MEDIA PLANET | SICUREZZA AZIENDALE

LUGLIO 2007

UNA GUIDA PER UNA CORRETTA GESTIONE DEL RISCHIO AZIENDALE ED INFORMATICO

UNA PUBBLICAZIONE MEDIAPLANET

MEDIA PLANET

Sicurezza per i cittadini e per le imprese

di Gigi Tagliapietra – Presidente del CLUSIT Associazione Italiana per la Sicurezza Informatica

Proteggere i sistemi informativi dagli attacchi degli hacker per garantire il funzionamento delle nostre infrastrutture.

Gli incidenti che hanno bloccato per ore l'intero DNS (Domain Name System) della Spagna lo scorso anno e più recentemente l'attacco al sistema DNS italiano fino all' "assedio" a cui sono stati sottoposti recentemente i sistemi di una nazione come l'Estonia che ha dovuto chiedere aiuto anche alla Nato, mostrano concretamente come la rete sia un sistema strategico per un paese, una infrastruttura critica analoga alle reti che trasportano l'energia, agli acquedotti, ai sistemi di trasporto.
La rete delle informazioni ha però caratteristiche del tutto singolari che ne fanno un insieme straordinario ma anche particolarmente vulnerabile e critico.
I sistemi informativi sono condizione per il funzionamento delle altre infrastrutture di un Paese, dalle segnalazioni ferroviarie, al controllo del traffico aereo, dal monitoraggio di fabbriche ai sistemi di gestione dell'energia per cui un incidente informatico, malevolo o fortuito che possa essere, può produrre effetti domino sconvolgenti.
In più la rete delle informazioni, come già avviene per altri sistemi critici come quello energetico, vanifica il concetto di confine nazionale che diventa di giorno in giorno del tutto improprio per garantirne la continuità operativa.

CONOSCI IL TUO NEMICO

Uno dei cambiamenti più significativi degli ultimi anni riguarda il "nemico".
La minaccia più grave ai milioni di cittadini e di imprese che utilizzano la rete per lo sviluppo di servizi e lo scambio di prodotti, viene sempre più da gruppi criminali organizzati e strutturati come vere e proprie multinazionali della delinquenza: la rete, che è sempre stata per la criminalità un mezzo di comunicazione, è ora mercato e terreno d'affari. Agli hacker in cerca di notorietà, si sono sostituiti criminali che vogliono assolutamente mantenere l'anonimato, agli smanettoni che con l'intrusione nei sistemi altrui volevano dimostrarne le debolezze ma nel contempo la loro superiorità e capacità tecnica, si sono sostituiti delinquenti che avendo il lucro come scopo, non vanno certo per il sottile e non si curano del danno arrecato ma della velocità con cui possono arraffare il bottino. Non voglio dire che siano scomparsi gli hacker di prima maniera, ma la loro incidenza sul totale del crimine informatico è sempre più marginale e cogliere la differenza, capire chi sta minacciando i nostri sistemi, se è un ragazzino o un ciberterrorista, deve essere una condizione per adeguare le nostre difese e contromisure.

GIGI TAGLIAPIETRA

Dal gennaio 2005 è Presidente del CLUSIT (Associazione Italiana per la Sicurezza Informatica). Per il CLUSIT ha avviato e gestito l'iniziativa che si occupa di tutela dei minori che va sotto il nome di "Progetto Fataturchina". E' membro dei comitati di certificazione del Lloyd Register e di TUV Italia e ha partecipato al gruppo di lavoro sulla security awareness di ENISA.

Dal 1978 si occupa professionalmente di reti di computer e di sicurezza informatica e ha realizzato importanti progetti di securizzazione per grandi aziende italiane e multinazionali.

In collaborazione con due famosi illustratori per l'infanzia ha scritto un libro per spiegare la sicurezza informatica ai bambini pubblicato dall'editore Fatatrac di Firenze.

LA CONSAPEVOLEZZA DEGLI INDIVIDUI

Chi sono gli attori più importanti per proteggere efficacemente un bene così prezioso come la rete? Chi deve assumersi la responsabilità di un'azione quotidiana che sappia rispondere con efficacia alle nuove minacce? Gli utenti stessi.
Come è stato per il web 2.0 in cui sono gli utenti i veri artefici del cambiamento, sono loro i produttori dei nuovi contenuti di Flickr e di YouTube, così anche per la sicurezza della rete sono gli utenti, con la loro attenzione quotidiana che possono creare una barriera capillare e vigile a presidio della rete. Serviranno sicuramente tecnologie appropriate, regole condivise e procedure di comportamento in caso di incidente come è stato fatto per preparare le popolazioni alle grandi calamità naturali e per limitarne al minimo i danni.
Ma serve soprattutto un grande sforzo collettivo per alfabetizzare alla sicurezza tutti gli utilizzatori della rete, perchè sappiano, con i loro comportamenti attenti, difendere sè stessi e gli altri dalla vulnerabilità che non può essere eliminata da un sistema così diffuso e complesso.
E' stato questo il tema della conferenza Europea sulla sicurezza promossa dal Governo Tedesco a fine del suo semestre di presidenza dell'Unione, è questo il tema che guida il progetto di Online Sicuro promosso dal CLUSIT e sostenuto dal Governo Italiano per fornire ai cittadini informazioni, suggerimenti e aiuto in caso di incidente.

LA CONDIVISIONE DELLE INFORMAZIONI

Come per i cittadini anche per le aziende la risposta alle nuove sfide della sicurezza non è soltanto una sfida tecnologica o di investimenti, che certamente non devono mancare, ma è soprattutto un cambio di mentalità che porti le aziende che condividono medesimi ambiti di rete, per territorio, settore o dimensione a scambiarsi informazioni, ad aiutarsi reciprocamente nel contrastare attacchi e minacce che solo apparentemente riguardano il singolo ma in realtà danneggiano interi comparti dell'economia.
Lo scambio di informazioni è il solo strumento per fronteggiare minacce e vulnerabilità ancora ignote e virus di cui non si hanno i vaccini come l'igiene, la prevenzione e la cooperazione tra paesi è la sola risposta a malattie per cui non si hanno ancora medicine.

DALL'EGOISMO ALLA SOLIDARIETA'

Non è solamente un cambio di mentalità o di cultura o di organizzazione, è tutto questo assieme ad un cambiamento profondo per il mondo della sicurezza che abbandona le metafore egoistiche dei castelli e dei ponti levatoi, dei sani in mezzo agli appestati e abbraccia invece una visione collaborativa e solidale, in cui la sicurezza di ciascuno dipende da quella dell'altro.
Lo abbiamo scoperto con il Phishing, con i BotNet: ognuno di noi rappresenta una vulnerabilità per la rete, un punto di ingresso e di attacco per tutti i partecipanti.
Se TU non sei sicuro nemmeno IO lo sono, ed è solamente con un grande lavoro comune che potremo proteggere e far crescere questo nuovo mondo straordinario. ◆

Una guida che tratta le problematiche della sicurezza informatica in campo aziendale e la gestione del rischio in un'impresa

SOMMARIO

IN COLLABORAZIONE CON Clusit Associazione Italiana per la Sicurezza Informatica

MEDIA PLANET
Mediaplanet with reach and focus
www.mediaplanet.com

Mediaplanet é una casa editrice leader in Europa per la pubblicazione di supplementi tematici allegati a quotidiani e portali online di economia, politica e finanza.
Per ulteriori domande: Staffan Gustavsson, +39 02 36269430

SICUREZZA AZIENDALE – UNA PUBBLICAZIONE DI MEDIAPLANET

Project Manager: Omar Piras, Mediaplanet +39 02 36269422
Testi: Massimiliano Riatti, giornalista scientifico
Produzione/Layout: Giandomenico Pozzi, SGE Servizi Grafici Editoriali
Stampa: Seregni Grafiche Srl, Paderno Dugnano
Distribuzione: Il Sole 24 Ore
Foto: istockphoto.com

