Sponsor

Rapporto 2012 OAI

a cura di
Marco R.A. Bozzetti

Osservatorio sugli Attacchi Informatici in Italia

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

Finito di stampare nel mese di dicembre 2012
da Àncora Arti Grafiche srl - Milano

per conto di Soiel International
Via Martiri Oscuri, 3 - 20125 Milano
E-mail: soiel@soiel.it
www.soiel.it

Rapporto
2012 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 2012.
Un grazie particolare agli Sponsor, all'editore Soiel International, al dott. Francesco Zambon, all'ing. Maurizio Mapelli che con i loro contributi hanno consentito la realizzazione del presente Rapporto.

INDICE

1. Introduzione

Il presente Rapporto 2012 OAI, Osservatorio Attacchi Informatici in Italia, fa riferimento agli attacchi informatici rilevati nel corso del 2010, 2011 e del 1° quadrimestre 2012. È la terza edizione, dopo il Rapporto 2011 ed il Rapporto 2009-10, ed è la prima volta che questa iniziativa viene sponsorizzata da alcune importanti aziende della domanda, il Gruppo Lottomatica, e dell'offerta ICT[1], Accenture, IBM, Orsyp, Sernet, Seeweb, Trend Micro, oltre che da AIPSI, Associazione Italiana Professionisti Sicurezza Informatica, capitolo italiano della associazione mondiale ISSA, che considera OAI uno dei principali servizi offerti ai propri soci.
Alla fine del Rapporto 2012, da pag. 39 a pag. 47, sono inserite in ordine alfabetico le schede di presentazione degli Sponsor, con l'approfondimento delle loro attività nel campo della sicurezza informatica.
Le precedenti edizioni[2] furono scaricabili ai 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 (clienti, fornitori, ecc.).
L'iniziativa OAI ha visto crescere, rispetto all'edizione precedente, il numero di Patrocinatori, che annovera ora, oltre alla collaborazione con la Polizia delle Comunicazioni, 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 Emilia Romagna, Club per le Tecnologie dell'Informazione delle Marche, 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 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* di 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.
Obiettivo primario di OAI è di fornire concrete indicazioni sugli attacchi intenzionali ai sistemi informatici delle Aziende e degli Enti pubblici italiani, che possano indicare 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 ICT soprattutto a livello dei decisori "non tecnici", figure tipicamente ricoperte dai vertici dell'organizzazione che decidono e stabiliscono i budget ed i progetti attuativi. 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 il sovente uso di termini tecnici. Per facilitare la lettura, è disponibile in §9 un glossario degli acronimi e dei termini tecnici specialistici usati.

[1] ICT, Information and Communication Technology
[2] Gratuitamente scaricabili dal sito web dell'Autore, www.malaboadvisoring.it, e da quello dell'Editore Soiel International, www.soiel.it

1.1 Aspetti metodologici dell'indagine

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 2012 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.

Il Questionario 2012 è stato posto on line per circa tre mesi, da fine luglio 2012 a fine ottobre 2012, 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. Il campione dei rispondenti non è predefinito e selezionato a fini statistici, ma si basa sulle risposte volontarie. Come descritto in §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, così come ha provveduto a verificare i dettagli delle risposte con "altro" ed eventualmente a conteggiarle nelle altre risposte previste.

Nel Rapporto si confrontano in alcuni casi 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 le percentuali (%) dei Rapporti OAI sono in funzione del numero di rispondenti, risposta per risposta. A parte i campioni diversi nelle tre edizioni, le risposte differiscono domanda per domanda sia per il numero complessivo di rispondenti, non sempre il medesimo anche nello stesso anno, sia nel caso di possibili risposte multiple.

Nell'edizione 2012 il questionario è totalmente anonimo: non viene richiesta alcuna informazione personale e/o identificativa del compilatore e della sua azienda/ente, non viene rilevato e tanto meno registrato il suo indirizzo IP, sulla banca dati delle risposte non viene nemmeno specificata la data di compilazione. Tutti i dati forniti vengono usati solo a fini statistici e comunque il livello di dettaglio sulle caratteristiche tecniche dei sistemi ICT non consente in alcun modo di poter 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. 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 essere più espletati.

L'evoluzione moderna dei sistemi informativi si è consolidata su Internet e sui siti web, evolvendo velocemente verso logiche collaborative e di web 2.0, oltre che verso logiche di terziarizzazione tipo XaaS (Software/Platform/Infrastructure/Storage/Network/ecc. as a Service), il così detto 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" (P2P), 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 lap-top, 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, PC, tablet e smartphone personali, 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; dall'altro vede una minore necessità di competenze, oltre che una maggiore e facile reperibilità degli strumenti necessari a effettuare attacchi deliberati e nocivi.

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 lo statunitense CSI (Computer Security Institute), il First (Forum for Incident Response and Security Team) o quelli provenienti dai principali Fornitori di sicurezza informatica, quali IBM, Trend Micro ed altri (in §10 un elenco delle principali e più aggiornate fonti). Questi studi forniscono con cadenza periodica informazioni molto dettagliate per i principali paesi e individuano i principali trend; dati specifici riguardanti l'Italia normalmente non sono 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 da richiamo mediatico o come una tematica da 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[3]. Si definì una metodologia di indagine in collaborazione con gli esperti dei vari Enti patrocinatori, per raccogliere sul campo i dati presso un insieme di enti e di imprese (che si spera possa sempre più ampliarsi nel tempo) e per fornire con cadenza annuale e gratuitamente i risultati.

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

Dato il successo riscosso nelle prime due edizioni, l'iniziativa OAI continua 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. 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.
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 nuovo volume di prossima pubblicazione a cura dell'Autore e di Francesco Zambon "Sicurezza digitale" edito da Soiel International.
Per il Questionario OAI 2012 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 2012 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).
Alcuni degli attacchi sono tra loro correlati in quanto sequenziali: ad esempio le modifiche non autorizzate ai dati o al software richiedono prima l'accesso non autorizzato ai sistemi; non sempre nelle risposte il compilatore ha tenuto conto di questo, e si vedrà nelle prossime edizioni di condizionare e vincolare opportunamente tali sequenzialità.
In questa edizione sono stati aggiunti, attacco per attacco, domande inerenti l'impatto più o meno grave che la sua occorrenza ha provocato all'azienda/ente.

4. Caratteristiche dei rispondenti e dei sistemi ICT

Il Questionario OAI 2012 fa riferimento agli attacchi subiti nel 2010, nel 2011 e nel primo quadrimestre 2012. L'indagine è stata svolta nel corso del 2012 mettendo il questionario on-line da fine luglio a fine ottobre 2012, ed

Tabella 1

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 nascondibili 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 vengono procurati seri danni).
8. **Accesso e uso non autorizzato degli elaboratori, delle applicazioni supportate e delle relative informazioni**.
9. **Modifiche non autorizzate ai programmi applicativi e di sistema, alle configurazioni, ecc**.
10. **Modifiche non autorizzate ai dati e alle informazioni.**
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. **Utilizzo codici maligni (malware)** di varia natura, quali virus, Trojan horses, Rootkit, bots, exploits, sia a livello di posto di lavoro che di server.
13. **Saturazione risorse informatiche e di telecomunicazione**: oltre a DoS (Denial of Service), DDoS (Distributed Denial of Service) e Botnet, si includono in questa classe anche mail bombing, spamming, catene di S. Antonio informatiche, ecc.
14. **Attacchi alle reti, fisse o wireless, e ai DNS (Domain Name System)**.

il Rapporto finale è stato prodotto nel mese di novembre 2012.

Come indicato in §1.1, il bacino delle persone contattate per compilare il questionario si aggira attorno alle 6000 persone, rispetto a più di 1800 della scorsa edizione.

Pur avendo più che triplicato il numero potenziale di compilatori, si sono avute difficoltà nell'ottenere risposte, soprattutto da alcuni settori, nonostante i numerosi e ripetuti solleciti inviati anche in maniera mirata ai settori con meno risposte. Le risposte avute alla fine sono state 206, rispetto alle 130 e alle 105 delle due precedenti edizioni. Un incremento significativo, ma con un numero di risposte ancora estremamente 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, ecc.

Come già evidenziato in precedenza, il numero di risposte ricevute sono sufficienti e significative a fornire delle concrete indicazioni sugli attacchi ai sistemi informativi in Italia. L'analoga iniziativa statunitense CS[4]I, consolidata da anni e modello di riferimento anche per l'OAI, raccoglie un campione di poco più di 500 interlocutori per tutti gli Stati Uniti. Il rapporto di circa 1:2,5 (rispetto all'1:4 e all'1:5 delle precedenti edizioni) di rispondenti tra i due rapporti, tenendo anche conto delle diverse coperture geografiche Italia ed USA, è più che sufficiente ai fini indicativi, se non strettamente statistici, ed agli obiettivi di OAI.

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, dai fornitori ed i consulenti, che gestiscono per l'azienda/ente la sicurezza informatica, fino ai responsabili di massimo livello delle aziende piccole e piccolissime (proprietari, presidenti e amministra-

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

tori) che direttamente o indirettamente conoscono e gestiscono i 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 le figure di vertice della struttura (Presidenti, Amministratori Unici o Delegati, Direttori Generali), al terzo posto i responsabili della sicurezza informatica (CISO). Seguono altri ruoli quali i responsabili delle tecnologie (CTO, Chief Technology Officer), le terze parti, fornitori e consulenti che gestiscono la sicurezza ICT, ed ultimi i CSO. Una percentuale non trascurabile dei rispondenti, pari al 12%, ha selezionato "Altri": tale opzione include tipicamente figure operanti nell'Unità Organizzativa Sistemi Informativi (UOSI), competenti sulla sicurezza e sugli attacchi subiti, che non hanno uno dei ruoli di cui sopra ma che con loro collaborano.
La percentuale alta di figure con potere decisionale 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.
Rispetto al Rapporto 2011 la composizione è analoga, e la maggior differenza è proprio sulla percentuale di quest'ultima categoria "Altri", che dal 6% raddoppia.
La fig. 2 illustra la suddivisione dei compilatori per i settori merceologici di appartenenza delle loro aziende/enti. In questa edizione, tenendo anche conto dei suggerimenti avuti, si sono ridotti nel questionario i macro settori merceologici di riferimento rispetto all'edizione precedente. Le modifiche riguardano:

- l'eliminazione del settore ICT, ripartito in "Industria" per le aziende che producono dispositivi ICT, e in "Servizi e distribuzione" per le aziende che vendono ICT, le software house, gli integratori di sistemi e la consulenza;
- l'inserimento di "Telecomunicazioni e Media" e di "Sanità";
- l'accorpamento di "Servizi" con "Distribuzione", nel precedente rapporto separati ed indicata quest'ultima con il termine inglese di "Retail".

Come si evidenzia dalla fig. 2, soprattutto gli importanti (per l'ICT) settori dell'ambito finanziario, che include banche e assicurazioni, e della Pubblica Amministrazione, sia locale (PAL) che centrale (PAC), hanno risposto in maniera ancora esigua, nonostante le sollecitazioni, così come era successo anche per i precedenti Rapporti. Le motivazioni riguardano probabilmente sia il poco tempo disponibile da parte dei responsabili ICT e/o della sicurezza a rispondere, sia (soprattutto per banche ed ambienti finanziari) le autorizzazioni necessarie all'interno delle strutture per fornire questi tipi di informazioni.
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, gli altri segmenti si attestano tra il 10 ed il 20%.
L'area geografica di copertura dell'azienda/ente è, per il campione raccolto, prevalentemente nazionale, e solo il 22% circa ha una copertura internazionale, a livello euro-

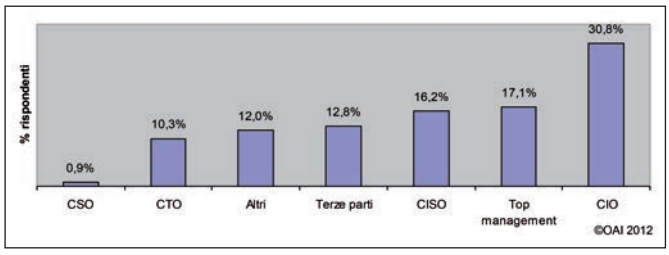

Fig. 1 - Ruolo rispondenti

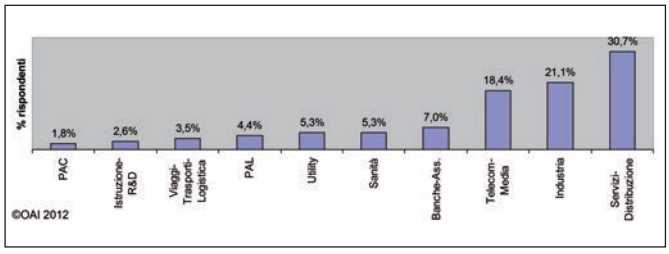

Fig. 2 - Settore merceologico di appartenenza

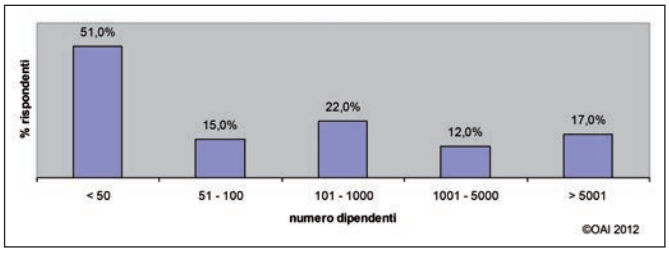

Fig. 3 - Dimensioni aziende/enti per numero dipendenti

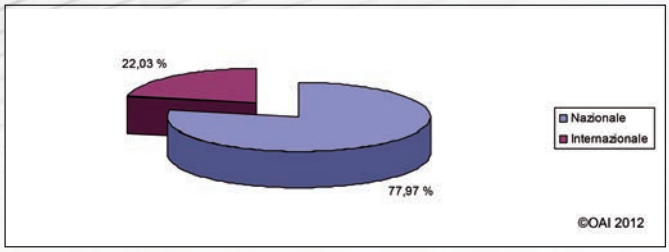

Fig. 4 - Copertura geografica azienda/ente

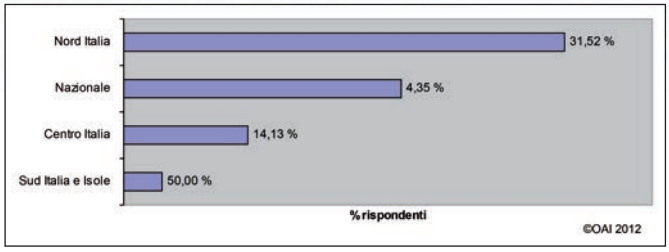

Fig. 5 - Ripartizione sul territorio nazionale

peo o mondiale, come mostrato dalla fig. 4. I rispondenti della presente edizione sono meno internazionali rispetto a quelli della precedente, che arrivavano a ben il 42%.
Nella fig. 5 i rispondenti dell'area solo nazionale sono dettagliati per copertura Nord-Centro-Sud e Isole o dell'intero territorio. Un terzo circa ha copertura nazionale, quasi la metà opera al Nord, il resto, a decrescere, al Centro e Sud ed Isole.
Dato che il Questionario 2012 copre una ampio arco temporale dal 2010 al 1° quadrimestre 2012, per la correttezza delle risposte fornite si è voluto accertare che l'azienda/ente esistesse e fosse operativa già dal 2010, in caso contrario si richiedeva di inserire la risposta <Mai> negli anni in cui non fosse esistita per le domande sugli attacchi subiti relative a quegli anni. Tra i rispondenti solo una società di consulenza ed un'azienda di telecomunicazioni si sono attivati dopo il 2010.
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 Data Center o "computer room" per le realtà più piccole, e la fig. 7 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 poi 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 organizzativo.
Come mostrato in fig. 7, i sistemi totalmente terziarizzati coprono circa il 21%, del campione, poco più di un terzo sono gestiti internamente ma, e questo è il dato più interessante, quasi il 44% ha soluzioni miste, gestendoli in parte internamente ed in parte esternamente: un chiaro indicatore del crescente ruolo della terziarizzazione e del cloud.

