powered by IBM

La sicurezza delle reti aziendali ai tempi di Facebook

I contributi della wiki IBM sull'utilizzo dei social network e la sicurezza delle infrastrutture IT in ambito di business.

Attribuzione
Non commerciale
Non opere derivate

INTRODUZIONE

"La sicurezza delle reti aziendali ai tempi di Facebook" è il titolo del progetto wiki promosso da IBM per discutere sul tema della sicurezza informatica e, nello specifico, su come l'utilizzo dei social network si ripercuote sulla sicurezza delle strutture aziendali, nonché sui rischi che ne derivano.

Il progetto è rivolto in particolare alle persone e alle aziende che non hanno fiducia nei social network a causa dei pericoli derivanti per i loro sistemi e la riservatezza dei dati. Si vuole pertanto diffondere la consapevolezza e la cultura per un uso responsabile: il fenomeno social network, infatti, ormai non è più arginabile e non si può eliminarlo nel contesto aziendale semplicemente bloccandone l'accesso. Per il bene dell'azienda, bisogna invece cercare di comprenderlo e guidarlo in modo adeguato e consapevole.

Il presente documento raccoglie interventi, best practice e spunti emersi durante l'attività della pagina wiki.

Il progetto è stato coordinato dal Dott. Roberto Marmo, consulente informatico e professore a contratto di informatica presso la Facoltà di Ingegneria della Università di Pavia e Facoltà Scienze MM.FF.NN. della Università Insubria di Como. www.robertomarmo.net

Alcuni spunti sono stati discussi all'evento IBM Security Day 2009: un estratto dell'intervento di Adrian Davis, responsabile ISF, si trova nella sezione "La possibilità di fare uscire informazioni riservate dal posto di lavoro tramite il canale"; le presentazioni della giornata sono invece pubblicate qui.

INDICE

WEB 2.0, SOCIAL MEDIA E SOCIAL NETWORK

Il Web 2.0 è l'insieme delle tecnologie collaborative per organizzare Internet come una piattaforma in cui tutti possono inserire i propri contributi ed interagire con gli altri utenti.

Il termine nasce da una frase coniata da O'Reilly e da Dale Dougherty nel 2004; il documento che ne ha ufficialmente sancito l'inizio risale al 30 settembre del 2005.
Nato da collegamenti ad Internet molto più veloci e dall'unione di varie tecnologie di facile apprendimento e uso, il Web 2.0 vuole segnare una separazione netta con la New Economy dell'inizio millennio definita come Web 1.0 e caratterizzata da siti statici, di sola consultazione e con scarsa possibilità di interazione dell'utente.
Altri approfondimenti su it.wikipedia.org/wiki/Web_2.0

"Social media" è un termine generico per indicare tecnologie e pratiche online con cui gli utenti creano e condividono i contenuti sul Web: un grosso cambiamento rispetto al Web 1.0, caratterizzato dalla presenza di una comunità concentrata sulla condivisione di contenuti.
Altri approfondimenti su it.wikipedia.org/wiki/Social_media

Una delle più grosse opportunità fornite dal Web 2.0 sono i social network o reti sociali, con cui le persone creano un profilo con i dati personali e possono comunicare con altri profili per creare nuove forme di socializzazione e di espressione.

Attualmente vari milioni di italiani possiedono un profilo, e questo si traduce di fatto in una enorme piattaforma di comunicazione. Facebook è l'esempio più noto; per l'ambito professionale esistono i business social network come LinkedIn o Viadeo in cui il professionista può promuovere le proprie capacità, aggiornarsi, trovare collaboratori e nuove opportunità.
Altri approfondimenti su it.wikipedia.org/wiki/Social_network

Ma i social network non riguardano solo le persone: la presenza di aziende è sempre più forte, sia per attività di marketing e pubblicità, sia come nuovo strumento per svolgere le attività di business, creare profili aziendali per promuovere l'impresa, fare nuovi affari eccetera. L'Enterprise 2.0 intende infatti adattare i concetti del Web 2.0 in ambito aziendale.
Altri approfondimenti su it.wikipedia.org/wiki/Enterprise_2.0

IL CONTESTO DELLA SICUREZZA INFORMATICA

La sicurezza informatica ha come obiettivi:

- controllare il diritto di accesso alle informazioni;
- proteggere le risorse da danneggiamenti volontari o involontari;
- proteggere le informazioni mentre esse sono in transito sulla rete;
- verificare l'identità dell'interlocutore, in particolare essere certi che sia veramente chi dice di essere.

Per creare sicurezza bisogna prima studiare:

- chi può attaccare il sistema, perché lo fa e cosa cerca;
- quali sono i punti deboli del sistema;
- quanto costa la sicurezza rispetto al valore da proteggere e rispetto al valore dei danni causati;
- con quale cadenza gli apparati/sistemi di sicurezza vengono aggiornati.

Il ciclo di vita della sicurezza informatica prevede:

1. **Prevention** - è necessario implementare delle misure per prevenire lo sfruttamento delle vulnerabilità del sistema;
2. **Detection** - è importante rilevare prontamente il problema; prima si rileva, più semplice è la sua risoluzione;
3. **Response** - bisogna sviluppare un piano appropriato di intervento in caso di violazione con individuazione delle responsabilità e azioni da intraprendere.

Occorre tenere ben presente l'importanza del documento di Auditing del sistema: il documento analizza la struttura del sistema e individua le operazioni atte a verificare il suo stato di salute con varie tipologie di verifica della sicurezza.

Gli elementi da considerare in un progetto di sicurezza informatica sono, nell'ordine:

1. beni da proteggere;
2. minacce;
3. agenti;
4. vulnerabilità;
5. vincoli;
6. misure di protezione.

Gli elementi elencati sono raccolti nel documento di Risk Analysis, che permette di sapere qual è il rischio di subire danni al sistema informatico e, conseguentemente, di preparare una mappa delle possibili contromisure da adottare.

La nascita di nuovi problemi per la sicurezza informatica

L'uso sempre più diffuso delle reti sociali ha portato a una forte crescita delle opportunità, dei vantaggi, della quantità di informazioni. Il rapido sviluppo, però, non ha ancora permesso un'esatta e profonda conoscenza da parte di molte persone dei meccanismi e della gestione della presenza nei social network. Ecco la forte crescita degli svantaggi e di ricadute negative dovute a furti e truffe di vario tipo, oltre alle eventuali fonti di distrazione e perdite di tempo. L'uso degli strumenti tradizionali della sicurezza informatica può fronteggiare solo in parte i nuovi pericoli e bisogna perfezionare tali strumenti per adattarli a una piattaforma di comunicazione in grado di far interagire persone con esigenze molto diverse.

LA DIFFUSIONE DELLE INFORMAZIONI

Secondo alcune statistiche redatte da fonti affidabili, quasi il 90% delle grandi aziende svolge la propria attività anche attraverso Internet o, almeno, possiede un sito Web di riferimento per la clientela: oltre alle numerose realtà private, anche tantissime strutture pubbliche offrono i loro servizi attraverso la grande Rete.

Questo scenario, che da un lato procura innegabili vantaggi ai cittadini, dall'altro genera situazioni di pericolo connesse alle possibili azioni criminali che alcuni malintenzionati potrebbero mettere in atto: danni economici, violazioni di privacy o, semplicemente, una perdita della credibilità derivante da azioni di defacement (termine anglosassone traducibile in "deturpazione", utilizzato per indicare un'azione svolta nei confronti di un sito Web allo scopo di cambiarne i contenuti), rappresentano solo una ristretta rosa di possibili esempi.
Per queste ragioni è assolutamente necessario che ciascun utente in rete operi attivamente in questa sorta di battaglia in difesa di coloro che da Internet vogliono trarre tutti i benefici possibili e contro quelli che, invece, sfruttano la Rete per perseguire fini più o meno illegali: un'azione del genere è possibile solo attraverso una corretta informazione e preparazione.
L'obiettivo primario è quello di fornire a ciascun utente le nozioni necessarie per implementare autonomamente sul proprio sistema quelle misure minime di sicurezza che gli consentano almeno di fronteggiare gli attacchi più comuni.
Così come in passato ha imparato ad adoperare con attenzione e criterio assegni bancari e carte di credito, l'utente deve oggi prendere confidenza con gli strumenti che possono difenderlo dalle aggressioni di tipo informatico.

Molto spesso, in relazione a queste tematiche, alcuni addetti ai lavori operano in modo poco trasparente nei confronti degli utenti finali, nascondendo preziosi consigli dietro a complesse terminologie ed ergendosi su di una specie di piedistallo.
Questo tipo di atteggiamento non aiuta certo a risolvere i problemi. Quindi, se dalla parte di chi ascolta è indispensabile una grande umiltà e attenzione, dall'altra occorre utilizzare un linguaggio chiaro che non ecceda nell'uso di termini e acronimi di scarsa comprensibilità.
A questo punto, soffermiamoci un attimo per delineare in modo sommario quali sono le specifiche che un sistema informatico deve possedere per poter essere considerato sicuro:

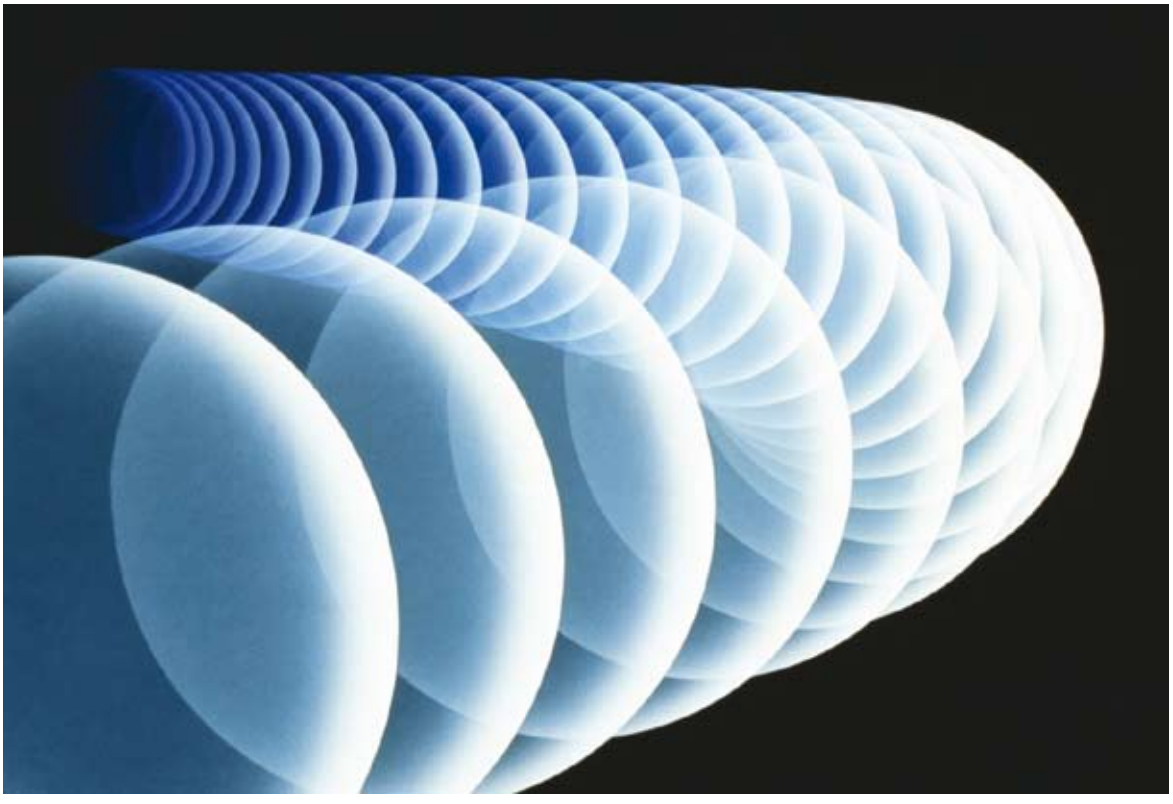
- il primo requisito è quello che viene definito **confidenzialità**, cioè la garanzia che le informazioni siano protette da letture non autorizzate accidentali o dolose;
- il secondo, definito **integrità** e **autenticità**, si raggiunge quando le informazioni sono protette da ogni possibile alterazione provocata da accessi non autorizzati accidentali o dolosi;
- l'ultimo requisito prende il nome di **disponibilità**, ed è assicurato quando le risorse dell'elaboratore risultano sempre disponibili agli utenti legittimi (con l'unica eccezione rappresentata dai momenti di blocco causati da guasti tecnici).

