Sponsor

Rapporto 2013 OAI

a cura di
Marco R.A. Bozzetti

Osservatorio Attacchi Informatici in Italia

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
2013 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 2013.
Un grazie particolare agli Sponsor, all'editore Soiel International, al dott. Francesco Zambon, all'ing. Maurizio Mapelli, ai dott. Antonio Apruzzese e Alessandro Galante della Polizia Postale, che hanno contribuito alla realizzazione del presente rapporto.

INDICE

1. Introduzione

L'iniziativa OAI, Osservatorio Attacchi Informatici in Italia, è l'unica indagine on line via web sugli attacchi informatici a livello nazionale su tutti i settori merceologici. Dall'elaborazione dei dati raccolti viene realizzato un rapporto annuale, che fornisce una realistica e concreta indicazione del fenomeno degli attacchi intenzionali in Italia, essenziale per impostare o aggiornare l'analisi dei rischi di un sistema informatico operante sul territorio nazionale, e di conseguenza adottare i più idonei strumenti di prevenzione e protezione. Obiettivo primario di OAI è infatti il fornire concrete indicazioni sugli attacchi intenzionali ai sistemi informatici delle aziende e degli enti pubblici italiani, 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 favorire lo sviluppo di sensibilità e cultura in materia di sicurezza informatica soprattutto a livello dei decisori "non tecnici", figure tipicamente ricoperte dai vertici dell'organizzazione che decidono i relativi budget ed i relativi progetti di miglioramento del livello di sicurezza.

Il presente Rapporto 2013 fa riferimento agli attacchi informatici rilevati nel corso del 2012 e del 1° semestre 2013. Costituisce la quarta edizione, dopo i precedenti rapporti del 2012, 2011 e del 2009-10 che nel loro insieme coprono gli attacchi subiti dal 2007 a metà 2013. 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] Gruppo Sernet, Seeweb, Technology Estate, Trend Micro.

Alla fine del rapporto sono inserite in ordine alfabetico le schede di presentazione degli Sponsor, con l'approfondimento delle loro attività nel campo della sicurezza informatica. Le prime due edizioni[4] furono scaricabili dai lettori gratuitamente appena pubblicate, e tutte le attività per la loro creazione furono basate sul volontariato, in particolare dell'Editore Soiel International e dell'Autore aiutato da alcuni esperti soci del ClubTI di Milano e di AIPSI. Il perdurare della crisi economica non ha consentito più tale approccio totalmente basato sul volontariato di persone e di aziende, e per coprire almeno i costi vivi e al contempo mantenere l'indipendenza e l'autorevolezza conquistata, si è fatto ricorso alle sponsorizzazione multiple, cui hanno aderito le Aziende/Enti citati, garantendo loro l'esclusiva per 4 mesi dalla pubblicazione per far scaricare, attraverso opportuni codici-coupon, il rapporto ad un insieme ampio, ma selezionato, di loro interlocutori.

OAI 2013 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), Forum delle competenze digitali, 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 fondamentale 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

[1] AICA, Associazione Italiana Calcolo Automatico.
[2] AIPSI, Associazione Italiana Professionisti Sicurezza Informatica, capitolo italiano della mondiale ISSA.
[3] ICT, Information and Communication Technology.
[4] Gratuitamente scaricabili dal sito web dell'Autore, www.malaboadvisoring.it, da quello dell'Editore Soiel International, www.soiel.it, e dai siti di vari Sponsor e Patrocinatori.

tale ottica e per creare una certa continuità tra un'edizione e l'altra del rapporto, l'Editore Soiel International e l'Autore hanno dato vita ad una rubrica mensile OAI pubblicata sulla rivista Office Automation: tutti questi articoli sono disponibili on-line sui già citati siti web dell'Autore e dell'Editore. L'Autore ha inoltre creato e gestisce il Gruppo OAI su LinkedIn.
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 in § 9 un glossario degli acronimi e dei termini tecnici specialistici usati.

1.1 Aspetti metodologici dell'indagine 2013

Il rapporto OAI annuale si basa sull'elaborazione delle risposte avute al questionario on-line via web da parte soprattutto di 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 soprattutto per le piccole organizzazioni. L'Autore, l'Editore Soiel ed i Patrocinatori hanno invitato a compilare il Questionario 2013 le persone con i profili sopra elencati con messaggi di posta elettronica, facendo riferimento alle 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 "social network" inerenti l'ICT e la sicurezza informatica, in particolare su LinkedIn e Facebook, e molti dei Patrocinatori hanno pubblicato "banner" e segnalazioni di invito sulle home page dei loro siti web.
Il Questionario OAI 2013 è stato posto on line per circa due mesi, da fine settembre 2013 a fine novembre 2013, ed in questo arco temporale il bacino dei potenziali rispondenti ha ricevuto più inviti e solleciti.
Nel complesso il numero delle persone contattate si aggira attorno a seimila, appartenenti ad un ampio insieme di aziende ed enti pubblici centrali e locali.
L'indagine annuale OAI non ha (e non vuole e non può 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 nel § 4, il numero e l'eterogeneità delle aziende/enti dei rispondenti, sia per settore merceologico che per dimensione, è comunque significativo per fornire chiare e preziose indicazioni sul fenomeno degli attacchi in Italia e sulle sue tendenze: indicazioni specifiche che nessun altro rapporto fornisce per l'Italia.
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.
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 quattro 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 per produrre sintesi e grafici; comunque il livello di dettaglio sulle caratteristiche tecniche dei sistemi ICT non consente in alcun modo di poter individuare l'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 stesso. L'Autore e l'Editore garantiscono inoltre la totale riservatezza sulle risposte raccolte, utilizzate solo per la produzione del presente rapporto.

2. 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, 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.

L'evoluzione moderna dei sistemi informativi si è consolidata su Internet e sui siti web, evolvendo velocemente verso logiche collaborative oltre che verso logiche 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 collegamenti "peer-to-peer", 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 sta sparendo, 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 anche per il lavoro. Questo fenomeno, indicato con il termine di "consumerizzazione", è ormai molto diffuso nelle piccole e nelle grandi organizzazioni, e 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. Lo sviluppo del software ha compiuto passi significativi: la programmazione a oggetti è ben consolidata e diffusa, gli standard SOA (Service Oriented Architecture) con i web service, ormai così consolidati che difficilmente vengono citati, consentono una reale interoperatività e un assemblaggio dei programmi applicativi più semplice e modulare.

La pila dei protocolli TCP/IP e l'ambiente web costituiscono la piattaforma standard di riferimento per l'intera infrastruttura ICT e per il trattamento di qualsiasi tipo d'informazione, con eterogeneità di sistemi e di funzioni.

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, 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 gli strumenti necessari.

Ma quali sono gli attacchi che tipicamente 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) e quelli provenienti dai principali fornitori di sicurezza informatica a livello mondiale, quali Trend Micro (in § 10 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 effettuare concrete analisi dei rischi e attivare le idonee misure di prevenzione e protezione, oltre a "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 più da come lo si usa e lo si gestisce, che dalle tecnologie impiegate: organizzazione, informazione e coinvolgimento di tutto il personale sono altrettanto importanti, se non di più, dell'installazione di firewall, anti malware, sistemi di identificazione e autenticazione, back-up e così via.

Proprio per colmare tale vuoto informativo in Italia, con la prima edizione del rapporto OAI si decise di rilanciare l'attivazione di un Osservatorio Nazionale, ereditando l'esperienza passata avuta con OCI, Osservatorio Criminalità Informatica, di FTI-Sicurforum[5]. 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 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 i costi vivi, e si posiziona come l'unica indagine indipendente effettuata sulla realtà italiana, basata sulle risposte al questionario annuale da parte di chi effettivamente gestisce la sicurezza ICT nell'azienda/ente.

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'organizzazione stessa, o infine, come spesso accade, da una combinazione tra 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 ai saggi di Pacifici e Sarzana di Sant'Ippolito contenuti nel volume Bozzetti, Pozzi 2000, e al recente libro "Sicurezza digitale" dell'Autore e di Francesco Zambon edito da Soiel International[6].
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 a coloro cui il questionario è indirizzato: tipicamente i responsabili dell'area ICT (CIO) e, laddove esistano, della sicurezza ICT (CISO) o figure simili, anche di fornitori e consulenti di terze parti cui viene terziarizzata la gestione della sicurezza ICT, o una sua parte.
La tassonomia degli attacchi informatici considerata nel Questionario 2013 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 § 9).
Rispetto alla tassonomia della edizione 2012, in questa sono stati aggiunti gli attacchi mirati e APT, pur sapendo la difficoltà di individuare attacchi di tale tipo; sono state poi meglio specificate le tipologie di attacco 8, 9 e 10 che sono tra loro sequenziali: ad esempio le modifiche non autorizzate ai dati o al software richiedono prima l'accesso non autorizzato ai sistemi.

[5] Per i Rapporti OCI del 1997, 2000 e 2004, pubblicati da Franco Angeli, si veda http://www.forumti.it/
[6] 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: se non si paga, il sistema informatico viene attaccato procurando danni).
8. **Accesso a e uso non autorizzato dei sistemi visti come un'unica entità "host"** (1° livello).
9. **Accesso e modifiche non autorizzate ai programmi applicativi e di sistema, alle configurazioni ecc** (2° livello).
10. **Modifiche non autorizzate ai dati e alle informazioni** (3° livello).
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) e Botnet, si includono in questa classe anche mail bombing, catene di S. Antonio informatiche, ecc.
14. **Attacchi alle reti, fisse o wireless e ai DNS** (Domain Name System).
15. **Attacchi APT**, Advanced Persistent Threats, **e attacchi mirati (targeted)** basati su uso contemporaneo e/o persistente di più tecniche sofisticate di attacco.

4. Caratteristiche dei rispondenti e dei sistemi ICT

Come indicato in § 1.1, il bacino delle persone contattate via posta elettronica per compilare il questionario si è aggirato attorno alle 6000 persone, analogamente alla scorsa edizione. Ed anche quest'anno sono stati effettuati ripetuti solleciti mirati ai settori merceologici che fornivano meno risposte, por poter disporre di un campione abbastanza bilanciato tra i diversi settori. Le risposte avute sono state 299, rispetto alle 206, 130 e 105 delle precedenti edizioni. Un incremento significativo, ma con un numero di risposte ancora basso rispetto al bacino contattato. Le motivazioni per un così basso ritorno sono molteplici, e differenti a secondo del tipo e delle dimensioni dell'azienda/ente: politiche interne di non comunicare questo tipo di informazioni, necessità di chiedere permessi a più alti livelli, mancanza di tempo del possibile compilatore, incapacità di rispondere a tutte le domande.

Il numero di risposte ricevute sono comunque sufficienti e significative a fornire delle concrete indicazioni sugli attacchi ai sistemi informativi in Italia. L'analoga iniziativa statunitense CSI[7], e modello di riferimento per OAI, raccoglieva (fino al 2011) un campione attorno ai 350 rispondenti per tutti gli Stati Uniti. Tenendo anche conto delle diverse coperture geografiche Italia ed USA, il campione di risposte è più che sufficiente ai fini indicativi, se non statistici, ed agli obiettivi dell'indagine.

4.1 Chi ha risposto: ruolo e tipo di azienda/ente

Il bacino di utenza contattato è costituito da CIO, CSO, CISO e da altre figure, ai fornitori ed i consulenti, che

[7] CSI, Computer Security Institute, si veda http://gocsi.com/survey

gestiscono per l'azienda/ente la sicurezza informatica, fino ai responsabili di massimo livello soprattutto nelle aziende piccole e piccolissime (proprietari, presidenti e amministratori) che direttamente o indirettamente conoscono e decidono per i loro sistemi informativi e la relativa sicurezza.

La fig. 1 sintetizza 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", le figure operanti sulla sicurezza nell'Unità Organizzativa Sistemi Informativi (UOSI), al terzo posto i vertici della struttura (Presidenti, Amministratori Unici o Delegati, Direttori Generali). 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, i responsabili della sicurezza informatica (CISO) e per ultimi i responsabili della sicurezza aziendale (CSO).

Facendo riferimento anche alle dimensioni dell'azienda/ente (fig. 3), è evidente che un esplicito ruolo di CISO è presente solo nelle strutture più grandi.

Il terzo posto del top management è un chiaro indicatore che, soprattutto nelle medie e piccole imprese (PMI), la sicurezza informatica è così importante per la continuità operativa del business da essere decisa e controllata dai vertici.

La fig. 2 illustra la suddivisione dei compilatori per i settori merceologici di appartenenza delle loro aziende/enti. In questa edizione, onde evitare possibili errore 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 (Codici Ateco H)
6. Attività finanziarie ed assicurative: assicurazioni, banche, istituti finanziari, broker, intermediazione finanziaria, ecc. (Codici Ateco M)
7. Servizi turistici, di alloggio e ristorazione: agenzie di viaggio, tour operator, hotel, villaggi turistici, campeggi, ristoranti, bar, ecc. (Codici 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 (Codici Ateco R)
9. Stampa e servizi editoriali (Codici 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 assi-

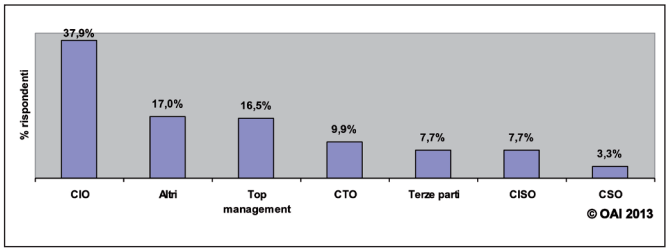

Fig. 1 - Ruolo rispondenti

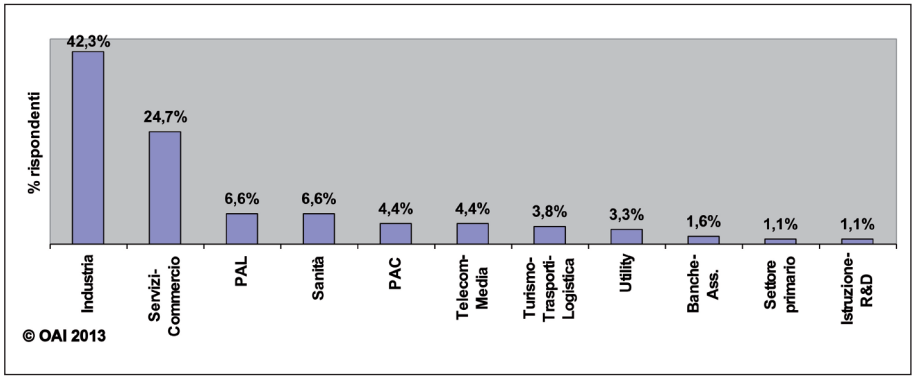

Fig. 2 - Settore merceologico di appartenenza

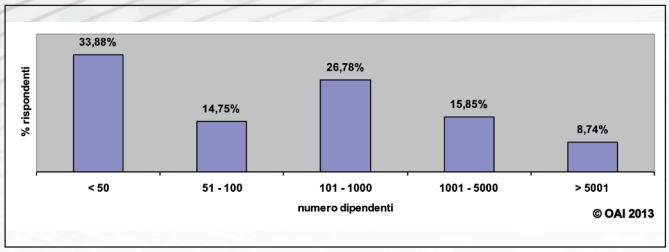

Fig. 3 - Dimensioni aziende/enti per numero dipendenti

stenza 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. (Codici Ateco Q)
14. Istruzione: scuole e università pubbliche e private (Codici Ateco P)
15. Associazioni, associazioni imprenditoriali e sindacati (Codici Ateco S94)
16. PAC, Pubblica Amministrazione Centrale
17. PAL, Pubblica Amministrazione Locale

A livello di rielaborazione dei dati, per rendere il grafico di fig. 2 più semplice e confrontabile con quello dell'edizione precedente, si sono raggruppati in "Servizi-Commercio" i punti 4, 7, 8, 9, 10, 11, 15. di cui sopra, e in "Turismo-Trasporti-Logistica" i punti 5 e 7.

In questa edizione, rispetto a quella precedente, il settore Industria è più rappresentato di quello dei servizi e commercio. Il buon incremento di rispondenti, maggiore del +43%, rispetto all'anno precedente ha riguardato prevalentemente l'ambito industriale. Pur con questo incremento, come nelle precedenti edizioni, rimangono ancora percentuali basse alcuni settori, in particolare per quelli del Turismo-Trasporti-Logistica e delle Banche e Assicurazioni. Le motivazioni sono diverse. I settori Turismo-Trasporti-Logistica non sono stati raggiunti che parzialmente dalla campagna di invito a rispondere, probabilmente perché sono relativamente pochi i loro riferimenti negli elenchi di e-mail dell'editore e dei patrocinatori. Per quanto riguarda Banche e Assicurazioni, pur avendo sollecitato direttamente vari responsabili dell'ICT, molti erano impegnati in quel periodo con iniziative della Banca d'Italia, altri hanno risposto che per policy interne non potevano rispondere a questionari tipo OAI.

La fig. 3 illustra la ripartizione percentuale delle aziende/enti dei rispondenti per dimensioni, in termini di numero di dipendenti; come negli anni precedenti la ripartizione è abbastanza bilanciata tra piccole, medie e grandi organizzazioni: il numero maggiore di rispondenti è in strutture con meno di 50 dipendenti, come è tipicamente la dimensione della stragrande maggioranza delle imprese italiane.

L'area geografica di copertura dell'azienda/ente è, per il campione raccolto, prevalentemente nazionale, ma il 23,6% circa ha una copertura internazionale, a livello europeo o mondiale, come mostrato dalla fig. 4.

Nella fig. 5 i rispondenti dell'area solo nazionale sono dettagliati per copertura Nord-Centro-Sud e Isole o dell'intero territorio. Più della metà dei rispondenti opera al Nord, più di un terzo opera sull'intero territorio nazionale e relativamente pochi, a decrescere, nel Sud-Isole e nel Centro.

Dato che il Questionario 2012 copre sia l'anno 2012

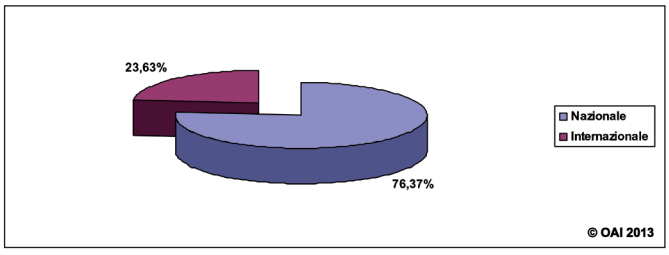

Fig. 4 - Copertura geografica azienda/ente

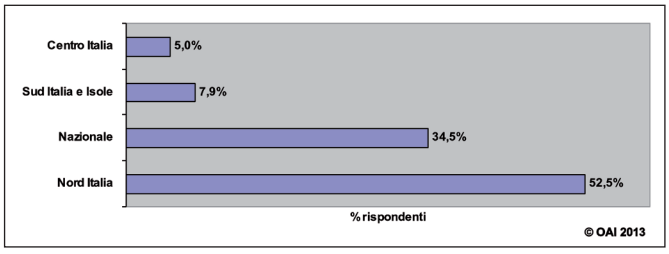

Fig. 5 - Ripartizione sul territorio nazionale

che il 1° semestre 2013, per la correttezza delle risposte fornite si è voluto accertare che l'azienda/ente esistesse e fosse operativa già nel 2012, in caso contrario si richiedeva di inserire la risposta <Mai> per il 2012: tra i rispondenti, una sola società ha iniziato ad operare nel 2013.
Per gli aspetti organizzativi sulla gestione della sicurezza informatica si rimanda a § 6.4.

