nei vari Rapporti OAI

mente da quelli eventualmente subiti, e facendo sempre riferimento alla medesima tassonomia di attacchi considerata (Tabella 1). Anche per queste domande, come per quelle relative al termine "impatto poco o molto significativo" di cui al §4 ed alla fig. 4-7, non si sono specificati, per rendere più agile e semplice il questionario, i criteri per considerare un attacco più "temuto": ad esempio impatto funzionale-operativo, sul business, economico, legale, ecc.

I primi tre attacchi più temuti sono nell'ordine il social engineering, il furto di informazioni dai dispositivi d'utente sia mobili che fisici, il malware; e di questi sia il primo che il terzo sono sul podio degli attacchi più diffusi nel 2014, come evidenziato in fig. 4-5. Si affianca ai primi tre, come livello percentuale sopra il 30%, il furto di apparati ICT, con un 35,3%. Nella fascia percentuale del 20% si collocano nell'ordine i ricatti informatici, il DoS/DDoS, lo sfruttamento delle vulnerabilità software, gli accessi e modifiche ai dati, i TA/APT, gli attacchi alla sicurezza fisica. È da sottolineare che in questa edizione TA, Targeted Attacks, e APT, Advanced Persistent Threats, che nella precedente edizione si posizionavano al 12° posto al 14,8%, salgono ora al 10° con vari punti percentuali in più: un segnale che questo tipo di attacco non solo va diffondendosi, come evidenziato in fig. 4-5 e 4-6, ma è soprattutto temuto da un sempre maggior numero di aziende/enti che paventano di esserne potenziali target. Nella voce "Altro" i pochi rispondenti che l'hanno selezionata non hanno specificato quali altri attacchi temono. La fig. 7-2 pone a confronto le previsioni di attacchi più temuti emerse nelle varie edizioni OAI, ordinati in base ai valori 2014, confronto al solito puramente indicativo data la diversità dei campioni che hanno risposto ai questionari nelle diverse edizioni. Anche se puramente indicativo, il grafico mostra come siano diverse le stime di attacco

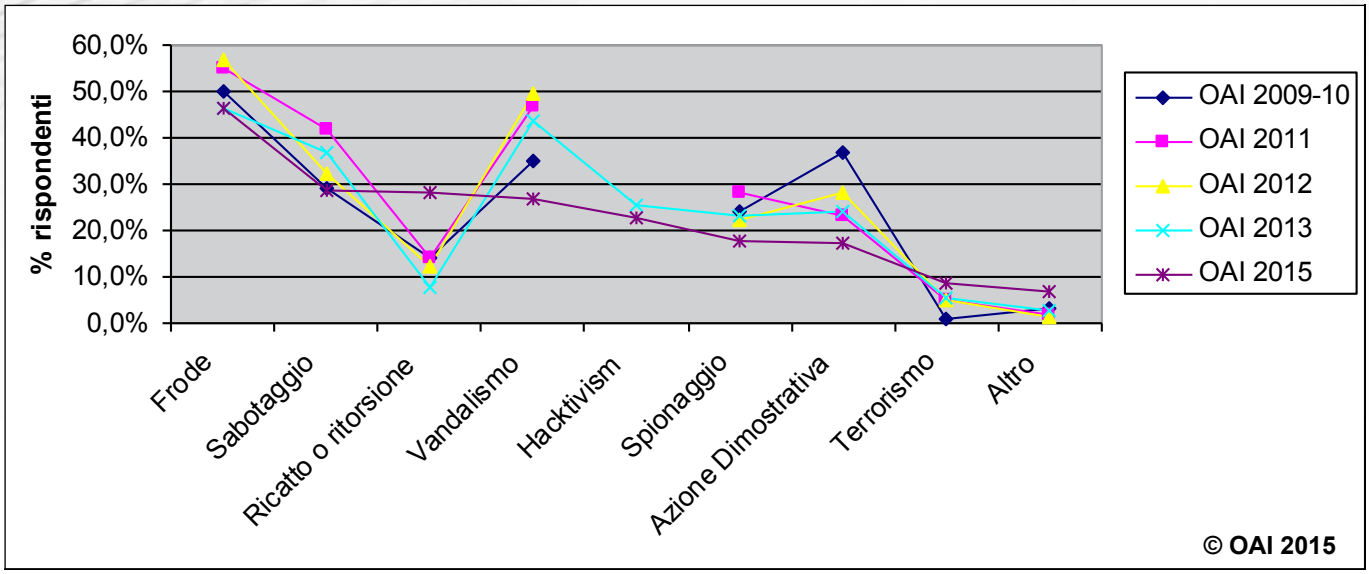

Fig. 7-5 Confronto dell'andamento delle motivazioni per gli "attacchi temuti nel futuro" nei vari Rapporti OAI

più probabile/temibile rapporto per rapporto: pur con campioni diversi e con probabili valutazioni diverse della semantica di "più temibile", le stime di criticità nel tempo sono cambiate per ogni tipo di attacco. Innumerevoli le considerazioni che possono scaturire da questo mutare della percezione dei potenziali rischi futuri. Le "frodi" sono andate riducendosi nel tempo (si danno ormai per scontate?), mentre sono rimasti "caldi" i codici maligni, il social engineering, il furto di informazioni da dispositivi fissi e mobili, i furti "fisici" di dispositivi ICT.

Considerando gli attacchi più temuti della fig. 7-1, la fig. 7-3, con risposte multiple, evidenzia quali sono le possibili motivazioni degli attaccanti secondo i rispondenti. Come nella precedente edizione, al primo posto per quasi la metà dei rispondenti è la frode informatica, che permette lauti guadagni illegali con bassi rischi di essere scoperti e puniti. Al secondo posto il sabotaggio, che era al terzo posto, seguito dal ricatto o ritorsione che era al terz'ultimo posto: evidente l'effetto dei ransomware diffusi anche in Italia nell'ultimo periodo.

Con una percentuale di poco inferiore, al quarto posto il vandalismo, causa probabile di parte degli attacchi "fisici". A decrescere le altre possibili motivazioni, a partire dall' hacktivism, con un 22%, lo spionaggio, sia per segreti industriali che politici, l'azione dimostrativa, che include anche gli attacchi del così detto "ethical hacking". All'ultimo posto la motivazione terroristica, nonostante i recenti, anche se limitati, attacchi jihadisti; la preoccupazione è per ora circoscritta ad aziende/enti di grandi dimensioni e di grande visibilità nazionale e internazionale. Con la voce "altro" sono stati specificati i furti di apparati e di informazioni per rivenderli al mercato nero.

Il confronto tra le stime sulle probabili motivazioni degli attaccanti riguardo al futuro nelle varie edizioni OAI è mostrato nella fig. 7-4. Pur con le variazioni di stima raccolte anno per anno, complessivamente la motivazione più temuta è la frode, seguita dal vandalismo e dal sabotaggio. La voce hacktivism, introdotta nella scorsa edizione, ha per questo motivo solo due valutazioni.

Come più volte sottolineato, occorre sempre considerare tali confronti come puramente indicativi, dato il campione diverso, e rammentare che i valori percentuali dipendo anche dal numero di rispondenti: al loro crescere si abbassa la percentuale di riferimento.