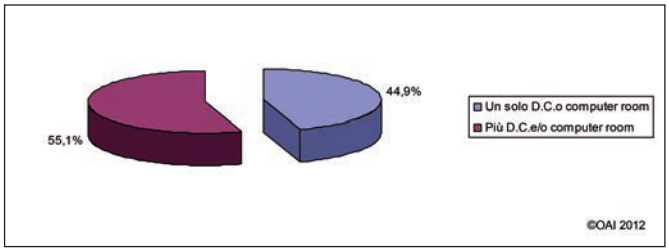

Fig. 6 - Data Center (D.C.) e computer room

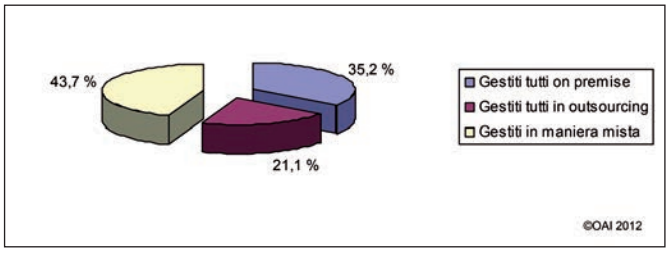

Fig. 7 - Modalità di gestione del sistema informativo

Questi dati evidenziano una significativa evoluzione della logica e della cultura italiana sull'ICT, se consideriamo che nel precedente Rapporto OAI (anche se il campione dei rispondenti era parzialmente diverso dall'attuale) ben il 72,3% dei sistemi erano gestiti totalmente all'interno.
Per comprendere le dimensioni dei sistemi informativi del campione emerso, la fig. 8 mostra in percentuale il numero di server presenti. I dati sono simili a quelli raccolti nella precedente edizione per le piccole e medie organizzazioni, con un numero di server fino a 100; aumentano significativamente per le grandi, oltre i 1000: il motivo è dato dalla virtualizzazione più ampia tipica delle medio-grandi organizzazioni.
La fig. 9 mostra le percentuali del numero di posti di lavoro fissi (PdL) per sistema informativo: poco meno del 60% dei rispondenti ha fino a 100 PdL fissi, di cui più del 22% per i piccoli sistemi, fino a 10 PdL. Questi dati confermano come nei piccoli sistemi informatici il numero di PdL fissi sia dello stesso ordine di grandezza dei server, talvolta anche inferiore, dato il basso numero di dipendenti, evidenziato nella fig. 3 che mostra come il 51% dei rispondenti è in organizzazioni con meno di 50 dipendenti: la tipica diffusissima situazione delle Piccole Imprese in Italia. Il campione emerso dalla fig. 2, inoltre, evidenzia come gran parte dei rispondenti appartiene al settore dei servizi e della piccola e grande distribuzione, delle TLC e dei media, nei quali spesso c'è un PdL per dipendente: anche questo dato è congruente con il dato della stessa fig. 3 sulla % di aziende con più di 1000 dipendenti, pari a circa un quarto del totale.
In termini di sicurezza i dispositivi mobili, in particolare smatphone e tablet, stanno giocando un ruolo fondamentale, data la loro rapida e pervasiva diffusione, oltre che per il fenomeno della "consumerizzazione" e del BYON, 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": per tale motivo il Questionario 2012 ha introdotto alcune specifiche domande in merito.
La fig. 10 mostra la percentuale per numero di dispositivi mobili di proprietà della azienda/ente e forniti ai dipendenti: il questionario non richiedeva di specificare i tipi diversi di dispositivi mobili, e ragionevolmente si presume che la maggior parte sia 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. Il 3% del campione, costituito da aziende/enti dei settori sanità e industria, non fornisce dispositivi mobili ai propri dipendenti.
La fig. 11 evidenzia il fenomeno della "consumerizzazione". Un primo dato che emerge è che nelle aziende/enti di quasi un terzo dei rispondenti non è consentito (ancora) il BYOD. Dove invece è permesso, la ripartizione percentuale per numero di dispositivi è ovviamente più alta.

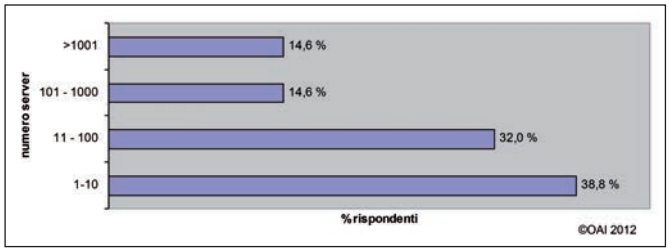

Fig. 8 - Numero complessivo di server fisici e virtuali

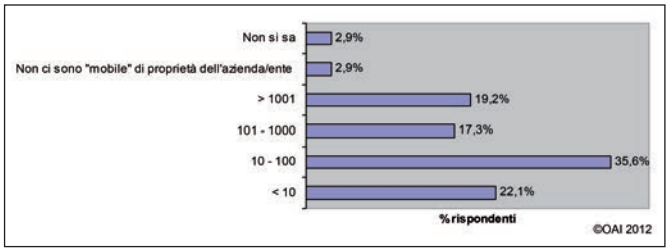

Fig. 10 - Dispositivi mobili dell'Azienda/Ente

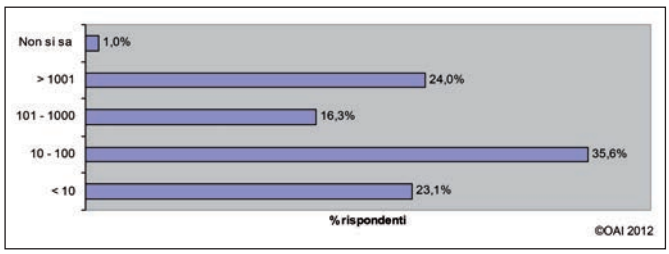

Fig. 9 - Posti di lavoro (PdL) fissi

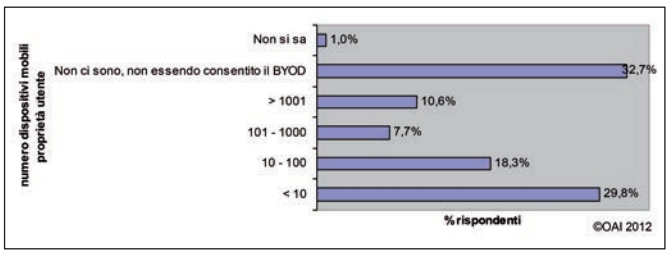

Fig. 11 - Dispositivi mobili proprietà utente finale

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 costituisce 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 le tipologie di sistema operativo per server in uso, ed la loro quantità in percentuale. Le risposte possibili sul questionario erano multiple. Il sistema Windows Server 2008 di Microsoft ha nel campione la più larga diffusione, cui segue Linux con una percentuale di poco inferiore. Windows Server 2003 è usato dal 59% e Unix dal 33,3%. Sono ancora attivi server con precedenti versioni di Windows ed è significativa la diffusione, per poco meno di 1/3 del campione, di sistemi Hypervisor per la virtualizzazione, che includono prodotti quali Z/VM, VMWare, ESX, XenServer, Hyper-V; questo dato è un indice del consolidamento e della razionalizzazione dei Data Center. L'alta percentuale dei server Windows 2008 è indice di un alto livello di aggiornamento tecnologico del campione, e le percentuali complessive dei mondi Windows e Linux-Unix ribadiscono la convergenza del mercato su questi due mondi. Per gli altri tipi di sistemi operativi rimangono da un lato i mainframe, tipicamente "host" centrali delle grandi organizzazioni quali banche e PAC, e dall'altro i sistemi AS 400, storicamente diffusi nelle PMI di fascia alta, con il loro OS 400. L'omogeneità dei sistemi è prevalente nelle strutture piccole o piccolissime: tipicamente chi sceglie Windows non utilizza Linux e viceversa. Nei sistemi di medie e grandi dimensioni è invece prevalente l'eterogeneità dei sistemi operativi, anche se ormai "limitata" agli ambienti Microsoft, Linux-Unix e Hypervisor per la virtualizzazione.

La figura fornisce percentuali simili a quelle della precedente edizione, a parte la leadership di Windows 2008 (molte le migrazioni da Windows NT, 2000 ed in parte 2003) e l'indicazione di un parco server sempre meno eterogeneo, con la presenza di pochi ambienti per sistema informativo, ma aggiornati.

In fig. 13, con risposte multiple e congruentemente con la tipologia dei sistemi operativi, il database (DB) più diffuso nel campione dei rispondenti è Microsoft SQL, che distanzia il secondo più diffuso, l'open source MySQL, che a sua volta sopravanza di poco Oracle. Anche questa classifica è sostanzialmente simile a quella dell'edizione scorsa. 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. Nello stesso sistema informativo possono essere presenti ed usati contemporaneamente diversi DB: tipicamente nei mainframe e nei sistemi di grandi dimensioni sia DB2 sia Oracle.

Anche in questo caso l'omogeneità è tipica degli ambienti piccoli o piccolissimi: per quelli Microsoft la scelta è tipicamente Microsoft SQL, per quelli Linux-Unix è MySQL. Molte aziende di medie dimensioni hanno un AS/400 come "host" centrale e sistemi dipartimentali - distribuiti basati o su sistemi Windows o Unix/Linux.

Come "Altro" sono specificati Postgres, Pervasive SQL ed Access.

Le fig. 14 e 15, entrambe con risposte multiple, inquadrano i principali ambienti e piattaforme architetturali in uso; le risposte sono multiple e confermano che due sono gli ambienti dominanti in quasi tutti i sistemi informativi: l'ambiente Microsoft e l'ambiente Java, PHP e simili (Perl, Pithon, ecc.). Più del 20% del campione ha ancora siste-

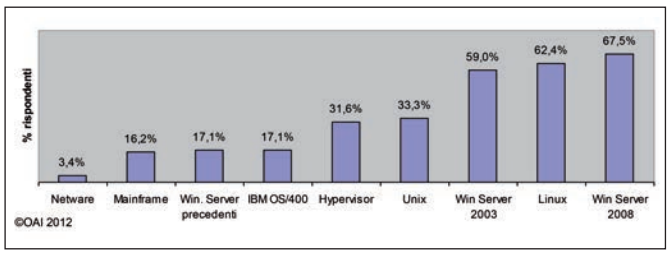

Fig. 12 - Sistemi Operativi dei server in uso

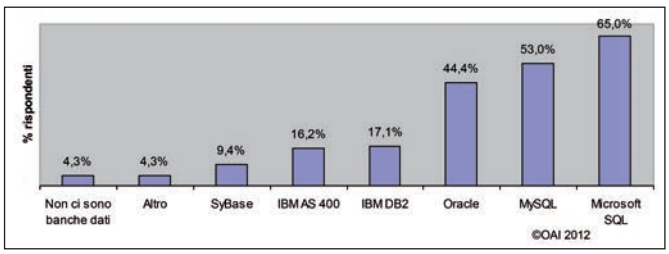

Fig. 13 - Banche dati in uso

mi legacy[5] e solo l'14,5% utilizza applicazioni in cloud, tipo Google App: altro chiaro indice della progressiva, seppur ancora limitata, adozione di soluzioni cloud applicative, a conferma dei dati della precedente fig. 7. Molti sistemi informativi utilizzano anche tutti e quattro gli ambienti, come confermato dalla fig. 15, che evidenzia come circa il 40% utilizza più piattaforme contemporaneamente. Più del 46% ha sistemi virtualizzati, indice che quasi la metà dei sistemi di medie e grandi dimensioni sono stati razionalizzati, e poco più del 23% usa sistemi basati su architetture SOA[6], Service Oriented Architecture, con i web services per garantire interoperabilità tra programmi scritti in linguaggi diversi ed operanti su piattaforme diverse.

Per quanto riguarda le reti, la quasi totalità dei rispondenti ha reti locali sia "wired" (LAN, Local Area Network) che "wireless" (WLAN, Wireless LAN), come mostrato in fig. 16 (risposte multiple).

La presenza di reti locali wireless, più o meno integrate con il resto del sistema informatico ed accessibili dai dispositivi mobili, apre 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 piccolissima percentuale non ha LAN, ma solo PC autonomi, ciascuno che si collega ad Internet.

Un solo rispondente del campione ha indicato che il suo sistema informatico non è connesso ad Internet (forse per errore o per errata interpretazione della domanda, dato che il sistema informativo in oggetto non è piccolissimo), tutti gli altri sì, con uno o più collegamenti anche da fornitori diversi, come mostrato in fig. 17. La figura evidenzia come più della metà del campione utilizza diversi fornitori, tipicamente anche con tecniche diverse.

La fig. 18 evidenzia alcuni aspetti nell'uso delle connessioni a Internet, sia per la sicurezza sia per la multimedialità. Il confronto con gli analoghi valori del Rapporto 2011, che erano mediamente più alti, indica che l'attuale campione emerso di sistemi informativi è forse meno avanzato dal punto di vista strettamente tecnico rispetto al precedente, anche se, aumentando il numero di rispondenti, le

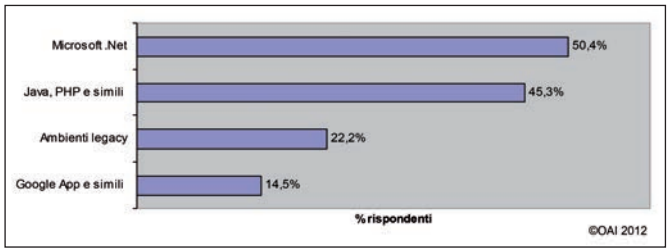

Fig. 14 - Principali ambienti e piattaforme architetturali in uso

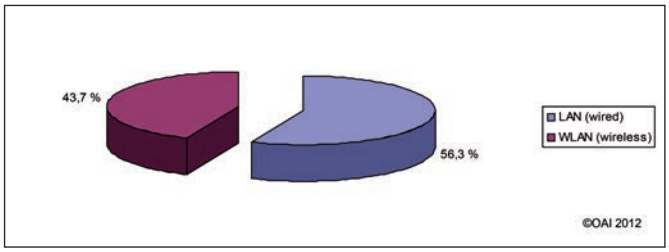

Fig. 16 - LAN e WLAN

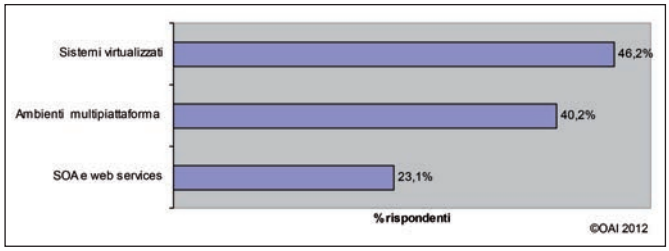

Fig. 15 - Logiche e tecnologie architetturali

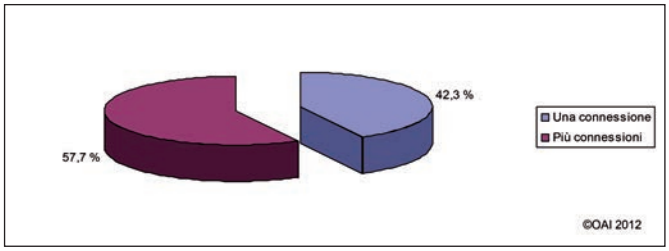

Fig. 17 - Connessioni ad Internet con uno o più fornitori

[5] Con il termine di "legacy", che significa "ereditato dal passato", si intende un sistema e/o un'applicazione esistente e funzionante da anni, tipicamente ormai obsoleto/a, ma che è ancora essenziale per il funzionamento dell'azienda/ente e che per motivi di costo e/o complessità e personalizzazione, non si è ancora ritenuto opportuno sostituire. È il caso di applicazioni di contabilità e finanza, oppure di gestione della produzione, della logistica, delle vendite non sostituiti da moderni pacchetti integrati ERP.

[6] Per approfondimenti si rimanda al volume di M. R. A. Bozzetti "SOA-Libro Bianco dell'evoluzione della Enterprise Architecture", pubblicato a dicembre 2009 da Soiel International (http://www.soiel.it/res/libro/id/2/p/manuale-soa)

medie percentuali si abbassano. La telefonia su Internet, VoIP (Voice over IP) è adottata da meno di un terzo del campione, mentre nell'edizione precedente era usata da circa la metà. Anche le tecniche di VPN, Virtual Private Network, e di SSL/TSL, Secure Socket Layer/Transport Layer Security[7] hanno percentuali complessive inferiori rispetto a quelle dell'edizione precedente. In entrambe le edizioni le risposte per queste domande erano multiple: il VPN è usato da poco più del 58%, mentre nell'edizione precedente si avvicinava al 70%. L'uso di HTTPS è usato da quasi il 42%, mentre nell'edizione precedente la percentuale era più del doppio.

Quest'ultimo dato richiede un commento: dato che le tecniche SSL/TLS sono usate anche in reti con VPN, il suo valore % avrebbe dovuto essere maggiore di quello 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 possibile uso di HTTPS per l'accesso ai loro siti web.

Le figg. 19 e 20 approfondiscono il tema della terziarizzazione e dell'uso del cloud computing, già emerso e commentato con le fig. 14 e 7. Tenendo presente che la domanda prevedeva la possibilità di risposte multiple, la prima figura mostra che poco meno di 1/5 dei rispondenti non terziarizza e quasi un 1/3 non usa soluzioni cloud, ma che poco meno della metà invece terziarizza in parte o in toto i suoi sistemi ICT: una conferma ai commenti della fig. 7 ed al profondo cambiamento avvenuto nelle aziende/enti italiani nei confronti della terziarizzazione dell'ICT. Il dato che più del 42% utilizza la terziarizzazione, che include anche i servizi cloud, deve essere confrontato, pur solo come indicatore dati i campioni diversi, con il 24,8% della precedente edizione ed il 14%. della prima edizione, e tenendo conto anche del fattore "riduzione" delle percentuali con il più ampio campione 2012. Questo incremento è un chiaro indicatore del cambio di mentalità e di percezione in Italia nel passare a forme di "sourcing", superando la "tradizionale" riluttanza, dovuta in precedenza soprattutto alla sicurezza e alla disponibilità, e favorita sicuramente dai problemi economici dovuti al perdurare della attaule crisi economica.

