powered by IBM

La sicurezza delle informazioni nell'era del Web 2.0

I contributi della wiki IBM sul tema della sicurezza informatica e di come gli strumenti offerti dal web 2.0 possano essere amministrati senza mettere a repentaglio la sicurezza dei sistemi.

Documento pubblicato in collaborazione con IBM sotto licenza Creative Commons.

INTRODUZIONE

"La sicurezza delle informazioni nell'era del Web 2.0" è il tema del progetto promosso da IBM per discutere sul tema della sicurezza informatica e, nello specifico, di come gli strumenti offerti dal web 2.0 possano essere amministrati senza mettere a repentaglio la sicurezza dei sistemi.

Il progetto è coordinato dal Dott. Roberto Marmo, consulente informatico, professore a contratto di informatica presso la Facoltà di Ingegneria della Università di Pavia e Facoltà Scienze MM.FF.NN. della Università Insubria – Como e studioso del web 2.0. http://www.robertomarmo.net.

Questo progetto vorrebbe idealmente proseguire il percorso iniziato con il tema "La sicurezza aziendale ai tempi di Facebook", promosso in occasione dell'evento IBM Security Day 2009. Accedi alla documentazione finale e scarica il documento in formato pdf oppure accedi alla pagina in cui si descrivono le finalità del progetto.

L'obiettivo di questo progetto

Il documento che si intende sviluppare in questo ambiente wiki intende rendere noti i nuovi rischi e pericoli derivanti dall'uso del web 2.0 con priorità rivolta all'ambito aziendale e della Pubblica Amministrazione. Il documento è rivolto in particolare a chi non ha sufficiente fiducia verso le potenzialità del web 2.0 a causa dei pericoli derivanti per la sicurezza informatica dei loro sistemi e la riservatezza dei dati. Si vuole pertanto diffondere la consapevolezza e la cultura per un uso responsabile.

INDICE

IL CONCETTO DI SICUREZZA INFORMATICA

La sicurezza informatica ha come obiettivi:
- il controllo del diritto di accesso alle informazioni;
- la protezione delle risorse da danneggiamenti volontari o involontari;
- la protezione delle informazioni mentre esse sono in transito sulla rete;
- la verifica dell'identità dell'interlocutore, in particolare la certezza 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 il problema, più semplice è la sua risoluzione.
3. **Response:** è necessario sviluppare un piano appropriato di intervento in caso di violazione con individuazione delle responsabilità e le 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 lo stato di salute del sistema 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. Questo documento permette di conoscere qual è il rischio di subire danni al proprio sistema informatico e, di conseguenza, di preparare una mappa delle possibili contromisure da adottare.
Il Vulnerability Assesment permette di raccogliere informazioni sul sistema informatico tramite la registrazione dei potenziali problemi di sicurezza individuati. Si decide poi di proseguire con il Penetration Test per controllare la sicurezza del sistema informatico con una serie di attacchi mirati alla ricerca di problemi di sicurezza.

La nascita di nuovi problemi per la sicurezza informatica

Tutto ciò ha portato all'uso sempre più diffuso con una forte crescita delle opportunità, dei vantaggi, della quantità di informazioni. Il rapido sviluppo, però, non ha ancora permesso una 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.

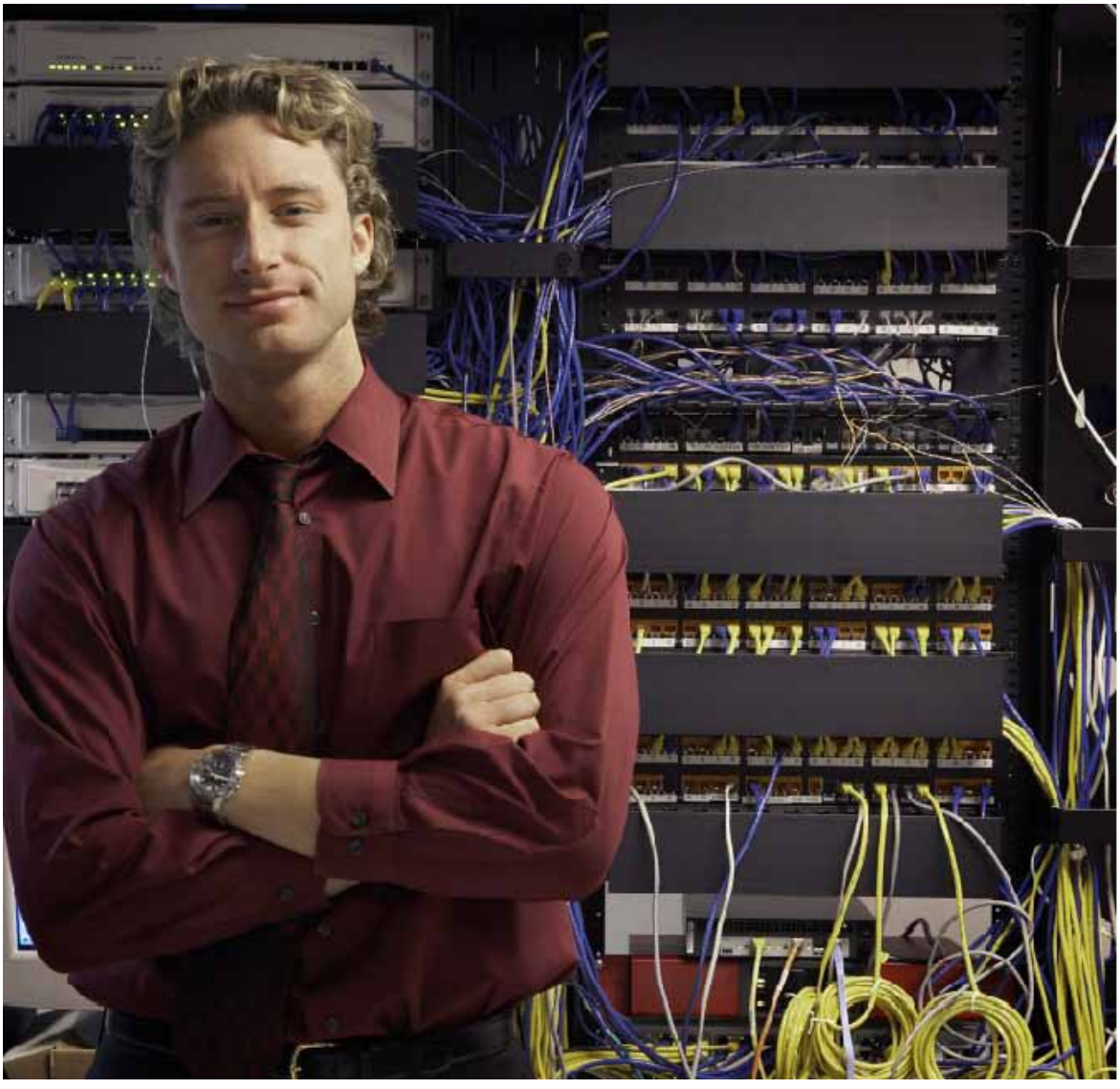
Il ruolo dell'amministratore
Il ruolo di amministratore della sicurezza deve comprendere l'educare e rendere consapevoli di rischi derivanti da uso in ambito lavorativo.

Quali sono le nuove responsabilità e il nuovo ruolo del responsabile della sicurezza ICT?

Il responsabile della sicurezza deve certamente ridurre il rischio che in ufficio il social network venga utilizzato in modo indebito. Deve innanzitutto creare chiare regole di disciplina da aggiornare periodicamente, in cui indicare 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 all'attività aziendale.

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



INFORMATION TECHNOLOGY E SICUREZZA

Spesso si dimentica che la sicurezza di un'infrastruttura IT non è data soltanto dai sistemi utilizzati per arginare una serie di problematiche (attacchi esterni o interni, social engineering, sicurezza dei sistemi operativi o degli applicativi...), ma da tutta una serie di fattori che possono essere analizzati con strumenti validi. Se, ad esempio, abbiamo un sistema che esegue svariati processi (in modalità utente non privilegiato) è possibile creare un software ad hoc che consenta di creare errori (es. "divisione per zero") che possono portare il sistema in una situazione "non giusta" tale da consentire all'utente che esegue il software malevolo, di avere privilegi superiori (es. root). È molto difficile scoprire/testare tutti i processi in esecuzione sul proprio sistema, nell'esempio precedente si procede sfruttando vulnerabilità del cuore stesso del sistema operativo, ma è possibile che il programmatore abbia veramente sbagliato nella stesura di un determinato software, che in alcune situazioni particolari (non testate precedentemente al rilascio) portano ad un rischio veramente grave.

Esistono molti strumenti che permettono un'attenta analisi di ciò che è presente nei nostri sistemi IT. Anche in Italia la diffusione di best practice utilizzate (e nate) in paesi anglosassoni, è in continua evoluzione. Tra tutti questi strumenti è doveroso citare "IT Infrastructure Library - ITIL" nella sua versione 3. ITIL è un insieme di best practice per la gestione di un sistema IT, descrivendone i processi, le funzioni e le strutture che sono di supporto a molte aree di un sistema IT.

Tra tutti questi processi vengono descritte le linee guida di un sistema di gestione della sicurezza delle informazioni, adattato per essere applicato in vari ambiti.

Gli standard internazionali di riferimento di gestione di servizi IT, appartengono alla famiglia ISO/IEC 20000, che è suddivisa in varie parti.

Mentre un attore del panorama IT che si attiene a questi standard può "certificarsi" secondo le linee guida della norma ISO, se utilizza ITIL non è obbligato a seguire le norme ISO, ma è sicuro che seguendo queste ultime sarà comunque in grado di progettare una struttura IT con le dovute caratteristiche business continuity, delivery, maintenance, security...

Per la gestione della sicurezza ci sono quattro standard che appartengono alla famiglia ISO/IEC 27000:

1) 27001:2005 Information Security Management Systems - Requirements
2) 27002:2005 Code of Practice for Information Security Management
3) 27005:2008 Information Security Risk Management
4) 27006:2007 Requirements for Bodies Providing Audit and Certification of Information Security Management Systems

Ed in più: ISO/IEC 27799:2008 Health Informatics - Information Security Management in Health Using ISO/IEC 27002

Le altre in preparazione (alcune quasi completate e rilasciate tra la fine del 2009 e l'inizio del 2010):

- 27000 introduzione con i principi, i concetti ed un glossario dei termini
- 27003 guida all'implementazione della 27001 e 2
- 27004 analisi per un sistema di gestione della sicurezza
- 27007 guida per gli auditor di sistemi di gestione della sicurezza verso le specifiche della ISO/IEC 27001
- 27032 Cybersecurity (dovrebbe essere l'insieme delle linee guida per gli Internet Service Provider e gli utenti della rete)
- 27033 Network security (preventivate sette sezioni)
- 27034 Sicurezza delle informazioni per le applicazioni IT

Parecchie linee guida appartenenti ad ITIL e alle linee guida ISO/IEC sono sovrapponibili o comunque "molto vicine" fra loro e consentono una gestione EFFICACE del proprio sistema IT.

L'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, ecc.

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 ecc.) 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 ecc.), è certamente auspicabile non trovarsi mai in una di queste situazioni.

La prassi seguita dall'aggressore è quasi sempre la stessa: quando egli 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.

Pertanto, l'analisi dei rischi è elemento fondamentale per la scelta delle misure di sicurezza appropriate secondo il valore delle risorse da proteggere e dei potenziali danni.

CREARE E GESTIRE UN SISTEMA PER LE DOMANDE DI SICUREZZA

Gran parte dei nostri account su Internet, che siano e-mail, registrazioni a siti, Paypal, eBay o altro, presenta una vulnerabilità non da poco: **la domanda di sicurezza**. Chiedere il nome della madre da signorina, o la città dove siamo nati, o il nome del nostro primo cane o gatto poteva essere una buona idea (?) anni fa, ma oggi dobbiamo fare i conti con un aumento esponenziale del numero di siti dai quali è possibile ottenere facilmente tali dati sul nostro conto. Mettere ampi stralci della propria vita in piazza su Facebook e altri social network può semplificare il lavoro a un ipotetico aggressore telematico che desideri impossessarsi di uno qualsiasi dei nostri account. E se anche non fossimo noi a rivelare dettagli della nostra vita, potrebbero farlo, in buona fede, i nostri amici su quegli stessi social network.

Dimentichiamoci quindi di ritenere sicure informazioni come quelle, o altre sempre inerenti alla nostra vita "semi-pubblica", come il modello di auto che guidiamo o la data del nostro matrimonio, per fare altri due esempi.

Poiché la domanda di sicurezza è una procedura sempre più usata durante la registrazione ai siti, dobbiamo trovare un modo per continuare a usarla e allo stesso tempo impedire agli altri - anche alle persone che ci conoscono - di trovarla.