Analizzando gli stessi dati non a barre ma per linee, come riportato nella fig. 7-5, si evidenzia graficamente come l'andamento delle stime nei diversi anni, motivazione per motivazione, sia simile, fornendo quindi una sostanziale convergenza di opinioni. La differenza più evidente è quella del ricatto, fortemente aumentata nelle rilevazioni del 2014. Le curve delle edizioni fino al 2012 presentano un punto di discontinuità sulla motivazione hacktivism, causato dal suo inserimento solo nel 2013.

ALLEGATO A

Il campione emerso dall'indagine

Il bacino delle persone contattate via posta elettronica per compilare il questionario si è aggirato attorno alle 4.500 persone. Come per le precedenti edizioni, sono stati effettuati ripetuti solleciti mirati ai settori merceologici che fornivano meno risposte, per poter disporre di un campione abbastanza bilanciato tra i diversi settori. Le risposte avute sono state 424, rispetto alle 299, 206, 130 e 105 delle precedenti edizioni. Un incremento significativo, dovuto sia al crescente ampliamento del bacino di aziende/enti contattati, sia all'attività promozionale dei patrocinatori e degli sponsor, sia alla autorevolezza man mano acquisita da OAI.
Il numero di risposte ottenute rispetto al numero di contatti è basso, e le possibili cause sono molteplici, e differenti a secondo del tipo e delle dimensioni dell'azienda/ente contattata: politiche interne di non comunicare questo tipo di informazioni, necessità di chiedere permessi a più alti livelli, mancanza di tempo e/o di voglia per compilare, incapacità di rispondere ad alcune domande, e così via. Il numero di risposte ricevute sono comunque sufficienti e significative a fornire delle concrete indicazioni sugli attacchi ai sistemi informatici in Italia.

A.1 CHI HA RISPOSTO: RUOLO E TIPO DI AZIENDA/ENTE

Il bacino di utenza contattato è costituito 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. A-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, con "Altri", il personale interno che, a tempo pieno o no opera sulla sicurezza ICT, al terzo posto i vertici della struttura, al quarto posto i responsabili della

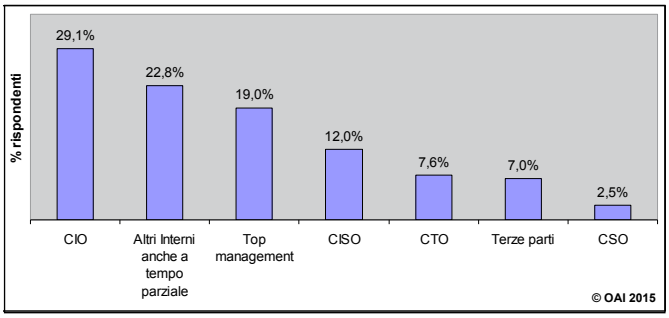

Fig. A-1 Ruolo rispondenti

sicurezza informatica (CISO). Seguono con valori inferiori al 10% i responsabili delle tecnologie (CTO, Chief Technology Officer), le terze parti, fornitori e consulenti che gestiscono la sicurezza ICT, e per ultimi i responsabili della sicurezza aziendale (CSO).
Facendo riferimento anche alle dimensioni dell'azienda/ente (fig. A-3), risulta che un esplicito ruolo di CISO è presente solo nelle strutture più grandi. Il terzo posto del vertice aziendale è un indicatore che, soprattutto nelle piccole imprese, la sicurezza informatica è gestita proprio dal vertice, quasi sicuramente con l'ausilio di fornitori e forse di consulenti.
La fig. A-2 illustra la suddivisione dei compilatori per i settori merceologici di appartenenza delle loro aziende/enti. Anche in questa edizione, onde evitare possibili errori di posizionamento, si è fatto stretto riferimento alla classificazione ATECO, dettagliando nel questionario:

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,

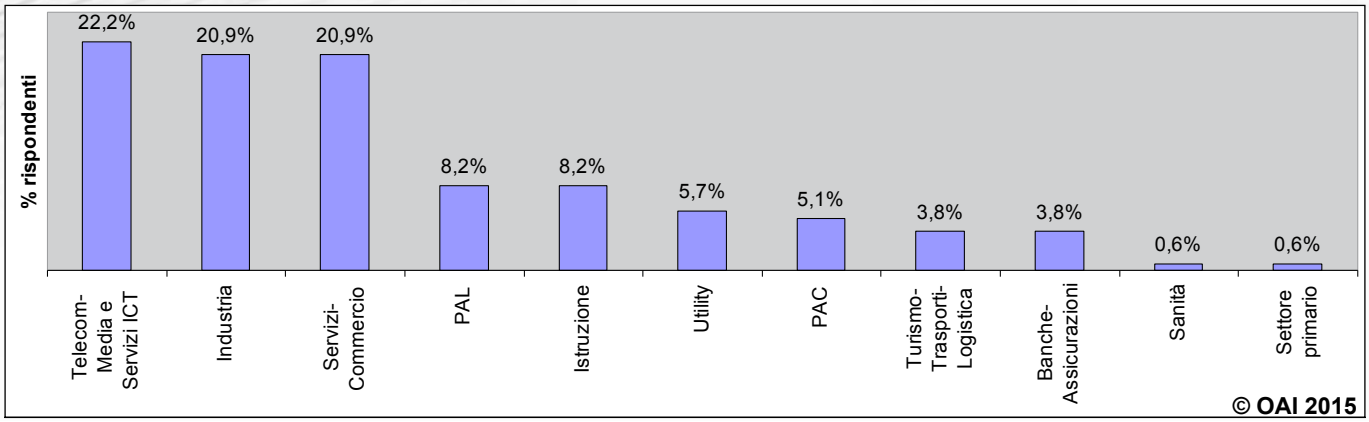

Fig. A-2 Settore merceologico di appartenenza

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

A livello di rielaborazione dei dati, per rendere il grafico di fig. A-2 più semplice e confrontabile con quelli delle edizioni precedenti, si sono raggruppati in "Telecom-Media e Servizi ICT" i punti 11 e 12 di cui sopra, in "Servizi-Commercio" i punti 4, 7, 8, 9, 10, 15, e in "Turismo-Trasporti-Logistica" i punti 5 e 7.

Data l'importanza per l'indagine OAI, oltre che per il loro peso come numero di rispondenti, "Telecom-Media e Servizi ICT" non è stata inserita in "Servizi-Commercio" che risulta il settore più rappresentato. Seguono percentualmente alla pari il settore Industria e quello dei servizi e commercio. Nel campione emerso sono ben rappresentati, anche con ampia diversificazione per dimensioni, gli ambienti industriali, del commercio e dei servizi; meno rappresentati, rispetto alla loro ampia diffusione in Italia, i settori Turismo-Trasporti-Logistica, Banche e Assicurazioni, Pubblica Amministrazione, soprattutto quella locale.