Risk Management: benefici di una strategia

Una valida premessa è che non esiste la sicurezza informatica totale. Infatti sono tanti e tali i fattori in gioco, a partire dagli errori umani fino alle catastrofi naturali, che è impossibile controllarli e gestirli tutti. Il migliore approccio è quello che vede la ricerca di una soluzione ottimale, perseguendo il principio di un sufficiente livello di protezione, attraverso sistemi e misure progettate per affrontare situazioni ritenute critiche, o per limitare falle di sicurezza pericolose. La posizione che solitamente si osserva da parte di chi deve amministrare i beni aziendali è quella di operare per tutele differenziate, senza ragionare trasversalmente per ambiti operativi. Quindi ad esempio potranno essere assicurate le attrezzature informatiche, ma non sarà posta nessuna cura alle procedure generali che vedono protagoniste queste attrezzature, né si sarà posta attenzione ad una soluzione tampone in grado di arginare il problema sorto. E' pur vero che è sempre necessario considerare il budget a disposizione per l'intervento, cercando di non disperdere in mille percorsi quanto disponibile, ma operando al fine di massimizzare i benefici.
Il consiglio degli esperti è di dare corso ad una approfondita e seria analisi funzionale dell'organizzazione, quasi una fotografia della realtà aziendale, che comprenda caratteristiche strutturali, processi e flussi operativi, comportamenti e relazioni umane, obiettivi e priorità, benefici e costi. E' ciò che in altri settori viene definito come due diligence: il suggerimento è di prenderne a prestito tutte le specifiche funzioni e cognizioni per realizzare un documento di report ricco di contenuti informativi e di soluzioni adattative.
Il concetto di sicurezza informatica quindi è una filosofia generale di comportamento che non vuole correggere il problema eventualmente verificatosi, ma porre come cardine la prevenzione del rischio ed un atteggiamento interessato al problema da parte degli amministratori di una azienda, non solo dei responsabili del comparto IT. Riprendendo il discorso, quindi, un primo approccio al problema potrebbe essere rappresentato dall'analisi dei rischi, ovvero una valutazione obiettiva di tutte le possibili falle della sicurezza nel sistema informatico e ancora di più nella organizzazione del lavoro e dei collegamenti tra gli organi interni ed esterni dell'azienda.
Si possono valutare tutti gli asset hardware e software installati presso tutte le sedi e le filiali, tutti gli apparati di rete, e tutti i device interconnessi. Poi è possibile valutare lo stato generale dell'organizzazione che presiede all'utilizzo di tali dispositivi, ricomprendendo dirigenti, impiegati, lavoratori generici, agenti, addetti alla sicurezza informatica ecc.
Tutte queste valutazioni hanno lo scopo di comprendere il sistema nella sua interezza non limitandosi all'infrastruttura informatica che ne rappresenta solo lo strumento operativo. La normativa negli ultimi anni ha esplicitamente richiesto una migliore e più efficiente gestione dei procedimenti relativi all'informazione all'interno delle aziende. Non a caso la Risk Analisys è prevista come primo approccio per redigere il Documento Programmatico per la Sicurezza (DPS) come previsto dall'art. 6 del D.P.R. 318/99.
La definizione successiva di una politica per la sicurezza trae origine proprio dallo studio mirato a comprendere come proteggere al meglio i dati propri e di terzi soggetti, a maggior ragione quelli sensibili.
Sovente infatti accade "che una azienda si trovi per esigenze di business a collezionare una notevole quantità di informazioni che devono rimanere riservate. La diffusione di tali dati genererebbe una pesante ripercussione legale con conseguenze impredicibili e una perdita immediata d'immagine verso i clienti e i partner. In una fase successiva alla Risk Analisys possono essere progettate e implementate soluzioni tecnologiche che siano conformi a queste prime valutazioni. ◆

Effettività dei modelli organizzativi ai sensi del D.Lgs. 231/01

AVV. GIANCARLO BESIA
Partner Responsabile Area Compliance PIT Consulting

GIAMPIERO LAMPASONA
Amministratore Delegato PIT Consulting

I modelli organizzativi introdotti dal D.Lgs.231/01 predicano, tra l'altro, condotte etiche e lecite per i destinatari. L'efficacia dei modelli e la loro capacità esimente dipendono dall'effettività degli stessi, ovvero dal livello di conoscenza delle condotte attese da parte dei destinatari e dal livello di conformità delle prassi operative rispetto alle stesse condotte attese. Compito dei vertici (esecutivi e di controllo) è quello di vigilare sul livello di effettività del modello. Tale attività può essere svolta grazie a strumenti che permettono di valutare il livello di effettività e suggerire azioni correttive o migliorative, fornendo altresì informazioni a supporto dei soggetti responsabili per l'adeguatezza organizzativa. ◆

GFI Security Lab: un centro europeo Technology Independent per la Security Governance

Etica, competenze consolidate e un'organizzazione "team work based" per affiancare le aziende nella creazione del valore

La consulenza di professionisti che operano nel settore da diversi anni unita a un'esperienza tecnica unica, acquisita grazie al gran numero di progetti realizzati, consente a GFI Italia di perseguire un approccio integrato alla sicurezza, che tiene nella giusta considerazione gli aspetti tecnici, ma anche quelli strategici, organizzativi, economici e legali.

Con i suoi 450 dipendenti, GFI Italia, presenza nazionale del Gruppo GFI Informatique – oltre 8000 dipendenti a livello mondiale - opera in materia di sicurezza delle informazioni e delle reti a livello nazionale ed europeo attraverso il suo Security Competence Center, una struttura nata per progettare, realizzare e gestire servizi e architetture ICT e di Security Governance per i settori Telco, Utility, Finance, Pubblica Amministrazione, Industria e Servizi.
"Da sempre aiutiamo le aziende a crescere creando per loro strutture IT affidabili e sicure" ha affermato Eugenio Pontremolesi, General Manager di GFI Italia, "e con loro è cresciuta anche la nostra esperienza che ci permette di individuare ogni volta i margini di miglioramento su cui operare combinando le esigenze di sviluppo e di competitività dettate dal mercato con l'offerta tecnologica sempre più dinamica e in continua evoluzione".
Attraverso il Security Competence Center, struttura che vanta oltre 40 professionisti qualificati e certificati (Lead Auditor ISO 27001, CISA, ISO 9001, CISM, ITIL, ecc.) esperti in servizi e soluzioni di sicurezza logica, fisica e organizzativa, GFI Italia è in grado di collaborare con le aziende in un campo caratterizzato da una continua evoluzione e da un'esigenza di aggiornamento costante, rimanendo sempre vicina ai propri Clienti, presidiando il territorio nazionale, ascoltando e indirizzando i loro bisogni, e offrendo loro un servizio di consulenza in grado di identificare la "migliore" soluzione possibile.

In un contesto in cui competitività, qualità ed efficienza sono i requisiti minimi per la sopravvivenza di qualsiasi organizzazione, le aziende si dimostrano sempre più attente al tema delle certificazioni, entrate a far parte anche delle decisioni strategiche.Le certificazioni sono il risultato finale di un percorso che, attraverso l'ottimizzazione di tutti i processi aziendali, permette alle aziende di concentrare l'attenzione sulla capacità di comprendere e soddisfare le esigenze del Cliente, garantendo un'elevata affidabilità attraverso l'utilizzo di metodologie compliant.

Per questo, il Security Competence Center di GFI Italia è un Security Lab specializzato nel seguire e supportare la clientela in tutte le fasi di assessment, di compliance (Basilea II, SOX, ISO 20000, Dlgs196/03) e di accreditamento per la certificazione della sicurezza organizzativa e infrastrutturale. Le certificazioni di software e di sistemi sono sempre affiancate a quelle di processo tramite team specializzati per la certificazione ISO 27001 e ITIL (ISO 20000).
Il Security Lab grazie alla presenza di valutatori abilitati dagli Organi Istituzionali è un Laboratorio di Valutazione della sicurezza di architetture, sistemi, applicazioni, software e prodotti ICT a norma ISO 15408 e ITSEC ed opera ai massimi livelli di garanzia, sia in ambito civile che classificato. Inoltre, un Technical Auditing Team, composto da specialisti accreditati, si occupa delle attività di Vulnerability Assessment, Ethical Hacking, Hardening, Information Security Monitoring e Computer Forensics Analysis.

Oltre a soluzioni nei settori della business continuity e del risk management, il Security Competence Center progetta e realizza architetture di networking e perimeter security (IAM & SSO) facendo leva su solide esperienze e partnership tecnologiche qualificanti quale quella con l'azienda israeliana Check Point.
GFI Italia è infatti Platinum Partner di Check Point, l'azienda leader nella sicurezza su Internet, con una vasta gamma di soluzioni per la sicurezza delle reti, dei dati e la loro gestione.
L'esigenza delle aziende di avere un'architettura di sicurezza affidabile ed unificata che renda sicure sia le comunicazioni - con dipendenti, fornitori, partner e clienti - che le risorse di business, trova risposta nella piattaforma NGX di Check Point che comprende un ampio range di soluzioni dedicate alla sicurezza perimetrale, delle reti interne, delle connessioni web e della posta elettronica. Tra le più recenti novità dell'azienda israeliana, c'è un dispositivo per la gestione unificata delle minacce (UTM) adattato alle esigenze di PMI e imprese multi-sede, l'UTM-1, che assicura una protezione completa e multi-livello contro minacce Internet quali spyware, virus o attacchi alla rete.

La partnership con Check Point si inserisce in una strategia di miglioramento continuo che consente a GFI Italia di progettare per le aziende e per la Pubblica Amministrazione soluzioni per ottimizzare e rendere sicura l'infrastruttura IT, in linea con le più moderne metodologie e standard nazionali ed internazionali.
Potendo contare su personale qualificato ed aggiornato distribuito sul territorio e su partnership di valore, GFI Italia opera da 40 anni con la missione di rappresentare un punto di riferimento nel mercato IT nazionale ed internazionale, restando sempre fedele alla propria identità di azienda affidabile e dinamica e sostenendo costantemente lo sviluppo dei nostri clienti.

GFI Italia SpA
Via Mosca, 52 – 00142 Roma
Tel 06/514651 - Fax 06/51465000
www.gfitalia.it

Nel 2006 l'«image spam» è cresciuto fino a diventare circa il 50% di tutto lo spam

Image spam: l'invasione delle immagini spazzatura

FABIO ROLI
DIPARTIMENTO DI INGEGNERIA ELETTRICA ED ELETTRONICA,
UNIVERSITA DI CAGLIARI - ROLI@DIEE.UNICA.IT

Nel 2004 gli "spammer" tirarono fuori dal cilindro una nuova idea per evadere i filtri utilizzati per bloccare i loro messaggi: incorporare il testo dello spam in una immagine allegata ad un normale messaggio di posta elettronica.
L'idea degli spammer era estremamente ingegnosa poiché tutti i filtri anti-spam dell'epoca si limitavano ad analizzare il testo digitato nella mail, ma non erano in grado di "vedere" ed analizzare il testo contenuto in una immagine allegata. Dal 2004 questo tipo di spam, detto "image spam", è cresciuto in modo enorme, fino a diventare nel 2006 circa il 50% di tutto lo spam, secondo la stima dei MacAfee Avert Labs.
Le grosse dimensioni delle immagini di spam possono creare seri problemi ai server di posta. La prima linea di difesa proposta dai ricercatori è stata quella di dotare i filtri anti-spam di un modulo di riconoscimento ottico dei caratteri (modulo OCR, Optical Character Recognition) per la lettura del testo nelle immagini.
Tale soluzione è stata rapidamente aggirata dagli spammer con tecniche di oscuramento e camuffamento delle immagini che rendono impossibile la lettura automatica del testo, senza tuttavia compromettere troppo la leggibilità per un essere umano. Gli spammer hanno sfruttato il fatto che l'uomo riesce a leggere testi camuffati che sono oggi ancora impossibili da leggere per un computer.
Ricerca accademica e produttori di filtri stanno passando al contrattacco con tecniche che consentono di rilevare i tentativi di camuffamento del testo o di evidenziare particolari caratteristiche delle immagini spazzatura. L'image spam rappresenta oggi la nuova frontiera della guerra alla posta spazzatura. Frontiera dove i contenuti illeciti saranno sempre più veicolati per immagini. L'unico lato positivo dell'image spam è che esso costringerà a forti innovazioni per dare la "vista" a tutti gli strumenti dedicati al controllo delle comunicazioni sulla rete Internet. Forse dalla guerra all'image spam usciranno anche gli strumenti per identificare automaticamente siti e filmati dai contenuti illegittimi o osceni, e la rete Internet avrà finalmente i suoi "occhi" con cui proteggere i suoi utenti più indifesi. ◆

Internet Security Aziendale, quali sono le problematiche

Come proteggersi nel mondo aziendale e su internet.
Quali sono i rischi reali per le nostre imprese.