Iniziamo con analizzare alcune caratteristiche di questa domanda di sicurezza e della relativa risposta:

1. una volta inserita di solito non la si usa quasi mai, quindi è facile dimenticarla;

2. per noi non deve essere necessariamente immediata da trovare o da ricordare, perché dopotutto la si deve usare solo nei casi di emergenza, basta che alla fine si riesca a reperirla;

3. a volte viene chiesto di inserire molteplici domande e risposte di sicurezza;

4. molti siti ci invitano a cambiare regolarmente la password, ma non la domanda di sicurezza. Potremmo quindi essere chiamati a ricordarcela anche dopo molti anni;

5. non è possibile trascriverla.

Riguardo l'ultimo punto, qualcuno potrebbe obiettare che vi è sempre la possibilità di inserire risposte casuali tenendone poi traccia con un programma di salvataggio delle password, tuttavia ciò snaturerebbe il senso della domanda di sicurezza, che dovrebbe essere considerata "l'ultima spiaggia" nei casi in cui detti programmi risultassero indisponibili.

Come fare quindi per fornire una risposta robusta ma allo stesso tempo da noi accessibile in caso di emergenza? Ecco una serie di soluzioni che potranno aiutarci a gestire meglio questo problema.

1. AGITARE E MESCOLARE

Nel caso il sito ci consentisse di scrivere la nostra domanda di sicurezza e la relativa risposta, sarebbe utile creare un quesito difficile da risolvere per tutti fuorché per noi, dopodiché mischiare le risposte e codificarle assieme.

Alcuni esempi di domanda:

D: Numero di telaio della mia seconda auto e totale della mia dichiarazione dei redditi del 1998, nell'ordine di ciò che è arrivato prima.

D: Numero di protocollo del rogito per l'acquisto della mia casa di Perugia e numero della prima carta d'identità che ho chiesto al Comune di Roma, nell'ordine di ciò che ho ottenuto prima.

D: Il voto che ho preso alla maturità moltiplicato per gli anni di ginnasio che ho effettivamente frequentato, diviso per gli anni di lavoro che ho trascorso prima di conoscere mia moglie.

Se in molti di questi esempi la risposta sembra lunga da trovare anche per l'interessato, ricordate il punto 2. di cui sopra: fornire la risposta alla domanda di sicurezza generalmente diviene necessario solo in caso di emergenza, quindi non importa quanto sia lunga la ricerca, l'importante è che alla fine solo noi saremo in grado di trovarla.

Vantaggi: Si tratta di parametri immutabili nel tempo e difficilmente reperibili in pubblico, perché pochi sono soliti pubblicare tali

informazioni dentro un post in un blog o nel proprio profilo su Facebook.

Svantaggi: È probabile che per ritrovare la risposta dovremo andare a scartabellare un po' di vecchi documenti, di cui dovremo necessariamente conservare una copia. Inoltre, malgrado siano alquanto difficili da trovare, non è escluso che qualcuno con le adeguate risorse e il tempo necessario sia in grado di reperire l e risposte. Infine, è un metodo che si può usare solo quando il sito ci permette di scrivere le domande.

2. RISPOSTE INVERTITE

Per confondere le idee a tutti fuorché a noi, è possibile immaginarsi un certo ordine con cui invertire domande e risposte. Ad esempio se chiedono il cognome da nubile di vostra madre voi inserite la città in cui siete nati, e viceversa.

Vantaggi: È un metodo semplice da ricordare e di immediato utilizzo. Si può usare anche quando il sito non ci permette di scrivere da noi la domanda di sicurezza, a patto che usi domande banali.

Svantaggi: Bisogna mantenere questo metodo segreto. Non funziona quando il sito ci offre domande non banali (ad es. il nome della prima scuola) e al tempo stesso non ci permette di scrivere le domande da soli. Infine, bisogna ricordarsi quali argomenti sono stati scambiati fra loro, o si rischierà di fare confusione.

3. REALTÀ AD HOC

È uno dei metodi più curiosi e affascinanti, ma anche il più pericoloso per chi non ha una mente disciplinata. Si inventano alcuni dettagli di un mondo immaginario che abbiamo creato ad hoc e che conosciamo solo noi, dove molte informazioni sono alterate. Ad esempio se in realtà siamo nati a Roma, il cognome di nostra madre da nubile è Rossi e al liceo siamo andati al Dante Alighieri, possiamo invece stabilire che siamo nati a Milano, il cognome di nostra madre è Bianchi e al liceo siamo andati al Petrarca. Così facendo la risposta alla domanda di sicurezza "dove sei nato" sarà Milano, anche se ovunque nei nostri documenti e nei nostri social network ci sarà scritto che siamo nati a Roma. Un eventuale malintenzionato non avrà modo di conoscere le risposte, proprio perché le avremo inventate di sana pianta.

Vantaggi: È praticamente impossibile che un malintenzionato individui le risposte scavando nella nostra vita privata. Le risposte inoltre sono di facile utilizzo da parte nostra, non ci sarà bisogno di scartabellare nulla, se non la nostra fantasia.

Svantaggi: Queste informazioni andranno ricordate per sempre, e proprio perché irreali sarà particolarmente difficile ricordarle tali e quali ad esempio fra dieci o venti anni. Inoltre, non bisognerà ovviamente condividere pubblicamente i dettagli di questo "mondo parallelo".

4. APRIRE IL LIBRO A PAGINA N

Usare un vecchio libro come fonte di risposte alle nostre domande di sicurezza è uno dei metodi più romantici e allo stesso tempo abbastanza efficace, basta non rivelare il titolo del libro né l'autore. Quando dovremo scrivere una domanda di sicurezza, sarà sufficente indicare "Pagina venti, quarta riga, quinta parola" e il gioco è fatto. Ovviamente sarà necessario avere quel dato libro sempre a portata di mano. Per sempre.

Vantaggi: È un metodo relativamente sicuro, a patto che manteniate segreti i dati del libro (autore, titolo, edizione). Se avete il libro a portata di mano, trovare le risposte sarà molto rapido.

Svantaggi: Dovrete avere quel libro sempre con voi. Perdetelo e con esso perderete tutte le risposte alle domande di sicurezza, almeno fino a quando non lo ricomprerete (sperando di riuscire a trovare esattamente la stessa edizione). Non funziona ovviamente quando il sito non ci permette di scrivere le domande.

5. SCAVARE NELLA PROPRIA MEMORIA A LUNGO TERMINE

Qui camminiamo su un terreno sdrucciolevole, quindi sta a voi decidere se usare o meno

questo metodo. Scavate nella vostra memoria e andate a ripescare ricordi vividi di eventi che vi sono capitati almeno dieci anni fa, se non ancora prima. Può essere qualsiasi cosa, basta che abbia lasciato un ricordo indelebile nella vostra memoria. Alcuni ricordi sono immutabili nel tempo, persistono anche quando siamo molto in là con gli anni, quindi perché non usarli a nostro vantaggio? Se ad esempio un giorno siete caduti con la bicicletta in modo alquanto disastroso, vi ricorderete quella caduta più di ogni altra. La domanda potrà essere "Dove mi trovavo quella volta che sono caduto rovinosamente dalla bicicletta?".

Attenzione tuttavia a non creare delle domande con risposte facili da indovinare. Una domanda sbagliata potrebbe essere "Era giorno o era notte quando sono caduto rovinosamente dalla bicicletta?", visto che bastano due tentativi per indovinare la risposta giusta. Stessa cosa con gli anni, mai chiedersi "Quanti anni avevo quando..." perché a meno che non siate Matusalemme, saranno sufficienti poche decine di tentativi per trovare la risposta giusta.

In generale, se volete usare questo metodo, ponetevi nei panni di un malintenzionato e cercate di capire quanto possa essere facile indovinare la risposta anche senza conoscerla. Evitate quindi riferimenti ai tratti somatici di una persona (es. "Di che colore ha gli occhi Tizio?") perché possono essere individuati dopo pochi tentativi. Inoltre, se avete sempre abitato nella stessa città (e questo potrebbe essere facilissimo da individuare, basta scaricare un qualche curriculum che avete messo in rete), non ponete domande del tipo "Dove abitavo quando...".

Cercate dei particolari che nessuno conosce, ma che allo stesso tempo sono ben piantati nella vostra memoria. Inoltre, per rendere la procedura più difficile, ponete la domanda in modo criptico per tutti fuorché per voi. Ad esempio se ricordate bene come da bambini avete avuto un incidente che vi ha lasciato un bernoccolo sulla testa, chiedete "Cosa mi diede quel bernoccolo?" Sarà inutile per un eventuale malintenzionato elencare tutto il pentolame di casa, quando alla fine a darvi quel bernoccolo fu vostro fratello maggiore (notare il piccolo trabocchetto insito nella domanda, quando usiamo il termine "cosa").

Se possibile poi usate termini generici quel tanto che basta a rendere la vita più difficile a chi cerca di indovinare la risposta. Se volete necessariamente indicare il nome di una città, non scrivete "In che città mi trovavo quando...", scrivete piuttosto "In che posto mi trovavo quando..." perché aprirebbe molti altri ipotetici scenari da individuare, visto che un "posto" può essere un edificio, un locale, una stanza, eccetera.

Fate poi attenzione a non creare delle risposte lunghe, perché i sistemi automatici di solito confrontano la risposta lettera per lettera. Una domanda del tipo "Perché l'allenatore mi prese nella squadra di calcio?" oggi potrebbe essere risposta con un "Perché mi disse che ero bravo", ma fra dieci anni potremmo non ricordarci le parole esatte che abbiamo usato per scrivere la risposta, e un semplice "Perché ero bravo" o "Perché mi disse che ero capace" non verranno riconosciute come esatte, anche se il senso è lo stesso.

Infine, non usate ricordi condivisi, come ad esempio il luogo dove avete chiesto a vostra moglie di sposarvi, perché gli altri "protagonisti" dell'evento potrebbero averlo raccontato ad amici o pubblicato on-line, soprattutto se si tratta di un evento particolare anche per loro. Ripescate il più possibile dalla vostra infanzia o dalla vostra gioventù, poiché andrete a trovare ricordi che hanno resistito alla prova degli anni, quindi pressoché indelebili.

Alcuni esempi di domanda corretta:

D: Cosa avevo fatto a Marina?

Commento: La domanda è generica quanto basta, e benché il ricordo sia condiviso (Marina fa parte dell'evento) probabilmente non era così importante per l'altro protagonista, sempre che quest'ultimo sia in grado di riconoscersi nell'evento. La risposta può essere qualsiasi cosa, un disegno, una dichiarazione, uno sgambetto... l'importante è che questa domanda evochi in noi - e solo in noi - subito la risposta giusta.

D: Chi incontrai sul ponte?

Commento: Anche se in questo caso il ricordo è condiviso, non si sa da chi. La persona può essere chiunque, se di persona si tratta. Per indovinare la risposta probabilmente non basterebbe l'intero libro dei nomi, soprattutto se nella risposta oltre al nome si inserisce anche il cognome. E se invece di una persona ci riferiamo a un animale? Lo sappiamo solo noi. Anche in questo caso ovviamente la domanda ci deve far balzare alla memoria subito la risposta giusta. L'evento deve essere indelebile, non qualcosa accaduto lunedì scorso.

D: Dove venni truffato durante quel viaggio?

Commento: Il ricordo non è condiviso, il viaggio è generico per tutti fuorché per noi. Inoltre il termine "dove" non lascia intendere se ci riferiamo a una città, un paese, un negozio, un albergo o altro.

Alcuni esempi di domanda sbagliata:

D: In che ruolo giocai in quella partita di calcio?

Commento: Giusto il riferimento a un evento sportivo che solo il protagonista riesce a individuare, ma sbagliato il riferimento al ruolo giocato. In campo ci sono undici giocatori, servirebbero quindi solo undici tentativi per individuare la risposta giusta (sedici se contiamo anche arbitri e allenatore).

D: Quanti anni avevo quando mi ruppi il braccio cadendo dalla bicicletta?

Commento: Sbagliato il riferimento a un evento così specifico tale da essere individuato anche da altri. Sbagliato inoltre indicare come risposta un numero abbastanza limitato e collegato all'età.

D: Quante guglie aveva l'edificio?

Commento: Giusto il riferimento a un edificio generico per tutti tranne che per il protagonista. Sbagliato il riferimento a un numero comunque limitato e facile da individuare. Quante guglie potrà avere un edificio? Una? Tre? Venti? Nessuna? Alla fine la risposta si trova.

Vantaggi: La risposta è molto difficile da scoprire, soprattutto se il ricordo viene scelto bene e se non ne avete mai parlato pubblicamente. Nel caso dobbiate utilizzare la risposta di sicurezza, l'unico posto che dovrete andare a scavare sarà la vostra memoria a lungo termine.

Svantaggi: Se il ricordo non è indelebile, o se è sovrapponibile ad altri, l'informazione rischia di andare persa o confusa con altre. Serve un po' di tempo per trovare il ricordo giusto e formulare la domanda in maniera appropriata. Infine, se formuliamo una domanda troppo generica, rischiamo di non ricordarci più quale aspetto del ricordo volevamo portare in risalto.