Appare subito evidente la difficoltà di soddisfare integralmente specifiche di questo genere, sia a causa del fattore umano, sia per le caratteristiche di alcuni elementi in gioco, che già per propria natura sono afflitti da alcune fragilità intrinseche: uno degli esempi più calzanti è rappresentato dalla famiglia di protocolli denominata TCP/IP (Transmit Control Protocol/Internet Protocol), universalmente utilizzata nell'ambito delle comunicazioni sulla rete Internet ma soggetta a diverse debolezze architetturali a causa della sua obsolescenza. I problemi nei quali ci si imbatte nel tentativo di soddisfare i requisiti citati sono appunto:

Confidenzialità
Difficile da soddisfare, dato che molte comunicazioni avvengono in chiaro (cioè senza alcuna codificazione che le renda illeggibili agli intrusi). Quindi, tutto quello che transita per la Rete può essere facilmente intercettato, mediante apposite tecniche (sniffing), da chiunque. La situazione è comunque destinata a modificarsi in meglio, in quanto, essendo oggi palesi i rischi derivanti dalla comunicazioni in chiaro, sono sempre di più i servizi che utilizzano modalità di comunicazione cifrata.

Integrità e autenticità
Non si possono ottenere con gli strumenti standard, i quali non sono in grado di garantire che i dati pervenuti non siano stati modificati durante il percorso e, soprattutto, non possono fornire la certezza che l'indirizzo del mittente da noi rilevato corrisponda a quello reale. Un aggressore, attraverso una particolare tecnica (spoofing), può intervenire su un pacchetto di dati in transito, alterando alcune delle sue informazioni originali come, appunto, l'indirizzo di origine.

Disponibilità
Risulta evidente che neppure l'ultimo requisito può essere soddisfatto. Infatti, sono molti gli elementi in gioco che possono mettere completamente fuori servizio un sistema: difetti nel software adoperato, presenza di virus, attacchi di tipo denial of service, eccetera.



ANALISI DEI RISCHI

Molte persone hanno l'abitudine di memorizzare nei loro elaboratori numerose informazioni di una certa importanza, come per esempio dati relativi ai conti bancari, password di carte di credito e bancomat eccetera.

Questo modo di agire, pur non costituendo di per sé un problema, diviene estremamente rischioso quando la macchina destinata a contenere questi dati viene connessa a una rete informatica: da quel momento, infatti, se non sono state prese le opportune precauzioni, le probabilità che un aggressore esterno possa accedere ai nostri dati sono davvero molto alte. Paure di questo tipo, che fino a qualche tempo addietro potevano forse essere considerate esagerate, sono oggi confermate da reali riscontri e, qualora qualcuno avesse ancora dei dubbi in merito, questi possono essere rapidamente dissipati attraverso la semplice lettura dei file di log generati da un comune personal firewall (un software di protezione largamente diffuso); la lettura di questi file evidenzia chiaramente come un elaboratore connesso in rete (per esempio, a Internet) sia continuamente insidiato da svariati tentativi di intrusione finalizzati alla rilevazione di eventuali vulnerabilità utili per la conquista di un accesso illegittimo.

I problemi che un'intrusione può causare sono numerosi: si va dalla violazione della privacy, attraverso l'accesso a foto e documenti personali, ai danni di carattere economico, derivanti dal rilevamento del numero della nostra carta di credito o dei parametri per accedere al nostro servizio di home banking, incautamente memorizzati all'interno dell'elaboratore.
Quelli appena citati sono solo alcuni esempi dei rischi cui un utente può andare incontro ma, nonostante la posta in palio sia alta, molte persone continuano a ritenere la sicurezza informatica un problema esclusivo di coloro che gestiscono dati di una certa importanza, non rendendosi conto che perfino una macchina dedicata al gioco, priva di qualsiasi dato personale, può essere fonte di grossi guai per il suo proprietario qualora non adeguatamente protetta: un intruso che riesca ad assumerne il controllo potrebbe adoperarla per accedere a siti Internet dai contenuti illegali (pedopornografia, terrorismo) o per attaccare altri sistemi informatici (banche, aziende, agenzie governative) o, ancora, per memorizzare temporaneamente materiale illegale (come, per esempio, informazioni derivanti da attività di spionaggio).
Gli esempi che si possono fare sono davvero tanti, ma il risultato è sempre lo stesso: la paternità di queste azioni ricadrà sempre sull'ignaro proprietario della macchina compromessa, che risponderà in prima persona per ogni reato commesso.
Egli, ovviamente, potrà far valere le sue ragioni dichiarandosi estraneo ai fatti ma, considerando che questo non avverrà in tempi brevi e che nel frattempo si dovranno subire tutte le conseguenze del caso (perquisizione, arresto, interrogatori), è certamente auspicabile non trovarsi mai in una di queste situazioni.
La prassi seguita dall'aggressore è quasi sempre la stessa: quando decide di effettuare operazioni illegali su di un certo obiettivo remoto, adopera una o più macchine delle quali ha precedentemente assunto il controllo, macchine che, come abbiamo visto in precedenza, appartengono a utenti del tutto ignari.

Fortunatamente, la conquista di un sistema informatico non è immediata ma avviene per gradi, e i tempi che la caratterizzano sono strettamente connessi sia al tipo di vulnerabilità da sfruttare sia al grado di preparazione dell'attaccante.

INFORMATION TECHNOLOGY E SICUREZZA

Il mondo dell'IT (Information Technology) racchiude in sé tutto l'insieme delle odierne tecnologie adoperate al fine di elaborare, memorizzare e utilizzare informazioni. I dati contenuti nei PC e nelle reti informatiche, però, sono esposti a rischi sempre maggiori da contrastare.

Gli accessi illegittimi alle informazioni residenti sui sistemi di elaborazione, la compromissione o furto dei dati, rappresentano oggi una grave minaccia, sempre più difficile da contrastare. La costante apertura di nuove reti verso Internet, unita alla rapida crescita di connessioni di tipo permanente (come, per esempio, quelle realizzate tramite la tecnologia ADSL) anche tra le utenze private, ha creato un fertile terreno per questo genere di minacce in quanto, a causa della continua immissione in rete di nuovi sistemi, sono cresciuti esponenzialmente i possibili bersagli da attaccare. Alla luce di questo si rende necessario implementare efficaci politiche di sicurezza capaci di contrastare dinamicamente questi pericoli, che minano sia la sicurezza del singolo utente privato sia quella delle grandi reti informatiche. Un'azione del genere non è realizzabile con interventi estemporanei e non ben pianificati poiché, per contrastare efficacemente questi rischi, occorrono competenze specifiche. Sebbene l'elevata dinamicità di questo ambiente, in continua evoluzione secondo tempistiche e modalità assolutamente imprevedibili, non consenta di essere esaustivi, si cercherà di contrastare questa limitazione mediante l'esposizione dei concetti chiave alla base di ogni tecnica.

Il problema della sicurezza informatica

In questo particolare ambiente è sempre valido quel detto paradossale che recita: "solo una macchina spenta può essere considerata una macchina sicura". Solo in apparenza sciocca, questa affermazione racchiude in sé una grande verità, che si traduce in una sorta di monito per chi opera nell'IT, e cioè: un elaboratore acceso, per quanto si siano prese tutte le possibili precauzioni, rimane potenzialmente vulnerabile. L'essenza di questa sconcertante affermazione è basata sull'inequivocabile considerazione che continuamente, nel mondo, si scoprono e vengono rese pubbliche nuove vulnerabilità che riguardano i sistemi informatici.
Questa situazione, grazie ai dettagli offerti dagli scopritori, permette a una miriade di potenziali aggressori di violare in modo più o meno grave i sistemi afflitti dalla vulnerabilità resa pubblica.
In questo scenario ha luogo una frenetica gara tra i legittimi utilizzatori dei sistemi che cercano di rimediare al problema e i malintenzionati che, invece, tentano di sfruttare queste nuove informazioni per i loro fini.

Per quanto talvolta non si possa rendere un sistema totalmente sicuro nei confronti di una certa vulnerabilità, è ovvio che un sistema scarsamente o per nulla protetto è sempre preferito dagli aggressori rispetto a un altro nel quale sono attive alcune protezioni.
A questo punto viene spontaneo chiedersi come mai queste informazioni dettagliate, che permettono di approfittare delle vulnerabilità di un particolare sistema, vengano repentinamente rese pubbliche (generalmente attraverso Internet) non solo da malintenzionati ma, soprattutto, da rispettabilissimi addetti ai lavori. La risposta a questo inquietante quesito può essere sintetizzata in una sola frase: full disclosure, che in italiano si può tradurre con il dovere di dire tutto, rappresenta la corrente di pensiero di coloro che difendono a spada tratta la libertà di diffondere tutti i dettagli relativi alle vulnerabilità venute alla luce. La loro scelta è guidata dalla convinzione che solo in questo modo i legittimi utilizzatori potranno immediatamente correre ai ripari. Questa nobile intenzione viene quindi addotta a giustificazione degli eventuali risvolti negativi che scaturiscono dalla full disclosure, risvolti rappresentati dalla possibilità che gli aggressori possano sfruttare le preziose informazioni sulle vulnerabilità ancora prima dei legittimi utilizzatori. Numerosi siti rendono disponibili nelle loro pagine un elenco aggiornato delle vulnerabilità scoperte e, proprio per questa ragione, è assolutamente indispensabile che ogni singolo utente/amministratore li consulti frequentemente o, ancor meglio, qualora il servizio fosse disponibile, si abboni alle loro newsletter specifiche.

Cerchiamo di sintetizzare il tipico modo di operare di un aggressore informatico. Le sue azioni, dal momento in cui viene scelto un certo obiettivo fino alla conclusione dell'attacco (qualunque esso sia), possono essere suddivise, sommariamente, in tre distinte fasi:

1. **Indagine -** rappresenta il momento preliminare dell'attacco informatico, in cui l'aggressore cerca di raccogliere, nel modo meno invasivo possibile, il maggior numero di informazioni sull'obiettivo designato;
2. **Verifica -** l'aggressore cerca di identificare tutti gli elementi utili per l'auspicata conquista dell'obiettivo come, per esempio, account, risorse condivise, eccetera;
3. **Accesso -** l'aggressore cercherà di violare il sistema designato sfruttando ogni sua possibile vulnerabilità e avvalendosi di tutte le informazioni rilevate nelle fasi precedenti.

IDENTITÀ DIGITALE

Paradossalmente, la nostra immagine digitale è talvolta più importante di quella reale. Esistono esempi eclatanti in tal senso, come quello relativo ad una persona che, risultando deceduta nel database consultato dall'operatore di un ufficio pubblico, si sforzava di far comprendere a quest'ultimo l'eclatante errore senza alcun successo: nonostante si trovasse innanzi a lui, indiscutibilmente viva, l'unico risultato fu quello di sentirsi dire, laconicamente, "mi dispiace, ma lei risulta deceduta".

E se è già così difficile convincere circa l'evidenza della nostra esistenza in vita, figuriamoci in altri contesti, quando in gioco ci sono fattori meno appariscenti ma non per questo di minore importanza, come ad esempio il nostro stato patrimoniale, l'esito di un concorso sostenuto o, semplicemente, il pagamento di una multa: in questi casi la strada da seguire per rettificare un errore (del quale, per altro, solitamente, non siamo responsabili) sarà alquanto impervia.
Messi da parte i risvolti esilaranti, non ci vuole molta immaginazione per intuire in quale direzione le nostre società si stanno muovendo: un percorso per nulla rassicurante verso una graduale perdita d'importanza della nostra identità reale a vantaggio di quella digitale, che, vista la sua crescente valenza, dovrebbe essere gestita in modo adeguato.
Quest'ultimo è il vero nocciolo del problema. Infatti, pur condividendo la necessità di attribuire importanza alla nostra identità digitale, è necessario ottenere opportune rassicurazioni circa la corretta amministrazione di quest'ultima da parte delle figure preposte: purtroppo, vedremo che le cose non stanno proprio in questi termini. Cerchiamo adesso di identificare quali sono le figure strettamente connesse con la gestione di questo nuovo universo digitale.
Possiamo subito anticipare che lo scenario degli ultimi anni ha radicalmente stravolto i canonici ruoli, permettendo che il potere transitasse dalle mani di alcuni verso altri: figure che detenevano un potere quasi assoluto all'interno di alcuni ambienti, come ad esempio i dirigenti delle grandi aziende pubbliche, silenziosamente e senza che se ne rendessero conto hanno ceduto il loro potere ad altri personaggi che prima gravitavano discretamente all'interno delle aree tecniche. Amministratori di sistema, responsabili delle reti ed altre figure connesse alla gestione dei sistemi informatici hanno man mano iniziato la loro ascesa al potere, divenendo elementi cruciali nelle strutture in cui operano.
Questo lento ma inarrestabile passaggio di poteri è stato agevolato dall'incapacità delle vecchie figure dirigenziali di tenere il passo con il repentino stravolgimento causato dal nuovo ordinamento digitale: l'assenza di competenze specifiche e/o il totale disinteresse per la loro acquisizione è stata la causa principale di queste trasformazioni.
Figure professionali i cui poteri erano un tempo circoscritti alle sole aree tecniche si sono trovate improvvisamente capaci di influenzare le sorti delle aziende dove operano, in quanto, almeno potenzialmente, in grado di accedere ad ogni tipo di informazione.
L'aspetto preoccupante di tutto questo è rappresentato dalla constatazione che, nonostante queste figure detengano un enorme potere, solo in tempi recenti la legislatura si è occupata di attribuire loro precise responsabilità oggettive. Molte aziende pubbliche e private, inoltre, durante il transito dal regime tradizionale a quello digitale, si sono affidate a figure non professionali, lasciando la gestione dei loro sistemi nelle mani di gente poco competente.
Questa sorta di Far West informatico, iniziato tanti anni fa con l'attenuante della carenza di figure professionali adeguate all'interno delle strutture, permane ancora oggi all'interno di alcune realtà anche molto importanti (specialmente pubbliche), nonostante la situazione attuale non sia più quella di qualche lustro addietro: certamente nessuno di noi si affiderebbe a un autodidatta appassionato di chirurgia; invece, molto spesso, siamo costretti a metterci senza riserve nelle mani di persone che non possiedono i requisiti minimi per garantire la corretta gestione delle nostre informazioni, con tutti i rischi che ne possono conseguire.