4.2 Caratteristiche dei sistemi informatici

Questo paragrafo fornisce indicazioni sui sistemi informatici delle Aziende/Enti nei o per i quali operano i compilatori del questionario. Volutamente, le informazioni richieste non sono di dettaglio: questo al fine di garantire un ulteriore livello di riservatezza per chi ha risposto, impedendo l'identificazione del sistema dai dettagli tecnici, e in secondo luogo per non appesantire l'impegno con un'eccessiva richiesta di tempo per la compilazione.
I dati richiesti sono finalizzati ad inquadrare la "macro" struttura del sistema informatico, individuata dal numero di Data Center (D.C.) e da come sono gestiti, dal numero complessivo di server e di posti di lavoro, dai sistemi operativi e dai database in uso.
La fig. 6 schematizza se il sistema informativo è basato su uno o più D.C. o "computer room" per le realtà più piccole e per quelle decentrate, e la fig. 7 illustra come questi sono gestiti, se internamente (si usano anche in italiano i termini inglesi "on premise" o "in house") o sono terziarizzati o se in un mix di gestione interna ed esterna. In caso di sistema informatici costituiti da un insieme di PC singoli ed autonomi distribuiti sul territorio interconnessi tra loro senza server, questi sono stati assimilati a sistemi distribuiti con più "computer room".
Da questi dati emerge, e verrà confermato con successivi dati più avanti, come i sistemi informativi dei rispondenti, pur di dimensioni e capacità diverse, si collocano prevalentemente in una fascia medio-alta dal punto di vista tecnico e delle misure tecniche di sicurezza in atto.
Come mostrato in fig. 7, la maggior parte dei sistemi informativi, quasi il 60% del campione, è in parte o totalmente terziarizzata, con uso anche di cloud computing. Una parte comunque considerevole, quasi il 41%, è ancora totalmente gestito all'interno dell'azienda/ente.
Questi dati confermano quanto già evidenziato nel precedente rapporto: il cambio di mentalità e di approccio nei riguardi della terziarizzazione e dell'ICT "as a service". Si consideri che il campione del Rapporto OAI 2010 indicava che ben il 72,3% dei sistemi erano gestiti totalmente all'interno. In pratica nel giro di poco più di due anni questa percentuale si è quasi dimezzata, pur se il campione dei rispondenti era parzialmente diverso dall'attuale.
Per comprendere le dimensioni dei sistemi informativi del campione emerso dall'indagine, la fig. 8 mostra in percentuale il numero di server, sia fisici che virtuali, presenti nei vari ambienti di produzione, di test e di sviluppo. I dati sono percentualmente analoghi a quelli raccolti nelle precedenti edizioni: la stragrande maggioranza dei siste-

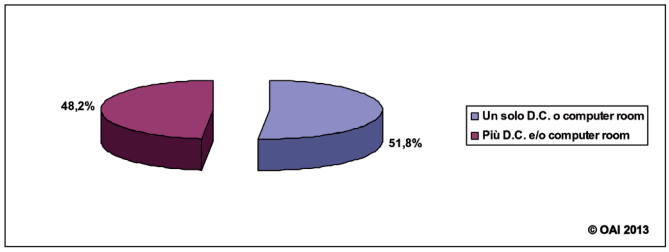

Fig. 6 - Data Center (D.C.) e computer room

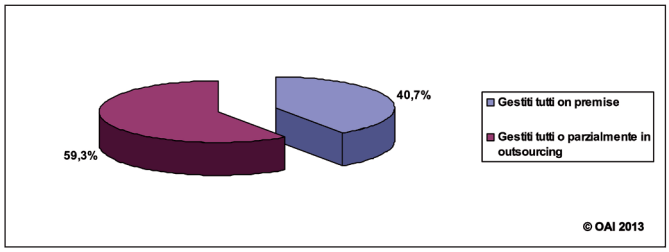

Fig. 7 - Modalità di gestione del sistema informativo

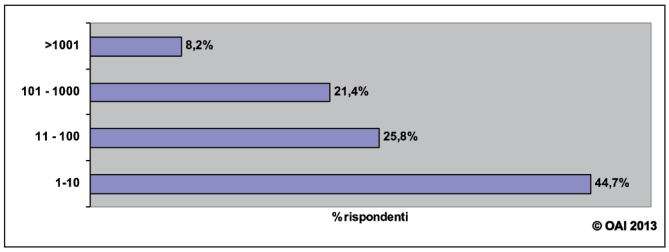

Fig. 8 - Numero complessivo di server fisici e virtuali

mi ha al massimo fino a 100 server, con ben più del 44% del totale che arriva solo a 10, come è tipico per strutture di piccole organizzazioni.
La fig. 9 mostra le percentuali del numero di posti di lavoro fissi (PdL) per sistema informativo: quasi il 55% dei rispondenti ha fino a 100 PdL fissi,e tra questi la grande maggioranza è tra 10 e 100 PdL; a questo si aggiunge il non trascurabile dato del 23,1% tra 101 e 1000 PdL, che conferma che il dato del 26,78% strutture tra 100 e 1000 dipendenti (fig. 3) e che un'altra buona parte del campione emerso è di aziende/enti di "medie" dimensioni. Tenendo conto che quasi la metà dei rispondenti ha fino a 100 dipendenti, come risulta dalla fig. 3, questo significa che più o meno ogni dipendente è dotato di un PC, indipendentemente dal settore merceologico e dal tipo di ruolo del dipendente.
In termini di sicurezza i dispositivi mobili, in particolare smatphone e tablet, stanno giocando un ruolo crescente e critico, data la loro esplosiva diffusione, oltre che per il fenomeno della "**consumerizzazione**" e del **BYON**, Bring Your Own Device, che consente all'utente finale di utilizzare i propri dispositivi mobili per attività sia personali che di lavoro. Tablet e smartphone di fatto rappresentano l'attuale era "post PC": e dalla scorsa edizione sono stati considerati nell'indagine. La fig. 10 mostra la percentuale per numero di dispositivi mobili di proprietà della azienda/ente forniti ai dipendenti: per non appesantire, il questionario non richiedeva di specificare i tipi diversi di dispositivi mobili, e ragionevolmente la maggior parte dovrebbe essere costituita da smartphone. Interessante notare che la diffusione maggiore in percentuale è data da aziende/enti con un numero di dispositivi mobili tra 10-100, confermando quanto evidenziato anche nella precedente edizione.
La fig. 11 evidenzia il fenomeno della "consumerizzazione": per ben più di un terzo dei rispondenti non è consentito (ancora) il BYOD, confermando anche in questo caso il dato emerso nel precedente rapporto, pur con un bacino di rispondenti diverso.
Nelle fig. 10 ed 11 la voce "Non si sa" indica una piccola percentuale che ha risposto di non conoscere i numeri e la realtà aziendale sul mobile: 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 includendo i CIO costituiscono la maggior parte dei rispondenti, possono ignorare le dimensioni di questo fenomeno. Queste risposte sono un concreto riscontro della correttezza dei compilatori che 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. 12 sintetizza, nel campione emerso dall'indagine, la diffusione dei principali sistemi operativi per server in uso. Le risposte possibili sul questionario erano multiple, in quanto i sistemi informatici, soprattutto quelli di medie e grandi dimensioni, usano contemporaneamente più

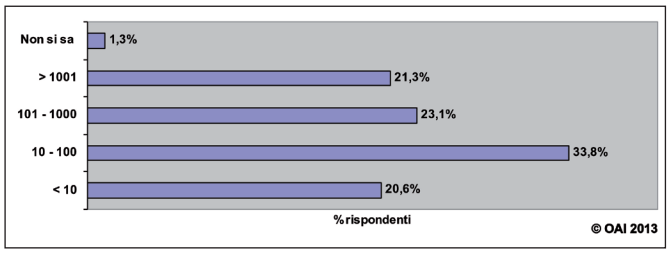

Fig. 9 - Posti di lavoro (PdL) fissi

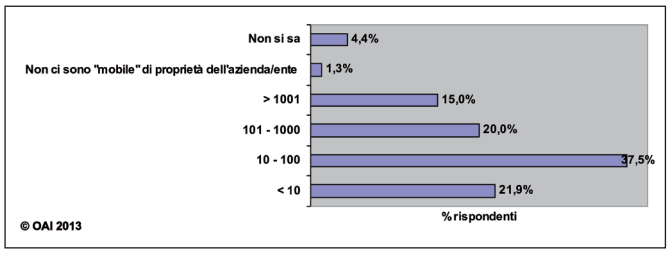

Fig. 10 - Dispositivi mobili dell'Azienda/Ente

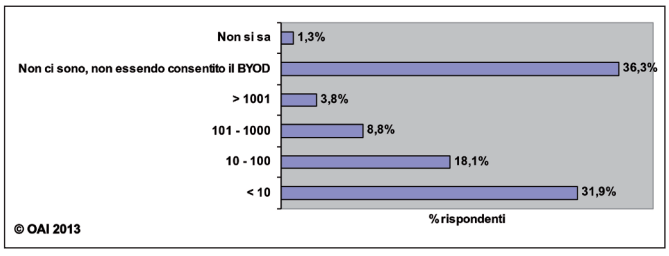

Fig. 11 - Dispositivi mobili proprietà utente finale

sistemi operativi. La fig. 12 evidenzia come Windows Server, nelle sue varie versioni, sia utilizzato dalla gran parte dei server del campione. Le più recenti versioni di Windows Server, la 2012 e la 2010, sono abbastanza diffuse, con circa il 40% ciascuna, ma come è logico sono più diffuse complessivamente le precedenti versioni, quali 2008, 2003 e forse anche 2000, incluse nella voce "Windows Server pre 2010", che arriva quasi al 65%. Mainframe, come l'IBM System z e supercomputer costituiscono una nicchia non trascurabile attorno al 10%, tipicamente come "host" centrali di grandi organizzazioni quali industrie a livello internazionale, banche e PAC. I sistemi Linux coprono più della metà del campione, e quelli Unix poco più di un 1/5.

La figura evidenziata una forte diffusione, con una quota del 45,3%, di sistemi operativi tipo "hypervisor" per la virtualizzazione dei server, che includono prodotti quali Z/VM, VMWare, ESX, XenServer, Hyper-V. Insieme a quelle su Windows server 2010 e 2012, queste percentuali indicano che il campione emerso ha un buon livello di aggiornamento tecnico. I sistemi AS 400, storicamente diffusi nelle PMI di fascia medio-alta, con il loro OS 400, mantengono in Italia una quota interessante, simile a quella rilevata nella precedente edizione (17,1%); questo dato ulteriormente conferma che i sistemi informatici di medie-grandi dimensioni sono eterogenei, ma anche come il mercato sia ormai dominato da due famiglie di prodotti: i sistemi operativi Windows ed i sistemi operativi Linux-Unix.

In fig. 13, con risposte multiple e congruenti con la diffusione dei sistemi operativi di cui sopra, il database (DB) più diffuso è Microsoft SQL, che copre circa i 3/4 dei rispondenti, seguito dall'open source MySQL, diffuso quasi per la metà dei rispondenti, che a sua volta sopravanza di poco Oracle. La presenza di mainframe IBM e di AS/400 porta alla presenza dei DB tipici per questi ambienti, l'IBM DB2 e il DB IBM AS/400, anche se con percentuali assai più basse. Nello stesso sistema informativo possono sono spesso usati contemporaneamente diversi DB.

Qualche sistema di piccole dimensioni non ha alcun DB, e lo storage si basa solo su file system. Come "Altro" sono specificati per lo più DB quali Postgres, PostgreSQL, Access, seguiti da Adabas, Firebird, Ingres, InterBase, Lotus Domino.

I dati sui DB confermano il buon livello tecnico e l'eterogeneità di massima dei sistemi informativi del campione, anche se l'omogeneità è tipica degli ambienti piccoli o piccolissimi: per quelli Microsoft la scelta è di solito Microsoft SQL, per quelli Linux-Unix è MySQL.

Per quanto riguarda le reti ed Internet, come mostrato in fig. 14 tutti i sistemi informativi dei rispondenti sono collegati ad Internet (a parte un solo caso, forse un errore, comunque non considerato nel calcolo e quindi nella figura), con una o più connessioni fornite anche da fornitori diversi. La stragrande maggioranza dei sistemi ha reti locali "wired" (LAN, Local Area Network), ma quelle "wireless"

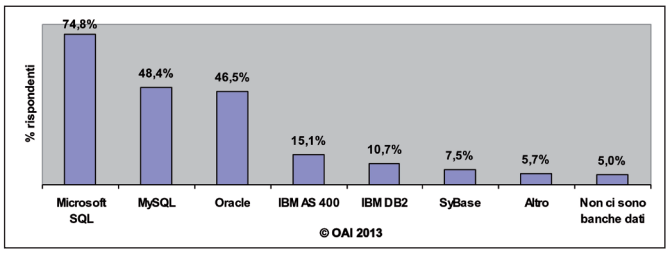

Fig. 13 - Banche dati in uso (risposte multiple)

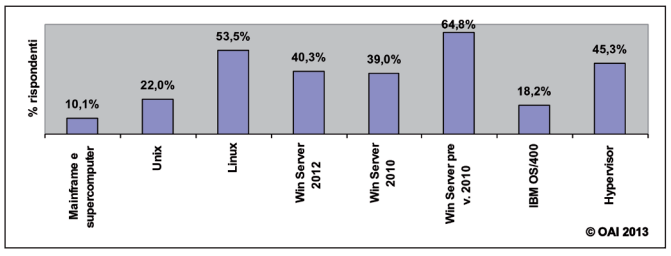

Fig. 12 - Sistemi Operativi dei server in uso (risposte multiple)

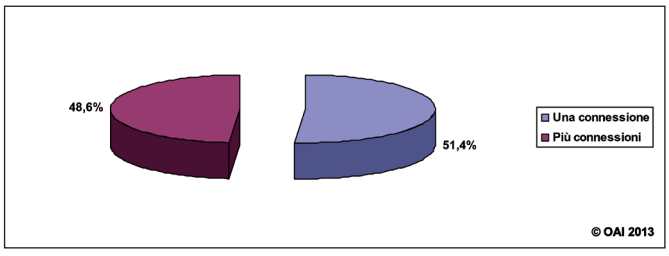

Fig. 14 - Connessioni ad Internet con uno o più fornitori

(WLAN, Wireless LAN) arrivano al 70%, come mostrato in fig. 15. Questo significa che nella maggior parte dei casi coesistono LAN e WLAN: queste ultime, più o meno integrate con il resto del sistema informatico ed accessibili dai dispositivi mobili, aprono un ampio fronte di attacchi, sia a livello delle infrastrutture ICT, sia delle applicazioni sui server e sui dispositivi mobili usati dagli utenti finali. Una piccola percentuale, il 5%, non ha reti locali ma solo PC autonomi, ciascuno che si collega ad Internet: è il tipico caso di piccole e piccolissime strutture. Questo è il caso di piccolissime aziende, assai diffuse in Italia, con due o tre persone operanti. I collegamenti ad Internet, oltre che ad "esportare" sulla rete applicazioni quali i siti web e/o per accedere a siti ed applicazioni, sono usati anche per la telefonia su Internet, chiamata VoIP, Voice over IP: essa è adottata da circa il 42% del campione, simile al dato dell'edizione precedente.

In termini di sicurezza su internet, quasi i 2/3 utilizza VPN, Virtual Private Network, e quasi il 43,8% utilizza tecniche di SSL/TSL, Secure Socket Layer/Transport Layer Security[8] per stabilire collegamenti sicuri.

Quest'ultimo dato richiede un commento: dato che le tecniche SSL/TLS sono usate anche in reti con VPN, avrebbero dovuto avere una percentuale maggiore del VPN; dato che la rilevazione porta ad una percentuale inferiore, questo significa che rispondenti con VPN possono aver segnalato SSL/TLS solo nei casi di uso di HTTPS per l'accesso ai loro siti web e/o a siti ed applicazioni remote. Le fig. 17 e 18 forniscono più approfondite indicazioni sulla terziarizzazione e sull'uso del cloud computing, rispetto a quanto rilevato nella fig. 7. Tenendo presente che la domanda prevedeva la possibilità di risposte multiple, la prima figura mostra che quasi 1/4 dei rispondenti non terziarizza affatto. Per il restante che terziarizza, quasi il 37% utilizza housing-hosting in maniera parziale o totale, il 15% terziarizza la gestione operativa, completa o parziale, del sistema informatico ed il 10,6% terziarizza a società o professionisti specializzati la gestione della sicurezza ICT dei propri sistemi. La fig. 18 dettaglia, sempre con risposte multiple, l'uso o non dei servizi cloud. Dal campione emerge che più di 1/3 del campione non usa alcun tipo di soluzione cloud, similmente alla passata

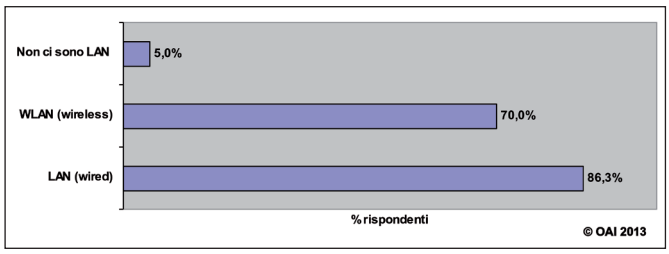

Fig. 15 - LAN e WLAN (risposte multiple)

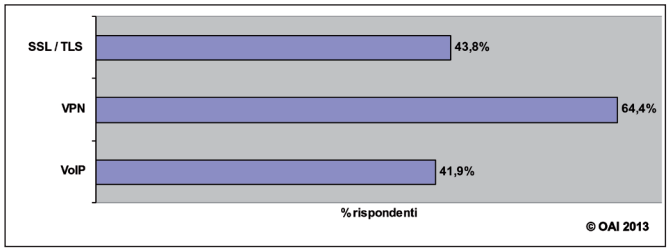

Fig. 16 - Utilizzo di VoIP, VPN, SSL/TLS (risposte multiple)

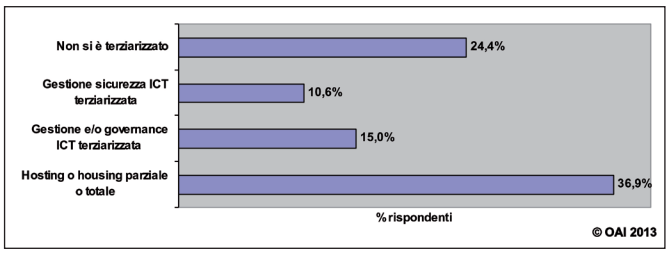

Fig. 17 - Terziarizzazione dei sistemi e della loro gestione (risposte multiple)

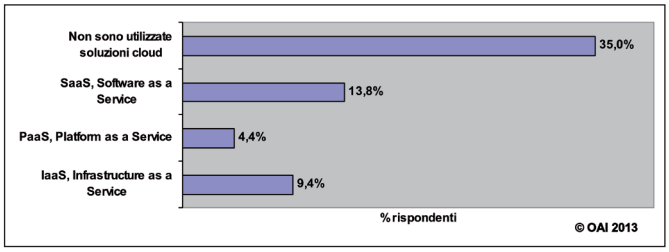

Fig. 18 - Uso di cloud (risposte multiple)

[8] Sono le tecniche usate per lo scambio crittato di dati dal protocollo HTTPS disponibile su tutti moderni browser ed usato per connessioni sicure ai web, tipicamente per transazioni bancarie, per prenotazioni, per acquisti, per pagamenti, ecc.