Le infrastrutture di rete sono da diverso tempo diventate un fattore determinante per il business aziendale, alla luce del fatto che anche una PMI ha di solito una schiera di soggetti che necessitano di relazionarsi a livello informativo con la realtà aziendale anche a distanza (agenti, filiali, punti vendita ecc.). In qualunque azienda i sistemi informatici e le infrastrutture di rete devono sempre poter garantire l'affidabilità e la sicurezza agli utenti, in caso contrario si assisterebbe in breve tempo al fallimento del business stesso in quanto gli ordini, la contabilità, le strategie aziendali, il know-how e tutto il patrimonio di segretezza dell'azienda sarebbe esposto all'azione di terzi non identificati. L'arrivo di internet ha nel contempo migliorato e peggiorato le cose: se da un lato ha consentito collegamenti a costo zero in meno di un secondo con l'altra parte del globo, ha di fatto incrementato esponenzialmente i rischi per la sicurezza di chi opera attraverso questo canale. Dato che il trasferimento dell'informazione trova oggi una implementazione pratica nelle reti aziendali è chiaro che il primo passo per l'analisi dei rischi è quello relativo alla Network Security, con l'obiettivo di realizzare una policy di sicurezza infrastrutturale.
Le debolezze e le vulnerabilità della struttura di rete sono limitabili attraverso l'implementazione di sistemi Firewall, di Intrusion Detection, di reti private virtuali VPN Ipsec, di sistemi di URL filtering. E' naturale poi che vengano posti sotto osservazione i computer, siano essi server o client, per comprendere come all'interno di una struttura a questo punto ben protetta, possano verificarsi falle di sicurezza dovute alle applicazioni o all'utilizzo delle stesse da parte di soggetti non autorizzati.
La presenza ulteriore di sistemi di Log management ed Event Management permetterà all'amministratore di rete di conoscere con esattezza tutti i dettagli relativi al flusso di informazione e agli avvenimenti che coinvolgono la struttura informatica e gli utilizzatori. L'implementazione di un sistema che consenta il riconoscimento e la correlazione di eventi è utile per portare alla luce situazioni pericolose che altrimenti passerebbero inosservate.
I firewall ad esempio sono necessari per impedire l'accesso non autorizzato di esterni alla rete aziendale, d'altra parte la definizione delle regole interne dovrà essere centralizzata per consentire all'amministratore di rete di intervenire rapidamente anche a distanza. Infatti più l'architettura amministrativa e di gestione è corretta, lineare e semplice, meno errori di configurazione si avranno nel sistema.
L'Intrusion Detection è importante quando non si ha la certezza che il firewall stia agendo nel modo migliore, anche perché a volte l'attacco potrebbe provenire dall'interno e non dall'esterno. In tempo reale è possibile disporre di uno strumento capace grazie a dei sensori di rilevare eventi malevoli o discordanti con la politica aziendale siano essi localizzati su segmenti di rete o sui server. Le VPN sono lo strumento attraverso il quale è possibile mettere in comunicazione entità che si scambiano dati cifrati dopo una loro autenticazione forte. In pratica viene creato un tunnel protetto su una rete libera, come internet, dove viaggiano dati sicuri. Questo tunnel è virtuale, ma nell'immaginario è proprio come un segmento diretto e protetto di scambio di informazioni. Uno dei più sentiti problemi delle aziende è quello di controllare e limitare il traffico verso alcuni siti Internet per ridurre gli effetti dannosi indotti (inserimento nelle liste di spamming, consumo di banda Internet, download di software pericoloso), aumentare la produttività dei propri dipendenti e ridurre la probabilità che la propria LAN sia origine di attività maligne o criminose sulla rete.
Un sistema di URL filtering consente proprio questo, ed eventualmente è dotato anche di alcune funzionalità aggiuntive, come ad esempio gestire l'accesso degli utenti interni ad Internet, bloccare la condivisione di file effettuata con connessioni peer-to-peer (P2P), gestire l'instant messaging, gestire l'uso di streaming media ed altre applicazioni che sono dispendiose in termini di utilizzo di banda Internet e prevenire l'installazione di spyware. ◆

Hacker: esperto o criminale informatico?

Quando l'abilità tecnica e la genialità creativa superano le barriere e gli ostacoli della disciplina ufficiale, il confine tra lo spettacolare e il criminale diventa labile. Una analisi storica per capire le origini di questo fenomeno.

Quando si osservano programmi televisivi relativi ad internet e alle nuove tecnologie o si apprendono dai giornali fatti e notizie in merito ad attacchi informatici alle reti di telecomunicazione, viene spesso utilizzato il termine "hacker", che già di per se stesso suscita una certa curiosità nel pubblico ascoltatore. Ma che cosa è esattamente un hacker? Si tratta sostanzialmente di una persona (o un team di persone) che si impegna nell'affrontare sfide intellettuali e di strategia con lo scopo di superare delle limitazioni che gli vengono imposte, come ad esempio le barriere informatiche, non limitatamente ai suoi ambiti d'interesse ma in tutti gli aspetti della sua vita. In molte occasioni, in relazione al settore informatico, colui che esercita nella pratica questa filosofia di vita, è anche colui che tende ad apprendere i segreti dei dispositivi elettronici ed informatici per riuscire ad introdursi in sistemi e reti protette, con lo scopo "scientifico" e "culturale" di dimostrare la propria abilità, forse più a se stesso che ad altri. Però, essendo tale attività esercitata anche da chi cerca un profitto, un utile personale a scapito di altri, il termine hacker ha finito per connotare il tipico criminale informatico, la cui definizione corretta però sarebbe "cracker". Storicamente il termine fu utilizzato all'inizio degli anni 50 al MIT, dove nel gergo studentesco il termine hack indicava una azione goliardica. Uno studente degli anni '50 alle prese con lo smontaggio di un dispositivo elettronico poteva descrivere la sua attività come "hacking". In seguito il termine fu attribuito alle incursioni sotterranee non autorizzate nel campus del MIT, ovvero "tunnel hacking". Quando le attività di incursione o di scherzo riguardarono la telefonia, in gergo fu coniata la definizione di "phone hacking", oggi phreacking. Con il tempo il termine hacking fu utilizzato in associazione ad una attività di miglioramento dell'efficienza complessiva di un sistema, ed hacker erano coloro che vi si dedicavano. Quando al MIT giunse uno dei primi modelli di computer lanciati sul mercato, il termine fu associato alla composizione di programmi e routine software anticonvenzionali, senza ricorrere a procedure della letteratura informatica ufficiale. Tutto ciò denotava uno spirito creativo capace di "aprire un varco" nella metodologia ordinaria per fornire soluzioni innovative. Nei successivi anni '70 il termine hacker era diventato già elitario, collegato a chi era abile nella programmazione dei computer. In pratica per essere un "hacker" una persona doveva essere in grado di scrivere programmi capaci di non limitarsi ad una buona tecnica, ma raggiungendo una vera e propria genialità intrinseca. Con l'avvento delle reti geografiche, di ARPAnet e poi di internet, il significato fu poi trasferito, come connotato negativo, all'immagine di un rapinatore elettronico in stile punk, che agiva contro la società da vero e proprio rinnegato ed emarginato, per intrufolarsi in sistemi e reti creando danni o carpendo informazioni riservate. In altri casi l'immagine dell'hacker è stata associata al quindicenne studente modello capace di violare dei segreti di stato, nella valenza più generale di "genio del computer". Una azione di hacking oggi non viene più considerata come una semplice ragazzata o scorribanda informatica, ma è una attività pianificata e organizzata capace di destare l'attenzione specifica anche delle forze dell'ordine per la gravità penale dei fatti ascrivibili a tale azione. Un hacker pertanto nella moderna accezione viene considerato sia un esperto programmatore di computer e dispositivi di telecomunicazione sia un soggetto potenzialmente pericoloso per la sicurezza informatica. ◆

Un approccio innovativo per combattere il Cybercrime: l'Hacker's Profiling

CLUSIT è partner nel progetto di ricerca internazionale "HPP" (Hacker's Profiling Project) dell'ISECOM, Institute for Security and Open Methodologies. Lo scopo di HPP è quello di arrivare alla stesura - ed alla conseguente libera diffusione, sotto licenza GNU/FDL - di una metodologia di profiling, da applicare nei casi di computer-crime: violazioni, frodi, attacchi informatici. Per un approfondimento: http://hpp.recursiva.org

Il Sacro Graal della correlazione

La correlazione di allarmi nei sistemi IDS è un problema complesso, per cui non esistono ancora soluzioni efficaci nemmeno a livello di ricerca. La speranza di risolvere i problemi di una tecnologia non matura (gli IDS) con una tecnologia embrionale (la correlazione) potrebbe costare cara agli early adopter.

