Rapporto 2011 OAI

Osservatorio Attacchi Informatici in Italia

a cura di
Marco R. A. Bozzetti

Ringraziamenti

L'autore e Soiel International ringraziano tutte le persone che hanno risposto al questionario on-line e tutti i Patrocinatori che, con le loro idee e suggerimenti, hanno aiutato alla preparazione dell'Osservatorio.
Un grazie particolare alla Dott.ssa Consuelo Sironi e alla dott. Roberta Brigatti che hanno strettamente collaborato con l'autore per l'analisi dei dati raccolti e per la preparazione dei relativi grafici e tabelle, e al dott. Francesco Zambon per l'aiuto ed i suggerimenti forniti.

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

Finito di stampare nel mese di novembre 2011
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

1. Introduzione

Il presente rapporto è la seconda edizione annuale dell'OAI, Osservatorio Attacchi Informatici in Italia. Esso fa riferimento agli attacchi informatici rilevati nel corso del 2009 e del 1° quadrimestre 2010, e segue la prima pubblicazione del Rapporto OAI 2009, che faceva riferimento agli attacchi rilevati nel 2007 e nel 2008.
Dopo il successo della prima edizione del Rapporto, l'iniziativa OAI ha visto crescere il numero di Patrocinatori, che annovera ora, oltre alla collaborazione con la Polizia delle Comunicazioni, AIPSA (Associazione Italiana Professionisti Security Aziendale), AIPSI (Associazione Italiana Professionisti Sicurezza Informatica), Assintel di Confcommercio (Associazione Nazionale Imprese ICT), Assolombarda di Confindustria, Aused (Associazione Utilizzatori Sistemi e Tecnologie dell'informazione), ClubTi di Milano, CDI di Torino, CDTI di Roma, ClubTI Liguria, ClubTI Marche, ClubTI Campania, ClubTI Umbria, ClubTI Emilia Romagna, FTI (Forum delle Tecnologie dell'Informazione), FidaInform (la Federazione dei ClubTI Italiani) con tutti i vari ClubTi federati sul territorio nazionale, Inforav (Istituto per lo sviluppo e la gestione avanzata dell'informazione), itSMF Italia (information technology Service Management Forum).
Per fornire un aggiornamento e creare una certa continuità tra un' edizione e l'altra del Rapporto, l'Editore Soiel International e l'autore M.R.A. Bozzetti hanno dato vita ad una rubrica mensile di OAI pubblicata sulla rivista Office Automation. Tutti gli articoli sono disponibili on-line sul sito dell'autore (www.malaboadvisoring.it).

L'obiettivo primario di OAI è di fornire concrete indicazioni sugli attacchi intenzionali ai sistemi informatici delle Aziende e degli Enti pubblici italiani, che possano essere di riferimento, autorevole e indipendente, per l'analisi e la gestione dei rischi a livello nazionale. Ulteriore e non meno importante obiettivo è quello di favorire lo sviluppo di sensibilità e cultura in materia di sicurezza delle informazioni e delle comunicazioni (in breve sicurezza ICT) soprattutto per i "non tecnici", figure tipicamente ricoperte dai manager e dai vertici dell'organizzazione che decidono e stabiliscono i budget anche per la sicurezza ICT.

Il Rapporto annuale si basa sull'elaborazione delle risposte avute al questionario on-line sul sito Soiel da parte di CIO (Chief Information Officer), CSO (Chief Security Officer) e CISO (Chief Information Security Officer) appartenenti ad aziende ed enti pubblici centrali e locali.
Il compilatore del questionario può rimanere totalmente anonimo e per motivi di riservatezza non sono richieste informazioni di dettaglio, così da non consentire di risalire da un questionario anonimo all'azienda/ente cui fa riferimento.
L'autore e l'Editore garantiscono la totale riservatezza sui dati raccolti, che non vengono forniti in nessun modo a terzi: OAI utilizza e utilizzerà tali dati solo per le analisi e per la produzione di rapporti, senza mai citare casi o esempi specifici.

Per facilitare la lettura del rapporto, che inevitabilmente fa riferimento a concetti tecnici, è a disposizione in § 9 un glossario degli acronimi e dei termini tecnici specialistici usati.

2. Le motivazioni dell'Osservatorio sugli Attacchi Informatici in Italia

Con la pervasiva e crescente diffusione e 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 le quali 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 "Cloud Computing" e XaaS (Software/Platform/Infrastructure/Storage/Network .... as a Service). Anche grazie alla diffusione di dispositivi mobili d'utente, che sono ormai dei potenti com-

puter personali, delle reti senza fili (wireless), dei collegamenti "peer-to peer" (P2P), dei "social networking" e dei servizi ad essi correlati, ad esempio Facebook, LinkedIn e Twitter, il confine tra ambiente domestico e ambiente di lavoro è molto labile.
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, 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 comporta per l'attaccante una minore necessità di competenze, oltre che una maggiore disponibilità di sofisticati strumenti d'attacco e di ambienti di sviluppo per realizzarli e personalizzarli.
Data l'odierna pervasività dell'ICT, non sono più a rischio solo i sistemi personali o quelli delle aziende/enti, ma anche i sistemi di telecomunicazione e di controllo di processo e nel prossimo futuro i sistemi "embedded", ossia i sistemi ICT realizzati specificatamente per ed inclusi nei prodotti, dall'automobile all'elettrodomestico, dall'attrezzo ginnico alla domotica.
Ma quali sono gli attacchi che tipicamente affliggono i sistemi informativi delle aziende/enti 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) e quelli provenienti dai principali Fornitori di sicurezza informatica, quali Cisco, IBM, McAfee, Microsoft, Symantec, Sophos (in §10 un elenco delle principali e più aggiornate fonti). Questi studi forniscono con cadenza periodica informazioni per i principali paesi e individuano i principali trend. Dati specifici riguardanti l'Italia normalmente sono limitati o non 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.
L'occorrenza degli attacchi e lo stato dell'arte a essi relativo sono prevalentemente trattati dalla stampa 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 più, dell'installazione di firewall, anti malware, sistemi di identificazione e autenticazione, e così via.
Proprio per colmare tale vuoto informativo in Italia, con la prima edizione del Rapporto OAI si decise di rilanciare un Osservatorio Nazionale, ereditando l'esperienza passata avuta con OCI, Osservatorio Criminalità Informatica, di FTI-Sicurforum. 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.
Dopo il successo riscosso nella prima edizione, l'iniziativa OAI continua a crescere nonostante l'impegno richiesto e le difficoltà attuative dato l'approccio basato sul volontariato. I fenomeni tecnologici e di mercato dell'ICT si presentano in Italia con qualche ritardo rispetto agli Stati Uniti ed al nord Europa, pur con ritardi diversi nei diversi settori del business e delle pubbliche amministrazioni. Il Rapporto OAI, confrontato con gli analoghi rapporti internazionali e dei principali paesi, consente di comprendere e prevedere quali attacchi ai sistemi informativi diventeranno più probabili.

3. Le tipologie di attacco considerate

La sicurezza ICT è definita come la "protezione dei requisiti di integrità, disponibilità e confidenzialità" delle informazioni trattate, ossia acquisite, comunicate, archiviate e processate. Nello specifico:

- **integrità** è la proprietà dell'informazione di non essere alterabile;
- **disponibilità** è la proprietà dell'informazione di essere accessibile e utilizzabile quando richiesto dai processi e dagli utenti autorizzati;
- **confidenzialità** è la proprietà dell'informazione di essere nota solo a chi ne ha il diritto.

Per le informazioni e i sistemi connessi in rete le esigenze di sicurezza includono anche:

- **autenticità**, ossia la certezza da parte del destinatario dell'identità del mittente;
- **non ripudio**, ossia il fatto che il mittente o il destinatario di un messaggio non ne possano 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 o per fenomeni accidentali esterni.
Gli attacchi intenzionali possono provenire dall'esterno dell'organizzazione considerata, tipicamente attraverso Internet, oppure dall'interno dell'organizzazione stessa, o da una combinazione tra 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, e in particolare ai saggi di Pacifici e Sarzana di Sant'Ippolito contenuti nel volume Bozzetti, Pozzi 2000 (si veda in § 11).
La classificazione degli incidenti e degli attacchi per raccogliere i dati è definita in termini semplici, non tecnici e comprensibili a coloro cui il questionario è indirizzato: tipicamente i responsabili dell'area ICT (CIO) e, laddove esistano, della sicurezza ICT (CISO) e della sicurezza aziendale (CSO).

Rispetto alla prima edizione si è leggermente rivista la tassonomia degli attacchi informatici considerati, riportata qui di seguito (l'ordine non fa riferimento alla criticità o gravità dell'attacco, per la spiegazione dei termini gergali si rimanda al glossario in allegato):

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 sia da dispostivi mobili (palmari, cellulari, laptop) sia da tutte le altre risorse ICT
4. Frodi tramite uso improprio o manipolazioni non autorizzate e illegali del software applicativo (ad esempio utilizzo di software pirata, copie illegali di applicazioni, ecc.)
5. Attacchi di Social Engineering e di Phishing per tentare di ottenere con l'inganno (via telefono, e-mail, chat, ecc.) informazioni riservate quali credenziali di accesso, identità digitale, ecc.
6. Ricatti sulla continuità operativa e sull'integrità dei dati del sistema informativo (ad esempio: se non si paga, il sistema informatico viene attaccato e vengono procurati seri danni)
7. Accesso e uso non autorizzato degli elaboratori, delle applicazioni supportate e delle relative informazioni
8. Modifiche non autorizzate ai programmi applicativi e di sistema, alle configurazioni, ecc.
9. Modifiche non autorizzate ai dati e alle informazioni
10. Utilizzo vulnerabilità del codice software, sia a livello di posto di lavoro che di server (tipici esempi: back-door aperte, SQL injection, buffer overflow, ecc.)
11. Utilizzo codici maligni (malware) di varia natura, quali virus, Trojan horses, Rootkit, bots, exploits, sia a livello di posto di lavoro che di server
12. 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.

13. Attacchi alle reti, fisse o wireless, e ai DNS (Domain Name System)

Per facilitare la raccolta dei dati sugli attacchi subiti, articolandoli secondo la tipologia di cui sopra, il questionario è volutamente breve e senza dettagli sulle infrastrutture informatiche e sulle modalità di attacco e di difesa, così da renderlo il più possibile anonimo e non appesantirne la compilazione.

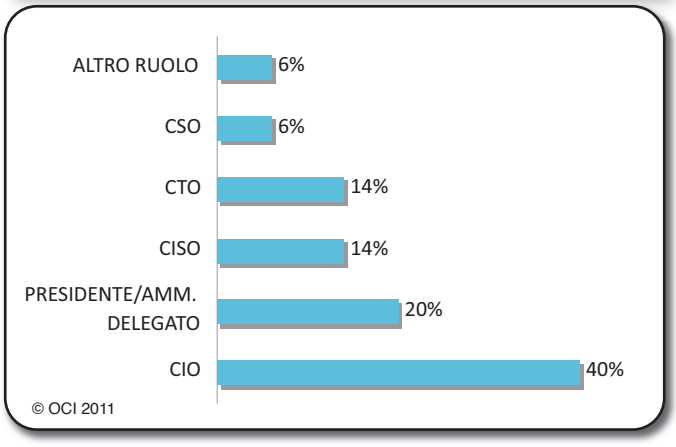
4. Caratteristiche del campione e dei sistemi ICT censiti per OAI 2011

Il questionario fa riferimento agli attacchi subiti nel 2009 e nel primo quadrimestre 2010.
Le persone contattate appartengano ai ClubTI federati in FidaInform e alle altre Associazioni che hanno patrocinato l'iniziativa, a cui si aggiungono quelle delle mailing list specializzate di Soiel International. Complessivamente il bacino delle persone contattate tramite posta elettronica si aggira attorno alle 1800 persone.
Pur avendo quasi raddoppiato il numero potenziale di compilatori del questionario, anche in questa edizione si sono avute difficoltà nell'ottenere risposte, soprattutto da alcuni settori, nonostante i numerosi e ripetuti solleciti inviati in maniera mirata ai settori dai quali si erano avute meno risposte.
La scadenza per il termine della raccolta dei questionari compilati è stata posticipata da fine dicembre 2010 a marzo 2011, ritardando in tal modo l'elaborazione del presente rapporto, ma colmando, almeno parzialmente, gli iniziali "vuoti": superato di poco il numero di 130 risposte complete ed esaurienti (rispetto alle poco più di 100 della prima edizione, con un incremento di quasi il 20%), si è deciso di chiudere la raccolta dei dati per non aumentare eccessivamente i ritardi nella pubblicazione.
Il numero di risposte sono sufficienti e significative a fornire delle concrete indicazioni sugli attacchi ai sistemi informativi in Italia. L'analoga iniziativa statunitense CSI, 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 è di 1:4 (rispetto all'1:5 della prima edizione) tra Italia e USA ed è più che sufficiente ai fini indicativi, se non strettamente statistici, dell'OAI; anche se per quest'ultimo si cercherà di incrementare anno per anno il numero di rispondenti e di sempre meglio bilanciarli tra i diversi settori sia pubblici che privati. Il campione dei rispondenti non è predefinito o selezionato a fini statistici, ma sulla base delle risposte volontarie via web e con l'obiettivo di fornire le effettive tendenze degli attacchi in Italia. Il numero e la ripartizione dei rispondenti, per tipo di settori e per dimensioni, forniscono valide e interessanti indicazioni che nessun altro rapporto fornisce specificatamente per l'Italia. Il campione del precedente Rapporto e di quello presente sono diversi, anche per l'aumento di rispondenti, ma da un punto di vista del mix e a livello qualitativo e indicativo sono confrontabili.

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

Il bacino di utenza contattato è costituito da CIO, CSO, CISO e da altre figure, quali consulenti ed esperti di enti esterni, che gestiscono per l'azienda/ente la sicurezza informatica, fino ai responsabili di massimo livello, tipicamente proprietari, presidenti e amministratori, unici o delegati, delle aziende medie e piccole. La fig.1 sintetizza la ripartizione dei compilatori per ruolo: al primo posto, come percentuale dei rispondenti, sono i responsabili dei sistemi informativi (CIO), al secondo posto le figure di ver-

FIG. 1 - Ripartizione dei compilatori per ruolo



tice della struttura (Presidenti, Amministratori Unici o Delegati, Direttori Generali); al terzo posto e con uguale percentuale, i responsabili della sicurezza informatica (CISO) e i responsabili delle tecnologie (CTO, Chief Technology Officer); ultimi i CSO ed altre figure quali consulenti e terze parti che gestiscono la sicurezza informatica. La percentuale relativamente 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.

La fig.2 illustra la suddivisione dei compilatori per i settori pubblici e privati di appartenenza.
La tassonomia dei settori merceologici considera l'industria manifatturiera, i servizi, il settore dell'ICT (che include sia le industrie manifatturiere che di servizi come le telecomunicazioni), la distribuzione (indicato con il termine inglese "retail" nella figura), il settore della finanza che include banche e assicurazioni, le pubbliche amministrazioni centrali e locali. Un 5% dei rispondenti non si è identificato nei macro settori elencati, classificandosi come "altro", ma non ha specificato a quale altro settore ritiene di appartenere.

La figura evidenzia come i settori dell'ambito finanziario (banche e assicurazioni) e della Pubblica Amministrazione, sia locale che centrale, abbiano risposto ancora in maniera troppo esigua, nonostante le innumerevoli sollecitazioni; una situazione analoga a quanto avvenuto anche per il precedente Rapporto. Le motivazioni riguardano 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 le dimensioni, come numero di dipendenti, delle aziende ed enti del campione, che risulta ben bilanciato tra piccole, medie e grandi.