La fig. A-3 mostra la ripartizione percentuale delle aziende/enti dei rispondenti per dimensioni, in termini di nume-

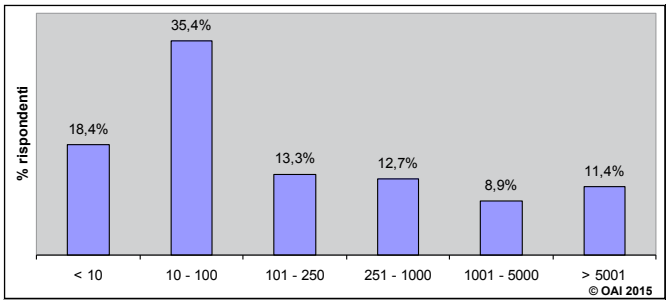

Fig. A-3 Dimensioni aziende/enti per numero dipendenti

Numero addetti	Numero Imprese
1	**2.655.768**
2-9	**1.578.054**
10-19	**137.212**
20-49	**54.218**
50-249	**22.039**
250 e più	**3.646**
Totale	**4.450.937**

Tabella A-1 Dati ISTAT su numero imprese per classe di addetti in Italia

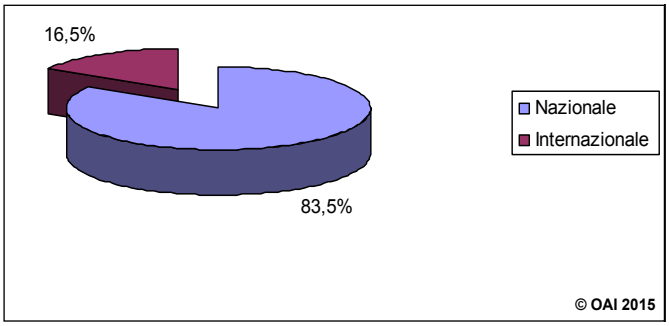

Fig. A-4 Copertura geografica azienda/ente

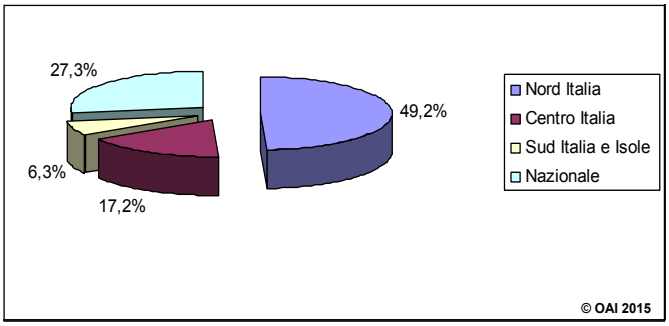

Fig. A-5 Ripartizione sul territorio nazionale

ro di dipendenti. Rispetto agli anni precedenti si è suddivisa in maniera diversa la fascia fino a 100 dipendenti, introducendo la fascia al di sotto dei 10, invece che al di sotto dei 50, e si è articolata la fascia tra 101 e 1000 in due voci, introducendo quella tra 101 e 250, limite dimensionale per le PMI, Piccole Medie Imprese. Il motivo è di meglio focalizzare la realtà delle PMI e delle piccolissime strutture, la più ampia in Italia, come dettagliato nella Tabella A-1 della più recente statistica (2011) pubblicata da Istat in merito.

Come negli anni precedenti la ripartizione è abbastanza bilanciata tra piccole, medie e grandi organizzazioni: il numero maggiore di rispondenti è in strutture tra 10 e 100 dipendenti.

L'area geografica di copertura dell'azienda/ente è, per il campione raccolto, prevalentemente nazionale, ma il 16,5% ha una copertura internazionale, a livello europeo o mondiale, come dettagliato dalla fig. A-4.

Nella fig. A-5 i rispondenti dell'area solo nazionale sono dettagliati per copertura Nord-Centro-Sud e Isole o dell'intero territorio. La metà circa dei rispondenti opera solo al Nord, il 27,3% opera sull'intero territorio nazionale e, a decrescere, solo nel Centro o solo nel Sud-Isole.

Per gli aspetti organizzativi sulla gestione della sicurezza informatica si rimanda a §6.4.

A.2 MACRO CARATTERISTICHE DEI SISTEMI INFORMATICI DEL CAMPIONE EMERSO DALL'INDAGINE

La prima domanda sui sistemi informatici dei rispondenti, con risposte multiple, riguarda la loro affidabilità e disponibilità, e le risposte sono mostrate nella fig. A-6: il 50% dei rispondenti dichiara di disporre di architetture ad alta affidabilità, almeno nell'ambito delle applicazioni più critiche per il business, ed il 35,4% di avere in uso un piano di Disaster Recovery (D.R.). Quest'ultimo dato è leggermente diverso da quanto rilevato sul D.R. nella fig. 6-7, ma è vicino alla media dei due valori riportati tra chi ha un piano e chi fa i test per provarlo: l'aggettivo "attivo" nella domanda su "chi ha un piano di D.R. attivo" non ha probabilmente fatto selezionare la risposta affermativa ad alcuni che hanno il piano ma non lo verificano periodicamente.

Per comprendere le dimensioni dei sistemi informativi del campione emerso dall'indagine, la fig. A-7 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 analoghi a quelli raccolti nelle precedenti edizioni: la stragrande maggioranza dei sistemi ha al massimo fino a 100 server (fisici e/o virtuali), con il 37,7%% del totale che arriva solo a 10, come è tipico per strutture di piccole dimensioni.

La fig. A-8 mostra le percentuali del numero di posti di lavoro fissi (PdL) per sistema informatico: quasi il 60 % dei

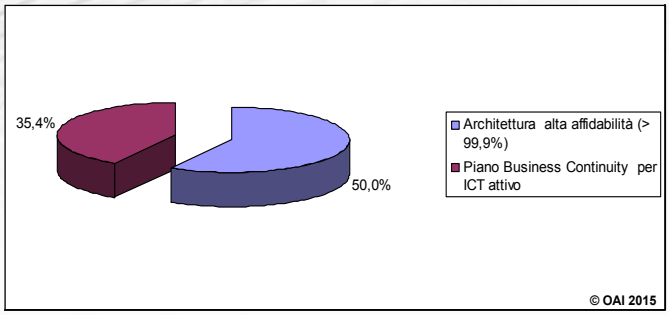

Fig. A-6 Alta affidabilità del sistema informatico (risposte multiple)