edizione. Tra chi utilizza il cloud, la quota maggiore, il 13,8%, usa SaaS, il 9,4% IaaS e solo il 4,4% PaaS.
Confrontando i dati sulla terziarizzazione e sul cloud, si evince che la terziarizzazione, in particolare housing e hosting, è più utilizzata dai rispondenti rispetto a soluzioni cloud. Come già evidenziato nel precedente rapporto, oltre che da altri recenti rapporti e guide[9] 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 e sulla disponibilità. Per il cloud l'aspetto "sicurezza" è una competenza-caratteristica tipica del fornitore, che deve riuscire a garantire al cliente il necessario (e richiesto) livello di sicurezza e fiducia (in inglese "trust").
Per la sicurezza informatica, soprattutto dopo gli attacchi STUXNET ai sistemi di controllo delle centrali nucleari iraniane[10], hanno assunto particolare rilievo i sistemi di controllo dei processi produttivi e di robotica. Come nella precedente edizione, OAI ha posto specifiche domande in merito, e la fig. 19 mostra i risultati raccolti dal campione, simili a quelli riscontrati nelle precedenti edizioni: quasi il 17% dispone di tali sistemi, rispetto al 14,4% e al 13,4% precedenti. Questo piccolo aumento è dato dal bacino di rispondenti più ampio e a maggioranza del settore industriale.
Una piccola % dei compilatori ha ammesso di non avere informazioni su tali sistemi. Spesso nelle grandi aziende italiane i sistemi informatici di controllo della produzione (e/o di processi chimici, nucleari, dei magazzini, ecc.) sono considerati "impianti", sotto il controllo della produzione, nemmeno contabilizzati come sistemi informatici. In tali casi può capitare che il compilatore del questionario, nella maggior parte dei casi il CIO o un suo collaboratore nell'UOSI, non conosca neppure la loro esistenza. Come già indicato per i sistemi mobili, questa percentuale di "non so" è una conferma della correttezza e serietà dei rispondenti, che avvalora la credibilità delle risposte date, e di conseguenza dei dati del Rapporto OAI 2013.
Per la parte del campione che ha questi sistemi ICT di controllo, essi si basano prevalentemente su ambienti Microsoft Windows e Dot.Net, come mostrato nella fig. 20; il 26,5% utilizza (anche o solo, la domanda prevedeva risposte multiple) ambienti Linux-Unix e quasi il 6% utilizza (anche o solo) ambienti proprietari. Anche in questo contesto i server Windows sono divenuti dominanti.
Sempre per questa parte di rispondenti, la fig. 21 mostra

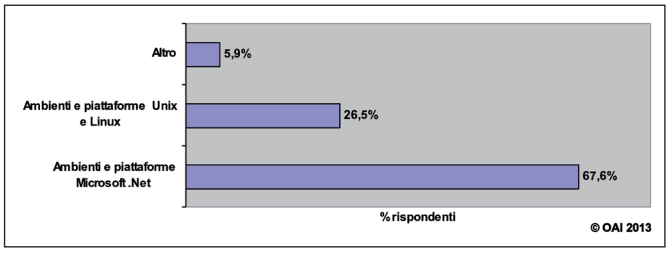

Fig. 20 - Piattaforme riferimento ambienti ICT per controllo processi industriali, ecc. (risposte multiple)

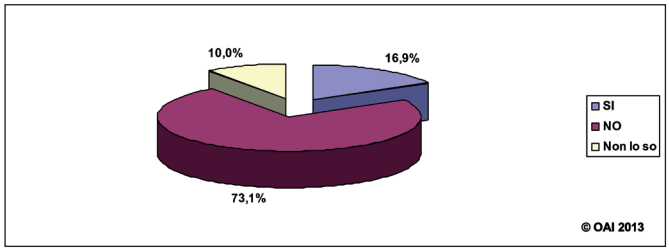

Fig. 19 - Sistemi ICT per robotica e controllo processi produzione

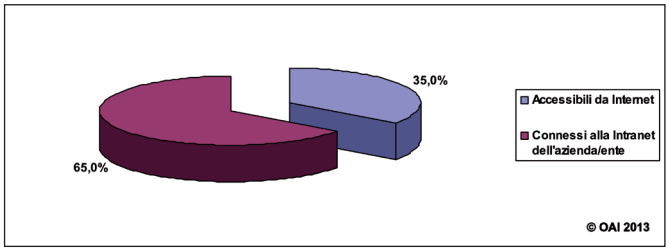

Fig. 21 - Connessione dei sistemi di controllo (risposte multiple)

[9] Si veda anche la "Guida al cloud - Nella Nuvola la stella cometa per il Manager" di M.R.A. Bozzetti, pubblicata da Soiel per Seeweb a novembre 2012 e scaricabile gratuitamente da http://www.malaboadvisoring.it/
[10] 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

(risposte multiple) che tali sistemi nel 65% dei casi sono collegati alla Intranet dell'azienda/ente, ed il 35% sono direttamente accessibili da Internet, ad esempio per gestione e/o manutenzione da remoto tramite società terze. La fig. 22 mostra che la gestione di questi sistemi ICT per il controllo industriale e la robotica sono gestiti e controllati centralmente in maniera integrata con l'intero sistema informativo dall'UOSI in poco più della metà dei casi, mentre per poco meno dell'altra metà sono autonomamente controllati e gestiti dalle specifiche Direzioni/Linee di Business che li utilizzano.

5. Gli attacchi informatici rilevati e la loro gestione

La fig. 23 mostra, percentualmente, il numero di attacchi rilevati dai rispondenti nel 2012 e nel 1° semestre 2013. Nel 2012 il 61,3% non ha mai rilevato un vero attacco intenzionale, 38,7% li ha invece subiti e rilevati, e tra questi il 6,7% ha subito più di 10 attacchi nell'anno. Nel 1° semestre il 68% non li ha rilevati, ma del 32% che li ha subiti ben il 7,3% ne ha rilevati più di 10. Tendenzialmente queste percentuali indicano che nel 2013, a consuntivo, si potrebbero registrare un numero di attacchi complessivamente superiori al 2012, e soprattutto superiori per numero di attacchi nell'anno sulla stessa azienda/ente. L'aumento del numero di attacchi nel 2013 è in effetti confermato da tutte le varie indagini pubblicate a livello internazionale.

La fig. 24 confronta il numero di attacchi subiti e rilevati dai rispondenti nei diversi Rapporti OAI dal 2008 al primo semestre 2013, ben sapendo che i campioni emersi in questi anni sono diversi come mix e come numero; il confronto è quindi statisticamente non corretto, ma, per i motivi illustrati in § 1.1, l'indicazione che emerge è significativa e rappresentativa di una precisa tendenza.

Il confronto evidenzia alcuni macrofenomeni rilevati anche da altri rapporti nazionali ed internazionali. Nell'arco temporale considerato, il 2008 rappresenta l'"annus horribilis" per la quantità di attacchi occorsi, e grazie agli interventi tecnici ed organizzativi di prevenzione e protezione seguiti, nell'anno seguente il numero di attacchi complessivi è diminuito di 10 punti percentuali, per poi oscillare attorno al 40%. Interessante evidenziare che nella fascia di "Più di 10" attacchi, la % in media tra il 2007 ed il 2012 è del 6,5%, con oscillazioni attorno a qualche decimo di punto, ma nel solo 1° semestre 2013 è aumentata al 7,3%, e tale incremento è sicuramente preoccupante ed un chiaro indicatore dell'incremento di attacchi nel 2013.

Facendo riferimento alle principali tipologie di attacco elencate nella Tabella1 e subite dai sistemi informativi del campione 2013, la fig. 25 mostra che:

- al primo posto permane il **malware** che nel 2012 ha coinvolto il 64,8% dei rispondenti, e nel 1° semestre 2013 il 57,7%; sull'evoluzione dei codici maligni si approfondisce in § 5.1;

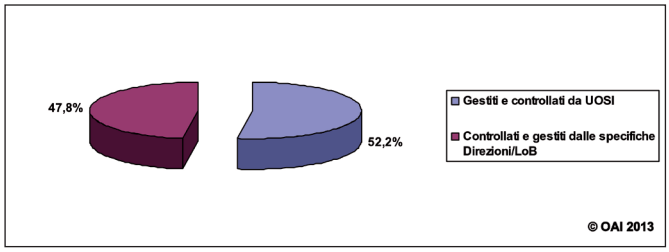

Fig. 22 - Modalità di gestione sistemi di controllo

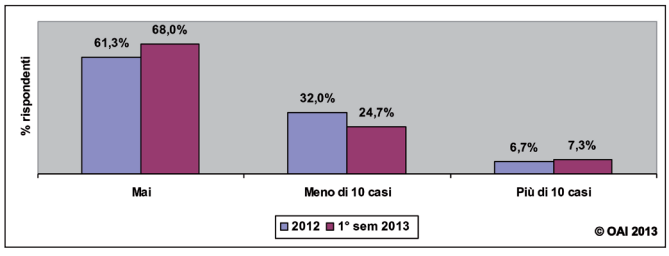

Fig. 23 - Attacchi rilevati nel 2012 e nel 1° semestre 2013

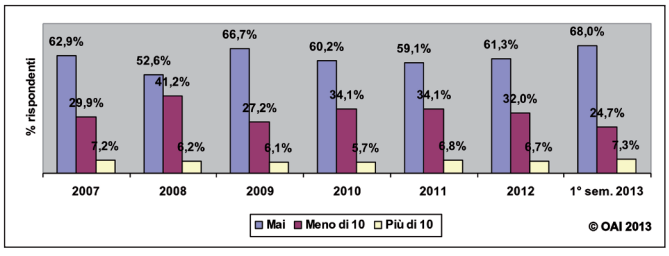

Fig. 24 - Attacchi rilevati dal 2007

- al secondo posto permane il **social engineering**, che nel 2012 ha colpito il 46,5% dei rispondenti, e nel 1° semestre 2013 il 44,4%. Il "social engineering" è alla base dei principali attacchi, anche complessi (si veda APT e TA), avvenuti negli ultimi anni, ed include come specifica tipologia il **phishing**, che dalla posta elettronica si è esteso negli ultimi anni agli SMS, alle chat, ai social network;
- al terzo posto si posiziona il **furto di dispositivi ICT** che nel 2012 ha colpito il 44,4% dei rispondenti, e nel 1° semestre 2013 il 33,1%; nella precedente edizione era al quarto posto preceduto dalla **saturazione di risorse** (DoS/DDoS), che è ora al quarto posto, con 34,5% nel 2012 e 28,9% nel 1° semestre 2013.

Il 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.

Tutti gli altri tipi di attacchi, a parte lo sfruttamento delle vulnerabilità nel 2012 che copre il 22,5% del campione, si attestano sotto il 20%, e 7 tipologie sono al di sotto del 10%.

Confermando i trend individuati anche da numerosi altri rapporti, al quinto posto per diffusione si attestano gli attacchi basati sullo **sfruttamento delle vulnerabilità** dei programmi, 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 i così detti **zero-day**, ossia le vulnerabilità o che non sono ancora state individuate dalla casa madre (ma dall'attaccante sì) o per le quali non è stato ancora pubblicata la "patch" di correzione. Passa poi dal 10° posto della scorsa edizione all'attuale 6° posto il **furto di informazioni da dispositivi d'utente mobili**, scavalcando **le frodi** che passano dal 6° al 7° posto.

Il furto di informazioni da dispositivi d'utente mobili può essere correlato sia al furto "fisico" dei dispositivi sia alle numerose vulnerabilità dei sistemi operativi, da Android a iOS di Apple, da Windows Phone 8 a Blackberry 10, e delle relative applicazioni, chiamate in gergo "app".

Data l'enorme e rapida diffusione dei sistemi mobili, l'era "post PC", essi rappresentano la (relativamente) nuova frontiera degli attacchi informatici, unitamente alle sempre più diffuse reti wireless, incluse le WLAN, Wireless LAN che li supportano. Gli **attacchi alle reti**, ora più facilmente e quindi più frequentemente portati alle reti wireless, si posizionano al 9° posto rispetto all'8° della precedente edizione, con un 9,9 % del campione nel 2012 ed un preoccupante 11,3% nel 1° semestre 2013.

All'8° posto **l'accesso e l'uso non autorizzato dei sistemi**, visti come un'unica entità, che costituisce il primo dei tre possibili livelli d'accesso gerarchici e concatenati ad un sistema ICT quale un server, router, firewall, storage, ecc. Dopo aver superato questo primo livello si può tentare di **accedere illegalmente**, come 2° livello, ad **una applicazione operante** sul sistema ICT attaccato, ed anche **modificarla e/o riconfigurarla**, ed infine, come 3° livello, **accedere e manipolare senza autorizzazione i dati trattati dall'applicazione** attaccata (2° livello) sul sistema ICT attaccato (1° livello).

La concatenazione riuscita dei tre

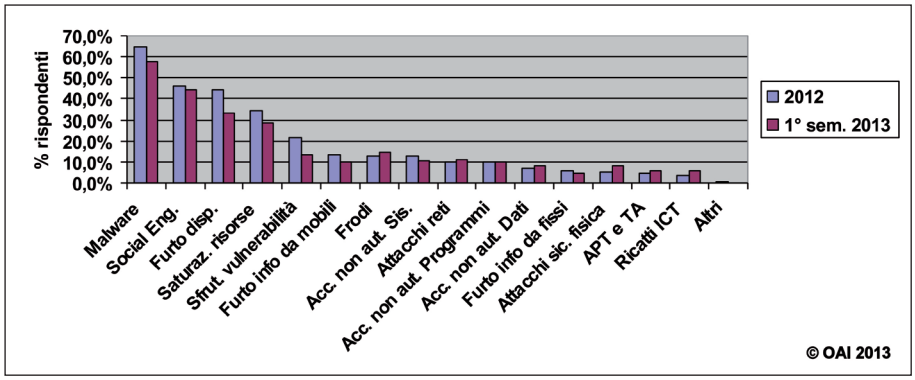

Fig. 25 - Diffusione tipologia attacchi subiti 2012 - 1° semestre 2013 (risposte multiple)

livelli di attacco può portare a serie e gravi conseguenze per la consistenza, integrità e correttezza dei dati e delle applicazioni che li trattano. Come nelle precedenti edizioni di OAI, questa critica trilogia d'attacco non sembra essere molto diffusa in Italia: nel 1012 i tre livelli d'attacco coprono rispettivamente il 12,7% (1°), il 9,9% (2°) e il 7,5% (3°). Nel 1° semestre 2013 rispettivamente 10, 6% (1°), 9,9% (2°) e 8,5% (3°).

L'accesso logico ai sistemi ICT senza averne i diritti avviene prevalentemente grazie alla conoscenza delle password di chi ne ha i diritti, ed è particolarmente critico quando si scoprono ed 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".

Il **furto dell'identità digitale** è alla base delle frodi informatiche, soprattutto per gli "account" di una persona fisica (ma anche giuridica, ossia di aziende/enti) in ambito bancario o di società di servizi.

La **frode informatica** si posiziona al 7° posto della classifica degli attacchi nel 2012 (era al 6° posto nel 2011), con un 12,7% del campione e con un 14,8% nel 1° semestre 2013. La riduzione percentuale riscontrata rispetto al Rapporto OAI 2012 è dovuta soprattutto al forte aumento del numero di rispondenti del settore industriale, e quindi della riduzione relativa, nell'ambito del campione complessivo, dei rispondenti dei settori dei servizi, delle banche ed assicurazioni, delle TLC e delle utility, che sono i settori più attaccabili e attaccati. Tipici esempi di frodi informatiche 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.

Concettualmente contiguo alla frode il **ricatto informatico**, spesso portato con codici maligni chiamati ransomware, posizionato nel 2012 in fondo alla classifica degli attacchi con un 3,5%, ma con un preoccupante incremento al 5,6% nel 1° semestre 2013.

Pur con percentuali basse e tra gli ultimi nella classifica, gli attacchi alla sicurezza fisica non sono trascurabili con un 7,7% nel 2012 e un 8,5% nel 1° semestre 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.

È opportuno infine evidenziare la tipologia introdotta da questa edizione degli attacchi **APT, Advanced Persistent Threats**, e degli attacchi mirati, i così detti **TA, Targeted Attacks**, basati su uso contemporaneo e/o persistente di più tecniche sofisticate di attacco. Costituiscono la frontiera più critica, in quanto si tratta di attacchi condotti da tecnici competenti e con notevoli risorse. TA ed APT sono di norma rivolti ad infrastrutture critiche per la nazione e che sconfinano con vere e proprie azioni di "guerra informatica": esempi[11] ormai ben noti di questi attacchi a livello mondiale, iniziati presumibilmente nel 2009, sono l'Operazione Aurora, Stuxnet, LuckyCat, DigiNotar, Global Payments Inc., Flame, e così via. Pur se di difficile identificazione, APT e TA iniziano ad essere presenti anche in Italia: per il 2012 i rispondenti hanno dichiarato che un non trascurabile 4,9% ha rilevato attacchi di questo tipo e che nel solo 1° semestre 2013 tale percentuale è salita al 5,6%. Dati che trovano conferma nell'indagine IDC[12] in Italia su un campione di grandi aziende ed enti dai 1000 dipendenti in su di tutti i settori merceologici, incluse le pubbliche amministrazioni: il 9,6% degli intervistati ha rilevato almeno un attacco APT, che ha determinato un impatto rilevante sul business aziendale nel 2,2% dei casi, mentre nel restante 7,4% dei casi l'attacco è stato neutralizzato in tempo oppure ha sortito un impatto limitato sul business aziendale.

[11] 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

[12] La ricerca, effettuata da IDC per Trend Micro, ha come titolo "La diffusione del rischio APT in Italia " ed è scaricabile da http://www.trendmicro.it/

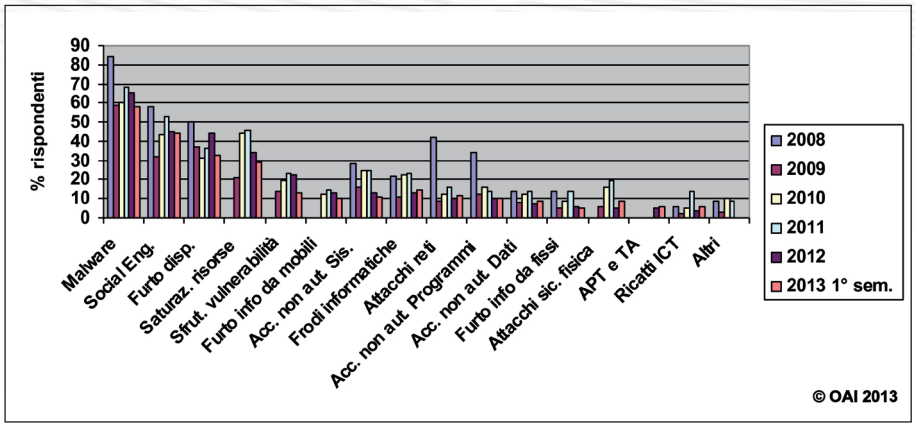

Fig. 26 - Confronto diffusione attacchi 2008-1° semestre 2013 (risposte multiple)

Il Questionario 2013, così come quelli delle precedenti edizioni, ha posto la voce "**Altri**" e la possibilità di specificare quale tipo di attacco, non classificato nella tipologia elencata in Tabella 1, era stato subito. Negli anni precedenti in questa voce venivano inclusi anche gli APT ed i TA, che con la presente edizione costituiscono una nuova tipologia. A parte pochi attacchi evidenziati che potevano essere inclusi nelle altre tipologie non è emerso per il 2012-13 alcun specifico attacco che non potesse rientrare nella tassonomia proposta.

La fig. 26 pone a confronto le percentuali di attacchi subiti dal 2008, pur con le considerazioni già espresse sui campioni diversi nelle quattro edizioni del rapporto OAI. Dal confronto nel grafico chiaramente emerge come:

- il 2008 rimane l'"annus horribilis" con la più alta percentuale per ciascun tipo di attacco considerato (alcuni non lo erano e manca la barretta relativa in figura);
- il "malware" rimane al primo posto in tutti gli anni come tipo di attacco più diffuso;
- "social engineering", saturazione risorse ICT (DoS/DDoS) e furto di apparati si alternano nelle sottostanti tre posizioni, con coperture % dei campioni dal 21 al 58%;
- dopo il 2008 è il 2011 l'anno con la più alta diffusione delle varie tipologie di attacco.