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 innanzitutto 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 includono l'estensione geografica del sistema informatico, la "macro" struttura del sistema indivi-

FIG. 2 - Ripartizione del campione per settore merceologico

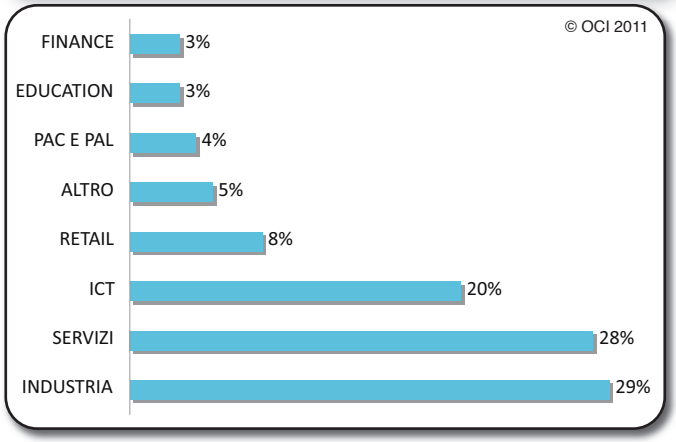


FIG. 3 - Ripartizione del campione per numero dipendenti

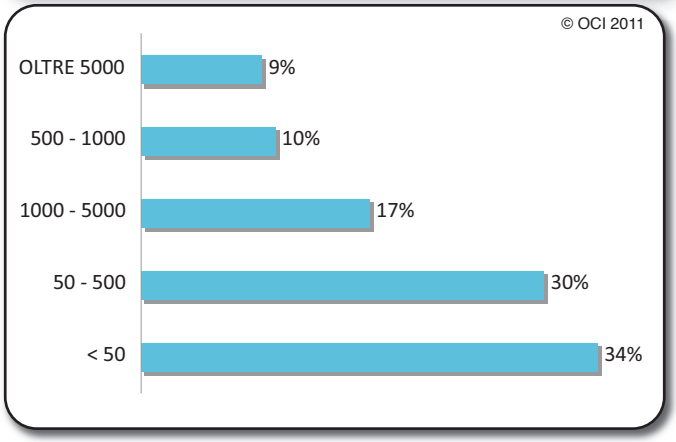


FIG. 4 - Ripartizione del campione per copertura geografica del sistema informatico

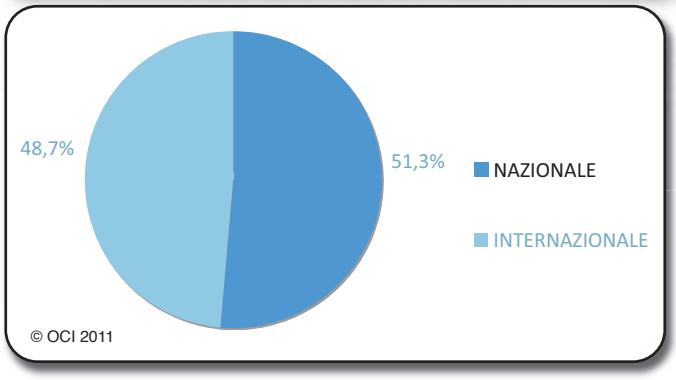


FIG. 5 - Ripartizione del campione per numero di server

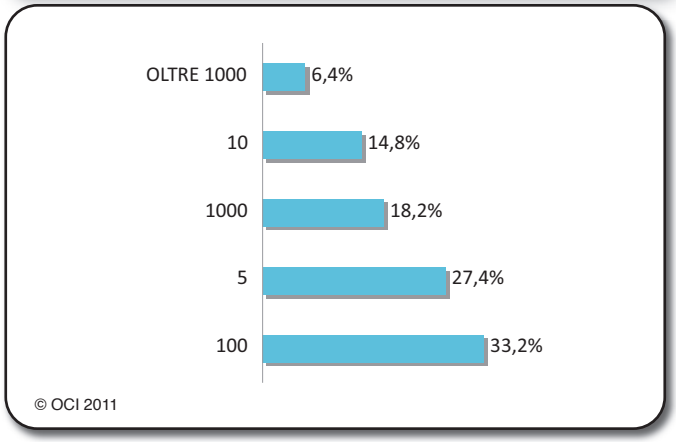


FIG. 6 - Ripartizione del campione per numero di posti di lavoro fissi per sistema informatico

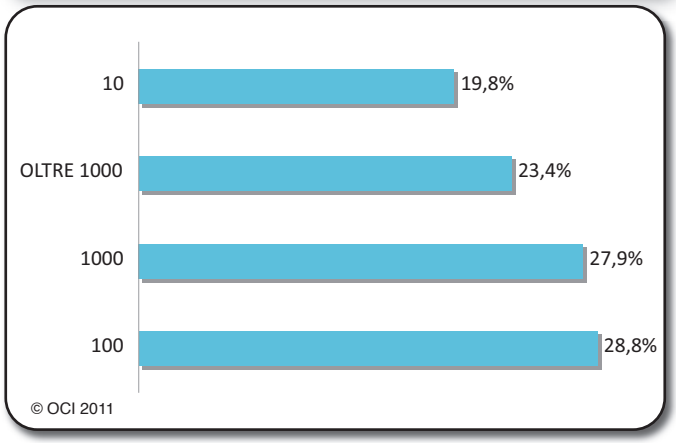
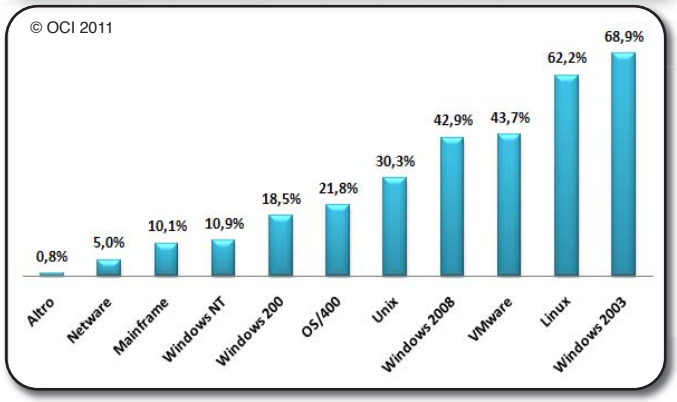


FIG. 7 - Ripartizione del campione per tipo di sistema operativo dei server



duata dal numero di server e di posti di lavoro, dai sistemi operativi e dai database in uso.
L'area geografica di estensione dei sistemi ICT censiti è per poco più della metà (51,3%) solo a livello nazionale, come è riportato in fig.4, ma il resto ha una copertura internazionale, sia in Europa che nel resto del mondo (48,7% dei rispondenti).
Le figg. 5 e 6 mostrano rispettivamente il numero di server e il numero di posti di lavoro per sistema censito. La maggioranza delle risposte riguarda sistemi di piccole-medie dimensioni, con 1-10 server e fino a 100 posti di lavoro. È il tipico ambiente informatico di una PMI, Piccola Media Impresa, e tale dato conferma la tipologia prevalente di aziende che hanno risposto, indicata nella precedente fig.2 e che costituiscono la maggior parte del tessuto economico italiano.

La fig.7 sintetizza le tipologie di sistema operativo per server in uso. Le risposte potevano essere multiple e la percentuale indicata per ogni sistema operativo rappresenta quanti hanno in uso quel sistema operativo sul totale del campione posto a 100. La quota maggiore è costituita dai sistemi Windows di Microsoft, con una larga diffusione di Windows 2003 che di poco sopravanza la percentuale di possessori di sistemi Linux. Significativa la diffusione dei sistemi di virtualizzazione VMware, con un 43,7%, che è indice del consolidamento e della razionalizzazione dei Data Center. Alta anche la percentuale dei server Windows 2008, indice di un buon livello di aggiornamento tecnologico, cui però fa da contraltare un

FIG. 8 - Ripartizione del campione per tipi di DataBase in uso

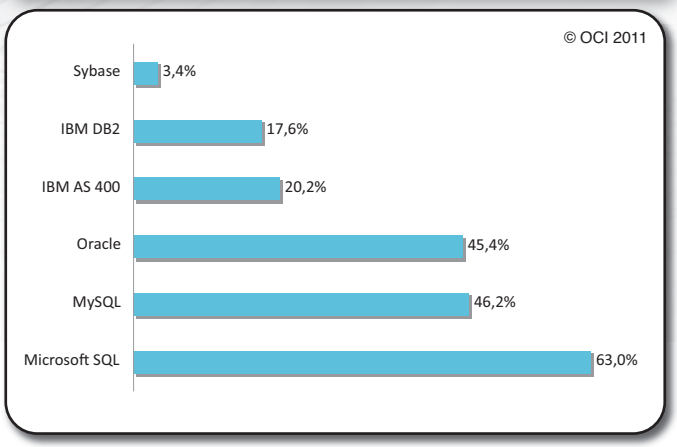
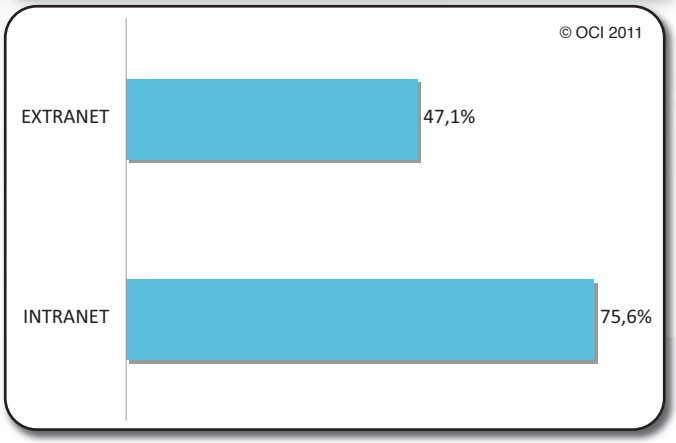


FIG. 9 - Tipologia delle reti in uso



10,9% degli ultra obsoleti NT che costituiscono un elemento di alta vulnerabilità per l'intero sistema informativo. Tipica della situazione italiana è la presenza di numerosi AS 400, molto diffusi nelle PMI di fascia alta, con un 21,8% di OS 400 e la presenza di mainframe come "host" centrale tipica delle grandi strutture quali banche e PA. La figura fornisce l'indicazione di un parco server eterogeneo, con la presenza di diversi ambienti per sistema informativo, ma prevalentemente aggiornati. L'omogeneità dei sistemi è prevalente solo nelle strutture piccole o piccolissime: tipicamente chi sceglie Windows non utilizza Linux e viceversa.

Congruentemente con la tipologia di sistemi operativi delle banche dati, riportata in fig.8, il database (DB) più diffuso nel campione dei rispondenti è Microsoft SQL, che distanzia il secondo più diffuso, l'open source MySQL, che sopravanza di poco Oracle.
La presenza di mainframe IBM e di AS/400 porta alla conseguente presenza dei DB tipici per questi ambienti, l'IBM DB2 e il IBM AS/400.
Data la prevalenza di ambienti eterogenei, nello stesso sistema informativo sono presenti diversi DB: nei mainframe sono spesso presenti sia DB2 che Oracle.
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 e/o Unix/Linux.

Per quanto riguarda le reti, considerando che tutti i sistemi informatici sono connessi ad Internet, la fig.9 evidenzia quanti hanno una intranet, più del 75% del campione, e quanti anche una extranet, il 47,1%. La fig.10 mostra la diffusione nei sistemi informativi delle reti wireless: il 68% con WiFi e il 26,1 % con UMTS (risposte multiple). La presenza di reti wireless, più o meno integrate con il resto del sistema informatico, 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. Circa la metà usa poi VoIP, Voice over IP, confermando la maturità per l'innovazione tecnologica del campione di aziende/enti che hanno partecipato all'indagine.
Nella fig.11 sono indicate le tecniche di sicurezza usate nelle reti: il 69,7% utilizza VPN, Virtual Private Network, per i collegamenti crittati con dispositivi e interlocutori remoti, mentre il 68,9% usa tecniche SSL/TSL per la crittografia dei collegamenti per l'accesso ai siti web. Data la diffusa e gratuita disponibilità di tali strumenti nei moderni browser, il dato è da considerarsi critico: significa che circa il 30% dei sistemi considerati non utilizza collegamenti crittati per collegamenti HTTP su Internet per transazioni critiche, quali quelle con le banche.

FIG. 10 - Tecnologie wireless in uso

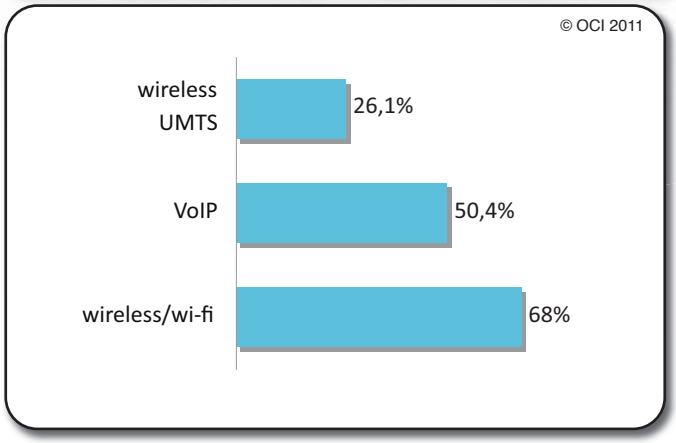
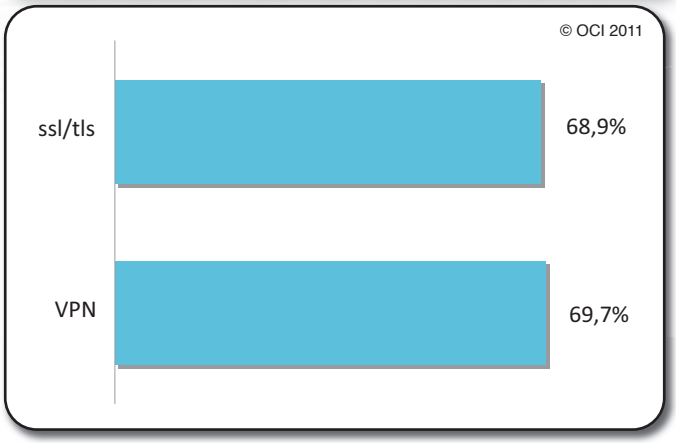


FIG. 11 - Principali tecniche di sicurezza delle reti in uso



La fig.12 mostra come i Data Center dei sistemi informatici dei rispondenti siano per la maggior parte gestiti internamente (on premise) e solo il 24,8% terziarizzati. Quest'ultimo dato è un chiaro indicatore della perdurante riluttanza in Italia a passare a forme di "sourcing", nonostante la forte pressione commerciale e di mercato per il Cloud Computing: i problemi di sicurezza e disponibilità, talvolta presunti, sono un fattore di freno. Il dato del 24,8% risulta comunque migliorativo se confrontato con quello dell'edizione precedente, che era pari al 14%.

Il questionario della presente edizione ha aggiunto domande sui sistemi di produzione e di controllo, come i sistemi SCADA: la parte del sistema informatico dedicata al controllo dei temi non considerati nella precedente edizione, ma che risultano molto critici in termini di sicurezza, come dimostrato dagli attacchi STUXNET ai sistemi di controllo delle centrali nucleari (per approfondimenti si veda l'articolo citato in § 10.5.

La fig.13 mostra che solo il 13,4% del campione ha sistemi di questo tipo, che tecnologicamente si basano,

FIG. 12 - Ripartizione del campione per gestione interna o terziarizzata del/dei Data Center

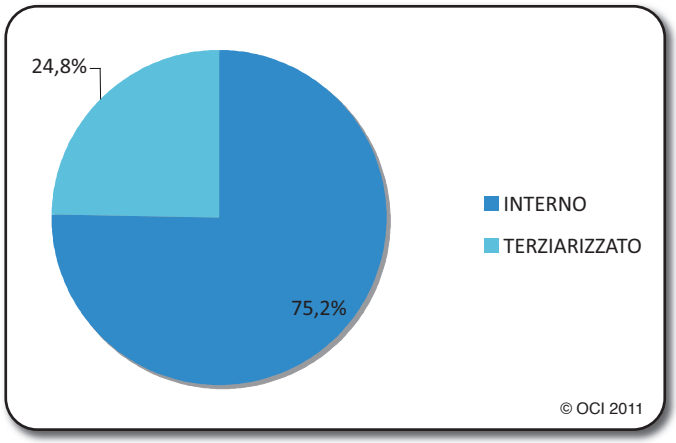
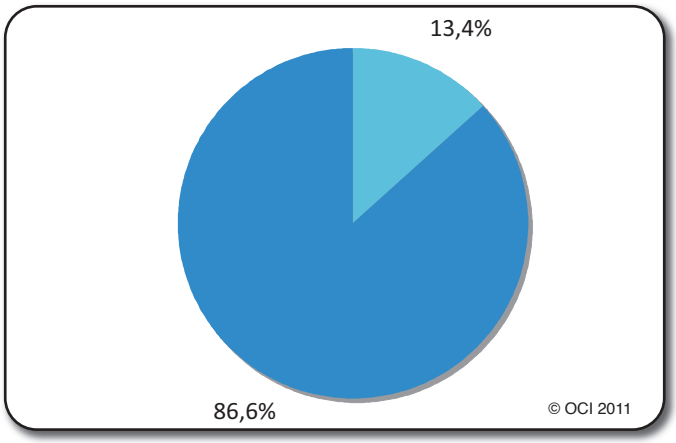


FIG. 13 - Ripartizione del campione per uso ICT nei processi di controllo e produzione



come indicato nella fig. 14, al 50% su ambienti Microsoft Dot.Net e per il 16,7% su ambienti Java.
La fig.15 mostra come questi sistemi di controllo sono in grande maggioranza, con una percentuale del 67%, connessi e quindi integrati con la intranet, mentre il resto opera isolatamente e non collegato con il sistema informativo.