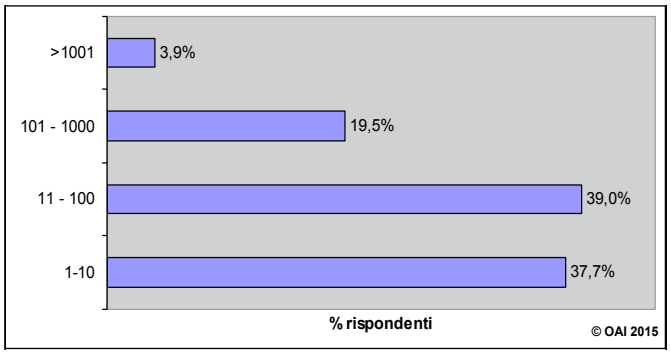

Fig. A-7 Numero complessivo di server fisici e virtuali

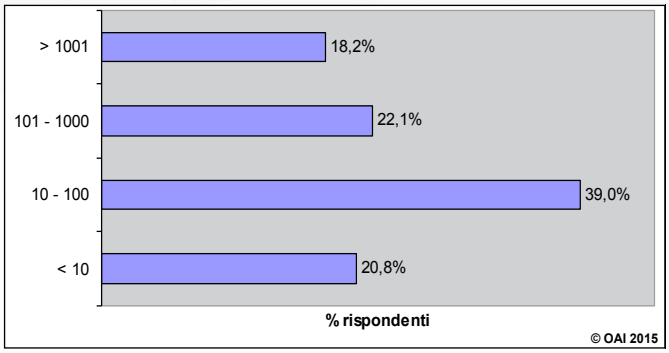

Fig. A-8 Posti di Lavoro (PdL) fissi

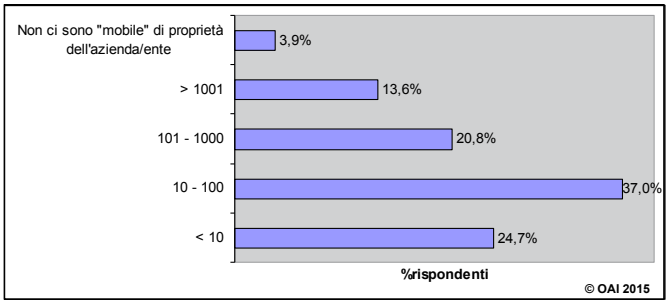

Fig. A-9 Dispositivi mobili dell'Azienda/Ente

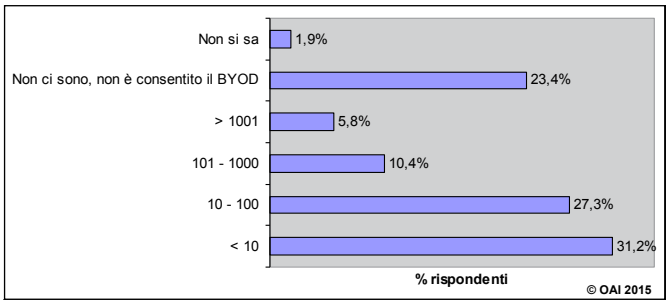

Fig. A-10 Dispositivi mobili proprietà utente finale

rispondenti ha fino a 100 PdL, il 22,1% tra 101 e 1000 PdL, ed il 18,2% oltre i mille.

La fig. A-9 mostra le percentuali del numero di dispostivi mobili di proprietà dall'azienda/ente forniti ai dipendenti: per non appesantire, il questionario non ha richiesto di specificare i tipi diversi di dispositivi mobili, e ragionevolmente la maggior parte dovrebbe essere costituita da smartphone. Interessante notare che il 3,9% dei rispondenti non ha (o non consente l'uso di propri) dispositivi mobili. La diffusione maggiore in percentuale è data dalla fascia tra 10-100, confermando quando rilevato nelle precedenti edizioni.

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 nell'indagine OAI.

La fig. A-10 illustra 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.

Il fenomeno è ormai diffuso in gran parte delle aziende/enti italiani, ma un non trascurabile 23,4% non lo consente. Nelle fig. A-10 la voce "Non si sa" indica una piccola percentuale che ha risposto di non conoscere i numeri e la realtà aziendale sul mobile di proprietà del dipendente: il motivo 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.

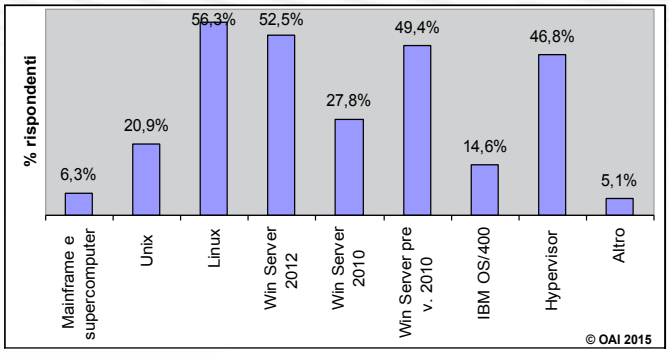

Fig. A-11 Sistemi Operativi dei server in uso (risposte multiple)

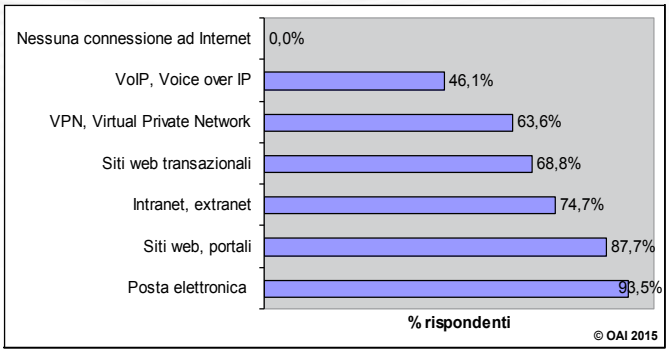

Fig. A-12 Uso di Internet (risposte multiple)

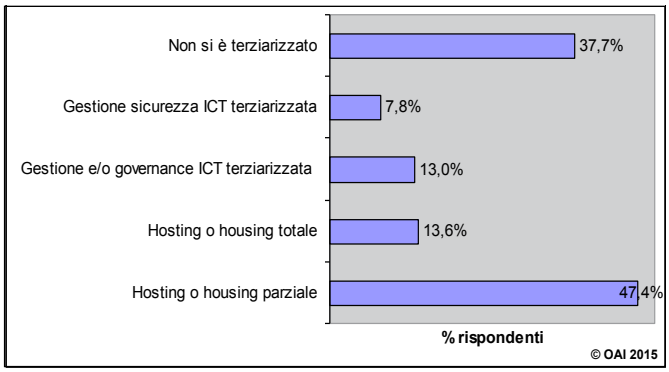

Fig. A-13 Uso della terziarizzazione (risposte multiple)

Tali risposte sono un concreto riscontro della correttezza dei compilatori che nella stragrande maggioranza non "inventano" dati se non li conoscono, ed ammettono di ignorare talune situazioni che non gestiscono: sincerità e correttezza che confermano la serietà e l'autorevolezza dei dati raccolti.

La fig. A-11, 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, gli OS Linux ed Unix siano utilizzati con percentuali paragonabili dalla gran parte dei server del campione: si deve considerare che i sistemi informatici, soprattutto quelli di medie e grandi dimensioni, sono solitamente "eterogenei", ossia usano contemporaneamente più sistemi operativi diversi; ed il fenomeno si è ulteriormente ampliato con la loro virtualizzazione. In ambito Windows è da sottolineare l'ampia diffusione dell' ultima versione, la 2012, con il 52,5%. Ancora diffuse le precedenti versioni dell'OS Windows Server, quali 2008, 2003 e forse anche 2000, incluse nella voce "Windows Server pre 2010", che arriva quasi al 50%. I sistemi Linux coprono più della metà del campione con un 56,3%, ed un 46,8% hanno gli OS "hypervisor" per la virtualizzazione dei server, che includono prodotti quali Z/VM, VMWare, ESX, XenServer, Hyper-V. Con percentuali decrescenti i sistemi Unix, che coprono circa 1/5 dei server, l'OS degli AS 400 e quelli per mainframe e super computer.

I sistemi AS 400, storicamente diffusi nelle PMI di fascia medio-alta, con il loro OS 400, mantengono in Italia una quota interessante del 14,6%. Gli OS per mainframe, come l'IBM System z e supercomputer costituiscono una nicchia attorno al 6,3%, tipicamente come "host" centrali di grandi organizzazioni quali industrie a livello internazionale, banche, assicurazioni e PAC.

I dati raccolti evidenziano come i sistemi informatici dei rispondenti 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.

Per rendere il questionario più leggero e semplice, nell'edizione di quest'anno non sono state poste domande sulle banche dati e sulle reti, ma si è voluto rilevare l'uso di Internet da parte dei sistemi informatici dei rispondenti.

La fig. A-12 mostra (con risposte multiple), che tutti i sistemi informatici hanno connessioni ad Internet, e che per la quasi totalità dei rispondenti, 93,5%, essa viene usata per la posta elettronica. Con percentuali decrescenti ma alte, Internet è usata per i siti web, anche transazionali, e per intranet/extranet. L'uso di collegamenti sicuri con VPN, Virtual Private Network, è attuato dal 63,6%, e la fonia su Internet , VoIP, Voice over IP, dal 46,1%.