6. CODIFICARE LE RISPOSTE

Questo metodo funziona da solo o in combinazione con uno qualsiasi dei metodi descritti sopra. È sufficiente trovare un modo per codificare le vostre risposte, con un codice semplice o complesso a seconda del vostro grado di capacità di gestire i codici segreti.

Ad esempio, un codice semplicissimo può essere quello di invertire l'ordine delle lettere delle risposte reali. Se la città di nascita è Roma, basterà scrivere Amor. Se il cognome da nubile di vostra madre è Rossi si dovrà scrivere Issor. E via dicendo. Semplice ma già efficace.

Un codice leggermente più complicato può prevedere la trasformazione di determinate lettere in numeri o in caratteri speciali. Ad esempio potremmo decidere di trasformare ogni lettera "L" nel numero "1", ogni lettera "S" nel segno del dollaro "$" e ogni lettera "A" nel numero "4". L'ipotetico luogo di nascita "Sassari" si trasformerebbe quindi in "$4$$4ri", o il cognome da nubile di nostra madre "Bianchi" diventerebbe "Bi4nchi".

Per rendere il tutto un po' più complicato basta combinare i due codici indicati sopra, la trasformazione delle lettere e la loro inversione, ed ecco che "Sassari" diverrebbe "ir4$$4$" e "Bianchi" diverrebbe "ihcn4iB".

L'importante ovviamente è ricordarsi il codice e mantenerlo immutato nel tempo. E naturalmente non condividere questo segreto con nessuno.

Vantaggi: Senza la conoscenza del codice è impossibile per un malintenzionato individuare le risposte corrette, mentre per noi sarà facile indicare il termine giusto dopo aver compiuto solo un paio di operazioni. Questo metodo si può utilizzare in combinazione con tutti gli altri metodi indicati sopra.

Svantaggi: Sarà necessario ricordarsi questo codice anche dopo molti anni, e non modificarlo mai.

La letteratura

Sorprendentemente, ho trovato pochi testi che trattano in profondità questo argomento. Il sito http://www.goodsecurityquestions.com viene citato da più fonti. Esso fornisce un'analisi accurata delle caratteristiche che deve avere una buona domanda di sicurezza, assieme a esempi e a una tabella http://www.goodsecurityquestions.com/compare.htm per confrontare alcune domande di sicurezza secondo tali caratteristiche.

Contrariamente a quanto indicato nel sito di cui sopra, non sono d'accordo sulla necessità di assegnare alla domanda di sicurezza la caratteristica di "semplice, facile da ricordare". Come già spiegato nell'elenco di caratteristiche all'inizio di questo articolo, non vi è una vera necessità di ricordare in due secondi la risposta alla domanda di sicurezza, l'importante è reperirla in un tempo ragionevole.

Infine un ultimo consiglio. Quando troverete il metodo che fa per voi, assicuratevi che sia per sempre. Già adesso dovrete andare a cambiare praticamente tutte le risposte alle domande di sicurezza che avete lasciato in giro prima di oggi. Sarebbe scomodo doverlo fare ogni volta che cambiate metodo.

COSA SI INTENDE PER WEB 2.0

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 e il documento che ne ha ufficialmente sancito l'inizio risale al 30 settembre del 2005.

"Il Web 2.0 è la rete intesa come una piattaforma con tutti i dispositivi collegati; le applicazioni Web 2.0 sono quelle che permettono di ottenere la maggior parte dei vantaggi intrinseci della piattaforma, fornendo il software come un servizio in continuo aggiornamento e che migliora con l'utilizzo delle persone, sfruttando e mescolando i dati da sorgenti multiple, tra cui gli utenti, i quali forniscono i propri contenuti e servizi in un modo da permetterne il riutilizzo da parte di altri utenti, e creando una serie di effetti attraverso "un'architettura della partecipazione" che va oltre la metafora delle pagine del Web 1.0 per produrre così user experience più significative". (traduzione da "Web 2.0: compact definition", Tim O'Reilly)

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 web statici, di sola consultazione e con scarsa possibilità di interazione dell'utente.

La tendenza attuale è quella di indicare come Web 2.0 l'insieme di tutti gli strumenti/le applicazioni online che permettono uno spiccato livello di interazione sito-utenti quali i blog, i forum, le chat, etc... In ambito aziendale, la condivisione del Web 2.0 permette di creare idee insieme a tutti i dipendenti, commentare gli sviluppi di progetti in collaborazione con i dipendenti.

Tutto ciò è stato reso possibile da collegamenti ad Internet molto più veloci e dall'unione di varie tecnologie di facile apprendimento e uso.

Come appena citato, Il Web 1.0 a differenza del Web 2.0 era composto prevalentemente da siti web "statici", che non davano alcuna possibilità di interazione con l'utente, eccetto la normale navigazione tra le pagine, l'uso delle e-mail e dei motori di ricerca.

Il Web 2.0 viceversa costituisce un approccio filosofico alla rete che ne connota la dimensione sociale, la condivisione, l'autorialità rispetto alla mera fruizione. Il ruolo dell'utente in questo senso diventa centrale, esce dalla passività che lo contraddiceva nel Web 1.0 per diventare protagonista tramite la creazione, modifica e condivisione di contenuti multimediali a propria scelta.

Tendenzialmente per descrivere le caratteristiche del Web 2.0 si procede spesso per confronto con il Web 1.0, indicando come nel passaggio di versione gli elementi fondamentali si sono evoluti o sono stati sostituiti da nuovi. Si tratta di un modo di rappresentare il Web 2.0 divulgativo e non prettamente tecnico, ma piuttosto efficace per riconoscere l'evoluzione dei sistemi su Internet.

Ad esempio nell'era Web 1.0 la costruzione di un sito web personale richiedeva la padronanza di elementi di linguggio di programmazione HTML, viceversa oggigiorno con i blog chiunque è in grado di pubblicare i propri contenuti, magari dotandoli anche di una veste grafica più accattivante, senza possedere alcuna particolare preparazione tecnica specifica.

Le differenze tra Web 1.0 e web 2.0 potrebbero essere schematizzate come segue:

Web 1.0	Web 2.0
Top-Down	Bottom - Up
Contenuti in sola lettura	L'utente genera contenuti
Siti personali	Blogging
Sistemi di gestione dei contenti	Wikis
Servizi venduti sul web	Web - services
Client - server	Peer – to -Peer
Companies	Communities
Pubblicazione	Partecipazione
Directories (tassonomia)	Tagging (folksonomia)
Stickiness	Syndacation

Web 1.0 vs Web 2.0
Fonti varie

Concludendo, gli ingredienti del Web 2.0 sono: informazione, interazione, partecipazione, contributi creati degli utenti, connessione a reti sociali.

Altri approfondimenti su http://it.wikipedia.org/wiki/Web_2.0

Su questo link http://www.dynamick.it/web-20-una-definizione-in-10-punti-534.html si può trovare come viene definito da Tim O'Reilly in "What is Web 2.0", da Paul Graham nel suo "Web 2.0" e da Jason Fried nel libro "User Survey".

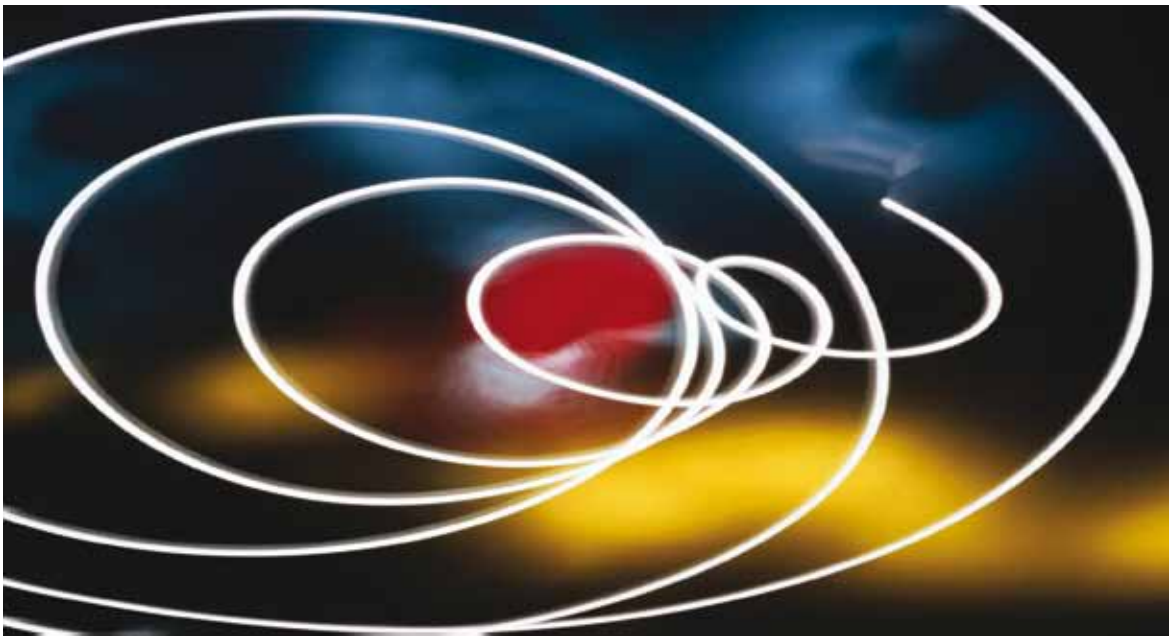
Social media è il termine generico per indicare tecnologie e pratiche online con cui gli utenti creano e condividono i contenuti sul web, un grosso cambiamento rispetto al web 1.0 caratterizzato dalla presenza di una comunità concentrata sulla condivisione di contenuti.
Altri approfondimenti su http://it.wikipedia.org/wiki/Social_media

Certamente 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, creando di fatto 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 ecc.
Altri approfondimenti su http://it.wikipedia.org/wiki/Social_network

Social network non riguarda solo le persone, la presenza di aziende è sempre più forte sia per attività di marketing e pubblicità sia come nuovo strumento per svolgere l'attività aziendale, creare il profilo aziendale per promuovere l'azienda, fare nuovi affari, ecc. L'Enterprise 2.0 intende infatti adattare i concetti del web 2.0 in ambito aziendale.

Il termine Enterprise 2.0 descrive un insieme di approcci organizzativi e tecnologici orientati all'abilitazione di nuovi modelli organizzativi basati sul coinvolgimento diffuso, la collaborazione emergente, la condivisione della conoscenza e lo sviluppo e valorizzazione di reti sociali interne ed esterne all'organizzazione.
Dal punto di vista organizzativo l'Enterprise 2.0 è volto a rispondere alle nuove caratteristiche ed esigenze delle persone ed a stimolare flessibilità, adattabilità ed innovazione.

Dal punto di vista tecnologico l'Enterprise 2.0 comprende l'applicazione di strumenti riconducibili al cosiddetto Web 2.0 – ovvero blog, wiki, RSS, folksonomie e, in un'accezione



più allargata, l'adozione di nuovi approcci tecnologici ed infrastrutturali.
Come detto l'Enterprise 2.0 deriva dal Web 2.0 ed è spesso usato per indicare l'introduzione e l'implementazione di Social Software all'interno di un'impresa ed i cambiamenti sociali ed organizzativi ad esso associati.
Il termine è stato coniato da Andrew McAfee, professore della Harvard Business School, nel paper seminale "Enterprise 2.0: The Dawn of Emergent Collaboration", pubblicato sul MIT Sloan Management Review.
La definizione puntuale secondo McAfee di Enterprise 2.0 è:

"l'uso in modalità emergente di piattaforme di social software all'interno delle aziende o tra le aziende ed i propri partner e clienti."
Così come visto per il Web 2.0 possiamo vedere anche in modo schematico quali sono le differenze tra Enterprise 1. 0 e 2.0:

Gli strumenti web 2.0 disponibili su Internet sono molteplici, una parte di questi con l'aggiunta di altri più specifici di un contesto aziendale formano l'insieme dei tool Enterprise 2.0.

Su Internet si possono trovare diverse classificazioni di questi strumenti, ad esempio da "Centre for Learning & Performance Technologies" (http://www.c4lpt.co.uk/Directory/Tools/collaboration.html)

Altri approfondimenti su http://it.wikipedia.org/wiki/Enterprise_2.0

Le applicazioni realizzate con l'approccio Web 2.0 sono spesso indicate come RIA - Rich Internet Application, ovvero applicazioni con uso intensivo di Internet. Le tecnologie RIA rappresentano approcci migliori con cui gli sviluppatori possono realizzare e distribuire interfacce utente semplici da usare, ricche e dinamiche. L'aspetto fondamentale del RIA è che l'interfaccia utente non deve essere rivisualizzata completamente dopo ogni interazione. In tal modo, si crea capacità di risposta e interattività del sistema.
Ajax (Asynchronous JavaScript and XML) è una tecnologia molto diffusa per l'aggiornamento dinamico di una pagina web senza esplicito ricaricamento da parte dell'utente, fondamentale nelle pagine web dei social network.