FIG. 14 - Ripartizione del campione per tipologia sistemi di controllonei processidi produzione

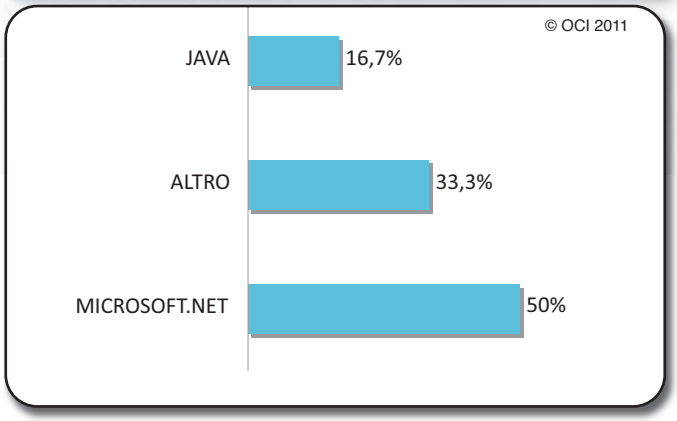
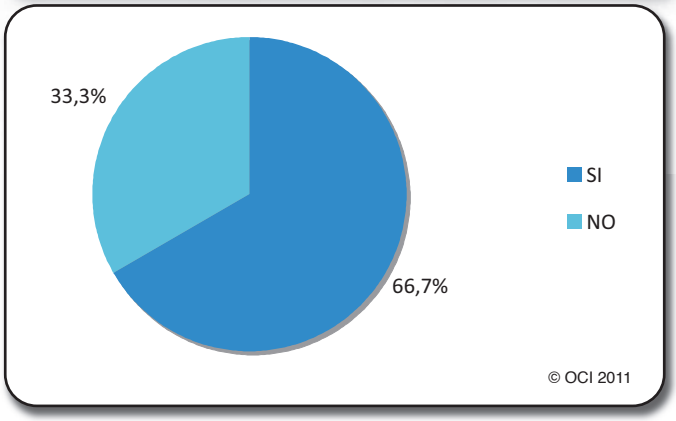


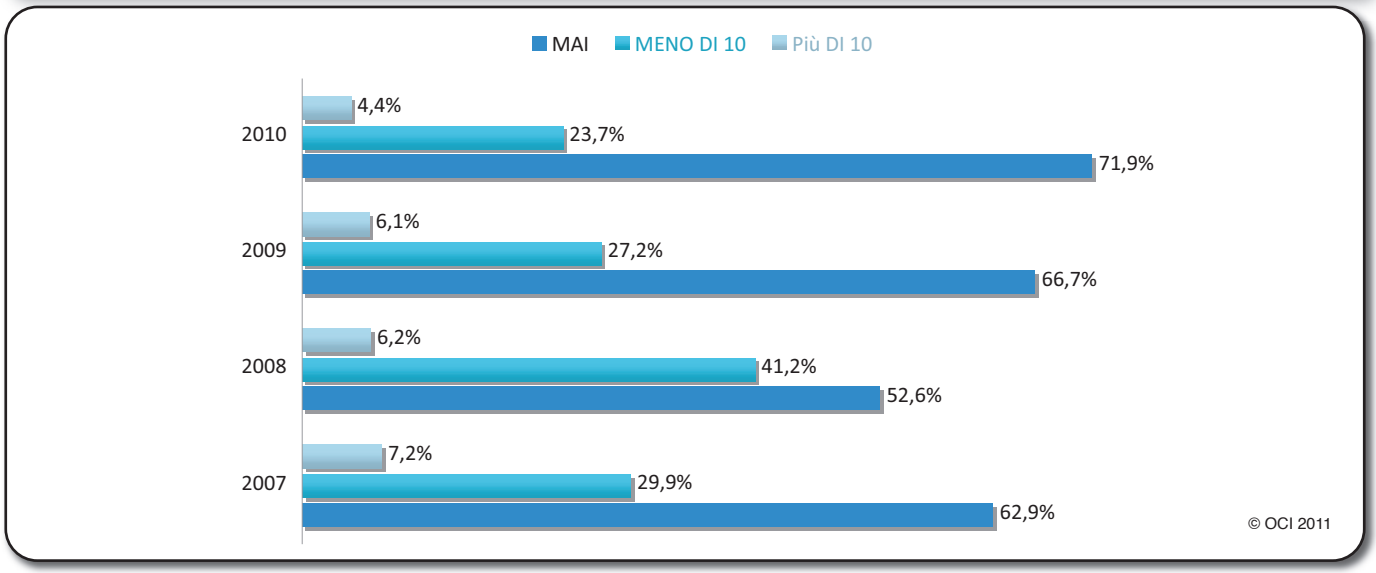
FIG. 15 - Connessione sistemi controllo al sistema informativo



5. Gli attacchi informatici rilevati e la loro gestione

La fig.16 rappresenta la sintesi dei diversi Rapporti OAI dal 2007 al 2010 (primo quadrimestre) in termini di attacchi subiti in percentuale sul campione considerato. Il grafico mostra un continuo miglioramento, a parte l'anno nero 2008, per la diminuzione degli attacchi. Dal 2008 sono anche diminuiti gli attacchi ripetitivi. A fronte di questo miglioramento complessivo, confermato anche dal più ampio e migliore utilizzo degli strumenti di prevenzione e

FIG. 16 - Numero attacchi complessivi 2007/2010



protezione (si veda § 6), è aumentata la gravità e l'impatto, anche economico, degli attacchi riusciti in talune grandi aziende.
La fig.17 sintetizza complessivamente gli attacchi maggiormente subiti nell'arco temporale considerato, indipendentemente dal numero di ripetitività.
La fig.18 infine mette a confronto gli attacchi subiti dal 2008 al 1° quadrimestre 2010 e chiaramente evidenzia come i singoli attacchi siano nel tempo scesi percentualmente, pur sapendo che i tentativi di attacchi sono in crescita come numero, tipologia e complessità. Questo significa che, sull'insieme del campione, le misure di prevenzione e protezione messe in atto hanno contrastato efficacemente gli attacchi.
A questo si deve aggiungere che è cresciuta negli utenti la consapevolezza e la sensibilità sul problema della sicu-

FIG. 17 - Principali attacchi subiti

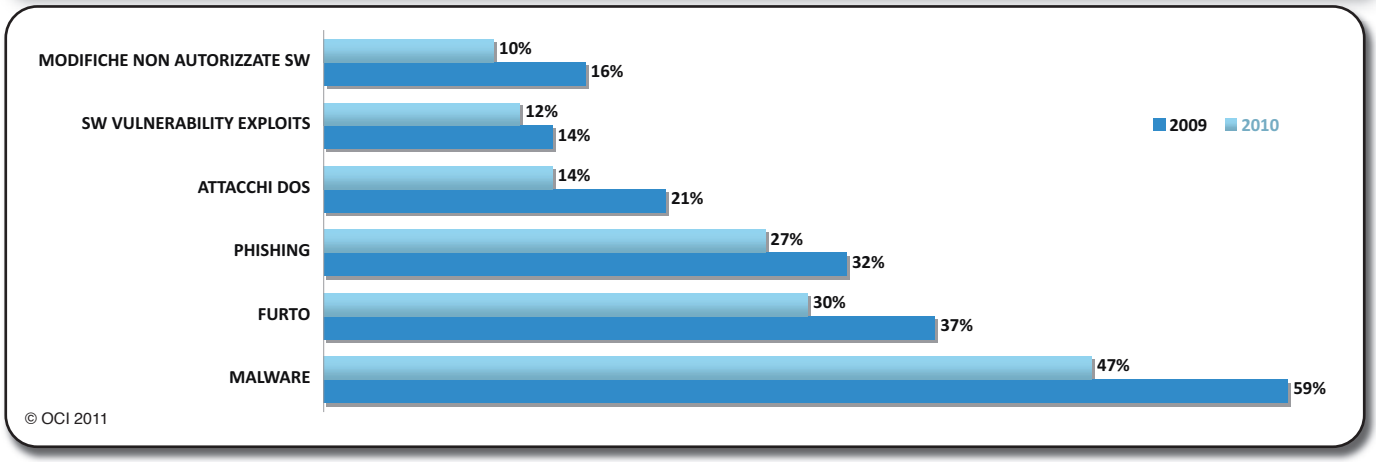
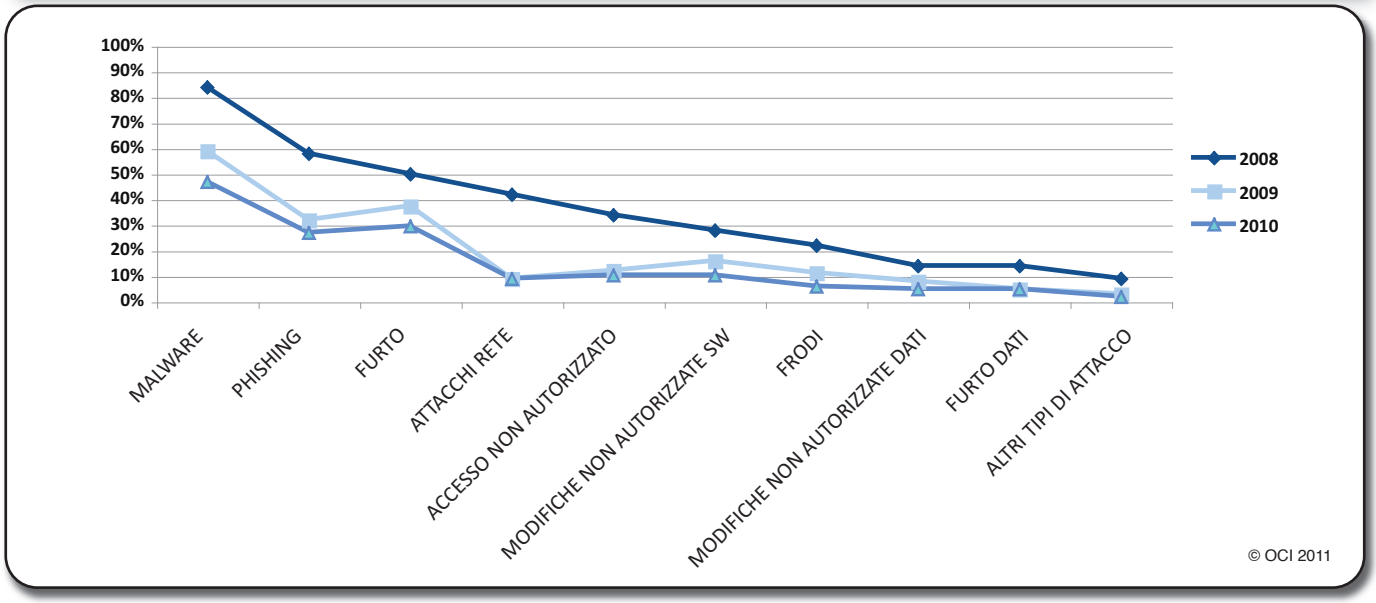


FIG. 18 - Confronto principali attacchi subiti 2008/2010



rezza nell'uso degli strumenti informatici. Si noti che i tipi di attacco in ascissa non sono nell'ordine dal più alto al più basso per quanto riguarda il 2009. La figura è corretta e congruente con la fig.16.

Molte sono le considerazioni che si possono trarre da un'attenta analisi delle citate figure; nel seguito ci si focalizzerà soprattutto sulla diffusione dei tipi di attacco tra il campione considerato e sulla ricorrenza di più di 10 attacchi dello stesso tipo per singolo sistema informativo.

I codici maligni, chiamati anche con il termine inglese di malware, risultano ancora in testa alla classifica degli attacchi più diffusi: il 46,6% dei rispondenti ha subito un attacco di questo tipo, ma il dato è migliorato rispetto all'84% rilevato nella precedente edizione di OAI relativa al 2008. Si è quasi dimezzata la percentuale, sicuramente grazie ad un miglior uso degli strumenti di prevenzione, ma il fenomeno rappresentato dai codici maligni nelle sue varie forme rappresenta, non solo per l'Italia, un dato molto preoccupante, nonostante l'uso diffuso di antivirus e antispyware.
Il termine "codice maligno" include un vario insieme di programmi sviluppati e diffusi con il solo scopo di provocare danni ai computer sui quali sono attivati. Spesso i malware sono genericamente indicati come virus, ma i virus sono solo uno dei tipi di codici maligni; altri tipi sono 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. Si deve però tener conto che non esiste una chiara nomenclatura standardizzata su tali termini e talvolta essi vengono usati con significati diversi dagli stessi fornitori di "antimalware" a fini commerciali e di marketing, con la conseguente confusione terminologica che ne deriva.
Per tale motivo nel questionario OAI si è preferito usare il termine generico di "codice maligno" e di non entrare nel dettaglio dei vari tipi.
Come approfondito in § 10.1, i codici maligni si basano soprattutto sulle vulnerabilità dei programmi software, che a loro volta rappresentano una debolezza "intrinseca" e "fisiologica" di qualsiasi artefatto umano. Talune vulnerabilità non sono eliminate da patch e fix in tempi brevi, e talvolta gli aggiornamenti per eliminarle ne introducono di nuove.

Alcuni rapporti internazionali hanno approfondito il tema dei codici maligni, e tutti confermano i trend di vulnerabilità che si estendono anche alle nuove tecnologie, per esempio ai sempre più diffusi sistemi virtualizzati, come approfondito nell'articolo citato in § 10.7.
Si confermano quindi le considerazioni già espresse nel precedente Rapporto:

- la maggior parte delle vulnerabilità possono essere sfruttate da remoto via rete;
- i tempi per la correzione delle vulnerabilità sono, per taluni casi, lunghi e possono superare un intero anno;
- le maggiori vulnerabilità, sia in numero che in gravità, riguardano sempre più gli ambiti (piattaforme) web e soprattutto le applicazioni web personalizzate; in tale contesto gli attacchi si basano prevalentemente su SQL "injection" oltre che su XSS (cross-site scripting);
- molte vulnerabilità sono causate da uno sviluppo del software personalizzato e senza competenza e sensibilità sulla sicurezza, come approfondito nell'articolo citato in § 10.2;
- le maggiori vulnerabilità per le stazioni di lavoro sono nei browser, nelle applicazioni multimediali come Flash e nei lettori (gratuiti) dei principali formati testuali, come Acrobat Reader per i formati .pdf, come approfondito nell'articolo citato in § 10.4;
- richiedono particolare attenzione le vulnerabilità dei sistemi VoIP e wireless, come approfondito nell'articolo citato in § 10.3.