Le fig. A-12 e A-13, con risposte multiple, mostrano l'u-

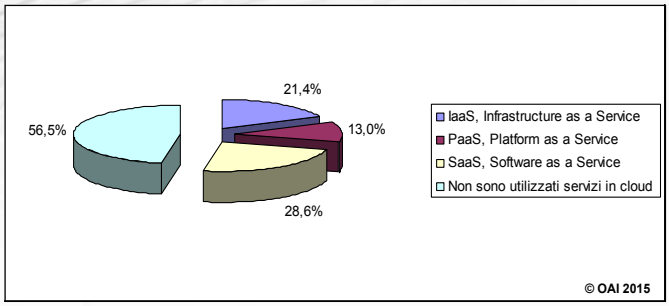

Fig. A-14 L'uso di soluzioni cloud (risposte multiple)

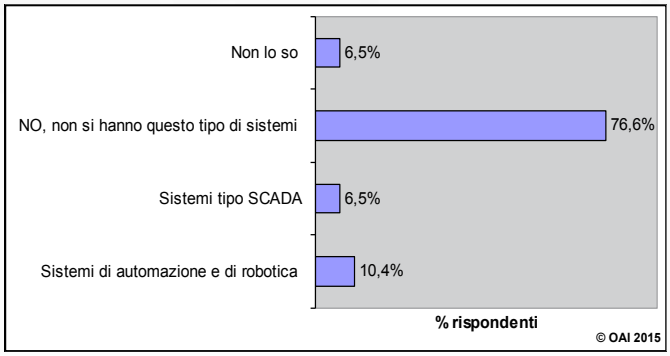

Fig. A-15 Robotica, automazione industriale e controllo processi (risposte multiple)

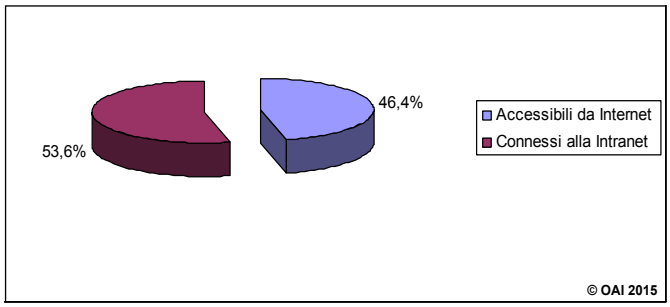

Fig. A-16 Connessioni dei sistemi di controllo e di automazione (risposte multiple)

so della terziarizzazione dell'ICT e di soluzioni cloud. 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% con percentuali ancora inferiori viene terziarizzata la gestione e la sicurezza dei propri sistemi informatici.

La fig. A-14 evidenzia che più della metà del campione, il 56,5%, non usa alcun tipo di soluzione cloud. Tra chi utilizza il cloud, la quota maggiore, il 28,6%, usa SaaS, il 21,4% IaaS ed il 13% PaaS. Tali percentuali sono maggiori di quelle rilevate nelle precedenti edizioni di OAI, e questo comprova che le soluzioni cloud sono sempre più adottate in Italia.

Confrontando i dati sulla terziarizzazione e su cloud, si evince che la terziarizzazione, in particolare housing e hosting, è più utilizzata dai rispondenti rispetto a soluzioni cloud. Come già emerso nel precedente rapporto, oltre che da altri recenti rapporti e guide[41] 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 probabilmente a timori sulla sicurezza effettivamente erogata. Per il cloud l'aspetto "sicurezza" é una competenza-caratteristica tipica del fornitore, che deve garantire al cliente il necessario (e richiesto) livello di sicurezza e fiducia.

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 e di robotica, tutti oggigiorno basati su tecnologie informatiche, e come tali attaccabili. Per la sicurezza informatica, soprattutto dopo gli attacchi STUXNET ai sistemi di controllo delle centrali nucleari iraniane[42], hanno assunto particolare rilievo i sistemi di controllo dei processi produttivi e di robotica, oltre che dell'IoT, trattato in §4.2.3. Come mostrato nella fig. A-15, la maggior parte del campione, 76,6%, non ha questo tipo di sistemi. Per chi ne dispone, il 10,4% ha sistemi di automazione, controllo e/o robotica, ed il 6,5% ha specifici sistemi tipo SCADA. Una piccola % dei compilatori ha ammesso di non avere informazioni su tali sistemi. Spesso nelle grandi aziende italia-

[41] 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 e scaricabile da http://www.malaboadvisoring.it/

[42] 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

ne 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 OAI 2015.
La fig. A- 16 mostra (risposte multiple) che tali sistemi nel 53,6% dei casi sono collegati alla Intranet dell'azienda/ente, e nel 46,4% sono direttamente accessibili da Internet, ad esempio per gestione e/o manutenzione da remoto, anche tramite società terze.

ALLEGATO B

Profili SPONSOR

AICA

AICA, Associazione Italiana per l'Informatica e il Calcolo Automatico, è la prima e più importante associazione dei cultori e dei professionisti ICT. Fondata nel 1961, è un ente senza scopo di lucro che ha come finalità lo sviluppo delle conoscenze digitali nel nostro Paese in tutti i loro aspetti, da quelli concettuali a quelli più applicativi e tecnologici. È il luogo di incontro accreditato tra gli attori chiave del settore, siano essi professionisti, docenti, studenti, cultori della materia oppure enti pubblici e privati quali università, amministrazioni, scuole, imprese, centri di ricerca. È inoltre il luogo di confronto sui temi della società digitale: dalle prospettive professionali e occupazionali alla diffusione delle competenze a strati sempre più ampi della popolazione.
Le iniziative di AICA sono numerose e si articolano in più aree.

- **Pubblicazioni:** Mondo Digitale è l'unica rivista italiana di cultura informatica segnalata in Scopus Index ed è da anni riferimento obbligato del settore.
- **Progetti e ricerche:** varie le iniziative promosse, tra le quali, come esempio, quella intitolata al costo dell'ignoranza informatica, che ha valutato lo spreco economico sostenuto dal sistema Paese per l'inadeguata conoscenza e padronanza delle tecnologie digitali da parte del personale nei vari settori merceologici, incluse le Pubbliche Amministrazioni; oppure, le ricerche sulla Storia dell'Informatica, con particolare riferimento ai contributi italiani, tra le quali l'evento "per fili e per segni" in collaborazione con FidaInform.
- **Convegni e Seminari:** organizzati generalmente in collaborazione con Istituzioni, Università e scuole di eccellenza sono preziose occasioni di incontro e di scambio, di esperienze per i cultori della materia. Molti di questi incontri sono a carattere locale, a cura delle Sezioni Territoriali della Associazione. Due sono a livello nazionale, Didamatica e il Congresso Annuale.
- **Giovani Talenti:** da oltre 10 anni, AICA organizza, in collaborazione con il MIUR (Ministero dell'Istruzione, dell'Università e della Ricerca) la partecipazione e la selezione degli studenti di scuole secondarie superiori alle Olimpiadi Italiane di Informatica (OII).
- **Competenze e Certificazioni:** AICA, insieme a tutti i suoi partner comunitari, ha individuato nella certificazioni europee sviluppate dal CEPIS (Council of European Professional Informatics Societies), lo strumento più efficace per valorizzare le competenze delle persone, siano esse utenti o professionisti ed è responsabile per l'Italia dei seguenti programmi internazionali:
  - e-Citizen, per la cittadinanza digitale necessarie a garantire a tutti la fruizione dei servizi Internet;
  - ECDL, European Computer Driving Licence, la Patente Europea del Computer, per la alfabetizzazione informatica con più di due milioni di italiani, sino ad oggi, certificati;
  - e-CFplus, sviluppato partendo da e-CF (e-Competences Framework, sistema europeo strutturato di competenze che descrive ad alto livello conoscenze e abilità richieste nel contesto dei processi ICT), dettaglia le competenze e professionalità digitali in maniera adeguata per riconoscerle, valutarle e svilupparle per imprese ed enti pubblici. E-CFplus arricchisce le 40 competenze e-CF con oltre 2200 componenti elementari raggruppati in 157 insiemi omogenei di conoscenze e abilità; queste componenti arricchiscono i 23 profili previsti dalle Linee Guida AgID e i profili professionali personalizzati che ogni organizzazione, con l'eventuale supporto metodologico AICA, può definire.

