SOIEL INTERNATIONAL
Eventi e riviste per l'organizzazione aziendale

e

ClubTI
Club per le Tecnologie dell'Informazione

FIDA INFORM

presentano

oai OsservatoriO AttacchInformatici

Rapporto 2009 OAI
Osservatorio sugli Attacchi Informatici in Italia

A cura di Marco R. A. Bozzetti

Con il patrocinio di:

aipsa Associazione Italiana Professionisti Security Aziendale

aipsi ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

ASSOLOMBARDA

FTI FORUM per la TECNOLOGIA della INFORMAZIONE

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

In collaborazione con

polizia delle comunicazioni

Rapporto 2009 OAI
Osservatorio sugli Attacchi Informatici in Italia

A cura di Marco R. A. Bozzetti

Ringraziamenti

L'autore, il ClubTi di Milano, Fida Inform 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 che ha strettamente collaborato con l'autore per l'analisi dei dati raccolti e per la preparazione dei relativi grafici e tabelle.

Indice

1. Introduzione

FidaInform, la Federazione dei ClubTI Italiani distribuiti sul territorio nazionale che associano i "decisori" sull'ICT sia lato domanda che lato offerta, e il ClubTI di Milano (per approfondimenti si rimanda ai rispettivi siti www.fidainform.it e www.clubtimilano.net) hanno deciso di rilanciare l'Osservatorio sugli Attacchi Informatici in Italia (OAI), con il supporto organizzativo ed economico di Soiel International, editore della rivista della Federazione, *ICT Professional*. Rilanciare, in quanto un simile Osservatorio era già stato creato negli anni passati, dal 1997 al 2004, da FTI-Sicurforum, che patrocina la nuova iniziativa insieme ad altri Enti, quali AIPSA, AIPSI, Aused, Inforav e con la collaborazione della Polizia delle Comunicazioni.

Obiettivo principale dell'OAI è fornire concrete indicazioni sugli attacchi ai sistemi informatici delle Aziende e degli Enti Pubblici italiani che possano essere di riferimento nazionale, autorevole e indipendente, per l'analisi del rischio.

Nelle prossime edizioni, con cadenza annuale, sarà pubblicato e divulgato il rapporto sugli attacchi informatici occorsi nell'anno precedente. L'indagine è svolta tramite un questionario posto on line su web e con l'invio dell'invito a compilarlo ai CIO (Chief Information Officer), CSO (Chief Security Officer) e CISO (Chief Information Security Officer) di più di mille aziende ed enti pubblici centrali e locali. Il compilatore può rimanere anonimo, e per ovvi motivi di riservatezza non sono richieste informazioni di dettaglio sull'azienda/ente e sui sistemi informativi, così da non consentire di risalire alla stessa.

L'Osservatorio infine garantisce la totale riservatezza sui dati raccolti, che non vengono forniti in nessun modo a nessun interlocutore: OAI utilizza e utilizzerà tali dati solo per le analisi e per la produzione di rapporti, senza mai citare casi o esempi specifici.

Ulteriore e non meno importante obiettivo è favorire lo sviluppo di sensibilità e cultura in materia di sicurezza delle informazioni e delle comunicazioni (in breve sicurezza ICT) soprattutto a livello dei "non tecnici", tipicamente i manager e i vertici dell'organizzazione che decidono e stabiliscono i budget.

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

Con la pervasiva applicazione delle tecnologie informatiche e di comunicazione, i sistemi ICT sono divenuti il nucleo fondamentale e insostituibile per il supporto e l'automazione dei processi e il trattamento delle informazioni delle organizzazioni in ogni settore di attività. Di qui l'importanza della loro affidabilità e disponibilità, senza la quale gli stessi processi, anche i più semplici, non possono essere più espletati praticamente.

L'evoluzione moderna dei sistemi informativi si è consolidata su Internet e sui siti web, e sta velocemente evolvendo verso logiche collaborative e di web 2.0, oltre che verso logiche di terziarizzazione tipo XaaS (Software/Application/DB/Platform/Infrastructure as a Service) e di "cloud computing". Anche grazie alla diffusione di dispositivi mobili d'utente, che sono dei veri potenti computer, delle reti senza fili (wireless), dei collegamenti "peer-to peer" (P2P), dei "social networking" e dei servizi ad essi correlati, ad esempio Facebook, LinkedIn, 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, con i web service, consentono una reale interoperatività, un modulare e più facile assemblaggio di programmi applicativi.

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 un'eterogeneità sia di sistemi che di funzioni.

La veloce evoluzione tecnologica, di cui i temi sopra elencati rappresentano solo alcuni degli aspetti più noti, da un lato rende i sistemi informatici sempre più complessi e difficili da gestire, con crescenti vulnerabilità, dall'altro vede una minore necessità di competenze, oltre che una maggiore facilità di reperibilità degli strumenti, necessari a effettuare attacchi deliberati e nocivi.

La preoccupazione per queste linee di tendenza generali sulla sicurezza ICT è poi stata accentuata dai terribili eventi dell'11 settembre 2001, che hanno reso più credibili e più probabili eventi di terrorismo e di guerra elettronica miranti a colpire le infrastrutture "critiche" di un Paese o di intere aree (sistemi dei trasporti, dell'energia, della finanza, etc.) attraverso l'attacco ai sistemi ICT di gestione e controllo che le governano. Tali infrastrutture sono ormai totalmente informatizzate e da esse dipendono la maggior parte delle attività umane, sia in ambito lavorativo che domestico, dei popoli occidentali. A conferma di tali criticità e timori, è significativa la nomina di Howard Schmidt, precedentemente Presidente di ISSA, a Consigliere di

Obama per la sicurezza informatica negli USA (i media l'hanno definito "Cyber Zar") e in Italia la creazione del CNAIPIC, Centro Nazionale Anticrimine Informatico Protezione Infrastrutture Critiche, e della figura di Consigliere Ministeriale sulla Sicurezza Informatica, affidata a Domenico Vulpiani, prima Direttore del Servizio Polizia Postale e delle Comunicazioni.

Ma quali sono gli attacchi che tipicamente affliggono i sistemi informativi italiani? E come si fa a reagire di fronte a tali attacchi? Numerosi sono gli studi e i rapporti a livello internazionale, condotti da Enti specializzati, quali ad esempio lo statunitense CSI (Computer Security Institute), il First (Forum for Incident Response and Security Team) o quelli provenienti dai principali Fornitori di Security, quali Cisco, IBM, McAfee, Microsoft, Symantec, Sophos (in §10 un elenco delle principali e più aggiornate fonti). Questi studi forniscono con cadenza periodica informazioni, anche molto dettagliate, per i principali paesi e individuano i principali trend. Dati specifici riguardanti l'Italia normalmente non sono presenti, salvo casi abbastanza eccezionali, e si devono pertanto estrapolare dalle medie europee. Ma la disponibilità di dati "locali" 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 che per "sensibilizzare" sul tema della sicurezza informatica il personale a tutti i livelli, dai decisori di vertice agli utenti.

L'occorrenza degli attacchi e lo stato dell'arte a essi relativo sono stati prevalentemente trattati o come una notizia sensazionale da richiamo mediatico o come una tematica da specialisti, con termini tecnici difficilmente comprensibili ai non addetti ai lavori. Il reale livello di sicurezza di un sistema ICT dipende più da come lo si usa e lo si gestisce, che dalle tecnologie impiegate: organizzazione, informazione e coinvolgimento di tutto il personale sono altrettanto importanti, se non di più, dell'installazione di firewall, anti malware, sistemi di identificazione e autenticazione, back-up e così via.

In conclusione, proprio per colmare tale vuoto informativo in Italia, si è deciso di rilanciare l'attivazione di un Osservatorio Nazionale grazie al ClubTI di Milano, a Fida Inform e a Soiel International con il patrocinio di altre Associazioni e Istituzioni interessate, ereditando l'esperienza passata avuta con OCI e FTI-Sicurforum, definendone la metodologia di indagine in collaborazione con gli esperti dei vari Enti patrocinatori, raccogliendo sul campo i dati presso un insieme significativo di enti e di imprese e fornendo con cadenza periodica i risultati.

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, processate. Nello specifico:

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

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

- **autenticità**, ossia la certezza da parte del destinatario dell'identità del mittente;
- **non ripudio**, ossia il fatto che il mittente o il destinatario di un messaggio non ne possono negare l'invio o la ricezione.

L'attacco contro un sistema informatico è tale quando è 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, quali allagamenti, terremoti, incendi, ecc.

Gli attacchi intenzionali possono provenire dall'esterno dell'organizzazione considerata, tipicamente da Internet e/o da accessi remoti, o dall'interno dell'organizzazione stessa, o da una combinazione tra personale interno ed esterno. Per approfondimenti sulle logiche, le motivazioni e le tipologie degli attaccanti, oltre che sulle loro competenze e sulla loro cultura, si rimanda all'ampia letteratura in materia, e in particolare ai saggi di Pacifici e Sarzana di Sant'Ippolito contenuti nel volume Bozzetti, Pozzi 2000.

La classificazione degli incidenti e degli attacchi per raccogliere i dati sugli attacchi è definita in termini semplici, non tecnici e comprensibili da coloro cui il questionario è indirizzato: tipicamente i responsabili dell'area ICT (CIO) o, laddove esistano, della sicurezza ICT (CISO). La classificazione prevista per questo primo Rapporto OAI considera i seguenti attacchi informatici (l'ordine non fa riferimento alla criticità o gravità dell'attacco, per la spiegazione dei termini gergali si rimanda al glossario in allegato):

1) Accesso a e uso non autorizzato degli elaboratori, delle applicazioni supportate e delle relative informazioni;

2) Modifiche non autorizzate ai programmi applicativi e di sistema, alle configurazioni ecc.;

3) Modifiche non autorizzate ai dati e alle informazioni;

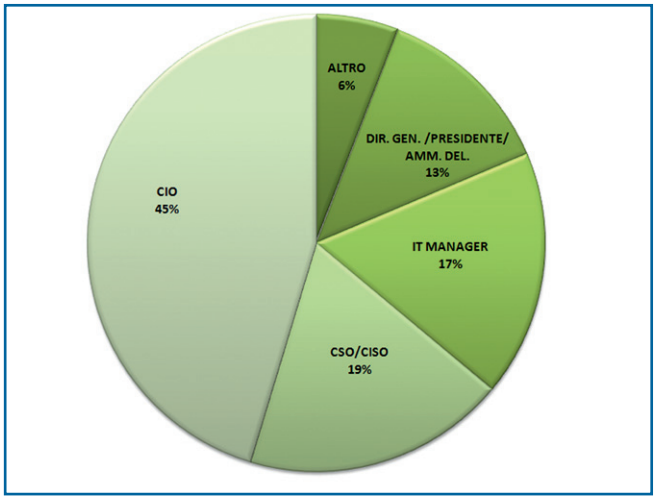
4) Utilizzo di codici maligni (malware) di varia natura, quali virus, Trojan horse, Rootkit, bots, exploit, sia a livello di posto di lavoro che di server;

5) Utilizzo di vulnerabilità del codice software, sia a livello di posto di

lavoro che di server; tipici esempi back-door aperte, SQL injection, buffer overflow ecc.;
6) Saturazione risorse informatiche e di telecomunicazione; oltre a DoS (Denial of Service) e DDoS (Distributed Denial of Service), si includono in questa classe anche mail bombing, catene di S. Antonio informatiche, spamming ecc.;
7) Furto di apparati informatici contenenti dati (laptop, hard disk, floppy, nastri, chiavette USB ecc.);
8) Furto di informazioni o uso illegale di informazioni da dispositivi mobili (palmari, cellulari, laptop) e da tutte le altre risorse;
9) Attacchi alle reti, fisse o wireless, e ai DNS, Domain Name System;
10) Frodi tramite uso improprio o manipolazioni non autorizzate e illegali del software applicativo (ad esempio utilizzo di software pirata, copie illegali di applicazioni ecc.);
11) 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 o il furto d'identità digitale;
12) Ricatti sulla continuità operativa e sull'integrità dei dati del sistema informativo;
13) Altri tipi di attacco, quali ad esempio attacchi di tipo misto (Blended threat), sabotaggi, vandalismi con distruzione di risorse informatiche.

Per facilitare la raccolta dei dati sugli attacchi subiti, articolandoli secondo la tipologia di cui sopra, il questionario è stato realizzato on line su web, 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.