Tornando alla "classifica" in fig. 17, al secondo posto per diffusione si trovano i furti di dispositivi ICT, tipicamente i PC laptop e gli smartphone: essendo piccoli e portatili, essi hanno un fiorente mercato "dell'usato" e sono facilmente sottraibili, dato che si possono nascondere banalmente in una borsa, in una tasca o sotto una giacca. La maggior parte dei professionisti ha uno o più smartphone e porta sempre con sé il proprio laptop (ed ora stanno crescendo i tablet) tra casa e luoghi di lavoro. Oltre ai dispositivi intelligenti, PC-tablet-smartphone, le chiavette per hard disk removibili sono ulteriori dispositivi di potenza crescente (si arriva ora ai tera) e facilmente sottraibili o smarribili.
Nella precedente edizione del rapporto i furti erano classificati al terzo posto: la forte crescita dei dispositivi mobili

ha fatto compiere un passo in avanti a questo tipo di attacco assai "tradizionale".
Al terzo posto di questa graduatoria una specifica forma di social engineering assai diffusa in Italia: il phishing. In ogni modo la percentuale del 37% nel 2009 è ben migliore del 50% nel 2008, che includeva però tutte le forme di social engineering. Nel complesso questi dati migliorativi sono confermati dai dati del 2010, anche se relativi al solo 1° quadrimestre. Tale riduzione è sicuramente indicativa del fatto che l'utenza finale inizia ad essere consapevole dei pericoli derivanti da questi tipi di "tentata truffa" e sufficientemente matura per non cascarci. Anche per il 2009-10, come negli anni precedenti, la quasi totalità del phishing riguarda il contesto finanziario.
Gli attacchi di tipo DoS e DDoS continuano ad avere una certa rilevanza e diffusione, collocandosi al 4° posto con un 21% nel 2009.
Tutti gli altri 9 tipi di attacchi su un totale di 13 sono al disotto del 20% del campione, con un miglioramento globale rispetto al precedente rapporto, che nel 2008 vedeva solo 5 tipologie al di sotto del 20%, su di un totale di 12. Questa tendenza di nuovo conferma che le misure di sicurezza tecniche ed organizzative messe in atto, oltre alla sensibilizzazione ed alla formazione degli utenti, forniscono evidenti risultati positivi.

Significativo, negli ultimi anni, il crescere di attacchi complessi, molteplici e persistenti, soprannominati APT, Advanced Persistent Threat. Sono attacchi specifici per un determinato sistema informatico, che quindi presuppongono una sua specifica e dettagliata conoscenza, costituiti da un insieme parallelo e complementare di strumenti (social engineering, codici maligni, backdoor, SQL Injection, ecc.) che cercano di colpire in più punti l'obiettivo, e che durano nel tempo, in quanto cercano di individuare i punti deboli della difesa e di superarli con le diverse tecniche di cui dispongono. Per un approfondimento sugli ATP si rimanda all'articolo citato in § 10.8.
Un dato interessante è, nel complesso, la bassa percentuale di frodi informatiche dichiarate dal campione, che all'incirca la metà rispetto al 22% della scorsa edizione. Questo dato, che sembra essere in contrasto con quanto evidenziato dalla stampa e da questo stesso rapporto,non deve trarre in inganno. La rilevazione tiene conto del numero di frodi, non della loro gravità e del loro impatto sull'azienda/ente: il trend è che le frodi diminuiscono come numero, ma crescono come gravità e come incidenza economica sull'attaccato.

Per quanto riguarda l'aspetto dell'iterazione dell'attacco nel medesimo anno, l'analisi dei dati mostra che le ripetizioni numericamente più significative riguardano i codici maligni ed i furti, come d'altronde è facilmente prevedibile. Anche per le ripetizioni la situazione del 2009-10 è nettamente migliorata, essendo minore rispetto a quella del 2007-08.

Le figure dalla 19 alla 23 dettagliano i tipi di attacchi subiti per macro settore. Tale analisi non era presente nel precedente rapporto, ma si è ritenuto opportuno effettuarla per poter verificare se taluni attacchi sono più o meno tipici e significativi per un determinato settore o un altro. I dati elaborati devono essere considerati come indicatori qualitativi, dato che come già evidenziato in § 4, taluni settori, in particolare PAC/PAL e settore bancario-finanziario, hanno fornito un numero limitato di risposte. E proprio i dati di questi due settori evidenziano alcune differenze e scostamenti rispetto agli altri settori.

I settori industri e servizi, come mostrano le fig.19 e 20, hanno andamenti simili: al primo posto con il 60% i codici maligni, cui seguono i furti di apparati con il 31 e 32 % rispettivamente, ed il phishing con il 16%.

Il settore ICT, riportato in fig.21, già mostra tipologie e percentuali diverse: al primo posto sempre il malware, ma solo con il 37%. Al secondo posto si classifica il phishing con un 21%, al terzo posto, a pari merito al 14%, gli attacchi DoS/DDoS e alle reti.
Nel complesso il campione delle aziende ICT ha una percentuale di attacchi mediamente inferiore agli altri settori a parte gli attacchi alle reti, indicatore di un probabile forte uso di connessioni da remoto sia wired che wireless.

Ulteriormente diversi i dati emersi da PAC/PAL (fig.22) e dagli ambiti finanziari ed assicurativi (fig.23). Per PAC/PAL la tipologia più diffusa d'attacco è il phishing, con un elevato 70%, cui segue il malware al 65% e le

FIG. 19 - Attacchi subiti per macro settore - INDUSTRIA

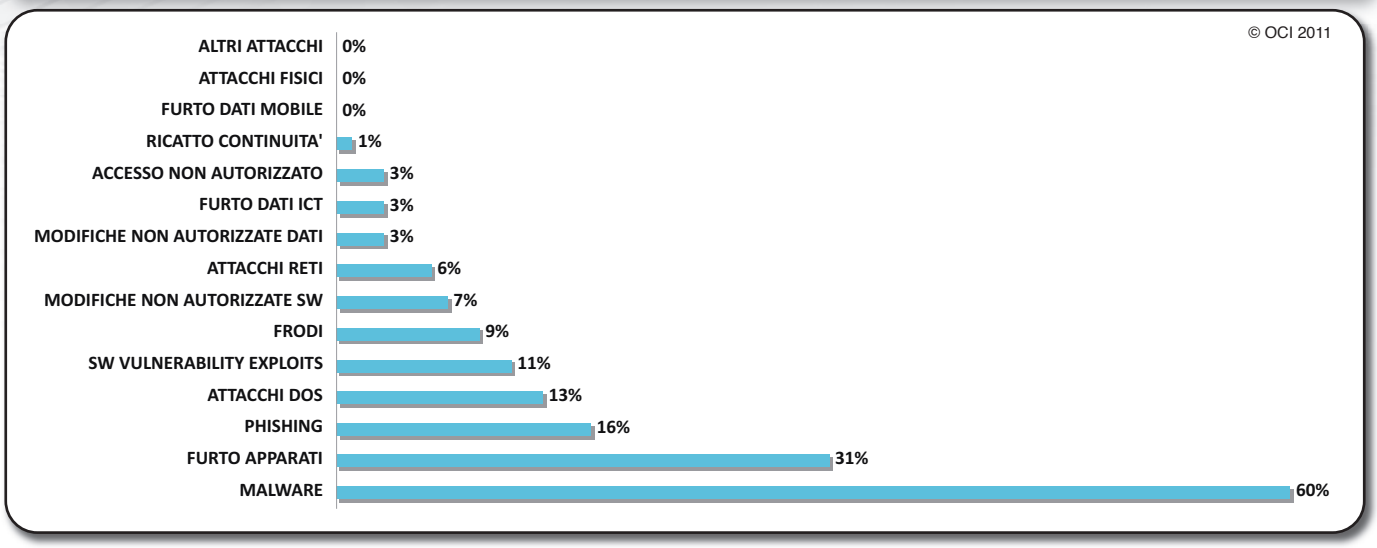
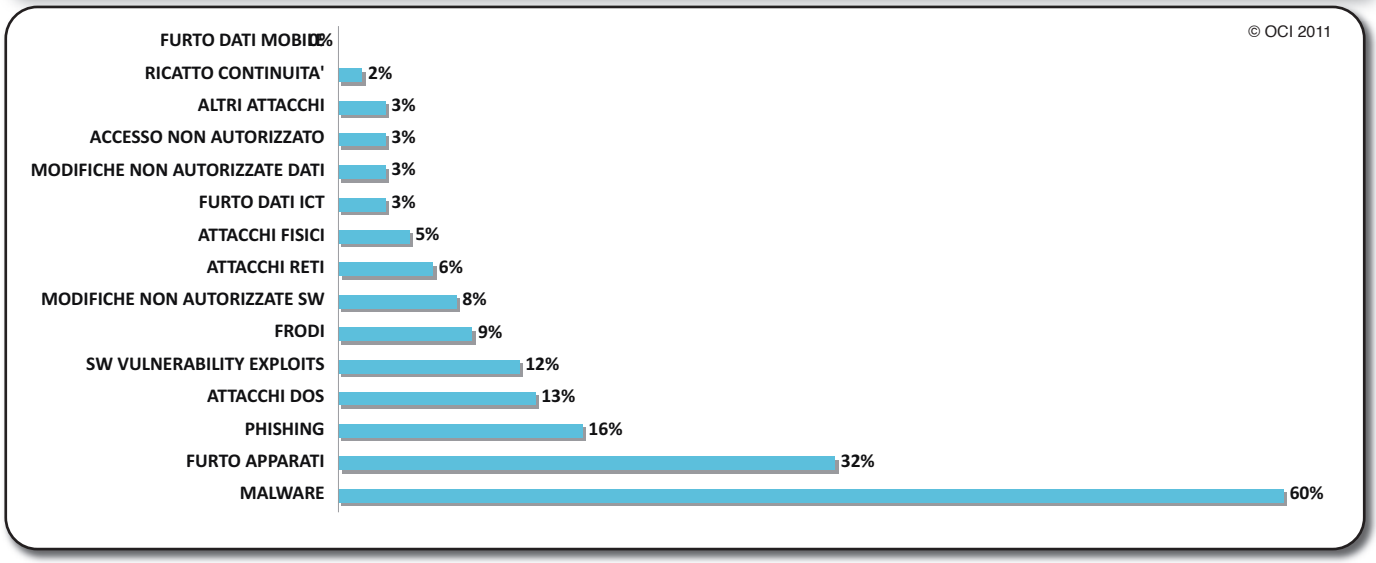


FIG. 20 - Attacchi subiti per macro settore - SERVIZI



frodi al 45%. Anche le altre tipologie di attacco hanno percentuali elevate, ad eccezione delle frodi e dei ricatti sulla continuità operativa che i rispondenti non hanno rilevato. I dati emersi per questo settore evidenziano un livello di sicurezza, ma soprattutto di formazione degli utenti, inadeguato, come il 70% di phishing rileva, almeno per quanto riguarda i pochi enti che hanno risposto.

Il settore bancario-finanziario vede al primo posto i codici maligni con un 70%, cui segue con un 60% il furto di apparati e con il 50% gli attacchi DoS/DDoS. Altre 6 tipologie di attacco non hanno avuto alcuna rilevazione. Balza all'occhio l'alto numero di furti di apparati ICT, con una percentuale che non si immaginerebbe in uffici ed ambienti che si presume dovrebbero essere ben protetti.

FIG. 21 - Attacchi subiti per macro settore - ICT

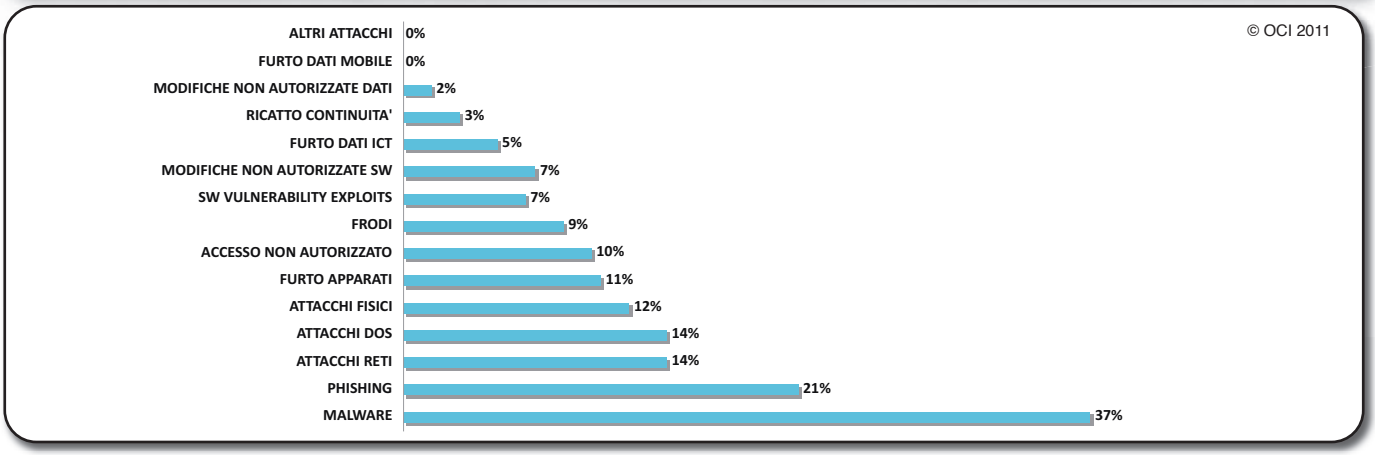


FIG. 22 - Attacchi subiti per macro settore - PAC e PAL

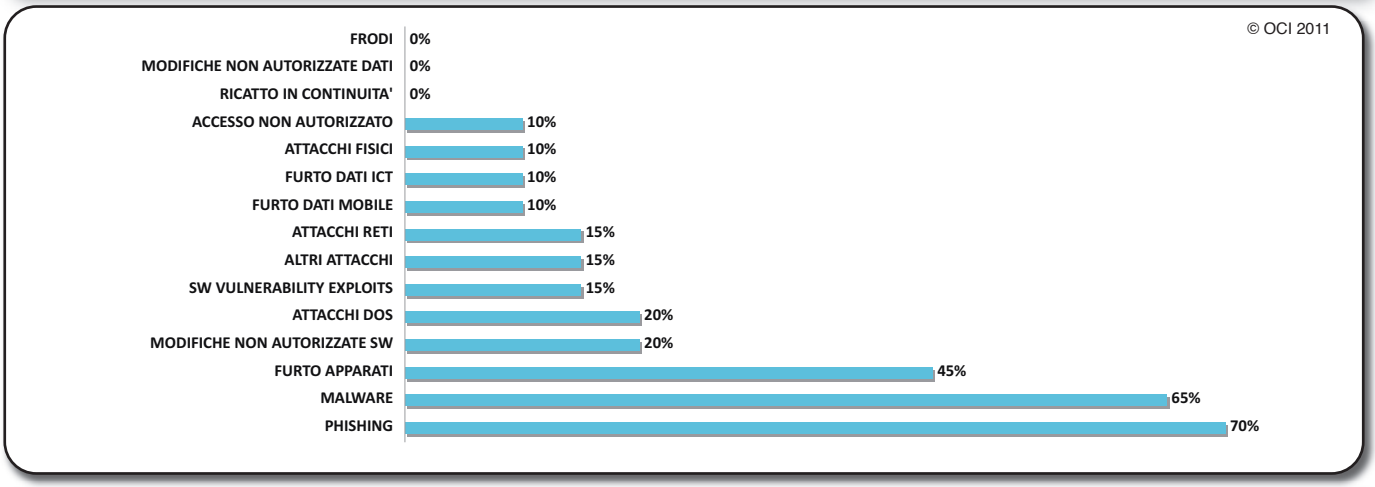
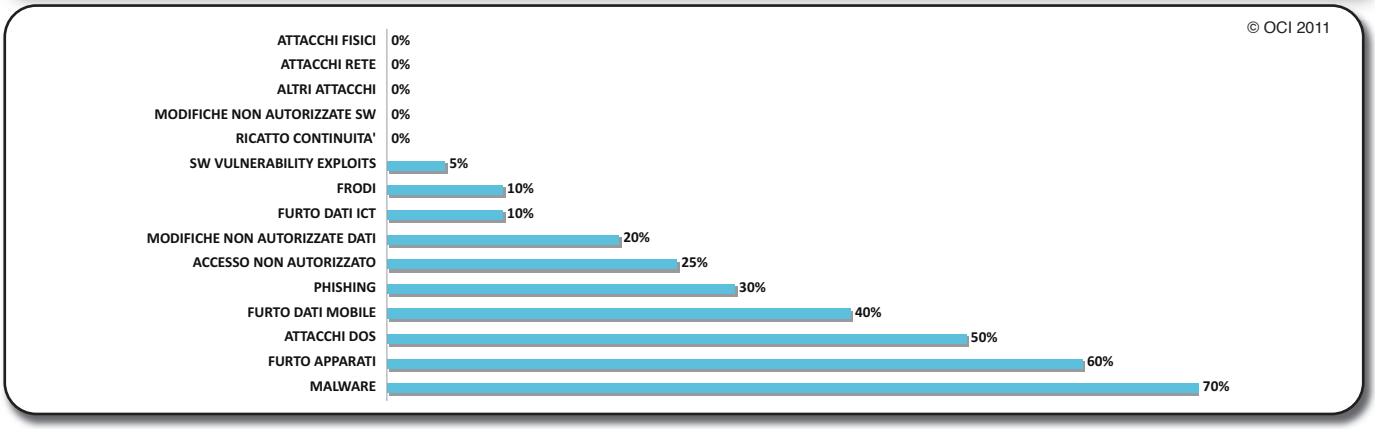


FIG. 23 - Attacchi subiti per macro settore - ASSICURAZIONI & FINANZA



5.1 Rilevazione, valutazione e gestione degli attacchi

Nella Sezione 2 del questionario sono poste alcune domande su come l'azienda/ente rilevi, valuti e gestisca l'occorrenza di attacchi.
Purtroppo, come nel precedente Rapporto, pochi compilatori hanno risposto alla domanda sulla provenienza delle segnalazioni di un attacco, probabilmente perché nella maggior parte dei casi non vengono individuate e registrate. Il risultato in % delle poche risposte ricevute sul totale dei rispondenti, è raffigurato nella fig.24 e risulta plausibile e ragionevole: le rilevazioni arrivano prevalentemente dai sistemi di monitoraggio e controllo, e a queste seguono le segnalazioni dirette provenienti dagli utenti che si accorgono di malfunzionamenti, furti o di dati impropriamente manipolati.