IL FURTO DELL'IDENTITÀ DIGITALE TRAMITE SOCIAL ENGINEERING

Il Social Engineering ("S.E." da qui in avanti) è tipicamente alla base di ogni azione (attacco) che abbia come scopo il furto di identità e credenziali di accesso. Le motivazioni sono da ricercare sia nella storia propria dell'hacking che nella psicologia.

Sicuramente il fenomeno dei Social Network e la continua espansione degli stessi facilita il furto di identità, anche tramite azioni di SE: dal phishing "classico" (bancario) sino a derivazioni sugli stessi temi, dove l'obiettivo – indipendentemente dal Social Network per cui l'aggressore "si spaccia" – è il furto delle credenziali di accesso ai Social Network (Facebook, Linkedin, etc..) e conseguentemente della cosiddetta "identità digitale" di un individuo.
É poi importante distinguere gli stessi Social Network: se Facebook ha un profilo di utenza molto generico, che include dai teenager ai dipendenti di aziende, Linkedin ha invece un profilo di utenza professionale. La differenza è ovvia: un aggressore avrebbe molta facilità nell'attaccare ad esempio utenti di Facebook, in quanto – teoricamente – i know-how presenti tra l'utenza e gli strumenti di difesa dovrebbero essere sensibilmente inferiori rispetto a quelli di un'utenza professionale, quale Linkedin.
Infine, vi è un'ultima distinzione, così come riportato da ENISA (ENISA Position Paper n° 1: Security Issues and Recommendations for Online Social Networks, October 2007) nel suo paper sui Social Network: la tipologia di utenza in funzione della geografia mondiale.
É infatti emerso come alcuni Social Network (praticamente sconosciuti in Italia e/o in Europa), siano invece di enorme diffusione in alcune parti del mondo, e viceversa. A titolo di esempio ricordiamo Orkut ed Ecademy.
Come pericoli "classificabili" per gli utenti dei Social Network, in questi ultimi tempi si è assistito ad un preoccupante aumento dei casi di "stalking", così come di bullismo (Bullying) e, non ultimo, Spionaggio Industriale (Industrial Espionage). A contorno, azioni di Spam, Phishing, Company Reputation.

Un esempio di pericolo per l'identità digitale nei business social network: il whaling
Il furto di identità digitale viene messo in atto per rubare dati con cui falsificare un documento di identità cartaceo per truffe e debiti, oppure viene attuato per creare falsi profili con cui fare acquisti su Internet, diffamare altre persone, generare equivoci e brutte figure tra la vera persona ed i suoi amici. I casi criminali ormai sono tantissimi e molti personaggi pubblici ne sono stati vittima.
Il whaling è l'attacco condotto con l'informatica per far cadere nella rete dei truffatori i grossi profili aziendali, come l'amministratore delegato e i dirigenti. Si tratta, purtroppo, di una vera e propria caccia alla balena molto redditizia per i cybercriminali e un attacco con alte probabilità di successo perché costruito in maniera molto personalizzata per ogni singolo obiettivo professionale di alto profilo: infatti vengono usate le informazioni rese pubbliche dai dipendenti stessi.

Il modus operandi dei criminali informatici è il seguente. Dopo aver cercato le informazioni sulle vittime nei business social network o nei siti Web aziendali, il criminale invia e-mail in cui consiglia di cliccare su allegati o indirizzi in realtà molto pericolosi. La vittima cade facilmente nel tranello perché l'e-mail inviata non ha le sembianze dello spam, sembra proveniente da una società collegata in qualche modo a quella della vittima, viene fatto riferimento a un interesse o un hobby del malcapitato. L'obiettivo è infettare il computer della vittima con programmi in grado di intercettare tutto quello che viene digitato su una tastiera, quindi anche informazioni importanti come username e password, documenti riservati e coordinate bancarie. Il caso finora più clamoroso si è verificato nell'aprile 2008 e ha coinvolto 20.000 dirigenti di aziende statunitensi. L'e-mail conteneva un falso ordine di comparizione in tribunale con i nomi completi ed accanto i nomi ed i contatti telefonici delle rispettive aziende. Le persone cliccavano subito per leggere i dettagli sulla presunta causa legale e venivano rimandati a un falso sito della Corte Americana, dove venivano invitati a scaricare ed installare un software aggiuntivo obbligatorio per visualizzare correttamente tutti i documenti legali. In realtà, si scaricava un software pirata in grado di copiare le credenziali di log-in utilizzate sui siti Web delle banche e rispedirle subito ai criminali per rubare denaro.

CONTROLLO DEL DATORE DI LAVORO SULL'USO DEI SOCIAL NETWORK DURANTE L'ORARIO DI LAVORO

Questa è una diatriba alquanto intrigante. L'utilizzo del Social Network durante l'orario di lavoro è, in alcuni casi, un valore aggiunto: per esempio su Social Network quali Linkedin, un'attenta analisi dei profili e dei contatti, così come di news, discussioni ed aggiornamenti, permette all'azienda di ottenere informazioni "quasi di intelligence", relativamente ad aziende competitor, personale di altre società e così via.

Certamente, lo stesso non si può dire per Social Network più generici quali Facebook ma, ancora una volta, tutto dipende dal contesto aziendale e dalla tipologia di attività principale che si segue a livello professionale. Per fare un esempio davvero banale, se sono un investigatore privato, il tempo speso su un Social Network "giocoso" quale Facebook è in realtà da considerare alla stregua di un investimento aziendale, o dell'open source-based Intelligence, e rientra all'interno di azioni quali Competitive Intelligence e Competitive Scouting (cfr. anche OSSTMM 3.0: www.osstmm.org nella sezione "Competitive Intelligence").

LA POSSIBILITÀ DI FARE USCIRE INFORMAZIONI RISERVATE DAL POSTO DI LAVORO TRAMITE IL CANALE

Questo rischio è verosimile ed estremamente alto. Il problema parte da vulnerabilità di tipo Web, quali XSS (Cross-Site Scripting) che permettono e/o amplificano l'invio di Virus e Worm verso il target (utenti dei siti di Social Network). Negli ultimi mesi abbiamo assistito ad un forte incremento di tali attacchi, specialmente verso Facebook.

Dobbiamo anche pensare a problemi creati dalle informazioni trasmesse attraverso i social media:

- foto o video scattati all'interno dell'azienda o durante riunioni ed eventi possono rivelare informazioni delicate sull'attività aziendale;
- i dipendenti usano applicazioni per condividere i dati sui viaggi di lavoro, rivelando così all'esterno dove sono i clienti, il raggio di azione delle attività aziendali, ecc.;
- documenti aziendali riservati possono, per colpa o per dolo, essere diffusi tramite questi canali.

Il rischio di fuoriuscita di dati sensibili dal contesto aziendale è certamente alto, ma l'utilizzo di strumenti sociali che permettono uno scambio veloce e a basso costo delle informazioni si diffonderà sempre di più, mano a mano che i nativi digitali accederanno a posizioni lavorative. La perdita di informazioni avviene, talvolta anche la perdita di dati sensibili.

La vera sfida non è tanto bloccare l'uso dei media sociali, ma imparare a gestirli in modo creativo, permettendo alle persone di utilizzarli e insegnando loro il modo migliore per farlo. (Estratti dall'intervento di Adrian Davis, Security Day 2009)

CREARE PORTE DI INGRESSO NON CONTROLLATE E PERICOLOSE NELLA RETE AZIENDALE

L'uso di sistemi come le chat diffuse in molti social network potrebbe aprire altre porte di comunicazione senza un controllo adeguato e tramite cui potrebbero entrare software molto pericolosi.

Questo punto non è molto essenziale né veramente problematico: il problema nasce per strumenti quali Skype (software proprietario), mentre per i Social Network, alla fin fine, il tutto si restringe - si fa per dire - a browser e navigazione Internet "standard" per cui valgono le buone regole di protezione.
Ciò significa quindi che vulnerabilità ed attacchi Web-based possono essere vettori di contagio per worm, virus, trojan, key logger, botnet e, conseguentemente, impattare - anche fortemente - l'infrastruttura aziendale.

Al fine di ridurre il livello di potenziale vulnerabilità delle macchine di una rete (ma anche di una singola macchina), è opportuno verificare che siano attivi soltanto i servizi e/o protocolli necessari: la presenza di elementi superflui, infatti, rappresenta una grave minaccia alla sicurezza.
Una buona abitudine è quella di verificare attentamente questo genere di cose sia durante il processo di installazione del sistema operativo, sia in seguito, periodicamente, al fine di assicurarsi che non siano stati attivati (anche involontariamente) servizi e/o protocolli non necessari.

La presenza di elementi del genere non inutilizzati, che di fatto aprono verso l'esterno un certo numero di porte TCP/IP, è fonte di numerosi problemi sia sotto l'aspetto delle prestazioni in quanto la loro presenza consuma risorse di sistema, sia sotto quello della sicurezza dato che l'utente ignora la loro presenza e, quindi, non si farà carico di applicare le patch per la sicurezza rilasciate in seguito dal produttore, creando in questo modo un fertile terreno per gli exploit dei potenziali aggressori.

INTERCETTAZIONE DELLE INFORMAZIONI RISERVATE DURANTE L'USO AZIENDALE

Questo pericolo non è imputabile totalmente ai social network, quanto piuttosto alla mobilità delle persone ed alla penetrazione dell'always-on nella vita quotidiana.

Queste informazioni, infatti, potrebbero essere intercettate a causa di vulnerabilità del PC client (pensiamo alle connessioni in luoghi pubblici quali aeroporti, internet point, hotel, fiere, eventi, conferenze) piuttosto che del PDA. I Social Network, insomma, non sembra abbiano in questo contesto una forte rilevanza ed incidenza. Certamente, però, se su un Gruppo di Discussione pubblico due colleghi della stessa azienda fanno disclosure di informazioni sensibili o critiche, il problema emerge, ma allora è questione di policy, awareness e formazione, non di Social Network.

Bisogna comunque fare una riflessione. Mesi fa, una società di sicurezza statunitense (Netragard) è stata ingaggiata da una grande realtà aziendale, per eseguire un Penetration Test. La particolarità è che l'attacco è stato eseguito utilizzando quasi esclusivamente Facebook come "vettore", dato che il personale dell'azienda richiedente comunica al proprio interno principalmente e proprio tramite Facebook. Dopo alcuni mesi di "setup", l'attacco è stato lanciato, con esiti devastanti.
Il post è disponibile su: seclists.org/fulldisclosure/2009/Feb/149

ALTERAZIONE ILLEGITTIMA AZIENDALE AI FINI DI MARKETING

Questo è un pericolo non solo reale e concreto, ma anche una minaccia già presente ed utilizzata dal mondo criminale. Svariati sono, ad esempio, i casi di siti di antivirus "fasulli", la cui URL è richiamata da e-mail di phishing molto "verticali", dove, invece che l'AV, l'ignaro utente scarica – ed installa – malware di vario tipo, tipicamente trojan.

Anche in questo caso i social network e social media non fanno altro che permettere un'amplificazione – e conseguente contagio "di massa" o, comunque, distribuito e veicolato attraverso utenti ignari, ma che nutrono relazioni di trust l'uno con l'altro – dell'attacco, moltiplicando il numero di potenziali vittime.
Un altro pericolo proviene dall'uso illegittimo delle password. Immaginiamo un malfattore che entra in possesso delle password di profilo e gruppo su un social network creato da un'azienda concorrente. Potrebbe cambiare le informazioni, leggere i contatti e i messaggi, modificare il messaggio di marketing creando molti danni di immagine.