FIG.1 RIPARTIZIONE DEI COMPILATORI PER RUOLO



4. Caratteristiche del campione e dei sistemi ICT censiti per OAI 2009

Il questionario fa riferimento agli attacchi subiti nel 2007 e nel 2008.
L'indagine è stata svolta nel corso del 2009, mettendo in linea il questionario on-line dal 20 ottobre al 30 novembre 2009.
Le persone contattate appartengano ai ClubTI federati in FidaInform e alle altre Associazioni che hanno patrocinato l'iniziativa, cui si aggiungono quelle delle mailing list specializzate di Soiel International.
Complessivamente il bacino dei contattati via posta elettronica si è aggirato attorno alle 1000 persone.
Dopo il primo invito a compilare il questionario inviato all'intero campione considerato, con una breve, ma completa, descrizione dell'iniziativa e dei suoi obiettivi e, dopo aver verificato le prime risposte sono stati inviati messaggi via posta elettronica prevalentemente ai settori che non avevano risposto al primo invito.
Pian piano, e con più invii selettivi, si sono colmati, almeno parzialmente, gli iniziali "vuoti": come dettagliato nel §4.1 successivo: ai primi di dicembre 2009, superato di poco il numero di 100 risposte complete ed esaurienti, si è deciso di chiudere la raccolta dei dati per il Rapporto 2009.
Il numero di 100 e le loro risposte sono state ritenute 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 circa 500 interlocutori per tutti gli Stati del Nord America. Il rapporto 1:5 tra Italia e USA è quindi più che sufficiente ai fini indicativi, e non strettamente statistici, dell'OAI, anche se per quest'ultimo è obiettivo, dal 2010 in avanti, di accrescere il numero di risponditori e di meglio bilanciarli tra i diversi settori sia pubblici che privati.

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 delle aziende, tipicamente e in particolare per quelle piccole e piccolissime.
La **fig. 1** sintetizza la ripartizione dei compilatori per ruolo: la maggior parte è costituita dai Responsabili dei sistemi informativi (CIO).

FIG. 2 STRUTTURA MERCEOLOGICA DEL CAMPIONE

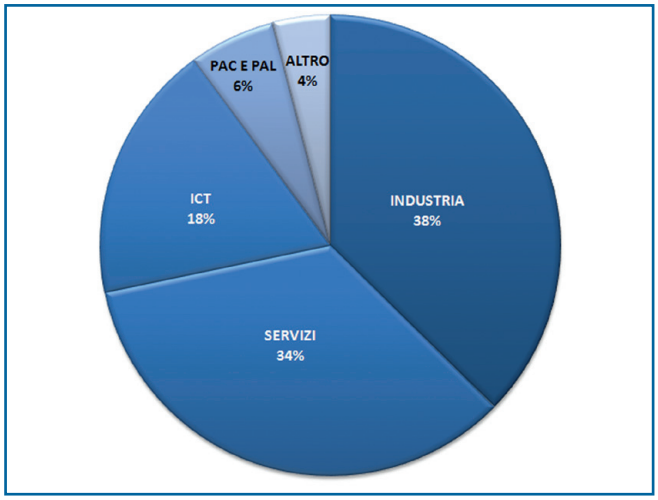
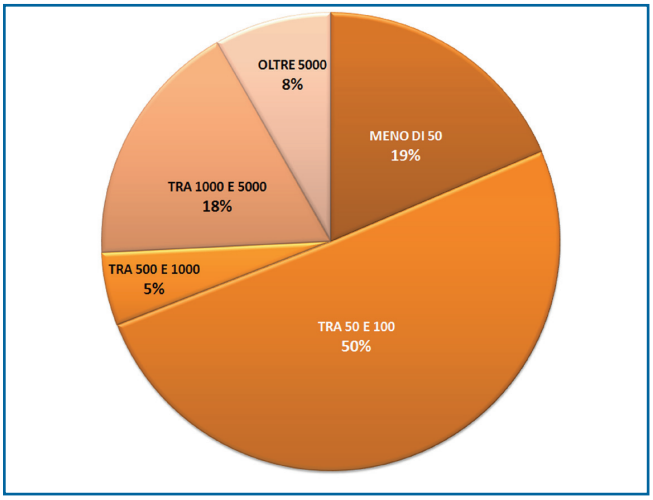


FIG 3 DIMENSIONE DELLE STRUTTURE CUI APPARTENGONO I COMPILATORI PER NUMERO DI DIPENDENTI



La **fig. 2** illustra la suddivisione dei compilatori per i settori pubblici e privati di appartenenza .

I settori merceologici considerati sono stati l'industria manifatturiera, le telecomunicazioni, la distribuzione, i servizi, le banche, le assicurazioni, le pubbliche amministrazioni centrali e locali.

Come si evince dalla fig. 2, il campione dei compilatori non risulta ben bilanciato per settore di industria e/o di Ente pubblico come si sarebbe voluto e come si è cercato di fare.

Nonostante i ripetuti solleciti inviati nominalmente ai CIO, CSO e CISO di tutti questi settori, la maggior parte delle risposte proviene dall'industria manifatturiera.

Il motivo delle risposte inferiori alle attese, almeno per taluni settori, è principalmente dovuto al fatto che l'OAI è un'iniziativa nuova, che deve ancora acquisire autorevolezza tra gli addetti ai lavori, oltre che al grande pubblico dei CIO e di chi utilizza i sistemi informatici. Il carico di lavoro delle varie figure professionali dell'ICT è sempre maggiore, così come crescenti sono le richieste di rispondere a questionari da parte di società di ricerca di mercato, di fornitori, di enti di ricerca e di università. Il poco tempo disponibile e le tante richieste di sondaggi, interviste e questionari porta a selezionarle drasticamente. In più, il tema degli attacchi informatici è di per sé delicato, talvolta problematico, se non addirittura imbarazzante: e molti preferiscono non rispondere a questionari sulla sicurezza dei loro sistemi informativi.

Si è ragionevolmente confidenti che con le prossime edizioni annuali la copertura divenga man mano più ampia, con la crescente diffusione del Rapporto OAI e la crescita della sua autorevolezza.

Come spiegato anche in § 2, il numero complessivo dei compilatori risulta comunque significativo per il tipo di indagine dell'OAI, che è conoscitiva e di orientamento su un bacino di interlocutori ben selezionato e qualificato, e che non è e non ha alcuna pretesa di essere una analisi statistica.

In termini di dimensione delle aziende/enti di appartenenza dei compilatori, la **fig. 3** mostra come la maggior parte appartenga a strutture di medie dimensioni (tra i 50 e i 500 dipendenti); hanno poi risposto in maniera abbastanza bilanciata gli appartenenti a strutture grandi, tra i 1000 e 5000 dipendenti, e quelle piccole, con meno di 50. Un numero minore di compilatori appartiene a strutture molto grandi, con più di 5000 dipendenti.

4.2 Caratteristiche dei sistemi informatici

Le figure che seguono forniscono un'idea del tipo di 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 la riservatezza di 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 del questionario.

I dati richiesti includono l'estensione geografica del sistema informatico, la "macro" struttura del sistema individuata 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 la maggior parte nazionale, come è riportato in **fig. 4**, ma molti (37% dei rispondenti) spaziano al di fuori dell'Europa. È interessante notare come la percentuale extraeuropea è ben superiore rispetto a quella europea.

Le **fig. 5 e 6** mostrano rispettivamente il numero di server e il numero di posti di lavoro per sistema censito.

Nel complesso 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 ecnonomico italiano.

La **fig. 7** sintetizza le tipologie di sistema operativo per server in uso: la quota maggiore è costituita dai sistemi Windows di Microsoft, dalla versione 2000 in avanti, pareggiata in pratica dalla somma dei sistemi Unix e Linux, questi ultimi preponderanti sui primi. Si deve tener conto che nella maggior parte dei casi censiti, il sistema informativo è eterogeneo, con la presenza di diversi ambienti. E questo è tanto più vero quanto più grande è l'Azienda/Ente.