La fig. 25 mostra, in percentuale, i principali criteri con i quali viene valutata la criticità e quindi la gravità dell'attacco. Le risposte sono multiple.

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. Con percentuali simili sono poi considerati i costi derivanti dalla non conformità alle leggi vigenti (compliance) e dalla perdita d'immagine. 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 74% 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% delle risposte che indicano i costi di indisponibilità dell'ICT come il secondo indicatore di gravità. Tra i criteri indicati nel questionario, è significativo che più del 41% delle risposte preveda come ulteriore criterio di valutazione la "compliance" alle normative in vigore. Nel precedente rapporto il valore era intorno al 30%, e l'aumento è un indicatore della maggior consapevolezza, in particolare sulla privacy.
Alla domanda sulla stima del danno economico derivato da uno o da più attacchi riusciti non si è avuta alcuna risposta. Il motivo della mancanza totale di risposte è da un lato da ricercare nella difficoltà di valutazione, oltre che dalla difficoltà di avere l'autorizzazione a fornire, qualora ci fossero, informazioni così delicate e riservate.

Sulla gestione dell'attacco, due le domande nel questionario:
a) è stato comunicato alle autorità competenti, e se no perché?
b) subito l'attacco, in quanto tempo sono state ripristinate le condizioni precedenti?

FIG. 24 - Da dove sono pervenute le segnalazioni di attacco

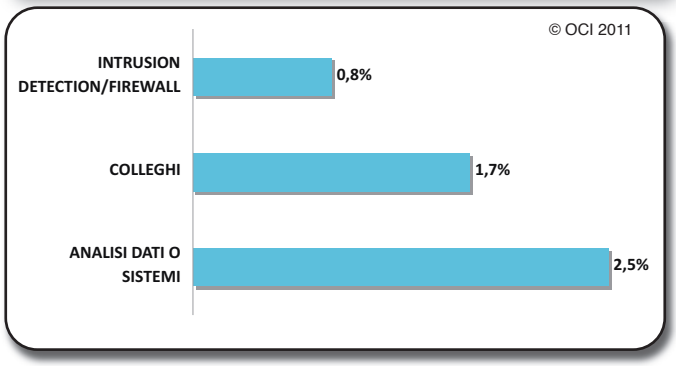


FIG. 25 - Criteri per la valutazione della gravità dell'attacco subito

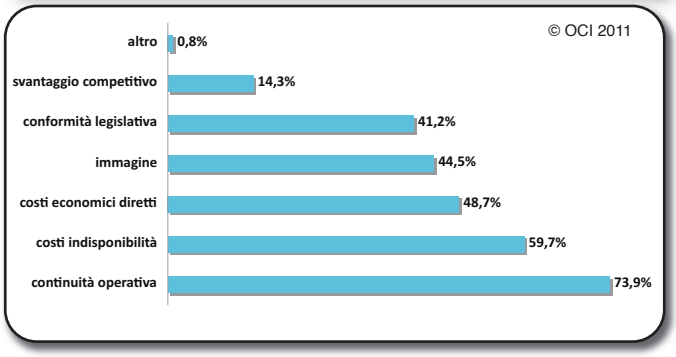


FIG. 26 - Comunicazione attacco all'esterno

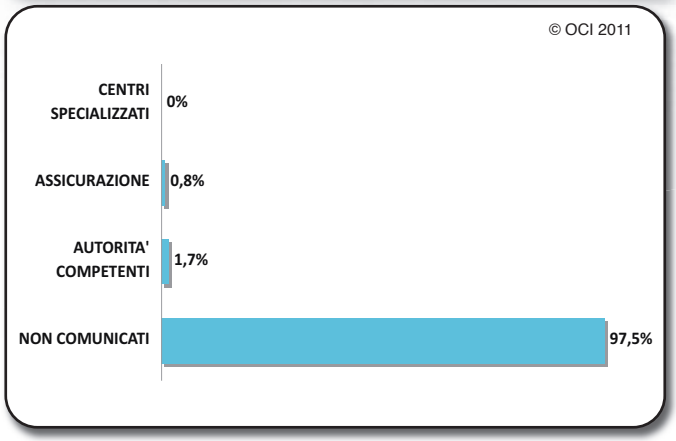
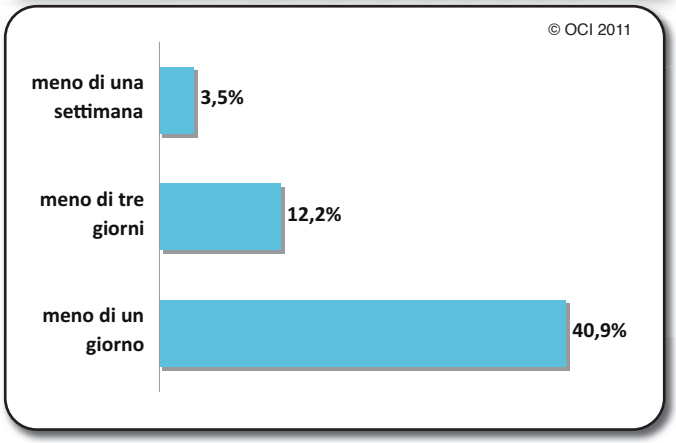


FIG. 27 - Tempo medio occorso per il ripristino dei sistemi ICT a seguito di un attacco



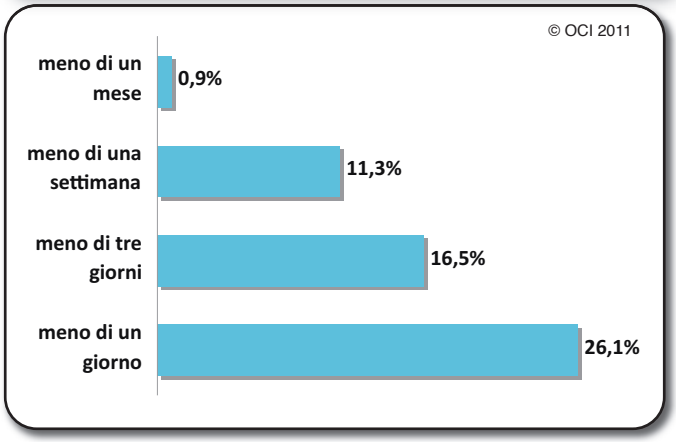
Come evidenziato nella fig.26, la quasi totalità dei rispondenti non comunica l'avvenuto attacco, né alle competenti autorità, né alle assicurazioni (in quanto ancora pochi sono assicurati contro i rischi informatici). Solo una minima parte informa centri specializzati quali il CERT.

Per quanto riguarda i tempi di ripristino a seguito di un attacco, la fig.27 mostra, per i tempi medi, che nella maggior parte dei casi la situazione "ante" è ripresa al massimo in una settimana, e per più del 40 % dei rispondenti in media le conseguenze di un attacco sono ripristinate nell'arco di un solo giorno.

Questi tempi sono confermati anche nel "caso peggiore" occorso, illustrato nella fig.28. Anche nel caso peggiore il sistema è ripristinato quasi sempre entro una settimana. Tali dati confermano ulteriormente che il campione di rispondenti appartiene alla fascia "alta" in termini di attuazione e gestione delle misure di sicurezza ICT. Dall'altro lato è presumibile anche che una buona parte degli attacchi rilevati non ha avuto gravissimi impatti sui sistemi.

In entrambe le figg.27 e 28 un'alta percentuale non ha risposto alla domanda, probabilmente perché nessuno registra o prende nota dei tempi, anche approssimativi e qualitativi di ripristino, oppure perché gli attacchi subiti non hanno comportato modifiche al software ed alla sua configurazione.

FIG. 28 - Il caso peggior come tempo di ripristino



6. Strumenti e politiche di sicurezza ICT adottate

Rispetto al questionario e al Rapporto della scorsa edizione, il capitolo sugli strumenti di prevenzione e protezione è stato articolato dettagliando maggiormente sia gli aspetti tecnici che quelli organizzativi.

6.1 Sicurezza fisica

La fig.29 schematizza le principali misure in uso, con risposte multiple: le percentuali sono buone per tutte e tre le

FIG. 29 - Strumenti usati per la sicurezza fisica

macro aree considerate. Più del 90% dei rispondenti è dotato di sistemi per garantire la continuità elettrica, l'84% dispone di protezioni perimetrali ed effettua controlli degli accessi alle persone fisiche, più del 75% ha i locali del Data Center climatizzati. Tali percentuali confermano che il pur variegato campione di rispondenti appartiene alla fascia medio-alta in termini di sicurezza informatica.

6.2 Sicurezza logica

Gli strumenti per la sicurezza logica si differenziano in funzione delle unità ICT da proteggere.
A livello di reti, come indicato nella fig.30, la quasi totalità dei rispondenti è dotato di dispositivi firewall e di DMZ, DeMilitarized Zone, con una forte crescita rispetto al 47% della precedente edizione. Per proteggere le comunicazioni da remoto, l'80% dichiara di utilizzare soluzioni VPN. Tale dato differisce dal 70% circa indicato nella fig.11, ma indica comunque un largo uso di VPN nel campione. Significativo che il 47% (contro il 44% della scorsa edizione) abbia potenziato il livello di sicurezza sulle reti wireless, che costituiscono una parte crescente delle tecniche di comunicazione, integrate funzionalmente nella rete complessiva del sistema informativo che tende ad integrare nella stessa infrastruttura ICT, basata su TCP/IP, ogni tipo di informazione.

La fig.31 sintetizza la diffusione dei principali strumenti per la protezione dei sistemi, in particolare dei server. I software antivirus e antispyware sono usati da quasi tutti, il 97%, contro un 95% rilevato nella scorsa edizione . Molto significativo è il fatto che ben il 70% circa dichiari

FIG. 30 - Strumenti usati per la protezione delle reti

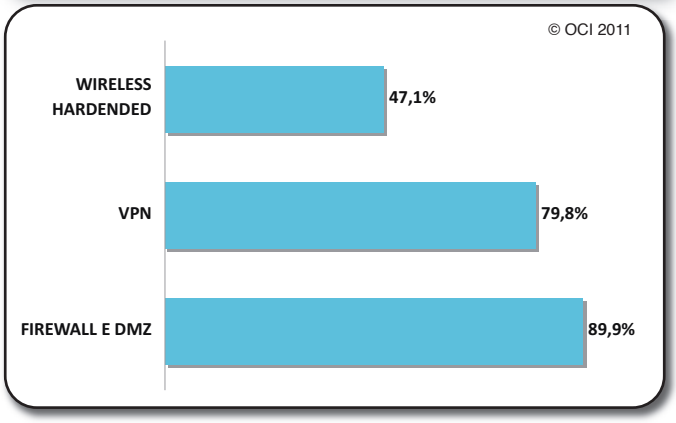


FIG. 31 - Strumenti usati per la protezione dei sistemi

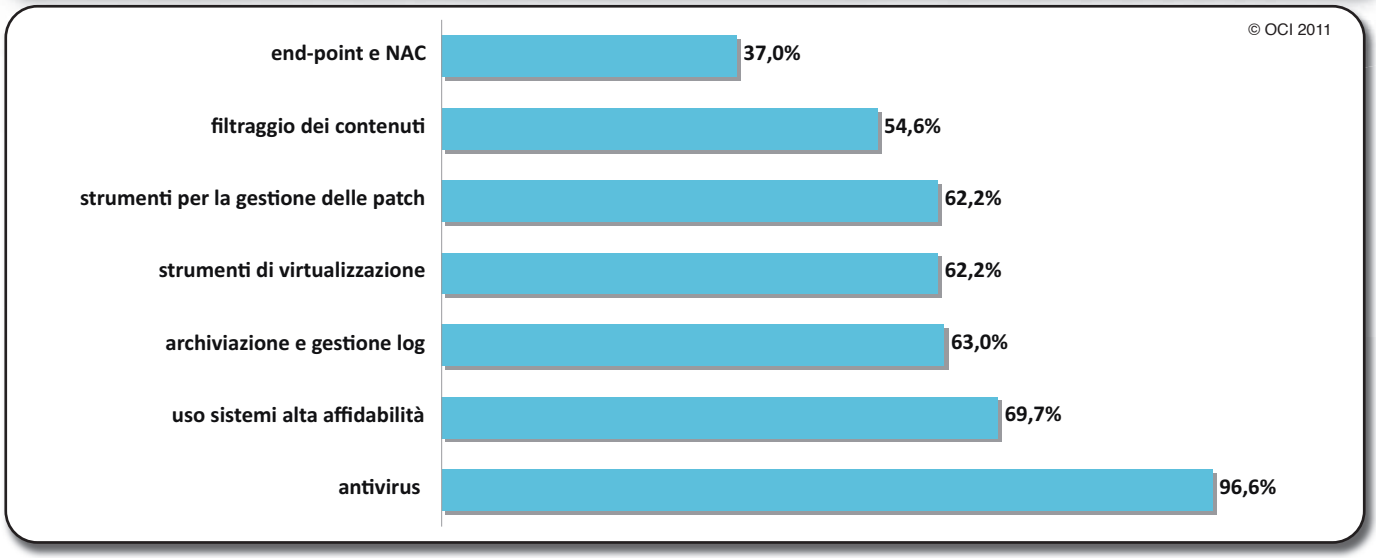
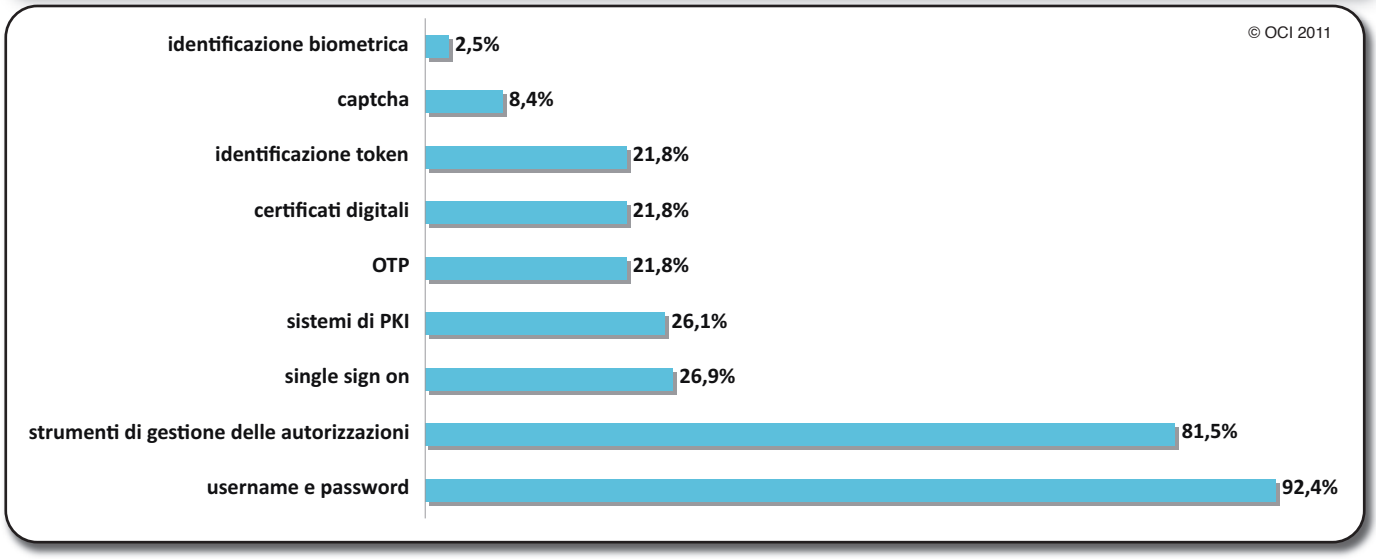