Enterprise 1.0	Enterprise 2.0
Organizzazione gerarchica	Organizzazione orizzontale
Frizioni	Semplicità nei flussi organizzativi
Burocrazia	Agilità operativa
Rigidità	Flessibilità
Innovazione guidata dalle tecnologie	Innovazione guidata dall'utente
Team centralizzati	Team distribuiti
Barriere	Spazi aperti
Gestione del sapere	Conoscenza aperta
Sistemi informativi strutturati	Sistemi informativi emergenti
Tassonomie	Folksonomie
Standard proprietari	Open standard
Scheduling delle attività	On demand
Time to Market lungo	Time to Market breve

Enterprise 1.0 vs Enterprise 2.0
Fonte: Adattamento da Forrester Research

SERVIZI OFFERTI DAL WEB 2.0

Il web 2.0 è caratterizzato da una serie di servizi innovativi come:

- wikipedia, enciclopedia caratterizzata da libera e gratuita fruizione dei contenuti da parte di tutti gli utenti, in un lavoro corale e collettivo destinato all'inserimento di nuove voci e alla correzione delle voci esistenti. Sito http://it.wikipedia.org;
- social network, per creare reti di relazioni tra le persone e condividere informazioni, foto, eventi, ecc. Il più famoso è Facebook mentre per le relazioni professionali si passa a LinkedIn o Viadeo. Altre informazioni sulla versione precedente di questa wiki destinata alla sicurezza dei social network;
- blog, possibilità molto semplice per tenere un diario personale visibile online. Il più famoso è WordPress;
- raccolte di fotografie commentate e classificate dagli utenti come Flickr;
- condivisione di link come Del.icio.us.;
- RSS Really Simple Syndication per la diffusione frequente di contenuti sul web da parte di blog e siti.

CLOUD COMPUTING PER IL WEB 2.0

Il cloud computing può dare una risposta di efficienza a molte problematiche aziendali: ad esempio consente un risparmio in termini di hardware di esercizio. La sua adozione non deve trascurare gli aspetti di sicurezza: in particolare l'azienda deve potersi fidare di chi offre il servizio.

La sicurezza nel cloud significa garantire soluzioni affidabili in grado di tenere in sicurezza le informazioni indipendentemente dal posto in cui sono memorizzate. Peraltro il cloud può innalzare i livelli di sicurezza aziendale tramite l'accentrare in un'unica soluzione tutta la gestione sicura di rete, server, memoria.

Sottolinea Bruce Schneier: *"se il computer è all'interno della nostra rete abbiamo tutti i mezzi per proteggerlo. In un modello come quello del cloud computing, non possiamo fare altro che fidarci di chi ci offre il servizio, perché non abbiamo altra possibilità di controllo".*

WEB 2.0 PER SENSIBILIZZARE ALLA SICUREZZA INFORMATICA

Una delle migliori difese utili alla sicurezza informatica consiste nel creare comportamenti virtuosi delle persone.

Le opportunità di interazione del web 2.0 sono utili anche per sensibilizzare le persone alle problematiche della sicurezza.

Nel link seguente http://sicurezza626lavoro.wordpress.com/2010/01/27/web-2-0-e-sicurezza-sul-lavoro/ possiamo leggere un blog dedicato ai problemi della sicurezza del lavoro, un ambito diverso dall'infomatica ma utile per avere delle idee. Peraltro la costruzione tramite wiki di questo documento è un altro esempio. In merito ai social network, si può pensare alla creazione di gruppi di persone interessate all'argomento per fornire idee e aggiornamenti.

WEB 2.0 PER LA PUBBLICA AMMINISTRAZIONE

Secondo l'enciclopedia Wikipedia in diritto il termine amministrazione pubblica (o pubblica amministrazione denotata anche con la sigla PA) ha un duplice significato:

- in senso oggettivo è una funzione pubblica (funzione amministrativa), consistente nell'attività volta alla cura degli interessi della collettività (interessi pubblici), predeterminati in sede di indirizzo politico;
- in senso soggettivo è l'insieme dei soggetti che esercitano tale funzione.

L'aggettivo "pubblica" che qualifica il termine amministrazione fa capire che quest'ultimo ha un significato più ampio: qualsiasi persona o ente svolge attività volta alla cura dei propri interessi privati o di quelli della collettività di riferimento.

Le applicazioni Web 2.0 per la pubblica amministrazione sono interessanti su vari fronti tra cui:

- fare crescere la partecipazione politica dei cittadini;
- fornire strumenti semplici ai cittadini con cui contribuire al miglioramento dei servizi;
- creare relazioni aperte e trasparenti tra cittadini e amministrazione;
- costruire un'amministrazione più semplice e interconnessa tramite software a basso costo.

L'importante è considerare il Web 2.0 come una parte di un progetto ampio di e-governance stando bene attenti alle problematiche di violazione della privacy e alla scarsa qualità dei servizi offerti.

L'e-government tramite il Web 2.0 è strategico per raggiungere la modernizzazione del servizio pubblico verso l'utente in termini di:

- semplificazione delle procedure;
- orientare l'utente nella scelta e nell'uso dei servizi;
- i cittadini collaborano per fornire nuovi servizi;
- i cittadini criticano il funzionamento dei servizi;
- trasparenza degli atti amministrativi;
- servizi più usabili.

E verso i funzionari pubblici in termini di:

- integrazione, efficienza e innovazione;
- collaborazione interistituzionale;
- knowledge management tramite social bookmark, RSS, blog;
- gestione risorse umane;
- aggiornamento.

Un documento di David Osimo con alcuni casi di studio in lingua inglese è disponibile qui.

VULNERABILITÀ DEL WEB 2.0

Una vulnerabilità è un punto debole di un sistema informatico che potrebbe essere usato per creare problemi di sicurezza informatica al sistema.

Spesso nascono da una programmazione superficiale e negligente che non tiene conto delle possibilità di un attacco alla sicurezza.

La sicurezza applicativa identifica le problematiche della sicurezza delle applicazioni web.

Le soluzioni tradizionali di sicurezza informatica non sono adeguate a questa problematica perché:

- Firewalls e antivirus non possono bloccare tutti gli eventuali attacchi al livello applicativo poiché la porta 80 deve essere disponibile per essere utilizzata;
- gli strumenti di scansione della rete non identificano le vulnerabilità a livello applicativo;
- gli sviluppatori di applicazioni Web non hanno conoscenze adeguate di sicurezza applicativa.

Diventa necessario pensare la sicurezza durante l'intero ciclo di sviluppo delle applicazioni, in modo che lo sviluppo degli aspetti di sicurezza venga pienamente integrato nel ciclo di vita delle applicazioni.

Oltre alle vulnerabilità tipiche del Web come SQL Injection, nuove vulnerabilità nelle applicazioni per il Web 2.0 nascono dall'uso di framework con alta interazione client/server basati su XML.

IBM rende disponibili su www.ibm.com/security/xforce i risultati del suo rapporto annuale IBM X-Force Trend and Risk per il 2009 sulle minacce più diffuse, quali il phishing e le vulnerabilità relative ai documenti digitali.

Nelle aziende moderne il confine tra pubblico e privato è reso sempre più sottile grazie all'uso del Web 2.0, specialmente con l'arrivo dei giovani dipendenti che si aspettano di poter accedere dal posto di lavoro ai servizi che normalmente usano in casa.
Pertanto, al fine di evitare problemi di sicurezza occorre sviluppare regole di comportamento interne sull'uso del web. Infatti, si possono avere tecnologie in grado di identificare e risolvere i problemi, ma se non ci sono le persone competenti e i processi adeguati allora possono nascere incidenti pericolosi. Tutto questo sta portando alla nascita della cultura aziendale 2.0.

I rischi per la sicurezza dalle applicazioni web 2.0

Le applicazioni Web 2.0 sono spesso caratterizzate dall'avere una forte interazione tra gli utenti, che porta a un conseguente incremento dello scambio di dati tra gli utenti stessi, come accade per i siti di Social Network. Questo fenomeno, sebbene non sia di per sé negativo, richiede una maggiore attenzione ai problemi di sicurezza logica che tra l'altro siamo già abituati ad affrontare nel Web "tradizionale". Infatti, nell'ambito della elevata interazione tra client e server il punto debole della sicurezza consiste nella possibilità di modificare i messaggi scambiati tra client e server al fine di creare pericoli.

Mettendoci nell'ottica dell'azienda che vuole consentire l'accesso al Web 2.0 per i propri utenti, e concentrandoci sulle problematiche di sicurezza che queste scelte possono indurre, ci si può focalizzare su due categorie di problemi:

1) Malware Intrusion - sono 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 eseguiti dall'host interno all'azienda, rischiano di compromettere la sicurezza dell'intera rete. Prendendo spunto da quanto pubblicato nel report dell'ENISA (http://www.enisa.europa.eu/act/res/other-areas/social-networks/security-issues-and-recommendations-for-online-social-networks), risulta che diversi SN non applicano i controlli di sicurezza necessari non solo a garanzia dello stato del SN stesso (es. SAMY Worm), ma a tutela degli utenti connessi (es. attacchi XSS). Va inoltre considerato che il rischio di "insicurezza" viene amplificato dal continuo aumento di informazioni scambiate, rendendo il controllo dei contenuti un fattore sempre più critico e fondamentale alla sicurezza degli utenti e al 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 tipo Malware Intrusion si affrontano "architetturalmente" partendo dal perimetro della rete aziendale, in modo da eliminare all'ingresso eventuali malware veicolati attraverso la connessione al SN. Tipicamente i sistemi in grado di realizzare questo tipo di filtraggio sono:

- Network Intrusion Prevention;
- Network Antivirus;
- Url Content filtering;
- Mail content inspection.

Fino alle tecnologie di protezione degli host tipo:

- Host Antivirus;
- Host Intrusion Prevention.

La minaccia tipo Data Extrusion o Data Leakage, al contrario del Malware Intrusion, deve essere affrontata cercando di applicare i controlli di sicurezza il più vicino possibile ai dati, tipicamente sulle macchine degli utenti:

- Endpoint Data Loss Prevention

o, dove questo non fosse possibile, analizzando i flussi di trafico direttamente sulla rete:

- Network Data Loss Prevention per intercettare e bloccare le informazioni confidenziali che vengono pubblicate sul SN o su altre applicazioni web.

Web content filtering significa fare il filtraggio dei contenuti per controllare il traffico generato dai social network.

Alcune linee guida per realizzare applicazioni web sicure:

- controllo delle operazioni di autenticazione dell'utente, aggiornamento delle politiche di autorizzazione alle risorse, verifica della robustezza delle password;
- riduzione delle superfici esposte all'attacco, tramite un elenco chiaro ed esaustivo delle componenti logiche e strutturali dell'applicazione e delle divisioni con relative interfacce, eliminazione di componenti inutili ma potenzialmente dannosi, riduzione della possibilità di manipolazione dell'input durante il passaggio tra le varie componenti
- struttura dell'applicazione con componenti e ogni componente deve essere blindato per non offrire risorse ai maleintenzionati;
- controllo dei privilegi permessi all'utente per l'accesso alle funzioni dei componenti;
- controllo degli input provenienti dall'utente prima di eseguirli, sia input espliciti tramite form sia impliciti come gli header Http e altri dati provenienti dai server;
- scrittura attenta dei messaggi di errore per non mostrare informazioni in grado di far scoprire struttura e comportamenti dei componenti sensibili;
- costante aggiornamento dei sistemi;
- gestione della sessione utente, apertura mantenimento e chiusura per evitare furti degli id sessione e la contemporanea presenza dello stesso utente in più sessioni differenti;
- gestione dei file log dell'applicazione per il tracciamento delle sessioni, del comportamento dell'utente e della comunicazione tra le componenti;
- creazione di un sistema di avviso in caso di condizioni anomali;
- difesa da denial of service.

Nei prossimi paragrafi verranno affrontate le principali vulnerabilità da tenere presente durante lo sviluppo di un'applicazione.

WEB 2.0 VERSUS WEB 3.0

L'Università di Berkley ha recentemente calcolato che tra il 1970 e il 2000 (un arco temporale di 30 anni) è stata prodotta la stessa quantità di informazioni che è stata generata dalla preistoria ad oggi, grazie soprattutto al web.

Il Web con 1 miliardo e 200 mila siti, 60 milioni di log, 1,6 milioni di post (messaggi) multimediali prodotti ogni giorno, (solo in Italia sono presenti circa 300 mila Blog) cresce esponenzialmente.

Il Web 2.0 è per alcuni una nuova visione di Internet che sta influenzando il modo di lavorare, interagire, comunicare nella Rete, per altri una evoluzione di Internet.

Una rivoluzione silenziosa che consentirà un insieme di approcci innovativi nell'uso della rete, dati indipendenti dall'autore che viaggiano liberamente tra un blog e un'altro subendo trasformazioni e arricchimenti multimediali, di passaggio in passaggio, tramite la condivisione di **e-comunità**, l'idea che si approfondisce sempre più con la possibilità di diventare popolare, o esplodere in forme virali (ideavirus).