FIG. 4 AREA GEOGRAFICA DI ESTENSIONE DEI SISTEMI ICT CENSITI

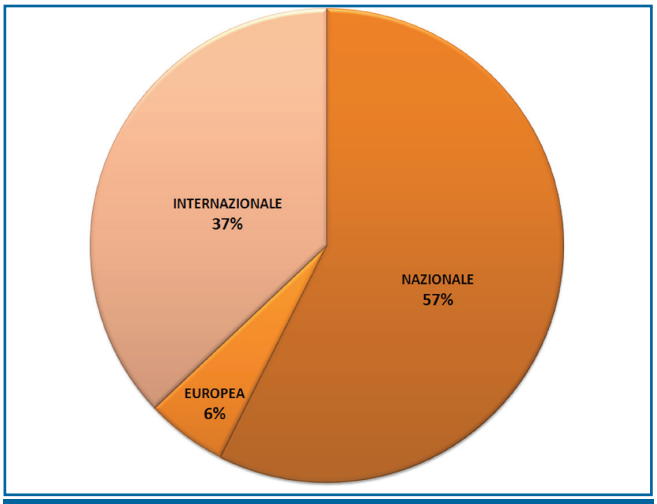


FIG. 5 NUMERO DI SERVER PER SISTEMA

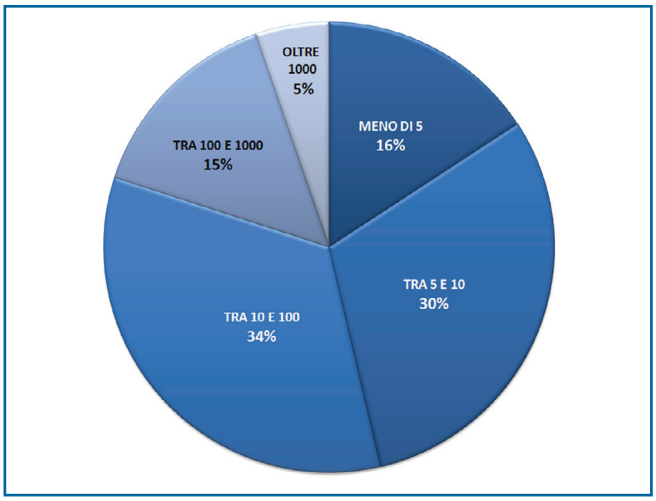


FIG. 6 NUMERO DI POSTI DI LAVORO PER SISTEMA

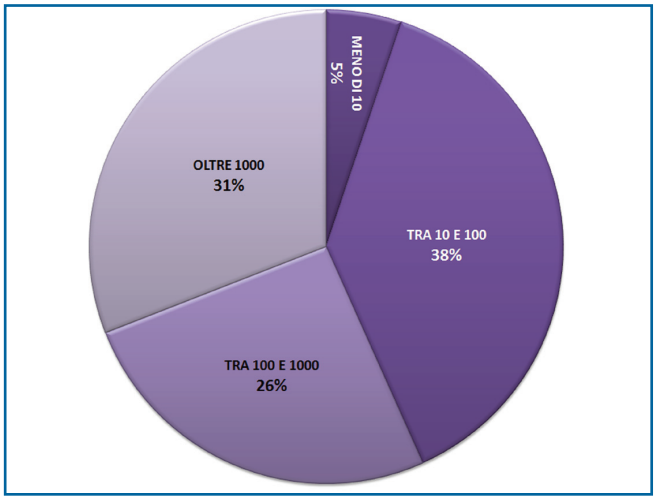


FIG 7 SISTEMI OPERATIVI PER I SERVER IN USO

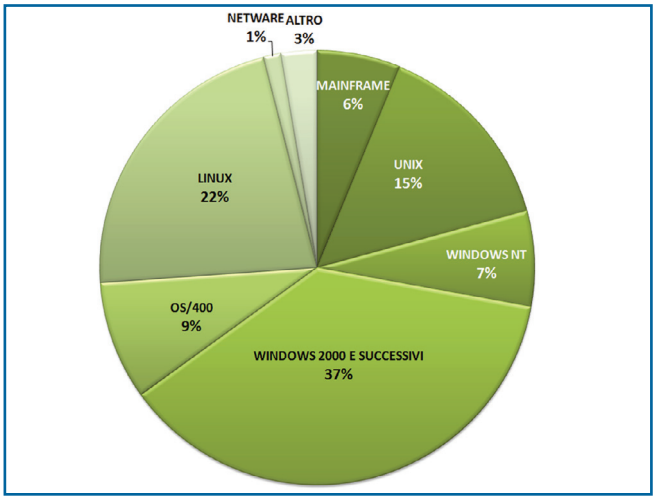


FIG. 8 I DATABASE IN USO

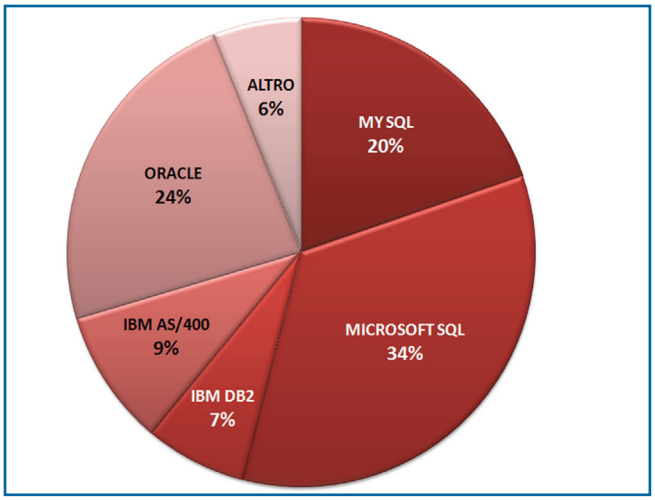


FIG. 9 LE INFRASTRUTTURE DI COMUNICAZIONE

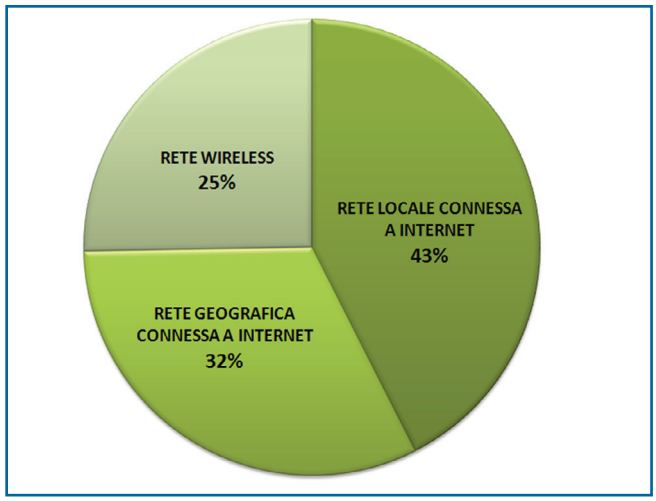
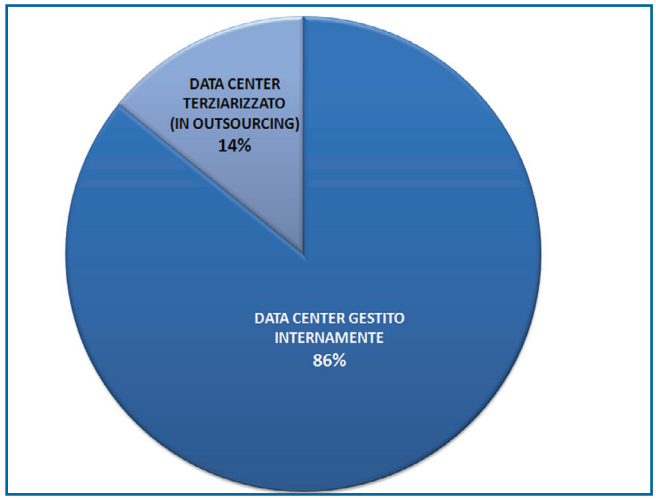


FIG. 10 LA GESTIONE DEL DATA CENTER



L'omogeneità dei sistemi è prevalente solo nelle strutture piccole o piccolissime: tipicamente o solo Windows o solo Linux. Non trascurabile in Italia la presenza di sistemi IBM AS/400 e per le aziende di grandi dimensioni di un mainframe come "host" centrale. Dall'analisi si evidenzia come siano ancora attivi sistemi obsoleti e, quindi, molto vulnerabili come Windows NT.

Congruente con la tipologia di sistemi operativi quella delle banche dati, riportata in **fig. 8**.

Il database (DB) più diffuso nel campione dei rispondenti è Microsoft SQL, seguito da Oracle e da MySQL. La presenza di mainframe IBM e di AS/400 porta alla conseguente presenza dei DB tipici per questi ambienti, l'IBM DB2 e il DB 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.

Anche in questo caso, l'omogeneità è tipica degli ambienti piccoli o piccolissimi: per quelli Microsoft la scelta è, tipicamente, per Microsoft SQL, per quelli Linux-Unix MySQL.

Molte aziende di medie dimensioni hanno un AS/400 come "host" centrale e sistemi dipartimentali - distribuiti basati o su sistemi Windows o Unix/Linux.

Per quanto riguarda le infrastrutture di comunicazione, la **fig. 9** sintetizza quali strutture di rete sono in uso nei sistemi informativi di chi ha risposto al questionario. Per le percentuali risultanti si deve tener conto che erano disponibili risposte multiple. Il risultato è che la stragrande maggioranza è basata su una o più reti locali, LAN (Local Area Network), collegate a Internet. Più del 50% di queste ha una copertura geografica e, dato molto significativo, più del 40% ha collegamenti "wireless" (senza fili), tipicamente con Wi-Fi, GMS e UMTS.

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.

Per quanto riguarda la gestione dei sistemi informativi, e in particolare del Data Center, la **fig. 10** mostra come la maggior parte dei sistemi sia gestita direttamente e internamente alle Aziende, e solo il 14% abbia terziarizzato la gestione del Data Center.

5. Gli attacchi informatici rilevati e la loro gestione

La **fig. 11** mette a confronto il numero di attacchi rilevati rispettivamente negli anni 2007 e 2008 come valore in percentuale sul totale dei rispondenti.

È interessante evidenziare come, nel 2007, quasi il 63% dei compilatori del questionario affermi di non aver subito (o rilevato) attacchi: nel 2008 tale numero si riduce al 52,6 %, quindi con un aumento di attacchi rilevati pari, in percentuale sull'anno precedente, a poco più del 10%.

In termini di attacchi, Il 2007 è stato un "annus horribilis", soprattutto per il massiccio e significativo numero di frodi informatiche, confermato dalle analisi di tutti i principali Osservatori internazionali (un elenco non esaustivo in § 10): un esempio per tutti è costituito dal furto di centinaia di migliaia di identità digitali per le carte di credito in TJ Maxx, una catena di grandi magazzini negli Stati Uniti e a Porto Rico. Questo furto, ai tempi, fu considerato la più grande violazione di dati personali nella storia.

Il 2008 è stato in qualche misura ancora peggio e tale trend potrebbe sembrare strano o errato: con l'aumentare della consapevolezza dei problemi sulla sicurezza informatica e l'adozione crescente di misure e tecniche e organizzative, il trend dovrebbe essere di riduzione degli attacchi e delle vulnerabilità dei sistemi.

Invece no, i problemi e i rischi della sicurezza informatica continuano a crescere, e un indicatore forte di tale crescita è la già citata attenzione che il mondo politico e i governi stanno iniziando a dare alla sicurezza informatica. Perfino l'ONU, a seguito della riunione a Davos di fine 2009, sta studiando opportune dichiarazioni per considerare gli attacchi informatici ai sistemi critici di un paese come una "dichiarazione di guerra".

FIG. 11 ATTACCHI RILEVATI 2007/2008 A CONFRONTO

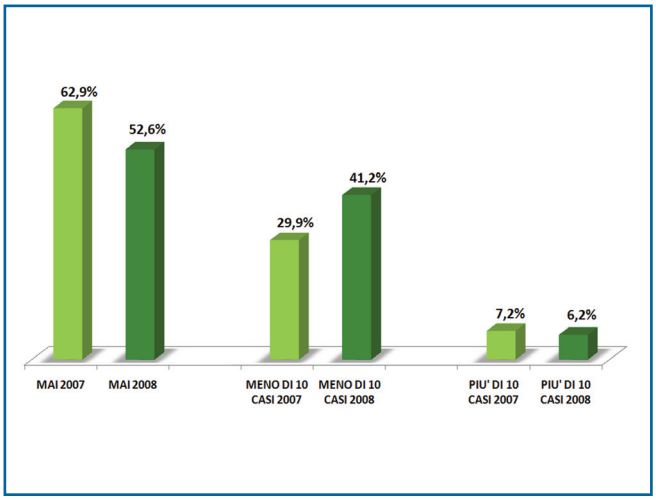


FIG. 12 RILEVAZIONE ATTACCHI 2007/2008 SUL CAMPIONE CHE HA RISPOSTO

	NESSUNO		DA 1 A 5		DA 6 A 10		OLTRE 10	
TEMI	2007	2008	2007	2008	2007	2008	2007	2008
Accesso a ed uso non autorizzato degli elaboratori, delle applicazioni supportate e delle relative informazioni	70%	66%	20%	24%	6%	6%	4%	4%
Modifiche non autorizzate ai programmi applicativi e di sistema, alle configurazioni ecc.	72%	71,5%	24%	24,5%	4%	2%	0%	2%
Modifiche non autorizzate ai dati e alle informazioni	93,9%	86%	6,1%	10%	2%	4%	0%	0%
Utilizzo codici maligni (malware) di varia natura, quali virus, Trojan horses, Rootkit, bots, exploits, sia a livello di posto di lavoro che di server	23,5%	15,7%	54,9%	60,8%	11,8%	7,8%	9,8%	15,7%
Furto di apparati informatici contenenti dati (laptop, hard disk, floppy, nastri, chiavette USB ecc.)	56%	50%	34%	34%	6%	12%	4%	4%
Furto di informazioni o uso illegale di informazioni da dispositivi mobili (palmari, cellulari, laptop)	90%	91,8%	8%	4,1%	2%	4,1%	0%	0%
Furto di informazioni o uso illegale di informazioni da tutte le altre risorse	88%	86%	6%	10%	6%	4%	0%	0%
Attacchi alle reti, fisse o wireless, e ai DNS (Domain Name System)	60%	58%	34%	34%	4%	2%	2%	6%
Frodi tramite uso improprio o manipolazioni non autorizzate e illegali del software applicativo (ad esempio utilizzo di software pirata, copie illegali di applicazioni ecc.)	78%	78%	18%	16%	2%	6%	2%	0%
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 e il furto d'identità digitale	56%	42%	16%	30%	14%	6%	14%	22%
Ricatti sulla continuità operative e sull'integrità dei dati del sistema informativo (ad esempio se non paghi attacco il sistema e ti procuro danni, magari con dimostrazione delle capacità di attacco e di danno conseguente...)	94%	94%	2%	2%	4%	2%	0%	2%
Altri tipi di attacco, quali ad esempio attacchi di tipo misto (Blended threat), sabotaggi, vandalismi con distruzione di risorse informatiche. Se individuato, segnalare il tipo di altro attacco subito	88%	91%	8%	4%	4%	4%	0%	0%

La Tabella in **fig. 12** fornisce il dettaglio, per tipologia di attacco, di quanti hanno rilevato, in percentuale, uno o più attacchi dello stesso tipo nei due anni considerati.
Molte sono le considerazioni che possono derivare da un'attenta analisi di questi dati, nel seguito ci si focalizzerà soprattutto su tre aspetti, che individuano trend particolarmente significativi:
a) la diffusione dei tipi di attacco tra il campione considerato
b) l'incremento o il decremento, tra un anno e l'altro, del tipo di attacco
c) la ricorrenza di più di 10 attacchi dello stesso tipo per singolo sistema informativo.
In termini di diffusione, la **fig. 13** mostra la graduatoria degli attacchi più comuni e ricorrenti.

FIG. 13 ATTACCHI PIÙ DIFFUSI NEL 2008

DIFFUSIONE ATTACCHI PER TIPOLOGIA 2008	COPERTURA (%)	GRADUATORIA
Utilizzo codici maligni (malware) sia a livello di posto di lavoro che di server	84%	1°
Attacchi di Social Engineering e di Phishing	58%	2°
Furto di apparati informatici contenenti dati (laptop, hard disk, floppy, nastri, chiavett	50%	3°
Attacchi alle reti, fisse o wireless, e ai DNS (Domain Name System)	42%	4°
Accesso e ed uso non autorizzato degli elaboratori, delle applicazioni supportate e da	34%	5°
Modifiche non autorizzate ai programmi applicativi e di sistema, alle configurazioni ed	28%	6°
Frodi tramite uso improprio o manipolazioni non autorizzate e illegali del software app	22%	7°
Modifiche non autorizzate ai dati e alle informazioni	14%	8°
Furto di informazioni o uso illegale di informazioni da tutte le altre risorse	14%	8°
Altri tipi di attacco, quali ad esempio attacchi di tipo misto (Blended threat), sabotagg	9%	10°
Furto di informazioni o uso illegale di informazioni da dispositivi mobili (palmari, cellu	8%	11°
Ricatti sulla continuità operativa e sull'integrità dei dati	6%	12°

FIG. 14 VARIAZIONE DELLE TIPOLOGIE DI ATTACCHI RILEVATI TRA 2007 E 2008

INDICATORE TASSO DI CRESCITA - DECRESCITA ATTACCHI

	NESSUNO		DA 1 A 5		DA 6 A 10		OLTRE 10	
TEMI	2007	2008	2007	2008	2007	2008	2007	2008
Accesso e ad uso non autorizzato degli elaboratori, delle applicazioni supportate e delle relative informazioni	70%	66%	20%	24%	6%	6%	4%	4%
Modifiche non autorizzate ai programmi applicativi e di sistema, alle configurazioni ecc.	72%	71,5%	24%	24,5%	4%	2%	0%	2%
Modifiche non autorizzate ai dati e alle informazioni	93,9%	86%	6,1%	10%	2%	4%	0%	0%
Utilizzo codici maligni (malware) di varia natura, quali virus, Trojan horses, Rootkit, bots, exploits, sia a livello di posto di lavoro che di server	23,5%	15,7%	54,9%	60,8%	11,8%	7,8%	9,8%	15,7%
Furto di apparati informatici contenenti dati (laptop, hard disk, floppy, nastri, chiavette USB ecc.)	56%	50%	34%	34%	6%	12%	4%	4%
Furto di informazioni o uso illegale di informazioni da dispositivi mobili (palmari, cellulari, laptop)	90%	91,8%	8%	4,1%	2%	4,1%	0%	0%
Furto di informazioni o uso illegale di informazioni da tutte le altre risorse	88%	86%	6%	10%	6%	4%	0%	0%
Attacchi alle reti, fisse o wireless, e ai DNS (Domain Name System)	60%	58%	34%	34%	4%	2%	2%	6%
Frodi tramite uso improprio o manipolazioni non autorizzate e illegali del software applicativo (ad esempio utilizzo di software pirata, copie illegali di applicazioni ecc.)	78%	78%	18%	16%	2%	6%	2%	0%
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 e il furto d'identità digitale	56%	42%	16%	30%	14%	6%	14%	22%
Ricatti sulla continuità operative e sull'integrità dei dati del sistema informativo (ad esempio se non paghi attacco il sistema e ti procuro danni, magari con dimostrazione delle capacità di attacco e di danno conseguente...)	94%	94%	2%	2%	4%	2%	0%	2%
Altri tipi di attacco, quali ad esempio attacchi di tipo misto (Blended threat), sabotaggi, vandalismi con distruzione di risorse informatiche. Se individuato, segnalare il tipo di altro attacco subito	88%	91%	8%	4%	4%	4%	0%	0%

In termini di variazione degli attacchi tra il 2007 e il 2008, la **fig. 14** fornisce un'indicazione qualitativa, tramite le freccette rosse, di incremento o decremento o stabilizzazione della loro occorrenza sul campione considerato.