Si può pensare di sfruttare le potenzialità della nuova dimensione "sociale" del Web in modo tale da creare una nuova immagine aziendale che si rivolga ad un target eterogeneo e che sia, quindi, più vicina al consumatore. Il "biglietto da visita" che ci proponiamo di costruire deve essere necessariamente studiato in maniera unica, dinamica, originale, ma soprattutto si deve sviluppare in un contesto veritiero e vicino al suo target. Per garantire la buona riuscita di questa operazione, bisogna dedicare molto tempo alla comunicazione, ai consigli e all'ascolto della propria community. Non si può essere frettolosi perché il suo consolidamento richiede tempo e pazienza. Inoltre, bisogna tenere sotto controllo le informazioni che ne scaturiscono: il nostro Brand va difeso! Questo non è sempre facile, perché nelle maree di Internet si possono incontrare utenti non soddisfatti che ne parlano male.

Si sa che un commento negativo gode di una velocità di propagazione maggiore di qualsiasi flusso di informazioni positive, ma a volte si possono sfruttare le critiche per instaurare un dialogo con i propri clienti. In questa pratica, ci sono delle regole etiche che è opportuno seguire, come quella di "mettere la faccia" in modo umano, ma anche professionale, nel sostenere un brand. A volte è facile se i commenti negativi sono poco pesanti (ad esempio se il commento è "è caro!", si può puntare sulla qualità del servizio offerto), altre sono molto difficili ed impossibili da controbattere, ne è un esempio una nota marca sportiva che è stata accusata di aver sfruttato mano d'opera minorile.
L'importante è cercare di difendersi in modo pulito, senza bannare o attaccare nessuno, in modo democratico e civile. Ma come si fa ad essere sempre informati sui giudizi che ci circondano? A differenza della comunicazione offline, nell'online esistono degli strumenti come Google Alert in cui effettuare le ricerche: basta saper cercare, e noi siamo qui per aiutarvi.

CONTROLLO DELLE INFORMAZIONI INSERITE DAGLI ISCRITTI AL CANALE DI COMUNICAZIONE

Immaginiamo una persona che entra in un gruppo creato su un social network e comincia a parlare male di un marchio, a caricare file con contenuti illegali in una pagina aziendale. Questa persona non sta violando nessun sistema, sta usando semplicemente i classici strumenti, perché chi ha costruito la pagina sul network non ha adeguatamente protetto i diritti di modifica della pagina da parte di persone diverse dall'amministratore.
Data la notevole velocità di propagazione delle informazioni nel network, i danni creati all'immagine aziendale sono gravissimi.

ACCESSO AL CANALE DI COMUNICAZIONE DA DIPENDENTI NON AUTORIZZATI

Se l'azienda delega ad un dipendente l'incarico di gestire il social media con le varie pagine, e-mail eccetera, cosa succede nel caso questa persona si assenti dal lavoro? Come deve comportarsi un dipendente delegato? Per fare un paragone, è simile al problema della lettura della e-mail aziendale da parte di un altro incaricato con le precauzioni necessarie per non violare la privacy dell'incaricato dell'e-mail aziendale.

RISCHI DERIVANTI DALL'ANALISI AGGREGATA DEI DATI A SCARSA VALENZA INDIVIDUALE

Oltre ai rischi direttamente riconducibili a specifiche attività condotte in modo più o meno consapevole dagli utenti di una rete (intesa nell'accezione più ampia del termine), esiste un'altra categoria di rischi che non sono legati a uno specifico evento scatenante, in quanto conseguenza del verificarsi congiunto di due o più avvenimenti.

La particolare natura del problema rende molto difficoltosa l'individuazione delle relative contromisure e, soprattutto, non consente di dispiegare in campo i tradizionali strumenti di difesa: in questi casi è necessaria un'analisi molto più approfondita, operata secondo dei criteri meno canonici e più euristici. In queste circostanze, infatti, più che il pedissequo utilizzo di strumenti software e contromisure standard, risulta decisiva l'esperienza sul campo, le competenze possedute e la lungimiranza di chi amministra le politiche di sicurezza, unici fattori in grado di fornire quella visione euristica alla quale si è fatto prima accenno: partendo da questi prerequisiti, si potrà effettuare un'analisi del proprio scenario operativo e, conseguentemente, giungere alle conclusioni che consentiranno di stabilire le opportune contromisure da adottare per eliminare o quantomeno contrastare efficacemente questa categoria di rischi.

L'aspetto critico in ambito sicurezza che desidero sottolineare non è legato alle singole informazioni di un certo valore che, proprio per questa loro caratteristica, sono generalmente ben protette (o, almeno, lo dovrebbero), ma ai risultati ottenibili mediante una visione congiunta di più informazioni di scarso valore (quindi poco protette e spesso ottenibili senza grandi difficoltà) che, una volta aggregate, acquistano una valenza ben superiore alla somma dei loro singoli valori: si tratta di un aspetto spesso tenuto in poco conto dagli addetti ai lavori che, frequentemente, risultano vulnerabili a questi problemi.
Il nocciolo della questione, al quale fino ad adesso ci siamo riferiti solo implicitamente, è rappresentato da quelle attività che in letteratura informatica ricadono nella categoria delle "tecniche di indagine", una serie di operazioni preliminari a un attacco informatico, generalmente condotte da un aggressore al fine di recuperare alcune informazioni di base sull'obiettivo da violare, informazioni che verranno poi integrate da altri elementi ricavati mediante tecniche più mirate ma, tipicamente, molto più invasive e quindi facilmente rilevabili da chi riceve queste "attenzioni". Proprio per quest'ultima ragione, ogni aggressore cercherà di ricavare più informazioni possibili con le tecniche di primo livello (tecniche di indagine) piuttosto che con le altre; in certi casi limite, potrebbero perfino non essere necessarie ulteriori operazioni, in quanto le informazioni ricavate in questa prima fase potrebbero già consentire di portare a compimento l'attacco senza la necessità di ricorrere a ulteriori strumenti e/o informazioni.
In questa particolare fase di ricerca delle informazioni, dominano certamente le tecniche di "ingegneria sociale" (social engineering), ossia quelle azioni di raggiro e/o persuasione volte all'ottenimento di informazioni riservate, utili per poter violare un sistema informatico e seguite da un gran numero di altri metodi, strumentali, sociali o ibridi, in grado di svolgere efficacemente questo compito.

Mentre un tempo la ricerca delle informazioni utili agli scopi dei malintenzionati era un'impresa alquanto difficoltosa a causa delle poche fonti disponibili (principalmente siti Web aziendali, newsgroup, IRC), realtà come "Facebook" (o altri similari come Youtube, MySpace, Linkedin) rendono oggi disponibili informazioni preziose organizzate in modo organico, che si rivelano una vera e propria manna per coloro che desiderano compiere azioni illecite, anche al di fuori della sfera informatica (si pensi, ad esempio, ai rischi derivanti dai furti di identità). La grande diffusione che in questi ultimi anni ha interessato i social network ha contribuito non poco a ingigantire, in modo preoccupante, tutte le problematiche connesse a questa prima fase non invasiva (e il termine "non invasiva" è qui sinonimo di "non rilevabile") di raccolta delle informazioni, problematiche che ancor prima

dell'avvento delle reti sociali risultavano molto difficili da affrontare in modo risolutivo.

Malfunzionamenti (bug) nei software di gestione di alcuni social network, utilizzo di specifici strumenti (exploit) reperibili in rete e, infine, scarsa attenzione nella protezione dei propri dati (spesso amplificata dalle troppo permissive regole predefinite adottate dai gestori dei siti), sono alcune delle cause che consentono un pericoloso accesso ai dati gestiti nelle reti sociali, le quali, ricordiamo, a seconda del tipo di network, possono contenere anche molti dettagli relativi all'ambito lavorativo (società, mansione, privilegi, ecc.). Oltre al noto Facebook, tipicamente indirizzato alle utenze private, ne esistono altri come Ecademy o Linkedin, pensati per una fascia professionale di utenza. Il facile accesso a certe informazioni, incautamente memorizzate sulle pagine di questi siti e sapientemente aggregate dagli aggressori, può fornire a questi ultimi un solido ariete capace di demolire anche le protezioni di rete più sofisticate.
Meccanismi di autenticazione poco robusti, uniti alla propensione nell'utilizzare credenziali alquanto semplici (password corte o facilmente individuabili), consentono soventemente di accedere a questi dati senza ricorrere a nessuna tecnica e/o strumento particolare; il modo con il quale sono strutturati i siti di social network, inoltre, genera negli utilizzatori un apparente senso di sicurezza legato alla (falsa) convinzione che quanto immesso sarà poi visibile esclusivamente a una ristretta cerchia di persone. Cosa che, per svariati motivi, non sempre si verifica.

Il formalismo matematico che descrive un "social network" è quello dei "grafi", una serie di nodi connessi tra loro secondo alcune regole, una particolare struttura che consente di aggregare in modo efficiente informazioni apparentemente non relazionate tra loro: questa caratteristica, che rende spesso le reti sociali oggetto di studio in ambito sociologico, offre agli aggressori un portentoso strumento di indagine a 360 gradi (la possibilità di legare ogni individuo a un altro mediante le amicizie dichiarate rappresenta soltanto una delle enormi potenzialità offerte dalle strutture di questo genere, una vera e propria voragine nell'ambito della privacy).
La completezza delle informazioni accessibili (nome e cognome, data di nascita, foto, preferenze politiche, particolari privati e professionali, ecc.) sono elementi determinanti che consentono di dar corpo a un'ampia rosa di attività criminali, tra le quali quelle a carattere informatico rappresentano solo una sparuta minoranza.
La volontà degli utenti che in un certo momento decidono di rimuovere definitivamente i dati precedentemente memorizzati viene poi vanificata dalle caratteristiche peculiari possedute dalla rete Internet che, sia a causa della scarsa cura messa nel compiere l'operazione da parte dei gestori dei siti, sia per l'intervento di meccanismi di cache o di copie effettuate da altri utenti, rende di fatto quasi impossibile l'eliminazione completa dei dati i quali, quindi, potrebbero essere visibili (magari in altre forme) per tantissimi anni.

Quanto appena detto in questa sorta di sintetica disamina sugli effetti collaterali delle reti sociali e, più in generale, sui pericoli derivanti dall'analisi aggregata di informazioni a scarsa valenza individuale, evidenzia l'enorme difficoltà che si pone innanzi a coloro che, a qualunque titolo, devono assumersi l'onere di garantire l'implementazione di corrette politiche di sicurezza.
Questo, astraendoci dagli specifici fattori (come, per esempio, il social network), è riconducibile all'estrema ed esponenziale dinamicità dello scenario operativo: certezze considerate ormai acquisite possono repentinamente perdere consistenza, costringendo gli operatori a rivedere ogni aspetto alla luce di nuovi e poco conosciuti parametri, come è avvenuto in questi anni con il diffondersi delle tecnologie wireless (che hanno riportato in auge problematiche che si sperava fossero ormai relegate al passato).

Per queste ragioni, la sola buona volontà di chi opera nel settore non rappresenta più, come un tempo, un elemento determinante, in quanto deve necessariamente essere coadiuvata da un puntuale e costante aggiornamento delle competenze, il tutto in un'ottica euristica dei possibili scenari di rischio.

RISCHI DERIVANTI DALL'INSTALLAZIONE DELLE APPLICAZIONI DI TERZE PARTI

Una delle recenti evoluzioni dei social network riguarda la possibilità data a tutti gli iscritti di sviluppare le applicazioni, ovvero un software di vario genere che l'iscritto può inserire nel suo profilo e inviare agli amici del suo network. Tramite l'applicazione, l'iscritto al network può esprimersi e farsi conoscere, può divertirsi con il giocare, comprare musica, scambiare materiali multimediali con gli amici, risolvere quiz e test, interagire con una marca. Può anche usare software per automazione di ufficio, elaborare immagini, eccetera.

Il successo di Facebook è dovuto anche alla disponibilità e facilità di programmazione delle applicazioni tramite le chiamate API (it.wikipedia.org/wiki/API); gli altri social network hanno poi man mano rilasciato i permessi per lo sviluppo. Si parla di diffusione virale quando una persona usa l'applicazione e automaticamente tutti i suoi amici vengono a sapere di tale uso e ne vengono invogliati per superare i risultati ottenuti dalla persona o per provare l'efficacia dell'applicazione. Questa, infatti, è in grado di accedere ai database del social network per estrarre i riferimenti degli amici di chi la sta usando al fine di mandare loro un messaggio personalizzato in grado di suscitare interesse. Le applicazioni Facebook hanno generato un forte successo in monetizzazione dello sviluppo e creazione di campagne marketing: per citare alcuni esempi un'applicazione dedicata a un gioco legato a una marca in 3 settimane ha raggiunto milioni di utenti nella sola Italia.