Per la parte delle aziende/enti che terziarizzano, la fig. 20, con risposte multiple, dettaglia alcuni dei servizi terziarizzati ed il tipo di servizi cloud in uso. Volutamente ai fini di OAI, le risposte previste nel questionario erano focalizzate sugli aspetti di gestione e sul cloud. Interessante rilevare che poco più del 11% ha terziarizzato la gestione della sicurezza dei sistemi informativi e poco più del 10% la gestione e/o la "governance" dell'intero sistema informativo. Per i servizi cloud, in linea con quanto indicano le varie ricerche di mercato e gli studi in Italia, le percentuali d'uso di IaaS e SaaS[8] sono vicine, e assai minore risulta l'uso di IaaS.

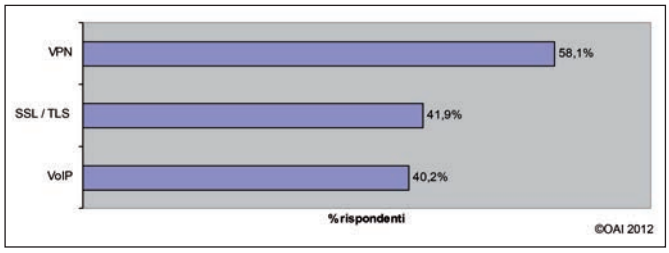

Fig. 18 - Utilizzo di VoIP, VPN, SSL/TLS

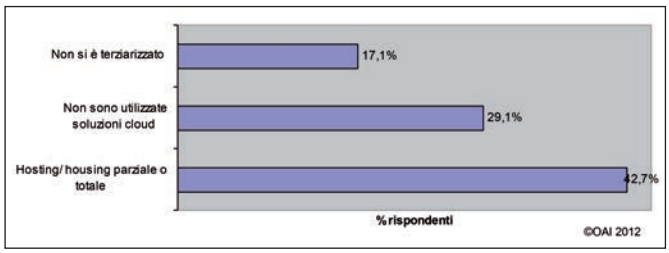

Fig. 19 - Uso della terziarizzazione e del cloud

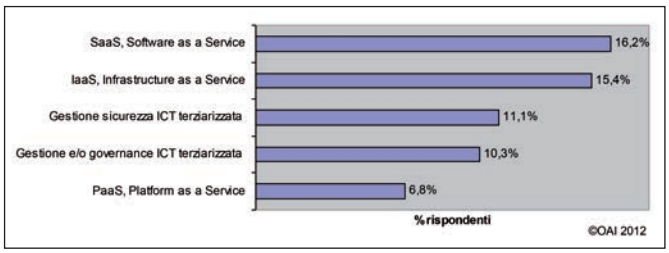

Fig. 20 - Uso di alcuni tipi di terziarizzazione e di cloud

[7] 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.

[8] Si veda anche la recente "Guida al cloud - Nella Nuvola la stella cometa per il Manager" di M.R.A. Bozzetti, pubblicata da Soiel per Seeweb a novembre 2012

Nell'ambito della sicurezza informatica, soprattutto dopo gli attacchi STUTEX ai sistemi di controllo delle centrali nucleari[9], hanno assunto particolare rilievo i sistemi di controllo dei processi produttivi, di robotica, ecc. Come nella precedente edizione, OAI ha posto alcune domande in merito a questi sistemi ICT. La fig.21 indica quante aziende dispongono di tali sistemi. Le percentuali sono simili rispetto all'edizione precedente: solo il 14,4% ne dispone, l'edizione precedente indicava il 13,4%. Anche su queste domande del questionario, come in precedenza sui sistemi mobili, 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, tipicamente il responsabile dei sistemi informativi o un suo dipendente dell'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 2012. Per la parte che ha e sa di avere, tali sistemi ICT di controllo, essi si basano prevalentemente su ambienti Microsoft Dot.Net, ma esistono anche ambienti Java o simili per il 40% ed "altro" per il 13,3%, costituiti da ambienti proprietari; anche questa domanda prevedeva risposte multiple.

Anticipando il capitolo §6 sugli strumenti di sicurezza in uso, come mostrato nella fig. 23, quasi il 38% di questi sistemi di controllo sono connessi via Intranet al sistema informativo, e quindi in qualche misura integrati con esso; i due mondi sono reciprocamente protetti da firewall ad hoc, ed un 17,4% sono gestiti da remoto via Internet, probabilmente tramite società terze. Il resto di questi sistemi opera isolatamente e non collegato con il sistema informativo dell'azienda.

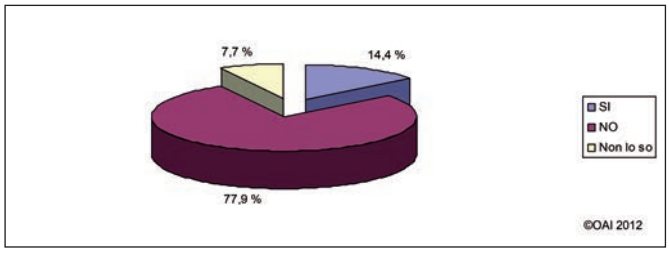

Fig. 21 - Sistemi ICT per controllo processi produzione e robotica

5. Attacchi informatici rilevati e la loro gestione

La fig. 24 rappresenta la sintesi dei diversi Rapporti OAI dal 2007 al 2012-primo quadrimestre in termini di attacchi subiti in percentuale sui campioni di rispondenti emersi con le varie edizioni OAI: i campioni sono diversi come mix e come numero ma, per i motivi illustrati in §1.1, sono confrontabili almeno a livello indicativo. Il grafico mostra come dal 2009 sia cresciuto in percentuale il numero di aziende/enti che hanno subito attacchi: la % del "Mai" decresce", ed anche il 1° quadrimestre

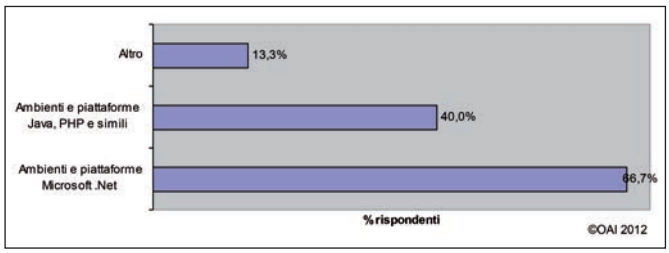

Fig. 22 - Piattaforme riferimento ambienti ICT per controllo processi industriali, robotica, ...

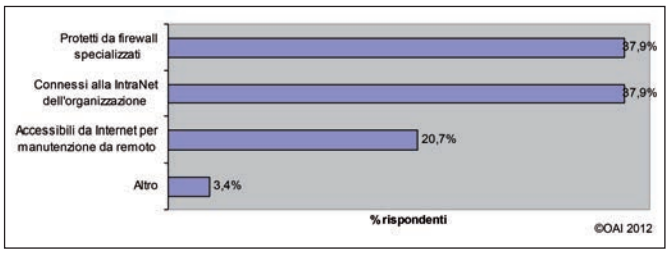

Fig. 23 - Connessione dei sistemi di controllo al sistema informativo

[9] Per approfondimenti si veda l'articolo dell'Autore "Attacchi ai sistemi di controllo industriale e alle infrastrutture" su Office Automation n. 11 novembre 2010, p. 88-89, e scaricabile da http://www.malaboadvisoring.it/index.php?option=com_content&view=article&id=31&Itemid=50

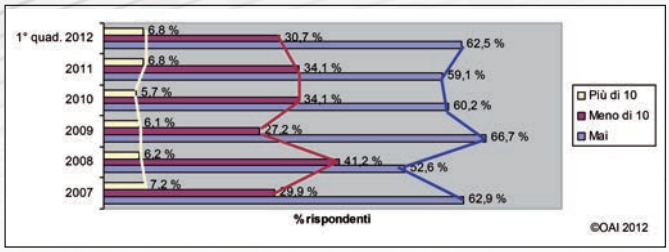

Fig. 24 - Attacchi complessivi rilevati dal 2007

2012 vede percentuali preoccupanti, e pur considerando il fattore "riduttivo" delle percentuali dovuto al maggior numero di rispondenti della presenta edizione rispetto alle precedenti. Dopo il "buco nero" del 2008, considerato l'"annus horribilis" per la quantità di attacchi occorsi, si vede un netto miglioramento nel 2009, sicuramente a fronte della risposta data in termini di interventi sugli strumenti di prevenzione e protezione, oltre che di gestione della sicurezza ICT. Ma nell'eterno gioco di guardie e ladri, dal 2010 è ripreso l'aumento di attacchi. Come numero di attacchi rilevati, la fascia di "Meno di 10" è nella media esatta di 1/3 del campione tra il 2007 ed il 2011, ma si è stabilizzata nel 2010-11 a più di un punto %, ed il valore di 30,7% nel solo 1° quadrimestre per il 2012 tendenzialmente indica un ulteriore significativo incremento per l'anno in corso. Nella fascia di "Più di 10" attacchi nell'anno, la % in media è del 6,4% del campione, ma nel 2011 è andata leggermente aumentando: ed analogamente la percentuale emersa per il 2012 è preoccupante.

Facendo riferimento alle principali tipologie di attacco elencate nella Tabella1 e subite dai sistemi informativi del campione 2012, la fig. 25 mostra che:

- al primo posto permane il "malware" che nel 2011 ha coinvolto il 68,9% dei rispondenti:
- al secondo posto nel 2010 si è posizionata la "saturazione di risorse" (DoS/DDoS), passata al terzo posto nel 2011 e preceduta dal "social engineering" che include il "phishing";
- al quarto posto si posiziona, sia per il 2010 che per il 2011, il "furto di dispositivi ICT".

Tutti gli altri tipi di attacchi si attestano tra il 12% ed il 25% dei componenti del campione.

Importante sottolineare come tutte le % per tipo di attacco subito nel 2011 sono aumentate rispetto al 2010, a parte "l'accesso a e uso non autorizzato degli elaboratori, delle applicazioni supportate e delle relative informazioni", come evidenziato nella fig. 25 dalla linea del 2011 che è sempre al di sopra di quella del 2010, a parte il tipo d'attacco sopra menzionato.

Nonostante l'uso diffuso di antivirus e antispyware sia a livello di posti di lavoro che di server, i "**malware**", o **codici maligni**, rimangono l'attacco più diffuso.

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 nuovo libro di prossima pubblicazione "Sicurezza digitale".

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 in forte crescita, come evidenziato in fig. 25, dal 19,8% al 23,5% nel 2011, e che lo pone in settima 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 2011 e maggiormente dettagliate in rapporti specializzati come quelli di IBM X-Force[10] e di Trend Micro[11], oltre che negli articoli in italiano della Rubrica OAI mensile nella rivista Office Automation[12]:

- la maggior parte delle vulnerabilità possono essere sfruttate da remoto via rete;

[10] Si veda http://www-03.ibm.com/security/xforce/
[11] Si veda in particolare http://www.trendmicro.com/us/security-intelligence/current-threat-activity/index.html
[12] 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

- i tempi per la correzione delle vulnerabilità dei programmi software da parte dei fornitori sono talvolta lunghi e possono superare un intero anno;
- le maggiori vulnerabilità, sia in numero che in gravità, riguardano principalmente le piattaforme web e le applicazioni web personalizzate, oltre a 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 XSS (cross-site scripting), per i 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 "mobile";
- le maggiori vulnerabilità per i PC sono nei browser, nelle applicazioni multimediali come Flash e nei lettori (gratuiti) dei principali formati testuali, come Acrobat Reader per i formati .pdf;
- richiedono particolare attenzione le vulnerabilità dei sistemi VoIP e wireless;
- il software di base e delle "app" dei dispositivi mobili smartphone e tablet, essendo relativamente recenti ed in continua evoluzione sotto la spinta della forte concorrenza tra Android e Apple iOS, presentano vulnerabilità sfruttate da molti attacchi, che ultimamente si concentrano proprio in questo settore.

Il fronte dei sistemi mobili, e di conseguenza delle reti wireless, è la nuova frontiera degli attacchi, soprattutto come punto di accesso ai sistemi informativi, superato il quale si possono portare ulteriori attacchi e di tipo diverso ai sistemi target. Gli **attacchi alle reti** sono aumentati, sempre come % del campione che li ha subiti, dal 12,3% nel 2010 al 16% nel 2011, e con un preoccupante 18,5% nel 1° quadrimestre 2012.

Il fenomeno degli attacchi ai sistemi mobili ha portato alla specifica domanda nel Questionario 2012, non presente nei precedenti, sul "furto di informazioni e loro uso illegale da **dispositivi mobili**", che si affianca all'analoga sui **posti di lavoro fissi**: La percentuale di **furti di informazione** occorsi dai dispositivi mobili passa dal 12,3% nel 2011 al 14,8% nel 2011, mentre per i fissi dall'8,6% al 13,6%. È da sottolineare l'incremento ben più forte sui fissi, dovuto anche alla facilità di estrarre dati tramite le chiavette USB e gli hard disk mobili con interfaccia USB.

Tra furti di informazione quello più significativo e diffuso è il **furto dell'identità digitale**, che include i vari account per l'accesso a servizi, da quelli bancari a quelli telefonici, dai mercati digitali fino ai social network.

Molto interessanti i dati in merito al furto dell'identità digitale raccolti dalla Polizia Postale e delle Comunicazioni[13]. La fig. 25-1 mostra il forte incremento di tali furti dal 2010 al 2011, e tendenzialmente l'ulteriore incremento nel 2012. Per l'anno 2011 la fig. 25-2 dettaglia la suddivisione percentuale per tipi di codici identificativi rubati e conferma che la stragrande maggioranza di identità digitali rubate riguarda quelle per il commercio elettronico, seguite da quelle di home banking.

Il furto di informazioni sui dispositivi mobili è da correlare anche con il furto dei dispositivi ICT, al 4° posto nella

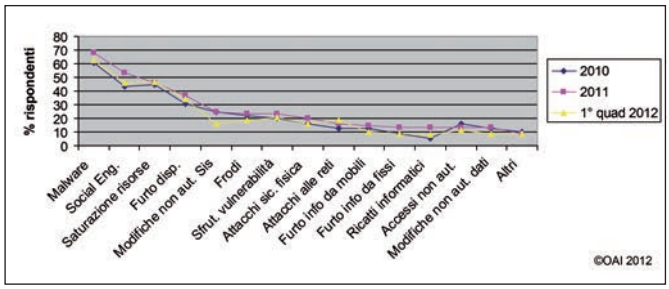

Fig. 25 - Principali attacchi subiti dal 2010

Fig. 25-1 - Furto di identità: numero di casi in Italia

[13] Dati presentati da Antonio Apruzzese, Direttore del Servizio Polizia Postale e delle Comunicazioni al Convegno AIPSHSSA del 18/10/2012 a Roma

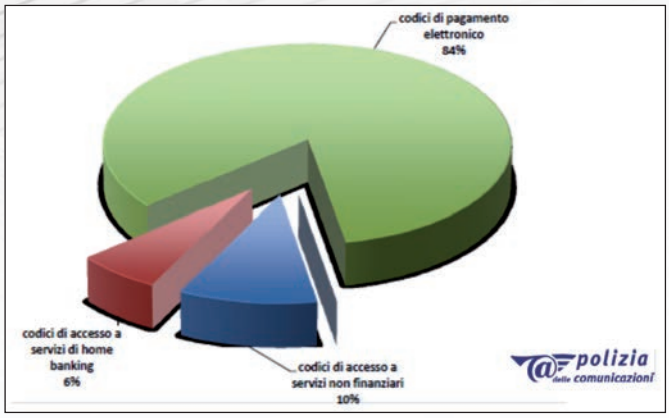

Fig. 25-2 - Furto di identità: ripartizione nel 2011 per tipi di codice

classifica degli attacchi più diffusi nel 2010 e nel 2011. L'esplosione della diffusione di tablet e di smartphone ha ampliato il bacino dei potenziali oggetti da rubare, più per venderli sul mercato "nero" che per rubare le informazioni in essi contenuti.

I **furti di dispositivi ICT** 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 ai mouse o alle stesse tastiere, i lap top, gli hard disk, ecc.

Nel 2011 al 2° posto negli attacchi si posiziona il "social engineering" con un 53%, aumentato di ben 10 punti percentuali rispetto al 2010, dove era al terzo posto preceduto dalla saturazione di risorse al 44,4%. Il "**social engineering**" è alla base dei principali attacchi, anche complessi, avvenuti nell'ultimo triennio, 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 5° posto l'"accesso a e uso non autorizzato degli elaboratori, delle applicazioni supportate e delle relative informazioni", con un 24,7% del campione sia nel 2010 che nel 2011. **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", soprattutto con 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 servizi.