Il Questionario 2013, così come quello del 2012, ha richiesto, a seguito di 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. 27. La maggior parte degli attacchi nel complesso sono occorsi fino a dieci volte per anno con impatti poco significativi, ed hanno interessato quasi il 70% del campione. Più di 10 attacchi con impatti poco significativi hanno interessato circa 1/5 del campione. I **forti impatti** si sono avuti nel 2012 in media nel 5,5% dei casi ma con un incremento di più di un punto percentuale nel 1° semestre 2013. Le libere indicazioni di "impatto molto significativo" che alcuni rispondenti hanno fornito riguardano la non voluta formattazione di una SAN, il blocco e la non usabilità dei dati di back up, il blocco dei sistemi UPS, il recupero dati in camera bianca.

Confrontando questi dati con quelli dell'edizione precedente, pur con tutte le precauzioni più volte sottolineate data la differenza del campione, emerge che gli ordini di grandezza degli impatti significativi sono simili.

Sempre in termini di impatto, una domanda specifica chiedeva la stima del danno economico, cui pochissimi hanno risposto. Le poche indicazioni avute variano da pochi centinaia di Euro a € 70.000. Specifiche indagini a livello internazionale hanno fornito indicazioni in merito, che comunque devono essere prese con grandi precauzioni per il contesto italiano.

Una recente indagine del Kaspersky Lab[13] a livello mon-

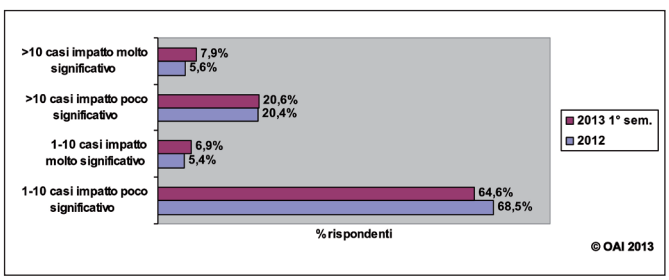

Fig. 27 - Impatto dell'attacco

diale stima che un singolo attacco di malware abbia un costo medio di $ 74 per utente, e possa arrivare fino a $ 600. Un indagine[14] del Ponemon Institute condotta negli Stati Uniti ha accertato un incremento del costo degli attacchi del 78% rispetto a 4 anni fa. I costi maggiori, secondo tale indagine, sono causati da DoS/DDoS, da intrusioni sui siti web e dagli attacchi di vario genere che vedono il coinvolgimento anche di personale interno. Tali costi riguardano principalmente la perdita di informazioni e l'interruzione delle attività: la perdita di informazioni costituisce il 43% dei costi, e nel 2013 si stima una riduzione del 2% rispetto all'anno precedente. Le interruzioni di attività contribuiscono ai costi per il 36% ed hanno un aumento del 18% rispetto al 2012.

La recente indagine del CSIS[15], Center for Strategic and International Studies, mette in relazione il costo del cybercrime con il PIL, Prodotto Interno Lordo, stimando che questo crimine rappresenta una quota compresa tra lo 0,4% e l'1,4% del PIL mondiale: nell'estremo superiore una perdita valutabile attorno ai mille miliardi di $, cifra ritenuta tutto sommato contenuta, se confrontata con le perdite dovute al traffico di droga, che rappresentano il 5% del PIL mondiale.

Sulla valutazione dei danni subiti e sui criteri della loro valutazione, nell'ambito dell'indagine OAI, si veda anche il prossimo capitolo 6.

5.1 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 posti di lavoro che di server.

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 in § 9 e per ulteriori approfondimenti al già citato libro "Sicurezza digitale" dell'autore.

I codici maligni si basano soprattutto sulle vulnerabilità dei programmi software, che talvolta non sono eliminate in tempi brevi da patch e fix; spesso poi gli aggiornamenti per eliminarle ne introducono di nuove. Lo sfruttamento delle vulnerabilità del software, sia a livello applicativo che di software di base (middleware), al di là dei malware, è una tipologia di attacco diffusa, come evidenziato in fig. 25, dove risulta in 5° posizione.

Sulle vulnerabilità del software, che si estendono con le nuove tecnologie quali ad esempio i sempre più diffusi sistemi virtualizzati ed i sistemi mobili, in primis gli smartphone, vengono confermate le considerazioni già espresse nel precedente Rapporto 2012 e dettagliate in rapporti specializzati come quelli di IBM X-Force[16] e di Micro Trend[17], oltre che nei già citati articoli dell'autore nella Rubrica OAI sulla rivista Office Automation[18]:

- la maggior parte delle vulnerabilità possono essere sfruttate da remoto via rete;
- i tempi per la correzione delle vulnerabilità dei programmi software da parte dei fornitori sono talvolta lunghi e possono superare anche un intero anno;
- le maggiori vulnerabilità, sia in numero che in gravità, riguardano principalmente le piattaforme web e le applicazioni web personalizzate, e i sistemi mobili che vi accedono (app e browser su smartphone e tablet); per i primi gli attacchi si basano prevalentemente su SQL "injection" e su "cross-site scripting" (XSS), per i

[13] "Security in a multi-device world: the customer's point of view": http://media.kaspersky.com/pdf/Kaspersky_Lab_B2C_Summary_2013_final_EN.pdf

[14] "2013 Cost of Cyber Crime Study": http://www.hpenterprisesecurity.com/register/2013-fourth-annual-cost-of-cyber-crime-study-global

[15] http://csis.org/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf

[16] Si veda http://www-03.ibm.com/security/xforce/

[17] Si veda in particolare http://www.trendmicro.com/us/security-intelligence/current-threat-activity/index.html

[18] Si veda http://www.soiel.it/res/editoria/p/editoria.html per l'ultimo numero della rivista sfogliabile dagli utenti registrati, oppure http://www.malaboadvisoring.it/index.php?option=com_content&view=article&id=31&Itemid=50 per poter scaricare tutti gli articoli pubblicati nella rubrica

secondi sulle vulnerabilità dei sistemi operativi dei sistemi mobili e sulle locali applicazioni;
- molte vulnerabilità degli applicativi sono causate da uno sviluppo del software approssimativo e senza attenzione alla sicurezza, sia sui server che sui "client" e "mobile";
- le maggiori vulnerabilità per i PC sono nei browser, nelle applicazioni multimediali come Flash, e nei lettori dei principali formati testuali, come Acrobat Reader per i formati .pdf;
- richiedono particolare attenzione le vulnerabilità dei sistemi VoIP e wireless, spesso sottostimate;
- il software di base e delle "app" dei dispositivi mobili smartphone e tablet, essendo in continua evoluzione sotto la spinta della forte concorrenza tra Android, Microsoft Windows Phone e Apple iOS, presentano vulnerabilità sfruttate da molti attacchi, che ultimamente si concentrano proprio in tali ambiti.

Per approfondimenti ed aggiornamenti sugli attacchi e sulle vulnerabilità si rimanda ad un primo elenco di siti web di riferimento, che non ha alcuna pretesa di essere completo ed esaustivo, in § 10.2.

5.2 Le nuove e più critiche minacce

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 e 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.

La Tabella 2, derivata dal recente "ENISA Threat Landscape Report 2013"[19], elenca le principali minacce individuate come più critiche per le aree emergenti dell'I-CT: infrastrutture critiche, sistemi mobili, reti sociali (social networking), cloud computing, big data, Internet delle cose.

Nella Tabella 2 la freccia verticale verso l'alto indica una prospettiva di crescita della minaccia, 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.

5.3 Frodi informatiche e la risposta delle autorità italiane

L'orientamento degli attacchi informatici alle frodi e al ritorno economico, come evidenziato anche dalle successive fig. 64 e 65, vede il contrasto e la risposta da parte delle autorità competenti, in particolare della Polizia Postale e delle Comunicazioni e l'Autorità Giudiziaria.

Nell'ottica del crimine informatico con valenza economica un elemento chiave è il furto dell'identità digitale, che include i vari account per l'accesso ai servizi, da quelli bancari a quelli telefonici, e dei mercati digitali fino ai social network. In tale contesto i crimini informatici più diffusi in Italia riguardano il phishing, l'home banking ed i pagamenti con carte di credito e similari, indicati con il termine di "monetica".

Il fenomeno è rilevante e sono estremamente interessanti i dati forniti in merito dalla Polizia Postale e delle Comunicazioni, ed aggiornati per il 2013.

La Tabella 3 mostra la situazione relativa al phishing e agli attacchi nell'ambito dell'home banking. La Tabella 4 mostra analoghi dati relativi alle frodi informatiche via carte di credito.

Entrambe le tipologie si basano prevalentemente sul furto dell'identità digitale, ottenuta sovente con tecniche di

[19] http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats

Minacce (Top Threats)	Attuale Trend	Infrastrutture ICT critiche	Mobile Consulting	Social Networking	Cloud Computing	Trust Infrastructure	Big Data	Internet delle cose
Drive by Downloads	^	^	^	^	^	^	^	
Worms/Trojans	^	^	^	^	^	^	^	^
Code Injection	^	^	^	>	^	^	^	
Exploit Kids	^	>	^	^	^	^	^	
Botnets	>	^	^	^	^			
Danni fisici/furto/smarrimento	^	^	^	^	^	^	^	^
Furto di identità/Frode	^		^	^	^	^	^	^
Denial of Service	^	^			^			^
Phishing	^	^	^	^	^	^	^	^
Spam	>			^				
Rogueware/Ransomware/Scareware	^							
Fughe di dati (Data Breaches)	^		^		^	^	^	
Perdita di informazioni (Information Leakage)	^	^	^	^	^	^	^	
Targeted Attacks	^	^				>	^	^
Watering Hole	^							

Tabella 2 - Le principali minacce nelle aree ICT emergenti (Fonte: ENISA)

phishing, con le quali si possono avere sia i codici di autenticazione per l'home banking sia quelli per le carte di credito.

Confrontando le Tabelle 3 e 4 risulta evidente che la monetica ha un'incidenza, come somme sottratte, di ben più del doppio dell'home banking. Molto superiore il numero di denunce, di deferimenti all'Autorità Giudiziaria e di arresti.

Home Banking - Phishing	2013
Casi denunciati	13.717
Arrestati	9
Deferiti Autorità Giudiziaria	530
Somme sottratte (€)	12.993.919

Tabella 3 - Statistiche sui crimini di phishing e su home banking (Fonte: Polizia Postale e delle Comunicazioni)

Monetica	2013
Casi denunciati	65.327
Arrestati	85
Deferiti Autorità Giudiziaria	5.253
Somme sottratte (€)	38.717.714

Tabella 4 - Statistiche sui crimini sulla monetica (Fonte: Polizia Postale e delle Comunicazioni)

5.4 Individuazione, valutazione e gestione degli attacchi

Nella Sezione 3 del questionario sono state poste domande su come l'azienda/ente rilevi, valuti e gestisca gli attacchi.

La fig. 28 mostra la provenienza delle segnalazioni di un attacco (risposte multiple): le segnalazioni arrivano per circa 1/3 del campione dai sistemi di monitoraggio e controllo, ivi inclusi i sistemi di "intrusion prevention" e "detection" (IPS/IDS), e dall'analisi dei dati. A questi seguono con percentuali simili le segnalazioni da colleghi, l'analisi e/o verifica di dati dei sistemi attaccati, la constatazione diretta del danno subito (ad esempio il blocco di un sistema, una elaborazione scorretta, ecc.). Con percentuali inferiori al 10%, le segnalazioni provengono dagli utenti esterni, da clienti e fornitori che via Internet si accorgono di malfunzionamenti e/o di dati scorretti.

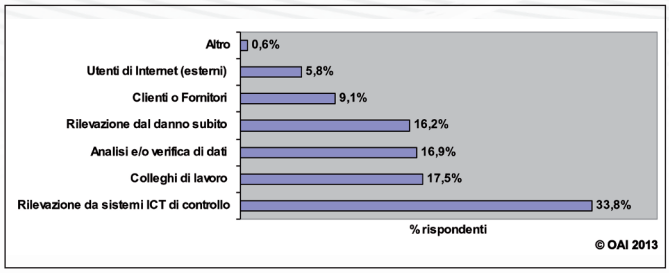

Fig. 28 - Da chi sono pervenute le segnalazioni (risposte multiple)

Come "altro" un rispondente ha indicato che la segnalazione è venuta dalla holding, che probabilmente ha individuato l'attacco tramite i propri sistemi di monitoraggio e controllo centralizzati.

Sulla valutazione dei danni subiti, economica e non, la fig. 29 mostra che quasi il 43% del campione che ha subito attacchi (contro il 72,3% della scorsa edizione) non effettua alcuna valutazione, ma il 41,3% la effettua (contro il 18,1% della scorsa edizione): e di questi una leggera maggioranza la effettua per ogni tipo di danno, mentre una parte di poco ridotta la effettua solo per danni significativi.

Pur con le più volte evidenziate cautele per il diverso mix del campione, il confronto tra le due ultime edizioni evidenzia la tendenza a stimare il danno subito.

La fig. 30 mostra i principali criteri seguiti per valutare la gravità dell'attacco e dei suoi impatti sull'azienda/ente.

Le risposte, multiple, indicano che per i 2/3 del campione il criterio più importante è la **continuità operativa**, cui seguono, per più della metà, i costi dovuti all'indisponibilità dei servizi ICT e al danno di immagine. I valori di tali criteri sono identici a quelli rilevati con il precedente rapporto. Seguono i costi diretti subiti con l'attacco ed i costi derivanti dalla non conformità alle leggi vigenti (compliance). Solo un non trascurabile 17,6%, prevalentemente di piccole organizzazioni, non ha criteri di valutazione.

Le attuali ripartizioni percentuali sono simili a quelle del precedente rapporto e confermano che i sistemi ICT costituiscono la tecnologia abilitante a tutti i processi, e quindi al business: se non funzionano, o funzionano male, non funziona la stessa azienda/ente.

L'attacco è veramente grave se mina la continuità operativa per quasi il 70% dei compilatori: una risposta così ampia indica come ci sia, da parte di quasi tutti i compilatori e in particolare dei CIO, una corretta logica di business nella gestione dei sistemi informativi e della loro sicurezza.

La conferma dell'importanza della continuità operativa è data da più della metà dei rispondenti che indicano i costi di indisponibilità dell'ICT come il secondo indicatore di gravità. Tra i criteri indicati nel questionario, è significativo che 1/3 circa preveda come ulteriore criterio di valutazione la "compliance" alle normative in vigore. La legislazione sulla privacy si fa sentire, ma è ora forse meno percepita dalle piccole imprese con le recenti normative di semplificazione e di abolizione del DPS, Documento Programmatico sulla Sicurezza.

Sulla gestione dell'attacco, 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. 31 (risposte multiple), quasi 1/3 dei rispondenti che hanno subito attacchi non comunica e circa 1/4 avvisa le competenti autorità (solitamente la Polizia Postale

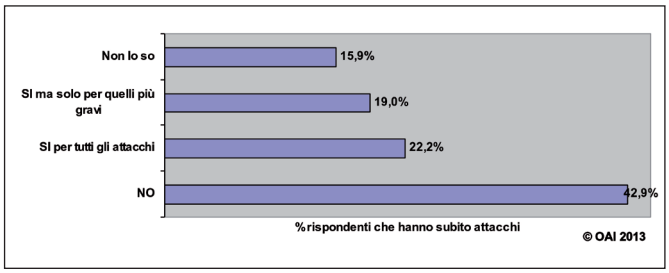

Fig. 29 - Valutazione del danno subito

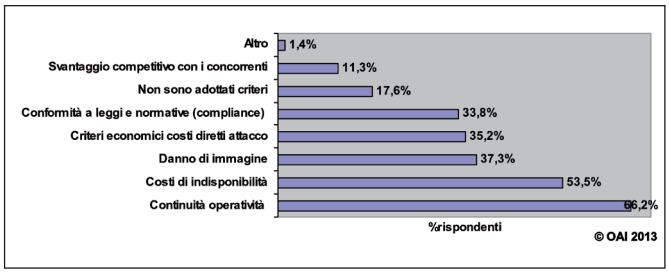

Fig. 30 - Criteri di valutazione della gravità dell'attacco (risposte multiple)

e delle Comunicazioni[20]); quasi 1/5 comunica ai propri Fornitori affinché intervengano, ed una analoga percentuale di rispondenti dichiara di "non sapere". Solo il 9% informa anche centri specializzati quali il CERT[21] ed una piccolissima percentuale informa l'assicurazione con la quale ha stipulato una polizza. Questa bassa % conferma che ben poche aziende/enti sono assicurate contro i rischi informatici, data anche la complessità ed il costo di tali polizze. L'alta percentuale dei "non so" dipende dal fatto che in molte organizzazioni la comunicazione è effettuata dalla struttura "pubbliche relazioni" e dagli uffici legali, e non dall'UOSI: molti rispondenti appartengo a quest'ultima e quindi possono non sapere chi si occupa delle relazioni esterne e dei problemi legali. La principale motivazione per la non comunicazione, come da fig. 32 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: l'UOSI 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 stabilite. La tutela dell'immagine, come motivazione, ha solo un 10%. La fig. 33 fornisce un'indicazione di quali azioni i rispondenti hanno intrapreso a seguito di un attacco. Le risposte possibili erano multiple, dato che sono multiple le azioni da intraprendere sia a livello tecnico che organizzativo ed eventualmente legale. Quasi 1/3 del campione 2013 attiva le ultime patch sul software, ed il 27% circa acquisisce ulteriori strumenti di prevenzione e protezione. 1/4 circa attiva delle indagini interne; il 17,6% elimina i sistemi attaccati o a rischio (spesso sono molto obsoleti, soprattutto come software di base), e con percentuali a decrescere sono aggiornate le policy e le procedure organizzative inerenti la sicurezza informatica, sono installati ed attivati nuovi strumenti di sicurezza, gli utenti finali (e gli operatori) devono seguire corsi di sensibilizzazione, formazione e addestramento, vengono rimpiazzati hardware e software vulnerabili, ed infine si richiede l'intervento di legali e/o di esperti esterni. Per quanto riguarda i tempi di ripristino a seguito di un attacco, la fig. 34 mostra, per i tempi medi, che nella maggior parte dei casi la situazione "ante" è ripresa in **meno di un giorno**, e complessivamente in circa l'80% dei casi la situazione è ripristinata **entro 3 giorni dall'attacco**. A parte un probabile ottimismo dei compilatori, questi tempi indicano da un lato che gli strumenti di prevenzione e protezione sono ora più diffusi e

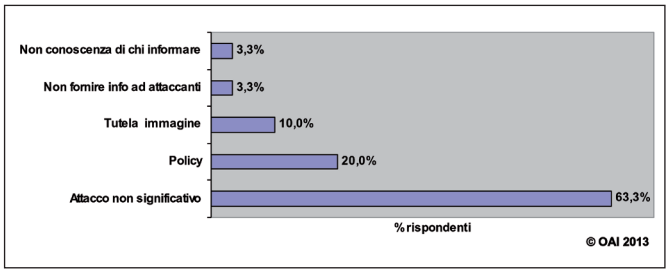

Fig. 32 - Motivazioni per la "non comunicazione" all'esterno dell'attacco (risposte multiple)

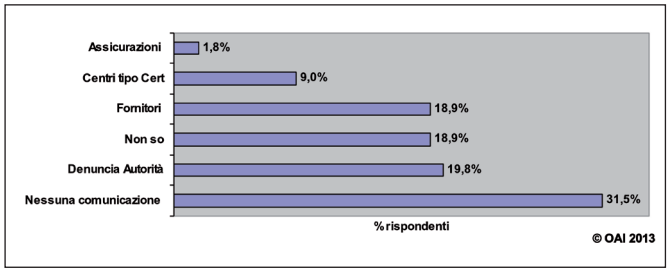

Fig. 31 - Comunicazione all'esterno dell'avvenuto attacco (risposte multiple)

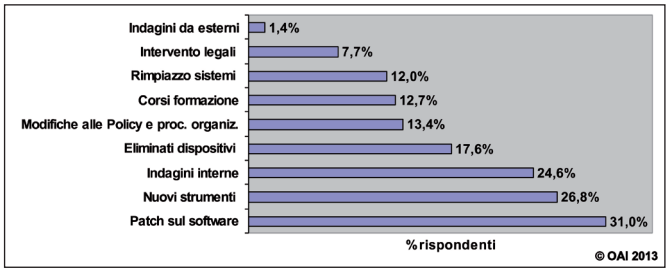

Fig. 33 - Azioni dopo un attacco (risposte multiple)

[20] Si veda http://www.poliziadistato.it/articolo/23393/

[21] I CERT, Computer Emergency Response Team, sono organizzazioni che a livello nazionale raccolgono le segnalazioni di incidenti informatici e delle vulnerabilità che provengono dalla comunità degli utenti. A livello internazionale si veda http://www.cert.org/, a livello nazionale http://www.galileo.it/crypto/cert-it.htm

più efficaci (si veda anche § 6), dall'altro che la stragrande maggioranza degli attacchi, almeno per il campione, non ha serie conseguenze, come già evidenziato dalla fig. 27. Gli attacchi veramente penetranti ed impattanti, pur se pochi, hanno serie conseguenze ed il ripristino richiede una settimana o più, e comunque, da quanto rilevato, non più di un mese. L'ordine di grandezza dei tempi "medi" è confermata anche dai tempi "massimi" occorsi nei casi peggiori di ripristino, illustrati nella fig. 35. I pochi attacchi specificati che hanno richiesto più di una settimana per il ripristino riguardano infezioni da virus e attacchi DoS/DDoS.