Le informazioni diventano opensource condivisibili, o IPinformation come preferiscono chiamarle altri, che nagivano liberamente nel **nuovo Web**.

La rete ha trasformato ogni business in un business globale e ogni consumatore in un consumatore globale, la società verso una società della conoscenza, e l'economia verso un'economia digitale, la **wiki economia**, la collaborazione di "massa" in favore del vantaggio competitivo.

Il Web 2.0 è anche un nuovo modo di elaborare le informazioni basato su tecnologie "less is more" (tecnologie di facile apprendimento, uso e accessibilità). La condivisione e l'accesso alle informazioni ormai riguarda tutti, tutti potenzialmente possono diventare produttori di informazioni e di idee.

La società del futuro sarà digitale, mutevole, interattiva, basta osservare la notevole esplosione di nuovi media comunicativi. All'interno di ciò sta crescendo anche il netwoking Aziendale, le Reti aziendali.

Web 2.0 (connect people). Gli scettici del Web 2.0 e della conoscenza condivisa in generale puntano il dito sulla autorevolezza e sulla validità dei contenuti **user-generated**. La mancanza di un filtro preventivo sulle informazioni generate dagli utenti, come avviene invece nel mainstream, potrebbe essere considerato un punto debole del Web 2.0. La diffusione molecolare dell'informazione è resa possibile con terminali portatili connessi alla rete, infatti gli utenti (potenziali "gateway umani"), possono usufruire di una pluralità di dispositivi intelligenti, integrati nei più svariati tipi terminali mobili capaci di riconoscere e rispondere ininterrottamente in modo discreto e invisibile, ciò che va sotto il nome di **tecnologia enable**, abilitante. Nonostante la rivoluzione dal basso, del cliente-utente, fatta con gli strumenti del Web 2.0 interattivi e collaborativi, solo una ristretta élite determina i contenuti nel grande panorama del Web, è la **regola dell'1%** (su 100 utenti web solo 1% di essi è attivo nel produrre informazione,contenuti).

Tuttavia l'autorevolezza dei contenuti può autogenerarsi tramite una selezione dei contenuti stessi attraverso meccanismi di social network insiti nella rete stessa, al di là dei numero dei link e click per post pagina. Il concetto di **conoscenza condivisa** come creazione e diffusione di contenuti sembra stridere con la formazione culturale ed individuale a cui siamo stati abituati, e mi riferisco al mondo del lavoro, della formazione, dell'università. Servirebbe un'evoluzione verso modalità digitali di pensiero più consona a quella delle nuove generazioni- utenti (**digital natives**). Esistono poi anche i digital explorers, coloro cioè chi vanno per necessità nella cultura digitale per cercare ciò che può servire a raggiungere scopi che non siano fini alla cultura digitale stessa. Spesso viene a crearsi così un **gap**, da una parte i geeks (digital natives), dall'altra i dummies (digital immigrants) che faticano a relazionarsi e comunicare anche al di là dello spazio virtuale, nel mezzo un'ampio spazio per i "gestori

dell'interazione" sociale e comunicativa tra i due gruppi.

Versus WEB 3.0 (connect infomation) *"Una delle migliori cose sul web è che ci sono tante cose differenti per tante persone differenti. Il Web Semantico che sta per venire moltiplicherà questa versatilità per mille...il fine ultimo del Web è di supportare e migliorare la nostra esistenza reticolare nel mondo". (Tim Berners Lee).*

Dopo l'invenzione del linguaggio **xml** (eXtensible Markup Language, metalinguaggio utile allo scambio dei dati) impiegato in diverse applicazioni Web 2.0, ora gli sforzi di ricerca si stanno concentrando nel suo impiego in **tecnologie semantiche**. Generalmente la ricerca di una parola sui motori di ricerca attuali, non contestualizzata, può generare un **overload** di risultati e quindi un eccesso di risposte inutili. Per ovviare in parte a tale effetto viene in soccorso la "tecnologia semantica" che dà rilevanza al significato reale dei termini e considera il contesto in cui sono inseriti, consentendo una ricerca più precisa e riducendo le risposte ridondanti. Si tratta di una visione completamente nuova nel web, basata sul concetto che ognuno,ogni creatore di contenuti può determinare una propria ontologia delle informazioni. A tal fine vengono impiegati sistemi di OSM (Ontology Systems Management) che possono utilizzare diversi linguaggi standard, come l'RDF (Resource Description Framework) o l'OWL (Web Ontology Language) che consententono nuovi costrutti. Con OWL è possibile scrivere delle ontologie che descrivono la conoscenza che abbiamo di un certo dominio, tramite classi, relazioni fra classi e individui appartenenti a classi. Con il Web 2.0 e i Social Network abbiamo pensato che fosse arrivato il futuro ora sappiamo che sono solo il presente, nel futuro c'è il Web Semantico, il **Web 3.0**

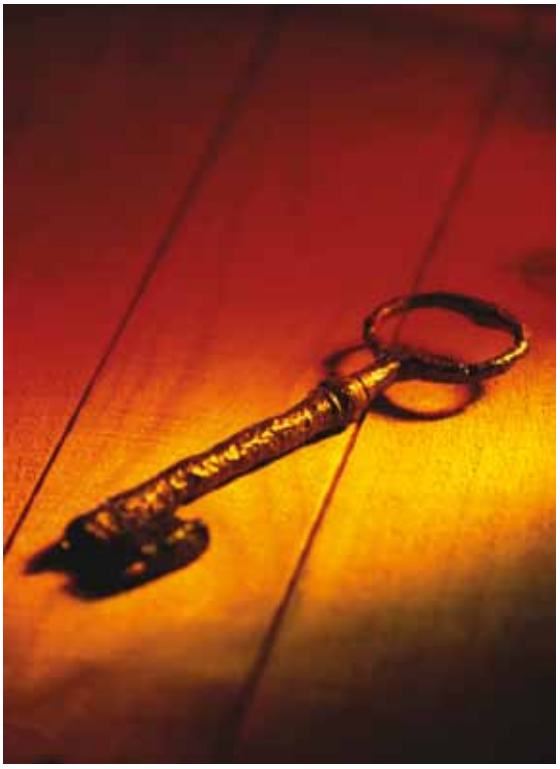
PRIVACY 2.0

Gli obiettivi degli hacker in ambito Web 2.0 non sono più le reti di computer ma le informazioni e le proprietà intellettuali memorizzate nel web. Pertanto non sono più sufficienti i classici mezzi di difesa. Il termine privacy 2.0 intende delineare un nuovo approccio alla gestione della privacy adeguato al Web 2.0.
Coinvolge il furto di identità nei social network, la consapevolezza ed il diritto all'oblio, e la definizione stessa di social network. Tanti argomenti, tanti aspetti legati alla privacy diversi ma che si sovrappongono in più punti formando una sorta di grafo multidimensionale che assume delle connotazioni diverse in base al punto di osservazione.
Sembra strano parlare e soprattutto esigere un certo grado di privacy in un ambiente 2.0 legato sempre più alle reti sociali ed alla condivisione. La questione viene spesso semplicisticamente etichettata come un falso problema: *"se voglio mantenere la mia privacy non mi registro ad un social network"*. Posizione esasperata infruttuosa: deve esistere una soluzione mediatrice che passa dalla consapevolezza del mezzo, del suo utilizzo reale e potenziale.
Sebbene da un punto di vista statistico la platea di utenti dei social network non è così giovane come si potrebbe pensare, è opportuno vedere il fenomeno da una prospettiva diversa.
Consapevolezza.
Quanti di noi, utilizzatori ad esempio di Facebook, hanno verificato le impostazioni della privacy? Quanti hanno letto i termini di accettazione del servizio in fase di registrazione? Quanti hanno monitorato i loro cambiamenti?
Quanti hanno realmente la percezione di cosa sia il datamining, il behavioral advertising, profilazione massiva? Quanti si sono interrogati sulla "*gratuità*" di Facebook? Quanti sanno dove vanno a finire i propri dati?
Certo, quello che noi intendiamo fornire, non necessariamente dati reali.

Facebook in particolare è il primo strumento di profilazione massiva, volontaria e comportamentale destinata a creare la base dati privata del settore più dettagliata e completa mai vista.

Definizione contestuale di social network ed osservazioni

A valle delle considerazioni ed al contesto delineato risulta più semplice riuscire a definire cos'è un social network.
Una rete di informazioni condivise o, in sintesi, identità digitali condivise.
Si completano, si intrecciano, si sovrappongono ma costituiscono parte di un "io digitale" multidimensionale che trae origine dalla curiosità del nuovo strumento tecnologico e dalla possibilità, per certi versi, di avere meno barriere dell'"io reale" in cui troppo spesso non si può essere apertamente sè stessi.
In questo scenario, è ancora possibile parlare di furto di identità quando le informazioni oggetto di "furto" sono state rese dalla "vittima" stessa più o meno consapevolmente?
È più corretto parlare di "appropriazione" di identità?
C'è una profonda e determinante differenza che andrebbe valutata e normata di conseguenza.



Privacy 2.0: nuove generazioni, nuove responsabilità

Demonizzare non serve, occorre invece essere consapevoli e responsabili soprattutto verso le nuove generazioni.
Queste ultime sono nate e cresciute in cui è "*normale*" usare certi mezzi e vengono usati con la leggerezza e l'ingenuità propria della loro età.
È giusto che sia così: non devono essere le nuove generazioni a crescere troppo in fretta perché noi diamo loro a disposizione dei mezzi potenzialmente pericolosi.
Piuttosto, abbiamo noi il dovere di essere al loro fianco ed indicare loro un uso responsabile, attento e consapevole.
Le attenzioni e la prudenza non sono mai troppe visto che, in rete più che nella vita privata, non esiste il concetto di diritto all'oblio.
Non è fantascienza ipotizzare di essere scartati ad un colloquio di lavoro perché, anni prima, avete pubblicato bravate di cui, anche volendo, non avete sempre la possibilità o le competenze per una totale e definitiva rimozione.
La rete va verso il Web semantico, verso il Web 3.0 e sempre più ricorda, copia, clona, veicola, salva, archivia anche a nostra insaputa per innumerevoli motivi e tecnicismi.
Noi esperti di sicurezza, di comunicazione online, noi con il "doppio cappello" lo sappiamo bene e abbiamo il dovere di alzare la mano per porre la questione all'attenzione di tutti.
La condivisione e la consapevolezza sono le strade da seguire per contestualizzare ed affrontare responsabilmente la problematica Privacy 2.0 veicolando anche attraverso lo stesso Web 2.0 messaggi chiari, casi di studio ed esempi concreti di approcci e scenari che ne possono scaturire.

VIRUS INSERITI NELLA STRUTTURA DEI SITI

Anche siti popolari e importanti possono nascondere malware e sistemi per il reindirizzamento del navigatore dal sito desiderato verso siti pericolosi e inaffidabili. Occorrono prodotti in grado di classificare in tempo reale gli indirizzi dei siti per capire se i contenuti sono pericolosi.

PHISHING

Il phishing è una truffa mirata al furto di identità e di dati sensibili come password, numero carta credito ecc. La truffa si esegue tramite email false, ma anche contatti telefonici, che riproducono l'apparenza grafica dei siti di banche, poste, ecc.
L'utente riceve un invito a scrivere le proprie credenziali per difendersi da virus, eseguire aggiornamenti ecc. ma in realtà viene indirizzato verso un sito in grado di rubare le informazioni riservate e usarle subito per derubare le persone.
Si tratta purtroppo di un fenomeno in continua crescita e in costante aggiornamento, per cui si manifesta in forme sempre diverse.
All'inizio queste email contenevano grossi errori di italiano che li rendevano facilmente individuabili, adesso sono sempre più corrette e sofisticate e vale la regola d'oro del non cliccare sui link nell'email ma andare direttamente all'indirizzo del sito che ben conosciamo.
Per informazioni http://it.wikipedia.org/wiki/Phishing e il portale Anti-Phishing Italia su www.anti-phishing.it/
Anche i servizi offerti tramite il Web 2.0 sono colpiti da questo fenomeno con varie modalità.
Nel primo modo si riceve una email fasulla con l'apparenza grafica delle classiche email che riceviamo da parte del gestore del servizio web. L'email contiene, per esempio, una foto di una persona e un nominativo richiedente un contatto sul social network.
Cliccando sul link si viene rediretti verso un sito con l'apparenza simile a quella del social network, ma in realtà è depositato su un altro server e creato apposta per rubare login e password da rivendere al mercato nero.
Un'altra modalità consiste nell'invio di email con avvisi del cambiamento di password per motivi di sicurezza e invitando a aprire un file per ottenere la nuova password. Il file allegato è in realtà un virus in grado di creare danni.
Leggere il campo mittente di queste email non è spesso di grande aiuto, poiché viene abilmente falsificato mostrando i dati corrispondenti al servizio reale. Un rimedio consiste nel non cliccare sui link allegati ma andare direttamente al sito scrivendone l'indirizzo che ben conosciamo.
Conviene inoltre iscriversi a servizi di aggiornamento sulle vulnerabilità del servizio interessante, per essere aggiornati sulle nuove modalità di attacco e difesa.