La frode informatica si posiziona al 6° posto della classifica degli attacchi, con un 22,2% del campione nel 2010 che cresce al 23,5% nel 2011. 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.

Contiguo alla frode il **ricatto informatico**, sulla continuità operativa e sull'integrità dei dati: posizionato nel 2010 in fondo alla classifica degli attacchi con un 5,4%, nel 2011 ha un balzo al 13,6%, quindi quasi triplicando la copertura del campione. Un trend anticipato nei precedenti Rapporti ed approfondito nella già citata Rubrica OAI; questa forma di "pizzo informatico" è infatti molto più semplice da attuare, e può coinvolgere l'ampio bacino delle piccole e piccolissime imprese, gli studi professionali, i negozi.

La maggior parte degli attacchi informatici ha oggi come obiettivo un illegale ritorno economico, ma le frodi e i ricatti informatici non risultano ai primi posti. Varie le possibili spiegazioni, anche complementari: bassa percentuale di istituti finanziari nel campione, non conoscenza o non volontà di dichiarare l'occorrenza di una frode informatica, dato che in Italia le frodi sono orientate per ora prevalentemente alle persone fisiche.

Tutti gli altri nove tipi di attacchi, sul totale di 15, hanno percentuali inferiori al 20%, e molti attorno o sotto il 10%.

Il Questionario 2012, così come quelli delle precedenti edizioni, ha posto la voce "**Altri**" e la possibilità di specificare quale tipo di attacco, non includibile nella tipologia elencata, era stato subito: pur con percentuali non trascurabili, dal 10% nel 2010 al 9% nel 2011, non è stato specificato alcun tipo diverso da quelli previsti. Probabilmente rientrano in questi altri attacchi multipli tipo APT.

La fig. 26 pone a confronto le percentuali di attacchi subiti dal 2008, pur con le considerazioni già espresse sui campioni diversi nelle tre 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 sempre alte, dal 31% al 53%;
- frodi e ricatti informatici vanno aumentando, così come tutti gli altri tipi di attacco vanno aumentando in percentuale dal 2009.

Rispetto alle edizioni precedenti, il Questionario 2012 ha aggiunto alle domande sugli attacchi subiti, per ogni tipo di attacco, se questi hanno avuto impatti poco o molto significativi. Per non appesantire la lunghezza del 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 sull'impatto avuto dagli attacchi subiti, posto a 100 il numero complessivo di attacchi subiti per anno, è sintetizzato nella fig. 27.

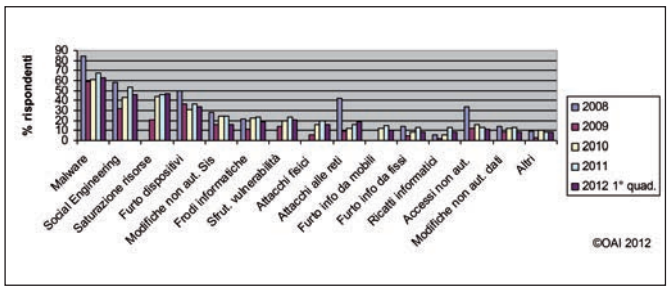

Fig. 26 - Confronto principali attacchi subiti dal 2008

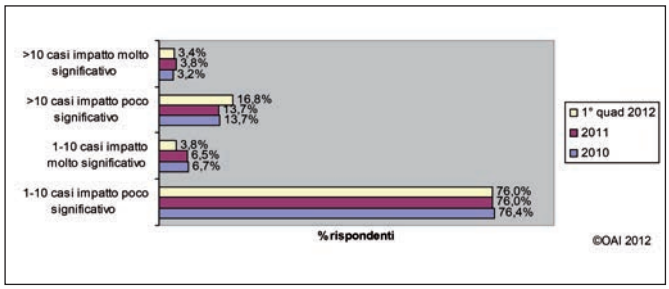

Fig. 27 - Impatto dell'attacco

La maggior parte degli attacchi nel complesso sono occorsi fino a dieci volte per anno con impatti poco significativi, con un trend praticamente stabile tra 2010 e 2011. Più di 10 attacchi con impatti poco significativi hanno analogamente un trend stabile tra 2010 e 2011, ma con un preoccupante incremento al 16,8% nel 1° quadrimestre 2012.

È significativo che alcuni compilatori abbiano risposto che taluni attacchi hanno comportato **forti impatti**, e con una percentuale non trascurabile fino a 10 casi, dal 6,7% al 6,5% nei due anni. Per più di 10 casi la percentuale si riduce di circa la metà.

Analizzando in dettaglio i questionari con l'indicazione di "impatto molto significativo" emerge che tali attacchi riguardano varie tipologie: furti di dispositivi ICT, attacchi fisici, accessi non autorizzati, modifiche non autorizzate dei sistemi e dei dati, "social engineering", codici maligni, utilizzo vulnerabilità (exploit), saturazione risorse, e sono occorsi ad aziende/enti dei settori merceologici Industria, PAC, Sanità, Servizi, TLC & Media, Utility.

Sempre in termini di impatto, una specifica domanda del Questionario 2012 chiedeva la stima del danno economico, cui pochi però hanno risposto. Le poche indicazioni avute variano da € 1.000 a € 60.000 per attacco. In Italia sono pochi i riferimenti al riguardo: una recente analisi[14] ha accertato un costo di € 200.000.000 per le 14.000 intrusioni riscontrate nei primi mesi del 2011, con una media di circa € 14.286 per attacco, e stima nel 2013 un costo complessivo in Italia nell'ordine dei 450-600 milioni di euro.

Sulla valutazione dei danni subiti e sui criteri della loro valutazione si veda il prossimo capitolo.

5.1 Rivelazione, 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

[14] Dati presentati da Antonio Apruzzese, Direttore del Servizio Polizia Postale e delle Comunicazioni al Convegno AIPSHSSA del 18/10/2012 a Roma

un attacco (risposte multiple): le segnalazioni arrivano prevalentemente 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 la constatazione diretta del danno subito (ad esempio il blocco di un sistema, una elaborazione scorretta, ecc.) e le segnalazioni da colleghi. Per finire, ma in percentuale molto minore, le segnalazioni provengono dagli utenti esterni, da clienti e fornitori che si accorgono di malfunzionamenti, furti o di dati scorretti.

Sulla valutazione dei danni subiti, economica e non, la fig. 29 mostra che la maggior parte del campione non effettua alcuna valutazione: solo poco più del 18% ha risposto affermativamente, ed alcuni di questi hanno indicato le stime dei costi per attacco sopra riportate.

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 il criterio più importante è la continuità operativa, cui seguono i costi dovuti all'indisponibilità dei servizi ICT e ai costi diretti subiti con l'attacco. Tali criteri sono identici a quelli rilevati con il precedente rapporto. Seguono il danno di immagine ed i costi derivanti dalla non conformità alle leggi vigenti (compliance). Solo una piccola percentuale di piccole imprese non ha criteri di valutazione.

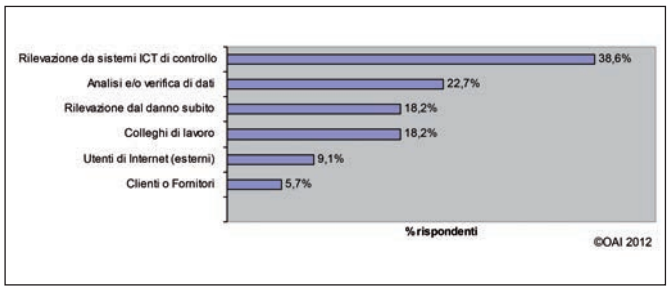

Fig. 28 - Da chi sono pervenute le segnalazioni di attacco

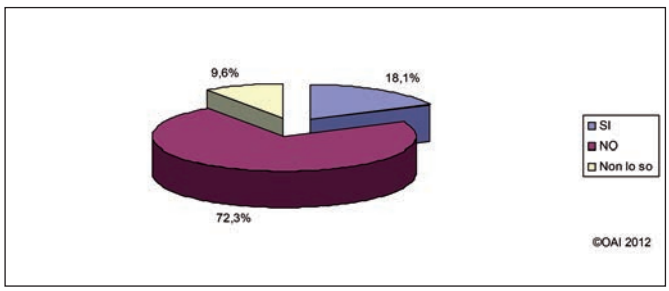

Fig. 29 - Valutazione del danno subito

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 essi 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 dal 60% circa che indicano i costi di indisponibilità dell'ICT come il secondo indicatore di gravità. Tra i criteri indicati nel questionario, è significativo che il 37,5% preveda come ulteriore criterio di valutazione la "compliance" alle normative in vigore: una percentuale in leggera diminuzione rispetto al 41% del precedete rapporto, ma superiore al 30% del primo. L'effetto privacy si fa sentire, ma è ora forse meno percepito dalle piccole imprese con le recenti normative di semplificazione e di non necessità 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), più di 1/3 dei rispondenti che hanno subito attacchi non comunica l'avvenuto attacco, e circa 1/4 lo comunica ai propri Fornitori affinché intervengano. Quasi il 17% avvisa le competenti autorità (in pratica la Polizia Postale e delle Comunicazioni[15]), la metà di questi informa centri specializzati quali il CERT[16]

[15] Si veda http://www.poliziadistato.it/articolo/982/

[16] 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

e solo una piccola percentuale informa l'assicurazione con la quale ha stipulato un contratto. Questa bassa % conferma che poche aziende/enti sono assicurati contri i rischi informatici, data anche la complessità e la spesa di tali polizze. Questi dati sono assai migliorativi rispetto a quelli rilevati nella precedente edizione, dove la quasi totalità dei rispondenti, il 97,5%, non comunicava affatto.
In termini di contrasto alla criminalità informatica da parte della Polizia Postale e delle Comunicazioni[17], la fig. 31-1 mostra il forte incremento di denunciati per furto di identità digitale, e la fig. 31-2 il numero di arresti conseguenti dal 2009 ai primi 7 mesi del 2012.
Il picco di arresti nel 2009 deriva probabilmente dall'anno nero 2008, nel 2009 e nel 2010 si sono di poco ridotti, per poi aumentare nel 2011 ed ancor più nel 2012.
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 tutelare l'immagine.
La fig. 33 fornisce un'indicazione di quali azioni sono state intraprese a seguito di un attacco. Le risposte possibili erano multiple, dato che sono multiple le azioni da

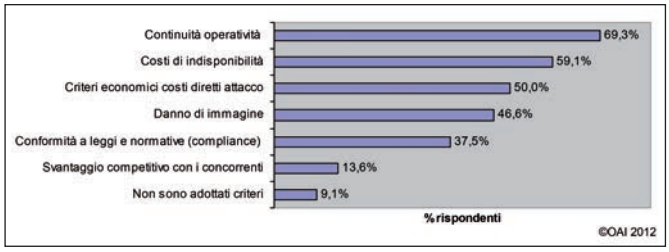

Fig. 30 - Criteri di valutazione della gravità dell'attacco

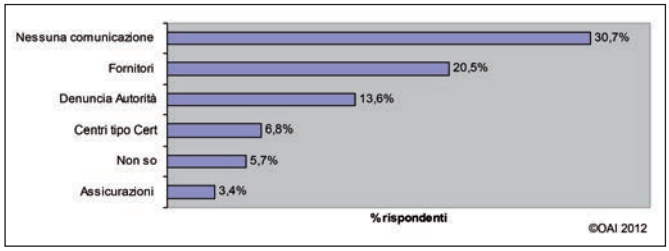

Fig. 31 - Comunicazione all'esterno dell'avvenuto attacco

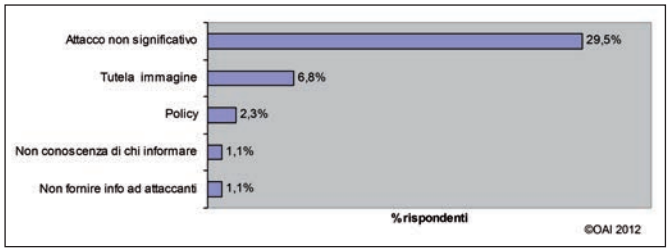

Fig. 32 - Motivazioni per la "non comunicazione" all'esterno dell'attacco

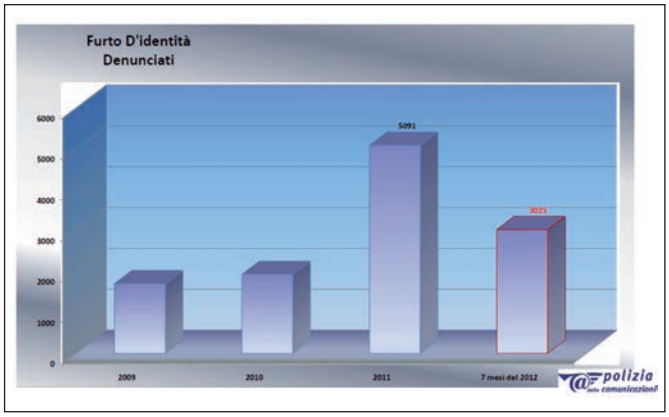

Fig. 31-1 - Numero di denunciati per furto di identità

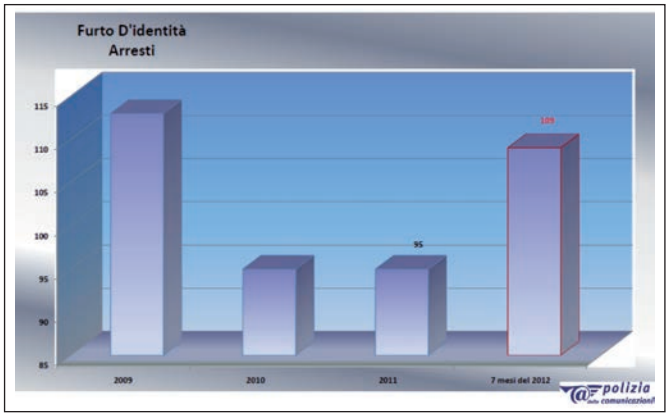

Fig. 31-2 - Numero di arresti per furto di identità

[17] Dati presentati da Antonio Apruzzese, Direttore del Servizio Polizia Postale e delle Comunicazioni al Convegno AIPSHSSA del 18/10/2012 a Roma

intraprendere sia a livello tecnico che organizzativo ed eventualmente legale. Il campione 2012 per poco più del 40% attiva le ultime patch sul software, e per 1/3 attiva delle indagini interne; con percentuali superiori al 30% elimina i sistemi attaccati o a rischio (spesso sono molto obsoleti, soprattutto come software di base), installa ed attiva nuovi strumenti di sicurezza e aggiorna le policy e le procedure organizzative inerenti la sicurezza informatica. Con percentuali decrescenti fa partecipare gli utenti finali (e gli operatori) a corsi di sensibilizzazione, formazione e addestramento, fino all'intervento di legali e/o di esperti esterni. Alla voce "altro" sono indicati interventi quali la riconfigurazione dei sistemi, la riformattazione di dischi, l'attivazione dei piani di Disaster Recovery e di continuità operativa.

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 il 90% dei casi la situazione è ripristinata **entro 3 giorni dall'attacco**. Questi dati sono molto migliori di quelli rilevati nelle precedenti edizioni. 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 più efficaci (si veda anche §6), dall'altro che la stragrande maggioranza degli attacchi, almeno per il campione emerso, non ha serie conseguenze, come d'altro canto emerso nella fig. 27. Gli attacchi veramente penetranti ed impattanti, pur se pochi, hanno serie conseguenze ed il ripristino richiede ben più di una settimana.

L'ordine di grandezza dei tempi "medi" è confermata anche dai tempi "massimi" occorsi nei casi peggiori di ripristino, illustrati nella fig. 35. I due casi segnalati con il questionario, che hanno richiesto più di una settimana per il ripristino, riguardano:

- ripristino integrale dei dati di una NAS, Network Attached Storage, a seguito di cancellazione volontaria e deliberata dei dischi con blocco delle procedure di salvataggio;
- intrusione nei server come amministratore di sistema, con blocco salvataggi e cancellazione dell'ambiente di produzione oltre che dei dati sui sistemi di storage (raid) e di "mirroring".

Sono tipici casi di intrusione come amministratore, che ha cancellato tutto o parte dell'ambiente di produzione, partendo dai dati sui sistemi di "storage". Il numero di rispondenti per queste domande sui tempi di ripristino è stato inferiore rispetto alla media di risposte dell'intero questionario, ma molto superiore rispetto alla precedente edizione, probabilmente anche perché nessuno registra o prende nota dei tempi, anche approssimativi e qualitativi di ripristino, e/o perché gli attacchi subiti non hanno comportato modifiche al software ed alla sua configurazione.