Anche da una prima vista delle freccette in **fig. 14** si evidenzia come la maggior parte degli andamenti sia in crescita, seppur con valori diversi e in taluni casi con un andamento ondivago per numero di occorrenze.

Il primato degli attacchi spetta ai codici maligni, diffusi nel campione per l'84%, che ricoprono anche il secondo posto come maggior incremento tra 2007-08 nella Tabella di **fig. 12** con un 8%.

L'attacco dei codici maligni rappresenta per l'Italia un fenomeno ancora preoccupante, nonostante l'uso diffuso di antivirus e antispyware, come indicato nella Tabella di **fig. 17 al § 6.**

Tale dato è comunque in linea con quello rilevato dal Rapporto CSI che pone i virus al primo posto nel 2008 per diffusione, con un netto 50%, seppur leggermente in decrescita rispetto al 2007, dove la diffusione era pari al 52%.

Come spiegato nel libro "Sicurezza digitale" il termine "codice ma-

ligno" (in inglese "malware") 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, i spyware, e così via. Per una prima sintetica descrizione di tali termini si rimanda all'Allegato. Si deve tener conto che non esiste una chiara nomenclatura standardizzata su tali termini e talvolta essi vengono usati con significati diversi dagli stessi fornitori di strumenti di protezione a fini commerciali e di marketing, con un conseguente aumento della confusione terminologica.

Per tale motivo nel questionario OAI si è preferito usare il termine generico di "codice maligno", e di non entrare, per i motivi già spiegati, nel dettaglio dei vari tipi.

Altri rapporti internazionali hanno approfondito il tema, e per il 2008 è emerso che, tra i vari tipi, il più diffuso è stato il cavallo di troia con una diffusione del 46%, seguito con il 14% dai worm, il 12%° dai backdoor, il 6% dai PUP; i virus occupano l'ultimo posto con una diffusione rilevata al 5% del campione USA (i dati sono del Rapporto 2008 di IBM X-Force), a indicare che l'uso sistematico di strumenti antivirus sta ormai dando i suoi frutti.

I codici maligni si basano anche, ma non solo, sulle vulnerabilità dei sistemi, poichè sono in grado di sfruttarle al meglio.

Secondo i dati estrapolati dai vari Rapporti internazionali, la vulnerabilità dei sistemi è aumentata nel 2008 rispetto al 2007 in quantità e in gravità, sia a livello ambienti server che PC. In tali analisi si evidenzia che

- la maggior parte delle vulnerabilità può essere sfruttata da remoto via rete;
- dopo più di un anno dalla loro individuazione, quasi la metà delle vulnerabilità non aveva ancora disponibile dei correttivi;
- per i sistemi operativi, le maggiori vulnerabilità si sono riscontrate per Linux e Apple MAC X10;
- la percentuale maggiore di vulnerabilità e di maggior gravità è stata riscontrata negli ambiti (piattaforme) web, e soprattutto nelle applicazioni web personalizzate; in tale contesto gli attacchi si basano prevalentemente su SQL "injection" oltre che su XSS (cross-site scripting);
- per i PC le maggiori vulnerabilità sono nei browser, anche se diminuite in percentuale rispetto agli anni precedenti, in particolare sui controlli ActiveX, e per gli "embedded exploit" ad esempio nell'uso dei file PDF e delle applicazioni multimediali come Flash;
- sono elevate le vulnerabilità nei software per VoIP, Voice over IP, ma la loro incidenza è per ora limitata dalla loro minore diffusione rispetto ai sistemi operativi e ai browser.

Facendo riferimento alla Tabella di **fig. 17** sugli strumenti di protezione in uso, è significativo che il 95% del campione usi sistemi antivirus e antispyware: ma che cosa fa il restante 5%?

Una possibile spiegazione potrebbe essere che nella comunità di chi si occupa di sicurezza informatica e di sistemi ICT, alcuni considerano inutile e/o inappropriato l'uso dei sistemi anti-malware, normalmente attivi su ogni PC-Client e su ogni server, in quanto appesantirebbero troppo l'elaborazione di ogni trattamento dati. Essi preferiscono selezionare e bloccare quanto più possibile a livello di firewall l'ingresso dei dati nei sistemi, e intervenire, qualora comunque filtrasse un codice maligno, con gli opportuni interventi sistemistici.

Tornando alla "classifica" in **fig. 13**, al secondo posto per diffusione si trovano gli attacchi di "social engineering" (traducibile in italiano come "ingegneria sociale", ma si preferisce il termine inglese), con un 58% del totale. Essi sono invece al primo posto per il maggior tasso di crescita tra 2007-08, con un 18% di aumento. Questi attacchi abbracciano un ampio spettro di casi, tutti relativi al comportamento, alle abitudini, il più delle volte alla disponibilità, alla non conoscenza e alla non malizia dell'utente cui si vogliono carpire fraudolentemente e a sua insaputa informazioni sulle sue identità digitali, quali codici bancari, password, ecc. La maggior parte delle frodi, il più delle volte scoperte troppo tardi, avviene a livello individuale proprio tramite attacchi di questo tipo, che includono anche il phishing. Questo fenomeno è talvolta incluso, statisticamente, in quello dello spamming: rientra infatti nello spamming della posta indesiderata, ma ha obiettivi fraudolenti verso taluni utenti finali poco esperti e più ingenui.

"Spamming" e "phishing" nel corso del 2008 sono stati "specializzati" più e meglio verso i diversi "target" d'utenza, richiedendo loro l'effettuazione di determinate attività come, ad esempio, confermare l'esistenza di un conto bancario, la correttezza dei dati, ecc. La quasi totalità del phishing riguarda il contesto finanziario.

A livello mondiale è cresciuta la battaglia (anche delle forze di polizia) contro i siti che generano questo tipo di traffico: questi ultimi sono prevalentemente nel dominio .com, e un numero crescente nel dominio .cn (per la Cina), e hanno una vita media (ossia il tempo in cui sono operativi) al massimo di una settimana; le aree geografiche di provenienza del maggior numero di questi siti sono USA, Russia e Cina.

Al terzo posto in **fig. 13**, con il 50% del totale, il furto di dispositivi, tipicamente i lap-top: essendo piccoli e portatili, essi hanno un fiorente mercato "dell'usato" e sono rubabili, dato che si nascondono facilmente in una borsa o sotto una giacca, cappotto o impermeabile. La maggior parte delle figure professionali porta sempre con sé il proprio computer, tra casa e luoghi di lavoro, e questo rende assai più complesso, se non praticamente impossibile, un effettivo controllo. Anche per quanto riguarda questo dato i risultati dell'OAI sono in linea con quelli statunitensi del CSI, che nel 2008 ha rilevato una percentuale pari al 42% per quello che riguarda questo attacco. Anche in termini di incremento tra 2007 e 2008, questo genere di attacco raggiunge il podio al 3° posto, con un incremento del 6%.

Al quarto posto, con un 42% di diffusione, gli attacchi alle reti (fisse e wireless) e ai DNS, con un +2% di incremento rispetto al 2007. La diffusione capillare e crescente di Internet e delle reti "wireless" è determinante per la diffusione di tali attacchi, che sono propedeutici per gli accessi non autorizzati ai sistemi, in particolare ai siti web, agli ambienti applicativi supportati e alle informazioni da questi ultimi trattati.

Al quinto posto si piazza l'accesso a e l'uso non autorizzato delle risorse ICT, con un 34% di diffusione ed un +4% di incremento rispetto al 2007, ponendosi quindi al 4° posto per tasso di crescita. E subito dopo, con un 28% di diffusione e un +4% di incremento (che lo posiziona al secondo posto, a pari merito con i codici maligni in termini di crescita) l'attacco più critico e pericoloso, la modifica non autorizzata ai dati e alle informazioni. Più critico e pericoloso in quanto mina il patrimonio informativo aziendale, che è ormai uno dei principali "asset" anche a livello di bilancio; una modifica non autorizzata può essere difficilmente rilevabile in tempi brevi, qualora non siano attivi opportuni strumenti di controllo e verifica; e altrettanto lungo e complesso è ricostruire il dato originale, talvolta con problemi anche legali e/o fiscali. La modifica non autorizzata di un dato è l'ultimo passo nella catena di un attacco strutturato che inizia superando le difese delle reti, che accede ai sistemi, poi alle applicazioni e infine ai dati trattati e archiviati sulle banche dati o sui file system.

La distinzione tra gli attacchi per superare i vari livelli di accesso non è sempre ben rilevata e distinguibile. Ma un conto è un accesso non autorizzato effettuato per carpire illegalmente informazioni, senza alterarle; ben altro è la modifica dei programmi software, delle configurazioni e, soprattutto, dei dati.

Anche il Rapporto CSI, pur con denominazioni in parte diverse, evidenzia come questi tipi di attacchi siano diffusi e si diffondano con tassi crescenti.

Gli altri tipi di attacchi rilevati si posizionano ai livelli inferiori della "classifica" di **fig. 13**, con quote di diffusione man mano più basse e con tassi di crescita a loro volta bassi.

Per quanto riguarda l'aspetto dell'iterazione dell'attacco nel medesimo anno, la Tabella di **fig. 12 (e di fig.14)** mostra un andamento oscillante, attacco per attacco, sia come diffusione che come incremento. Il fatto che siano occorsi più di 10 attacchi dello stesso tipo nell'anno significa che da parte dell'attaccante c'è una forte volontà ripetitiva, o per l'interesse a sfondare le misure di sicurezza, o perché queste ultime sono ritenute prima o poi superabili.

È significativo che gli attacchi di social engineering primeggino per più di 10 occorrenze sia come diffusione (22%), sia come incremento (8%), rispetto al 2007.

5.2 Rivelazione, valutazione e gestione degli attacchi

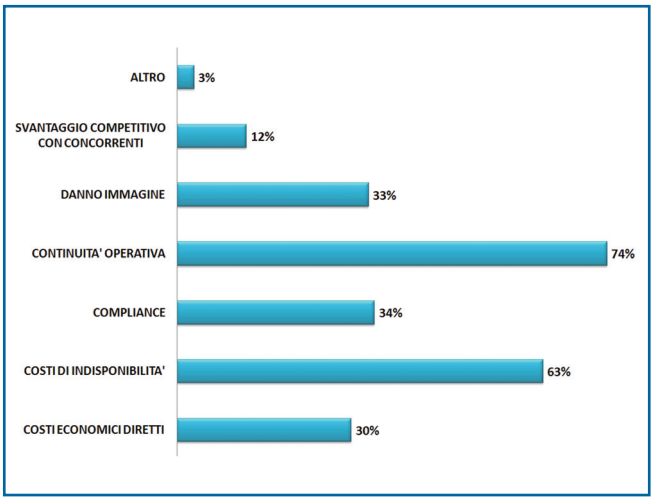
Nella Sezione 2 del questionario sono state poste alcune domande su come l'azienda/ente rilevi, valuti e gestisca l'occorrenza di attacchi, sia che essi vadano o non "a buon fine". Volutamente, almeno per questo primo Rapporto, non sono state richieste valutazioni economiche sui danni: da un lato a causa di un'"intrinseca" difficoltà di valutazione, dall'altra per la "segretezza" di tali dati, che, se eventualmente individuati, ben difficilmente possono essere forniti all'esterno.

Sulle provenienze delle segnalazioni di un attacco le risposte sono state poche, probabilmente perché normalmente non chiaramente individuate e registrate. Le risposte ricevute indicano che le rilevazioni arrivano prevalentemente dai sistemi di monitoraggio e controllo, ivi inclusi i sistemi di "intrusion prevention" e "detection" (IPS/IDS), e a queste seguono le segnalazioni dirette provenienti dagli utenti che si accorgono di malfunzionamenti, furti o di dati impropriamente manipolati.

La **fig. 15** mostra, in percentuale, i principali criteri con i quali viene valutata la criticità e quindi la gravità dell'attacco.