Nel moderno panorama di continui attacchi e compromissioni di reti informatiche, viene da chiedersi dove e perchè si siano arenati tutti i progetti che avevano a che fare con l'intrusion detection, ovvero con il monitoraggio continuo dei sistemi in cerca di segni d'effrazione.
Una delle motivazioni chiave addotte dagli early adopter delle tecnologie IDS è la difficoltà nel monitoraggio, in termini di analisi dei falsi allarmi, di tuning dei sistemi, e soprattutto in termini di ricostruzione degli eventi, incrociando i dati da una molteplicità di sonde di rete (specie in architetture complesse e distribuite) e di sonde host-based sui server critici. Un'altra motivazione è che i sistemi IDS attuali non sono in grado di rilevare gli attacchi "zero-day", ovvero gli attacchi rivolti contro vulnerabilità non note e catalogate. Infatti, al di là del marketing, tutti i sistemi di intrusion detection in commercio sono fondamentalmente "misuse based", ovvero usano una base di regole (più o meno sofisticata ed aggiornata) per identificare gli attacchi. Risulta ovvio che, a meno di casi fortunati, un sistema del genere non può identificare attacchi nuovi. L'anomaly detection (ovvero l'analisi statistica e mediante algoritmi di apprendimento del comportamento normale del sistema, alla ricerca di eventuali deviazioni) è l'unica possibile risposta per rilevare un attacco contro una vulnerabilità non pubblica.
Purtroppo, gli algoritmi anomaly-based sono raramente usciti dalle istituzioni di ricerca, e solo alcune piccole compagnie producono sistemi IDS basati su queste tecniche. Ma, anche qualora si dovessero finalmente diffondere, rimarrà il problema di come correlare tra loro gli allarmi di IDS host-based e network-based, misuse-based e anomaly-based. Purtroppo, il vocabolo "correlazione" è stato ampiamente usato ed abusato dai produttori di tecnologie IDS, generando molta sfiducia negli acquirenti. Difatti, spesso viene spacciata come "correlazione" la semplice raccolta, aggregazione e centralizzazione di alert provenienti da fonti distribuite. Questo è un problema di tipo tecnico, già risolto con successo. Il problema scientifico e tecnologico rilevante, tuttavia, è che nella maggior parte dei casi le informazioni raccolte sono prive di qualsiasi forma di semantica (non è raro trovarle archiviate sottoforma di testo libero).
Alcuni IDS misuse-based sono stati opportunamente integrati con basi di conoscenza che consentono ad uno strumento di correlazione di analizzare il contenuto degli allarmi. Tuttavia, a causa della mancanza di standard solidi in questo senso, tale opportunità è limitata alle sonde di un singolo vendor, cosa che in realtà eterogenee è spesso inapplicabile. Inoltre, permane il problema di come correlare i log degli IDS con quelli, ad esempio, di firewall o antivirus, che raramente sono di un singolo produttore. Infine, bisogna prendere coscienza che il problema chiave di "come correlare le informazioni tra loro" è lungi dall'essere risolto.
Ciò che ci aspetteremmo da un sistema di correlazione sono dei "riassunti" compatti degli eventi, che eliminino informazioni ridondanti circa gli attacchi, e che per quanto possibile ricostruiscano relazioni di causa/effetto e scenari d'aggressione. Vorremmo cioè che l'output ci consentisse ad esempio di seguire la sequenza di azioni effettuate da un aggressore, e identificarne più facilmente la finalità. Pertanto un sistema di questo genere sarebbe tanto più efficace quanto più in grado di ridurre il numero di informazioni presentate all'analista, senza perdere di completezza.
Alcuni sistemi cercano di risolvere questo problema con un motore a regole che associa tra loro attacchi che ricadono in "scenari noti". Questo meccanismo soffre una volta di più dei problemi della misuse detection, e di fronte ad un aggressore creativo o a nuove minacce non può essere efficace. Di male in peggio, alcuni sistemi addirittura sono semplici applicatori di regole e richiedono all'utente finale di definire le sue regole di correlazione. In altri casi, più raramente, vengono utilizzati sistemi di tipo statistico per sopprimere alert che fanno parte del rumore di fondo e cercare di identificare le "novità".
Questo è un meccanismo che può funzionare, ma sicuramente non giunge all'obbiettivo. Infine, nessuno dei sistemi esistenti è sufficientemente generico per essere adattato all'anomaly detection. Quasi tutti i motori si basano su molteplici forme di conoscenza pregressa: per esempio, dei valori di "gravità" di un tipo di attacco, oppure una sua classificazione, quando non delle intere "firme di scenari"; tutte informazioni che mal s'adattano all'integrazione di sistemi anomaly-based.
Purtroppo, da un'analisi seria dell'offerta, si può facilmente cogliere come il progetto di algoritmi per la correlazione di allarmi sia un problema nuovo, aperto e che ancora necessita di molto studio ed investimento in ricerca e sviluppo. La maggioranza degli strumenti, commerciali e non, oggi si basa su algoritmi che non possono prescindere dalla particolare situazione e dal particolare tipo di analizzatori, e purtroppo spesso anche dalla pre-esistenza di regole statiche di correlazione.
I problemi arrivano fino alla definizione di cosa significhi "correlazione", e al significato dei dati in ingresso ai sistemi, ovvero all'eterogeneità (o assenza) della semantica di ciascun formato. C'è ancora molta, molta strada da fare, prima di poter realizzare un sistema di correlazione automatica che non sia semplicemente un soprammobile. ◆

Progetto ITAISAC: Verso la costituzione di un ISAC italiano

Gli ISAC (Information Sharing and Analisys Center) sono strutture che riuniscono esperti e tecnici che condividono informazioni e dati relativi ad attacchi e vulnerabilità informatiche. Il loro scopo è acquisire una visione integrata e aggiornata dei rischi, delle minacce, degli attacchi che possono compromettere il funzionamento delle infrastrutture. L'obiettivo è creare un sistema di alerting in caso di nuove minacce; costruire una rete di responsabili delle principali organizzazioni che controllano le infrastrutture critiche del paese (risorse alimentari, risorse idriche, energia, trasporti, telecomunicazioni, salute pubblica, sistema economico-bancario, servizi di emergenza, governo, difesa, industria...) per accelerare il ripristino della normalità in caso di attacco o emergenza dovuta a cause naturali.
Gli Usa hanno iniziato ad occuparsi dell'argomento nel 1996, quando Clinton ha istituito la "Commission on Critical Infrastructure Protection" (PCCIP). Gli eventi dell'11 settembre '01 hanno spinto l'amministrazione Bush a proseguire su questa strada. Attualmente negli USA ci sono diversi ISAC operativi, ciascuno dei quali presidia un settore (sanità, finanza, autostrade, chimica, etc.) più una struttura di coordinamento trasversale, il Council.
In Italia il CLUSIT ha deciso di partire con un ISAC trasversale, con le aziende che stanno dimostrando interesse, in particolare nel settore delle Telecomunicazioni.

CLUSIT Associazione Italiana per la Sicurezza Informatica

Il Clusit, nato nel 2000 presso il Dipartimento di Informatica e Comunicazione dell'Università degli Studi di Milano, è la più importante associazione italiana nel campo della sicurezza informatica. Oggi rappresenta oltre 500 organizzazioni, appartenenti a tutti i settori del Sistema-Paese, in particolare: Ricerca, Industria, Commercio e Distribuzione, Banche e Assicurazioni, Pubblica Amministrazione, Sanità, Consulenza e Audit, Servizi, Telecomunicazioni, Informatica.

www.clusit.it: una fonte autorevole
Il sito del Clusit mette a disposizione una grande quantità di informazioni e di notizie utili:
- Documenti tecnici e scientifici
- Calendario di eventi e seminari
- Link ai siti di maggiore interesse
- Rassegna stampa
- Elenco dei soci e link alle loro aziende
- Newsletter mensile

Per i soci sono disponibili aree ad accesso esclusivo.

Perchè associarsi a Clusit
Il Clusit è aperto ad ogni persona fisica o giuridica che abbia a cuore il tema della sicurezza informatica.
I vantaggi per i soci:
- Partecipazione gratuita a seminari tecnici e divulgativi
- Accesso gratuito ai Quaderni Clusit ed ai materiali didattici
- Informazioni tempestive sulle novità nel mondo dell'ICT security
- Partecipazione a progetti europei
- Contatto privilegiato con il mondo accademico e della ricerca