Per maggiori informazioni: http://www.aicanet.it/

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 italiano di ISSA® è parte della più grande associazione non-profit di professionisti della sicurezza che vanta più di 10.000 membri 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 nell'Area Soci del 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 speaker per conto di AIPSI/ISSA.

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

Itway è un gruppo Italiano, nato a Ravenna nel 1996, quotato alla Borsa di Milano nel segmento STAR dal 2001, con sedi in Italia e in Spagna, Portogallo, Grecia, Turchia, Emirati Arabi (Dubai), Libano; esso porta le sue competenze in ambito servizi tramite **Business-e,** che da oltre 15 anni offre servizi di sicurezza e affianca i propri clienti per metterli in grado di anticipare i cambiamenti del mercato e realizzare nuove opportunità di business in ambienti innovativi e sicuri.
Attraverso il proprio team di esperti, Business-e guida i propri clienti nell'individuazione delle migliori tecnologie di sicurezza e di protezione del business, delle persone, delle infrastrutture, ecc.
Le competenze, che Business-e mette a disposizione delle aziende, sono relative a servizi di controllo, integrazione, sviluppo ed ingegnerizzazione di piattaforme di security, sia di tipo logico che fisico. Con le sue competenze integra, sia soluzioni off-the-shelf, che soluzioni disegnate ad hoc per i propri clienti e basate su open source.
Le competenze tecniche sono arricchite da conoscenze di processo, standard, legal, ecc. In ambito consulenziale vengono forniti servizi di governance, di assessment, tra cui; penetration test, vulnerability assessment, social engineering, application security assessment, security plan, forensic analysis e secure code review, formazione, ecc.
Le esperienze Business-e hanno portato alla realizzazione di soluzioni e applicazioni sicure in ambiti quali il retail, industria, finance, pubblica amministrazione ecc. Fornendo servizi sia on-site che in cloud, con particolare attenzione ad aspetti connessi con la protezione dalla perdita di dati riservati (anche causati da furto o smarrimento di dispositivi mobili), alla protezione delle informazioni riservate e privilegiate e della proprietà intellettuale contro il rischio proveniente dall'interno dell'organizzazione (soluzioni **Be-Trusted®**). Le competenze di Business-e permettono lo sviluppo e la gestione di soluzioni sicure, in ambito cyber security, anche in collaborazione con partner strategici con i quali Business-e ha i più elevati livelli di certificazione.
Business-e gestisce in outsourcing e/o in co-sourcing le infrastrutture e la sicurezza con diverse tipologie di servizio, facendosi carico di amministrare l'infrastruttura esistente ed eventualmente completarla per renderla conforme a più elevati livelli di affidabilità e resilienza.
Il **Network Operation Center** (NOC) e il **Security Operation Center** (SOC) di Business-e sono specializzati nell'erogazione di servizi di Managed Security Services completamente erogati da strutture italiane e di servizi on-site per la sicurezza informatica, il networking e il system management.

Per maggiori informazioni: www.business-e.it

HP Enterprise Security - La sicurezza integrata quadrimensionale di HP

HP Enterprise Security Products (HP ESP) è fornitore leader di soluzioni per la security intelligence aziendale disegnate per ridurre i rischi contro le piu' odierne e avanzate minacce. Le soluzioni di HP ESP, ArcSight, Atalla, Fortify e TippingPoint, consentono di adottare un approccio proattivo alla sicurezza e di interrompere il ciclo di vita di un attacco con prevenzione e rilevamento delle minacce in tempo reale. HP Security Research, istituto riconosciuto a livello mondiale, complementa il portafoglio di HP ESP per la difesa di informazioni, applicazioni e reti fornendo soluzioni concrete contro le minacce piu' attuali e il diffondersi del Cyber Crime organizzato.

Per comprendere e combattere adeguatamente il Cyber Crime occorre pensare come l'avversario. Quali sono le nuove frontiere del crimine cibernetico organizzato? Come contrastarlo? La sicurezza va ripensata in un'ottica quadridimensionale: identificare le nuove minacce, riconoscere le diverse fasi di un attacco, rendere sicure le applicazioni ed integrare la sicurezza a livello del dato realizzando un efficace Adversary Management System.

Attraverso un'offerta di soluzioni hardware e software ampia e diversificata, la divisione Enterprise Security Products di HP, mette a disposizione della aziende enterprise un insieme di componenti e strumenti adatto a rispondere alle esigenze di rilevamento delle minacce esterne e interne e a predisporre azioni di risposta che intervengono per proteggere dati, rete e applicazioni.

Grazie ai suoi centri di ricerca e l'offerta di servizi distribuiti a livello globale HP mette a disposizione delle aziende una "intelligence" di sicurezza globale e aggiornata in tempo reale che contribuisce ad accelerare la risposta a minacce e predisporre azioni proattive nei confronti di nuove minacce come le APT (Advanced Persistent Threat).

Alcune delle principali soluzione di HP Enterprise Security Products:

- HP TippingPoint Next Generation Firewall e IPS - I sistemi firewall di nuova generazione (NGFW) forniscono il livello di visibilità necessario sulle applicazioni, chi sta accedendo a tali applicazioni per poi consentire di predisporre le policy richieste per bloccare e controllare le applicazioni non richieste, per contrastare il malware avanzato e le minacce APT.
- HP TippingPoint Advanced Threat Appliance (ATA) - Sfrutta i Next-Generation Firewall, gestiti attraverso la HP TippingPoint Security Management System (SMS), per bloccare immediatamente le minacce evitandone la propagazione attraverso la rete degli attacchi mirati e persistenti (APT).
- HP Application Defender - L'autoprotezione in cloud HP ha introdotto nella sua offerta tecnologie di "Runtime Application Self Protection" (RASP) l'autoprotezione in cloud che consentono di analizzare il codice in tempo reale e di attuare contromisure sulla base dei risultati.
- HP Fortify per un codice sicuro - Con la gamma di soluzioni Fortify, HP ESP fornisce una risposta efficace alle esigenze di sviluppare codice sicuro, di eliminare alla fonte le possibili vulnerabilità con test di tipo statico, dinamico e in tempo reale per la sicurezza del codice.
- La gamma Atalla – Le soluzioni Atalla abilitano un approccio alla protezione dei dati che sfrutta tecniche innovative di cifratura, proteggendo i dati on-premises e nel cloud , rendendo sicure le transazionielettroniche.
- Le soluzioni HP ArcSight - HP ha raggruppato all'interno della famiglia ArcSight le soluzioni software indirizzate a proteggere i dati attraverso il monitoraggio, l'analisi e la correlazione di eventi di sicurezza provenienti da differenti tipologie di sorgenti.