Di gran lungo il criterio più importante è la continuità operativa, a conferma 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 più del 70% dei compilatori: una risposta così ampia indica come ci sia da parte di quasi tutti i compilatori, in particolare dei CIO, una corretta logica di business nella gestione dei sistemi informativi e della loro sicurezza. La conferma dell'importanza della continuità operativa è data da più del 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 30% delle risposte preveda come ulteriore

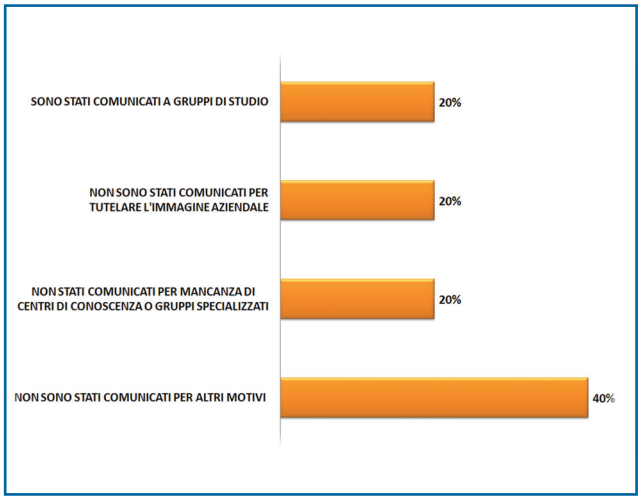
FIG. 15 LOGICHE PER LA VALUTAZIONE DELLA GRAVITÀ DELL'ATTACCO



criterio di valutazione la "compliance" alle normative in vigore. La legge sulla privacy (l'ultimo in vigore è il D.Lgs. 196/2003) ha sicuramente posto e forzato "de iure" l'attenzione sulla sicurezza dei sistemi informativi.

I dati in merito all'informare gli organi istituzionali come la Polizia delle Comunicazioni, in caso di attacco , seppur prevedibili, sono allarmanti: in pratica non si segnala l'occorrenza di un attacco, così come evidenziato nella **fig. 16**. Solo il 20% fornisce informazioni sull'attacco ad "enti esterni" (indicati da "gruppi di studio" nella figura), ossia a consulenti esterni perché analizzino cause e possibili rimedi tecnici e organizzativi.

FIG. 16 COMUNICAZIONE ALL'ESTERNO IN CASO DI ATTACCO



Tra le principali motivazioni di "non comunicazione", anche se non obbligatoria per legge, è preoccupante rilevare che per il 20% è corrisponde alla "non conoscenza" di tali Enti. Una percentuale pari alla ben più accettabile motivazione di non far sapere che si sono subiti attacchi per tutelare l'immagine.

6. Strumenti e politiche di sicurezza ICT adottate

La Tabella in **fig. 17** sintetizza le misure e gli strumenti di sicurezza attualmente in atto nei sistemi informativi, elencandole in graduatoria per percentuale d'adozione sul campione dei compilatori del questionario. Le risposte fanno riferimento all'ultimo anno considerato, ossia al 2008. Nel questionario sono state volutamente inserite misure sia di tipo tecnico sia di tipo organizzativo.

Come già sottolineato nel § 5, le aziende/enti che hanno risposto sono posizionate nella fascia alta, con sistemi informatici abbastanza ben dotati di strumenti tecnici e organizzativi per la loro sicurezza.

I software antivirus e antispyware sono praticamente usati da tutti (95%); i dispositivi firewall, DMZ (DeMilitarized Zone) e i sistemi di identificazione e autenticazione dell'utenza tramite identificativo e password sono adottati da più dell'80% dei compilatori. E il 48% utilizza firewall a livello applicativo, tipicamente per separare i webserver dagli application server e dai database server.

Una percentuale collocabile tra il 50 e l'80% dei rispondenti fa uso di strumenti quali VPN (Virtual Private Network), gestione log, gestione "patch" e aggiornamenti, monitoraggio e controllo sistemi ICT.

Importante evidenziare come il 52% dei rispondenti dichiari di aver definito e di gestire politiche organizzative per la sicurezza ICT. Questo è un indicatore significativo del livello di maturità, per il campione considerato, della sicurezza informatica, confermato da un ancor più significativo 38% che ha formalizzato tali procedure organizzative, e dal 26% che ha automatizzato con opportuni software la gestione della sicurezza informatica.

Il 47% dei sistemi informativi è in logica "alta affidabilità" e il 44% ha "rafforzato" (hardened) in termini di sicurezza le reti "wireless". Il 39% afferma di avere pianificato/attivato soluzioni di "Disaster Recovery", la crittografia è usata dal 42% dei rispondenti nella trasmissione dei dati, e dal 23% per la loro archiviazione.

Una percentuale tra il 30 e il 37%, quindi circa 1/3 dei rispondenti, fa uso di sistemi IPS/IDS e per la gestione delle vulnerabilità.

Si riduce al 20 % l'uso di sistemi PKI, Public Key Infrastructure, e dei certificati digitali per l'autenticazione forte degli utenti, e si riduce al 17% l'uso di "token" di identificazione quali "smart card" e chiavette USB. Queste percentuali sono un chiaro indicatore di come tali tecniche, anche se ben consolidate, non siano ancora ampiamente accettate, probabilmente anche a causa di una certa complessità per la loro attivazione e per il loro uso da parte degli utenti. È significativo rilevare un 6% nell'uso di strumenti di identificazione biometrica. Pur essendo una percentuale piccola, è un chiaro indice di quali saranno nel prossimo futuro i più sicuri e "amichevoli" mezzi di identificazione: riconoscimento firma autografa biometrica, riconoscimento facciale e dell'impronta digitale, ecc. Gli strumenti già ci sono e una loro crescente diffusione consentirà di ridurne i prezzi.

FIG. 17 TECNICHE E STRUMENTI DI SICUREZZA ADOTTATI, ANCHE ORGANIZZATIVI

STRUMENTI E METODOLOGIE DI PROTEZIONE IN USO	PERCENTUALE
Antivirus e antispyware	95%
Firewall e DMZ	85%
Identificazione dell'utente con identificativo d'utente e password	84%
VPN (Virtual Private Network)	79%
Strumenti di gestione delle autorizzazioni (Active Directory, Ldap, Access Control List, policy server)	77%
Uso di strumenti per la gestione delle patch, degli aggiornamenti, delle release	60%
Monitoraggio e controllo funzionalità e prestazioni dei sistemi	58%
Archiviazione e gestione dei log	52%
Politiche (policy) tecnico-organizzative di sicurezza ICT	52%
Firewall e Reverse proxy a livello applicativo	48%
Uso sistemi ad alta affidabilità	47%
Rete Wireless hardened (ad esempio reti chiuse)	44%
Crittografia dei dati in transito (https ecc.)	42%
Disaster Recovery Planning	39%
Uso di procedure organizzative formalizzate nel supporto ai processi inerenti la sicurezza informatica	38%
Sistemi di Individuazione delle Intrusioni (IDS, Intrusion Detection System)	37%
Sistemi di prevenzione delle intrusioni (IPS, Intrusion Prevention Systems)	32%
Vulnerability assessment – scansioni della rete e dei sistemi - Hardening	30%
Crittografia dei dati archiviati (hard disk, chiavi USB ecc.)	23%
Sistemi di PKI (Public Key Infrastructure)	20%
Identificazione dell'utente "forte" con certificati digitali	20%
Uso di strumenti informatici per il supporto dei processi inerenti la sicurezza informatica	26%
Identificazione dell'utente anche tramite apparati "token" (quali chiavi USB, smart card, dispositivi One Time Password ecc.	17%
Software di sicurezza End-Point e NAC, Network Access Control	17%
Utilizzo di un SGSI, Sistema Gestione Sicurezza Informatica, integrato e centralizzato	16%
Uso di specifici strumenti per il controllo della sicurezza intrinseca degli applicativi (ispezione del codice, test di penetrazione ecc.)	8%
Identificazione dell'utente biometrica	6%
Archiviazione remota e sicura dei backup	1%

Per il 2008 sono ancora limitate, ma non trascurabili, le percentuali di chi usa sistemi di sicurezza "end-point", e sistemi della gestione della sicurezza integrati e centralizzati (SGSI, Sistemi Gestione Sicurezza Informatica). Se si confronta il loro 17% con il 58% dei sistemi di monitoraggio e controllo, si può ragionevolmente desumere che questi ultimi sono usati prevalentemente solo per il controllo delle funzionalità e delle prestazioni dei sistemi, e non sono stati ampliati per includere anche il controllo e la gestione della sicurezza, che probabilmente viene gestita "a silos" verticali e separati per i diversi ambienti (Microsoft, Linux/Unix, Data Base, siti web, ecc.).

Veramente preoccupante il minimo uso (8%, probabilmente da parte delle grandi organizzazioni finanziarie e di qualche multinazionale) di controlli sulla sicurezza intrinseca del software usato, ivi inclusi gli applicativi. Lo sviluppo del software è ormai ben consolidato con le logiche della programmazione a oggetti: la realizzazione di programmi si basa prevalentemente sull'assemblaggio di moduli preesistenti, e sulla loro personalizzazione o su loro piccole modifiche. Esistono innumerevoli moduli, gratuiti o a pagamento in Internet, la maggior parte dei quali interoperanti con altri grazie agli standard della SOA, Service Oriented Architecture, indipendentemente dai linguaggi con i quali sono stati scritti e dai sistemi operativi e dagli ambienti sui quali sono eseguiti. Ma questi moduli sono stati progettati e implementati in maniera intrinsecamente sicura? Chi li utilizza e li assembla per realizzare altri programmi verifica che siano veramente sicuri?

Nel complesso delle risposte avute, risulta assai basso il valore dell' 1% per l'archiviazione remota e sicura dei backup: la sistematica copia dei back-up (o dell'intero sistema) su storage remoti, tipicamente tramite fornitori terzi (provider), è una pratica efficace e poco costosa, soprattutto con la disponibilità di collegamenti xDSL, ed è strano che siano così pochi a utilizzare questo tipo di servizio.

Le considerazioni sopra esposte fanno riferimento all'analisi dei dati ricevuti indipendentemente dal settore di appartenenza.

I grafici seguenti dettagliano l'uso dei sistemi di sicurezza per i seguenti macro settori:

- **Industria**: include l'industria manifatturiera e farmaceutica **(fig. 18)**;
- **Servizi**: include Banche, Assicurazioni, Utilities, Distribuzione/Retail, Trasporti, Servizi Professionali, Sanità, Istituzioni Finanziarie non Bancarie, Istruzione & Ricerca **(fig. 19)**;
- **Settore ICT**: si è preferito tenerlo separato per la sua importanza nel contesto della sicurezza informatica e include sia produttori sia erogatori di servizi di telecomunicazione e informatici **(fig. 20)**;
- **Pubbliche Amministrazioni:** PAC e PAL **(fig. 21)**;
- **Altro**: include coloro che non hanno specificato l'appartenenza ad una categoria **(fig. 22)**.

Le scale in ordinata nelle varie figure sono tutte normalizzate al 100% per facilitare il confronto.

Innumerevoli considerazioni possono emergere nel confrontare i dati di queste figure sull'utilizzo degli strumenti di sicurezza per settore, e