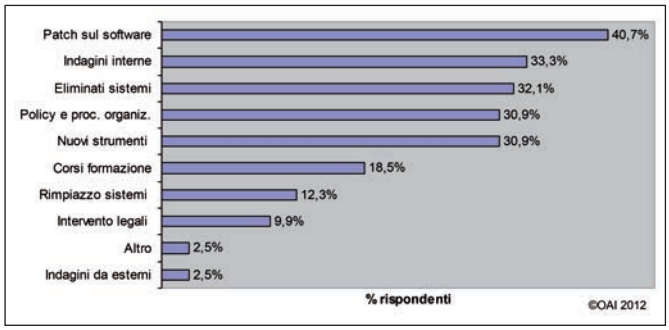

Fig. 33 - Azioni (multiple) dopo un attacco

6. Strumenti e politiche di sicurezza ICT adottate

Il presente capitolo sugli strumenti di prevenzione e protezione considera sia gli aspetti tecnici che quelli orga-

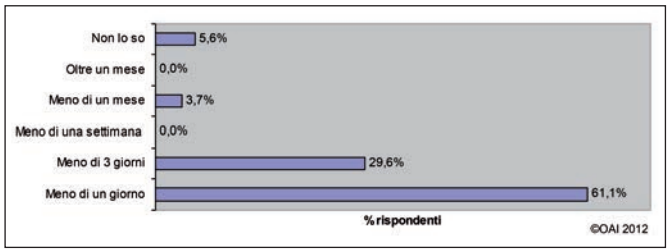

Fig. 34 - Tempi medi di ripristino

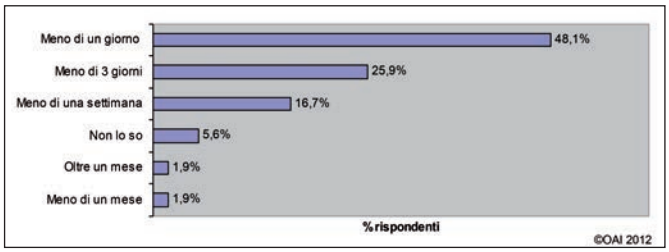

Fig. 35 - Tempi massimi di ripristino (caso peggiore)

nizzativi, 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, con risposte multiple: le percentuali sono buone per tutte e tre le macro aree considerate. Più dell' 80% dei rispondenti è dotato di sistemi per garantire la continuità elettrica (erano al 90% nella precedente edizione), il 70% circa dispone di protezioni perimetrali ed effettua controlli degli accessi alle persone fisiche (erano l'84% nell'edizione 2011) e quasi il 68% ha i locali del Data Center (o della computer room) climatizzati e/o con rilevatori di fumo, gasa, umidità, ecc. (erano più del 75% nella precedente edizione). Tali percentuali confermano che il pur variegato campione di rispondenti appartiene alla fascia medio-alta in termini di sicurezza informatica, ma forse un poco inferiore rispetto al campione 2011.

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 multiple, la grande maggioranza dei rispondenti è dotato di dispositivi firewall e di DMZ, DeMilitarized Zone, e più della metà è dotato di soluzioni ridondate sia a livello di collegamenti-reti, sia a livello di sistemi critici: architetture ad alta affidabilità con "mirroring", "clustering", ecc. Per proteggere le comunicazioni da remoto, il 71,6% dichiara di utilizzare soluzioni VPN, Virtual Private Network. Significativo che quasi il 47% abbia potenziato il livello di sicurezza delle reti wireless, che costituiscono una parte crescente delle tecniche di comunicazione, integrate funzionalmente nella rete complessiva del sistema informatico, e che possono presentare forti vulnerabilità se non correttamente protette. Solo una piccola percentuale, ma non trascurabile, non è al momento dotata di alcuna specifica protezione per le reti: è il caso tipicamente per piccoli e piccolissimi sistemi informativi.

Come percentuale l'attuale quadro è di circa 10 punti inferiore rispetto al campione dell'edizione precedente, a parte il rafforzamento delle reti wireless che ha % quasi uguali.

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 come i precedenti è simile a quello dell'edizione passata, ma con qualche punto percentuale in meno; con l'allargarsi della base di rispondenti si appiattisce leggermente la valenza tecnica-organizzativa complessiva, causa anche la maggioranza di organizzazioni di piccole dimensioni (il 43,6% con meno di 10 dipendenti, si rimanda alla fig. 3).

I software antivirus e antispyware sono usati dalla maggior parte dei rispondenti, l'80,2%, rispetto al 97% ed al 95% delle scorse edizioni dell'OAI: significa che quasi di

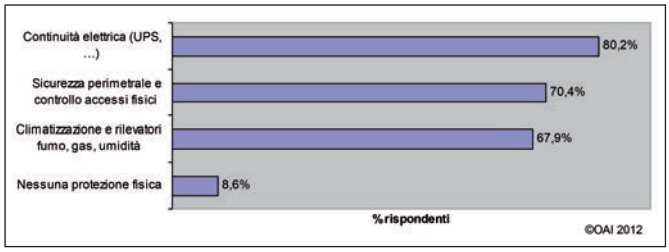

Fig. 36 - Strumenti sicurezza "fisica" in uso

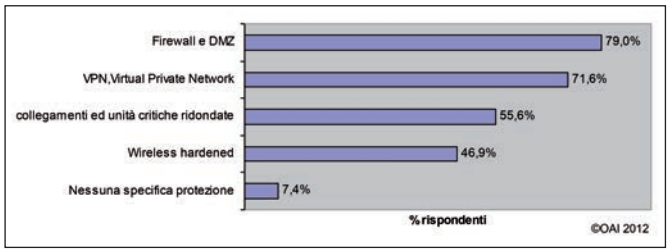

Fig. 37 - Strumenti sicurezza logica in uso per le reti

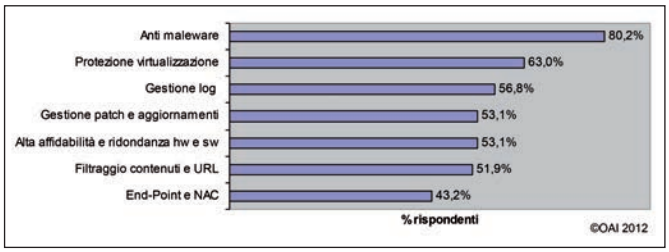

Fig. 38 - Strumenti sicurezza logica in uso per i sistemi

1/5 dei rispondenti non usa (o non sa che vengono usati) programmi anti-malware sui server. Al riguardo si deve tener conto che una scuola di pensiero dei sistemisti Linux/Unix non ritiene necessario l'attivazione di programmi antivirus sui server.
Al contrario è significativo che il 63% usi strumenti di protezione nell'ambito della virtualizzazione dei server, e che il 53,1% (contro il 70% ed il 47% scorsi) dichiari di usare sistemi ad alta affidabilità, una percentuale analoga alla ben più tradizionale ed operativa gestione delle patch e degli aggiornamenti, che risulta, a giudizio personale dell'Autore, piuttosto bassa: ma lo era anche nei precedenti rapporti, rispetto agli altri strumenti più complessi e sofisticati. La gestione dei log, con un 56,8% è più alta, e questo deriva anche dall'obbligo di essere conformi alla normativa sugli amministratori di sistema per la privacy. Seguono a breve distanza il filtraggio dei contenuti e delle URL, tipiche attività dei moderni firewall, e gli strumenti (tipicamente software) di sicurezza End-Point ed i NAC, Network Access Control. Questi ultimi arrivano al 43,2% rispetto al precedente 37%, ed è un indicatore della aumentata attenzione a controllare "prima dell'accesso" l'identità dell'utente e quanto sia sicuro il posto di lavoro 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 di controllo degli accessi logici. Il mezzo più diffuso è il consueto uso di un identificatore e di una password per l'identificazione digitale dell'utente del sistema informativo, associato a strumenti di controllo degli accessi e di profilazione dei diritti sugli applicativi: strumenti che vanno dall' Active Directory di Microsoft, all'analogo LDAP usato prevalentemente negli ambienti Linux/Unix, alle ACL, Access Control List, ai Policy Server, e così via. Grazie anche alla spinta delle Pubbliche Amministrazioni ed alle CRS, Carte Regionali dei Servizi, i certificati digitali raggiungono il 3° posto, usati da 1/3 dei sistemi informativi del campione: nella precedente edizioni erano al 5° posto, con un 21,8%. In tale logica, e soprattutto nell'ambito di grandi sistemi, cresce anche la presenza di piattaforme PKI, Public Key Infrastructure, usate dal 28,4% del campione. 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 non trascurabili, da circa il 20% al 26%. L'identificazione biometrica, pur con una percentuale sul campione di solo il 6,2%, incomincia a diffondersi (era al 2,52% nella scorsa edizione), sia grazie alla sua maggior affidabilità, sia ai costi calanti, sia, a parere dell'Autore, al suo uso nell'ambito della grafometria per 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 (le risposte erano multiple) per più della metà dei rispondenti sono i firewall ed i reverse proxy prima dei server applicativi e dei data base, che ulteriormente controllano i diritti di accesso e filtrano i contenuti.
Per garantire la sicurezza delle applicazioni, queste devono essere sviluppate in modo "intrinsecamente" sicuro, in funzione dei linguaggi e delle piattaforme di sviluppo ed applicative usate: una considerevole parte del campione, il 44,4% dichiara di avere definito e/o di seguire e far seguire apposite linee guida, e più di 1/4 verifica, anche a livello contrattuale, che gli sviluppatori terzi seguano tali linee guida. Una quota leggermente inferiore, il 22,2%, ef-

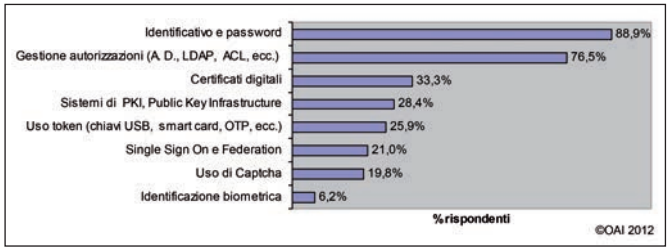

Fig. 39 - Strumenti in uso per l'identificazione, l'autenticazione e l'autorizzazione

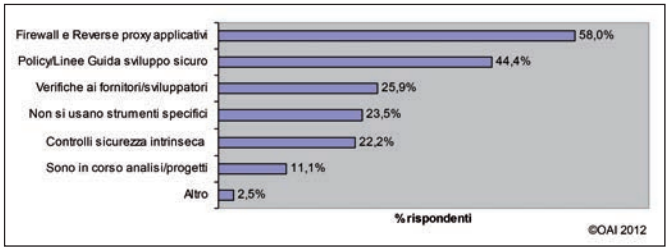

Fig. 40 - Strumenti in uso per la sicurezza logica degli applicativi

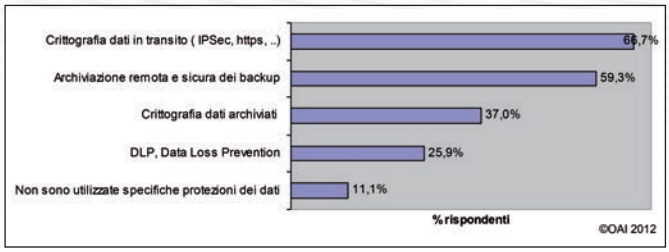

Fig. 41 - Strumenti in uso per la sicurezza logica delle informazioni

fettua inoltre ispezioni sul codice (code inspection) e test di penetrazione per verificare la mancanza di vulnerabilità e di bachi prima della messa in produzione degli applicativi e di loro aggiornamenti. Questi dati evidenziano come più della metà dei rispondenti abbiano preso coscienza delle possibili gravi vulnerabilità degli applicativi ed effettuino opportuni controlli. controlli. Il 23,5%, quota comunque non trascurabile, non ha ancora alcun strumento di controllo a livello applicativo, e l'11,1% ha in corso studi di fattibilità e/o progetti per introdurre questi tipi di strumenti.
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 66,7%, utilizza la crittografia nella trasmissione dei dati in rete, tipicamente nelle transazioni via web con HTTPS: dato molto simile al 67% della precedente edizione, che lo poneva però al secondo posto, preceduto dall'archiviazione sicura dei back-up, allora al primo posto con un 78,2%. Questo è un indice della diffusione dei protocolli sicuri HTTPS e FTPS, disponibili praticamente in tutti i browser ed usati per transazioni commerciali e bancarie via Internet. L'attuale rilevazione porta al secondo posto, con quasi il 60%, le soluzioni di archiviazione remota, tipicamente con ISP/ASP e fornitori cloud; tali dati sono talvolta crittati, per salvaguardarli ulteriormente. La tendenza è di replicare in remoto tutti i dati, o quelli più critici, anche grazie ai prezzi interessanti dell'IaaS.
Più di 1/3 critta anche localmente i dati archiviati , e più di 1/4 utilizza tecniche e strumenti di DLP, Data Loss Prevention. Il 25% dei rispondenti utilizza la crittografia per proteggere i dati archiviati, rispetto al 23% precedente.

6.3 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: i dati raccolti indicano un buon livello su questo tema essenziale per garantire un livello realmente idoneo di protezione al sistema informativo.
Il monitoraggio e il controllo delle funzionalità e prestazioni dei sistemi ICT è in vari modi attuata da più dell'80% dei rispondenti (rispetto al precedente 79,8%), ma solo il 14,8% (in precedenza il 16%) utilizza un SGSI, Sistema Gestione Sicurezza Informatica, integrato e centralizzato, ed il 9,9% (in precedenza l'8%) fa uso di un SCC, Security Command Center, presso società specializzate.
Il forte divario tra l'80% ed il 14,8% riconferma l'osservazione riportata già dall'edizione precedente: la gestione della sicurezza è ancora gestita prevalentemente a isole, a silos verticali e separati per i diversi ambienti quali Microsoft, Linux/Unix, Data Base, siti web, ecc. In molti casi, soprattuitto nei sistemi informativi di piccole e medie dimensioni, la gestione è effettuata server per server a livello di consolle di sistema operativo.
Importante evidenziare come correttamente quasi la metà dei rispondenti gestisce i log degli operatori e degli amministratori di sistema, anche grazie alle normative per la privacy, mentre i log degli utenti scendono al 6° posto nel grafico, ma con un apprezzabile 40%. Alta la diffusione di sistemi per l' individuazione delle intrusioni, chiamati IDS, Intrusion Detection System, e di sistemi di prevenzione delle intrusioni, chiamati IPS, Intrusion Prevention Systems. Alta anche la quota di chi gestisce le vulnerabilità (vulnerability assessment) ed effettua scansioni della rete e dei sistemi per un continuo miglioramento e rafforzamento delle difese (hardening).
Scendono le quote, ma con valori non trascurabili, da 1/3 ad 1/4 del campione, relative ai test periodici e

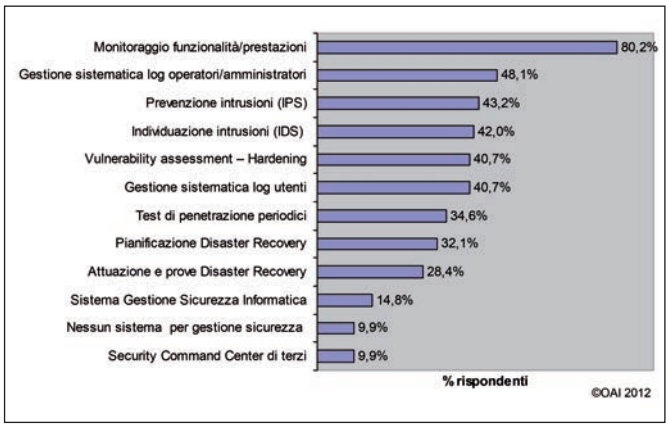

Fig. 42 - Strumenti in uso per la gestione della sicurezza ICT

sistematici di penetrazione per verificare l'effettiva tenuta delle misure di sicurezza in essere, e relative ai piani e alle soluzioni di Disaster Recovery, oltre che all'effettuazione periodica di prove di ripristino emulando situazioni di disastro. Solo poco meno del 10% dichiara di non avere e/o usare strumenti di gestione della sicurezza informatica.
Un aspetto importante e propedeutico nella gestione della sicurezza ICT è la sistematica e periodica analisi dei rischi. Come evidenziato nella fig. 43, solo il 23,9% del campione (contro ben il 67% scorso) afferma che tale analisi viene effettuata, ed il 12,5% ammette di non saperlo. Questa rilevazione è peggiorativa rispetto a quella del precedente rapporto, ed è confermata dalla successiva fig. 44, che evidenzia come solo un'analoga percentuale abbia forme di assicurazione del rischio residuo dopo gli attacchi, avendo effettuato quanto richiesto dall'assicurazione per limitarli opportunamente.