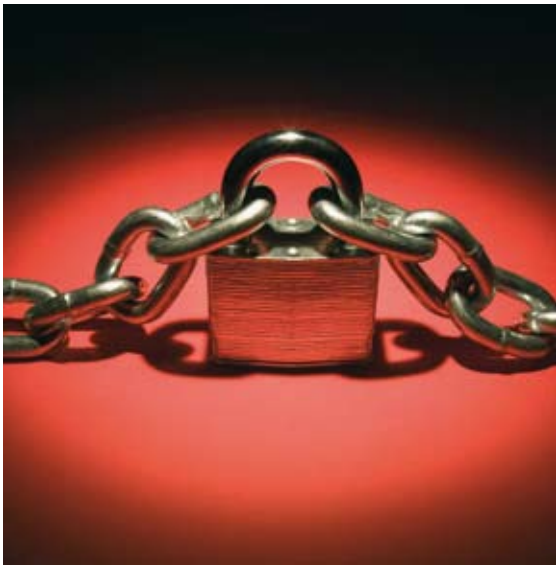
Chi intende utilizzare le applicazioni deve rendersi conto dei rischi legati all'accesso al database dei profili del social network e alla non perfetta costruzione degli schemi di sicurezza da parte degli autori: del linguaggio di programmazione, dell'applicazione e del network. Occorre sempre capire come modificare le impostazioni per la privacy relativa all'applicazione, per esempio in Facebook si può andare in alto a destra e cliccare sul menu "Impostazioni" e poi su "Impostazioni applicazioni" per capire come le applicazioni accedono ai dati del profilo personale. Occorre, soprattutto, non installare con leggerezza e superficialità un'applicazione, si deve andare subito a leggere la presentazione delle funzioni, cercare di capire chi è l'autore, cercare sul motore di ricerca eventuali informazioni e critiche.

RISCHI DERIVANTI DALL'ESPOSIZIONE DEI NOMINATIVI DEI CLIENTI

Sui social network si può creare una pagina fan, un gruppo di persone o altri strumenti per invogliare le persone a seguire lo sviluppo di un'attività commerciale, agevolare la comunicazione tra aziende e clienti, far conoscere i nuovi prodotti, eccetera. Si tratta di nuovi strumenti ampiamente discussi e i cui vantaggi sono stati analizzati in vari libri su come fare business con i social network.

Le persone possono pertanto iscriversi e il loro nominativo e la loro fotografia compariranno nell'elenco degli iscritti. Se non vengono applicate specifiche impostazioni di privacy, questo elenco è visibile da tutti, anche dalle persone non iscritte. Molte aziende non vogliono usare questi strumenti, perché hanno paura di mostrare questo elenco di persone ai concorrenti, che potrebbero ricontattarle e convincerle a passare alla loro azienda.

Si tratta in realtà di una possibilità molto difficile: alcune pagine fan hanno decine di migliaia di iscritti e contattarli uno a uno implica un grosso lavoro, inoltre i social network impediscono la spedizione di decine di e-mail al giorno.



ATTACCHI DI PHISHING

Il phishing è una truffa mirata al furto di identità e di dati sensibili come password o numero carta credito. La truffa si esegue tramite e-mail false, ma anche contatti telefonici, che riproducono l'apparenza grafica dei siti di banche, poste eccetera.
L'utente riceve un invito a scrivere le proprie credenziali per difendersi da virus o eseguire aggiornamenti, ma in realtà viene indirizzato verso un sito in grado di rubare le informazioni riservate e usarle subito per attività illecite.

Si tratta purtroppo di un fenomeno in continua crescita: secondo il rapporto Symantec, il 17% delle e-mail ricevute sono tentativi di phishing, e l'Italia è al terzo posto nelle preferenze dei truffatori. All'inizio queste e-mail contenevano grossi errori di italiano che li rendevano facilmente individuabili, adesso sono sempre più corrette e sofisticate. Vale la regola d'oro del non cliccare sui link nell'e-mail, ma di andare direttamente all'indirizzo del sito che si conosce.
Per informazioni: it.wikipedia.org/wiki/Phishing
e portale Anti-Phishing Italia su www.anti-phishing.it

Anche Facebook è sempre più colpito da questo fenomeno, in tre modi.
Nel primo modo si riceve una e-mail fasulla con l'apparenza grafica delle classiche e-mail che riceviamo da Facebook. L'e-mail contiene una foto di uomo o donna e un nominativo richiedente l'amicizia. Se clicchiamo sul link, veniamo rediretti verso un sito simile a Facebook ma in realtà modificato per rubare login e password da rivendere al mercato nero.
Un'altra e-mail del genere avvisa di un cambiamento di password e invita a aprire un file per ottenere quella nuova.
Il terzo modo riguarda il trovarsi sulla bacheca un messaggio del tipo "lol i cant believe these pics got posted…its going to be BADDDD when her boyfriend sees these" con un link dalla struttura simile a quello reale (www.facebook.com/profile.php) per ingannare le persone. Se clicchiamo su un link di questo tipo veniamo rediretti verso un sito con l'apparenza simile a Facebook ma in realtà modificato per rubare login e password.
Conviene cambiare la password e cancellare subito il messaggio per evitare che altri nostri amici lo leggano e si diffonda creando danni.

Regola generale valida per qualsiasi tipo di account online: cambiare periodicamente la password e non usare termini facilmente ricavabili dalle proprie informazioni personali pubblicate in rete!

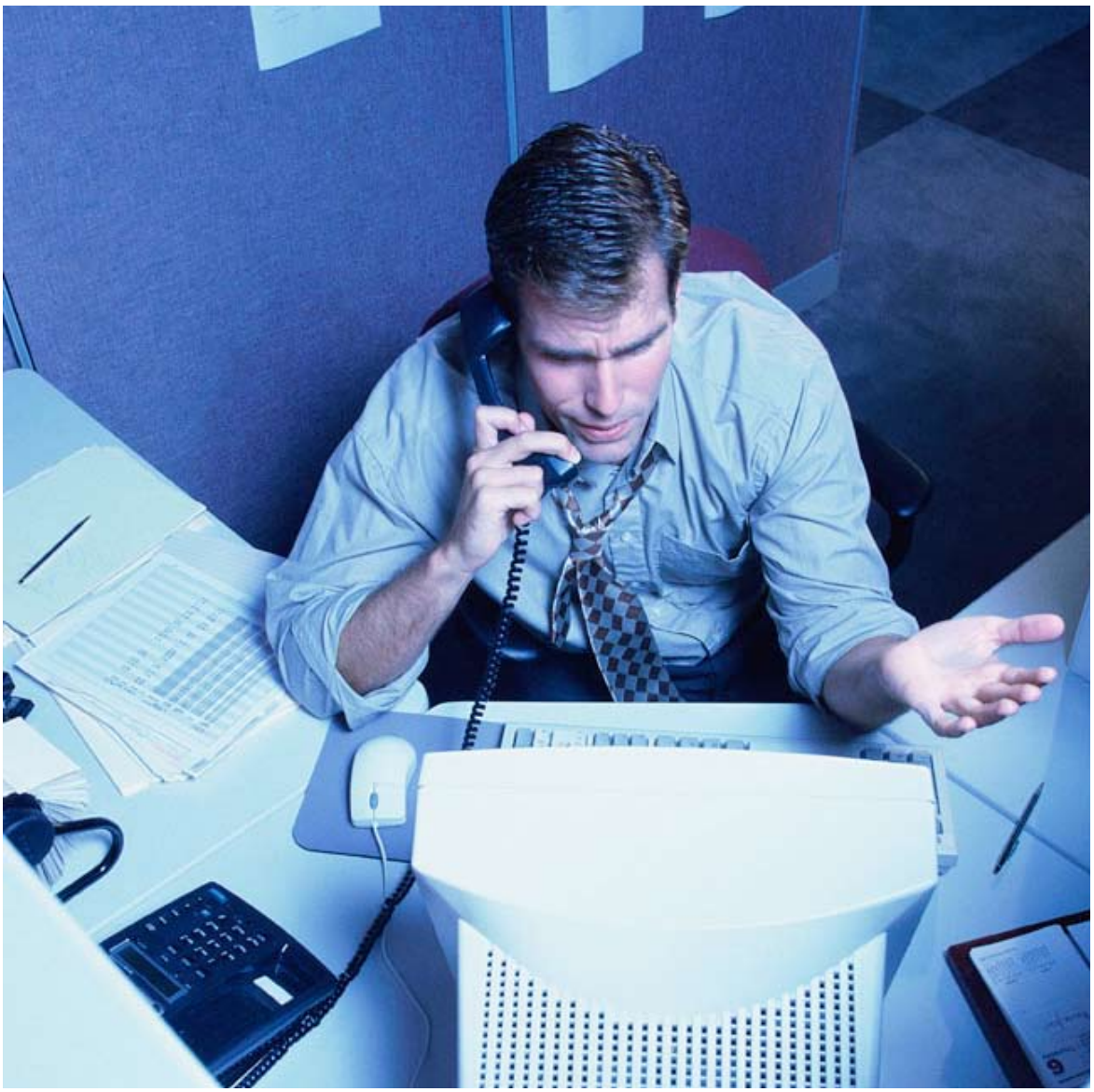
Altre informazioni su: facebookitalia.blogspot.com/2008/01/il-phishing-getta-le-reti-su-facebook.html

IL RUOLO DELL'AMMINISTRATORE

Il ruolo di amministratore della sicurezza deve comprendere l'educare e rendere consapevoli dei rischi derivanti dall'ambito lavorativo. Ma quali sono le nuove responsabilità e il nuovo ruolo del responsabile della sicurezza ICT?

Il responsabile deve, in primo luogo, ridurre il rischio che in azienda il social network venga utilizzato in modo indebito.
Deve innanzitutto creare chiare regole di disciplina da aggiornare periodicamente, indicando chiaramente quali sono i comportamenti: tollerati, da evitare, in grado di generare una verifica. Il documento deve poi essere fatto ampiamente circolare tra i dipendenti.
In merito alle modalità di verifica, bisogna sempre tener presente che i controlli a distanza sono vietati. Occorre sempre un accordo con i sindacati e comunque bisogna evitare la raccolta di informazioni troppo intrusive nella privacy dei dipendenti. Tipicamente, viene individuata una categoria di siti adeguati per svolgere l'attività aziendale e una categoria di siti proibiti perché non adeguati ad essa.

Occorre inoltre preparare un sistema di deleghe in caso di assenza dell'addetto alla gestione del social network per fini aziendali.



CONSIGLI PER L'USO DEI SOCIAL NETWORK

Come ben noto, l'uso di antivirus, anti-spyware e altri strumenti classici di protezione è un requisito essenziale per la difesa dai pericoli. Ecco alcuni spunti specifici per l'uso sicuro dei social network in ambito aziendale:

1. la sicurezza è fatta da uomini, procedure, strumenti;
2. usare password diverse per ogni social network, la cui composizione non deve essere ricavabile leggendo i profili personali, quindi niente nomi del proprio cane, date di nascita eccetera;
3. chi deve gestire il profilo aziendale sul social network deve tenere distinti i contatti personali dai contatti creati per il lavoro;
4. essere discreti e scegliere con cura quali informazioni condividere;
5. mantenere un certo grado di scetticismo nel giudicare le informazioni trovate sul social network;
6. non accettare inviti a creare contatti da sconosciuti, non sentirsi obbligati a rispondere.

Il profilo personale

I social network, se usati in modo adeguato,difficilmente creano problemi legati alla sicurezza.
Tutte le informazioni che vengono pubblicate nel profilo, infatti, sono intenzionalmente rese pubbliche ed a questi dati possono accedere direttamente solo le persone a cui volontariamente abbiamo consentito l'accesso.

Dopo aver creato un profilo su un SN è bene cercare di limitare il più possibile l'accesso di terzi ai nostri dati modificando le opzioni predefinite; è opportuno quindi riflettere su cosa pubblicare nella nostra pagina. Bisogna stabilire due politiche: la prima riguarda gli utenti a cui consentiamo l'accesso, la seconda il tipo di informazioni che inseriamo nel profilo.
Suggerimenti:

- **per gli utenti consentiti**: limitare il numero di contatti a quelli strettamente necessari evitando di aggiungere persone al solo scopo di incrementare il numero di contatti;
- **informazioni profilo**: inserire informazioni coerenti allo spirito del social network e non eccedere con quelle personali. Evitare di rendere noti dati sensibili come orientamento religioso, opinioni politiche, abitudini sessuali.