FIG. 32 - Strumenti usati per Identificazione, Autenticazione, Autorizzazione

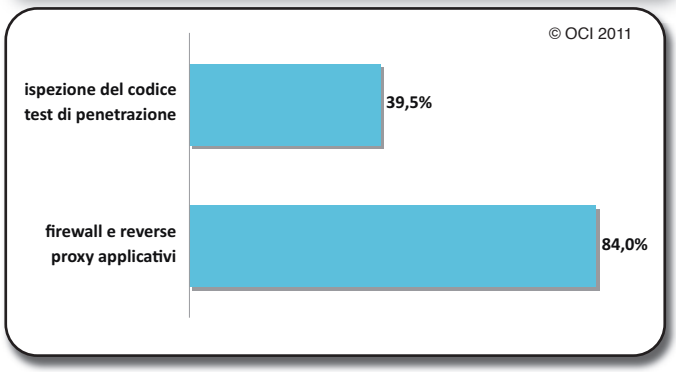


di usare sistemi ad alta affidabilità, quindi ridondati e probabilmente almeno in parte virtualizzati, contro il 47% della scorsa edizione.
Anche per gestire la normativa sugli amministratori di sistema per la privacy, ma non solo, il 63% utilizza sistemi di archiviazione e gestione dei log. Sempre sopra il 60% l'utilizzo di strumenti per l'aggiornamento dei software e delle patch, e a scendere il filtraggio dei contenuti in ingresso e in uscita dalla rete, e i sistemi di sicurezza end-point e di NAC, Network Access Control.
La fig.32 dettaglia i meccanismi usati per l'identificazione, l'autenticazione ed il controllo degli accessi.
Il mezzo più diffuso, con oltre il 92%, è il semplice uso di username e di password per l'identificazione e l'autenti-

cazione di una persona, associato a strumenti di controllo degli accessi e di profilazione dei diritti sugli applicativi, usati dall' 81,5% del campione.
Tutti gli altri meccanismi più sofisticati, dai certificati digitali con PKI, Public Key Infrastructure, al Single Sign On hanno una diffusione molto minore. L'identificazione biometrica, pur avendo fatto passi da gigante negli ultimi tempi sia in termini tecnici che economici (sempre meno cara) è ancora assolutamente embrionale con un 2,52%, valore diverso dal 6% rilevato nello scorso Rapporto e dovuto al mix diverso di rispondenti. Le attuali percentuali, a parte quest'ultima sulla biometria, sono migliorative anche con 5 punti in più, ma rimangono basse e costituiscono un chiaro riscontro di come tali tecniche, anche se ben consolidate, non siano ancora conosciute e accettate, forse anche a causa di una certa complessità per la loro attivazione, gestione e uso da parte degli utenti.

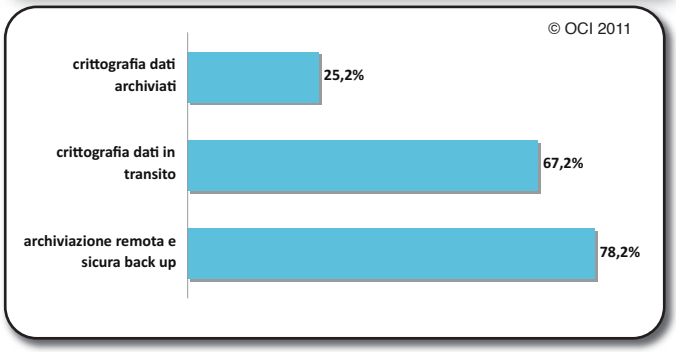
La fig.33 dettaglia l'uso di specifici strumenti per la protezione degli applicativi, oltre alla profilatura dei diritti d'accesso di cui sopra. Gli strumenti più diffusi, con ben l'84%, sono i firewall ed i reverse proxy fisici o logici posti prima degli application e dei data base server, che ulteriormente controllano i diritti di accesso e filtrano i contenuti.
Per garantire la sicurezza "intrinseca" delle applicazioni prima della loro messa in produzione, ed evitare pericolose vulnerabilità, una considerevole parte del campione, il 39,5%, dichiara di effettuare ispezioni sul codice (code inspection) e test di penetrazione per verificare, anche solo a campione, la mancanza di vulnerabilità degli applicativi. Questo è un dato molto importante, soprattutto se confrontato col preoccupante 6% rilevato nella scorsa edizione, in quanto indica che almeno un terzo delle aziende/enti considerati ha preso coscienza delle possibili gravi conseguenze delle vulnerabilità degli applicativi e di conseguenza effettua un qualche controllo (si spera soprattutto prima della loro messa in produzione).

FIG. 33 - Principali strumenti usati per la protezione degli applicativi



Per la protezione dei dati, che costituiscono il reale e più importante "asset ICT" dell'azienda/ente, la fig.34 mostra che una buona maggioranza, il 78%, archivia in maniera sicura le copie di back-up in sedi diverse (remote) dal proprio Data Center, probabilmente anche grazie a fornitori terzi; tale dato corregge l'improbabile 1% rilevato nell'edizione precedente. Va inoltre crescendo l'uso della crittografia per i dati in transito con un significativo 67% rispetto al 42% del precedente rapporto: è un indice della diffusione dei protocolli sicuri https e ftps, disponibili praticamente in tutti i browser ed usati in particolare per transazioni commerciali e bancarie via Internet. Il 25% dei rispondenti utilizza la crittografia per proteggere i dati archiviati, rispetto al 23% precedente.

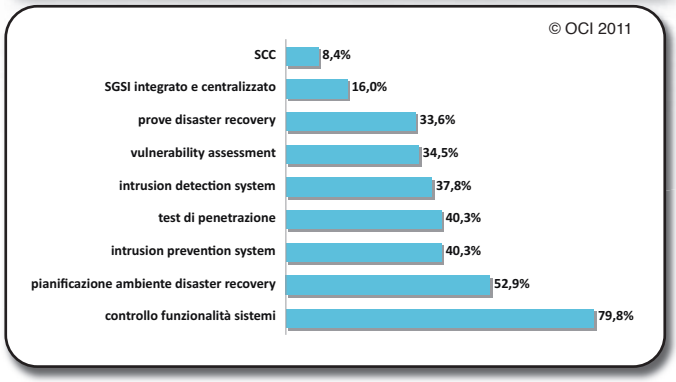
FIG. 34 - Principali strumenti usati per la protezione dei dati



6.3 La gestione della sicurezza ICT

La fig.35 mostra quali strumenti di gestione della sicurezza ICT sono utilizzati, sempre in percentuale sull'intero campione e con risposte multiple: i dati raccolti indicano un miglioramento, rispetto all'edizione precedente, su questo tema essenziale per garantire un livello realmente idoneo di protezione del sistema informativo.

FIG. 35 - Gestione della sicurezza ICT



Il monitoraggio e il controllo delle funzionalità e prestazioni dei sistemi ICT sono in vari modi attuati dall'80% dei rispondenti (rispetto al precedente 58%), ma solo il 16% utilizza un SGSI, Sistema Gestione Sicurezza Informatica, integrato e centralizzato, e solo l'8% fa uso di un SCC, Security Command Center, tipicamente presso società specializzate. Il forte divario tra l'80% ed il 16% significa che la gestione della sicurezza è ancora prevalentemente a isole omogenee, a silos verticali e separati per i diversi ambienti quali ad esempio Microsoft, Linux/Unix, siti web, ambienti ERP, CRM, ecc.

Più della metà del campione, il 53%, ha in essere piani e soluzioni di Disaster Recovery, e il 34% effettua periodicamente prove di ripristino emulando situazioni di disastro. Sistemi di individuazione delle intrusioni (IDS, Intrusion Detection System) sono usati dal 38%, e con 2 punti percentuali in più (dal 40%) i sistemi di prevenzione delle intrusioni (IPS, Intrusion Prevention Systems): numeri non trascurabili che evidenziano come le logiche di prevenzione incomincino ad essere attuate. Tale percentuale è confermata da un 40% che effettua periodicamente test di intrusione, per verificare la tenuta delle misure di sicurezza in atto, e da un 34% che gestisce le vulnerabilità (vulnerability assessment) ed effettua scansioni della rete e dei sistemi per un continuo miglioramento e rafforzamento delle difese (hardening).

Un aspetto importante e propedeutico nella gestione della sicurezza ICT è la sistematica e periodica analisi dei rischi. Il 67% del campione afferma che tale analisi viene effettuata (fig.36), e il 38,6% che viene gestito il rischio residuo (fig.37) ad esempio assicurandosi.

FIG. 36 - Effettuazione analisi dei rischi

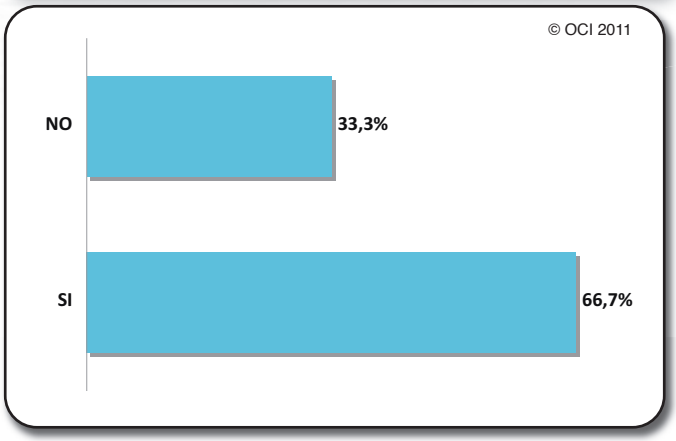
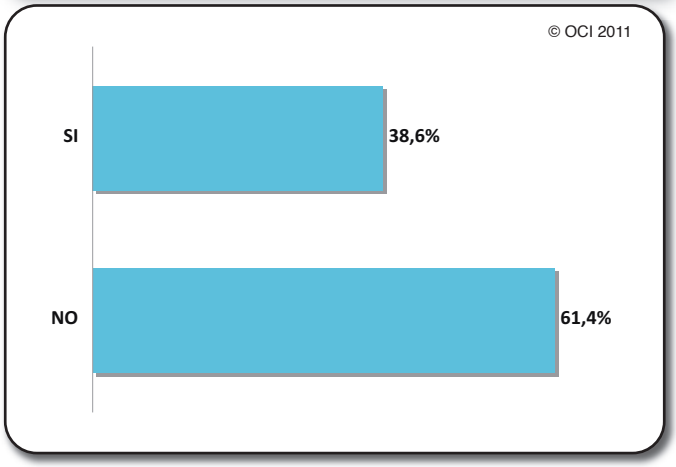


FIG. 37 - Gestione rischio residuo



6.4 Le misure organizzative

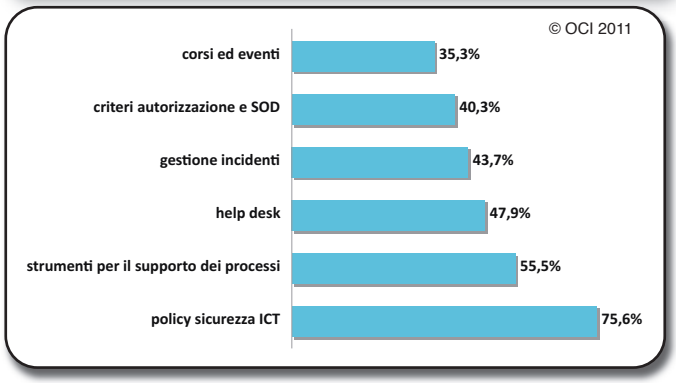
Gli aspetti organizzativi sono determinanti per gestire correttamente ed efficacemente la sicurezza di un sistema informativo: aspetti spesso trascurati, anche perché considerati da alcuni come troppo burocratici o di interesse solo per le grandi e grandissime strutture.

Quanto emerge dalle risposte al questionario conferma che le aziende/enti del campione, pur diversificato, rappresentano nel contesto italiano un'elite per quanto riguarda la sicurezza informatica e che le attività pluriennali di sensibilizzazione e di trasferimento di conoscenza da

parte di riviste, convegni, associazioni di categoria e specifiche di settore hanno dato e stanno dando i loro frutti.

La fig.38 fornisce un primo quadro generale su come si espletano tali aspetti.
Il quadro, anche rispetto al precedente Rapporto, è positivo e promettente: il 76% circa afferma di avere delle policy tecnico-organizzative di sicurezza, contro un già positivo 58% precedente, e il 55% utilizza strumenti informatici a supporto dei processi inerenti la sicurezza ICT. In termini di procedure organizzative interne, il 48% è dotato di help desk per il supporto agli utenti informatici, e il 43,7% gestisce in maniera strutturata incidenti e problemi informatici. Il 40% ha definito e utilizza criteri di autorizzazione con la logica della separazione delle responsabilità (SoD, Separation of Duties).

FIG. 38 - Contromisure organizzative e dei processi per la sicurezza



Un 35% partecipa periodicamente a corsi ed eventi di sensibilizzazione, formazione e addestramento per la sicurezza ICT.
Per quanto riguarda le aziende che hanno già adottato o hanno intenzione di munirsi di "policy" per la sicurezza informatica, la fig.39 evidenzia che il 60% le ha già in uso e le ha fatte conoscere ai propri interlocutori, mentre per il 40% sono in via di definizione e stanno per essere adottate.

In maggior dettaglio per chi già ne usufruisce, la fig. 40 mostra quali sono i mezzi di comunicazione e diffusione: la prevalenza è via intranet seguita a breve distanza dalla posta elettronica; con maggior distanza in percentuale la comunicazione interna a mezzo stampa o tramite seminari e corsi.