6. Strumenti e politiche di sicurezza ICT adottate

Il presente capitolo sugli strumenti di prevenzione e protezione considera sia gli aspetti tecnici che quelli organizzativi, e suddivide gli strumenti per sicurezza fisica, logica, organizzativa e di gestione.

6.1 Sicurezza fisica

La fig. 36 schematizza le principali misure in uso a protezione dei Data Center e delle "computer room": queste ultime sono i locali nei quali vengono concentrate le risorse informatiche di un ufficio periferico o di una piccola struttura. Quasi il 3/4 dei rispondenti è dotato di sistemi per garantire la continuità elettrica, da UPS ad autonomi gruppi di continuità. Il 70% dispone di sistemi di climatizzazione e quasi il 65% 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, circa il 60%, ha nei locali del Data Center e/o delle computer room rilevatori di fumo, gas, umidità e poco più della metà effettua controlli degli accessi delle persone fisiche tramite guardiania, bussole, lettori di badge ed altri strumenti, fino al riconoscimento biometrico. Una quota ben più piccola, ma non trascurabile (quasi il 15%) non ha di fatto alcuna seria misura di protezione fisica per i locali ove sono contenuti i sistemi ICT, a parte le serrature sulle porte di accesso. Nella voce "Altro" alcuni rispondenti hanno riportato la separazione "fisica" in locali diversi, anche geograficamente, dei sistemi ridondati con dati critici.

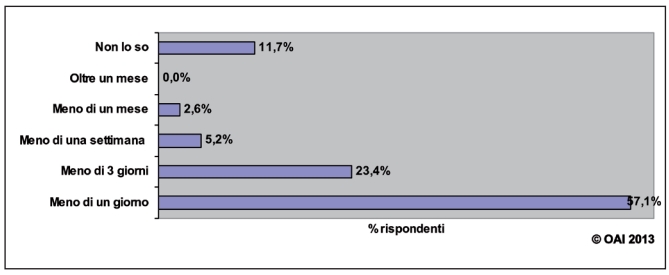

Fig. 34 - Tempi medi di ripristino

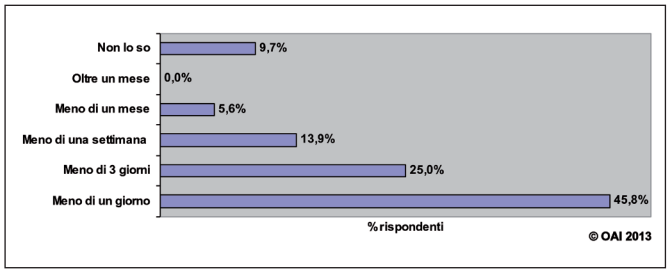

Fig. 35 - Tempi massimi di ripristino (caso peggiore)

6.2 Sicurezza logica

Gli strumenti per la sicurezza logica si differenziano in funzione delle unità ICT da proteggere, e, come dal questionario, sono articolati in:

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

A livello di reti, come indicato nella fig. 37 con risposte

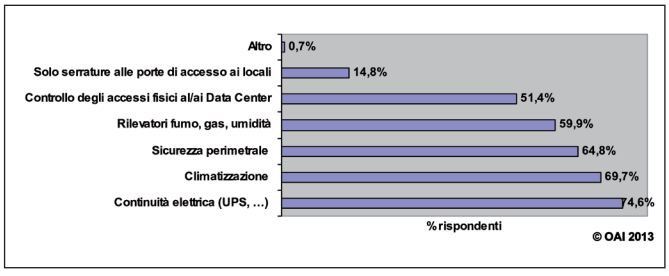

Fig. 36 - Strumenti sicurezza "fisica" in uso (risposte multiple)

multiple, i 3/4 dei rispondenti è dotato di dispositivi firewall e di DMZ, DeMilitarized Zone, e quasi il 65% dichiara di utilizzare soluzioni VPN, Virtual Private Network per proteggere le comunicazioni da remoto. Circa la 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 27,5%, rispetto al 47% circa della passata indagine, ha potenziato il livello di sicurezza delle reti wireless, che possono presentare serie vulnerabilità se non correttamente protette. La forte riduzione percentuale rispetto allo scorso anno è da attribuirsi all'incremento e al diverso mix di rispondenti. Una piccola percentuale, l'8,5%, non è al momento dotata di alcuna specifica protezione per le reti: è il caso per piccoli e piccolissimi sistemi informativi.
Nella voce "Altro" alcuni rispondenti hanno riportato soluzioni per la mitigazione di attacchi DDoS/DoS e l'uso di reti/collegamenti ad alta affidabilità forniti dai provider.
La fig. 38 fornisce un 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 dell'edizione passata, ma con qualche punto percentuale in meno; con l'allargarsi della base di rispondenti si appiattisce la valenza tecnica-organizzativa complessiva, causa anche la maggioranza di organizzazioni di piccole dimensioni (il 33,8% con meno di 50 dipendenti, si veda fig. 3).
I software antivirus e antispyware sono usati dalla maggior parte dei rispondenti, 70,4%, rispetto al l'80,2%, 97% e 95% delle scorse edizioni dell'OAI: significa che più di 1/4 dei rispondenti non usa (o non sa che vengono usati) programmi anti-malware sui server. La riduzione percentuale che emerge dipende non solo dall'ampliamento del numero di rispondenti, già evidenziata, ma dal voluto non uso di questi strumenti, il più delle volte in ambito Linux. Taluni ritengono che i sistemi anti malware sui server penalizzino le prestazioni dei sistemi più che proteggerli, e che comunque richiedano interventi specifici da parte di specialisti in caso di individuazione di codici maligni.
Il 52,8% utilizza strumenti di filtraggio dei contenuti e delle URL, tipiche attività dei moderni firewall; protezione passata in percentuale al terzo posto rispetto al sesto della scorsa edizione, chiaro indice che il mondo dei web è ormai al centro della sicurezza informatica insieme al "mobile". Il 50,7% dichiara di usare sistemi ad alta affidabilità, una percentuale di poco superiore alla ben più tradizionale ed operativa gestione delle patch e degli aggiornamenti, che risulta al 49,3% del campione. Questo dato è significativo: poco più della 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 preoccupante 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!
La gestione dei log copre anch'essa circa la metà dei rispondenti, e tale diffusione deriva anche dall'obbligo di essere conformi alla normativa sugli amministratori di sistema per la privacy. Un terzo del campione utilizza

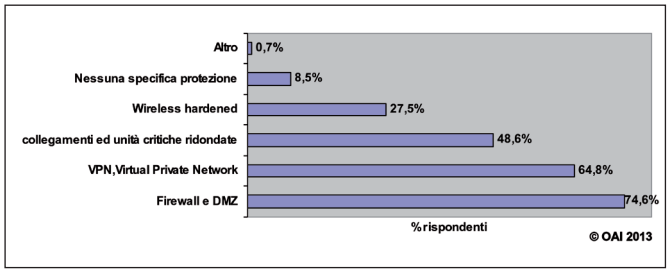

Fig. 37 - Strumenti sicurezza logica in uso per le reti (risposte multiple)

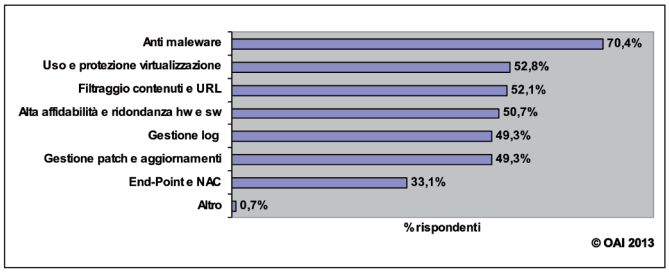

Fig. 38 - Strumenti sicurezza logica in uso per i sistemi (risposte multiple)

strumenti (tipicamente software) di sicurezza End-Point ed i NAC, Network Access Control. Tale percentuale, significativa anche se inferiore a quella rilevata nella precedente edizione, conferma l'attenzione a controllare "prima dell'accesso" l'identità dell'utente e quanto sia sicuro il posto di lavoro (PdL) da cui chiede l'accesso, tenendo anche conto dei PdL mobili: si pensi alla necessità di nuovi e maggiori controlli con il BYOD. La fig. 39 mostra la situazione del campione, con risposte multiple, per gli strumenti di identificazione, autenticazione e controllo degli accessi logici ai sistemi ed alle applicazioni. Il mezzo più diffuso è la consueta coppia identificatore utente - password, associata a strumenti di controllo degli accessi e di profilazione dei diritti dell'utente sugli applicativi e sui dati trattati: 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 anche alla spinta della PEC, Posta Elettronica Certificata, oltre all'uso delle CRS, Carta Regionale dei Servizi, i certificati digitali raggiungono il 3° posto, con il 30,3% del campione. Le piattaforme KPI, Public Key Infrastructure, necessarie per erogare servizi basati sui certificati digitali, sono diffuse solo in 1/5 del campione; una conferma della bassa accettazione delle KPI, dovuta soprattutto alla loro complessità. Le tecniche di SSO, Single Sign One, crescono con una copertura di quasi il 30% rispetto al 21% della scorsa edizione.
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, pur con una percentuale sul campione di solo il 6,3%, incomincia a diffondersi (era al 6,2 e al 2,52% nella scorse edizioni), sia grazie alla sua maggior affidabilità, sia ai costi calanti, sia soprattutto per l'uso della firma grafometrica che permette la digitalizzazione e la gestione totalmente informatica dei documenti firmati.
La fig. 40 dettaglia l'uso di strumenti per la protezione degli applicativi, al di là della profilatura dei diritti d'accesso vista prima. Gli strumenti più diffusi (risposte multiple), 66,2%, sono i firewall ed i reverse proxy posti a difesa dei server applicativi e dei data base, che ulteriormente controllano i diritti di accesso e filtrano i contenuti. Tutti gli altri strumenti hanno percentuali molto inferiori, e per quasi il 30% non sono al momento presenti strumenti: di questi, il 13,4% dichiara che sono in corso progetti o analisi di fattibilità.
Il 39,4% ha prodotto e fatto conoscere, soprattutto ai propri fornitori, policy e linee guida sulle caratteristiche tecniche che deve avere un programma sicuro, ed il 26,1% afferma di far seguire tali raccomandazioni agli sviluppatori ed ai fornitori. Il 21,8% utilizza specifici strumenti per il controllo della sicurezza intrinseca degli applicativi, quali l'ispezione del codice, i test di penetrazione ecc. per verificare la mancanza di vulnerabilità prima della loro messa in produzione.

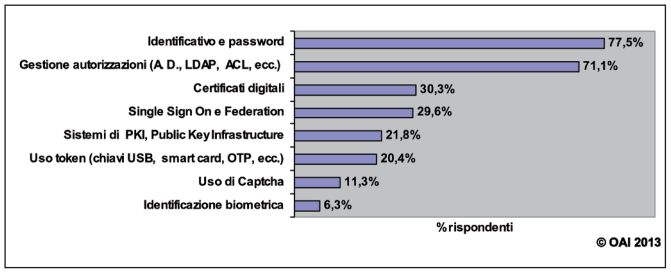

Fig. 39 - Strumenti in uso per l'identificazione, l'autenticazione e l'autorizzazione (risposte multiple)

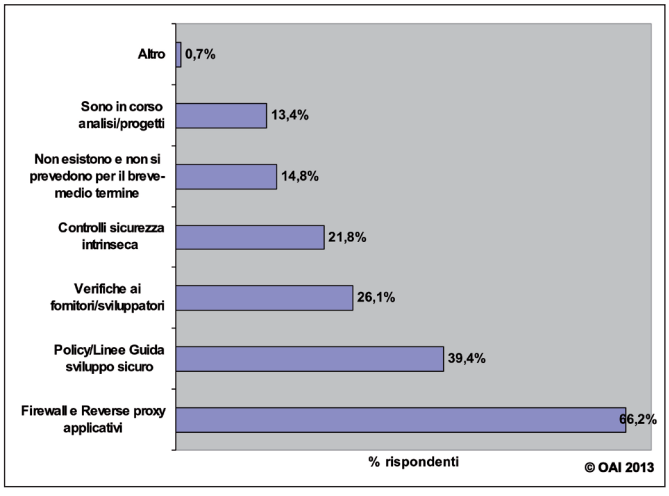

Fig. 40 - Strumenti in uso per la sicurezza logica degli applicativi (risposte multiple)

Questi dati evidenziano come i 2/3 dei rispondenti abbiano preso coscienza delle possibili gravi vulnerabilità degli applicativi ed effettuino opportuni controlli.
Per la protezione dei dati, che costituiscono il reale e più importante "asset ICT" dell'azienda/ente, la fig. 41 mostra che una buona maggioranza, il 62,7%, utilizza l'archiviazione remota, tipicamente con ISP/ASP (Internet/Application Service Provider) e fornitori cloud; la tendenza è di replicare in remoto tutti i dati, o quelli più critici, anche grazie ai prezzi interessanti dell'IaaS, Infrastructure as a Service. Nella scorsa edizione tale strumento era al secondo posto, e si è scambiato ora con l'uso della crittografia nella trasmissione dei dati in rete, 58,5%, tipicamente nelle transazioni via web con HTTPS o con FTPS. Questo è un indice della diffusione di questi protocolli sicuri disponibili in tutti i browser e attivati sui web server non solo per transazioni commerciali e bancarie via Internet.
Più di 1/4 critta i dati archiviati, anche grazie ai servizi in cloud, ed il 22,5% utilizza tecniche e strumenti di DLP, Data Loss Prevention. Una percentuale non trascurabile di quasi il 10% non usa alcuna specifica tecnica per la protezione dei dati.

6.3 La gestione della sicurezza ICT

La fig. 42 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 sistema informativo.
Il monitoraggio e il controllo centralizzato delle funzionalità e delle prestazioni dei sistemi ICT sono in vari modi attuati dal 64,1% dei rispondenti, maggiormente diffusi anche grazie alla terziarizzazione e alle soluzioni cloud. Tale percentuale è diminuita rispetto alle edizioni precedenti (80 e 79,8%): la causa è da attribuirsi all'aumento ed al mix diverso dei rispondenti. A fronte di questa percentuale, ben il 39,4% non ha o non utilizza sistemi centralizzati di monitoraggio e controllo, ma opera in maniera "reattiva" su ogni singolo sistema quando si accorge di o gli viene segnalato un malfunzionamento. E' una gestione della sicurezza a isole e/o a silos verticali e separati per i diversi ambienti (ad esempio Microsoft e Linux/Unix) e per le diverse applicazioni.
Soprattutto nei sistemi informativi di piccole e medie dimensioni, la gestione è effettuata server per server a livello di singola consolle di sistema operativo.
Relativamente alta la diffusione di sistemi di prevenzione delle intrusioni, gli IPS, Intrusion Prevention System, che supera di qualche punto la diffusione dei sistemi per l' individuazione delle intrusioni, gli IDS, Intrusion Detection System. Il 28,2% di rispondenti effettua prove di attacco per saggiare la tenuta degli strumenti di sicurezza, e più di 1/4 dei rispondenti potenzia la sicurezza (hardening) con sistematiche analisi delle vulnerabilità (vulnerability assessment) e scansioni delle reti e dei sistemi. Tutti questi dati sono chiari e positivi indicatori che sta aumentando la consapevolezza che nella sicurezza informatica occorre passare da una logica "reattiva" ad una "proattiva".
La gestione dei log ha un peso non trascurabile, in particolare per operatori e amministratori di sistema, anche grazie alle normative per la privacy.

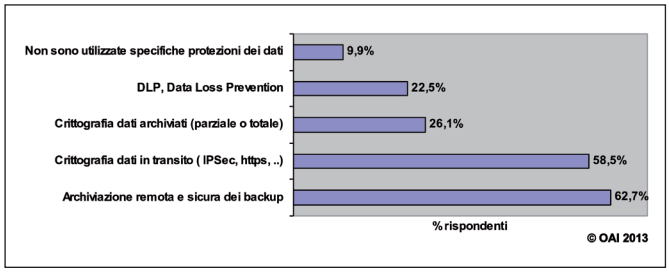

Fig. 41 - Strumenti in uso per la sicurezza logica delle informazioni (risposte multiple)

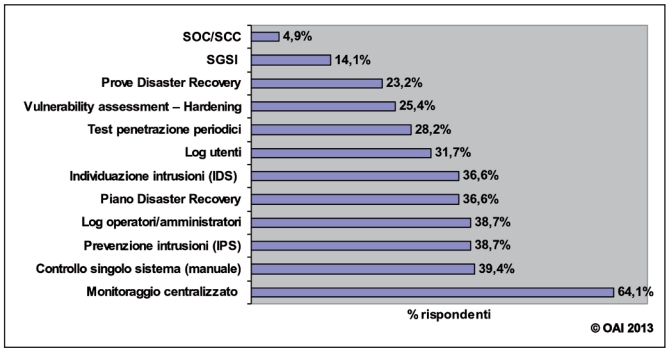

Fig. 42 - Strumenti in uso per la gestione della sicurezza ICT (risposte multiple)

I piani di Disaster Recovery, ora facilitati dall'utilizzo del cloud, sono effettuati dal 36,6% del campione, ma solo il 23,2% effettua periodicamente prove di ripristino emulando situazioni di disastro. Questo dato conferma quelli rilevati nelle edizioni precedenti, ed evidenzia come in Italia la seria prevenzione sia più formale e burocratica che effettiva, anche nelle medie-grandi organizzazioni.
Percentuali decisamente inferiori per chi utilizza sistemi integrati e centralizzati per gestione della sicurezza ICT (chiamati SGSI, Sistema Gestione Sicurezza Informatica), e per chi fa uso di un SOC, Security Operation Center, o di un SCC, Security Command Center, sovente terziarizzati a società specializzate.
Un aspetto fondamentale nella gestione della sicurezza ICT è la sistematica e periodica analisi dei rischi. Come evidenziato nella fig. 43, solo il 27,1% (contro il 23,9% dello scorso anno) afferma che tale analisi viene effettuata, ed il 6% non lo sa. Il 9,8% del campione intende effettuare l'analisi dei rischi nel prossimo futuro.
La fig. 44 mostra che solo il 22,6% dei rispondenti ha già in essere forme assicurative sul rischio informatico, e che il 7,5% prevede di dotarsene nel prossimo futuro.