6.4 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 strutture.
Quanto emerge dalla risposte conferma che le aziende/enti del campione, pur diversificato, rappresentano anche in questa edizione, come nella precedente, 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 è in generale abbastanza positivo, anche se con quote percentuali inferiori di 20 punti rispetto all'edizione precedente, riconfermando ulteriormente l'abbassarsi del livello con l'ampliamento del campione: quasi il 62% (rispetto al precedente 76%) ha definito ed utilizza **policy tecnico-organizzative** di sicurezza, e con percentuali superiori al 35%, quindi più di 1/3 del campione, ha specifiche procedure per governare la gestione della sicurezza e dell'help desk; si è vicini al 30% nella gestione strutturata degli incidenti e dei problemi, oltre che nella definizione dei ruoli e dei compiti delle varie figure addette alla sicurezza, tenendo conto della necessità di ben separare le singole responsabilità, indicata spesso con l'acronimo dall'inglese SoD, Separation of Duties. Ancora una buona quota percentuale adotta strumenti informatici di supporto e di ausilio ai processi per la gestione della sicurezza informatica, tipicamente work-flow, banche dati di supporto all'help-desk, trouble ticketing, ecc. A scalare,

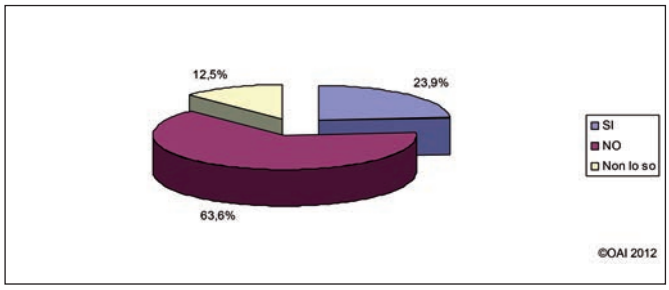

Fig. 43 - Effettuazione analisi dei rischi

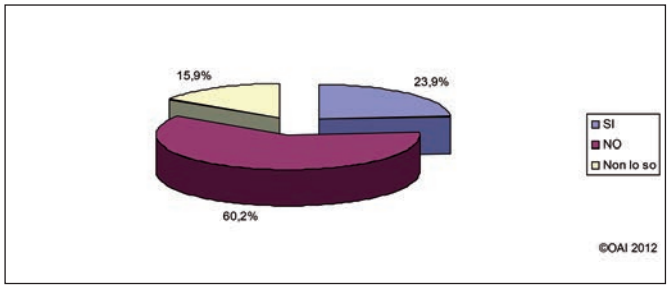

Fig. 44 - Assicurazione rischio residuo

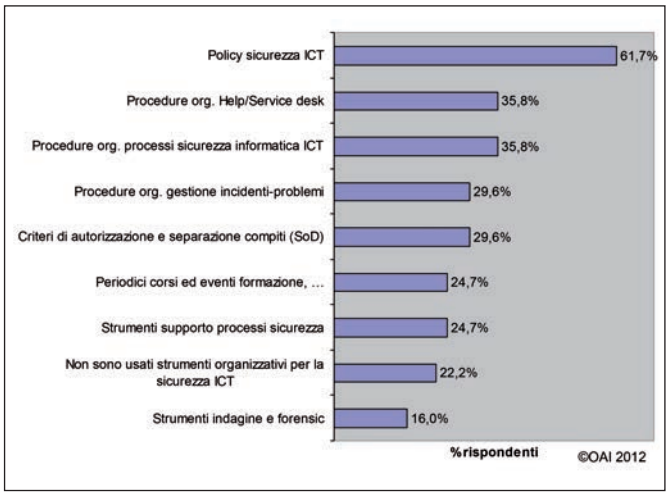

Fig. 45 - Principali contromisure organizzative

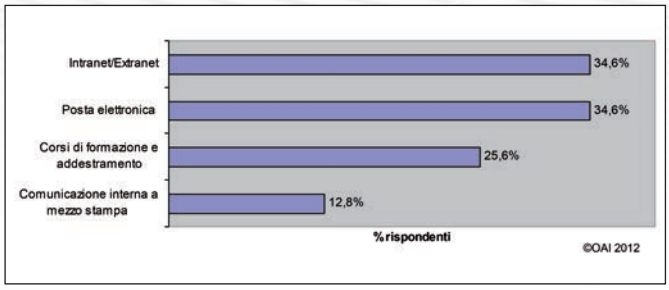

Fig. 46 - Comunicazione e diffusione delle policy

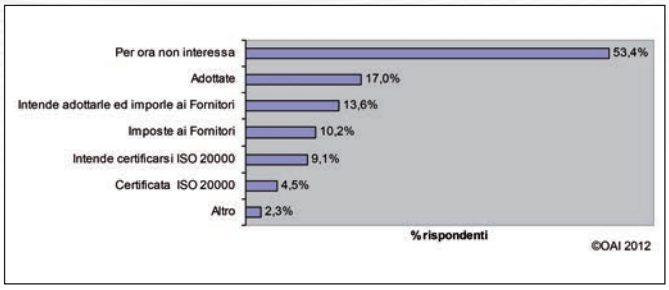

Fig. 47 - Conformità ad ITIL/ISO 20000 e a COBIT

e comunque con percentuali non trascurabili, altre attività dall'attuazione di periodici corsi e di eventi per la sensibilizzazione, formazione e addestramento di utenti e di specialisti, all'uso di strumenti di indagine e di "forensic".
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 di comunicazione e diffusione: la prevalenza è via Intranet seguita a breve distanza dalla posta elettronica, a decrescere percentualmente l'uso di seminari e corsi e, da ultimo, la comunicazione interna a mezzo stampa.

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 il COBIT per la gestione tattico-strategica allineata al business, ITIL v3 e l'ISO 20000[18] per la gestione operativa dell'ICT, la famiglia ISO 27000 per la gestione della sicurezza ICT, l'ISO 9000 per la gestione della qualità, ecc[19].
La fig. 47 evidenzia, con risposte multiple, come più della metà del campione non ha e non intende adottare "best practice" ITIL, Cobit o ISO 20000 e tanto meno certificarsi, il 17% le ha adottate funzionalmente e nella sostanza senza però certificarsi, e con percentuali minori le ha imposte ai fornitori, anche a livello contrattuale, o intende adottarle ed imporle ai propri fornitori.

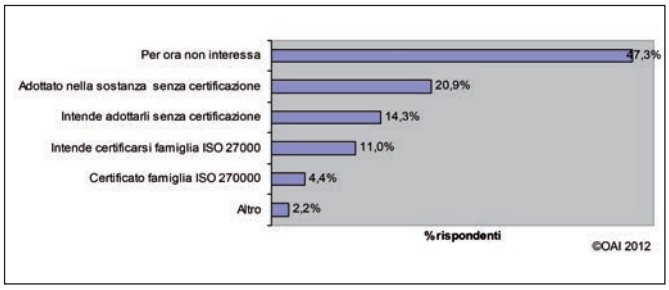

Fig. 48 - Conformità famiglia standard ISO 27000

Solo una piccola minoranza, il 4,5% è già certificata ISO 20000 (meno della metà del campione della scorsa edizione, che arrivava all'11%) ed il 9,1% intende certificarsi. La voce "Altro" include certificazione già in essere o pianificata presso la casa madre estera dell'azienda.
L'ampia famiglia di standard ISO 27000 riguarda in dettaglio la gestione della sicurezza ICT. Come mostrato nella fig. 48, quasi la metà del campione non è per ora interessato a far riferimento alla questa complessa famiglia di standard, e tanto meno a certificarsi. Circa 1/5 l'ha adottato in pratica ma senza certificarsi, ed a decrescere una quota dei rispondenti intende adottarlo nella sostanza o certificarsi nel futuro.
Solo il 4,4% del campione dichiara di essere certificato, molto probabilmente con ISO 27002. Per quanto riguarda la voce "altro" ha dettagli analoghi a quelli della precedente figura.
Per il campione 2012, così come mostrato nella fig. 49, la certificazione della qualità[20] è ben più diffusa, con circa 1/3 delle aziende/enti già certificati. Tale am-

[18] ISO 20000 standardizza logiche e processi di ITIL v2
[19] Per approfondimenti e confronti tra questi standard e best practice si rimanda al nuovo libro di prossima pubblicazione di M.R.A. Bozzetti e F. Zambon "Sicurezza Digitale" edito da Soiel International

piezza è anche dovuta al fatto che molti bandi di gara, in ambito pubblico e privato, richiedono che il fornitore abbia questa certificazione. Un 6,5% intende certificarsi nel prossimo futuro. Poco più del 15% ha adottato le logiche del gestione della qualità, ma senza certificarsi, 7,6% intende seguire tale logica nel prossimo futuro. Nel rapporto precedente la quota di certificati era più alta, con un 54%. Alcune aziende/enti devono inoltre essere certificate e seguire specifiche normative settoriali, tipicamente per le società quotate in Borsa, per quelle dei settori sanità, farmaceutico ed alimentare, per banche ed assicurazioni, ecc.: si pensi alla statunitense Sox[21] se si è quotati negli Stati Uniti, a Basilea 2-3 e alle norme della Banca d'Italia per le banche, norme ISVAP per le assicurazioni, ecc. In termini molto generali, e senza far riferimento alle specifiche norme, la fig. 50 mostra che solo il 17% dei rispondenti (rispetto al 20% della scorsa edizione) deve far fronte a questi ulteriori obblighi, facendo parte dei settori sopra indicati.

6.4.2 Audit

Nell'ambito della gestione della sicurezza una funzione importante è quella dell'auditing. La fig. 51 mostra che il 43,6% (era il 51% nella precedente edizione) dei rispondenti svolge tale funzione e che il 15,4% ha intenzione o ha a piano di espletarla.

La fig. 52 mostra il dettaglio di come venga espletata tale funzione da parte delle aziende/enti che già la svolgono: la maggioranza, il 61,8%, la svolge con periodicità regolare, ad esempio annuale, il 27,1% con ancora maggior frequenza, mentre il 17, 6% la svolge in maniera "irregolare", ossia non pianificata periodicamente, ma quando ritenuto necessario, ed una analoga percentuale la svolge in maniera continuativa, nell'ambito di un processo ben strutturato e di miglioramento continuo dell'ICT (tipicamente il CSI, Continual Service Improvements, di ITIL v3).

Una piccola percentuale, il 6,8%, la svolge solo in caso di incidenti o di attacchi gravi.

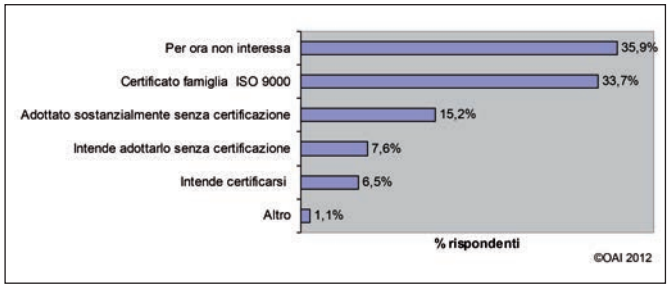

Fig. 49 - Conformità famiglia standard ISO 9000

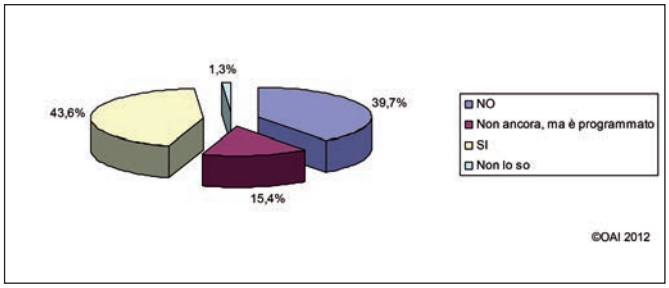

Fig. 51 - Effettuazione audit sul sistema informatico

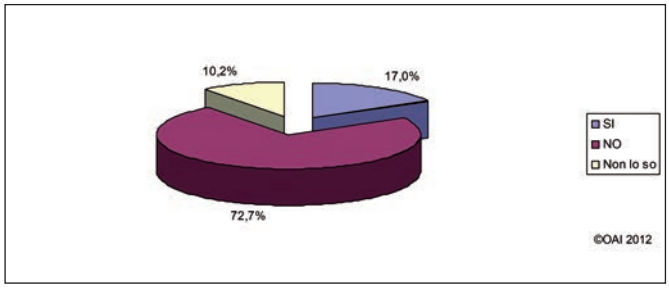

Fig. 50 - Conformità ad altri standard o normative di settore

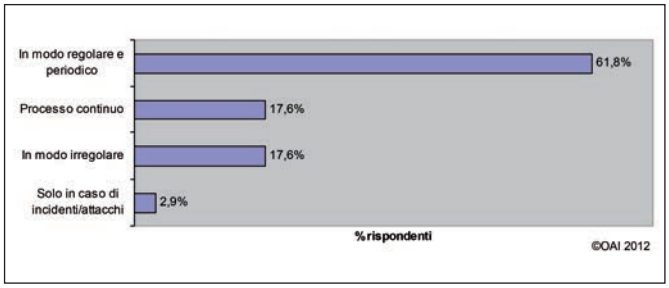

Fig. 52 - Modalità audit sul sistema informativo

[20] La certificazione per il "total quality management" impatta anche sulla sicurezza informatica e per tale motivo è stata considerata nel questionario e nel rapporto. Gli standard internazionali fanno riferimento alla famiglia ISO 9000

[21] 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

6.4.3 Struttura organizzativa interna per la sicurezza ICT

La struttura organizzativa interna per la gestione della sicurezza ha un ruolo importante e impatta sui vari processi e sulle procedure organizzative (anche per le certificazioni): nelle piccole organizzazioni talvolta tale ruolo non è né definito né attuato e quando necessario si ricorre in maniera estemporanea e in modalità d'emergenza a società e tecnici esterni. Come evidenziato dalla fig. 53, il 57,1% (era il 64,4% nella scorsa edizione) dei rispondenti ha definito un ruolo di "responsabile della sicurezza informatica", in inglese CISO, Chief Information Security Officer; il 14,3% non lo ha ancora definito ma è in procinto di farlo, il rimanente non ha per ora alcun responsabile esplicitamente definito. Nella maggior parte dei casi, il 40,7%, tale ruolo è collocato funzionalmente nell'ambito ICT, quindi all'interno dell'UOSI, come dettagliato in fig. 54. Nel 15,3% questo responsabile non è all'interno dell'UOSI ma in altre strutture interne e nel 28,8% dei casi sono definiti sia i ruoli di CSO che di CISO.

7. Attacchi più temuti nel futuro

La fig. 55, con risposte multiple, mostra quali sono gli attacchi ritenuti più probabili e più temuti nel prossimo futuro, tendenzialmente fine 2012-2013, indipendentemente da quelli eventualmente subiti, e facendo sempre riferimento alla medesima tassonomia di attacchi considerata (Tabella 1). Anche per queste domande, come per quelle relative al termine "impatto poco o molto significativo" di cui al Capitolo 5 ed alla fig. 27, non si erano specificati, per rendere più agile e semplice il questionario, i criteri per considerare un attacco più "temuto": ad esempio impatto funzionale-operativo, sul business, economico, legale, ecc. È interessante evidenziare come i primi tre attacchi più temuti sono nell'ordine quelli di "social engineering", il furto di informazioni dai dispositivi d'utente sia mobili che fissi, il "malware".

La fig. 56 pone a confronto le previsioni di attacchi più temuti emerse nelle varie edizioni OAI, confronto puramente indicativo data la diversità dei campioni diversi nelle diverse edizioni.