FIG. 18 DISTRIBUZIONE MISURE DI SICUREZZA INFORMATICA NEL SETTORE INDUSTRIA

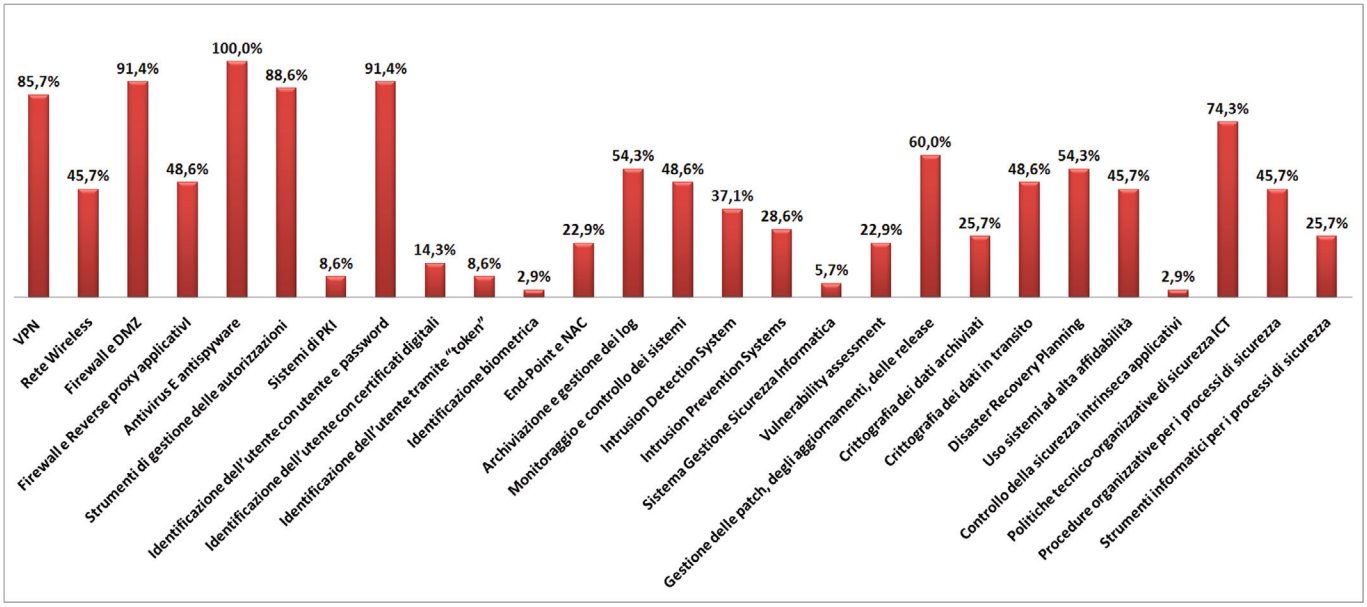


FIG. 19 DISTRIBUZIONE MISURE DI SICUREZZA INFORMATICA NEL SETTORE SERVIZI

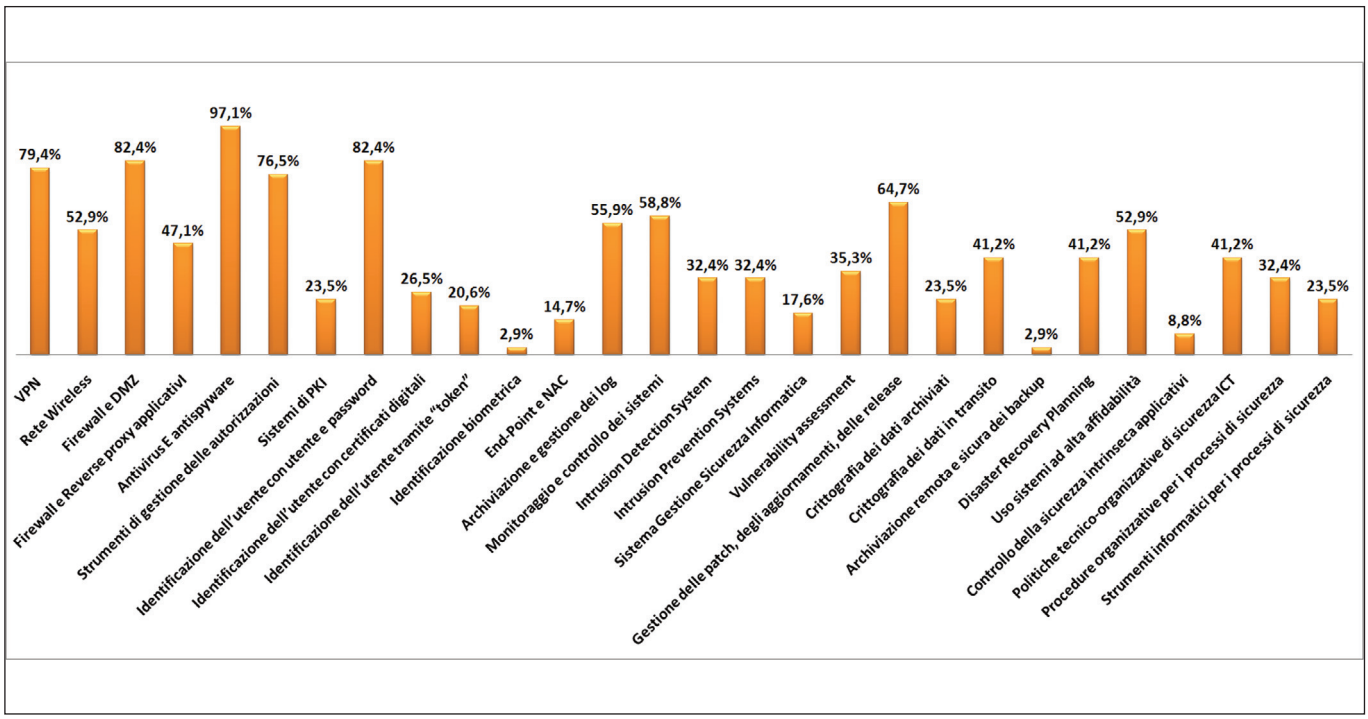


FIG. 20 DISTRIBUZIONE MISURE DI SICUREZZA INFORMATICA NEL SETTORE ICT

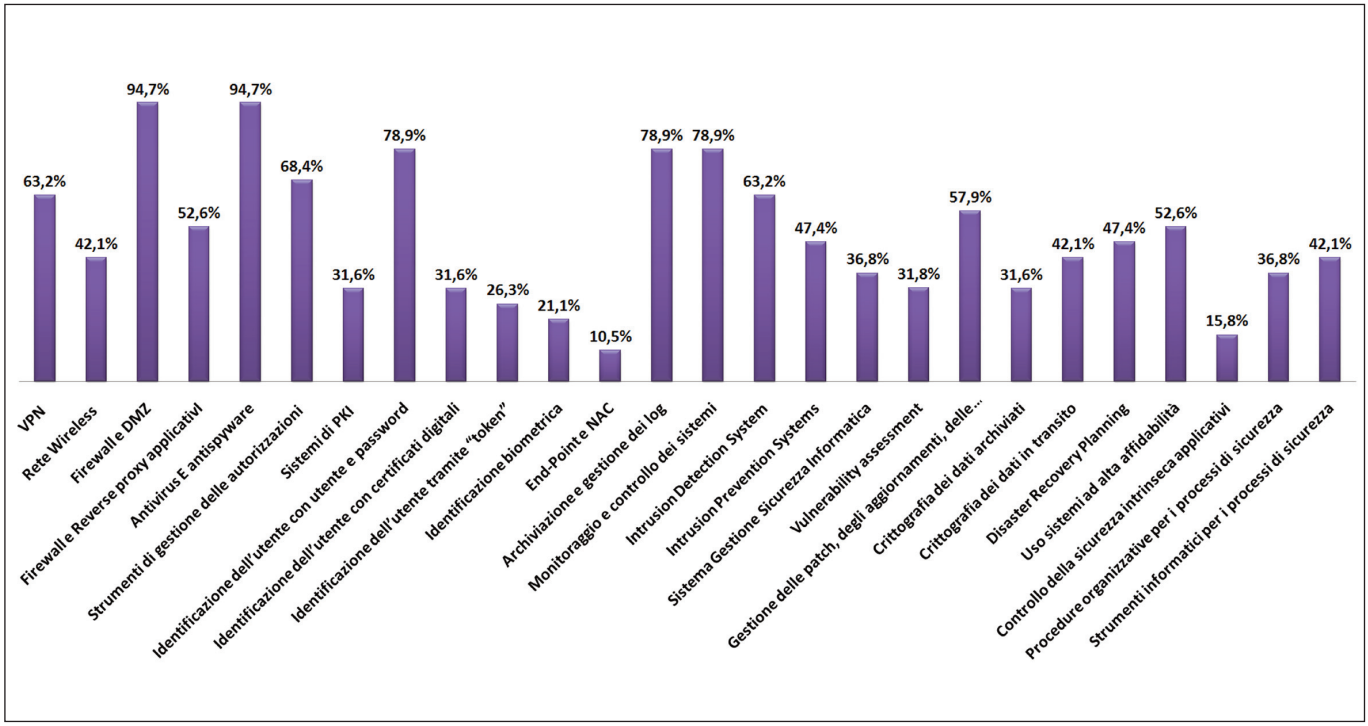


FIG. 21 DISTRIBUZIONE MISURE DI SICUREZZA INFORMATICA NEL SETTORE PUBBLICA AMMINISTRAZIONE

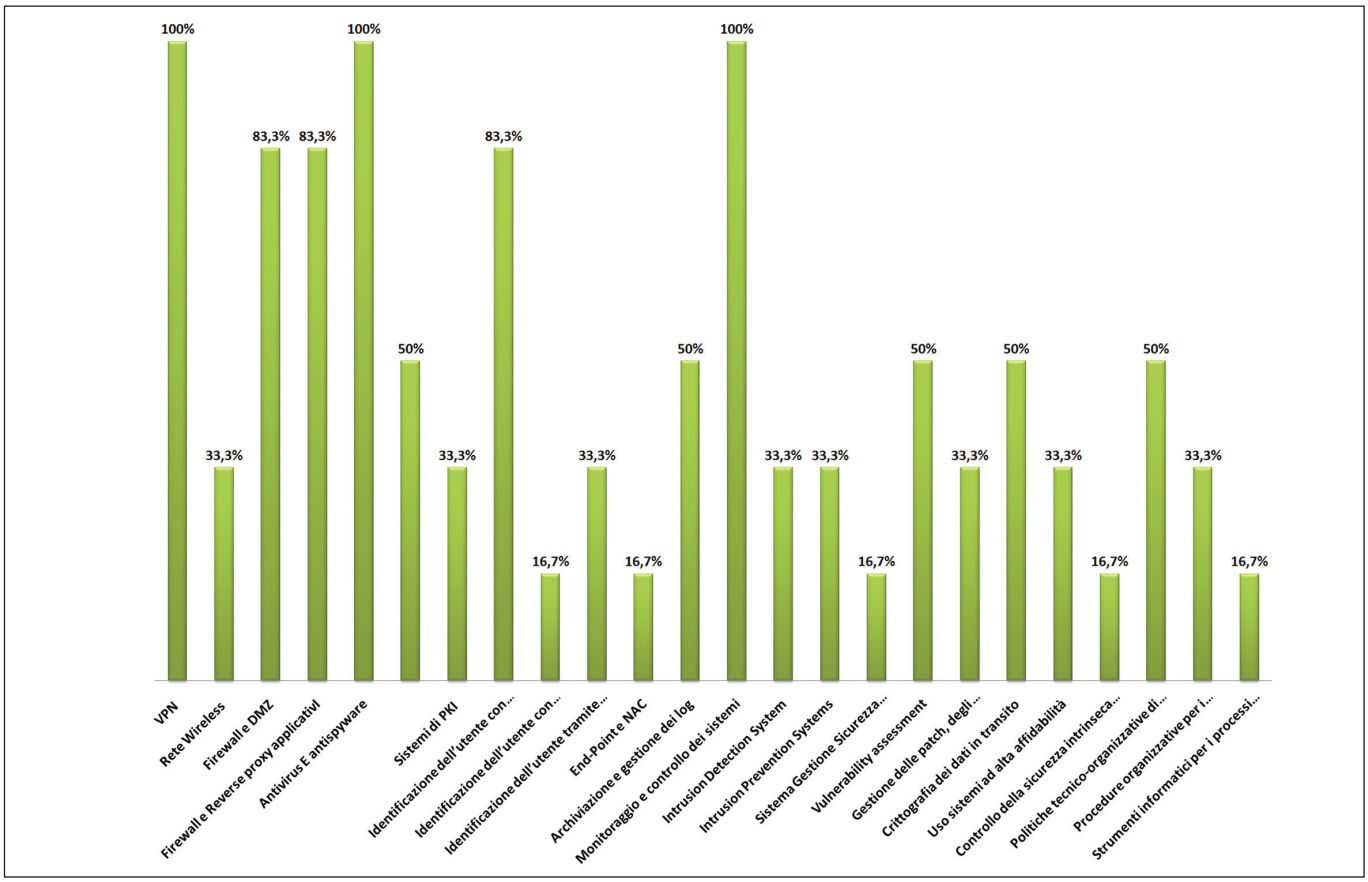
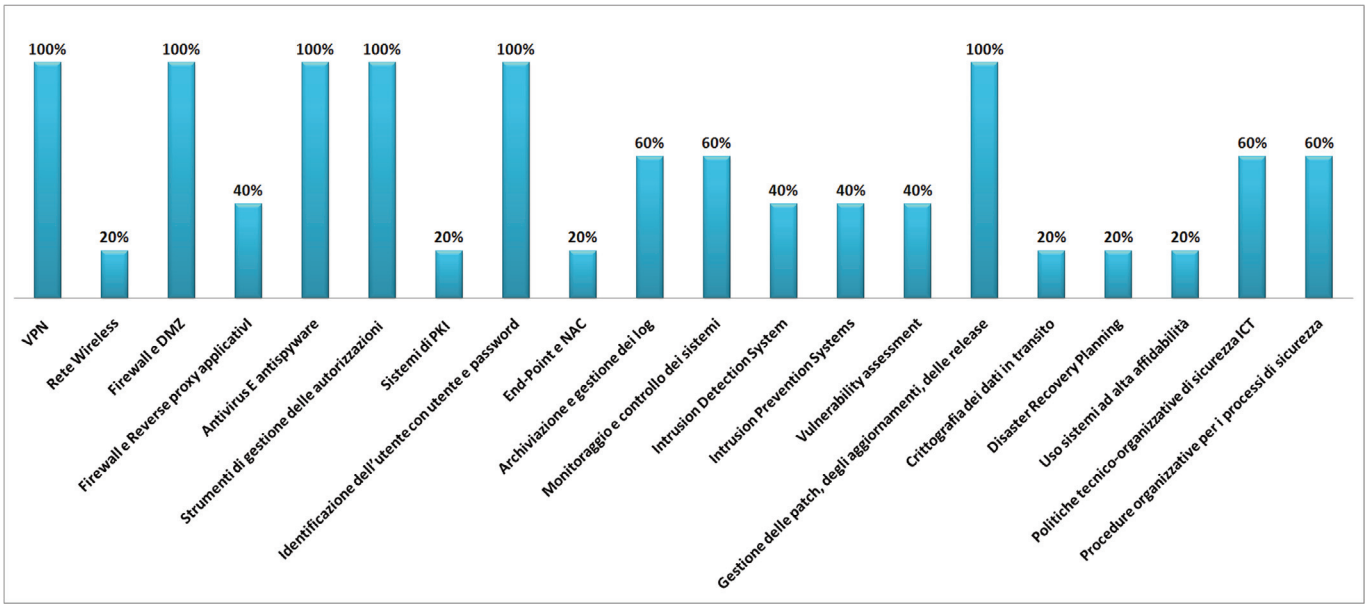


FIG. 22 DISTRIBUZIONE MISURE DI SICUREZZA INFORMATICA NEL SETTORE ALTRO



tra queste si ritiene opportuno evidenziare come:

- i settori servizi e ICT abbiano un buon "bilanciamento" tra i diversi tipi di misure e strumenti;
- il settore industria sia piuttosto carente sui vari strumenti di controllo, monitoraggio, IPS/IDS, e sui sistemi più avanzati di identificazione e autenticazione;
- le PA non dispongono o dispongono in maniera ridotta di sistemi ad alta affidabilità, di strumenti di crittografia, di autenticazione forte degli utenti. È anche limitata la diffusione di policy della sicurezza e delle procedure organizzative.