In entrambi i casi, è consigliabile tener conto dello scopo per cui abbiamo aperto il profilo su quel social network. Ad esempio, se abbiamo creato un account su Linkedin è meglio inserire informazioni riguardanti le proprie competenze e le esperienze lavorative, tralasciando quelle futili tipo cosa si sta facendo in quel momento o cosa si è mangiato a pranzo. Anche i nuovi contatti saranno resi accessibili con queste finalità. Importante sarà il tipo di rapporto che abbiamo instaurato con le persone e il tipo di informazioni che vogliamo render loro note.
É da considerare, infine, che il nostro profilo caricato nel SN rimarrà memorizzato ed usato a fini di marketing; difficilmente potremo eliminarlo o cancellarlo, con tutte le conseguenze che questo comporta.

LE TECNOLOGIE PER CONTROLLARE IL TRAFFICO

Le applicazioni Web 2.0 sono spesso caratterizzate da una forte interazione tra gli utenti che, come accade per i siti di Social Network, porta un conseguente incremento dello scambio di dati tra gli utenti stessi. Questo fenomeno, sebbene non sia di per sé negativo, richiede una maggiore attenzione ai problemi di sicurezza logica che siamo già abituati ad affrontare nel Web "tradizionale".

Restando in un contesto tecnico e ponendoci nell'ottica dell'azienda che vuole consentire l'accesso ai SN per i propri dipendenti e collaboratori senza compromettere la sicurezza dei suoi dati, ci si può focalizzare su due categorie di problemi:

1. **Malware Intrusion** - cioè i contenuti che possono essere scaricati dagli utenti attraverso il canale del SN: hyperlink, file o applicazioni che contengono o puntano a contenuti malevoli che, una volta raggiunto un host interno all'azienda, possono arrivare a compromettere la sicurezza dell'intera rete. Prendendo spunto da quanto pubblicato nel report dell'ENISA (www.enisa.europa.eu/act/res/other-areas/social-networks/security-issues-and-recommendations-for-online-social-networks), risulta che diversi SN hanno un controllo dei contenuti non adeguato, e il rischio di "insicurezza" è amplificato dal continuo aumento di informazioni scambiate, rendendo il controllo dei contenuti un fattore sempre più critico e fondamentale per la sicurezza degli utenti e il successo del SN.
2. **Data Extrusion** - riguarda i dati di proprietà dell'azienda che devono essere trattati solo in un contesto controllato secondo le policy definite, ma che possono essere resi pubblici attraverso la pubblicazione nel SN, causando potenziali problemi alla reputazione e alla proprietà intellettuale dell'azienda (si pensi alla condivisione di informazioni tecniche e non solo, come si vede spesso nei blog).

Per affrontare entrambi i problemi occorre adottare tecnologie in grado di analizzare in dettaglio i contenuti dei flussi di traffico.
In particolare le minacce del tipo Malware Intrusion si affrontano partendo dal perimetro della rete aziendale, in modo da eliminare all'ingresso eventuali malware veicolati attraverso la connessione al SN (tipicamente sistemi di Network Intrusion Prevention, Network Antivirus, Content Filtering etc.), fino a tecnologie di protezione degli host (es. Host Antivirus, Host Intrusion Prevention).
La minaccia del tipo Data Extrusion o Data Leakage deve invece essere affrontata cercando di applicare i controlli di sicurezza il più vicino possibile ai dati, tipicamente sugli host o, dove questo non fosse possibile, analizzando i flussi di traffico in uscita per intercettare e bloccare le informazioni confidenziali che vengono pubblicate sul SN o su altre applicazioni Web.

Il rischio purtroppo è che gli aspetti di sicurezza evidenziati portino l'azienda a mantenere un modello di collaborazione chiuso all'interno del suo perimetro. La consapevolezza di queste problematiche dovrebbe invece guidare nella scelta degli strumenti necessari a prevenire perdite di informazioni e nella definizione di policy aziendali che aiutino il dipendente all'uso corretto e sicuro dei SN in modo da poter beneficiare pienamente dei vantaggi che possono apportare.

CRITERI OTTIMALI PER LA SCELTA DELLE PASSWORD

Il fulcro sul quale ruotano la maggior parte dei problemi legati alla sicurezza dei sistemi di tipo informatico e dei servizi a essi relazionati (come ad esempio gli spazi personali afferenti alle reti sociali) è sicuramente legato al buon uso delle password; nonostante le continue conquiste tecnologiche, infatti, esse rappresentano ancora il punto nevralgico dei sistemi di sicurezza.

Un aspetto che in qualche modo può essere considerato rassicurante è legato alla constatazione che la maggior parte dei problemi legati alle password non scaturiscono da una debolezza intrinseca di questo tipo di meccanismo, bensì da una sua gestione impropria: vedremo che l'adozione di alcuni piccoli accorgimenti è sufficiente a rendere questo sistema quasi inespugnabile.
Purtroppo, come spesso avviene nell'ambito della sicurezza, molti utenti affrontano questo problema con leggerezza, scegliendo ed utilizzando le password in modo inadeguato e rendendo i loro sistemi estremamente insicuri.

Esistono delle regole di base che consentono la creazione di una buona password e che, oltre a garantire un giusto livello di complessità, non espongono (come tante volte avviene) l'utente al rischio di dimenticare la password proprio a causa della sua complessità.
Lo stratagemma consiste nell'utilizzare, come lettere costituenti la password, le iniziali di una frase che conosciamo bene: ad esempio, la famosa frase "essere o non essere, questo è il problema" produrrà la parola "eoneqèip".

Il metodo adoperato può essere ulteriormente migliorato sostituendo alcune lettere della password con dei numeri o dei caratteri speciali, come ad esempio la "i" con il numero 1, la "o" con il numero 0 o la "a" con il carattere speciale @. Applicando quanto appena detto al precedente esempio, otterremo la parola "e0neqè1p".

Purtroppo, almeno in linea teorica, nessuna password al mondo può essere ritenuta sicura al 100%: anche escludendo i rischi di smarrimento o furto, la sua decodifica da parte di un malintenzionato è solo una questione di tempo. Una corretta politica di scelta e di gestione può allungare molto questo periodo di tempo, rendendo l'operazione di decodifica inaccessibile alla maggior parte degli aggressori comuni: a seconda della complessità, il tempo necessario per l'individuazione potrebbe corrispondere a svariati anni-uomo (anche centinaia). Sarebbe possibile infatti solo attraverso l'utilizzo parallelo di un massiccio numero di elaboratori che, operando in sinergia, potrebbero frazionare il tempo necessario fino a renderlo accettabile. Se ne deduce che la soluzione non è alla portata di tutti, ma solo di grosse e potenti strutture, del livello di INTERPOL (International Criminal Police Organization), CIA (Central Intelligence Agency) o FBI (Federal Bureau of Investigation).

In merito a quanto appena detto, occorre aprire una breve parentesi per accennare al fatto che, negli ultimi anni, si è sentito spesso parlare dell'utilizzo congiunto (consenziente o meno) di tante macchine connesse a Internet allo scopo di raggiungere un certo obiettivo: questo scenario lascia intravvedere la possibilità di ridurre i tempi necessari all'individuazione di una password.

Riassumiamo quanto finora detto con alcuni consigli utili per la creazione e la gestione di una password; pur rappresentando solo delle linee guida di base, possono garantire una complessità adeguata e, di conseguenza, una buona robustezza:

- utilizzare almeno sette caratteri per la password, al fine di renderne difficile l'individuazione attraverso le tecniche di tipo Brute Force basate su tentativi reiterati nel tempo;
- non adoperare mai parole di senso compiuto o di carattere personale come nomi di persona, date di nascita, codici fiscali;
- usare in modo congiunto lettere maiuscole e minuscole, numeri e caratteri speciali come $ e @;
- non riutilizzare mai la stessa password in più contesti (macchine e/o servizi diversi) al fine di evitare un effetto a catena qualora questa venga individuata.

AUTORI

Cristina Berta

Crede fortemente nel pieno dispiegarsi della dimensione "sociale" del Web e si propone come creatrice di campagne mirate, in grado di creare rumore e curiosità intorno ad un Brand, come si evince dal suo sito: www.cibbuzz.com

Raoul Chiesa

OPSA, OPST, ISECOM Trainer
Founder, Presidente Onorario, @ Mediaservice.net Srl a Socio Unico (www.mediaservice.net)
Socio Fondatore, Comitato Direttivo e Comitato Tecnico-Scientifico, CLUSIT (www.clusit.it)
Senior Advisor, Strategic Alliances & Cybercrime Issues, Nazioni Unite @ UNICRI (www.unicri.it)
Director of Communications, Board of Directors Member, ISECOM (www.isecom.org)
Director of Communications, Board of Directors Member, OWASP Italian Chapter (www.owasp.org) at Large Member/ALS, ICANN (www.icann.org)
Osservatorio Privacy & Sicurezza - OPSI - AIP, Comitato Esecutivo (www.aipnet.it)

Angelo Iacubino

Project Manager - Dipartimento Informatica, Università degli Studi dell'Insubria (dscpi.uninsubria.it)
Consulente Informatico per aziende pubbliche e private
Direttore Alta Formazione e contenuti Web per Associazione Informatici Professionisti (www.aipnet.it)
Attività di docenza in master universitari e seminari didattici su tematiche riguardanti Sistemi Operativi, Reti Sociali, Computer Music, Programmazione, Linux&OpenSource
Interventi come relatore a diversi eventi nazionali in ambito ICT, Educational e Pubblica Amministrazione (www.disinformatica.com)
Ultime pubblicazioni: Facebook per la valorizzazione e promozione del museo (Atti Congresso AICA 2009, ISBN 978-88-9016-208-4); Creare Applicazioni per Facebook (Ed. FAG, ISBN 978-88-8233-814-5); Informatica e Musica, la Scienza si fa Arte (Ed. Insubria University Press, ISBN 978-88-95362-08-3); Un'introduzione efficace delle tecnologie Open Source nella Pubblica Amministrazione (Atti Congresso AICA 2007, ISBN 88-9016-203-1).

Roberto Marmo

Consulente informatico e professore a contratto di informatica presso la Facoltà di Ingegneria della Università di Pavia e Facoltà Scienze MM.FF.NN. della Università Insubria di Como, oltre che in vari Master.
Autore dei libri "Introduzione alla visualizzazione scientifica" (Editore Il Rostro); "Creare applicazioni per Facebook" (Ed. FAG, ISBN 978-88-8233-814-5). www.robertomarmo.net

Mario Mazzolini

Laureato in Ingegneria delle Telecomunicazioni presso il Politecnico di Milano con tesi dal titolo "Protocolli per la sicurezza del VoIP: stato dell'arte e scenari futuri". Ha svolto attività di consulenza nell'ambito della sicurezza informatica per aziende del settore ICT e assicurativo.

Simone Riccetti

Laureato in Ingegneria delle Telecomunicazioni al Politecnico di Milano. Da diversi anni si occupa di sistemi di sicurezza logica, architetture di rete e applicazioni IT.
É entrato a far parte di IBM nel 2007 come Senior IT Security Architect, con il principale compito di disegnare soluzioni di sicurezza che soddisfino i requisiti tecnici e di business dei clienti. Oltre all'attività in IBM, collabora con la Facoltà di Scienze MM.FF.NN. dell'Università dell'Insubria di Como, dove è professore a contratto di Reti e Applicazioni II presso il Corso di Laurea triennale in Scienze e Tecnologie dell'Informazione.

Roberto Saia

Autore di vasto materiale su temi informatici, svolge attività di docenza e consulenza collaborando con diverse aziende ed enti del settore IT; professionalmente impegnato da tempo nel campo dell'amministrazione delle reti informatiche, si occupa oggi prevalentemente dei problemi inerenti alla loro sicurezza.
Autore dei libri "Reti e sicurezza" (Ed. FAG, ISBN 978-88-8233-691-2) e "Sicurezza wireless e mobile" (Ed. FAG, ISBN 978-88-8233-774-2). www.robertosaia.it

BIBLIOGRAFIA

A proposito di hackers profiling:
Raoul Chiesa, Hacking Profile, Apogeo

A proposito degli aspetti giuridici:
Elvira Berlingieri, Legge 2.0 il Web tra legislazione e giurisprudenza, Apogeo

A proposito di social engineering:
Kevin Mitnick, L'arte dell'inganno, Feltrinelli

A proposito delle tecniche di programmazione delle reti sociali per capire le debolezze dei sistemi:
R. Marmo, A. Iacubino, Creare applicazioni per Facebook, FAG

A proposito della sicurezza delle reti cablate e wireless:
Roberto Saia, Reti e Sicurezza, FAG
Roberto Saia, Sicurezza wireless e mobile, FAG

ARTICOLI SU RIVISTE IN LINGUA INGLESE

Jan Nagy, Peter Pecho, "Social Networks Security", 2009 Third International Conference on Emerging Security Information, Systems and Technologies, pp. 321-325.