6.4 Le misure organizzative

Gli aspetti organizzativi sono determinanti per gestire correttamente ed efficacemente la sicurezza di un sistema informativo: 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, un'elite 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. 45 mostra un primo quadro generale, sostanzialmente positivo, su come sono gestiti i temi organizzativi della gestione della sicurezza dei sistemi informativi: erano possibili risposte multiple.
Il quadro generale è abbastanza positivo: il 60,2% ha definito ed utilizza **policy** e **procedure organizzative** in merito alla sicurezza informatica. In particolare, quasi un terzo del campione utilizza strumenti informatici per il supporto e l'automazione, parziale o totale, dei processi per la sicurezza ICT, tipicamente **work-flow**, banche dati di supporto all'**help-desk**, al **trouble ticketing**, ecc.; con percentuali molto simili vengono utilizzate specifiche procedure per la gestione degli incidenti, dei problemi e dell'help desk. Il 27,8% ha inoltre 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

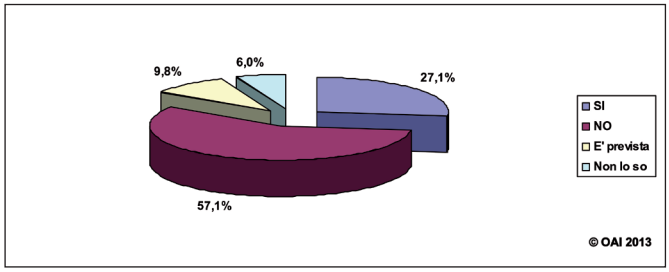

Fig. 43 - Effettuazione analisi dei rischi

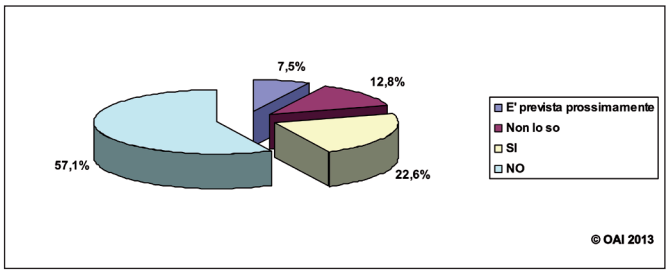

Fig. 44 - Assicurazione rischio residuo

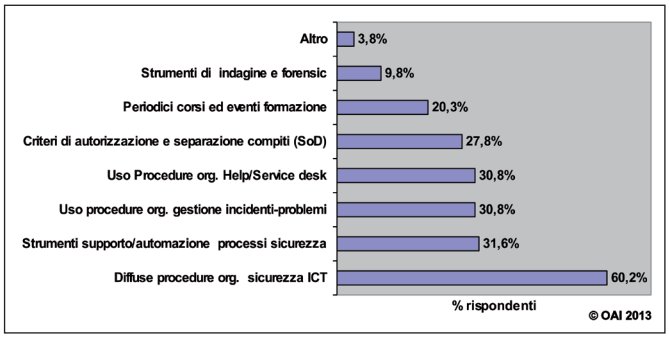

Fig. 45 - Principali contromisure organizzative (risposte multiple)

Duties. Circa 1/5 attua periodici corsi ed eventi per la sensibilizzazione, formazione e addestramento di utenti e di specialisti. Poco meno del 10% ha ed utilizza strumenti di indagine e di "analisi forensic", mentre con la risposta "Altro" una piccola percentuale, relativa a piccole strutture, dichiara di non avere in funzione alcuna procedura organizzativa, con i relativi supporti informatici.

Per le aziende/enti che hanno già adottato e in essere "policy" per la sicurezza informatica, la fig. 46 mostra, con risposte multiple, quali sono i principali mezzi per la sua comunicazione e diffusione: la prevalenza è via Intranet seguita a breve distanza dalla posta elettronica, cui seguono a decrescere percentualmente l'uso di seminari e corsi e, da ultimo, la comunicazione interna a mezzo stampati.

6.4.1 Conformità a standard e a "buone pratiche" (best practice)

Un forte ausilio nell'organizzazione della sicurezza ICT può venire da un' intelligente e contestuale adozione di standard e di "buone pratiche", in inglese "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[22] per la gestione operativa dell'ICT, l'ISO 9001 per la gestione della qualità dei servizi, ecc.[23]

Tali standard e best practice possono essere adottati formalmente, ossia certificandosi, o informalmente all'interno delle proprie strutture, e possono anche essere richiesti ai fornitori e ai provider perché li seguano nell'erogare i servizi loro richiesti.

La fig. 47 fa riferimento all'adozione della famiglia di standard ISO 27000 nell'ambito dell'azienda/ente, normalmente da parte della UOSI. Per non appesantire il questionario, volutamente 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 un SGSI deve svolgere. 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 quasi la metà dei rispondenti, il 42,9%, non è interessata o non ritiene necessario seguire tali standard nel proprio contesto. Il 21,4 segue tali standard come riferimento tecnico-organizzativo, ma non è e non intende certificarsi; in tale ottica il 15,4% intende seguirli nel prossimo futuro. Solo il 6,6% è già certificato, prevalentemente provider e società di servizi di grandi dimensioni, oltre a banche ed istituti finanziari. Come mostrato dalla fig. 48, poco meno del 10% del campione richiede ai propri fornitori, anche a livello contrattuale, la certificazione, mentre il 13,2% richiede loro di seguire in pratica tali standard pur senza essere certificati.

La certificazione per la best practice ITIL, ora alla versione

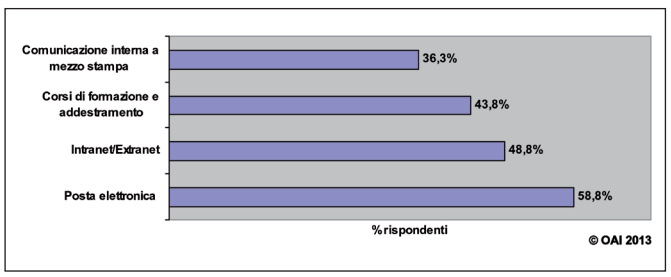

Fig. 46 - Comunicazione e diffusione delle policy (risposte multiple)

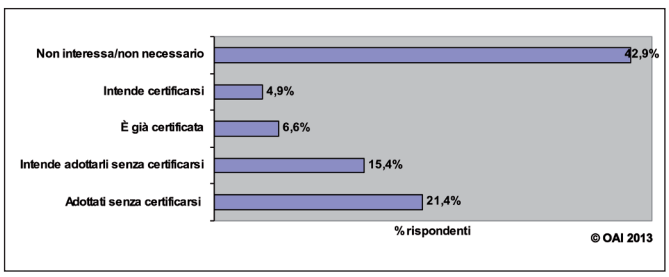

Fig. 47 - Adozione standard famiglia ISO 27000

[22] ISO 20000 standardizza logiche e processi di ITIL cui aggiunge logiche e componenti da Microsoft Operations Framework e da COBIT.

[23] 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.

3 ed. 2011, è a livello individuale mentre quella per lo standard ISO 20000 è a livello di azienda/ente. La fig. 49 evidenzia che la maggioranza dei rispondenti non è interessata o non ritiene necessaria questa certificazione. ITIL è invece più conosciuto e diffuso in Italia, anche grazie all'attività divulgativa dell'associazione itSMF: il 18,1% già lo ha adottato ed il 15,9% intende adottarlo a breve. Questo significa seguire l'impostazione dei servizi ICT e dei relativi processi dettagliati in ITIL, probabilmente con qualche persona che si certifica. ISO 20000 riscuote un interesse molto minore, e l'interesse per una prossima certificazione sarà sicuramente dettata da obblighi derivanti da qualche normativa o contratto.

La fig. 50 evidenzia le richieste del campione nei riguardi dei propri fornitori: l'8,2% già richiede che questi seguano funzionalmente e nella sostanza ITIL, quasi il doppio lo richiederà nel prossimo futuro. Solo il 3,8% richiede che il personale dei fornitori sia certificato ITIL. Una piccola percentuale richiede la certificazione ISO 20000, per i motivi sopra indicati. La fig. 51 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 practice, per la quale è stata recentemente rilasciata la versione 5. Solo il 7,7% lo ha già adottato, ed il 13,7% intende adottarlo nel prossimo futuro[24].

Ancora più basse le percentuali rilevate per la richiesta ai fornitori di seguire COBIT o di avere figure certificate, come mostrato nella fig. 52.

Nel complesso l'indagine 2013 evidenza come gli standard e le best practice per la governance strategica e/o operativa della sicurezza informatica, pur consolidate ed aggiornate da anni, stentino ancora ad essere adottate anche dalle grandi strutture. Una delle cause, che si evince in maniera evidente dalle risposte avute, è che tali normative sono poco conosciute e non ancora sistematicamente richieste nei capitolati e nelle gare di appalto.

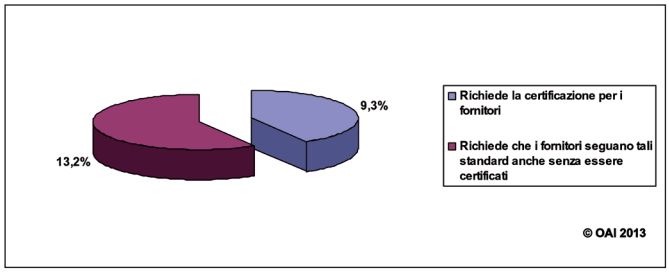

Fig. 48 - Richiesta ai fornitori conformità famiglia ISO 27000

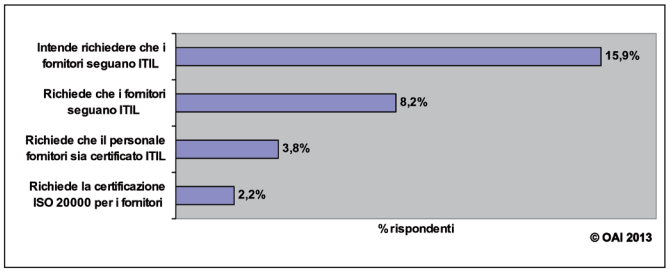

Fig. 50 - Richiesta ai fornitori conformità ITIL ed ISO 20000 (risposte multiple)

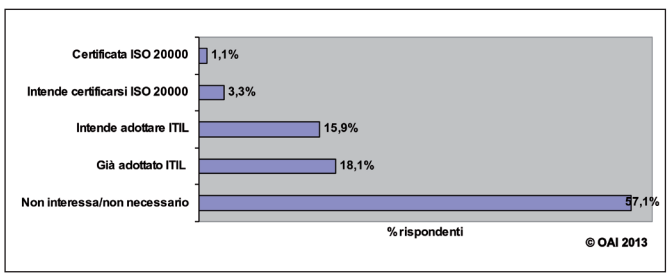

Fig. 49 - Adozione ITIL ed ISO 20000 (risposte multiple)

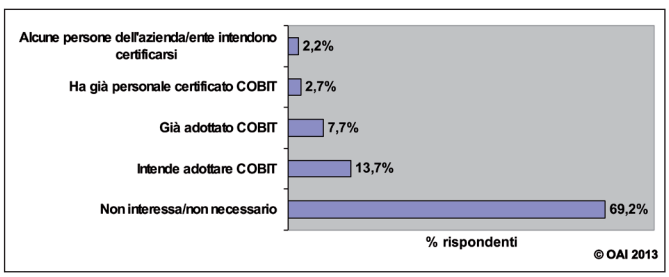

Fig. 51 - Adozione COBIT (risposte multiple)

[23] Le basse percentuali rilevate potrebbero derivare dal fatto che COBIT deve essere adottato dal senior management o essere imposto agli outsourcer: pochi compilatori del questionario risultano appartenere a queste categorie, e più in generale pochi compilatori forse conoscono bene e sono aggiornati sul tema.

Alcune aziende/enti devono inoltre essere certificate e seguire specifiche normative settoriali che hanno impatti sulla sicurezza e sulla gestione del sistema informatico. Tipici esempi la normativa statunitense Sox[24] 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, e così via.

In termini molto generali, e senza far riferimento a specifiche norme, la fig. 53 mostra che il 27,4% dei rispondenti (rispetto al 17% ed al 20% delle scorse edizioni) deve far fronte a questi ulteriori obblighi, facendo parte dei settori sopra indicati, ed il 4,6% lo sarà nel prossimo futuro. Quindi circa 1/3 del campione è o sarà a breve soggetto a specifiche norme di settore, che hanno tutte impatti sui sistemi informativi.

Un importante tema a cavallo tra le certificazioni e l'organizzazione interna per la sicurezza ICT è la richiesta per il personale interno o esterno che si occupa di sicurezza informatica di avere specifiche qualifiche/certificazioni professionali per la sicurezza ICT quali EUCIP, LoCSI, CISSP, SSCP, CISA, CISP, OPSA, ecc. Due recenti decreti italiani, il D. Lgs. n. 4/2013 sulle "professioni non regolamentate" ed il D. Lgs. n. 13/2013 sulla "certificazione delle competenze" stanno definendo le certificazioni personali, che nel prossimo futuro diverranno di fatto obbligatorie per chi opera nel settore ICT.

In termini generali, e senza far riferimento a specifiche certificazioni nazionali ed internazionali, la fig. 54 mostra che per la stragrande maggioranza dei rispondenti, il 63,6%, queste certificazioni e/o qualificazioni non sono richieste all'interno dell'azienda/ente, e che solo il 14,3% intende richiederle nel prossimo futuro. Percentuali simili per la richiesta di certificazioni-qualificazioni per il personale dei fornitori, come mostrato dalla fig. 55.

6.4.2 Audit

Nell'ambito della gestione della sicurezza un ruolo importante è giocato dall'audit. La fig. 56 mostra che il 35,3% dei rispondenti (percentuali maggiori, il 43,6% ed il 51% nelle precedenti edizioni, ma dovuto al più basso numero di rispondenti) svolge tale funzione e che il 21,8 % ha intenzione o ha a piano di espletarla. In prospettiva l'audit sarà quindi svolto nelle aziende/enti di ben più della metà del campione.

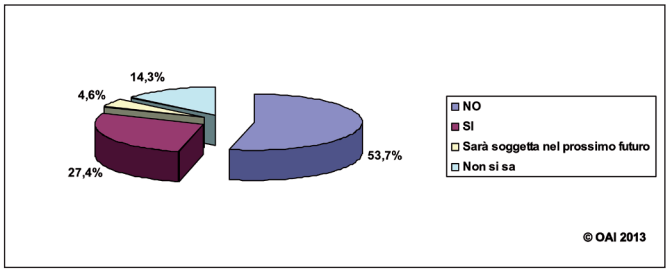

Fig. 53 - Conformità ad altri standard o normative di settore

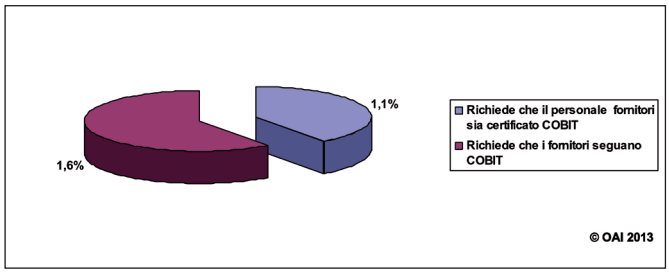

Fig. 52 - Richiesta ai fornitori conformità COBIT

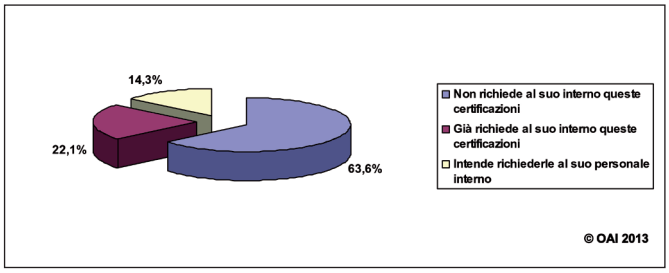

Fig. 54 - Richiesta al personale interno di specifiche certificazioni/qualificazioni sulla sicurezza informatica

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

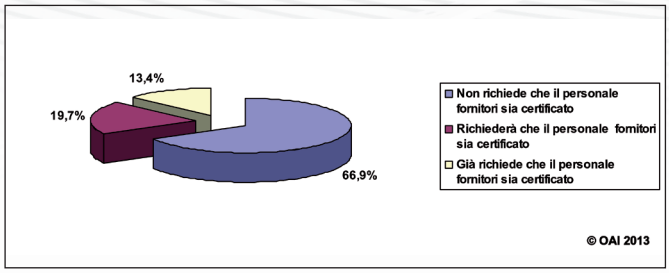

Fig. 55 - Richiesta al personale fornitori di specifiche certificazioni/qualificazioni sulla sicurezza informatica

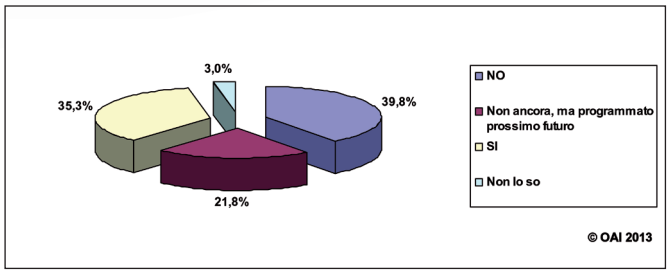

Fig. 56 - Attività di audit

La fig. 57 mostra il dettaglio di come venga espletato l'audit da parte delle aziende/enti che già lo effettuano: la maggioranza, 75,6%, contro il 61,8% della scorsa edizione, lo svolge con periodicità regolare, ad esempio annuale. L'11,1% lo svolge in maniera continuativa, nell'ambito di un processo ben strutturato e di miglioramento continuo dell'ICT. Il 6,7% la svolge in maniera "irregolare", ossia non pianificata periodicamente, ma quando ritenuto necessario, e con la stessa percentuale viene effettuato solo a seguito di incidenti o di attacchi gravi.

6.4.3 La struttura organizzativa interna per la sicurezza ICT

La struttura organizzativa interna all'azienda/ente per la gestione della sicurezza gioca un ruolo importante e 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. 58, il 38,3% ha definito un ruolo di "responsabile della sicurezza informatica", in inglese CISO, Chief Information Security Officer; il 6,1% non lo ha ancora definito ma è in procinto di farlo.

Ben più della metà non ha per ora alcun responsabile esplicitamente definito ed in carica: in tali casi, come evidenziato nella fig. 59, le funzioni del CISO sono svolte per lo più dal responsabile dei sistemi informativi, il CIO, e per il 37,1% sono terziarizzate a professionisti o società specializzate.

Per chi invece ha definito il ruolo del CISO, esso è allocato come illustrato nella fig. 60. Nei 2/3 dei casi tale ruolo è collocato funzionalmente nell'ambito ICT, quindi all'interno dell'UOSI. Nel 29,2% questo responsabile non è all'interno dell'UOSI ma in altre strutture interne all'azienda/ente (tipicamente sotto il CSO, Chief Security Officer, o in altre strutture di staff alla direzione generale). Una piccola parte, il 4,6%, delega questo ruolo a terze parti specializzate.