VULNERABILITÀ DI AJAX

Ajax è una sigla nata dall'unione di Asynchronous JavaScript e XML con cui si denota una tecnologia web in grado di fornire un aggiornamento asincrono all'applicazione web. In tal modo la trasmissione di dati tra client e server avviene secondo specifiche zone della pagina senza dover ricaricare tutta la pagina, ovvero l'utente avrà sempre una pagina con i contenuti aggiornati senza dover fare operazioni per ricaricare la pagina.

Alcune vulnerabilità di AJAX sono:
- esecuzione di codice dannoso in grado di sostituire i cookie quando il browser effettua una chiamata con AJAX;
- altre forme di cross-site scripting;
- si può evitare i controlli AJAX per fare richieste POST o GET dirette, però si espone l'applicazione ai pericoli.

Le Rich Internet Application (RIA) permettono un'esperienza di navigazione più ricca anche grazie all'inserimento di oggetti creati con Adobe Flash, controlli ActiveX o Applet. Questi oggetti sono scaricati sul client in formato binario ed esistono software per decompilarli e modificarli, con tali operazioni si potrebbe iniettare un oggetto pericoloso nel client superando tutti i controlli.

VULNERABILITÀ DI RSS

Grazie alle vulnerabilità Atom injection di RSS, un attaccante può mandare ("iniettare") nel flusso di notizie del codice scritto in JavaScript per compiere azioni dannose senza che il sistema di lettura RSS se ne accorga.

VULNERABILITÀ DI TIPO CROSS SITE SCRIPTING

L'acronimo XSS (*Cross Site Scripting*) identifica una vulnerabilità di sicurezza che interessa in modo specifico i siti di tipo dinamico afferenti al Web di seconda generazione (*Web 2.0*).

Gli attacchi Cross-site scripting sono costruiti usando software scritto con linguaggi di scripting, principalmente JavaScript, che partono dal sito web e attaccano il client dell'utente.
Tale software è eseguito sulla macchina dell'utente vittima dell'attacco e potrebbe aprire le porte ad altri attacchi.

Il software può essere depositato anche in un sito web non potenzialmente pericoloso ma vulnerabile alla manipolazione della struttura del sito da parte di persone non autorizzate.

Come in molti altri casi, gli *exploit* **XSS** basano il loro funzionamento sulle possibilità offerte dal codice con il quale sono state realizzate le applicazioni pensate per il *Web*: cioè su quelle parti di codice sviluppate senza tenere conto di alcune raccomandazioni basilari al fine dell'ottenimento di un sufficiente livello di sicurezza: nella fattispecie si tratta di una insufficiente attenzione nelle procedure deputate al controllo delle operazioni di tipo **POST** e **GET**, durante l'impiego del protocollo **HTTP** (*Hypertext Transfer Protocol*). Pertanto questa vulnerabilità è creata dalla mancanza di codifica (encoding) delle entità HTML e dalle elaborazioni eseguite senza fare controlli preventivi su cosa c'è scritto.

Gli exploit basati sul "*Cross Site Scripting*" permettono agli aggressori di alterare (in modo permanente o momentaneo) i contenuti della pagina *Web* da loro visualizzata, operazione che si presta a numerose e pericolose applicazioni come, ad esempio, la realizzazione di una pagina pensata "*ad hoc*" per carpire informazioni sensibili agli utenti che, successivamente, accederanno a quell'area del sito, realizzando "*de facto*" un vero e proprio *Phishing* (tecniche di inganno degli utenti che inducono a comunicare dati riservati) basato sulle risorse e la credibilità dell'inconsapevole (e legittimo) fornitore del servizio preso di mira.

Come prima anticipato, gli exploit basati su **XSS** possono essere fondamentalmente di due tipi, *permanenti e non permanenti*: nel primo caso le pagine prese di mira vengono permanentemente modificate dall'aggressore, mentre nel secondo le alterazioni sono soltanto momentanee e interessano, più che l'intero contenuto della pagina, soltanto il traffico relativo alle richieste **POST**/**GET** del protocollo **HTTP** (operando un opportuno reindirizzamento di queste richieste).

Un'altra classificazione delle tecniche principali:

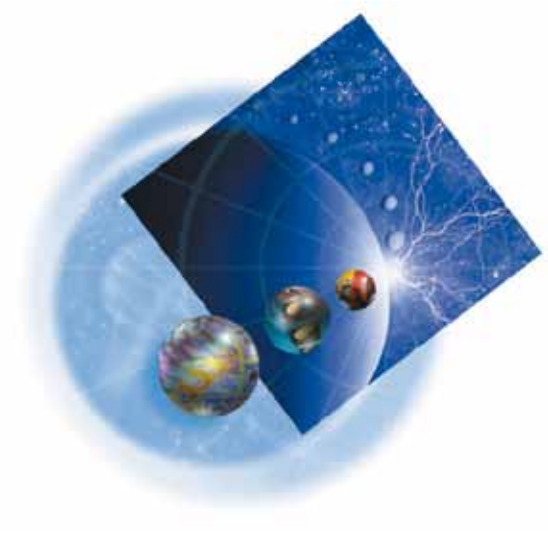
- **stored**: il client invia dati all'applicazione web, vengono memorizzati e rispediti agli altri utenti tramite le pagine dell'applicazione;
- **reflective**: il client web invia dati all'applicazione web, che vengono subito usati da script sul server e rispediti al browser;
- **DOM**: nella pagina web è stato inserito uno script in grado di accedere ai parametri nella URL request e li utilizza per generare codice HTML nella stessa pagina.

Gli effetti di un attacco del genere, ovviamente, sono direttamente proporzionali al numero di utenti che abitualmente visita il sito preso di mira e alla credibilità che questo riscuote tra questi ultimi: nel caso di siti a elevato volume di traffico come, ad esempio, un sito di "Social Network" o di "Home Banking", i rischi (e i danni concreti) verso cui si va incontro saranno certamente di notevole entità.

Le contromisure in questi casi, come già anticipato in precedenza, consistono nel verificare efficientemente quanto inserito dagli utenti nei campi editabili (campi di ricerca, di login e similari), facendo in modo che nessun contenuto attivo (come ad esempio uno script) possa essere mandato arbitrariamente in esecuzione.

Per esempio, nei sistemi di gestione dei blog è opportuno controllare cosa scrive l'utente al fine di rimuovere tag HTML e JavaScript non permessi.

Dato che non si tratta di problematiche di sicurezza nuove - basti infatti pensare ai vetusti attacchi di tipo "*SQL Injection*" che sfruttano un meccanismo simile (il mancato controllo di quanto inserito dagli utenti) - si può dedurre come, nonostante il tempo trascorso, la mole di informazioni disponibile e i gravi problemi verso i quali si va incontro, la cultura della sicurezza non prevalga ancora su quella dell'improvvisazione, con effetti deleteri e imprevedibili per l'intera comunità.



VULNERABILITÀ DI LINK INJECTION

Il Link Injection costituisce una delle vulnerabilità più pericolose per il sistema di blog WordPress. Nell'ambito del sistema di statistica degli accessi, il referer indica da quale url gli utenti sono giunti nel blog ed è molto utile per capire se i post sono stati linkati dall'esterno e per sapere cosa si dice in merito al contenuto del post.

Il primo tipo di vulnerabilità riguarda la possibilità di modificare il campo referer dell'header HTTP per inserire un link nella pagina di amministrazione del blog. Inoltre, il gestore del blog nota un traffico crescente di visite proveniente dal link inserito, potrebbe essere curioso di conoscere l'autore dei commenti ai suoi post e va a visitare il link inserito ritrovandosi in un sito potenzialmente pericoloso.

Il secondo tipo di vulnerabilità è costituita dalla possibilità di inserire codice Javascript e fare Cross Site Scripting nel riepilogo statistico, poiché viene stampato un input generato da un utente esterno.

VULNERABILITÀ DI DENIAL OF SERVICE

Il Denial of Service è un attacco denominato anche negazione del servizio perché interrompe la disponibilità di un servizio rendendolo inaccessibile ai legittimi utilizzatori. Nell'ambito delle applicazioni web consiste nell'interruzione dannosa di un'applicazione.

Viene causata con:

- comandi sql per attaccare un database;
- loop di richieste continue verso una risorsa e relativo crollo;
- gli account degli utenti vengono bloccati e messi fuori uso;
- spedizione di quantità di input tanto grandi da non poter essere gestiti e relativo crollo.

VULNERABILITA' DI SQL INJECTION

Le informazioni inserite dall'utente non vengono controllate e vengono inserite all'interno delle istruzioni SQL per costruire la query, dando possibilità all'utente di manipolare le query di accesso ai database in SQL. Ad esempio nel caso di informazioni da inserire nei campi login e password per entrare in un servizio, invece dei dati identificativi vengono inserite stringhe come 'or 1=1 -- invece dei valori previsti e si ottiene l'ingresso poiché la condizione inserita è sempre verificata.

SICUREZZA PROATTIVA NEL WEB DI SECONDA GENERAZIONE

Seppure certamente rivoluzionario nelle caratteristiche, il Web di seconda generazione, oggi sinteticamente definito Web 2.0, condivide numerosi aspetti con la precedente infrastruttura di prima generazione, costituendone, di fatto, una naturale e inevitabile evoluzione.

Mettendo da parte ogni più o meno sofisticata tecnica "*ad hoc*" adoperata per garantire la sicurezza in ambito *Web*, come in ogni branca ICT (*Information e Communication Technology*) esposta a rischi dal lato sicurezza, ritengo necessario effettuare un doveroso richiamo su quelle attività preliminari che costituiscono le fondamenta sulle quali si andranno poi a innestare tutti i dispositivi di sicurezza attivi: mi riferisco alle attività di tipo proattivo, cioè quelle operazioni volte a prevenire, più che fronteggiare, i potenziali problemi di sicurezza.

Riguardo al *Web 2.0*, numerosi studi di settore non hanno evidenziato particolari problemi di sicurezza esclusivamente riconducibili alle nuove tecnologie introdotte con il *Web* di seconda generazione, considerando l'avvento di questo nuovo scenario come un inevitabile sviluppo del precedente ambiente (*Web 1.0*) e come tale, quindi, gestibile con lo stesso approccio proattivo utilizzato fino a oggi.

Questo non si configura assolutamente come un invito ad abbassare la guardia, in quanto l'introduzione delle nuove tecnologie, come avviene in ogni rivoluzione in questo campo che comporta ripercussioni nell'ambito della sicurezza (come è accaduto, ad esempio, con l'avvento delle tecnologie *wireless*), deve far considerare ogni innovazione una serie di pericoli di tipo "*zero day*", a causa delle poche informazioni che caratterizzano gli elementi di nuova introduzione e, quindi, consigliare una maggiore attenzione nelle attività di definizione delle politiche di sicurezza da adoperare e/o nella modifica di quelle esistenti.

Exploit già noti come, ad esempio, il "*Cross Site Scripting*" (XSS) o il "*Cross Site Request Forgery*" (CSRF), espressamente pensati per le vulnerabilità tipiche dell'ambiente dinamico che caratterizza il *Web* di seconda generazione, possono essere contrastati efficacemente con lo stesso "*buon senso*" che necessitava in precedenza, intendendo per "*buon senso*" un efficiente connubio tra informazioni aggiornate e (conseguente) adeguamento dei sistemi di protezione in uso.

Questo tipo di approccio, che ho definito "*proattivo*", non è infatti legato a uno specifico dispositivo di sicurezza bensì a una "*forma mentis*" che oggi come non mai risulta sempre più vincente e indispensabile in ambito sicurezza: non dimentichiamo che al *Web 2.0* seguirà certamente un *Web 3.0, 4.0*, ecc. Questo impone un approccio mentale regolato da principi omnicomprensivi, svincolati da una specifica tecnologia o ambiente.

Il cattivo comportamento degli utenti, sia quelli che operano come fruitori di servizi, sia quelli che, invece, gestiscono questi ultimi, è sempre ai primi posti nella scala delle cause che consentono la buona riuscita di un attacco informatico: basti pensare che anche nel nuovo *Web 2.0*, tecniche come il "*Phishing*", più vicine all'ingegneria sociale (*Social Engineering*) piuttosto che allo sfruttamento di una vulnerabilità oggettiva dei sistemi, sono quelle che hanno creato (e creano) i danni più ingenti alle aziende e ai singoli individui.

In una immaginaria bilancia che vede posto su un piatto il peso dell'ormai abusata (ma sempre attuale) considerazione che "*solo una macchina spenta può essere considerata sicura*" e nell'altro il carico derivante dalla necessità di fruire in modo sicuro delle opportunità offerte da un settore in continua evoluzione, è ancora una volta l'atteggiamento proattivo fornito dal "*buon senso*" l'elemento discriminante capace di far pendere l'ago della bilancia da una parte o dall'altra.