Di particolare importanza gli aspetti organizzativi per gestire correttamente ed efficacemente la sicurezza di un sistema informativo: aspetti che erano, fino a pochi anni fa, assai deboli se non inesistenti in gran parte delle Aziende/Enti in Italia.

Come già evidenziato nel commentare la Tabella di **fig. 17**, la situazione, almeno per i compilatori del questionario, è nettamente migliorata: ben il 58% dei rispondenti afferma di avere delle policy di sicurezza.

Per la parte di chi si è già dotato di una "policy" per la sicurezza informatica, la **fig. 23** mostra il dettaglio di come è stata comunicata al proprio interno. Ai tradizionali mezzi di comunicazione, quali circolari cartacee e corsi, si affianca, e prevale percentualmente, l'invio tramite posta elettronica.

Solo una minima percentuale ha risposto di rendere disponibili le policy via Intranet: questo indica come l'Intranet aziendale, se esiste, sia ancora poco o per nulla usata per le comunicazioni dell'Unità Organizzativa Sistema Informativi.

Sempre in tema di organizzazione e gestione della sicurezza informatica, il questionario ha posto domande sull'attività di auditing per la sicurezza informatica.

La **fig. 24** indica che il 50% dei rispondenti effettua tale attività, che il 28% ha pianificato di attuarla a breve, e che solo il 22% non ce l'ha. Questo dato è un ulteriore indicatore che le aziende/enti che hanno risposto rappresentano nel contesto italiano un'elite per quanto riguarda la sicurezza informatica e la sua gestione.

La **fig. 25** dettaglia, per chi già svolge attività di auditing per i propri sistemi informativi, come essa venga attuata.

Dalla **fig. 25** emerge che la maggior parte dei rispondenti effettua controlli su base annuale, ma è interessante evidenziare come più del 10% delle risposte evidenzi che l'auditing è visto e gestito come un processo di miglioramento continuo dell'ICT e dei servizi che esso eroga all'azienda/ente.

FIG. 23 MEZZI CON I QUALI È STATA COMUNICATA LA POLICY SULLA SICUREZZA QUALORA SIA STATA DEFINITTA

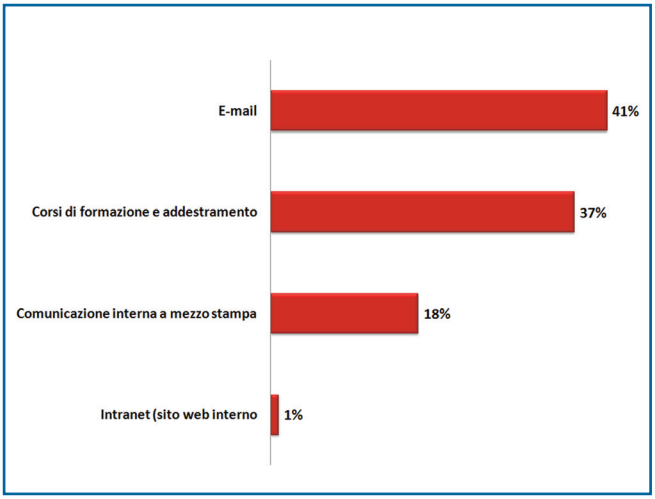


FIG. 24 FUNZIONI DI AUDITING PER LA SICUREZZA INFORMATICA

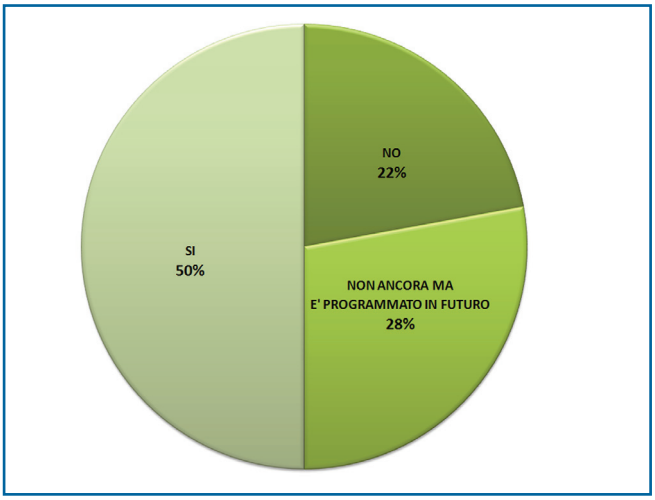
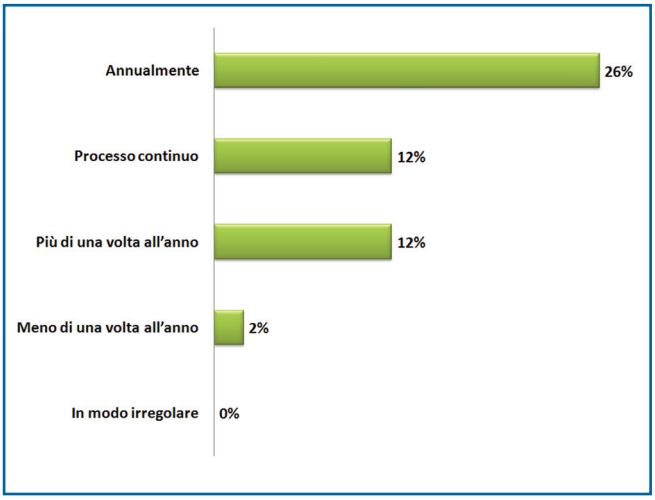


FIG. 25 AUDITING PER LA SICUREZZA DEI SISTEMI INFORMATIVI



Per completare la fotografia delle misure di sicurezza in atto, soprattutto di tipo organizzativo-procedurale, la **fig. 26** mostra che una nutrita maggioranza, il 61%, segue standard e best practice per la gestione della sicurezza ICT, di questi ben il 42% hanno già ottenuto la formale certificazione, come evidenziato nella **fig. 27**.

Gli standard e le best practice indicate nel questionario includono:

- ISO 27000 per la gestione della sicurezza informatica;
- ISO 20000-ITIL per la gestione dei servizi ICT;
- ISO 9000 per la gestione della qualità.

La **fig. 28** dettaglia come, tra coloro che sono conformi e/o certificati, il 16% è conforme alla famiglia di standard ISO 27000, e il 6% ha già effettuato il complesso e impegnativo processo di certificazione. Altrettanto interessante rilevare che il 20% già ha impostato la gestione dei suoi sistemi informativi secondo le best practice ITIL.

Importante poi evidenziare come il 28% segua le logiche della qualità totale, standardizzata dalla famiglia di standard ISO 9000 e di questi il 24% sia già certificato. Queste percentuali sono un'ulteriore conferma che il campione dell'indagine dell'OAI è nella fascia alta e che l'attività pluriennale di sensibilizzazione e di trasferimento di conoscenza da parte di riviste, convegni, associazioni di categoria e specifiche di settore ha dato e sta dando i suoi frutti.

FIG. 26 CONFORMITÀ A STANDARD E BEST PRACTICE

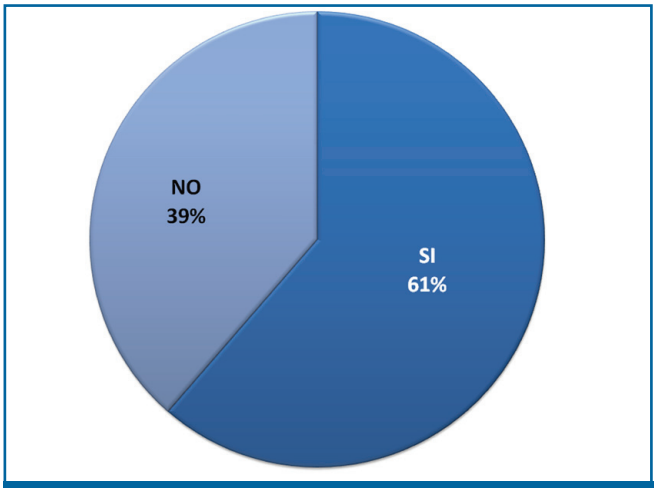


FIG. 27 CERTIFICAZIONE

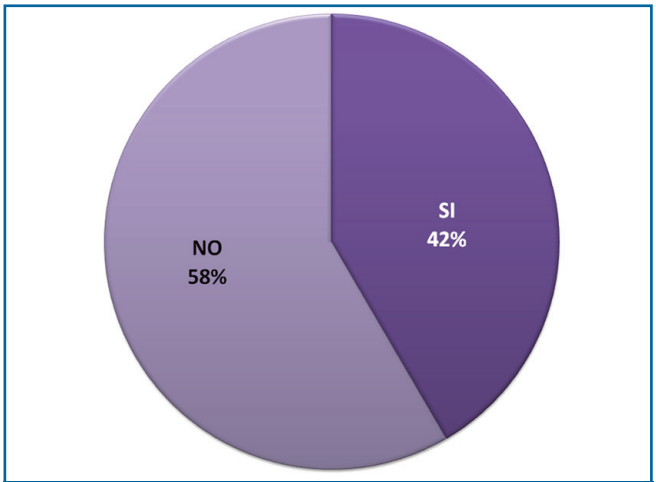
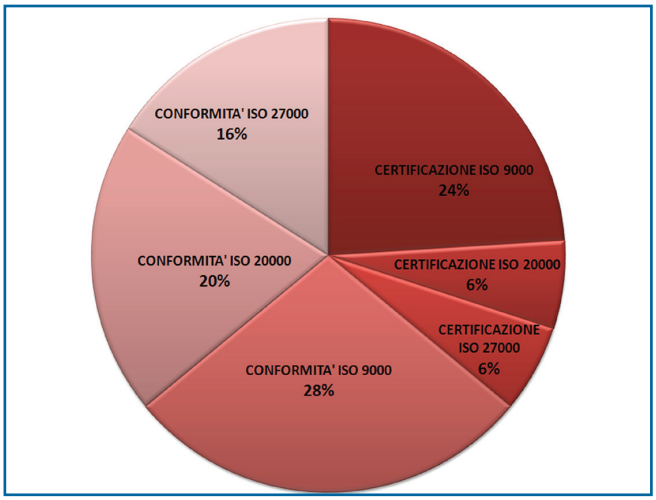


FIG. 28 DETTAGLIO CONFORMITÀ E CERTIFICAZIONI AGLI STANDARD



7. Gli attacchi più temuti e chi li potrebbe perpetrare

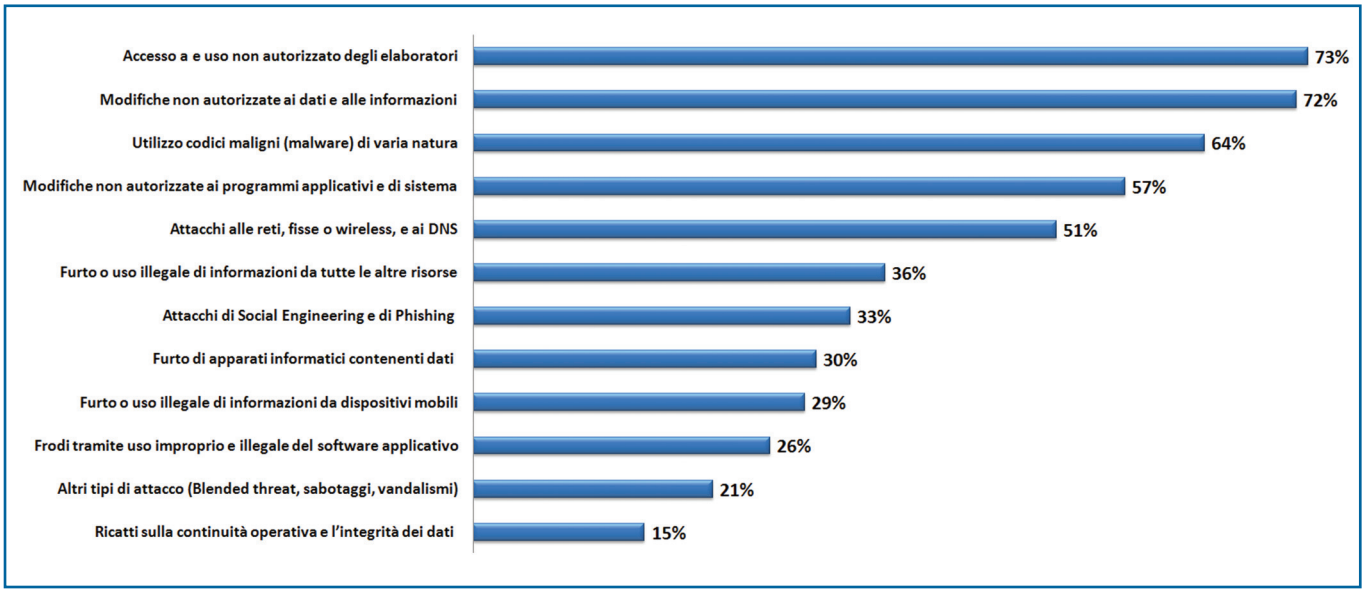
La sezione finale del questionario richiede una previsione di quali saranno gli attacchi più probabili e più temuti, e da quali motivazioni l'attaccante potrebbe o dovrebbe essere guidato.