Per maggiori informazioni: www.hp.com/it/security

Riesko è una piattaforma informatica per l'analisi e la gestione dei rischi, personalizzata e personalizzabile sulle diverse tipologie di rischi e sulle caratteristiche dell'azienda/ente che la utilizza. Essa è preimpostata e "verticalizzata" per le più diffuse e richieste tipologie di rischi, quali quelle per i sistemi informatici e la loro sicurezza, la sicurezza sul lavoro, la continuità operativa di una divisione o dell'intera azienda/ente, la gestione dei rischi nei progetti, la produzione, la logistica ed i magazzini, l'amministrazione-finanza-controllo, la gestione del personale, il marketing e le vendite, gli acquisti, ecc., tenendo anche conto delle varie normative nazionali ed internazionali che si devono seguire, e/o delle norme da adottare per le certificazioni.
Con l'eventuale supporto di esperti di provata ed autorevole esperienza, e sempre in stretta collaborazione con il Cliente, Riesko viene personalizzato ad hoc sulle specifiche esigenze e realtà del Cliente per fornire uno strumento di supporto decisionale contestualizzato e in buona parte automatizzato/automatizzabile.
Riesko è infatti un sistema "dinamico" in grado di integrarsi ed interoperare con sistemi informatici preesistenti, acquisendo così in tempo reale allarmi e segnalazioni di eventi critici dai sistemi che li controllano.
Riesko è allineato con i seguenti standard e buone pratiche internazionali:

- ISO 31000:2009 - Risk management – Principles and guidelines.
- Risk Management Standard della FERMA, Federation of European Risk Management Associations.
- Criteri dell' IRM, Institute of Risk Management.

Riesko dispone inoltre di librerie con l'elenco dei rischi, dei controlli e delle vulnerabilità così come definiti ed aggiornati da standard e best practice internazionali (ISO27000, COBIT, ITIL, NIST, ecc.). Oltre all'interoperabilità con altri sistemi ed alle librerie precodificate, le caratteristiche principali di Riesko includono:

- un approccio sistematico e guidato articolato nei seguenti passi:
  - la definizione del singolo rischio nel contesto probabile per una sua occorrenza, con la correlazione ai processi ed ai ruoli organizzativi coinvolti oltre che ad altri rischi; su tali basi viene poi effettuata una prima stima dell'impatto complessivo, anche economico, che può avere;
    per ciascun rischio sono effettuabili più analisi (in parallelo) per affinare la stima delle condizioni di possibile occorrenza e di possibile impatto;
  - per ogni analisi approvata vengono definite le misure tecniche ed organizzative per prevenirlo o ridurlo, con stima del loro costo ed impatto; possono essere considerate differenti misure in logica what-if sia in termini di contrasto che di costo;
  - il trattamento prescelto viene monitorato nella sua implementazione e nella sua efficacia;
- una "dashboard" che evidenzia in sintesi le situazioni di rischio critiche e le statistiche sull'andamento delle attività di valutazione - aggiornamento dei livelli di rischio e di applicazione delle misure di miglioramento adottate o da adottare; essa può essere configurata secondo le richieste del Cliente;
- una banca dati unica che raccoglie tutti i dati e la documentazione inerente i rischi e le misure;
- un insieme di rapporti di sintesi e di dettaglio generati sistematicamente e preparati sulle esigenze del Cliente.

Per maggiori informazioni: www.riesko.com

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

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. Per completare una soluzione realmente sicura per la gestione documentale, oltre alla suite grafometrica, che si può integrare con i più diffusi prodotti sul mercato grazie ad interfacce web services, Technology Estate propone la suite professionale e ben collaudata: **DOPE** di ICON Systemhaus GmbH, che copre l'intero processo di generazione documentale.
DOPE fornisce un sistema coerente di elaborazione testo per l'intera azienda, dalla creazione alla produzione in sistemi applicativi specializzati fino alla sua presentazione in linee ad alti volumi di stampa, con una una moderna interfaccia utente intuitiva e configurabile e facilmente e strettamente integrabile con le applicazioni esistenti.
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: www.technologyestate.eu

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 maggiori informazioni: www.trendmicro.it

ALLEGATO C

Riferimenti e fonti

C.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.
- 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.

C.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
- Blue Coat 2014 Mobile Malware Report: https://www.bluecoat.com/
- 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
- Cisco Annual Security Report
- CISCO Security Advisories, Responses, and Alerts: http://tools.cisco.com/security/center/publicationListing.x
- CIS-Sapienza: "2014 Italian Cyber Security Report", rapporto su base annuale sulla consapevolezza della minaccia e capacità difensiva della Pubblica Amministrazione Italiana, http://www.agid.gov.it/sites/default/files/presentazioni/2014CIS-Report_web.pdf
- 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
- F-security Lab: http://www.f-secure.com/en/web/labs_global/
- GARR-Cert: www.cert.garr.it fornisce i principali security alert per gli aderenti al Garr, la rete telematica tra Università italiane
- Kaspersky Lab Virus Watch: http://www.kaspersky.com/me/viruswatchlite?page=4&hour_offset=-2
- Kaspersky Threat Real Time Map: https://cybermap.kaspersky.com/
- IBM Internet Security Systems - X-force: http://iss.net/, fornisce sistematicamente segnalazioni su vari tipi di attacco e di vulnerabilità; per i rapporti periodici si veda http://www-03.ibm.com/security/xforce/downloads.html
- Internet Crime Complaint Center (IC3) è una partenrship 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
- Lookout 2014 Mobile Threat Report: https://www.lookout.com/resources/reports/mobile-threat-report
- Panda Security: http://www.pandasecurity.com/enterprise/security-info/ fornisce informazioni sugli attacchi sia a livello domestico che d'impresa,oltre che rapporti periodici
- Ponemon Institute: "2014 Cost of Data Breach Study: Italy", analisi dei costi del cyber crime anche per singoli paesi, http://www.ponemon.org/library/2014-global-report-on-the-cost-of-cyber-crime
- Ponemon Institute: "Cost of Cyber Crime Study", http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/
- 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 Central Micrososft: http://www.microsoft.com/it-it/security/pc-security/default.aspx#Aggiornamenti-di-sicurezza fornisce avvisi su vulnerabilità e malware per i prodotti Microsoft
- 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
- Symantec: sul sito italiano (http://www.symantec.com/it/it/security_response/) fornisce allarmi e segnalazioni su vari tipi di attacco e di vulnerabilità. In inglese è disponibile su base annuale Internet Security Threat Report
- Sophos Threat Center: http://www.sophos.com/it-it/threat-center.aspx fornisce aggiornati allarmi
- 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/
- Verizon: "Data breach investigations Report" annuali in http://www.verizonenterprise.com/DBIR/2013/
- Websense Security Labs: http://securitylabs.websense.com/
- World Economic Forum: annuale "Global Risk", che include anche considerazioni sui rischi informatici e di cyberwar; http://www.weforum.org/issues/global-risks