Anche se puramente indicativo, il grafico mostra come siano profondamente cambiate le stime di attacco più

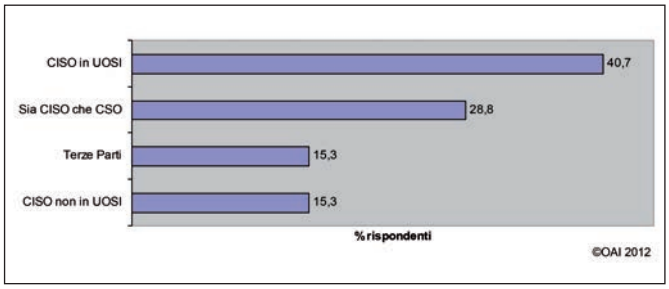

Fig. 54 - Posizionamente organizzativo CISO

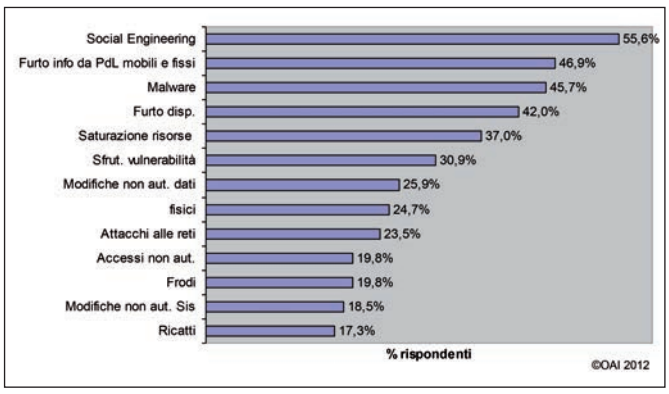

Fig. 55 - Attacchi maggiormente temuti nel futuro

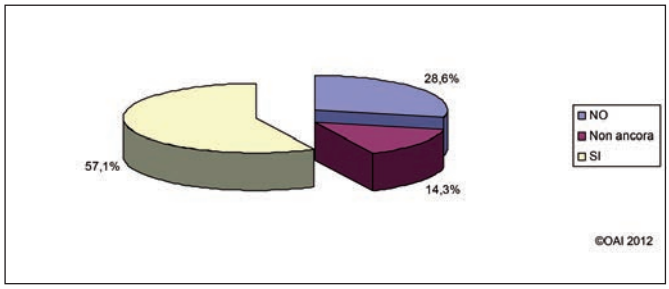

Fig. 53 - Esistenza ruolo responsabile sicurezza informatica (CISO)

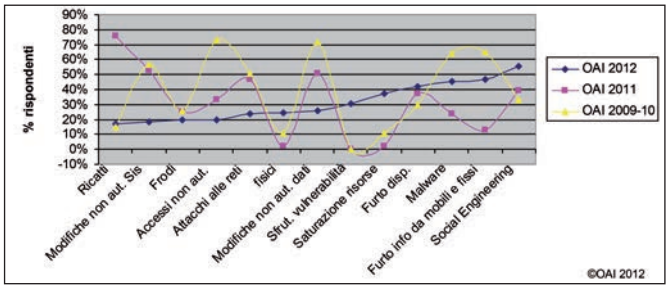

Fig. 56 - Confronti tra gli attacchi "temuti nel futuro" nei vari Rapporti OAI

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. Si notino, sempre a livello qualitativo, le forti differenze, di anno in anno, soprattutto per le frodi, i ricatti, gli accessi non autorizzati ai sistemi, le modifiche non autorizzate ai dati, lo sfruttamento delle vulnerabilità, il "malware", il furto dei dati dai dispositivi dell'utente, fissi e mobili. Sono probabilmente sottostimati o sovrastimati i veri rischi e le probabilità di occorrenza nel proprio contesto specifico, ossia nel proprio sistema informativo, condizionati forse più dall'influenza mediatica sui grandi attacchi, dal passa parola tra colleghi, dal sentito dire, dai nuovi strumenti e dall'evoluzione tecnologica,che dagli attacchi subiti e dai relativi impatti avuti.

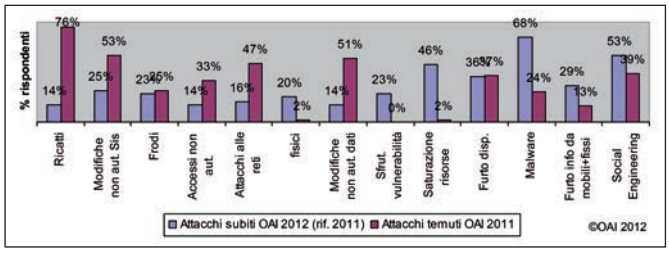

Fig. 57 - Confronti tra attacchi "temuti nel futuro" nel Rapporto 2010 ed "attacchi subiti" nel 2011

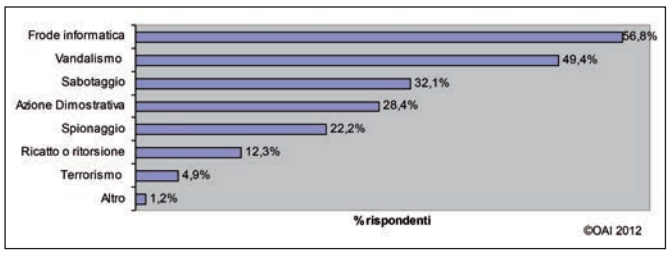

Fig. 58 - Possibili motivazioni per i futuri temuti attaacchi

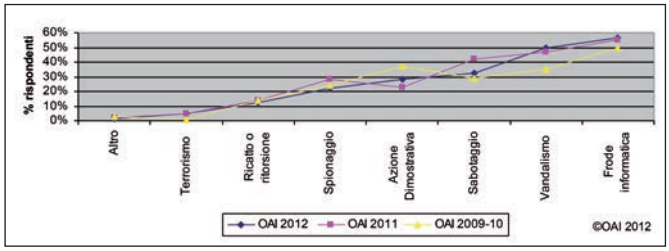

Fig. 59 - Confronto delle motivazioni per gli "attacchi temuti nel futuro" nei vari Rapporti OAI

La fig. 57 confronta gli attacchi futuri previsti e temuti del Rapporto 2010 con quelli effettivamente subiti nell'anno 2011 del presente Rapporto.
Emerge che gli unici più o meno indovinati riguardano il furto di dispositivi e le frodi.
Al contrario i più sbagliati, come molto temuto ma avvenuto in un (relativamente) limitato numero di casi, riguardano i ricatti, gli accessi non autorizzati ai sistemi, gli attacchi alle reti; tra quelli sbagliati come poco temuti ma avvenuti per una forte percentuale dei rispondenti: "malware", sfruttamento vulnerabilità, attacchi alla sicurezza fisica.
Ritornando agli attacchi più temuti nel prossimo futuro del presente Rapporto della fig. 55, la fig. 58, con risposte multiple, evidenzia quali sono le ipotesi di motivazioni degli attaccanti da parte del campione dei rispondenti.
Al primo posto è la frode informatica, che permette lauti guadagni illegali con bassi rischi di essere scoperti e puniti. Al secondo il vandalismo, causa probabile di parte degli attacchi "fisici" e dei furti.
Alte, ma ragionevoli, le percentuali del sabotaggio e dello spionaggio, oltre che dell'azione dimostrativa, che include anche gli attacchi dei così detti di "ethical hacking". Il timore di attacchi di tipo terroristico è relativamente basso, ed è circoscritto prevalentemente 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. 59, che evidenzia forti convergenze di opinione nel tempo: le curve sono simili e con scostamenti bassi.
Occorre sempre considerare tali confronti come puramente indicativi, dato il campione diverso, e rammentare che i valori percentuali dipendo anche dal numero di risposte avute per domanda: al crescere delle risposte si abbassa la percentuale, all'aumentare si riduce.

8. Prime considerazioni finali

I risultati emersi dall'indagine sono significativi e rappresentativi, a livello qualitativo se non statistico, di che cosa realmente avviene in Italia per gli attacchi ai sistemi informativi delle aziende e degli enti, e come questi ultimi

si proteggono, come cercano di prevenirli e come reagiscono qualora dovessero occorrere. Innumerevoli le considerazioni che possono emergere dai dati OAI 2012, soprattutto se correlati tra loro: nel seguito sono evidenziati da parte dell'Autore alcuni aspetti ritenuti significativi della realtà italiana.

L'insieme delle aziende/enti che hanno risposto al questionario rappresenta una fascia medio-alta del panorama italiano in termini di qualità dei sistemi e della loro gestione, e quindi anche di sicurezza ICT

I trend sugli attacchi emersi con il campione di rispondenti OAI 2012 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 gli stessi attualmente più diffusi (fig. 55);
- le motivazioni degli attaccanti sono soprattutto per un illegale guadagno economico, ossia per frodi, per spionaggio (anche industriale), per ricatti e sabotaggi (fig. 58); tale tendenza è consolidata negli ultimi anni (fig. 59); nonostante questo, gli attacchi più orientati a questi fini, appunto le frodi informatiche, i ricatti ed i sabotaggi, si rilevano come i meno temuti (fig.55). L'apparente contraddizione può essere spiegata (ma è solo un'ipotesi dell'Autore) dalla differenza tra la percezione generale di un fenomeno e la sua effettiva realizzazione 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 si basano quasi sempre:
  - 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 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 più spesso non corrette con le "patch" esistenti dagli utenti finali; quest'ultimo problema sta ulteriormente acutizzandosi con 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 più generale gestione dell'intero sistema informatico, e più in generale sulla limitata attenzione ed impegno agli 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, dell'uso di sempre più potenti chiavette USB e degli strumenti collaborativi ampliano enormemente le possibilità di rubare le identità digitali degli utenti e di acquisire facilmente informazioni riservate con le quali svolgere attacchi e compiere frodi informatiche.

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

- la maggior parte dei sistemi informativi è tecnicamente ben aggiornato, con architetture ad alta affidabilità e multipiattaforma;
- nonostante i noti problemi di banda larga in Italia, soprattutto al di fuori delle grandi città, una buona fetta dei rispondenti utilizza soluzioni in cloud (figg. 18-21) e terziarizza parte o tutta la gestione del proprio sistema informativo (fig. 7), ed una parte più piccola anche la gestione della sicurezza;
- 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 di 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;
- sul piano organizzativo, per una buona o comunque non trascurabile percentuale del campione, le aziende/enti sono "meno avanzate" che sul piano tecnico,

ma sembrano migliorare rispetto agli anni precedenti;
- aspetti positivi:
  - in buona parte delle organizzazioni è definita la figura del CISO (fig. 53), inserita nella UOSI, Unità Organizzativa Sistemi Informativi (fig. 54);
  - vengono seguite, almeno nella sostanza e per gli aspetti più importanti, le linee guida e le metodiche dei principali standard e delle "best practice" internazionali, ma è limitato l'interesse a certificarsi formalmente;
  - viene svolto l'auditing informatico con una certa regolarità (fig. 51 e 52);
  - cresce la consapevolezza dell'importanza della sicurezza ICT, almeno in termini di continuità operativa, a livello dei vertici/decisori dell'azienda/ente, soprattutto per quelle di medie grandi dimensioni;
- aspetti più critici:
  - gestione della sicurezza prevalentemente a livello di "silos", poco centralizzata ed integrata con la più generale gestione dell'intero sistema informativo (fig. 42);
  - analisi del rischio informatico poco diffusa (fig. 43);
  - embrionale la stima economica degli impatti a seguito di un attacco;
  - embrionale la riassicurazione del rischio residuo;
  - logiche di separazione delle responsabilità tra i vari attori della sicurezza ICT non ancora ampiamente diffuse;
  - i piani di gestione delle emergenze, incluso il "disaster recovery", anche se definiti e previsti, raramente sono poi provati in pratica;
- l'impatto degli attacchi risulta grave solo in un limitato numero di casi, pur al crescere del numero di attacchi e della loro sofisticazione; 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);
- la reazione in caso di attacco è prevalentemente tecnica (fig. 33) ma abbastanza efficace (figg. 34-35): il ripristino dei sistemi dopo un attacco avviene nella stragrande maggioranza dei casi entro lo stesso giorno o al più entro tre giorni; solo in rari casi i tempi sono più lunghi;
- in caso di attacco il coinvolgimento è prevalentemente dei fornitori (fig. 31) e raramente lo si denuncia alle autorità.

La connessione ad Internet, il supporto informatico alla quasi totalità dei processi e delle attività pubbliche e private, la forte crescita e diffusione dei sistemi mobili e quindi delle reti wireless, la diffusione della "consumerizzazione", dei siti collaborativi/web 2.0, dei social network sia a livello personale che di azienda/ente stanno da un lato realizzando una reale "società dell'informazione" ma dall'altro stanno esponendo a forti vulnerabilità e criticità tutti i sistemi ICT in uso.

La sicurezza dei sistemi informativi assume un ruolo crescente anche per le piccole e medie organizzazioni, che devono imparare e impegnarsi in una prevenzione continua e sistematica. Da qui l'importanza di poter disporre dei dati raccolti ed elaborati da OAI sul reale 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 ed operativo; 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 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 inter-

nazionale. L'intero mondo, sempre più digitale, funziona grazie ad applicativi software per gran 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 ultimamente a favore dei "ladri", proprio perché più organizzati e più decisi.
La maggior vulnerabilità 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. La sicurezza ICT non è tema semplice da affrontare, anche per la relazione con la tutela della riservatezza dei dati personali.
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 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, procedure di gestione delle emergenze e costante revisione dei livelli di sicurezza dei propri sistemi, modificando adeguatamente le misure adottate in relazione alla dinamica evolutiva tecnologica e applicativa.

Occorre che tutti gli operatori attuino politiche e iniziative per la sicurezza ICT in modo da rendere possibile uno sviluppo affidabile e condiviso del "mondo digitale" che altrimenti non potrà realizzarsi con successo, né dal punto di vista economico, né dal punto di vista sociale.

9. Glossario dei principali termini ed 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.
- **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, tipicamente DDOS
- **Buffer overflow**: consiste nel sovra-scivere in un buffer o in uno stack del programma dati o istruzioni con i quali il programma stesso può comportarsi in maniera diversa dal previsto, fornire dati errati, bloccare il sistema operativo, ecc.
- **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
- **Darknet**: sistema usato in Internet per monitorare la rete e possibili attaccanti, con funzinalità 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 attacco viene modificata solo la home-page a scopo dimostrativo.
- **Denial of service (DOS) e Distributed Denial of service (DDOS)**: attacco per saturare sistemi e servizi ed impedire la loro disponibilità
- **Dialer**: programma software che connette il sistema ad Internet, ad una rete o ad un computer remoto tramite linea telefonica (PSTN o ISDN); può essere utilizzato per attacchi e frodi.
- **DLP**, Data Loss Prevention: sistemi e tecniche per prevenire la perdita e/o il furto di dati nel corso del loro trattamento, archiviazione inclusa.
- **DNS**, Domain Name System: sistema gerarchico di nomi (naming) di host su Internet che vengono associati al loro indirizzo IP di identificazione nella rete.
- **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
- **Key Logger**: sistema di tracciamento dei tasti premuti sulla tastiera per poter carpire informazioni quali codici, chiavi, password
- **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 inglese per indicare la replica e la sincronizzazione di dati su due o più dischi
- **NAC**, Network Access Control: termine usato con più significati, che complessivamente indica un approccio architetturale ed un insieme di soluzioni per unificare e potenziare le misure di sicurezza a livello del punto di accesso dell'utente al sistema informativo;
- **OTP**, One Time Password: dispositivo che genera password da usarsi una sola volta per sessione/transazione.
- **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 TCP/IP: è un tipo di attacco DoS/DDoS
- **Port scanner**: programma che esplora una fascia di indirizzi IP sulla rete per verificare quali porte, a livello superiore, sono accessibili e quali vulnerabilità eventualmente presentano. È uno strumento di controllo della sicurezza, ma è anche uno strumento propedeutico ad un attacco.
- **PUP**, Potentially Unwanted Programs: programme che l'utente consente di installare sui suoi sistemi ma che, a sua insaputa, contengono codici maligni o modificano il livello di sicurezza del sistema. Tipici esempi: adware, dialer, sniffer, port scanner.
- **Race condition**: indica le situazioni derivanti da condivisione di una risorsa comune, ad esempio un file o un dato, ed in cui il risultato viene a dipendere dall'ordine in cui vengono effettuate le operazioni.
- **Rootkit**: Programma software di attacco che consente di prendere il completo controllo di un sistema, alla radice come indica il termine
- **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
- **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 motive di sicurezza, tipicamente per analizzarlo, per individuare attività anomale o per sventare attacchi. Può essere realizzato tramite darknet o honeynet.
- **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, ac-

quisti 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 usato 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
- **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.
- **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 pò di storia

- 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 fare e per far fare - II edizione", di prossima pubblicazione, Soiel International.