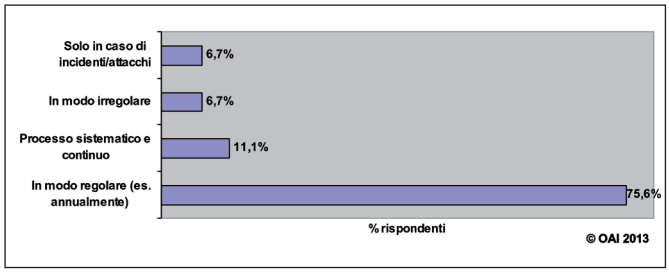

Fig. 57 - Modalità audit

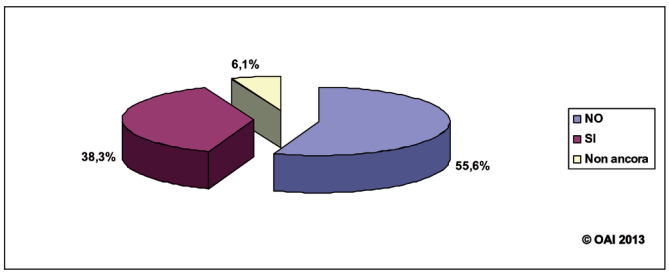

Fig. 58 - Esistenza ruolo responsabile sicurezza informatica (CISO)

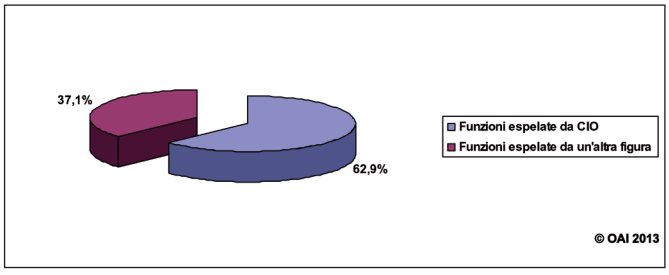

Fig. 59 - Se non è definito il CISO, chi svolge tali funzioni

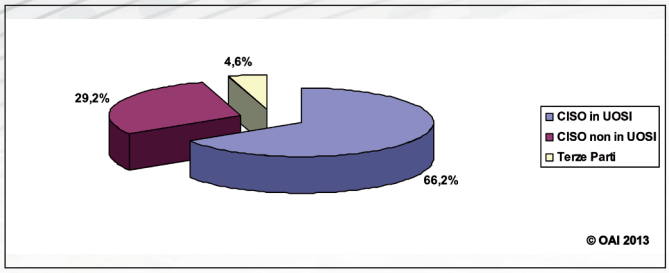

Fig. 60 - Posizionamento organizzativo CISO

7. Gli attacchi più temuti nel futuro

La fig. 61, con risposte multiple, mostra quali sono gli attacchi ritenuti più probabili e più temuti nel prossimo futuro, tendenzialmente nel 2014 ed oltre, indipendentemente da quelli eventualmente subiti, e facendo sempre riferimento alla medesima tassonomia di attacchi considerata della Tabella 1. Anche per queste domande, come per quelle relative al termine "impatto poco o molto significativo" di cui al Capitolo 5 ed alla fig. 27, non si sono specificati, per rendere più breve e semplice il questionario, i criteri per considerare un attacco più "temuto": ad esempio impatto funzionale-operativo, sul business, economico, legale, ecc.

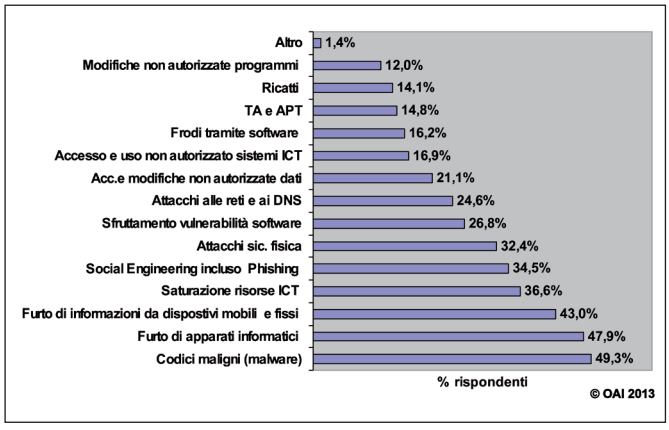

Fig. 61 - Attacchi maggiormente temuti nel futuro (risposte multiple)

È interessante evidenziare come i primi tre attacchi più temuti sono nell'ordine il malware, il furto "fisico" di apparati ICT, il furto di informazioni dai dispositivi d'utente sia mobili che fissi. Contrariamente all'edizione scorsa, il social engineering non è più sul podio ma si classifica al 5° posto. La nuova famiglia di attacchi introdotta, i TA, Targeted Attacks, e gli APT, Advanced Persistent Threats, si posiziona al 12° posto, ragionevolmente temuta solo da grandi organizzazioni potenziali target. Nella voce "Altro" sono stati specificati attacchi a sistemi di controllo industriale quali DCS, Distributed Control System, e SCADA, Supervisory Control And Data Acquisition, che molti considerano attacchi TA-APT.

La fig. 62 pone a confronto le previsioni di attacchi più temuti emerse nelle varie edizioni OAI, confronto al solito puramente indicativo data la diversità dei campioni che hanno risposto ai questionari nelle diverse edizioni.

Il grafico mostra come siano profondamente cambiate le stime di attacco più probabile e più temibile rapporto per rapporto: pur con campioni diversi e con probabili valutazioni diverse della semantica di "più temibile", le diversità nel tempo sono drasticamente cambiate tipo di attacco per tipo di attacco. Innumerevoli le considerazioni che possono scaturire da questo mutare della percezione dei potenziali rischi futuri. Sono rimasti sempre "caldi" i codici maligni, il social engineering, il furto di informazioni da dispositivi fissi e mobili, i furti "fisici" di dispositivi ICT. Sono andati in crescendo gli attacchi fisici e la saturazione delle risorse ICT. Tutti gli altri hanno avuto una stima in decrescita. La fig. 63 confronta gli attacchi futuri previsti e temuti del Rapporto 2011 con quelli effettivamente subiti nell'anno 2012 rilevati nella presente indagine. Anche questo confronto è da considerarsi puramente indica-

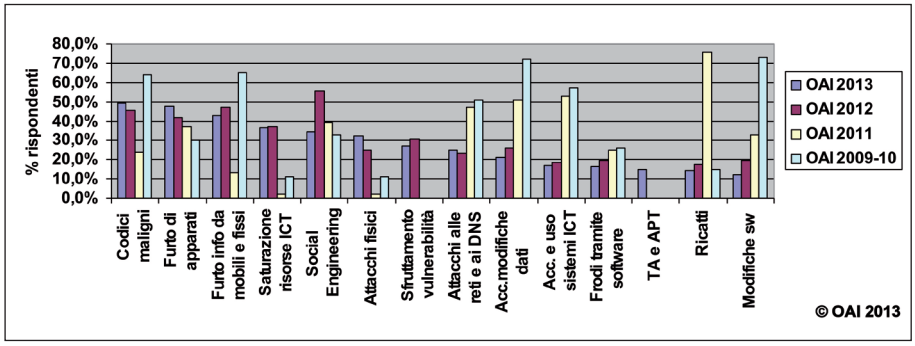

Fig. 62 - Confronto tra gli attacchi "temuti nel futuro" nei vari Rapporti OAI

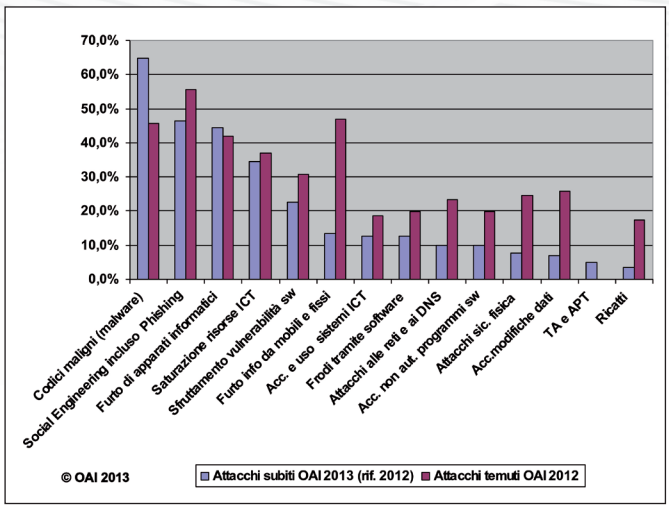

Fig. 63 - Confronto tra attacchi "temuti" e quelli "subiti" nel 2012 dal confronto tra Rapporto OAI 2012 e 2013

tivo, dati i due diversi bacini di rispondenti. Emerge che gli unici casi in cui stima ed effetto più o meno coincidono riguardano il furto di dispositivi e la saturazione di risorse, DoS/DDoS. Al contrario i casi più sbagliati, come molto temuto ma avvenuto in un (relativamente) limitato numero di casi, riguardano i ricatti, gli accessi e le notifiche non autorizzate ai dati, il furto di informazioni da apparati fissi e mobili, gli attacchi alla sicurezza fisica. I casi sbagliati come meno temuti rispetto alla loro effettiva occorrenza riguardano solamente i codici maligni. Considerando gli attacchi più temuti nel prossimo futuro della fig. 61, la fig. 64, con risposte multiple, evidenzia quali sono le possibili motivazioni degli attaccanti nelle ipotesi dei rispondenti. Rispetto alle edizioni precedenti di OAI, nel questionario della attuale edizione si è aggiunto il termine di "hacktivism". Praticamente intraducibile in italiano, esso deriva dall'unione di "hacker" e di "activism" e fa riferimento ad attacchi in rete e sui sistemi informativi per porre alla ribalta mediatica un determinato tema, ad esempio politico, religioso, ambientale, ecc. Di fatto può essere considerato come un'azione dimostrativa, ma al, contrario di quest'ultima, un attacco portato da hacktivism genera danni, mentre un'azione dimostrativa non li produce almeno volontariamente. Al primo posto delle motivazioni 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 vandalismo, causa probabile di parte degli attacchi "fisici" e dei furti. Al terzo il sabotaggio ed al quarto, per circa 1/4 del campione, l' hacktivism. Percentualmente di poco inferiori l'azione dimostrativa, che include anche gli attacchi del così detto "ethical hacking", e lo spionaggio, sia per segreti industriali che politici. Il ricatto informatico, che potrebbe colpire a livello massivo anche i piccoli e piccolissimi sistemi informatici di negozi, studi, e così via non è per ora temuto, così come gli attacchi di tipo terroristico, sicuramente circoscritti ad aziende/enti di grandi dimensioni e di grande visibilità nazionale e internazionale.

Il confronto tra le stime sulle probabili motivazioni degli attaccanti riguardo al futuro della presente edizione con quelle precedenti è mostrato nella fig. 65, che evidenzia

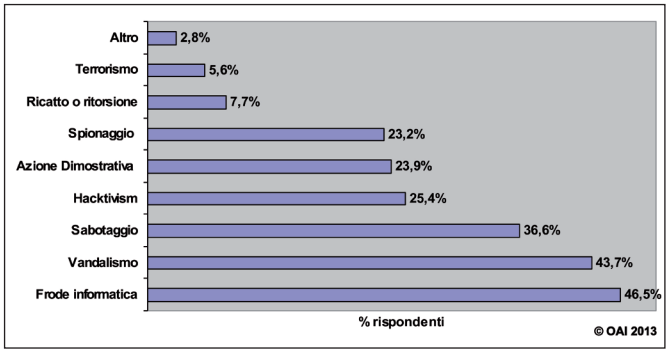

Fig. 64 - Possibili motivazioni per i futuri attacchi temuti (risposte multiple)

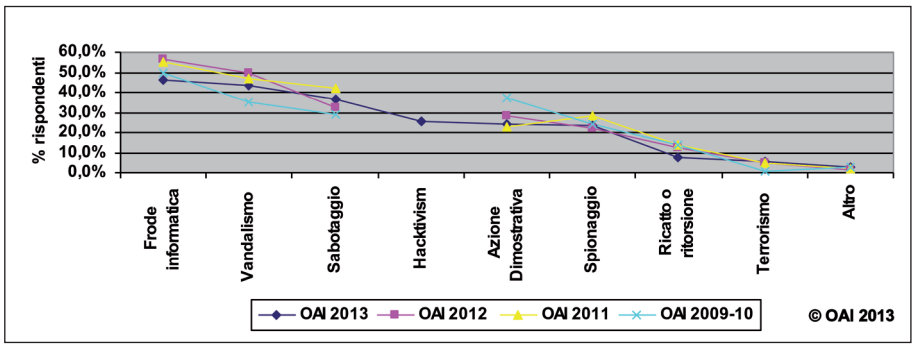

Fig. 65 - Confronto delle motivazioni per gli "attacchi temuti nel futuro" nei vari Rapporti OAI

stime molto simili nel tempo, quindi una sostanziale convergenza di opinioni. Le curve delle edizioni precedenti presentano un punto di discontinuità, avendo introdotto quest'anno la voce hacktivism. Al di là di questa variazione, le curve dei vari anni sono vicine e con scostamenti bassi. 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.

8. Considerazioni finali

I risultati emersi dall'indagine sono significativi e rappresentativi, a livello indicativo se non statistico, di che cosa realmente avviene in Italia per gli attacchi intenzionali ai sistemi informativi delle aziende e degli enti, e come questi si proteggono, come cercano di prevenirli e come reagiscono qualora dovessero loro capitare. Innumerevoli le considerazioni che possono emergere dai dati raccolti con l'indagine, soprattutto se correlati tra loro: nel seguito sono evidenziati alcuni degli aspetti emersi più interessanti, a parere dell'autore: alcuni convergono con i numerosi studi e rapporti internazionali, altri sono specifici della realtà italiana. Come nelle edizioni precedenti, le aziende/enti che hanno risposto al questionario rappresentano una fascia medio-alta del panorama italiano in termini di qualità dei sistemi informatici e della loro gestione, e quindi anche della sicurezza informatica.

I trend sugli attacchi emersi con il campione di rispondenti OAI 2013 sono sostanzialmente in linea con i trend descritti dai principali rapporti internazionali, a parte alcune specificità nazionali.

I macro-trend includono i seguenti aspetti:

- i più diffusi attacchi riguardano 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. 25);
- questi tipi di attacchi sono da anni tra i più diffusi, come rilevato in tutte le edizioni di OAI (fig. 26);
- i tipi di attacchi più temuti nel prossimo futuro sono prevalentemente quelli ora più diffusi (fig. 61);
- le motivazioni degli attaccanti sono soprattutto per un illegale guadagno economico (fig. 64); tale tendenza è consolidata negli ultimi anni come chiaramente evidenziato nella fig. 65. Nonostante questo, gli attacchi più orientati a questi fini, le frodi informatiche, i ricatti, gli accessi e le modifiche non autorizzate a sistemi, programmi e dati, non sono tra i più temuti (fig. 61). L'apparente contraddizione, emersa anche nell'indagine del 2012, può essere spiegata (ipotesi dell'autore) dalla differenza tra la percezione generale di un fenomeno e la sua effettiva possibile occorrenza nel contesto del proprio sistema informativo; ad esempio la frode informatica basata sul furto dell'identità digitale è sicuramente un fenomeno grave e crescente in generale, ma è ritenuto poco probabile, e quindi poco temuto, nella realtà di un sistema informativo di un'azienda di produzione meccanica;
- gli attacchi intenzionali si basano:
  - sulle vulnerabilità tecniche, dal software alle architetture e alle configurazioni dei sistemi informativi; con l'evoluzione tecnologica crescono nuove vulnerabilità, ad esempio con la virtualizzazione, con il cloud, e con i nuovi sempre più potenti dispositivi mobili. Le vulnerabilità sono complessivamente in crescita, talvolta non risolte dai fornitori, che non rilasciano le opportune correzioni; ma spesso non corrette con le "patch" esistenti dagli utenti, per la mancanza di una efficacie organizzazione di test delle nuove versioni e forse anche per il non rinnovo dei contratti di manutenzione del software causato dalle crescenti ristrettezze economiche;
  - sulla gestione della sicurezza ICT, non sempre sistematica ed integrata con la gestione dell'intero sistema informatico, e più in generale sulla limitata attenzione ed impegno per gli strumenti organizzativi di difesa;
  - sulla vulnerabilità delle persone e dei loro comportamenti, sfruttando sia la loro disponibilità e buona fede sia la loro disattenzione e/o ingenuità; la diffusione dei social network, della posta elettronica, dei motori di ricerca, l'uso di sempre più capaci chiavette USB e degli strumenti collaborativi amplia-

no enormemente le possibilità di rubare le identità digitali degli utenti ed acquisire facilmente informazioni riservate con le quali svolgere attacchi e compiere frodi informatiche.

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

- più del 60% del campione non ha subito attacchi né nel 2012 né nel 2013, ma quasi 1/3 ha subito attacchi fino a 10 volte, ed il 6,7% per più di 10 volte (fig. 23); nel 1° semestre 2013 si è rilevato un preoccupante aumento percentuale degli attacchi;
- l'impatto degli attacchi risulta grave solo in un limitato numero di casi; gli impatti effettivi sui sistemi informativi e sui business e/o attività-processi che supportano non sono nella maggior parte dei casi critici (fig. 27); questo è confermato dai veloci tempi di ripristino nella stragrande maggioranza degli attacchi subiti (fig. 34 e 35);
- il fenomeno della consumerizzazione (BYOD) è così sentito per la sicurezza informatica che ben più di 1/3 del campione non lo consente (fig. 11);
- indipendentemente dalle dimensioni e dal settore merceologico di appartenenza, la maggior parte dei sistemi informativi è tecnicamente ben aggiornato, ed una significativa parte dispone di architetture ad alta affidabilità e multipiattaforma;
- nonostante i noti problemi di banda larga in Italia, soprattutto al di fuori delle grandi città, ben più di 1/3 dei rispondenti terziarizza parte o tutto il proprio sistema informativo e la sua gestione (fig. 7 e 17);
- più di 1/4 dei rispondenti, il 27,5%, utilizza soluzioni in cloud (fig. 18);
- le misure di sicurezza sono più diffuse a livello infrastrutturale che applicativo e per la protezione dei dati; inizia comunque a diffondersi una maggior consapevolezza, e quindi attenzione, sulla sicurezza intrinseca del software messo in produzione e sulla protezione delle informazioni, che costituiscono un vero "patrimonio" (asset) per l'azienda/ente, e come tale da gestire e proteggere; quasi il 40% del campione effettua solo controlli a livello di ogni singolo sistema (fig. 42);
- a livello di "governo" della sicurezza informatica, l'approccio è solo parzialmente centralizzato ed integrato con la più generale gestione dell'intero sistema informativo (fig. 42) e prevalentemente basato sul "fai da te", interno o terziarizzato, con limitati riferimenti alle best practice quali ITIL e COBIT o standard quali la famiglia ISO 27000 (da fig. 47 a fig. 52); è molto significativo che siano ben poche le richieste ai fornitori di seguire sostanzialmente tali best practice o di avere le relative certificazioni a livello dell'azienda/ente o delle persone singole; queste ultime non sono nemmeno richieste al personale interno (fig. 54 e 55); la segnalazione di attacchi avviene da circa 1/3 del campione da sistemi di controllo e monitoraggio (fig. 28);
- sul piano organizzativo della sicurezza informatica, per una buona o comunque non trascurabile percentuale del campione, le aziende/enti sono "meno avanzate" che sul piano tecnico;

  a) aspetti positivi:
  - buona parte dei rispondenti ha definito, pubblicato e gestisce le "policy" sulla sicurezza e le relative procedure organizzative, anche di riferimento per i suoi fornitori (fig. 45 e 46);
  - viene svolto o verrà svolto l'auditing informatico da più della metà del campione (fig. 56) e per i 3/4 di chi già lo effettua in modalità periodica e regolare (fig. 57);
  - la continuità operativa è per 1/3 del campione il criterio di riferimento per la valutazione della criticità di un attacco (fig. 30);

  b) aspetti critici:
  - analisi del rischio informatico poco diffusa (fig. 43) ed ancor meno l'assicurazione del rischio residuo (fig. 44);
  - limitata l'analisi del danno subito (fig. 29) ed ancora embrionale, o limitata a poche aziende/enti, la sua stima economica;
  - logiche di separazione delle responsabilità tra i vari attori della sicurezza ICT non ancora diffuse (fig. 45);
  - i piani di gestione delle emergenze, incluso il "disaster recovery", anche se definiti e previsti, raramente sono poi provati in pratica (fig. 42).