Constantinos Patsakis, Alexandros Asthenidis, Abraham Chatzidimitriou, "Social networks as an attack platform: Facebook case study", 2009 Eighth International Conference on Networks, pp. 245-247.

Craig Asher, Jean-Philippe Aumasson, Raphael C.W. Phan, "Security and Privacy Preservation in Human-Involved Networks", iNetSec 2009, IFIP International Federation for Information Processing AICT 309, pp. 139–148, 2009.

Martin Pekárek, Stefanie Pötzsch, "A comparison of privacy issues in collaborative workspaces and social networks", Identity in the Information Society, special issue on Social Web and Identity.
Enkh-Amgalan Baatarjav, Ram Dantu, and Santi Phithakkitnukoon, "Privacy Management for Facebook".

ICISS 2008, LNCS 5352, Springer-Verlag, pp. 273-286, 2008.

Philip W.L. Fong, Mohd Anwar, and Zhen Zhao, "A Privacy Preservation Model for Facebook-Style Social Network Systems", ESORICS 2009, LNCS 5789, Springer-Verlag, pp. 303-320, 2009.

SITOGRAFIA

The Security Risks of Social Networks

Seven Deadly Sins of Social Networking Security

Hacking di applicazioni Web 2.0 con Firefox, di Redazione HTML.it

Guida sicurezza applicazioni Web, di Redazione HTML.it

European Network and Information Security Agency Recommendations for Online Social Networks

Social Network Security Workshop - Stanford University, Sept. 11th 2009

Facebook Security

Pagina del Garante della privacy sugli effetti collaterali dei social network

File formato Adobe PDF con la guida preparata dal Garante della privacy sugli effetti collaterali dei social network

GLOSSARIO

Access Point
Dispositivo che consente la connessione alla rete di più macchine in modalità wireless.

Account
Insieme dei dati personali e dei contenuti caricati su un social network. Viene indicato anche solamente con il nome dell'utente utilizzato per identificare la persona ed accedere al servizio online.

ACL
Insieme delle regole impostate, ad esempio, su un Firewall o un Router.

ADSL
Acronimo di Asymmetric Digital Subscriber Line, tecnologia che permette l'inoltro di informazioni digitali ad alta velocità attraverso la rete telefonica standard (analogica).

Adware
La parola è il risultato dell'unione dei termini anglosassoni "advertising" (pubblicità) e "software".

AES
Acronimo di Advanced Encryption Standard, un'implementazione del cosiddetto algoritmo Rijndael.

Alias
Falsa identità assunta su Internet, quindi anche sui siti di social network. L'utente può scegliere un nome di fantasia, uno pseudonimo, o appropriarsi dei dati di una persona realmente esistente per compiere atti illeciti.

ARP
Acronimo di Address Resolution Protocol, protocollo di risoluzione degli indirizzi operante nel livello Internet; esso risolve la corrispondenza tra indirizzi IP e indirizzi fisici MAC all'interno delle reti locali.

Autenticarsi
Accedere ad un sito scrivendo nome utente (chiamato anche "login" o "user name") e password (parola chiave riservata, da non perdere).

Backdoor
Indica un punto illecito e nascosto di accesso ad un sistema.

Bluetooth
Standard basato su onde radio operanti alla frequenza di 2,45-2,56 Ghz (banda ISM).

Bridge
Dispositivo in grado di unire reti di diverso tipo.

Broadcast
Metodo adoperato per trasmettere attraverso le reti, basato sull'invio contemporaneo dei dati a tutti le macchine della rete.

Browser
Software del tipo Firefox o Internet Explorer per navigare attraverso le pagine nel Web.

Bug
Indica gli errori commessi durante la programmazione di un certo software.

Business Social Network
Un social network creato appositamente per costruire relazioni professionali e di affari tra le persone che formano il network.

Cache
Memoria particolarmente veloce (solitamente di piccole dimensioni) adoperata per accedere rapidamente ad informazioni di frequente utilizzo.

CCMP
Acronimo di Counter Mode/CBC Mac Protocol (protocollo per il codice di autenticazione dei messaggi con concatenazione dei blocchi crittografati).

Checksum
Abbreviazione di SUMmation CHECK, identifica un particolare meccanismo di controllo dei bit inoltrati in una comunicazione, allo scopo di individuare eventuali errori.

CIA
Acronimo di Central Intelligence Agency.

Cifrario di Cesare
Uno dei più antichi algoritmi crittografici basato sul metodo denominato a sostituzione monoalfabetica.

Client
Adoperato in informatica per indicare una macchina che accede ai servizi offerti da un'altra macchina definita Server.

Condividere
Permettere ad altri utenti di accedere al materiale multimediale (testi, audio, video, foto) che è stato caricato online su un account o su un altro spazio di condivisione.

Condizioni d'uso
Regole contrattuali che vengono accettate dall'utente per accedere ad un servizio. Conviene leggerle con attenzione prima; non sono definitive perché possono essere modificate in corso d'opera dall'azienda erogante il servizio.

Connectionless
Tecnica di trasmissione dati del tipo non orientata alla connessione e senza alcun riscontro, cioè che non effettua alcun tipo di controllo sulle informazioni trasferite.

CRC
Acronimo di Cyclical Redundancy Check, algoritmo di controllo dell'integrità.

Crittografia
Termine di origine greca, il cui significato etimologico è "scritture nascoste".

Datagramma
Identifica un pacchetto di dati con opportuna intestazione contenente le informazioni occorrenti per la consegna dello stesso; sinonimo è anche il termine "pacchetto".

Debug
Processo di ricerca degli errori.

Defacement
Il termine anglosassone "defacement" (deturpazione) identifica un'azione svolta nei confronti di un sito Web allo scopo di cambiarne i contenuti.

DHCP
Acronimo di Dynamic Host Configuration Protocol, protocollo di rete per la configurazione dinamica dei Client.

Dialer
Deriva dal verbo inglese "to dial" che significa "comporre" ed è adoperato per indicare i software in grado di effettuare connessioni telefoniche.

DNS
Acronimo di Domain Name System, servizio che traduce i nomi delle macchine nei relativi indirizzi numerici e viceversa.

DoS
Acronimo di Denial of Service, rifiuto del servizio, situazione nella quale un servizio di rete non è più in grado di rispondere a nessuna richiesta; il DoS causa, quindi, la paralisi del servizio stesso.

Exploit
Il termine Exploit (sfruttare) identifica una tecnica o un Software in grado di sfruttare una certa vulnerabilità.

Fake
Sinonimo di Alias o di notizia falsa.

Fault Tolerance
Con questo termine si descrivono quei sistemi in grado di continuare ad operare nonostante il presentarsi di un'anomalia (guasto) parziale.

Feed
Servizio per avere l'abbonamento all'aggiornamento dei contenuti (ad esempio le news) senza dover controllare in continuazione la piattaforma. I feed si basano su RSS e si usano sulle piattaforme in cui appaiono costantemente nuovi contenuti.

Filtro
Software utile per ridurre il numero delle informazioni secondo certi criteri, in modo da averne poche e utili.

Fingerprinting
In italiano si traduce con "prendere le impronte digitali"; rappresenta una delle prime fasi di un attacco informatico.

Firewall
Sistema Software o Hardware di protezione che ha il compito di difendere dagli accessi abusivi un elaboratore (Firewall personale di tipo Software) o un'intera rete di Computer (Firewall di tipo Hardware).

Form
Caselle da compilare all'interno di una pagina Web.

Forum
Un gruppo di discussione virtuale presente sulla rete Internet.

Gateway
Dispositivo che ha il compito di collegare due reti; il termine si traduce letteralmente con le parole italiane "ingresso" o "passaggio".

Ghostware
Software che, in virtù di particolari tecniche di programmazione, sono in grado di rendersi invisibili all'utente.

GPL
Acronimo di General Public License, rappresenta la più diffusa licenza con la quale viene distribuito il Software Open Source; essa permette la copia, la modifica e la ridistribuzione libera, purché sempre assieme al codice sorgente.

Grado di separazione
Numero delle persone che formano la catena dei contatti tra due persone.

Grafo sociale
Visualizzazione tramite forme grafiche delle relazioni sociali tra le persone.

Half-duplex
Comunicazioni che possono operare in una sola direzione alla volta.

Handshaking
Attività preliminare condotta tra due macchine che desiderano instaurare una comunicazione bilaterale: lo scopo di questo processo è quello di accertare la disponibilità di entrambe le parti allo scambio dei dati. La sua traduzione letterale è "stretta di mano".

Hash
Funzione univoca (detta, anche, One Way) in grado di operare in un solo senso; questo significa che dal risultato di questa funzione non si può in alcun modo risalire ai dati in ingresso.

Header
Il termine "header" (intestazione) identifica la parte iniziale di una PDU (Protocol Data Unit: unità caratteristica di un protocollo); esso riporta delle importanti informazioni di controllo.

Heap
Particolare area della memoria dedicata all'immagazzinamento di dati importanti.

HIDS
Acronimo di Host based Intrusion Detection System, sistema di rilevazione delle intrusioni.

Home Banking
Possibilità di usufruire dei servizi bancari a domicilio, tramite il Computer o qualunque altro mezzo idoneo (televisione interattiva, telefono cellulare, etc.).

Honeypot
Unione dei termini "honey" e "pot" (si traduce come "vasetto di miele"), individua alcuni Software esca che simulano la presenza di sistemi reali.

Host
Utilizzato per indicare un generico dispositivo connesso ad una rete informatica come, ad esempio, un elaboratore o una stampante.

Hot Spot
Indica un punto di accesso Wireless (gratuito o a pagamento) ad Internet posto all'interno di un'area pubblica.

HTTP
Acronimo di Hypertext Transfer Protocol, protocollo adoperato per il trasferimento di pagine Web tra Web Server e Browser (applicazione Client utilizzata per visualizzare le pagine Web).

HUB
Dispositivo adoperato per connettere tra loro più macchine all'interno di una rete.

IANA
Acronimo di Internet Assigned Numbers Authority, Ente responsabile dell'assegnazione di nomi, indirizzi e protocolli.

ICF
Acronimo di Internet Connection Firewall, un Firewall di tipo Software integrato nel sistema operativo Microsoft Windows XP.

Identità
Sinonimo di "Account".

Informativa sulla Privacy
Pagina scritta dall'amministratore del servizio fornito su Internet con le informazioni in merito a come verranno utilizzati i dati personali inseriti dall'utente, chi potrà usare questi dati, come opporsi al loro trattamento. Altri dettagli sul sito www.garanteprivacy.it

IDS
Acronimo di Intrusion Detection System, un Software rilevatore di intrusioni.

IETF
Acronimo di Internet Engineering Task Force, organizzazione responsabile delle regole di invio di dati su Internet.

Internet
Deriva dall'unione della parola latina inter (fra) e quella anglosassone net (rete); identifica una rete di dimensioni planetarie.

InterNIC
Acronimo di Internet Network Information Center, centro informazioni sulla rete Internet.

Interpol
Acronimo di International Criminal Police Organization, una polizia a carattere internazionale.

IP
Acronimo di Internet Protocol, un protocollo della famiglia TCP/IP.

IPv4
Acronimo di IP Version 4, protocollo IP versione 4.

IPv6
Acronimo di IP Version 6, protocollo IP versione 6.

ISDN
Acronimo di Integrated Services Digital Network, la rete telefonica pubblica di tipo digitale.

ISOC
Abbreviazione di Internet SOCiety, organizzazione che promuove l'utilizzo e lo sviluppo della rete Internet.

ISP
Acronimo di Internet Service Provider, organizzazione che fornisce l'accesso alla rete Internet.

IT
Acronimo di Information Technology, identifica tutti i sistemi di elaborazione e trasmissione dei dati di tipo informatico.

ITU-T
Acronimo di International Telecommunication Union - Telecommunication Standardization Bureau, ovvero, Unione Internazionale delle Telecomunicazioni con il compito di regolare le comunicazioni di tipo telefonico.

IV
Acronimo di Initialization Vector, un vettore di inizializzazione utilizzato nel protocollo WEP.

K (opzione)
Vedi KoreK.

Kerckhoffs (legge di)
Legge che recita: la sicurezza di un crittosistema non deve dipendere dal tener celato il crittoalgoritmo, la sicurezza dipenderà solo dal tener celata la chiave.

Kernel
Rappresenta il nucleo centrale del sistema operativo.