ID Management: l'importanza di farsi riconoscere

Per qualsiasi realtà aziendale, di piccole o grandi dimensioni, è fondamentale individuare un sistema per gestire il controllo dell'identità del personale presente in un dato momento all'interno dei locali e degli spazi lavorativi. Questo per ragioni amministrative, sindacali, legali, fiscali e di sicurezza. Con una strategia adeguata non si rischia di trasformare una gestione ordinaria in una falla pericolosa dalle conseguenze imprevedibili.
Tutto sta nel tipo di implementazione che si va ad utilizzare, infatti è noto che la resistenza di una catena è quella del suo anello più debole. Dal punto di vista informatico l'anello più debole per molte imprese è proprio quello della gestione efficiente degli accessi e delle identità digitali.
Nello scenario ideale una azienda dovrebbe gestire in modo automatizzato l'accesso di ciascun utente alle applicazioni specifiche, con la possibilità di effettuare la disattivazione immediata di un account per impedire accessi non autorizzati (un caso tipico è costituito dal fatto che il dipendente termina il rapporto di lavoro con la società ed è quindi necessario disattivarne gli accessi). Invece esistono situazioni le più variegate possibili, dove ad esempio esistono account fantasmi ancora attivi nonostante non siano più utilizzati o scenari dove dei dipendenti sono costretti a doversi ricordare così tante password che devono optare per codici più semplici per ricordarseli tutti, vanificando quindi l'approccio di sicurezza. La prima valutazione da operare per rendere sicuro un sistema è relativa alla gestione dell'identity management.
Qualsiasi amministratore di rete sa per esperienza che si tratta di una delle attività più complesse per un sistema di sicurezza aziendale, basata non tanto sulla tecnologia, quindi smart card e altro, ma sulla capacità di rendere il sistema complessivamente in grado di identificare con precisione i soggetti che operano al suo interno.
Possono esistere diversi approcci strutturali, che nascono dalle possibilità offerte dal mercato, quali ad esempio la creazione di regole basate sulle identità digitali rilevate attraverso sistemi biometrici che consentano una creazione ad hoc del database degli utenti e dei permessi.
Giusto per non iniziare insicuri e poi rendersi conto a sistema terminato, di avere creato una roccaforte che già contiene al suo interno i nemici.
Quindi la chiave sostanziale è la possibilità di "personalizzare sicuri" perché un sistema di sicurezza è in fieri, cambia la propria struttura e si plasma sulle reali esigenze dell'azienda target.
Rimane quindi impossibile trasferire le politiche di protezione come un pacchetto a se stante da un contesto ad un altro.
E' sulla base della metodologia specifica di lavoro che vengono ad essere identificate le possibilità operative. Ad esempio una banca potrà basare la prima identificazione sulle impronte digitali al momento dell'ingresso agli sportelli, ma ciò potrebbe essere improponibile per l'identificazione di utenti che accedono in massa ad un determinato sito.
Il mercato si va consolidando, e il settore dell'identity management sta rapidamente evolvendo, con la presenza di produttori specializzati che vengono acquisiti da aziende più grandi e più generaliste.
La strategia giusta per gestire questo relativo stato di incertezza si fonda sulla realizzazione di processi di ID management in modo standardizzato: il peso di un eventuale passaggio ad una nuova tecnologia a questo punto potrebbe risultare inferiore, per una più contenuta rivisitazione architetturale. Quindi è necessario anche comprendere se il fornitore di sistemi di sicurezza fonda la propria proposta su concetti come "assemblaggio", "flessibilità", "scalabilità" e "riutilizzo" prima di affidarsi ad un sistema monolitico non gestibile altrimenti e quindi alla lunga destinato a divenire obsoleto e inutile.
Se invece si realizza una opportuna strategia di gestione delle identità, basata sia sulla implementazione della tecnologia di punta e ritenuta quindi più affidabile, sia sulla capacità di modificare il sistema stesso per i cambiamenti epocali, si sarà trovata la giusta combinazione per una valida ed efficace implementazione. ◆

EXPERT PANEL EXPERT PANEL EXPERT PANEL EXPERT PANEL EXPERT PANEL

La parola agli esperti

Marco Venuti
Pre Sales Director
South-EMEA
Novell Italia

In un mondo sempre più interconnesso e dove è ormai possibile accedere alle informazioni aziendali da qualsiasi luogo, che cosa stanno facendo le aziende e quali strumenti hanno a disposizione per proteggere i dati e le informazioni sensibili?
La crescita a due cifre del mercato della sicurezza informatica a cui abbiamo assistito negli ultimi anni mostra l'interesse delle aziende per le problematiche di sicurezza.
Negli anni passati l'attenzione è stata soprattutto rivolta a ciò che, semplificando, potremmo chiamare i pericoli sconosciuti/non prevedibili, con una strategia che si potrebbe riassumere dicendo "proteggiti da chi non conosci", e quindi si è parlato soprattutto di firewall, antivirus, ecc.
Oggi l'attenzione si è invece decisamente spostata sul "proteggiti da chi conosci", ovvero la gestione della sicurezza degli accessi informatici alla rete da parte delle persone, siano esse dipendenti, clienti o partner, ai contenuti e ai sistemi informativi. In altre parole, ci si è accorti che molte violazioni critiche hanno origine proprio "dentro le mura di casa".
Le soluzioni per proteggersi da questi problemi sono note sul mercato con diversi nomi, tra cui "identity and access management" - gestione del ciclo di vita delle utenze sui vari sistemi eterogenei presenti in azienda per garantire di avere sotto controllo il "chi fa cosa"; "security event management", che consente l'analisi in tempo reale delle attività sui vari dispositivi e applicazioni per identificare e reagire ad attacchi o violazioni dei diritti di accesso; infine, "endpoint security management" ovvero la "blindatura logica" dei PC per impedire attività quali la copia su chiavette USB di file o l'uso di qualsiasi programma non espressamente autorizzato, per prevenire possibili esportazioni di informazioni via rete.Una soluzione integrata che unisce queste componenti garantisce ciò che possiamo definire "security governance and compliance", ovvero il controllo e gestione di chi possiede i diritti di accesso ai sistemi, visibilità su chi ha effettivamente avuto accesso ai sistemi, e la prevenzione dell'asportazione di informazioni.

In che modo il problema dell'adeguamento normativo (compliance) influenza l'adozione da parte delle aziende di soluzioni tecnologiche per la sicurezza?
Le normative quali il Testo Unico sulla Privacy o la Sarbanes Oxley hanno creato il senso di urgenza sulla necessità sia di misure preventive di gestione della sicurezza logica sia di soluzioni centralizzate di auditing di quanto avviene sui sistemi.
Mentre prima la sicurezza era ...per così dire un'ossessione dell'IT, le normative hanno sensibilizzato il top management e incrementato il budget per la sicurezza.
Oggi infatti il motivo principale di adozione di una soluzione di Security Governance e Compliance è la ricerca della conformità ad una o più normative nazionali o internazionali.

Riccardo Cazzola
Vice Direttore Generale
Trust Italia

Cos'è una PKI?
PKI è l'acronimo di Public Key Infrastructure ..cioè infrastruttura a chiave pubblica..cioè?
Il termine PKI tecnicamente si riferisce alla tecnologia, le infrastrutture e le pratiche necessarie per utilizzare la crittografia a chiave pubblica o le firme digitali su applicazioni che siano distribuite su vasta scala.
In altre parole, siamo in presenza di un mix di tecnologie, regole e responsabilità al fine di creare un circuito di emissione, gestione ed utilizzo di una credenziale digitale forte (detto Certificato Digitale) il quale permette di identificarsi in modo certo ed univoco nella rete come le persone, le macchine e i Servizi.. una sorta cioè di passaporto elettronico.
In pratica come un documento di identità cartaceo però NON falsificabile e/o replicabile emesso da una autorità detta Certification Athority che ne garantisce appunto i due fondamentali concetti appena espressi.

Come funziona?
LA CA è una struttura tecnologica e di regole creata per emettere il Certificato Digitale e ne segue attraverso di essa il suo ciclo di vita (emissione – durata – sospensione –revoca).
La stesso Certificato Digitale una volta erogato potrà essere utilizzato (in quanto rispondente a standard tecnologici aperti) per poter effettuare le seguenti funzioni di base:
- Firmare un documento elettronico
- Firma e Crittografare la posta elettronica
- Identificarsi autenticarsi e crittografare le comunicazioni elettroniche (Web – VPN) attraverso vari programmi di posta elettronica e Web Browser.

Si noti bene che è molto importante che una PKI venga implementata rispettando i più alti parametri di sicurezza, anche superiori rispetto a quelli normalmente osservati per lo sviluppo di un comune sistema di protezione delle transazioni, dal momento che in questo caso anche la falla più apparentemente insignificante potrebbe generare danni enormi ad un'azienda.

Per chi è utile?
Quando un'azienda decide di implementare al proprio interno una PKI, evidentemente ha l'esigenza di proteggere il proprio patrimonio informativo attraverso ciò che la PKI garantisce, vale a dire: autenticazione, confidenzialità, non-ripudio, disponibilità.
Si parla, in altri termini, di rispondere ad un'esigenza di identificazione certa e di autenticazione forte nell'ambito del business virtuale.
Dunque, la PKI rappresenta senz'altro un'esigenza di primaria importanza per le aziende ed organizzazioni in genere, che intendono evitare che la propria identità sia replicabile rendendo potenzialmente il "il proprio mondo virtuale" fatto di servizi come ad esempio l'home banking – Servizi erogati dalla Pubblica Amministrazione – Acquisti – Disposizioni - Distribuzione di informazioni riservate (progetti strategie marketing – fatti personali) di fatto disponibile anche a chi NON è autorizzato.
Infatti, il ricorso, da parte di un'azienda, alla PKI, consente alla stessa di avvalersi di credenziali forti che permettono di dare servizi di varia natura agli utenti (che possono essere dipendenti di un'azienda, partner, reti di collaboratori, ma anche, più semplicemente) privati cittadini.

Massimo Cata'
Direttore
Programatic

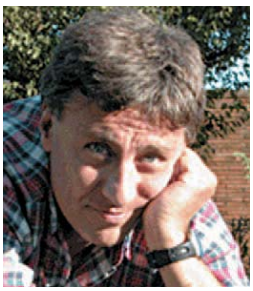
Quali sono i rischi per la sicurezza informatica? Sono rischi di tipo software o di altro tipo?
Software ed hardware possono essere oggetto di tentativi d'effrazione, sia di tipo logico che di tipo fisico, ma i sistemi informatici, per loro natura, non sarebbero in pericolo se, dietro gli stessi, non ci fosse l'essere umano che, per le motivazioni più diverse, può essere interessato a entrare in possesso di informazioni riservate. E' anche vero che, da alcuni anni, si sono diffuse tecniche di attacco che poco o nulla hanno a che fare con le vulnerabilità dirette dei sistemi.
Una di queste tecniche è il "social engineering". Pirati informatici e malintenzionati in genere, si camuffano per venire a conoscenza di informazioni che possono essere usate per organizzare attacchi informatici. Il "phishing", tecnica che si basa sul social engineering, ha mietuto molte vittime tra i clienti di organizzazioni bancarie. Siti web identici a quelli delle banche sono creati per attirare l'ignaro utente che, fidandosi di un messaggio di posta artefatto, rivela le sue credenziali al malvivente di turno.