APPROCCIO EURISTICO NELLA SICUREZZA NEL WEB SEMANTICO

Il difficoltoso compito di proteggere i sistemi informatici dalle minacce che regolarmente li insidiano è oggi reso più gravoso dagli schemi di funzionamento semantici che caratterizzano gli scenari afferenti alle applicazioni Web di seconda generazione.

La relativa facilità con la quale fino a qualche tempo addietro gli "*addetti ai lavori*" erano in grado di far fronte alle potenziali vulnerabilità dei sistemi informatici ha oggi lasciato il passo alla difficoltà di tenere testa a tutta una serie di nuove problematiche legate all'approccio semantico tipico dei servizi e delle applicazioni utente nell'ambito del Web 2.0.

Questo si verifica, *in primis*, a causa dell'impossibilità di porre in essere, come avveniva in passato, degli efficaci dispositivi di protezione automatica, in quanto, le peculiarità dell'ambiente rendono spesso impossibile discernere tra gli usi legittimi e illegittimi delle risorse.

La grande capacità di comunicazione e interazione con gli utenti offerte dal Web 2.0, oltre a creare nuovi pericoli da fronteggiare, amplifica in modo preoccupante alcune delle problematiche di sicurezza già note in precedenza come, ad esempio, quelle afferenti alle tecniche di phishing.

Per poter adeguatamente fronteggiare tale situazione, anche i dispositivi di protezione dovrebbero essere in grado di operare secondo la stessa logica semantica che caratterizza le nuove applicazioni e questo, almeno allo stato attuale, appare molto difficoltoso e per certi versi addirittura impossibile a causa dell'elevato numero dei fattori in gioco e per l'estemporaneità che caratterizza questi ultimi.

In un simile scenario un approccio alla sicurezza di tipo proattivo assurge come una delle poche carte vincenti, sottolinenando con questo l'efficacia di un "*modus operandi*" preventivo rispetto a uno "*in itinere*" o, peggio, successivo agli eventi: studio dei comportamenti sospetti mediante sistemi IDS (Intrusion Detection System) e applicazioni "esca" implementate su sistemi virtuali di tipo *honeypots/honeynets* rappresentano alcuni efficaci strumenti per realizzare un'infrastruttura di sicurezza proattiva capace di scongiurare, o perlomeno ridurre drasticamente, i potenziali rischi in ambito produttivo.

L'atipicità nel funzionamento delle applicazioni pensate per il Web 2.0, rispetto gli applicativi similari della precedente generazione, rende inefficaci molti exploit automatizzati un tempo utilizzati con successo dagli aggressori ma, parallelamente, amplifica l'efficacia di altre tecniche di attacco come, ad esempio, quelle legate all'ingegneria sociale (social engineering).

Quest'ultima è la ragione per la quale diminuisce l'efficienza degli strumenti di difesa automatici (come, ad esempio, i firewall) un tempo impiegati a vantaggio di quelli di analisi passiva (studio a posteriori dei file di log) e/o attiva (studio in tempo reale dei log e intervento contestuale sulla base di comportamenti/eventi noti).

Concludendo, a differenza di qualche tempo addietro, dove una buona sicurezza dei sistemi di produzione (hardening) poteva essere raggiunta in modo relativamente semplice, secondo degli schemi ben noti e consolidati (basti pensare alle capacità di "*stateful inspection*" nei dispositivi di protezione perimetrale o alla sicurezza del codice nel contrastare gli attacchi basati su "*SQL Injection*"), oggi i vecchi metodi devono essere necessariamente integrati con metodologie preventive capaci di operare in modo euristico senza sottostare ad alcun vincolo staticamente predefinito.

LINEE GUIDA PER REALIZZARE LA SICUREZZA 2.0

Passiamo a indicare alcune raccolte di suggerimenti per creare sistemi per il web 2.0 con una maggiore sicurezza.
Si parla in particolare di sicurezza applicativa come processo continuo con competenze specifiche.
L'importante è che lo sviluppatore deve fare studi specifici per questo tipo di sicurezza e deve pensare la sicurezza nel ciclo di vita del software.

Fattori da considerare:

- definire con precisione le porte ed i protocolli utilizzati dall'applicazione, per costruire un perimetro intorno e ridurre la superficie esposta agli attacchi;
- crittografia e protezione dei dati;
- proteggere i cookie di autenticazione di sessione tramite l'utilizzo del protocollo TLS o cifrandone il contenuto;
- controllare l'input e anche l'output per controllare la rispondenza con quanto previsto per l'applicazione;
- registrare nei log i seguenti eventi:
  a. autenticazione applicativa (login e logout, riusciti e non);
  b. accesso ai dati (lettura e scrittura);
  c. modifica di funzioni amministrative (per es. la disabilitazione delle funzioni di logging, la gestione dei permessi, ecc.);
- all'interno di una voce del file log occorre registrare le seguenti informazioni:
  a. data/ora dell'evento;
  b. luogo dell'evento (per es. macchina, indirizzo IP, ecc.);
  c. identificativo dell'entità che ha generato l'evento (per es. utente, servizio, processo, ecc.);
  d. descrizione dell'evento;
- prevedere meccanismi di conservazione dei log in file su cui sia possibile effettuare esclusivamente la scrittura incrementale o su supporti non riscrivibili;
- prevedere meccanismi di backup dei log;
- prevedere meccanismi di controllo degli accessi ai log.

In generale, il miglior modo per costruire un sistema sicuro consiste nell'inserire una logica di sicurezza fin dai primi passi della progettazione del sistema. In particolare, in un'applicazione web bisogna seguire un approccio di separazione dei livelli logici in grado di garantire:

- compartimentazione, per evitare di passare da un livello ad altri senza permesso;
- separazione di privilegi, per evitare di dare troppo spazio di manovra ai possessori dei privilegi;
- modularità del software, per facilitare il ricambio e la creazione delle componenti.

Un'applicazione web rispetta queste linee guida se è composta da questi tre livelli logici ben distinti:

1. livello di presentazione per creare l'interfaccia per la rappresentazione dei dati verso l'utente e la raccolta e controllo dei dati in ingresso messi dall'utente;
2. livello business logic che realizza il cuore dell'elaborazione dati secondo l'obiettivo dell'applicazione, deve essere in grado di rapportarsi con il precedente livello presentazione per ricevere i dati e spedire i risultati finali, oltre che con il successivo livello di accesso ai dati necessari per l'elaborazione;
3. livello di accesso ai dati per dialogare con i database e altri servizi in grado di fornire dati dinamici.

Ciclo di sviluppo del software:

1. analisi Requisiti e Casi utente: documentazione dei requisiti e dei test di sicurezza;
2. pianificazione del software: guida alla progettazioni di applicazioni web sicure, guida all'analisi delle minacce e dei rischi;
3. pianificazione dei test: guida per i testi di sicurezza;

4 scrittura del software: guida per l'analisi del software;
5 fase di test: guida per i test di sicurezza.

Rimedi da attuare:

1. revisione del software manuale o automatico tramite Static Code (analisi del codice senza eseguirlo) e Analysis Tools (software di analisi basati su librerie di vulnerabilità note);
2. Dynamic Analysis per analizzare l'applicazione Web quando è in fase di esecuzione. Nota anche come test Black Box, perché non si ha nessuna conoscenza di come è fatta l'applicazione. Si inizia esplorando l'applicazione per realizzare il modello del sito Web e determinare i vettori di attacco. Si invia una serie di richieste HTTP, si analizzano le risposte e si identificano le vulnerabilità;
3. Penetration Testing Tools per creare test di penetrazione manuale o automatico.

PROGETTI OPEN SOURCE PER LA SICUREZZA DELLE APPLICAZIONI WEB

OWASP è la sigla del progetto Open Web Application Security Project al sito http://www.owasp.org nato con l'obiettivo di creare la specifica cultura della sicurezza applicazioni web verso professionisti e aziende. Per raggiungere tale obiettivo l'OWASP si dedica alla diffusione di documenti riguardanti la definizione dei criteri di progettazione ed analisi del software, alla nascita di nuove idee, alla creazione di casi di studio, oltre che alla creazione di strumenti come le checklist per il vulnerability assessment e procedure per l'analisi del codice.

I documenti e il software prodotti sono gestiti con l'approccio Open Source, secondo cui ogni membro del progetto può avere tutta la conoscenza creata dai progetti e deve poter contribuire allo sviluppo in base alle proprie competenze.

La condivisione delle informazioni e del codice sorgente con un ampio numero di partecipanti in possesso di competenze diverse, tipico dell'approccio Open Source, potrebbe aumentare la qualità dei risultati, permettendo per esempio di trovare errori che ciascuno potrebbe non individuare usando il proprio punto di vista.

La top ten delle vulnerabilità critiche delle applicazioni web è uno dei documenti più noti di OWASP, un altro documento interessante è "OWASP Guide to Building Secure Web Applications".

In merito agli strumenti, WebGoat è un ambiente di insegnamento interattivo della sicurezza web contenente un insieme di vulnerabilità.

RETI 'FIDUCIOSE'

Aver fiducia tra le persone, vuol dire, in un certo senso, essere "sicuri" di quella persona o di quel gruppo di persone. Non cambia molto se applichiamo la stessa definizione ad un gruppo di oggetti informatici. Creare una rete in cui ogni oggetto abbia fiducia dell'altro con un qualche sistema è molto complesso, ma non impossibile. La prima operazione è sicuramente una ricognizione di quelli più deboli (e quindi facilmente attaccabili) e dei luoghi di "interscambio", dove non si ha un pieno controllo dell'oggetto non appartenente (direttamente) alla propria rete. Seguiranno poi tutte quelle fasi che consentono una definizione precisa per ogni componente dei dati che tratterà.
Si prenda come esempio un'infrastruttura di un Ente Pubblico. In questi ultimi anni il trattamento informatico di dati in una P.A. si è evoluto molto, rispetto a quando erano presenti solo sistemi indipendenti (e chiusi). Si è reso sempre più necessario lo scambio di informazioni tra Enti Pubblici di diversa natura sia tra loro che verso Aziende Private. Nel caso in cui due o più amministrazioni pubbliche devono comunicare fra loro, si rende necessario applicare delle regole al pari della comunicazione tra P.A. e Privati.

Tutte queste regole si possono tradurre in protocolli di sicurezza che devono essere utilizzati da tutte le parti in gioco. Un ente deve far interagire parte del suo sistema informativo con un altro, che a sua volta interagisce con un sistema di un'azienda non pubblica:

Ente A	Ente B	Azienda privata
Analisi della propria infrastruttura in vista dell'apertura verso l'esterno	1. Analisi del proprio sistema informativo per pemettere l'accesso dall'esterno 2. Analisi che consenta di esplorare tutte le possibili implicazioni del permettere l'accesso a parte dei propri dati dall'esterno da soggetti terzi (non P.A.)	Adeguamento dei propri sistemi
Definizione delle regole di comunicazione	Definizione delle regole di comunicazione	Definizione delle regole di comunicazione
Livelli di erogazione del servizio	1. Livelli di erogazione del servizio 2. Stesura dei protocolli di non divulgazione	1. Recepire i protocolli di non divulgazione 2. Creare le dovute misure di sicurezza verso il resto della propria infrastruttura informativa
Implementare dei canali sicuri per la comunicazione	Implementare dei canali sicuri per la comunicazione separati verso l'ente A e verso l'azienda privata	Implementare dei canali sicuri per la comunicazione
Test di affidabilità con subset di dati di test	Test di affidabilità con subset di dati di test	Test di affidabilità con subset di dati di test
Valutazione di eventuali eccezioni	Valutazione di eventuali eccezioni	Valutazione di eventuali eccezioni
Rendere operativa la collaborazione monitorando in modo continuo affidabilità e sicurezza	Rendere operativa la collaborazione monitorando in modo continuo affidabilità e sicurezza	Rendere operativa la collaborazione monitorando in modo continuo affidabilità e sicurezza

Come è possibile notare, parecchi punti sono in comune su tutti i fronti. Si supponga che l'azienda privata commetta un errore in fase di analisi che non viene rilevato nella fase di test, il monitoraggio continuo consente la rilevazione immediata del problema e, con le opportune politiche di *incident response*, di risolverlo nel più breve tempo possibile con la collaborazione di tutte le parti.
Le tecniche di analisi unite a delle politiche di sicurezza chiare e applicabili da tutti gli attori coinvolti, consentono di ridurre al minimo la possibilità di perdita e furto di dati o discontinuità del servizio, obiettivo primario di qualsiasi P.A.

Di solito quando si riscontra un problema si parte da quattro domande di base, come al gioco Cluedo:

1. Chi?
2. Dove?
3. Quando?
4. Come?

Ovvero cercare di individuare CHI, interno alla rete o esterno, ha commesso l'errore, DOVE è stato commesso, (ente A?, ente B?, nell'azienda privata?) QUANDO il fattore temporale è molto importante per capire se il problema è dovuto a particolari momenti nell'elaborazione o nella trasmissione dei dati (cronjob che lanciano particolari procedure che non rispettano i protocolli di sicurezza, magari ritenuti sicuri prima della collaborazione con gli altri) ed ultimo, ma non meno importante, il COME è potuto succedere. Non sempre è facile trovare risposte a tutte o parte delle domande, in special modo quando si analizzano sistemi complessi, ma gli strumenti che consentono di prevenire o comunque di limitare al minimo "il danno" ci sono e DEVONO essere utilizzati, in particolar modo dalla Pubblica Amministrazione.