KoreK
Si tratta di una serie di attacchi statistici molto efficienti, utilizzati nell'ambito degli attacchi alle reti Wireless, sviluppati da un personaggio soprannominato KoreK.

LAN
Acronimo di Local Area Network, rete di piccole dimensioni.

Laptop
Sinonimo di Notebook, identifica un Computer di tipo portatile.

LMHOSTS
File locale di tipo testo che ha lo scopo di effettuare l'associazione (Mapping) tra indirizzi IP e nomi NetBIOS di Server remoti con i quali si intende comunicare tramite il protocollo TCP/IP.

Log (file)
Nei file di Log sono registrati diversi tipi di attività inerenti al sistema: ad esempio, nel caso di un dispositivo Firewall, essi riportano i tentativi di accesso non autorizzati.

Logging
Attività di monitoraggio degli eventi.

Login
Operazione di accesso al sistema che si effettua, solitamente, attraverso l'immissione di una UserID e di una Password.

Loopback
Interfaccia di servizio prevista dai protocolli della famiglia TCP/IP; la sua presenza è molto utile per l'esecuzione di alcuni controlli.

Malware
Acronimo di Malicious-Logic Software, categoria di Software che svolge attività all'insaputa dell'utente (Virus, Spyware, Trojan, eccetera).

Mashup
Dall'inglese "to mash", mescolare. Indica la creazione di nuovi contenuti usando la ricombinazione di materiali già esistenti. Funzionano grazie alle interfacce di programmazione (API) aperte, create e diffuse da altre applicazioni web. Si possono così mescolare dati di una cartina geografica con fotografie, video, ecc. Molto diffuso in ambito Web 2.0.

Masquerading
Il termine identifica una tecnica utilizzata per il mascheramento degli Indirizzi IP.

MATA
Acronimo di Mobilization Against Terrorism Act, gruppo di leggi USA.

MIMO
Acronimo di Multiple Input, Multiple Output, particolare modalità di funzionamento dei dispositivi Access Point.

Mirror
Area di un sito Web che possiede gli stessi contenuti di un altro sito.

Modem
Abbreviazione di Modulator/Demodulator, dispositivo che consente il trasferimento di dati da un Computer ad un altro attraverso l'uso di un normale cavo telefonico.

Motore di ricerca
Funzione per facilitare la ricerca di notizie in tutta la rete Internet o in un certo sito. Si scrive in un campo la parola di cui si intende ricercare notizie e il software fornisce una selezione di link pertinenti.

Multicast
Metodo adoperato per trasmettere dati attraverso le reti basato sul seguente meccanismo: una singola macchina trasmittente invia un certo flusso di dati verso più macchine riceventi.

NAT
Acronimo di Network Address Translation, servizio di traduzione degli indirizzi di rete.

Network
Usato per indicare una rete di collegamento tra i computer, indica genericamente un insieme di nodi collegati da archi che indicano le relazioni tra i nodi.

Networker
Persona impegnata nel fare networking.

Networking
Creare nuove relazioni con sconosciuti tramite i social network.

NIC
Acronimo di Network Information Center, organismo preposto alla registrazione, assegnazione e gestione dei domini di tipo .it.

Nmap
Potente Software di scansione.

Nslookup
Abbreviazione di Name Server Lookup, è un comando presente su tutte le macchine che adoperano i protocolli della famiglia TCP/IP.

NTFS
Acronimo di New Technology File System, identifica un tipo di File System utilizzato nei sistemi operativi basati sul kernel NT.

NTP
Acronimo di Network Time Protocol, protocollo utilizzato per la sincronizzazione dell'orario in rete.

Null Session
Metodo per sfruttare una vecchia vulnerabilità presente nel meccanismo di autenticazione dei sistemi Microsoft Windows.

Open Source
Modalità di distribuzione (codice sorgente aperto) che permette l'accesso ai sorgenti del Software e consente sia la modifica che la libera ridistribuzione.

OS
Acronimo di Operating System, sistema operativo.

OSI
Acronimo di Open System Interconnection, modello di riferimento teorico.

Password Cracking
Software utilizzato per cercare, attraverso diversi metodi, l'identificazione di una password.

PAT
Acronimo di Port Address Translation, tecnica di traduzione implementata su alcuni dispositivi o sistemi operativi.

Payload
Dal gergo militare carica esplosiva, identifica l'azione commessa da un Virus al verificarsi di un certo evento.

Phishing
Operazioni che hanno lo scopo di ingannare l'utente inducendolo a comunicare dati riservati.

Phreaking
Prodotto dell'unione delle parole "phone" (telefono) e "freak" (persona stramba), identifica l'attività finalizzata a violare le reti telefoniche per trarne dei vantaggi.

Piattaforma
Indica l'insieme dei componenti Hardware e Software che costituiscono l'ambiente di esecuzione degli applicativi.

Ping
Comando adoperato per verificare la raggiungibilità di una macchina posta in rete.

Postare
Pubblicare un messaggio (post) in qualunque bacheca online o nei social media.

Privacy Policy
Sinonimo di Informativa sulla Privacy.

Provider
Fornitore di accesso alla rete Internet.

PSTN
Acronimo di Public Switched Telephone Network, la rete telefonica pubblica di tipo analogico.

PTW
Acronimo composto dalle iniziali dei nomi Pyshkin, Tews e Weinmann; identifica una tecnica per l'individuazione della chiave WEP in uso in una rete Wireless.

Random
Procedura di generazione che opera in modalità casuale (in inglese, appunto, "random").

RC4
Uno degli algoritmi di cifratura più utilizzati al mondo, realizzato dalla RSA Security.

Repeater
Si traduce con "ripetitore" e indica un dispositivo posto tra due segmenti di rete allo scopo di evitare perdite di segnale.

Report
Aggregazione di dati ottenuta in seguito all'applicazione di alcuni criteri di filtraggio.

Ricerca avanzata
I motori di ricerca offrono questo strumento per effettuare ricerche più dettagliate, occorre scrivere vari criteri di ricerca.

RIPE-NCC
Acronimo di Réseaux IP Européens - Network Coordination Center, centro di coordinamento per le reti della ricerca europea.

Risoluzione
Indica il processo di traduzione degli indirizzi attuato dai Server DNS.

Rootkit
Unione dei termini Root e Kit, si traduce in italiano come "equipaggiamento da amministratore"; ha lo scopo di occultare in un sistema informatico le operazioni eseguite da un aggressore.

Routing
Si traduce con instradamento, identifica il processo di movimentazione dei pacchetti all'interno delle reti.

RSS
Real Simple Syndacation, standard basato sull'XML indipendente da una piattaforma, per integrare nel sito Web messaggi o altri contenuti.

Run Time
Tempo di esecuzione, indica il periodo di esecuzione di un certo programma.

Script
Un insieme di istruzioni che può essere eseguito in modo automatico.

Server
Termine inglese che sta ad identificare un particolare elaboratore che rende disponibili dei servizi all'interno di una rete operante in modalità Client/Server, dove i Client sono gli elaboratori che fruiscono di detti servizi.

Server-side
Letteralmente “lato Server”, il termine è utilizzato per indicare le procedure operanti sulla parte Server.

Signature
Con il termine “Firme” (o Signature) si indicano dei file contenenti le caratteristiche peculiari che contraddistinguono certi elementi.

SMB
Acronimo di Server Message Block, protocollo standard utilizzato da Windows per la condivisione di file, stampanti e porte seriali.

SNA
Acronimo di Social Network Analysis, ovvero l’analisi matematica delle reti sociali, utile per la misurazione delle relazioni e dei flussi che si instaurano tra gli elementi della rete.

SNMP
Acronimo di Simple Network Management Protocol, protocollo utilizzato per il controllo e la gestione dei dispositivi connessi in rete.

Social Bookmarking
Vengono resi disponibili elenchi di segnalibri (bookmark) creati in condivisione dagli utenti. Possono essere per esempio link a siti Internet divisi per categorie. Gli elenchi sono consultabili e condivisibili con gli altri utenti della comunità.

Social Engineering
Si traduce ingegneria sociale, indica una serie di tecniche basate su azioni di imbroglio e/o persuasione volte ad ottenere informazioni riservate.

Social network
Traduzione inglese di “rete sociale”, è un network in cui i nodi rappresentano le persone e gli archi rappresentano le relazioni tra le persone.

Social software
Software che consente alle persone di incontrarsi, interagire e collaborare in rete per creare comunità online.

Socket
In letteratura informatica, il termine Socket identifica un’entità capace di inviare e ricevere dati.

SOHO
Acronimo di “Small Office, Home Office”, è generalmente utilizzato per identificare quella fascia di utenti che operano all’interno delle abitazioni domestiche o di piccoli uffici.

Spam
Sinonimo del termine più appropriato UBE (Unsolicited Bulk E-Mail), cioè, posta elettronica spedita senza permesso; originato dal nome di una famosa carne di maiale in scatola, indica la posta elettronica spedita in modo massivo e/o non richiesta dal destinatario.

Spoofing
Indica una serie di tecniche atte a camuffare la reale identità di chi compie una certa operazione.

Spyware
Risultato dell’unione dei termini anglosassoni “Spy” (spia) e “Software”; è un Software adoperato per raccogliere segretamente informazioni circa le abitudini dell’utente.

SSID
Acronimo di Service Set Identifier, elemento identificativo di una rete Wireless.

Stack
Insieme di protocolli.

Stand Alone
Utilizzo individuale dell'elaboratore, cioè non connettendosi ad alcuna rete.

Streaming
Modalità di trasmissione che permette la fruizione di contenuti multimediali senza che questi debbano essere preventivamente prelevati.

Switch Poisoning
Tecnica che interviene sul processo di commutazione di uno Switch al fine di alterarlo.

TAG
Serie di caratteri in linguaggio HTML adoperati per impartire particolari istruzioni.

Taggare
Scrivere un tag per un documento digitale. In merito ai social network si sente spesso l'espressione "sei stato taggato" per indicare che una persona ha inserito il proprio nome in una foto presente online (su social network o altri servizi); per sapere se qualcuno ci ha taggato, violando eventualmente la nostra privacy, basta fare una ricerca con il nostro nome nei social network.

TCP/IP Suite
Acronimo di Transmit Control Protocol/Internet Protocol, identifica una famiglia di protocolli.

TELNET
Servizio che consente di operare su una macchina remota in modalità terminale.

Terms of Use
Sinonimo di "Condizioni d'uso".

Throughput
Indica la banda effettiva rilevata in un certo periodo di tempo.

Timeout
Rappresenta un certo lasso di tempo nel quale si attende prima di dichiarare una certa operazione non riuscita.

Timestamp
Indica la data e l'ora dell'istante in cui un certo evento si è verificato.

TKIP
Acronimo di Temporal Key Integrity Protocol, protocollo che ha il compito di variare dinamicamente la chiave di cifratura WEP nell'ambito delle reti Wireless.

UBE
Acronimo di Unsolicited Bulk E-Mail, cioè posta elettronica spedita senza permesso.

Unicast
Metodo adoperato per trasmettere attraverso le reti, esso è basato sull'invio di un flusso di dati per ogni macchina ricevente.

Unix Like
Sistemi operativi derivati da Unix, come ad esempio Linux o FreeBSD.

URL
Acronimo di Universal Resource Locator, identifica l'indirizzo completo necessario per individuare una pagina nel Web.

Usenet
Rete adoperata per la gestione dei gruppi di discussione presenti sulla rete Internet.

User Agreement
Sinonimo di "Condizioni d'Uso".

VPN
Acronimo di Virtual Private Network, modalità di connessione sicura tra due reti di tipo privato attraverso una rete di tipo pubblico.

WAN
Acronimo di Wide Area Network, una rete informatica di grandi dimensioni.

War Dialing
Tecnica che analizza un intervallo di numeri di telefono al fine di rilevare la presenza di Modem configurati per l'accesso remoto alla rete interna.

Warez
Server che distribuiscono illegalmente Software commerciale.

Widget
Piccoli software di supporto che appaiono sul desktop di un computer o in un sito.

Wi-Fi
Abbreviazione di Wireless Fidelity, indica la tecnologia che permette di comunicare senza l'ausilio di cavi.

WINS
Acronimo di Windows Internet Naming Service, servizio di rete che si occupa di associare dinamicamente ed in modo automatico gli indirizzi IP ai relativi nomi macchina.

Wireless
Dall'inglese "senza fili", è adoperato come aggettivo per identificare quei dispositivi che non utilizzano cavi per il loro funzionamento.

W-Lan
Acronimo di Wireless Local Area Network, una rete LAN di tipo Wireless.

X.509
Standard per il formato dei certificati a chiave pubblica; pubblicato anche come standard ISO/IEC 9594-8.

Zero Configuration
Servizio di Microsoft Windows che permette la configurazione rapida degli adattatori di rete Wireless.