Quali sono i settori della società più esposti nella sicurezza informatica?
Qualsiasi computer è un potenziale bersaglio, quindi, non ci sono settori che possono considerarsi immuni. Ci sono settori che più di altri fanno notizia, per la popolarità dei nomi in gioco, per il tipo di attività svolta o per il fatto che coinvolgono l'uomo della strada, il consumatore.
Ad esempio, gli attacchi portati ad operatori bancari e finanziari fanno colpo, non solo perché l'argomento "denaro" stimola l'immaginario collettivo, ma anche perché la maggioranza di noi utilizza carte di credito, bancomat, sistemi di pagamento elettronico o conti correnti on-line. Per aumentare il livello di sicurezza, molti istituti bancari hanno introdotto strumenti d'identificazione basati su dispositivi che, generando un codice pseudo-casuale, fanno in modo che il cliente acceda o disponga operazioni con una password sempre diversa.

L'autorizzazione informatica è sufficiente a garantire la sicurezza delle transazioni?
Purtroppo, esistono tecniche di attacco che possono aggirare anche i sistemi d'identificazione più avanzata, attraverso l'intromissione del malintenzionato nel mezzo della transazione finanziaria. Il cliente crede di interagire con la sua banca, ma, tra lui ed il sito della stessa, si posiziona il malintenzionato che può catturare e modificare i dati trasmessi a suo piacimento.
L'identificazione univoca è necessaria, ma può non essere sufficiente a garantire la sicurezza delle transazioni.

Esiste la possibilità di tutelarsi da questo tipo di problemi?
Esistono software in grado di ridurre al minimo i rischi di frodi informatiche bancarie. Questi software analizzano in tempo reale le singole transazioni, tenendo conto di una serie di informazioni specifiche, del modo abituale di operare, degli importi normalmente movimentati, dei luoghi e dei momenti in cui queste avvengono, ecc.
Nel caso in cui uno o più elementi destino sospetto, il sistema lancia degli allarmi e, in base al livello di severità, attiva delle contromisure: la richiesta di un nuovo codice identificativo, la telefonata di un operatore che accerti la volontà del cliente e così via, sino al blocco automatico della transazione.

Mauro Zaccari
Gestione e Sviluppo offerta
GFI Italia



Michele Bianco
Security Competence Center Director
GFI Italia

L'imprenditore che guarda la sua azienda e comincia porsi il problema della sicurezza perché dovrebbe porsi il problema? Da dove dovrebbe iniziare?
Più il business evolve verso modelli aperti all'interscambio tra clienti, dipendenti, fornitori e partner, più diventa necessario guardare alla sicurezza informatica come ad una delle leve strategiche che consente all'azienda di "aprirsi al mondo" mantenendo l'integrità e l'affidabilità dei propri dati. In un campo in continua evoluzione come quello della sicurezza delle reti, un iniziale punto di approccio può essere affidarsi a consulenti esperti che, partendo dall'analisi della rete aziendale, trovino la soluzione ottimale in termini di tecnologie e di policy, guidando l'imprenditore attraverso le scelte più adatte alla dimensione e alla complessità della propria azienda.
(Mauro Zaccari)

Quali sono tempi, modalità e costi dell'implementazione?
Tempi e costi possono essere ridotti o diluiti nel tempo a patto che per individuare soluzioni appropriate al contesto ci si avvalga realmente di competenze etiche indipendenti dalle tecnologie. La sicurezza è spesso percepita come un costo associato a prodotti ma non é così. La sicurezza non é un prodotto, ma parte del processo organizzativo aziendale che se ben fatto determina un modo di lavorare, di trattare e proteggere dati e informazioni importanti per il business e per la tutela della privacy. *(Michele Bianco)*

Il futuro: in che direzione si andrà? Cosa succederà domani?
La cultura sta cambiando. La sicurezza passa da "costo" ad "opportunità" di creare valore per l'azienda. Una infrastruttura di sicurezza "certificata" e affidabile, coerente espressione del processo aziendale che attua le contromisure individuate dagli assessment potrà evolvere, essere "gestita" e monitorata sia dall'Impresa che dal partner attraverso indicatori (Security Key Performances Indicators) e cruscotti che serviranno a migliorare continuamente i processi interni, risparmiando sugli sprechi e consentendo di differenziare il proprio business da quello dei competitors.
(Michele Bianco)

Stefano Volpi
Vice President,
Southern Region & Mediterranean
IBM-ISS

La sicurezza deve essere intesa solo come acquisto di un prodotto tecnologicamente avanzato?
La legge sulla Privacy parla di soluzioni avanzate e la potenza dei prodotti risponde alla crescita di complessità delle minacce. Oggi però la sicurezza non è più concepibile come singolo prodotto. Prima, al sorgere di una nuova minaccia, corrispondeva lo sviluppo di una soluzione che ne mitigava il rischio, proteggendo il sistema da quella e sola minaccia. Una rincorsa che non può protrarsi all'infinito. Le imprese, del resto, stanno toccando con mano una lievitazione insostenibile della spesa in sicurezza.La tecnologia può e deve fare di più: ci sono sistemi che forniscono una protezione a 360 gradi di tutta l'infrastruttura (rete, server e pc) e che, soprattutto, introducono elementi d'automazione che tutelano da comportamenti distratti o scorretti.

Ma quanto valore aggiunge un progetto rispetto ad acquistare un singolo prodotto che magari fa più cose?
La differenza principale sta nell'approccio completo di una soluzione end to end. All'inizio, la sicurezza Internet si preoccupava di proteggere essenzialmente dagli attacchi provenienti dalla rete: era una sicurezza cosiddetta perimetrale. Oggi i confini del sistema informativo sono più labili, un singolo prodotto anche "multifunzione", non consente di controllare tutti i punti "deboli" di un'infrastruttura. Sul fronte della gestione, inoltre, il prodotto singolo non fornisce strumenti per governare la sicurezza con una visione d'insieme. Addirittura, può causare danni, con una falsa sensazione di sicurezza, quando nel concreto il livello di protezione può essere molto basso se non nullo.

Quindi nel concreto come si struttura un sistema di sicurezza?
L'unica risposta è quella della prevenzione. Bisogna adottare un approccio olistico, cioè un insieme di soluzioni che costituiscono una piattaforma. La nostra strategia parte dalla ricerca: difende dalle minacce indipendentemente dalle vulnerabilità presenti e dalle possibili varianti impiegate per sfruttarle.

Quale vantaggio deriva da impostare un'unica console di sicurezza per una visione d'insieme?
In primo luogo la semplicità, soprattutto se l''interfaccia è estremamente intuitiva. Ma il vantaggio essenziale deriva dalla capacità di correlazione degli eventi e dall'integrazione con le altre soluzioni. Gli eventi legati alla sicurezza in un sistema anche di medie dimensioni sono dell'ordine delle centinaia di migliaia al giorno. È umanamente impossibile soffermarsi su ciascuno, e poi molti di questi, presi singolarmente non significano molto, ma se abbinati ad altri possono rivelare l'inizio di un attacco che può essere completato in pochi secondi. La console presenta all'amministratore della sicurezza gli eventi con una scala di priorità, scartando quelli ininfluenti, permettendo di avere un'immagine immediata dello stato di sicurezza grazie a elementi grafici intuitivi.

Giuseppe Fortunato
Business Consultant Principal
Hitachi Data Systems

Che valore aggiunto rappresenta per una azienda una soluzione di storage?
Nelle infrastrutture storage spesso risiedono gli asset più preziosi per un azienda: le informazioni. Le informazioni sono legate in modo strettissimo al vantaggio competitivo dell'azienda e la modalità con la quale vengono conservate e rese disponibili alle funzioni aziendali è un fattore chiave di competitività. Oggi nelle moderne infrastrutture informatiche si distinguono chiaramente le funzioni destinate al calcolo, ovvero a sostenere il patrimonio applicativo aziendale, e quelle destinate alla gestione dei dati ed al loro accesso. Le aziende che hanno individuato il ruolo chiave delle infrastrutture storage nei loro processi aziendali possono contare su un vantaggio competitivo derivante dall'ubiquità del loro patrimonio informativo.

Che cosa significa Services Oriented Storage? Quale novità introduce nel settore un approccio di questo tipo?
L'approccio Service Oriented Storage di Hitachi Data Systems porta nel mondo delle infrastrutture dati dei concetti già noti nel campo applicativo e di vasto successo come ad esempio l'architettura SOA di Microsoft. Il concetto è di per se semplice ma molto efficace e si basa sull'astrazione delle funzioni che il layer storage mette a disposizione del mondo applicativo. L'astrazione consente di costruire sul layer dati un Know How e delle procedure operative (accesso, conservazione e protezione dei dati) che possono diventare un patrimonio aziendale nel tempo senza preoccuparsi troppo delle tecnologie sottostanti mascherate appunto da un livello intermedio di astrazione. Il livello di astrazione nel caso delle tecnologie storage è rappresentato dalla virtualizzazione delle tecnologie di memorizzazione così come già avviene per i server. La novità di questo approccio risiede nella possibilità di rendere indipendente dalla tecnologia prescelta l'accesso alle funzioni storage da parte del layer applicativo. Questa indipendenza permette di operare sui due livelli senza ripercussioni incrociate e con un maggiore controllo dei costi di gestione.