La sicurezza dei sistemi informativi assume un ruolo crescente anche per le piccole e medie organizzazioni, che devono anch'esse impegnarsi in una prevenzione continua e sistematica. Da qui l'importanza di poter disporre dei dati raccolti ed elaborati da OAI sullo stato dell'arte in Italia e di quanto, sotto il profilo delle scelte aziendali e organizzative, sia importante pensare alla sicurezza globale ICT come ad un aspetto fondamentale delle policy di continuità e di salvaguardia del patrimonio informativo questo in particolare nella attuale situazione di crisi economica perdurante, in cui tutte le risorse, anche economiche, non dovrebbero essere ridotte o tagliate a danno della sicurezza ICT, ma dovrebbero essere razionalizzate e ottimizzate. In un mondo ormai quasi totalmente informatizzato, qualsiasi infrastruttura, e in particolare quelle critiche, dipendono dal buon e continuo funzionamento dei sistemi informativi che le supportano e le monitorizzano. Il non funzionamento dei sistemi ICT ha conseguenze facilmente immaginabili: si pensi a un blocco anche solo per un giorno o due del servizio elettrico, del bancomat, dei sistemi di trasporto, dell'interoperabilità tra le banche, e ai danni enormi che causerebbero. A parte la "cyberwar", che non è più fantascienza ma possibile realtà, il sistema informativo di un'azienda/ente, anche di piccole dimensioni, è vitale ed essenziale per il funzionamento dei suoi processi e del suo business, che non sono orami più sostituibili con procedure manuali.

Per questo gli attacchi ai sistemi informatici sono divenuti un problema crescente e così critico da allarmare e interessare politici e governi sia a livello nazionale che internazionale. L'intero mondo, sempre più digitale, funziona grazie ad applicativi software per una parte dei quali gli stessi addetti ai lavori non sono in grado di conoscere l'intrinseca sicurezza: un gigante dai piedi d'argilla. Ma nonostante tutto la maggior parte dei sistemi funziona, e la loro sicurezza argina nella maggior parte dei casi gli attacchi, che fino ad oggi, almeno in Italia, sono stati relativamente limitati e non di grave impatto. La guerra tra "guardie" e "ladri" nel mondo digitale è continua, con risultati altalenanti ma spesso a favore dei "ladri", perché più organizzati, più decisi e liberi di selezionare i bersagli. La vulnerabilità più critica e più diffusa è nelle persone. Comportamenti scorretti o inconsapevoli mettono a rischio anche coloro che adottano le misure di sicurezza prescritte e necessarie per abbassare la soglia di rischio.

Come già evidenziato nei precedenti Rapporti, occorre un forte impegno culturale, organizzativo e tecnico, passando dalla fase "specialistica" nella quale la sicurezza ICT è prerogativa dei tecnici alla fase "consapevole", nella quale la percezione dei rischi ICT deve essere nota a tutti i livelli e la conseguente adozione di strategie di sicurezza deve essere oggetto di valutazione da parte del massimo livello decisionale delle singole organizzazioni, anche per l'impatto economico-organizzativo che tali strategie implicano. Rimangano sempre valide le raccomandazioni emanate da varie Istituzioni Internazionali e nazionali per la crescita della cultura della sicurezza ICT sia presso gli utenti sia presso i fornitori di prodotti ICT, secondo i seguenti assi fondamentali:

- consapevolezza: gli operatori devono essere consapevoli di dover dedicare risorse alla sicurezza;
- responsabilità: gli operatori devono essere responsabili della sicurezza dei propri sistemi;
- risposta alle emergenze: gli operatori devono agire in modo tempestivo e cooperativo per prevenire, rilevare e reagire a emergenze riguardanti la sicurezza;
- etica: gli operatori dovrebbero rispettare gli interessi degli altri, prendendo coscienza del fatto che uno scarso livello di sicurezza nei propri sistemi può determinare minacce per gli altri attori;
- valutazione dei rischi: gli operatori dovrebbero pianificare la valutazione dei rischi connessi ai loro propri sistemi;
- progettazione, realizzazione, gestione e valutazione della sicurezza ICT: gli operatori dovrebbero incorporare la sicurezza come elemento essenziale dei propri sistemi informativi e di rete, adottando un approccio globale, che includa la valutazione dei rischi, la predisposizione di misure e piani di sicurezza, le procedure di gestione delle emergenze e la sistematica revisione dei livelli di sicurezza dei propri sistemi, modificando adeguatamente le misure adottate in relazione alla dinamica evolutiva e tecnologica e organizzativa e del business.

9. Glossario dei principali termini e acronimi inglesi 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.
- **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.
- **Buffer overflow**: consiste nel sovra-scivere in un buffer o in uno stack del programma dati o istruzioni con i quali il programma stesso può comportarsi in maniera diversa dal previsto, fornire dati errati, bloccare il sistema operativo, ecc.
- **BYOD**, Bring Your Own Device: policy aziendale che consente l'utilizzo di dispositivi mobili di proprietà dell'utente anche nell'ambito dei sistemi dell'azienda/ente. Il fenomeno è chiamato anche consumerizzazione.
- **Captcha**, Completely Automated PublicTuring test to tell Computers and Humans Apart: l'acronimo indica una famiglia di test costituita da una o più domande e risposte per assicurarsi che l'utente sia un essere umano e non un programma software.
- **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.
- **Consumerizzazione**: vedi BYOD
- **Darknet**: sistema usato in Internet per monitorare la rete e possibili attaccanti, con funzionalità simili a quelle di un honeypot.
- **Deadlock**: un caso particolare di "race condition", consiste nella condizione in cui due o più processi

non sono più in grado di proseguire perché ciascuno aspetta il risultato di una operazione che dovrebbe essere eseguita dall'altro.

- **Deamon**: software di base operante in back-ground in un ambiente multi-tasking.
- **Defacing** o **defacement**: in inglese significa deturpare, e nel gergo della sicurezza informatica indica un attacco ad un sito web per modificarlo o distruggerlo; spesso con tale termine viene indicata la modifica della sola home-page.
- **Denial of service (DOS)** e **Distributed DoS (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**: correzzione di un programma software, usato spesso come sinonimo di patch.
- **Flash threats**: tipi di virus in grado di diffondersi molto velocemente.
- **FTPS**, File Transfer Protocol Secure: per il trasferimento di file crittati.
- **Hijacking**: tipico attacco in rete "dell'uomo in mezzo" tra due interlocutori, che si maschera per uno dei due e prende il controllo della comunicazione. In ambito web, questo termine è usato per indicare un attacco ove: le richieste di pagine a un web vengo dirottate su un web falso (via DNS), sono intercettati validi account di e-mail e poi attaccati questi ultimi (flooding).
- **Hoax**: in italiano bufala o burla, indica la segnalazione di falsi virus; rientra ta 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.
- **HTTPS**, HyperText Transfer Protocol Secure: per le transazioni crittate tra browser e sito web, e viceversa.
- **IaaS**, Infrastructure as a Service.
- **Information Leakage**: diffusione-dispersione non autorizzata di informazioni.
- **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 in pratica ricercate e distrutte le voci di registri, log, contrassegni e file temporanei, ecc. Possono operare sia a livello di sistema operativo (es. deamon sui server Unix/Linux), sui registri dei browser, ecc. Esistono innumerevoli programmi per gestire le registrazioni, anche se sono tecnicamente complessi.
- **Malware**: termine generico che indica qualsiasi tipo di programma di attacco.
- **Mirroring**: termine 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 tramite il quale viene chiesto un riscatto (ransom) per far funzionare correttamente il sistema.
- **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.
- **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 più generali attacchi.
- **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 i contenuto (pay load) dei pacchetti in rete, sia LAN che WAN.
- **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.
- **Trouble ticketing**: processo e sistema informatico di supporto per la gestione delle richieste e delle segnalazioni da parte degli utenti; tipicamente in uso per help-desk e contact center.
- **VPN**, Virtual Private Network: rete virtuale creata tramite Internet per realizzare una rete "private" e sicura per i soli utenti abilitati di un'azienda/ente.
- **XSS**, Cross - site scripting: una vulnerabilità di un sito web che consente di inserire a livello "client" dei codici maligni via "script", ad esempio JavaScript, ed HTML per modificare le pagine web che l'utente vede.
- **Watering Hole**: famiglia di attacchi che rientrano nella categoria dei Targeted Attack. Il termine,traducibile in" attacco alla pozza d'acqua", fa riferimento agli agguati di animali carnivori alle prede che si dissetano in una pozza d'acqua. La metafora è usata per attacchi mirati a siti web specialistici, ad esempio di finanza, di politica, di strategie, ecc., cui una persona o un'azienda target accede periodicamente.
- **Worm**: un tipo di virus che non necessita di un file eseguibile per attivarsi e diffondersi, dato che modifica il sistema operativo del sistema attaccato in modo da essere eseguito automaticamente e tentare di replicarsi sfruttando per lo più Internet.
- **Zero-day attach**: attacchi basati su vulnerabilità a cui non è ancora stato trovato rimedio.
- **Zombies**: vedi bots.

10. Riferimenti e fonti

Dal numero di marzo 2010 della rivista Office Automation, l'Autore tiene una **rubrica mensile OAI** per dare continuazione tra un rapporto annuale e l'altro e per promuovere sensibilità e conoscenza sugli attacchi ai sistemi informatici in Italia. Con queste stesse motivazioni è stato anche attivato un **Gruppo OAI** su **LinkedIn**.

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

- C. Sarzana di S. Ippolito: "Informatica e diritto penale", 1994, Giuffré Editore.
- FTI: "La sicurezza nei sistemi informativi – Una guida per l'utente", 1995, Pellicani Editore.
- FTI: "Osservatorio sulla criminalità informatica – Rapporto 1997", Franco Angeli.
- M. 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. 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. 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 978 88 90890109.

10.2 Le principali fonti sugli attacchi e sulle vulnerabilità

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

- ABILAB - Centrale d'allarme per attacchi informatici: www.abilab.it per l'ambito bancario, accessibile solo agli iscritti.
- CERT-CC, Computer Emergency Response Team - Coordination Centre: http://www.cert.org/certcc.html fornisce uno dei più completi ed aggiornati sistemi di segnalazioni d'allarme, rapporti sulle vulnerabilità; a livello US cura la banca dati sulle vulnerabilità (http://www.kb.cert.org/vuls/).
- Clusit (www.clusit.it): "Rapporto annuale sulla sicurez-

za ICT in Italia", interessanti considerazioni sull' elaborazione di dati provenienti da ricerche di terzi e da altri rapporti.

- CSI, Computer Security Institute http://gocsi.com/survey fornisce un dettagliato rapporto annuale sui crimini informatici negli US.
- 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/it/viruswatchlite?hour_offset=-2.
- 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 partnership tra FBI (Federal Bureau of Investigation), il National White Collar Crime Center (NW3C) e il Bureau of Justice Assistance (BJA): http://www.ic3.gov/default.aspx fornisce, oltre alla possibilità di denunciare negli US attacchi Informatici, informazioni sugli attacchi stessi e sui trend in atto per i crimini informatici.
- Microsoft Security Intelligence Report: http://www.microsoft.com/security/sir/default.aspx fornisce un approfondito rapporto semestrale su vulnerabilità e rischi.
- Panda Security: http://www.pandasecurity.com/enterprise/security-info/fornisce informazioni sugli attacchi sia a livello domestico che d'impresa,oltre che rapporti periodici.
- 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.
- 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.
- 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.
- 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.

Profilo dell'Autore

Marco Rodolfo Alessandro Bozzetti, ingegnere elettronico, è amministratore unico di Malabo Srl, società di consulenza e servizi sull'ICT ed ideatore e curatore di OAI, Osservatorio Attacchi Informatici in Italia, e di EAC, Enterprise Architecture Conference. Attraverso la sua società Marco conduce interventi consulenziali sia lato domanda che 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, di AIPSI e di Prospera. 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 che domanda ICT. Malabo dispone di un piccolo laboratorio sperimentale costituito da due server dual Xeon quad core con VMWare ESXi con storage condiviso sui quali installare e testare qualsiasi tipo di sistema operativo e/o applicativo.

La consulenza

Lato domanda l'intervento principale è di aiutare il cliente nell'uso efficace ed efficiente dell'ICT in modo da creare per lui un effettivo e misurabile valore; lo stesso obiettivo si applica per le aziende dell'offerta ICT, per le quali gli interventi spaziano da quelli per il miglior uso dell'ICT, a quelli più strategici per una reale crescita, per incrementare immagine e guadagni, per meglio posizionarsi sul mercato italiano e internazionale. Gli interventi sui sistemi informativi 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 ed all'italiano UNI 11506, la riorganizzazione dei processi ICT con intelligente e contestuale riferimento a ITIL v3 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 una risorsa ICT indirizzabile via Internet.
- **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.
- 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

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;
  - EUCIP, European Certification of Informatics Professionals, il sistema europeo che definisce le competenze e le figure professionali nel settore informatico, articolato su 22 profili delineati attraverso oltre 3.000 elementi di conoscenza, che vengono costantemente rivisti e aggiornati dal CEPIS e, per l'Italia, da AICA. EUCIP si inquadra nel più generale quadro di riferimento europeo, con validità legale, e-CF, e-Competences Framework europeo.

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 di ISSA® è parte della più grande associazione non-profit di professionisti della sicurezza che vanta oltre 10000 a livello mondiale. L'organizzazione di forum e di seminari di approfondimento e di trasferimento di conoscenze, la redazione di documenti e pubblicazioni, la certificazione LoCSI, Localizzazione Competenze 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 webcast, newsletter di ISSA e newsletter italiana di AIPSI.
- Trasferimento di conoscenza e formazione continua sulla sicurezza per l'aggiornamento e la crescita professionale dei Soci.
- Rappresentanza dei professionisti dell'Information Security, nell'ambito delle recenti normative italiane stabilite dal D.Lgs. 4/2013 sulle professioni non regolamentate.
- Certificazioni professionali per le competenze sulla sicurezza.
- Networking con altri professionisti del settore.
- Possibilità di costituire gruppi di lavoro e di 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.
- Promozioni interne per chi "porta" nuovi soci e/o contribuisce fattivamente all'attività dell'Associazione.

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

Seeweb nasce nel maggio 1998 da un dinamico gruppo di soci fondatori italiani per fornire servizi di alta qualità di hosting e housing tramite una prima propria Server Farm; nel tempo è cresciuta anche grazie ad acquisizioni esterne e ad una costante ed elevata attenzione a tecnologia, qualità, scalabilità e rapporto prezzo/prestazioni, collocandola ora tra le prime compagnie nazionali del settore. Nel 2009 Seeweb è la prima azienda in Italia, e tra le prime al mondo, a proporre soluzioni di cloud computing. Attualmente possiede quattro Data Center in Italia, due a Frosinone - di cui uno recentemente ampliato per complessivi 6300 mq e completamente dedicato alle infrastrutture per il cloud - e due a Milano, in via Caldera, cuore dell'Internet italiana. Per triangolare in altissima affidabilità Seeweb opera con un Data Center nel nord Europa e con connessioni a barda larga dai migliori provider di telecomunicazione. Oltre ai servizi di hosting, housing e colocation, Seeweb vanta un'offerta a 360° nella nuvola: Cloud Hosting, Cloud Server, Cloud Storage, Cloud Streaming, Foundation Server (quest'ultimo server dedicato fisico ma molto pensato per la virtualizzazione). Al cliente che voglia spostare le sue infrastrutture complesse su Cloud, Seeweb garantisce il massimo supporto nella consulenza, nella migrazione e nella fornitura di tutto quanto occorra a raggiungere il massimo delle performance (cloud infrastructure, VPN, appliance, load balancing, ecc.). Il picco di utilizzo della Cloud Infrastructure Seeweb nel corso del 2013 è arrivato a 6540 CPU e 18996 GB di RAM. Dati in costante crescita pur in un momento di riduzione degli investimenti.

Sicurezza e affidabilità

Nell'erogazione di questi servizi ICT affidabilità, qualità e sicurezza sono caratteristiche imprescindibili, per le quali Seeweb ha fin dagli inizi attuato, anche a livello contrattuale, un reale Service Level Agreement che arriva fino al 99,95% di garanzia con penale in caso di non rispetto. Per questi livelli di eccellenza Seeweb ha ricevuto numerosi premi e riconoscimenti a livello nazionale e internazionale, e secondo *audit Netcraft* è costantemente tra le prime 10 Hosting Company a livello mondiale per affidabilità e qualità del servizio. Il sistematico aggiornamento tecnico e organizzativo dei Data Center e dei sistemi ICT, completamente gestiti dal personale di Seeweb, ha portato anche a una particolare attenzione agli aspetti energetici ed eco-ambientali. I locali dei Data Center sono dotati di un sistema efficientissimo di sorveglianza elettronica e di controllo del clima, con allarmi locali e remoti su valori critici. La sala energia è separata e prevede climatizzazione dedicata e ridondata, sistema antincendio a saturazione, quadri di distribuzione separati e linee elettriche separate e compartimentate fino ai server. Questa alta efficienza energetica è stata premiata nel 2008 ponendo Seeweb tra le 10 aziende campioni del progetto *Dinameeting* di Regione Lombardia per lo sviluppo tecnologico, l'energia e la competitività delle PMI lombarde.

Oltre alle misure fisiche di sicurezza, si aggiunge la costante verifica, da parte degli amministratori di sistema, dell'efficienza dei sistemi, dei profili di traffico e delle eventuali attività malevoli. La gestione dei sistemi e della sicurezza informatica è centralizzata ed integrata, basata sulle più consolidate metodiche e best practice quali ITIL e COBIT, e con l'utilizzo di diversi ambienti di monitoraggio e controllo, tra cui Tivoli IBM Storage per i backup automatici e di Tivoli TSM per il disaster recovery. Seeweb dispone della certificazione di processo ISO9001, di compatibilità ambientale ISO14001, e di sicurezza nel trattamento dei dati ISO27001.

Per maggiori informazioni: www.seeweb.it

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 continuità operativa 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

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: http://www.technologyestate.eu/

Dal 1988, anno della sua fondazione, Trend è pioniere nelle tecnologie che proteggono dalle minacce sui nuovi dispositivi e piattaforme.

La Società
Quotata alla Borsa di Tokyo, ha attualmente 4.942 dipendenti e sedi in tutto il mondo, di cui due in Italia. Il fatturato nel 2012 ammontava a 1,174 miliardi di US $. Nel 2012, IDC nomina Trend Micro leader internazionale nella sicurezza server per il terzo anno consecutivo. Nel 2013 Trend Micro festeggia il 25° anniversario e Canalys Research la nomina numero 1 nella protezione dei contenuti per le 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 25 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 progetta su misura soluzioni per ogni situazione 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 e Dell 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: 4 miliardi di minacce bloccate al giorno per i clienti in tutto il mondo.

Intelligence e assistenza globali
Attraverso i TrendLabs, con oltre 1.000 esperti Trend Micro offre intelligence puntuale contro le minacce, assistenza e supporto ai clienti.

Per ulteriori informazioni: www.trendmicro.it

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