ALLEGATO D

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 ri-

sposte 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. Viene anche 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 condizione in cui due o più processi non sono più in grado di proseguire perché ciascuno aspetta il risultato di una operazione che dovrebbe essere eseguita dall'altro.
- Deamon: software di base operante in back-ground in un ambiente 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 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.
- 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.
- 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 riservate di un utente, basato sull'invio di un falso messaggio in posta elettronica che fa riferimento ad un ente primario, che richiede di collegarsi ad un server (trappola) per controllo ed aggiornamento dei dati.
- Ping of death: invio di pacchetti di ping di grandi dimensioni (ICMP echo request), che blocca la pila di protocolli TCP/IP: è un tipo di attacco DoS/DDoS.
- 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: programmi 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 le funzionalità di un sistema, tramite il quale viene chiesto un riscatto (ransom) per sbloccarlo.
- Rogueware: falso antivirus. È 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 attacchi.
- SGSI, Sistema Gestione Sicurezza Informatica.
- SIEM, Security Information and Event Management: sistemi e servizi per la gestione in tempo reale di informazioni ed allarmi generati dalle risorse ICT di un sistema informativo.
- Sinkhole: metodo per reindirizzare specifico traffico

Internet per motivi di sicurezza, tipicamente per analizzarlo, per individuare attività anomale o per sventare attacchi. Può essere realizzato tramite darknet o honeynet.

- SOC, Security Operation Centre.
- Social Engineering (ingegneria sociale): con questo termine vengono considerate tutte le modalità di carpire informazioni, quali l'user-id e la password, per accedere illegalmente ad una risorsa informatica. In generale si intende lo studio del comportamento individuale di una persona al fine di carpire informazioni.
- Sniffing-snooping: tecniche mirate a leggere il contenuto (pay load) dei pacchetti in rete, sia LAN che WAN.
- Smart city: città "intelligente" largamente dotata di infrastrutture e soluzioni ICT sia per i suoi abitanti e per interagire con loro, sia per migliorare il controllo del territorio, della sua sicurezza, dell'ambiente, della viabilità, ecc.
- 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.
- Trojan Horse (cavallo di Troia): codice maligno che realizza azioni indesiderate o non note all'utente. I virus fanno parte di questa categoria.
- TOR, The Onion Router: sistema di comunicazione anonima in Internet basato sul protocollo onion router e su tecniche di crittografia.
- Trouble ticketing: processo e sistema informatico di supporto per la gestione delle richieste e delle segnalazioni da parte degli utenti; tipicamente in uso per help-desk e contact center.
- VPN,Virtual Private Network: rete virtuale creata tramite Internet per realizzare una rete "privata" 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 esempio JavaScript, ed HTML per modificare le pagine web che l'utente vede.
- Watering Hole: famiglia di attacchi che rientrano nella categoria dei Targeted Attack. Il termine,traducibile in" attacco alla pozza d'acqua", fa riferimento agli agguati di animali carnivori alle prede che si dissetano in una pozza d'acqua. La metafora è usata per attacchi mirati a siti web specialistici, ad esempio di finanza, di politica, di strategie, ecc., cui una persona di 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 le connessioni esistenti.
- Zero-day attach: attacchi basati su vulnerabilità a cui non è ancora stato trovato rimedio.
- Zombies: vedi bots.

ALLEGATO E

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 OAI, Osservatorio Attacchi Informatici in Italia. Attraverso la sua società Marco conduce interventi consulenziali lato sia domanda sia offerta ICT ed offre servizi on line quali SLA Watch. 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 nel Consiglio Direttivo di AIPSI e di FIDAInform, socio fondatore e componente del Comitato Scientifico dell'FTI, socio del ClubTI di Milano e di AIPSI. È certificato ITIL v3 ed EUCIP Professional Certificate "Security Adviser". Ha pubblicato articoli e libri sull'evoluzione tecnologica, la sicurezza, gli scenari e gli impatti dell'ICT.

malabo
ICT Advisory

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 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 ICT, 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 e alla norma UNI 11506, la riorganizzazione dei processi ICT con intelligente e contestuale riferimento a ITIL e a COBIT, l'effettivo allineamento tra sistema informativo 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 Inventory necessita di un "agent" per ogni host.
- 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, che integra i servizi sopra elencati e che viene supportata anche da interventi in loco, con una intelligente e contestuale applicazione delle buone pratiche ITIL v3 e COBIT.
- Riesko, sistema analisi e gestione rischi ICT, anche in cloud, basato sui più consolidati standard e best practice (ISO 27001-2-5, NIST 800, Octave Allegro) e personalizzabile sullo specifico contesto del Cliente.
- Kit autovalutazione del ritorno economico e dell'analisi del valore di un sistema informatico, 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 e www.sla-watch.com

SOIEL INTERNATIONAL
Eventi e riviste per l'organizzazione aziendale

L'INFORMAZIONE AL SERVIZIO DELLA CONOSCENZA

Soiel International è presente da 35 anni nel mercato della comunicazione professionale, rivolta al settore dell'Information & Communication Technology e al comparto dell'arredo dell'ambiente ufficio.

RIVISTE

Le riviste sono accreditate nel mercato di riferimento per i contenuti e qualità del mailing, costruito nel tempo con la fidelizzazione dei lettori e le molteplici attività seminariali.

Executive.IT è il bimestrale realizzato in collaborazione con Gartner, rivolto al management aziendale che propone scenari, tecnologie, modelli e strategie per il successo del business attraverso l'utilizzo dell'ICT.

Office Automation è il mensile specializzato nell'ICT, promotore dei convegni e seminari sui temi delle nuove tecnologie e applicazioni. È rivolto ai manager che hanno la responsabilità di indirizzare le scelte tecnologiche, e ai protagonisti della catena del valore (produttori, distributori, rivenditori, system integrator, installatori...) il cui compito è guidare nella scelta delle soluzioni hardware e software che migliorano l'efficienza del business.

innov@zione.PA è il magazine dedicato ai temi dell'innovazione nel mondo della Pubblica Amministrazione centrale e locale.

Officelayout è la rivista per progettare, arredare e gestire lo spazio ufficio.

L'offerta editoriale propone anche manuali di approfondimento, libri e dizionari.

EVENTI

L'esperienza acquisita nella comunicazione, la professionalità e la qualità del mailing sono i pilastri su cui poggia dal 1994 l'attività di "comunicazione d'impresa" di Soiel International che comprende consulenza, progettazione e organizzazione di convegni, corsi, eventi promozionali.

I convegni con area espositiva di Soiel International e l'attività seminariale sviluppata ad hoc per le aziende integrano le possibilità di comunicazione offerte dall'attività editoriale e su essa basano la propria promozione.

Con una banca dati unica in Italia (oltre 320.000 nominativi) di operatori della domanda e dell'offerta nell'ICT e nel layout d'ufficio e la possibilità di utilizzare forme integrate di comunicazione, Soiel International si propone quale partner di riferimento per la realizzazione di eventi rivolti al mondo dell'utenza aziendale business e della catena del valore.

Nel corso del 2013 Soiel International ha promosso e gestito 95 eventi su tutto il territorio nazionale.

CORSI

Quale completamento dell'offerta informativa e formativa nasce nel 2000 l'attività dei Corsi, sviluppata in partnership con importanti società di consulenza ed esperti del settore e studiata per rispondere alle esigenze di formazione più specifiche.

Via Martiri Oscuri, 3 • 20125 Milano • Tel. 02 26148855 • Fax 02 93661295 • www.soiel.it

Con la collaborazione di:

Patrocinatori

SOIEL INTERNATIONAL
Eventi e riviste per l'organizzazione aziendale