10.2 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 sicurezza 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/sur-

vey fornisce un dettagliato rapporto annuale sui crimini informatici negli US;

- Commissariato Pubblica Sicurezza online - Ufficio Sicurezza Telematica: http://www.commissariatodips.it/stanze.php?strparent=10 fornisce un elenco degli attacchi più recenti e/o in corso, suggerimenti su come comportarsi, possibilità di discutere in un forum, di chiedere informazioni, di sporgere denunce su reati informatici; si veda anche http://www.poliziadistato.it/articolo/982/
- 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_EMEA/security/worldmap/cruscotto segnalazioni virus;
- 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://www-03.ibm.com/security/xforce/, fornisce sistematicamente segnalazioni su vari tipi di attacco e di vulnerabilità; per i rapporti periodici si veda http://www-935.ibm.com/services/us/iss/xforce/trendreports/
- Internet Crime Complaint Center (IC3) è una partenrship tra FBI (Federal Bureau of Investigation), il National White Collar Crime Center (NW3C) e il Bureau of Justice Assistance (BJA): http://www.ic3.gov/default.aspx fornisce, oltre alla possibilità di denunciare negli US attacchi Informatici, informazioni sugli attacchi stessi e sui trend in atto per i crimini informatici;
- Panda Security: http://www.pandasecurity.com/enterprise/security-info/ fornisce informazioni sugli attacchi sia a livello domestico che d'impresa,oltre che rapporti periodici;
- SANS Institute (www.sans.org): fornisce sistematicamente segnalazioni su vari tipi di attacco e di vulnerabilità;
- Security Central Micrososft: http://www.microsoft.com/it-it/security/pc-security/default.aspx#Aggiornamenti-di-sicurezza fornisce avvisi su vulnerabilità e malware per i prodotti Microsoft;
- Symantec: sul sito italiano (http://www.symantec.com/it/it/index.jsp) fornisce allarmi e segnalazioni su vari tipi di attcco 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.verizonbusiness.com/it/Products/security/dbir/
- Websense Security Labs: http://securitylabs.websense.com/; interessante il cruscotto com mappe geografiche dell'Attack Information Center in http://securitylabs.websense.com/content/CrimewarePhishing.aspx.
- 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, laureato in ingegneria elettronica al Politecnico di Milano, è amministratore unico di Malabo Srl, società di consulenza sull'ICT (si veda www.malaboadvisoring.it), 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 campi di intervento includono la governance ICT, la sicurezza informatica, il disegno di architetture hardware, software e di reti, la razionalizzazione e la gestione del sistema informativo, la definizione di strategie ICT, l'assessment delle tecnologie, 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-GEA LAB, oltre ad essere stato il primo responsabile dei sistemi informativi a livello "corporate" dell'intero Gruppo ENI. Fu uno dei primi a livello mondiale ad occuparsi di internetworking, operando attivamente anche presso vari Enti internazionali di standardizzazione e partecipando a progetti di ricerca sia nazionali che europei. Tra i risultati delle sue attività particolarmente rilevanti furono per il Gruppo Olivetti l'ideazione e l'implementazione di ONE, Olivetti Network Environment, per l'intero Gruppo ENI dell'enterprise architecture MICEA, per SMAU e per le principali Fiere europee di EITO, European IT Observatory.
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, di itSMF e di Prospera. È certificato ITIL v3.
Ha pubblicato articoli e libri sull'evoluzione tecnologica, la sicurezza, gli scenari e gli impatti dell'ICT.
Appassionato di alpinismo e sci, pratica anche jogging, sub e golf.

Profili SPONSOR

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

- Rappresentanza dei professionisti dell'Information Security.
- Networking con altri professionisti del settore.
- Possibilita' di costituire gruppi di lavoro e di condivisione informazioni su tematiche d'interesse comune.
- Accesso e/o 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 Iweb SSA.
- Ricevimento di ISSA Journal , la rivista mensile di ISSA.
- Accesso/ricevimento Webcast, della newsletter di ISSA e della newsletter italiana di AIPSI.
- 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.
- Certificazione di competenze sulla sicurezza.
- 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

Accenture è un'azienda globale di consulenza direzionale, servizi tecnologici e outsourcing. Combinando un'esperienza unica, competenze in tutti i settori di mercato e nelle funzioni di business e grazie ad un'ampia attività di ricerca sulle aziende di maggior successo al mondo, Accenture collabora con i suoi clienti, aziende e pubbliche amministrazioni, per aiutarli a raggiungere alte performance. Accenture conta più di 257 mila professionisti che servono clienti in oltre 120 paesi. A livello globale, i ricavi netti per l'anno fiscale 2012 (settembre 2011 – agosto 2012) ammontano a 27,9 miliardi di dollari.

Accenture in Italia
In Italia è presente dal 1957. Oggi tutte le società del gruppo Accenture impiegano circa 10.500 persone nelle sedi di Milano, Roma, Torino, Napoli, oltre a diversi uffici in Italia. Nell'anno fiscale 2012 Accenture ha registrato ricavi per 1 miliardo e 85 milioni di euro.

L'approccio al mercato
Il fattore distintivo di Accenture è quello di saper coniugare le competenze e l'esperienza dei suoi professionisti nei diversi settori di mercato - Communications, Media & Technology, Financial Services, Health & Public Service, Products, Resources - con competenze funzionali specialistiche di Consulenza Direzionale, Servizi tecnologici e Outsourcing.

Communications, Media & Technology
Telecomunicazioni, Elettronica &High Tech, Media & Entertainment

Financial Services
Banche e Servizi Finanziari, Assicurazioni, Capital Markets

Health & Public Service
Previdenza Sociale e Lavoro, Economia e Finanza, Sicurezza e Immigrazione, Giustizia, Poste, Sanità, Formazione e Istruzione, Difesa

Products
Automotive, Beni e Servizi di consumo, Impianti industriali, Sanità e aziende farmaceutiche, Grande distribuzione, Trasporti e Viaggi

Resources
Energia, Utilities, Chimica, Metalli, Cemento, Carta

I clienti di Accenture
Accenture può vantare un'ampia collaborazione con le più grandi aziende di tutti settori industriali e agenzie governative in tutto il mondo. In particolare nell'ultimo anno annovera tra i suoi clienti 94 delle aziende Fortune Global 100 e oltre tre-quarti delle Fortune Global 500. Tutti i principali 100 clienti si affidano ad Accenture da almeno 5 anni, 92 sono clienti da 10 anni. Relativamente all'Italia, Accenture ha come clienti 15 tra i primi 20 gruppi finanziari nazionali, le prime 4 società assicurative e 11 tra i primi 15 gruppi industriali.

Per maggiori informazioni: www.accenture.it

La IBM (International Business Machines Corporation) è tra le maggiori imprese del mondo e un marchio leader nel mercato dell'Information Technology. Fondata nel 1911, ha sede ad Armonk negli Stati Uniti e operazioni in oltre 170 Paesi.
IBM è la prima società di informatica in Italia, dove è presente dal 1927 con filiali e centri di supporto tecnico su tutto il territorio nazionale e si avvale della collaborazione di una rete di oltre 3.500 business partner.
La missione della IBM è sviluppare tecnologie informatiche avanzate e integrarle in soluzioni a sostegno dell'innovazione nelle imprese, nelle istituzioni e nella società. Con 5 Premi Nobel assegnati a suoi ricercatori, la IBM detiene primati in ogni area dell'IT, dai microprocessori ai supercomputer, dai server al software per lo sviluppo e la gestione di complesse infrastrutture informatiche. La IBM dedica alla sola ricerca oltre 3 mila persone e investimenti annui superiori ai 6 miliardi di dollari; da diciannove anni è la prima società per numero di brevetti negli Stati Uniti.
Allo stesso tempo, la IBM ha investe in competenze e strutture per affiancare i propri clienti nei loro processi di innovazione e aiutarli a tradurre la tecnologia in un valore che li differenzi e dia loro un vantaggio competitivo. In tutto il mondo, la società si rivolge al mercato con organizzazioni specializzate nei diversi settori (banche e servizi finanziari, industria, comunicazioni, settore pubblico, distribuzione, piccole e medie imprese). Nell'ambito deil servizi, che rappresentano oltre il 55% del fatturato e il 50 per cento dell'organico a livello mondiale, la consulenza occupa un ruolo di crescente importanza.
Da sempre protagonista nel mercato dell'information technology, IBM è uno dei provider leader mondiali di soluzioni di gestione dei rischi e della sicurezza. Dispone di un vasto portafoglio di soluzioni hardware e software, offerte di servizi professionali e gestiti che coprono tutta la gamma dei rischi informatici e di sicurezza aziendale, tra i quali quelli relativi alle persone, alle identità, ai dati e alle informazioni, alle applicazioni e ai processi, alle reti, ai server ed endpoint e alle infrastrutture fisiche.
In particolare, il team di ricerca X-Force cataloga, analizza e conduce ricerche sulle divulgazioni delle vulnerabilità sin dal 1997. Con oltre 50.000 vulnerabilità della sicurezza catalogate, possiede il più grande database delle vulnerabilità del mondo, che aiuta i ricercatori X-Force a comprendere le dinamiche che costituiscono la scoperta e la divulgazione delle vulnerabilità stesse.
IBM collabora con enti governativi, società e istituzioni a livello mondiale e favorisce l'adozione di open standard per rafforzare i protocolli aziendali e implementare un approccio olistico alla sicurezza.

Per maggiori informazioni: www.ibm.com/security.

Identità
Il Gruppo Lottomatica ha fondato la propria identità sul principio di crescita sostenibile, nella convinzione che nel settore dei giochi sia essenziale uno sviluppo responsabile attento agli aspetti sociali connessi al business. La responsabilità è una componente cruciale in un'attività che consiste prevalentemente nel gestire giochi regolamentati dai governi. Coerentemente con questa consapevolezza, fin dal 2009 Lottomatica, primo operatore in Italia e fra pochi in Europa, ha ottenuto dall'European Lotteries Association la certificazione di conformità agli standard di gioco responsabile e con il massimo livello previsto del Responsible Gaming Framework dalla World Lottery Association.

Missione
La missione del Gruppo Lottomatica è di consolidare e accrescere la propria posizione di leadership come operatore commerciale e fornitore di tecnologia sul mercato mondiale regolamentato dei giochi offrendo soluzioni, servizi e prodotti di alto livello, con integrità, responsabilità e creazione di valore per gli azionisti.

Strategia
La strategia del Gruppo può riassumersi nel seguente modo:
- garantire e continuare ad incrementare le vendite nei c.d. "same stores" (vendite relative ai contratti esistenti);
- aggiudicarsi contratti in nuove giurisdizioni strategiche e presentare offerte allettanti per ricoprire il ruolo di operatore delle lotterie;
- completare il lancio delle Video lottery terminal in Italia e lanciare le stesse anche in Nord America;
- lanciare nuove piattaforme di distribuzione soprattutto nei canali interattivi;
- continuare a ridurre il debito del Gruppo e confermare la politica di distribuzione dei dividendi.

ICT Security
Il contesto in cui opera il Gruppo in Italia presenta sfide importanti nell'ambito della gestione della sicurezza dei sistemi informativi:
- Ampia offerta di giochi e servizi;
- Canali di erogazione eterogenei (Rete di punti vendita capillare a livello nazionale, Web, Mobile, Smart TV);
- Ampia base Clienti e volumi transazionali gestiti;
- Requisiti di Compliance rispetto a fonti diverse di regolamentazione: normativa, concessoria, standard di certificazione qualità (quali ad esempio 27001).

La risposta alle sfide del contesto descritto è articolata e passa attraverso diverse direttrici:
- ICT Security Solutions: Utilizzo di piattaforme per la gestione della sicurezza dei sistemi centrali e dei Clienti finali all'avanguardia tecnologicamente ed in continua evoluzione, adattate alle specifiche esigenze del contesto;
- ICT Security Compliance Management: Organizzazione, risorse, competenze, processi e procedure che consentono il governo della compliance end to end: dalle prime fase di progettazione sino alla erogazione del servizio al cliente finale.

Per maggiori informazioni: http://www.lottomaticagroup.com/

ORSYP, fondata nel 1986, è una multinazionale specializzata nella consulenza e nei servizi dedicati alla "produzione informatica", con una profonda esperienza nell'ambito delle soluzioni destinate all'automazione e al controllo dei processi aziendali in architetture complesse ed eterogenee.
Con un organico di oltre 500 dipendenti, 3 centri di "Ricerca e Sviluppo" e 12 filiali nel mondo, ORSYP è una delle prime 5 società nell'ambito delle IT Operations ed è stata la prima a rilasciare uno schedulatore, Dollar Universe, con architettura "peer-to-peer" adatta anche in ambienti cloud.
Grazie alla competenza specialistica e al portfolio di soluzioni integrato, ORSYP è in grado di affiancare le imprese nella realizzazione di progetti di ottimizzazione dei Data Center mediante automazione, standardizzazione, controllo e pianificazione dei processi IT. Infatti, solo amministrando l'IT come un'industria si possono ottenere risultati misurabili, già nel breve periodo, conseguire risparmi e generare l'autofinanziamento necessario per realizzare progetti innovativi: questa è la filosofia "IT As A Factory" promossa da ORSYP.

ORSYP ha deciso di sponsorizzare la ricerca OAI 2012 in quanto automazione e sicurezza sono correlate: una maggiore automazione dei data center permette di aumentare la sicurezza informatica e di migliorare la sua gestione.

Per maggiori informazioni: www.orsyp.it

Seeweb è nata 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 due grandi Data Center in Italia, uno a Frosinone, recentemente ampliato per complessivi 6300 mq e completamente dedicato alle infrastrutture per il cloud, ed uno a Milano (in via Caldera, cuore dell'internet italiana); per triangolare in altissima affidabilità opera con un Data Center nel nord Europa e con connessioni a barda larga dai migliori provider di telecomunicazione.
A fianco dei servizi di hosting, housing e collocation, Seeweb ha una offerta a 360º nell'ambito cloud: Cloud Hosting, Cloud Server, Cloud Infrastructure, Cloud Storage, Cloud Streaming.
Il picco di utilizzo della Cloud Infrastructure nel corso del 2012 è arrivato a 5048 CPU e 13123 GB di RAM, e tali dati stanno ultimamente crescendo, a conferma del successo incontrato sul mercato, pur in un momento di forte crisi macro-economica.

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 ed 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 ed organizzativo dei Data Center e dei sistemi ICT, completamente gestiti dal personale di Seeweb, ha portato anche ad 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 è certificata ISO9001 per la gestione totale della qualità, ed ISO14001 per la compatibilità ambientale.

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

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 28 sedi in tutto il mondo, di cui una in Italia. Gli utili annuali per il 2011 ammontano a 1.200 miliardi di US $, di cui 62% Business e il 38% Consumer. Come quote di mercato a livello mondiale è #1 nella protezione server, nei primi 3 posti per la vendita di soluzioni dedicate alla protezione web, messaggistica ed endpoint secondo la più recente analisi IDC.
Management: Eva Chen, CEO e Co-fondatore, Mahendra Negi, COO&CFO, Steve Chang, Presidente e Fondatore.

Proteggiamo il viaggio verso il Cloud
Con oltre 20 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. Nell'analisi 2010 CIO Insight Vendor Value, Trend Micro si è classificata 2a nella Protezione, per aver offerto maggiore valore, migliore affidabilità e fedeltà superiore, e fra i primi 3 fornitori IT nel garantire l'assistenza richiesta.

Per ulteriori informazioni: www.trendmicro.it

APPUNTI

SOIEL INTERNATIONAL
Eventi e riviste per l'organizzazione aziendale

L'INFORMAZIONE AL SERVIZIO DELLA CONOSCENZA

La casa editrice Soiel International è presente da 34 anni nel mercato dell'editoria professionale, rivolta al dinamico settore dell'Information & Communication Technology e al comparto dell'arredo dell'ambiente ufficio, con riviste tecnico-professionali curate nei contenuti. L'obiettivo è quello di fornire ai professionisti degli strumenti di conoscenza innovativi e costantemente aggiornati.
Le riviste sono accreditate nel mercato di riferimento non solo per i contenuti, ma anche per la qualità del mailing costruito nel tempo con la fidelizzazione dei lettori e tramite molteplici attività seminariali.
Office Automation è il mensile di sistemi hardware e software per l'ufficio, telecomunicazioni, networking e cabling.
Executive.IT è il bimestrale realizzato in collaborazione con Gartner, che crea i contenuti redazionali, rivolto al management aziendale che propone scenari, tecnologie, modelli e strategie per il successo del business attraverso l'utilizzo dell'ICT.
innov@zione.PA è il mensile, in formato tabloid, per l'applicazione delle nuove tecnologie nella Pubblica Amministrazione centrale e locale.
Officelayout è il bimestrale per progettare, arredare e gestire lo spazio ufficio.
L'offerta editoriale propone anche manuali di approfondimento, libri e dizionari.

LA CONOSCENZA AL SERVIZIO DEL BUSINESS

Soiel International si presenta come partner per l'attività professionale nell'ICT, favorendo incontri tra il mondo dell'offerta e quello della domanda.
La lunga esperienza acquisita nella comunicazione, la professionalità offerta a una vasta platea di lettori e la qualità del mailing sono i pilastri su cui poggia l'attività di "comunicazione d'impresa" di Soiel International che comprende consulenza, progettazione e organizzazione di convegni, corsi, eventi promozionali nonché supporto alla realizzazione e confezionamento di materiale informativo aziendale (brochure, depliant, pannelli istituzionali e documentazione promozionale).
Nell'ambito dei progetti convegnistico-espositivi multisponsor, tutti in duplice edizione a Milano e Roma e alcuni presenti anche in altre aree geografiche di interesse per il business, Soiel International organizza i convegni con area espositiva **Sicurezza ICT** (dedicato alla sicurezza delle comunicazioni e delle informazioni in azienda), **Videosorveglianza su IP** (Tecnologie, architetture, aspetti implementativi e normativi), **Il Documento Digitale** (dedicato alla dematerializzazione dei documenti e alla gestione e archiviazione delle informazioni aziendali), **EAC** (Enterprise Architecture Conference: le architetture ICT nell'era del cloud), **Opensource Conference** (per capire come e perchè l'Open Source rappresenta un'opportunità per far evolvere l'ICT in azienda), **Connectivity** (L'integrazione di Cablaggio, Networking e Datacenter), **Big Data Congress** (A cosa servono, quali sono le infrastrutture ICT ideali e come valorizzare il business) e infine **I Giorni dell'ICT** che hanno luogo a Bari e Palermo (dedicati a Sicurezza e Videosorveglianza).

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