Perchè oggi è stata introdotta la Storage Virtualization? Per quali tipologie di utenti è consigliabile?
La storage virtualization è la base su cui Hitachi Data Systems fonda il concetto di Service Oriented Storage. Le tecnologie storage sono oramai mature e l'approccio service oriented permette di unificare le modalità di accesso e di gestione e di non doverle più cambiare nel tempo al cambiare della gestione.
Questo approccio è fortemente consigliato a quei clienti che desiderano mantenere più fornitori all'interno del loro parco storage ma un unico metodo di accesso e di gestione dei dati con una definizione delle classi di servizio indipendente dalle tecnologie prescelte.

Vittorio Giovani
Direttore Generale
Network Appliance Italia

Perchè è necessario intervenire nella sicurezza dei dati in ambito aziendale?
Oggi che il patrimonio informativo delle organizzazioni costituisce il vero cuore di ogni attività e che il knowledge worker ha sostituito le figure professionali di un tempo, le aree It relative a storage, security e information management sono sempre più contigue e interconnesse. Implementare una corretta gestione delle informazioni in chiave Ilm (Information lifecycle management) aderente alle normative più recenti, come Basilea 2, Documento Programmatico sulla Sicurezza e Sarbanes-Oxley, significa essere in grado di gestire in maniera completa, inclusi gli aspetti riguardanti la protezione ed il recupero immediato ed efficace, tutte le informazioni relative alla conduzione del business, in qualsiasi settore si operi.
Inoltre alle regolamentazioni si aggiunge una realtà di fatto: l'aumento esponenziale delle informazioni aziendali, quindi la necessità non è più solo archiviarle ma è proteggerle, gestirle nel loro ciclo di vita, oraganizzandole in maniera efficiente, affinchè siano una asset fruibile al meglio da tutte le funzioni aziendali.

Attraverso quali attività è possibile ottenere la sicurezza delle informazioni aziendali? (catalogazione ecc.)
Una delle prime operazioni che ogni azienda dovrebbe attuare è la comprensione della quantità e della tipologia di informazioni presenti in azienda (ricordiamoci che, al riguardo, circa l'80% di queste sono in forma non strutturata o semi-strutturata), di conseguenza la catalogazione e l'indicizzazione sono atti dovuti e necessari.
Occorrono quindi soluzioni che siano in grado di fare ciò, consentendo, in maniera semplice e rapida di ritrovare le informazioni nel momento in cui servono ma, al contempo, consentendo l'utilizzo sicuro, controllato e autorizzato. Partendo da questa attività si stabiliscono delle policy di messa in protezione delle informazioni aziendali in base alla loro criticità ed importanza.

Quali sono le politiche di sicurezza e a quali miglioramenti portano?
Ovviamente non esistono delle soluzioni univoche, in quanto ogni azienda deve fare i conti con due paramentri fondamentali che dipendono dal contesto di business all'interno del quale l'azienda si muove e del budget a disposizione.
Sicuramente il punto di partenza è il semplice back up, per poi arrivare al disaster recovery passando per la business continuity, questa comprendente sia la tematica relativa alla protezione logica continuativa delle informazioni , che a quella riguardante la protezione fisica delle stesse.

Moderni requisiti di uno storage system

Un ottimo sistema di storage deve possedere diverse caratteristiche che gli esperti del settore reputano indispensabili per una archiviazione perfetta:
1. la presenza di una indicizzazione e di un indirizzamento che consentano l'individuazione univoca dell'informazione singola.
2. un costo di gestione relativamente minimo.
3. la possibilità di conservare le informazioni per un ampio margine di tempo (anche anni).
4. la disponibilità di prestazioni elevate e un tempo di ricerca praticamente nullo.
5. una chiave di scalabilità per una crescita della funzione di storage in rapporto alle esigenze dell'utilizzatore.
6. l'integrazione con delle applicazioni realizzate per la gestione dell'informazione.
7. la facilità di gestire il sistema di storage con strumenti di controllo centralizzati

Salviamolo prima di perderlo!

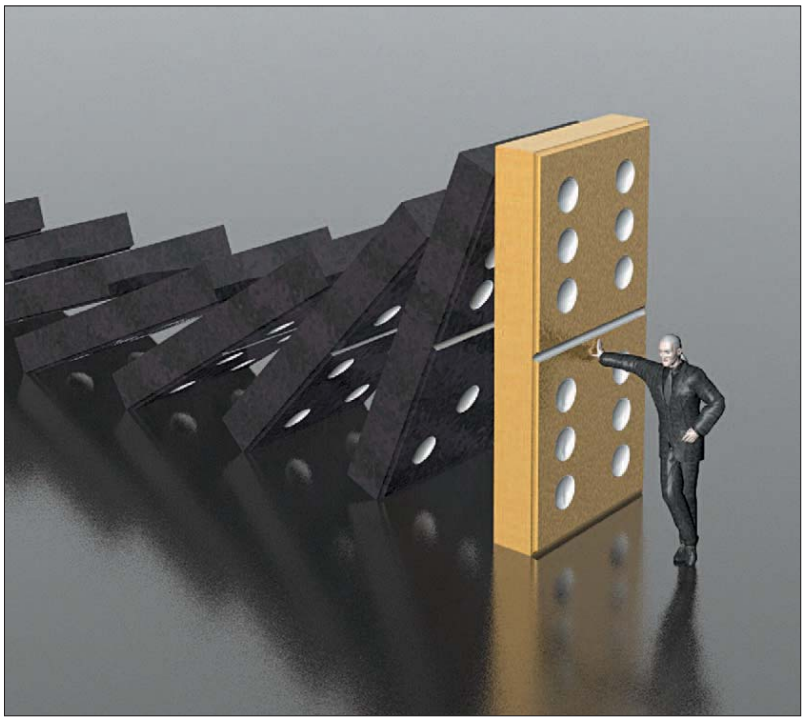
Il concetto di informazione è indiscutibilmente connesso a quello di archiviazione perchè ogni dato che visualizziamo rischia di essere vittima dell'oblio se non viene opportunamente conservato. Memorizzare è un fatto personale, ma talvolta potrebbe essere anche una scelta obbligata.

Con l'avvento di internet si è assistito ad un rapido cambiamento delle modalità di archiviazione, conservazione e recupero dei dati, con l'effetto più evidente di un incremento esponenziale della quantità di dati da archiviare. Non solo: i dati devono poter essere recuperati in tempo reale, ed in qualsiasi momento, 24 ore su 24 e 7 giorni su 7. Le possibilità offerte dalla tecnologia non mancano certo di soddisfare gli utenti e gli utilizzatori avanzati. Infatti la possibilità di archiviazione è ormai divenuta dell'ordine dei terabyte, quindi la possibilità di immagazzinare una quantità praticamente infinita di dati e informazioni. Non sempre è necessario che le copie dei dati siano archiviate su supporti ad elevata velocità, in quanto magari si è realizzata la memorizzazione degli stessi per esigenze d'archivio. Quindi è preferibile utilizzare supporti differenti dai dischi rigidi, quali ad esempio i nastri, più volte dichiarati come tecnologia in disuso, ma di fatto ineguagliabili in termini di rapporto costo-prestazioni per determinate applicazioni di storage. A questi sistemi negli ultimi tempi si sono affiancati i NAS (acronimo di Network Attached Storage) che sono complementari a livello funzionale alle SAN (acronimo di Storage Area Network). Il problema collegato all'implementazione di questi sistemi di archiviazione è legato alla crescente complessità di gestione delle risorse di storage. In pratica la ricerca immediata dell'informazione è correlata alla necessità di effettuare backup e recovery in tempi rapidissimi. Mentre un tempo la logica portava a considerare il backup come una operazione notturna della durata di parecchie ore, adesso assistiamo allo sviluppo di sistemi di archiviazione che consentono di copiare e archiviare solo i blocchi modificati successivamente all'ultimo backup incrementale e tutto ciò mentre il sistema fornisce informazioni agli utilizzatori. Il fermo macchina è un concetto inaccettabile, mentre un tempo era visualizzato nell'immaginario collettivo dei tecnici come la necessità naturale di manutenzione dei sistemi informatici. Questa situazione che riguarda tutti i dati digitali presenti in azienda, strutturati e non strutturati, si complica maggiormente nel caso di quelli del secondo tipo, infatti le informazioni non strutturate (o fixed content o informazioni referenziate) sono quelle informazioni non modificabili nel tempo, che devono essere disponibili con possibilità di accesso veloce e possedere altresì un riferimento univoco; inoltre questo tipo di informazioni ha generalmente una dimensione maggiore rispetto a quella dei dati strutturati. Un aspetto a se stante ma conseguente a questa differenziazione è rappresentato dalle implicazioni legali e amministrative collegate alla gestione dei dati: la conformità alle normative vigenti comporta talvolta l'obbligo di gestire tutti i dati come se appartenessero al secondo gruppo, con l'aggiunta della richiesta di non modificabilità del dato (vedi ad esempio i documenti di tipo fiscale). ◆

Una materia per fronteggiare possibili scenari di rischio

L'importanza di acquisire una capacità strategica per poter rispondere ad incidenti e continuare l'attività ad un livello accettabile.