VALUTARE LA SICUREZZA

Valutare la sicurezza significa stabilire un insieme di indici numerici in grado di ottenere una stima quantitativa del ritorno dell'investimento destinato a rafforzare le misure di sicurezza. Stabilire tali indici è molto complesso e vengono impiegati diversi parametri.
In generale, si parla di ROI come Return Of Investment ovvero ritorno dell'investimento e si usa la formula generale ROI = risultato economico / capitale investito.
Il ROIS riguarda nello specifico il calcolo del ritorno dell'investimento in sicurezza informatica.
Alcuni indicatori numerici sono:
Asset Value (AV): valore del bene da proteggere tramite l'apparato di sicurezza
Vulnerabilità (V): una debolezza dell'apparato che può essere sfruttata da una minaccia per arrecare danni
Minaccia (M): evento in grado di sfruttare la vulnerabilità dell'oggetto
Exposure Factor (EF): valore percentuale di perdita dovuta al singolo evento dannoso
Single Loss Expectancy (SLE): perdita dovuta al singolo evento di minaccia pari a SLE = AV * EF
Annualized Rate of Occurrence (ARO): numero di eventi dannosi attesi in 12 mesi
Annualized Loss Expectancy (ALE): perdita attesa in 12 mesi pari a ALE = SLE * ARO.

AUTORI

Luca Cavone,
Laureato in Ingegneria Elettronica presso l'Università degli Studi di Pavia, Master in Engineering Contracting and Management presso il MIP con la tesi di laurea "Individuazione ed applicazione degli strumenti dell'Enterprise 2.0 nella Gestione della Conoscenza nei processi di Project Management: il caso di una società di consulenza", sviluppata in collaborazione con Innovacting. Certified Project Management Associate secondo la metodologia IPMA (international Project Management Association). Assistant Project Manager nel settore Space&Defence. Membro di Italian Project Management Academy è co-fondatore e Chairman della relativa sezione giovani Young Crew Italia. Aree d'interesse: Project / Program e Portfolio Management, Risk Management, Marketing Strategico, Knowledge Management, Web ed Enterprise 2.0, Entrepreneurship e Business Development.
luca.cavone@tiscali.it
http://it.linkedin.com/in/lucacavone
http://twitter.com/LucaCavone

Gaetano Di Bello
Presidente dell'ALSI Associazione Laureati in Informatica e Scienze dell'Informazione www.alsi.it. Si è occupato di numerose iniziative di formazione indirizzata a varie categorie di professionisti. Nel 1998 crea il portale www.concorsi.it e la testata giornalistica "Concorsi.it: la guida alle opportunità" il punto di iferimento in Italia per l'informazione sul lavoro nella pubblica amministrazione.

Angelo Iacubino,
Ingegnere Informatico, Project Manager - Dipartimento Informatica dell'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).
www.disinformatica.com

Armando Leotta,
Laureato in Scienze dell'Informazione presso La Sapienza di Roma. Nel 2008 nello stesso Ateneo e Dipartimento ha conseguito il Master di II livello in Gestione della Sicurezza informatica per l'impresa e la Pubblica Amministrazione, concluso con un tirocinio trimestrale presso il CNIPA.
Certificato IRCA-RICEC Auditor / Lead Auditor per Sistemi di Gestione per la Sicurezza delle Informazioni (SGSI) a norma ISO/IEC 27001:2005 & BS 7799-2:2002, Certificato OMG UML Professional e OCEB (OMG Certified Expert in BPM), APM Group ITIL v3 e QRP Prince2, dal 2003 si occupa di Gestione della sicurezza e Management dei processi afferenti la sicurezza informativa nella Ragioneria Generale dello Stato. Nel 2009 conclude con AICA un percorso formativo che lo conduce alla certificazione EUCIP Professional/Elective IS Auditor. Responsabile per la RGS dell'Unità Locale di Sicurezza ULS MEF/Consip, autore di svariati articoli su riviste di settore.
info@armandoleotta.it
http://www.armandoleotta.it
http://blog.armandoleotta.com
http://it.linkedin.com/in/armandoleotta
http://twitter.com/ArMyZ

Roberto Marmo
Consulente informatico e professore a contratto di informatica presso la Facoltà di Ingegneria della Università di Pavia, Facoltà Scienze della Università Insubria, vari Master. La sua attività di ricerca scientifica è dedicata ai vari aspetti dei social network: dalle analisi di marketing alla programmazione di software all'analisi statistica SNA della struttura dei social network. Per l'editore FAG ha pubblicato i libri "Creare applicazioni per Facebook" e "Promuoversi con i business social network" sito
http://www.robertomarmo.net

Mario Mazzolini
Laurea specialistica in Ingegneria Informatica presso l'Università degli Studi di Pavia con tesi svolta in collaborazione con IBM dal titolo "Sicurezza delle applicazioni web - metodo di protezione delle sessioni". 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.

Daniele Pauletto
Nato e residente a Castelfranco Veneto, è coordinatore dell'ENIS del Veneto (European Network Innovative Schools), ICT Management dell'Associazione MTNet (Learning and Relation Network).Staff Tecnalia.it e CM Connecting-Managers, autore di diversi libri e pubblicazioni tra cui Web2.0 per tutti Social networking, dalle Reti sociali al Digital Network,e autore di diversi blog.
Mentelab

Roberto Saia,
Laureato in Informatica presso l'Università degli Studi di Cagliari, è autore di vasto materiale su temi inerenti la programmazione, il networking e la sicurezza delle reti, svolge attività di docenza e consulenza collaborando con diverse aziende ed enti del settore ICT; 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), "Sicurezza wireless e mobile" (Ed. FAG, ISBN 978-88-8233-774-2) e "Programmazione e controllo dei sistemi informatici" (Ed. FAG, ISBN 978-88-8233-863-3).
www.robertosaia.it

BIBLIOGRAFIA

A proposito di web 2.0:
Shuen, Amy. Web 2.0 strategie per il successo, Hops Tecniche nuove
Alberto D'Ottavi, Web 2.0 Le meraviglie della nuova internet
James Governor, Web 2.0 Architectures, O'Reilly

A proposito delle tecniche di sicurezza informatica:
Sinibaldi Alessandro, SICUREZZA DEL CODICE Guida alla scrittura di software sicuro, Editore HOEPLI, 2008
Shreeraj Shah, Web 2.0 Security: defending Ajax, RIA and SOA,
Michael Cross, Developer's Guide to Web Application Security, Syngress
Jeff Forristal e Julie Traxler, Hack Proofing Your Web Applications, Syngress
The Web Application Hacker's Handbook - Dafydd Stuttard and Marcus PintoWiley Publishing, Inc

A proposito di Web 2.0 ed Enterprise 2.0:
L. Cavone, G. Costantini, Individuazione ed Applicazione degli Strumenti dell'Enterprise 2.0 nella Gestione della Conoscenza nei processi di Project Management: il caso di una societa' di consulenza.

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 del social engineering e l'arte dell'inganno:
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
R. Marmo, Promuoversi con i Business Social Networks, FAG ISBN 978-88-8233-858-9

A proposito di controllo e programmazione dei sistemi e della sicurezza delle reti cablate e wireless:
Roberto Saia, Reti e Sicurezza, FAG
Roberto Saia, Sicurezza wireless e mobile, FAG
Roberto Saia, Programmazione e controllo dei sistemi informatici, FAG

A proposito di Web 2.0:
Daniele Pauletto Web2.0 versus Web3.0 in Adhocrazia. Sviluppo economico e competitività d'impresa, Franco Angeli Editore
Daniele Pauletto Digital Network in La tecnologia al potere, Guerini Associati

SITOGRAFIA

Building security into the software development life cycle

http://www-01.ibm.com/software/success/cssdb.nsf/CS/VCHN-7YUAWC?OpenDocument&Site=software&cty-en_us

ftp://ftp.software.ibm.com/software/rational/web/brochures/r_appscan_lifecycle.pdf

Guida alla sicurezza delle applicazioni web

http://sicurezza.html.it/guide/leggi/171/guida-sicurezza-applicazioni-web/

Il Taccuino di Armando Leotta (Privacy e consapevolezza, sicurezza e socialnetwork)

IBM Social Computing Guidelines

http://www.ibm.com/blogs/zz/en/guidelines.html

Top 10 Web 2.0 Attack Vectors di Shreeraj Shah

http://www.net-security.org/article.php?id=949&p=1

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 Adware 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.

Attivazione Procedura necessaria per verificare la genuinità di un software installato.

Autenticarsi Accedere ad un sito scrivendo il proprio nome utente (chiamati anche login o user name) e password (parola chiave riservata da non perdere)

Backdoor Indica un punto di accesso illecito e nascosto 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.

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

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

Buffer overflow Tecnica di attacco basata sull'alterazione del flusso di esecuzione di un'applicazione mediante la sovrascrittura di aree di memoria riservate, in grado di bloccare l'esecuzione dell'applicazione.

Bug Usato per indicare 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.

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 Bits inoltrati in una comunicazione allo scopo di individuare eventuali errori.

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 sono state caricate online su un account o altro spazio di condivisione

Condizioni d'uso
Regole contrattuali che vengono accettate dall'utente per accedere ad un servizio. Conviene leggerle con attenzione prima di accettarle. Non sono definitive perchè 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.

Craccare
Superamento delle protezioni di un programma o di un sistema informatico.

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

Crittografia
Termine di origine greca, il suo significato etimologico è Scritture nascoste.

Cross-site-scripting (XSS)
Tecnica di attacco per indirizzare codice maligno verso il browser della vittima.

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

Data Leakage
Fuga dei dati, deliberata o accidentale.

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 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.

DOM
Una rappresentazione della struttura delle pagine HTML .

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 falso con significati diversi in vari ambiti:
- utilizzo di identità altrui esistente o completamen falsa
- allarme relativo a virus inesistente
- file che ha contenuto diverso da quello atteso

Fault Tolerance
Con questo temine si descrivono quei sistemi che 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 in continuazione nuovi contenuti.

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

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 proteggere dagli accessi abusivi un elaboratore (Firewall personale di tipo Software) o un'intera rete di Computer (Firewall di tipo Hardware).

Flame
Tipico dei gruppi di discussione per indicare un attacco o reazione aggressiva nei confronti di altro utente del gruppo.

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

Forum
Un gruppo di discussione virtuale presente sulla rete Internet.

Funzioni di hash
Funzioni matematiche per comprimono i bit di un messaggio in un'impronta di dimensioni fisse chiamata hash, in modo che a messaggi diversi corrispondano impronte diverse.

Gateway
Dispositivo che ha il compito di collegare due reti; il termine Gateway 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 quel 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 entrambi 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. Denota anche l'impronta digitale di un messaggio calcolata tramite una funzione di hashing.

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 (miele) e pot (vasetto), 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, una stampante, etc.

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.

ICRA
Acronimo di Internet Contant Ratign Association, associazione non profit per difendere e aiutare la navigazione dei minori su internet.

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'effettuazione di alcuni controlli.

Lurker
Indica una persona che sta in agguato senza prendere parte attiva su internet.

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) i qualunque bacheca online o nei social media

Privacy Policy
sinonimo di Informativa sulla Privacy

Privilege escalation
tecnica di attacco utilizzata per eseguire la scalata dei privilegi al fine di eseguire azioni con permessi superiori a quelli posseduti.

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, Random).

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

Repeater
Si traduce 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 Rèseaux 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; esso 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 Syndication, standard basato sull'XML indipendente da una piattaforma, per integrare nel sito Web messaggi o altri contenuti Web.

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
Computer che rende disponibili dei servizi all'interno di una rete operante in modalità Client/Server dove i client sono gli elaboratori che fruiscono di tali servizi.

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

Session hijacking
Tecnica di attacco basata sull'intercettazione di una sessione al fine di dirottarla per accedere a risorse senza disporre dei permessi necessari.

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
Ingegneria sociale, una serie di tecniche basate su azioni di imbroglio e persuasione volte ad ottenere informazioni riservate.

Social network
Traduzione inglese di reti sociali, 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, acronimo di Unsolicited Bulk E-Mail, cioè, posta elettronica spedita senza permesso; originato dalla marca di una famosa carne di maiale in scatola, esso è adoperato per indicare 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.

SQL Injection
Tecnica di attacco che consente l'esecuzione di query in SQL in grado di attaccare il database per compiere operazioni illecite.

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

Stack
Insieme di protocolli.

Stand Alone
Utilizzo individuale dell'elaboratore, cioè, non connesso a nessuna rete.

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

Superficie di attacco
Insieme dei potenziali punti di accesso ad un sistema che possono essere sfruttati da un attaccante per comprometterne la sicurezza.

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 il termine "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 di 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.

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.