6.4.1 Conformità a standard e best practice

Un forte ausilio nell'organizzazione della sicurezza ICT può venire da un'intelligente contestuale adozione di standard e best practices ormai consolidate a livello internazionale e nazionale: tipici esempi il Cobit per la gestione tattico-strategica allineata al business, ITIL v3 e l'ISO 20000[1] per la gestione operativa dell'ICT, l'ISO 27000 per la gestione della sicurezza ICT, l'ISO 9000 per la gestione della qualità, ecc.
La fig.41 evidenzia come il 66% non intende certificarsi a standard e/o adottare standard e/o "best practice" quali ITIL, Cobit o ISO 20000, pur magari adottandole o facendovi ri-

FIG. 39 - Gestione policy di sicurezza ICT

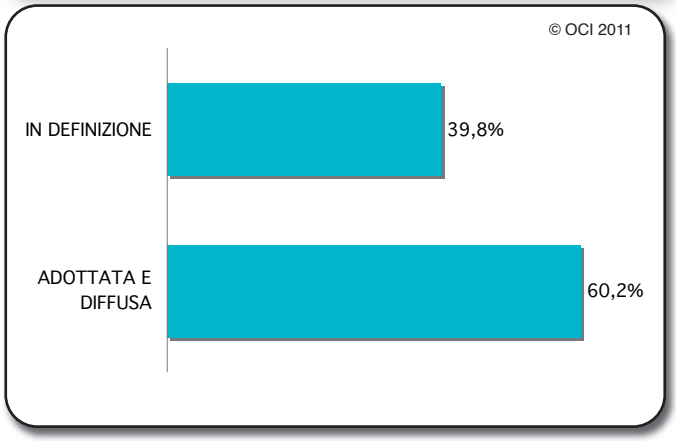


FIG. 40 - Comunicazione e diffusione delle policy

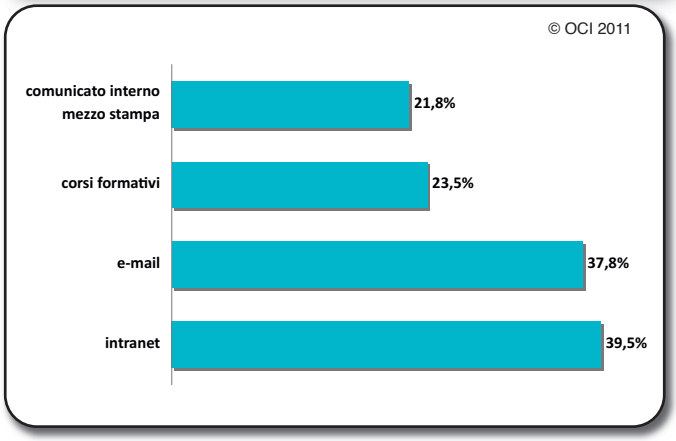


FIG. 41 - Conformità de facto e/o de jure a ITIL, Cobit e ISO

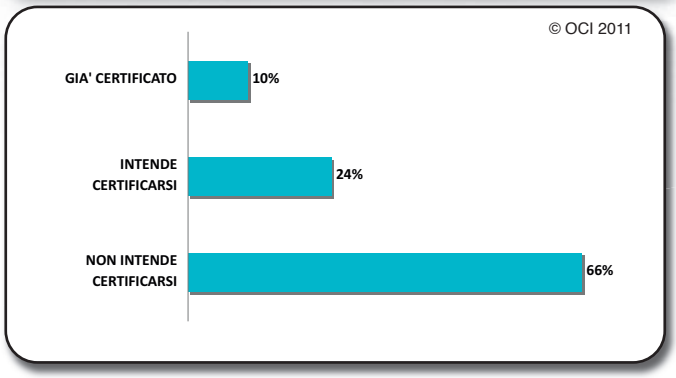
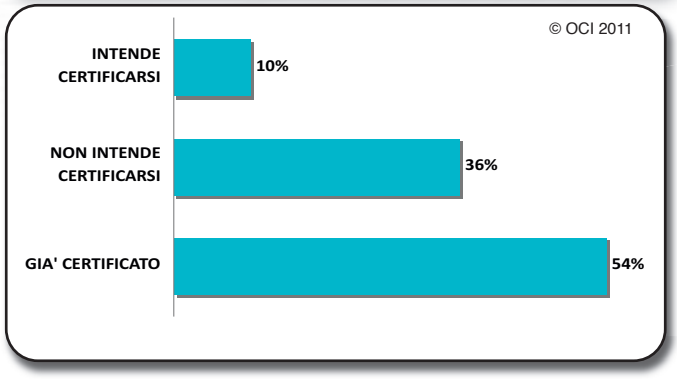


FIG. 43 - Conformità ISO 9000 sulla qualità



ferimento almeno in parte. Il 24% ha intenzione di certificarsi mentre il 10% è già certificato: questa piccola percentuale rappresenta prevalentemente le grandi organizzazioni.

Per quanto riguarda la famiglia di standard ISO 27000, il 10% del campione è già certificato, il 21% intende certificarsi nel prossimo futuro, il rimanente non intende certificarsi (fig.42).

Per il campione considerato la certificazione della qualità[2] è ben più diffusa; come indicato dalla fig.43, il 54% è già certificato, il 10% intende farlo nel prossimo futuro, il resto del campione non è interessato. Tale diffusione deriva anche dal fatto che tale certificazione è richiesta per poter partecipare alla maggior parte delle gare pubbliche.

Alcune aziende/enti devono essere certificate e seguire determinate normative: si pensi alla Sox se si è quotati negli Stati Uniti, a Basilea 2-3 e alle direttive della Banca d'Italia per le banche, all'ISVAP ecc.
La fig.44 mostra come solo il 20% dei rispondenti deve far fronte a questi ulteriori obblighi.

FIG. 42 - Conformità a ISO 27000

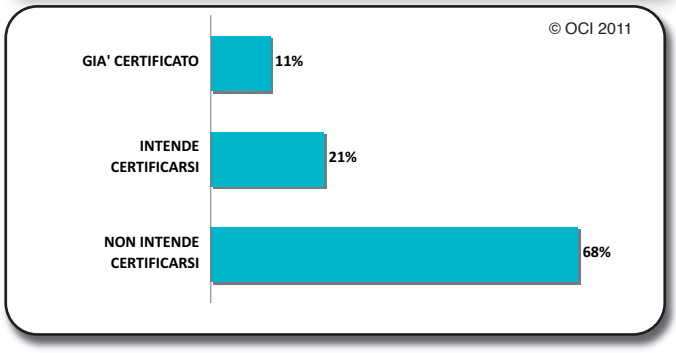
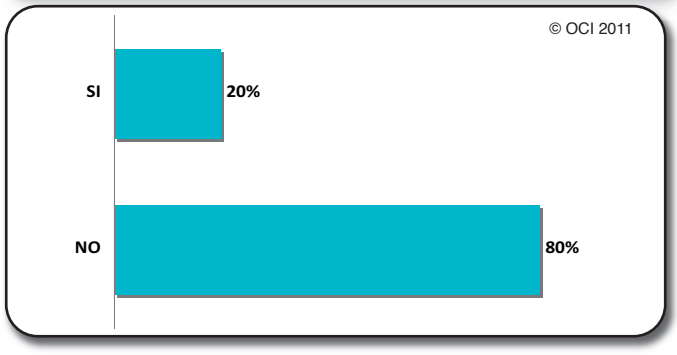
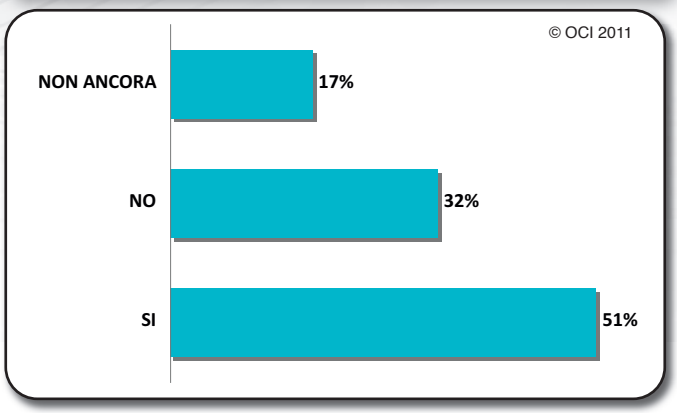


FIG. 44 - Conformità ad altri standard e normative



[1] ISO 20000 standardizza logiche e processi di ITIL v2
[2] La certificazione per il "total quality management" impatta anche sulla sicurezza informatica e per tale motivo è stata considerata nel questionario.

FIG. 45 - Funzioni di Auditing



6.4.2 Audit

Nell'ambito della gestione della sicurezza una funzione importante è quella dell'auditing. La fig.45 mostra che il 51% dei rispondenti svolge tale funzione e che il 17% ha intenzione o ha a piano di espletarla.

La fig.46 dettaglia di come venga espletata tale funzione da parte di quel 51% del campione che già la svolge: la maggioranza dei rispondenti (30,5%) la svolge su base annuale, il 27,1% con ancora maggior frequenza, mentre il 25,4% la svolge in maniera "irregolare", ossia non pianificata periodicamente, ma quando ritenuto necessario, infine il 6,8% la svolge con cadenza superiore all'anno. Come nel precedente rapporto, poco più del 10% gestisce l'auditing come un processo di miglioramento continuo dell'ICT e dei servizi che esso eroga.

6.4.3 La struttura organizzativa interna per la sicurezza ICT

La struttura organizzativa interna all'azienda/ente per la gestione della sicurezza ha un ruolo importante e impatta sui vari processi e le 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.47, il 64,4% dei rispondenti ha definito un ruolo di "responsabile della sicurezza informatica", il 10,2% è in procinto di definirlo, il rimanente non ha alcun responsabile e non intende individuarlo. Per la maggioranza delle persone che ricoprono tale ruolo nella propria organizzazione, nel 65,3% dei casi è funzionalmente collocato nella Unità Organizzativa Sistemi Informativi, quindi all'interno dell'unità organizzativa sistemi informativi e in tale contesto svolge il ruolo di CISO, come dettagliato in fig.48. Nel 25,3% questo responsabile non è all'interno dell'UOSI ma in altre strutture interne e solo nel 9,4 % dei casi sono definiti sia i ruoli di CSO che di CISO.

FIG. 46 - Frequenza dell'auditing sui sistemi informativi

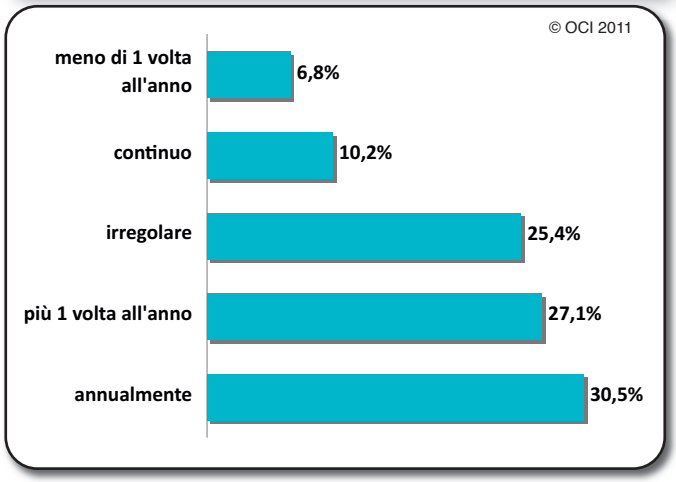


FIG. 47 - Ruolo responsabile sicurezza ICT (CISO)

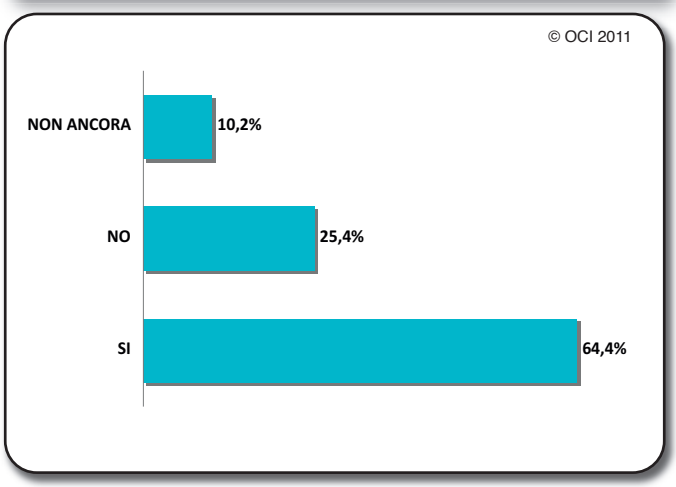
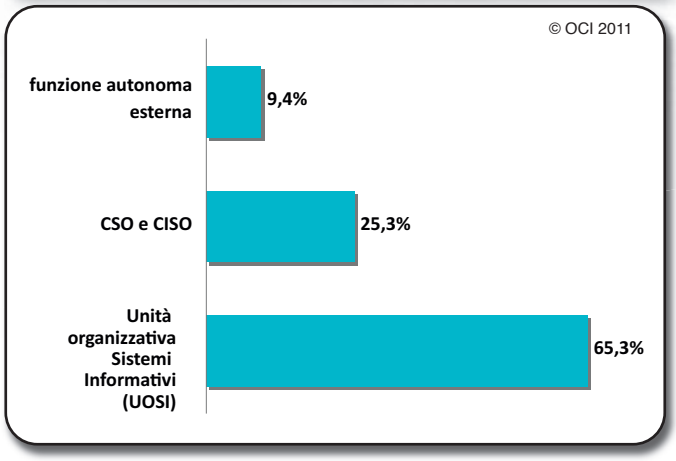


FIG. 48 - Logica organizzativa per il CISO



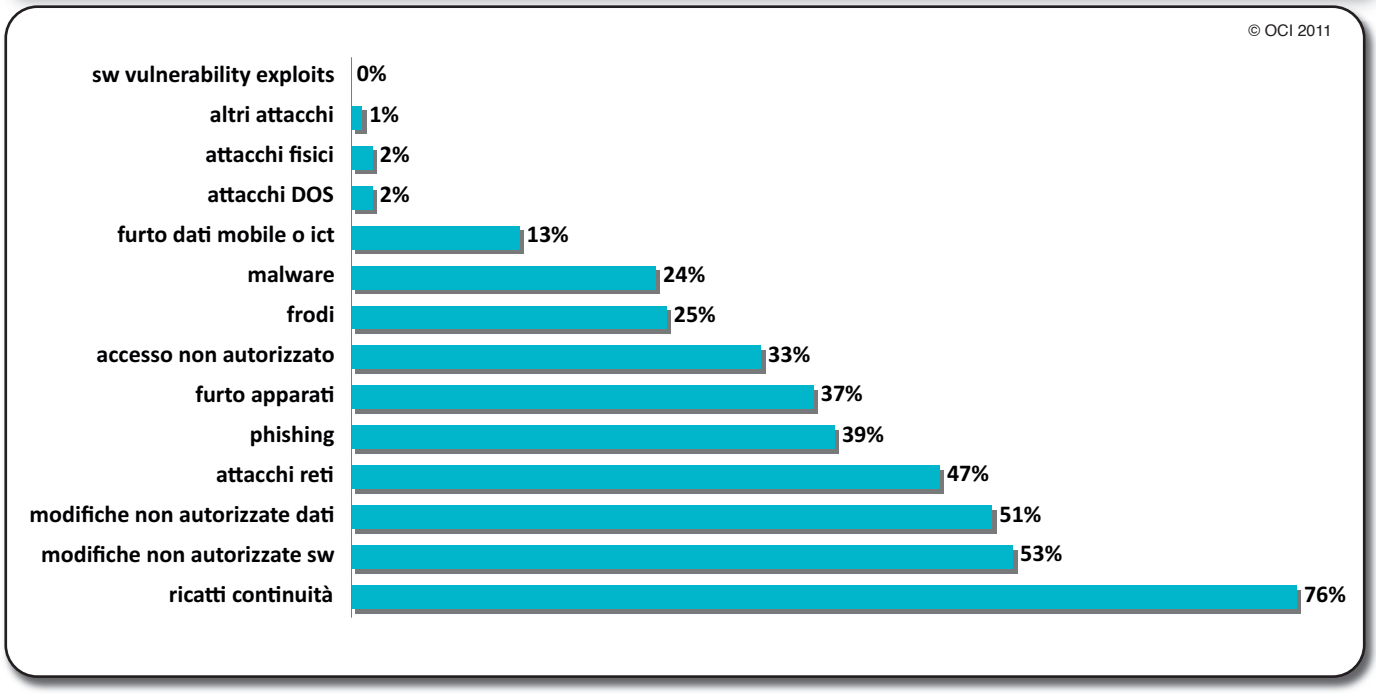
7. Gli attacchi più temuti

A conclusione del questionario è richiesta una previsione di quali saranno gli attacchi più probabili e più temuti, indipendentemente da quelli eventualmente subiti, e da quali motivazioni l'attaccante potrebbe essere guidato. La tassonomia di attacchi è quella usata per la rilevazione degli attacchi subiti, di cui al § 5, con possibilità di risposte multiple.

Il risultato dell'analisi dell'attuale Rapporto, riportato in fig.49, è significativamente diverso da quello rilevato nel precedente. Attualmente l'attacco più temuto, con il 76%, è il ricatto sulla continuità operativa e sull'integrità dei dati del sistema informativo, che nel precedente Rapporto risultava ultimo con un 15% sul totale dei rispondenti. Al secondo posto, con il 53%, le modifiche non autorizzate al sofware, cui seguono a breve distanza, 51%, le modifiche non autorizzate ai dati. Sono questi ultimi gli attacchi potenzialmente più critici in quanto vanno a minare il patrimonio informativo aziendale, ed erano nella precedente rilevazione al quarto ed al secondo posto, con un 57 % e con un 72 % rispettivamente.