Le risposte ottenute, sintetizzate nella **fig. 29**, ricalcano in gran misura gli attacchi subiti o di cui si è avuto notizia, tipicamente nei convegni, dalla stampa, dalle associazioni e dai siti specializzati.

Gli attacchi più temuti, superiori al 70% di tutti i rispondenti, sono l'accesso non autorizzato ai sistemi e ai dati/informazioni che trattano. Seguono, posizionandosi oltre il 60% o oltre il 50% delle risposte, i codici maligni, le modifiche non autorizzate ai sistemi e ai programmi applicativi e gli attacchi alle reti ed ai DNS.

La differenza percentuale tra modifiche non autorizzate ai dati/informazioni rispetto ai programmi applicativi rispecchia una realtà di fatto: è oggi assai più facile modificare, senza autorizzazione, dati e informazioni rispetto ai programmi applicativi e alle configurazioni dei sistemi. Per queste ultime occorrono competenze e conoscenze specifiche, e diritti d'accesso non facili da superare; per i primi possono essere sufficienti furbi attacchi di social engineering. E questo è confermato da più del 30% che teme il social enginering e il phishing, e da una percentuale poco inferiore che teme il furto di informazioni e/o il loro uso illegale; se consideriamo le attuali capacità di hard-disk esterni tascabili con interfaccia USB, che arrivano a 0,5-1 Tera, ben si comprende la facilità di asporto di grandi quantità di informazioni… con un semplice "copia e incolla".

FIG. 29 RIPARTIZIONE DEI POTENZIALI ATTACCHI MAGGIORMENTE TEMUTI



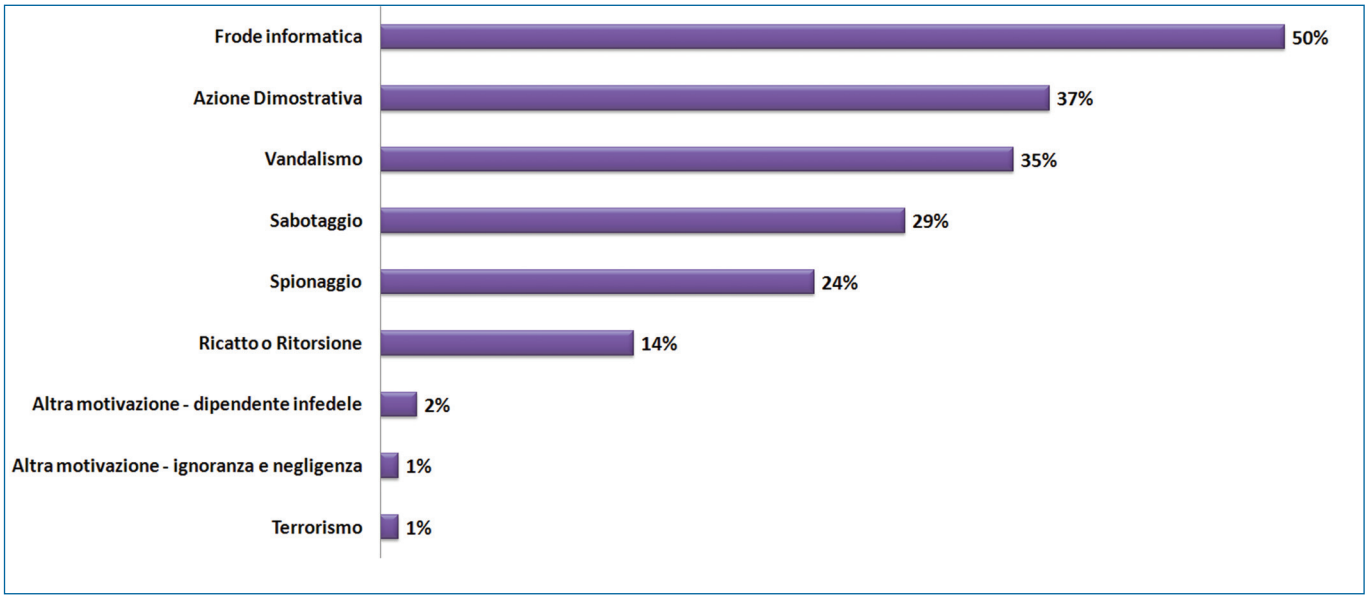
Di particolare interesse le motivazioni per gli attaccanti, riportate in **fig. 30**. Esse confermano quanto detto nel § 5 sulla prevalente origine criminale degli attacchi: il 50% ritiene, infatti, che la motivazione sia la frode informatica, con l'obiettivo di "fare soldi", e poco più del 35% sia per motivi dimostrativi. Poco meno di questa percentuale è attribuita a motivi vandalici, e a scendere sabotaggio, spionaggio e ricatto/ritorsione. Anche queste ultime sono azioni criminali, ma il loro obiettivo primario non è solamente economico.

L'atto di terrorismo ha una percentuale insignificante, almeno per il campione che ha risposto: i pochi rispondenti appartengono prevalentemente a organizzazioni di grande visibilità, che potrebbero essere nel mirino di gruppi terroristici.

Stupisce la percentuale molto bassa sull'ignoranza/negligenza degli operatori/utenti, in altre parole sui possibili danni causati da operazioni mal eseguite da parte degli addetti ai lavori, in particolare dal personale dei Data Center. Questi sono a tutti gli effetti degli attacchi, anche se non volontari, causati da operazioni errate o mal eseguite, ad esempio, per non aver ben letto i manuali di istruzione, oppure per errore. Ormai da tempo le statistiche dei vari rapporti internazionali rilevano che gli errori umani sui computer sono la principale causa dei danni a essi e da essi causati. Strano quindi che solo pochissimi compilatori abbiano previsto queste cause, che sono fisiologiche e significative per qualsiasi sistema informativo.

Poche anche le risposte relative ad altre motivazioni, quali il dipendente infedele; le azioni di un dipendente o ex dipendente arrabbiato con l'azienda/ente possono sicuramente rientrare in vandalismi, ritorsioni, azioni dimostrative, al limite anche allo spionaggio con aziende concorrenti.

FIG. 30 RIPARTIZIONE DELLE MOTIVAZIONI PER I POTENZIALI ATTACCHI MAGGIORMENTE TEMUTI



8. Conclusioni

L'analisi dei dati OAI 2009 conferma anche per l'Italia le tendenze emerse a livello internazionale, con alcune specificità tipicamente 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; l'adozione di policy, di standard e di best practice è un chiaro indicatore di tale tendenza;
- il fenomeno del social engineering è particolarmente grave e la sua efficacia è dovuta essenzialmente alla poca informazione e consapevolezza dei rischi di una parte non trascurabile degli utenti finali;
- nonostante la probabile fascia alta del campione OAI 2009, la gestione "intergrata" della sicurezza ICT è ancora limitata, così come gli strumenti informatici a supporto;
- solo di pochissimi, probabilmente grandi Aziende/Enti, i controlli sulla sicurezza intrinseca del software messo in produzione;
- la crescente adozione di (relativamente) nuove tecniche, quali la virtualizzazione dei sistemi, il web 2.0 e i sistemi collaborativi, i social network, i web service, il cloud computing e i servizi a consumo (XaaS) allarga fortemente la potenzialità di nuovi attacchi non ancora ben conosciuti e ben contrastati da idonee misure e strumenti.

Nel periodo considerato, gli anni 2007 e 2008, è avvenuto a livello mondiale, e anche per l'Italia, un salto qualitativo e quantitativo nell'ambito delle frodi informatiche. Gli attacchi volontari sono sempre più dettati da finalità criminali. I criminali informatici sono alla ricerca di informazioni che possano facilmente trasformare 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 PC dell'utente finale. In entrambi i casi si fa gran uso del "social engineering". Con l'utenza finale, oltre alle tecniche di "phishing", molte informazioni sono rubate grazie a "spyware" operanti a sua insaputa sui PC. Gli attacchi informatici sono un business di interesse crescente per la malavita organizzata.

I macro-trend sugli attacchi e sulle misure di prevenzione e di ripristino sono simili per l'Italia e per il resto del mondo. Gli attacchi "classici", prevalentemente basati sulle vulnerabilità dei sistemi, la fanno ancora da padrone, e si focalizzano prevalentemente sui siti web e sulle loro applicazioni. La mancanza di "patch" a breve per eliminare molte di tali vulnerabilità consente ampio spazio agli attaccanti, focalizzati a ottenere significativi ritorni economici.

Con varie tecniche, ivi inclusi il social engineering e l'uso improprio delle risorse ICT dall'interno delle strutture, crescono gli accessi non autorizzati a reti, sistemi, applicativi e dati, sia per carpire informazioni sia per manomettere tali ambienti e le informazioni trattate.

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 di queste ultime implica il non funzionamento delle infrastrutture stesse, con tutte le conseguenze facilmente immaginabili: pensiamo 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 essenziali per il loro funzionamento: 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 nonostante tutto fino ad oggi sono stati relativamente limitati e arginabili: ma per quanto e fino a quando non ci saranno forti e decisivi attacchi della criminalità organizzata e di stati "canaglia"?

Nel clima di allarme permanente che si è determinato dopo il settembre 2001, in una situazione nella quale Internet è simile alla caotica situazione del traffico stradale, nel quale 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.

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 negli scorsi anni da varie Istituzioni Internazionali, ad esempio le linee guida "Towards a Culture of Security" , elaborate dall'OCSE, per la crescita della cultura della sicurezza ICT sia presso gli utenti sia presso i forni-

tori 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. 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 baes 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.

Allegato

Glossario dei principali termini tecnici inglesi

- *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
- *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.
- *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.
- *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.
- *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.
- *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
- *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.
- *Zombies:* vedi bots.

L'autore

Ing. Marco Rodolfo Alessandro Bozzetti

Si occupa di ICT da più di 35 anni, è ha operato con responsabilità crescenti presso primarie imprese di produzione, quali Olivetti e Italtel, e di consulenza, quali Arthur Andersen.
È stato anche responsabile dei sistemi informativi dell'intero Gruppo ENI.
È Amministratore unico di Malabo Srl (www.malaboadvisoring.it) e opera 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, e fu ideatore di EITO, European IT Observatory, e di OCI, Osservatorio Criminalità ICT in Italia, pubblicato dall'FTI, Forum delle Tecnologie dell'Informazione. È stato Presidente di FidaInform, di SicurForum in FTI e del ClubTI di Milano, oltre che componente del Consiglio del Terziario Innovativo di Assolombarda.
È ora VicePresidente di FIDAInform, membro del Consiglio Direttivo del ClubTI di Milano e di AIPSI, Socio fondatore e componente del Comitato Scientifico dell'FTI, socio di itSMF.
Ha pubblicato articoli e libri sull'evoluzione tecnologica, la sicurezza informatica e sul lavoro, gli scenari e gli impatti dell'ICT.
Appassionato di alpinismo e sci, pratica anche vela, sub e golf.

Editore

Soiel International s.r.l. – Via Martiri Oscuri, 3 – 20125 Milano
Autorizz. – Trib. Milano n.432 del 22-11-1980.
Iscritta al Registro degli Operatori di Comunicazione n.2111

È vietata la riproduzione, anche parziale, di quanto pubblicato
senza la preventiva autorizzazione scritta di Soiel International o dell'autore Marco R. A. Bozzetti