Un'altra interessante indicazione della mutata percezione dei potenziali rischi futuri è che l'accesso non autorizzato, primo con il 73% nella precedente edizione, è sceso nell'attuale al 33%. Tale variazione sta ad indicare che i con-

FIG. 49 - Attacchi maggiormente temuti nel prossimo futuro



trolli degli accessi, se non rafforzati, sono comunque meglio gestiti, e si riduce l'uso improprio di identificativi d'utente e del conseguente accesso non autorizzato.
Rimane infine alto il timore di attacchi alle reti, dovuto anche alla diffusione del wireless: il dato precedente era 51%, l'attuale 47%. Analogamente per il social engineering ed il phishing, che dal 33% passano al 39%.

Le motivazioni principali per gli attacchi più temuti, risultano molto simili a quanto rilevato nella scorsa edizione e confermano l'origine criminale degli attacchi, discussa in § 5. Come mostrato in fig.50, il 55% dei rispondenti (contro il 50% della passata edizione) stima che la motivazione principale sia la frode informatica, con l'obiettivo di illegali guadagni economici. Aumentata la percentuale del vandalismo (47%), del sabotaggio (42%) e dello spionaggio (28%) contro il 35%, il 29% ed il 24% della passata edizione.
Scende al contrario la percentuale relativa all'azione dimostrativa, dal 37% all'attuale 23%,confermando una volta di più che gli attacchi sono prevalentemente a fine di lucro illegale.

Il timore di attacchi di tipo terroristico rimane basso, anche se aumenta dall'1% al 5%, e per lo più indicato da grandi enti i cui sistemi ICT potrebbero essere bersaglio di un'azione terroristica.

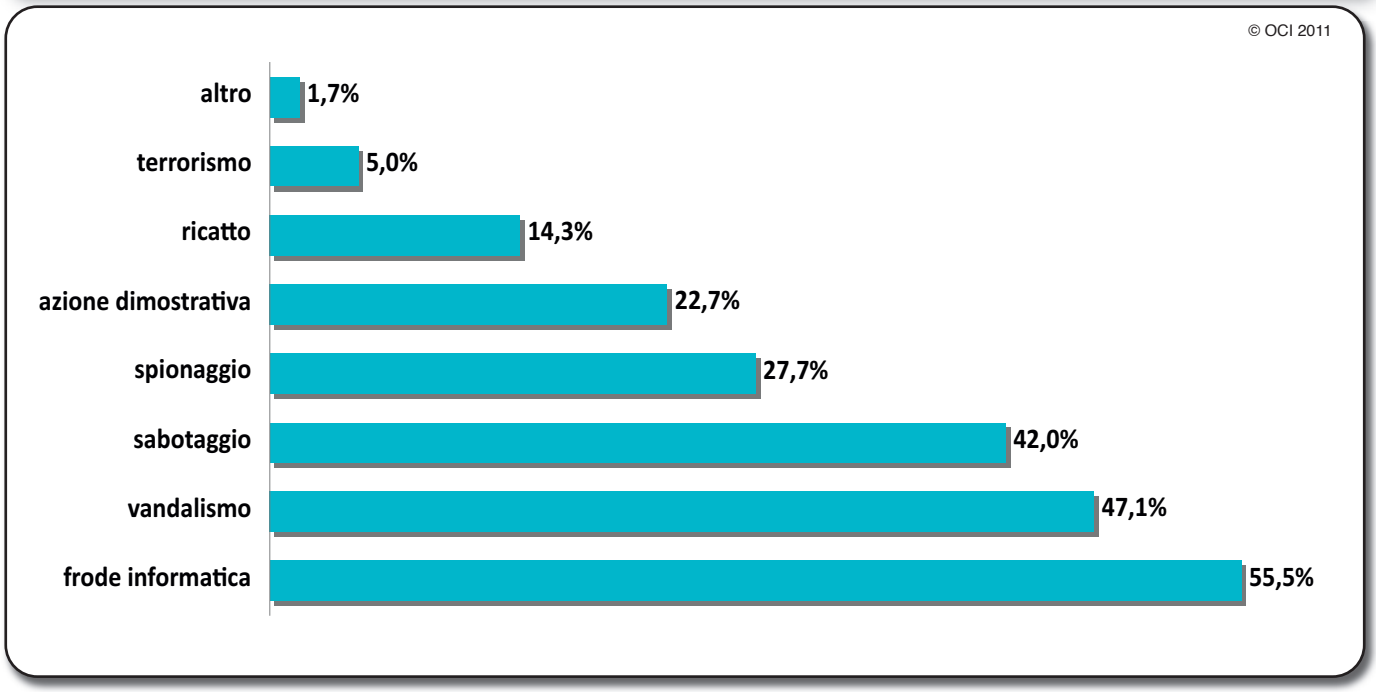
8. Conclusioni

Il Rapporto OAI 2011 evidenzia come da un lato si stiano rafforzando e diffondendo gli strumenti e le misure di sicurezza, tanto che il numero di attacchi subiti dal campione dei rispondenti è diminuito, ma dall'altro alcuni attacchi sono più sofisticati, e difficili da prevenire e contrastare.

Gli attacchi si basano prevalentemente:

a) sulle vulnerabilità del software di base e applicativo, sulle quali vengono realizzati i codici maligni. Le vulnerabilità sono in crescita, talvolta non risolte dai fornitori e spesso non sistemate con le apposite patch dagli utenti. Alcuni dati rilevati da altri Rapporti a livello mondiale nel 2010:

FIG. 50 - Probabili motivazioni per gli attacchi più temuti



- il numero massimo di vulnerabilità divulgate: 8562 (+27% rispetto al 2009);
- il 44% delle vulnerabilità non ha avuto patch di correzione;
- con la virtualizzazione si sono introdotte 373 nuove vulnerabilità;

b) sul social engineering, sfruttando la disponibilità e in taluni casi la disattenzione e/o l'ingenuità degli utenti finali;
c) sulla diffusione anche a livello aziendale dei social network, quali Facebook, Twitter, YouTube, LinkedIn, oltre che della posta elettronica, dei motori di ricerca, dell'uso di sempre più potenti chiavette USB e degli strumenti collaborativi, che ampliano le possibilità di acquisire facilmente informazioni riservate con le quali svolgere attacchi e compiere frodi sia a livello del singolo che a livello di azienda/ente.

La maggior parte degli attacchi sono finalizzati a frodi e a compiere significativi danni sull'obiettivo attaccato. Gli attacchi volontari sono sempre più dettati da finalità criminali, alla ricerca di informazioni che possano facilmente trasformarsi in profitto, ovviamente illecito: questo significa soprattutto carpire informazioni sulle carte di credito e i bancomat degli utenti e recuperare credenziali per l'accesso ai conti bancari. In tale ambito le modalità di attacco sono o verso i server bancari, per cercare di acquisire in maniera massiva tali informazioni, oppure verso i singoli tramite social engineering.
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 questo emerge 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 della politica di continuità e di salvaguardia del patrimonio operativo, soprattutto in una situazione di crisi come quello attuale in cui tutte le risorse, anche quelle economiche, non possono essere ridotte o tagliate a danno della sicurezza ICT, ma devono essere razionalizzate e ottimizzate.

Come per il precedente Rapporto, anche l'attuale conferma per l'Italia le tendenze emerse a livello internazionale, con alcune differenze dovute a specificità nazionali.
L'insieme delle aziende/enti che hanno risposto al questionario rappresentano una fascia medio-alta nel panorama italiano in termini di qualità dei sistemi e della loro gestione, e quindi anche di sicurezza ICT.
Dai dati raccolti e dalla loro analisi si può evidenziare, specificatamente per l'ambiente italiano, che:

- ai vertici aziendali si inizia ad aver consapevolezza dell'importanza della sicurezza ICT, almeno in termini di continuità operativa; prova ne è una maggior attenzione agli aspetti organizzativi, alla definizione di policy, alla formazione e sensibilizzazione degli utenti finali;
- la gestione dei sistemi informativi è prevalentemente interna;
- i sistemi informativi del campione adottano moderne tecnologie quali la virtualizzazione e le architetture ad alta affidabilità;
- standard e best practice internazionali sono sempre più conosciute, in parte seguite, ma la maggior parte dei rispondenti non è interessato alle relative certificazioni;
- i codici maligni rappresentano l'attacco più diffuso, ed il social engineering, in particolare con il phishing, rimane un fenomeno critico;
- nonostante la fascia alta dei rispondenti, le misure di sicurezza abbracciano i vari strumenti disponibili sul mercato, ma la loro gestione è prevalentemente " a silos" e non "intergrata";
- aumentano sensibilmente l'attenzione ed i controlli sulla sicurezza intrinseca del software messo in produzione;
- la struttura organizzativa per la gestione della sicurezza risponde prevalentemente al responsabile dei sistemi informativi.

Gli attacchi ai sistemi informatici sono un problema crescente e così critico da allarmare e interessare politici e governi sia a livello nazionale che internazionale.
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 delle infrastrutture comporta 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. Scendendo a livello dei singoli sistemi informativi dell'azienda/ente, anch'essi sono vitali per il funzionamento dei loro processi e del loro business, e non sono più sostituibili con procedure manuali.
I sistemi informativi sono sempre più complessi e quindi più difficili da monitorare e governare. 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 i livelli di sicurezza crescenti arginano i potenziali attacchi, che fino ad oggi, almeno in Italia, sono stati relativamente limitati e arginabili. La guerra tra "guardie" e "ladri" nel mondo digitale è continua e con risultati altalenanti.
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 nel precedente Rapporto, 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 pertanto tutt'ora 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 alcuni 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 inglesi sulla sicurezza (usati anche in italiano)

- ***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
- ***ATP, Advanced Persistent Threat***, attacco persistente e sofisticato, basato su diverse tecniche contemporanee
- ***Backdoor***: interfaccia e/o meccanismo nascosto che permette di accedere ad un programma superando le normali procedure e barriere d accesso
- ***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 Public Turing Test To Tell Computers And Humans Apart: l'acronimo individua una famiglia di test costituito da una o più domande e risposte per assicurarsi che l'utente sia un essere umano e non un programma.
- ***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.
- ***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 alla disponibilità di dispositivi e servizi
- ***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.
- ***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.
- ***Fix***: correzioni di un programma software, spesso usato come sinonimo di patch
- ***Flash threats:*** tipi di virus in grado di diffondersi molto velocemente
- ***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
- ***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
- ***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
- ***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 consentedi avere il completo controllo su un sistema.
- ***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
- ***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, acquisti eseguiti in rete, etc.) senza il suo consenso, utilizzandole poi per trarne profitto, solitamente attraverso l invio di pubblicità mirata
- ***SQL injection:*** tecnica di inserimento di codice in un programma che sfrutta delle vulnerabilità sul database con interfaccia SQL usato dall applicazione
- ***SSO, Single Sign On:*** unica autenticazione 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

- ***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 codci 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. Articoli di approfondimento

Dal numero di marzo 2010 della rivista Office Automation, l'autore tiene una rubrica fissa dell'Osservatorio sugli Attacchi Informatici in Italia per dare una continuazione tra un Rapporto annuale e l'altro e per promuovere sensibilità e conoscenza sugli attacchi ai sistemi informatici in Italia. Per questo motivo è stato anche attivato un Gruppo su LinkedIn. Come approfondimento sugli attacchi, sono citati nel presente Rapporto i seguenti articoli della Rubrica OAI pubblicati sulla rivista Office Automation e disponibili gratuitamente on line sul sito www.malaboadvisoring.it.

10.1 Vulnerabilità ed exploit, accoppiata letale *(Office Automation n.06 giugno 2010, p. 88-90)*
10.2 L'errore nella programmazione genera vulnerabilità *(Office Automation n. 07-08 luglio-agosto 2010, p. 88-89)*
10.3 Wireless e mobilità, fonti crescenti di attacchi *(Office Automation n. 09 settembre 2010, p. 88-89)*
10.4 Anche i documenti testuali nascondono vulnerabilità (*Office Automation n. 10 ottobre 2010, p. 88-89)*
10.5 Attacchi ai sistemi di controllo industriale e alle infrastrutture *(Office Automation n. 11 novembre 2010, p. 88-89)*
10.6 Gli attacchi di social engineering *(Office Automation n. 01 gennaio 2011, p. 90-91)*
10.7 Virtualizzazione: nuove vulnerabilità e nuovi attacchi *(Office Automation n.02 febbraio 2011, p. 88-90)*
10.8 Advanced Persistent Threats: attacchi più sofisticati e perforanti *(Office Automation n. 04 aprile 2011, p. 88-89)*
10.9 Botnet: come nascono, come difendersi *(Office Automation n. 05 maggio 2011, p. 86-88)*
10.10 SQL Injection: coem funziona, come proteggersi (Office Automation n. 07-8, luglio-agosto 2011, p. 88-89)
10.11 *Hacker, cracker e gli altri: chi sono e perché attaccano* (Office Automation n. 05 maggio 2010, p. 86-87)

11. Riferimenti bibliografici essenziali

Dall'OCI all'OAI: un po' di storia... ancora attuale

- 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.
- M. Bozzetti, R. Massotti, P. Pozzi (a cura di): "Crimine virtuale, minaccia reale", 2004, Franco Angeli
- M.Bozzetti: "Sicurezza Digitale - una guida per fare e per far fare", 2007, Soiel International.

Le principali fonti sugli attacchi e sulle vulnerabilità

Le fonti elencate non hanno la pretesa di essere esaustive e complete:

- CA Security Advisor di Computer Associate (http://www.ca.com/us/global-technology-security.aspx) fornisce avvisi su vulnerabilità e malware;
- Centrale d'allarme per attacchi informatici di ABILAB: 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/)
- CSI, Computer Security Institute (www.gocsi.com) 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;
- 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://iss.net/, fornisce sistematicamente segnalazioni su vari tipi di attacco e di vulnerabilità, oltre che rapporti periodici;
- 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 e fornisce, oltre alla possibilità di denunciare negli US Attacchi Informatici, informazioni sugli schemi di attacco 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: www.microsoft.com/italy/security/default.mspx 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 Security Labs: http://www.sophos.it/ fornisce aggiornati allarmi;
- Trend Watch della Trend-Micro http://us.trendmicro.com/us/trendwatch/current-threat-activity/index.html fornisce segnalazioni e trend sugli attacchi;
- 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.

Ing. Marco Rodolfo Alessandro Bozzetti

Si occupa di ICT da più di 35 anni, ha operato con responsabilità crescenti presso primarie imprese di produzione, quali Olivetti e Italtel, e presso società di consulenza tra cui Arthur Andersen. È stato anche responsabile dei sistemi informativi dell'intero Gruppo ENI.
È Amministratore unico di Malabo Srl (www.malaboadvisoring.it) e opera prevalentemente con GeaLab Srl, società di consulenza direzionale operante nell'ICT che nasce da GEA Consulenti Associati di Direzione Aziendale (www.gea.it).
È stato uno dei primi a livello mondiale a occuparsi di internetworking e di sicurezza ICT, fu ideatore di EITO, European IT Observatory, e di OCI, Osservatorio Criminalità ICT in Italia, report pubblicato dall'FTI, Forum delle Tecnologie dell'Informazione.
È stato Presidente di FIDA Inform, di SicurForum in FTI e del ClubTI di Milano, oltre che componente del Consiglio del Terziario Innovativo di Assolombarda.
È ora nel Consiglio Direttivo di FIDAInform e di AIPSI, Socio fondatore e componente del Comitato Scientifico dell'FTI, socio di IASA, itSMF, Prospera.
Ha pubblicato articoli e libri sull'evoluzione tecnologica, sulle architetture ICT, sulla sicurezza informatica, sugli scenari, sul business e sull'innovazione tramite l'ICT.
Appassionato di alpinismo e sci, pratica anche jogging, vela, sub e golf.

IN COLLABORAZIONE CON

CON IL PATROCINIO DI:

SOIEL INTERNATIONAL
Eventi e riviste per l'organizzazione aziendale