ANTHONY CECIL WRIGHT
SOCIO CLUSIT, PRESIDENTE ANSSAIF



Che cos'è la Business Continuity? Lo Standard BS25999-1 dà la seguente definizione "strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable pre-defined level"[1].
In pratica è una disciplina che mette in grado un'Azienda di adottare formalmente l'approccio reputato più idoneo a fronteggiare possibili scenari di rischio (ad esempio: un terremoto; un black-out; un incendio; un sabotaggio; ecc.), derivanti dal verificarsi di eventi causali che, sfruttando le vulnerabilità di uno o più asset (sistemi informatici, infrastrutture; persone; ecc.), impediscono di ottemperare ad obblighi istituzionali o provocano danni in grado di influire sulla capacità dell'azienda di continuare la propria attività di business. In passato l'attenzione delle Organizzazioni era principalmente diretta alla salvaguardia del patrimonio informativo, mediante la progettazione e la realizzazione di soluzioni di Disaster Recovery, la cui caratteristica principale era la ridondanza dei supporti magnetici e la disponibilità, all'occorrenza, delle necessarie attrezzature informatiche e di comunicazione posizionate in un altro sito, la cui distanza dal sito primario era funzione dei possibili scenari di rischio. Oggigiorno generalmente le aziende si sono dotate di un piano di Disaster Recovery (DRP).
Gli investimenti sono stati assai elevati, così come lo sono i costi di gestione; infatti, i costi sono crescenti in modo quasi esponenziale al diminuire del tempo massimo accettabile per la ripresa dell'operatività, interrotta da un evento imprevisto.

Il progetto per il DRP è stato generalmente portato avanti dalla funzione interna informatica.
Come vedremo più avanti, la Business Continuity (BC), invece, coinvolge tutta l'Azienda: dalla fase di analisi dei rischi, alla valutazione dell'impatto economico di un'interruzione coinvolgendo i "process owner", sino alla valutazione del Top Management sui rischi da accettare e quelli da mitigare. Non ultimo, in quasi tutte le realtà che hanno realizzato il piano di BC, lo sponsor aziendale è stato il Consiglio di Amministrazione (nel caso delle banche e degli intermediari finanziari, la normativa ne prevede già un forte coinvolgimento) e ciò ha assicurato un forte "committment" di tutta l'Azienda ed un giusto equilibrio costi / rischi .
Le soluzioni adottate si traducono, infine, in piani di continuità, nei quali sono descritti i ruoli, le responsabilità, le procedure da seguire, gli strumenti da utilizzare, e quanto altro serve per poter riprendere l'attività interrotta.

Trattasi perciò di un processo di ricerca di soluzioni condivise di limitazione dei danni, soprattutto preventive, ma anche di emergenza, consentendo l'operatività di quei processi di business che comporterebbero elevati danni economici già nelle prime ore di interruzione.

Se ritorniamo per un attimo al tema dei costi relativi al Disaster Recovery, come si può comprendere da quanto anzidetto, il tempo massimo accettabile di interruzione dell'operatività, ottenuto nel corso del ciclo di Business Continuity Management, è fondamentale per decidere quale soluzione di DRP adottare e, pertanto, è importante per un corretto equilibrio costi / rischi.
Ciò spiega perché la Business Continuity include il DR.
L'attenzione alla BC e lo sviluppo della metodologia sono praticamente nati dopo l'11 Settembre 2001, e si sono perfezionati nel corso di questi ultimi anni.
Il tragico evento ha messo in luce, come sappiamo, alcuni fatti innovativi: l'accadere di un evento prima di allora giudicato assolutamente improbabile (uso di aerei da attentatori suicidi; due enormi grattacieli colpiti...); ma, soprattutto, la perdita di tante persone, oltre ad uffici, sistemi e documenti cartacei.
Vi è stato anche un secondo evento, rappresentato dall'epidemia di SARS in Asia nel 2003.
Il numero di vittime è stato limitato, ma invece alto è stato il numero di Aziende che hanno dovuto interrompere improvvisamente le loro attività a causa dell'assenza di personale, in quanto ricoverato in ospedale o messo al domicilio coatto, in quarantena. Molte di queste sono fallite nei successivi due anni.
In Italia un grande impulso è derivato dall'esperienza che le Banche hanno fatto, a seguito dell'applicazione dell'accordo di Basilea sul capitale di rischio e alla normativa della Banca d'Italia, la cui preoccupazione – in linea con le altre Banche Centrali - deriva dai possibili impatti sul sistema finanziario italiano che si possono avere a seguito di eventi catastrofici.
Le banche, che hanno terminato nei tempi stabiliti i rispettivi progetti[2], hanno messo a disposizione un forte know-how basato sull'esperienza diretta. In particolare, si è potuto vedere che la maggioranza delle soluzioni di continuità adottate dalle Banche hanno sfruttato le persone e le infrastrutture esistenti, evitando così investimenti per duplicazioni.
In alcuni casi, sono stati formalizzati degli accordi con Società di Servizi in grado di prendere in carico parte dell'attività dell'Azienda. Molti di questi contratti non hanno richiesto l'esborso di somme anticipate.
Alcune significative esperienze consentono di affermare che implementare la BC non significa dovere affrontare elevati investimenti.
Intensa deve invece essere, da parte dell'Azienda, l'attività di sensibilizzazione del personale sul tema della continuità operativa e la formazione atta a consentire di mantenere correttamente l'impianto di BC.
Infatti, siccome l'Azienda non è immobile, non è statica, gli impatti mutano, così come le vulnerabilità, il livello di esposizione al rischio, il livello di accettazione dei rischi ("risk appetite"), ogni anno, o ad ogni variazione organizzativa significativa, l'Azienda deve ripercorrere il ciclo di BC (analisi del rischio, valutazione degli impatti, ecc.).
Importante, oltre alla formazione, è anche la simulazione, in quanto consente di ottenere vari vantaggi: provare l'efficacia dei piani redatti, familiarizzare e sensibilizzare il personale, abituare a prevedere, e a prepararsi ad ogni evenienza. L'esperienza ha dimostrato che dei potenziali disastri sono rimasti a livello di incidente, contenendo i danni, grazie proprio a questo approccio e allo spirito di squadra che si era creato fra il personale operante sui processi critici e quello tecnico di intervento. ◆

[1] "capacità strategica e tattica di una organizzazione di pianificare e rispondere ad incidenti e gravi interruzioni del business al fine di poter continuare l'attività di business ad un livello accettabile predefinito" [Trad. dell'Autore].

[2] La normativa, emanata nel luglio 2004, ha previsto l'adeguamento della continuità operativa ai nuovi scenari entri il dicembre 2006.

Il Premio Clusit per incoraggiare la ricerca universitaria

Al via la terza edizione del premio "Innovare la sicurezza delle Informazioni", riservato alle migliori tesi di laurea sulla materia. Il premio ha anche lo scopo di promuovere una collaborazione tra aziende, Università e studenti ed è già diventato un punto di scambio tra mondo produttivo e mondo scientifico, tra studenti e mondo del lavoro. Saranno premiate le 5 migliori tesi (2.000 Euro per il primo classificato).
Per un approfondimento: https://tesi.clusit.it/

Promozione, formazione e professionalità

Far crescere la cultura della sicurezza informatica in tutti gli ambiti è la missione primaria del Clusit. La tutela di una risorsa così critica come la rete dipende, infatti, dall'azione congiunta, consapevole e quotidiana di ciascuno, unita ad un alto livello di professionalità. Clusit organizza i seminari Clusit Education (https://edu.clusit.it) e collabora alla realizzazione di oltre 50 convegni all'anno. Clusit è il partner scientifico della più importante manifestazione fieristica del settore: Infosecurity Italia (www.infosecurity.it), la cui prossima edizione è prevista a febbraio 2008.

Mettere in sicurezza reti e sistemi di controllo

In un mondo ideale non ci sarebbe bisogno di porte, cancelli, lucchetti, allarmi e polizia. Ma come nel mondo reale anche il mondo virtuale ha bisogno di proteggersi da attacchi esterni e spesso accade anche che i sistemi vengano insidiati direttamente dall'interno.

A CURA DI **ENZO M. TIEGHI**
VISION AUTOMATION SRL - EMAIL: ETIEGHI@VISIONAUTOMATION.IT

Finalmente, purtroppo, si parla di security anche per reti e sistemi di controllo ed automazione.
Di security informatica si parla da diversi anni per i sistemi e le infrastrutture che ricadono sotto il dominio ICT (PC, reti Lan, reti wireless, server, router, switch, cablaggi, modem, ecc.). Certo, in un mondo ideale dovrebbe essercene bisogno, ma oggi, in molti là fuori (ma, attenzione, anche tanti qui dentro!) non vedono l'ora di farci passare qualche brutto quarto d'ora cercando informazioni e notizie preziose o spargendo qualcosa di malizioso nei nostri sistemi. D'altronde, nel mondo ideale non sarebbero necessari antifurti, lucchetti, serrature, armi e Polizia...
La tecnologia utilizzata oggi negli impianti di produzione, nei sistemi di controllo e di automazione di fabbrica è sempre più vicina (in pratica, diciamolo, la stessa) del mondo ICT (Information & Comunication Technology): reti Lan ethernet, protocolli IP, sistemi operativi Unix-Linux e Windows, ecc. I rischi però sono diversi: non si tratta della sola perdita di dati o informazioni, ma di lotti di produzione, danni ad impianti e macchinari, rischi di incidenti sul lavoro o di inquinamenti ambientali. Lo scenario ideale dal punto di vista della sicurezza informatica sarebbe quello di non mettere in comunicazione le reti di fabbrica e sistemi gestionali (utilizzando la tecnica del "cuscino d'aria" o air-gap) per fare in modo che le eventuali "contaminazioni" non arrivino ai sistemi di controllo e automazione.
Ci perderemmo però tutti i benefici dell'integrazione delle informazioni in fabbrica dei quali si parla da tanto tempo, per avere la fabbrica senza carta (paperless) e con tutti i sistemi che, dialogando tra loro, permettono la gestione ottimale sia del ciclo produttivo che della Supply Chain.
Ma forse non saremmo ancora "al sicuro"!
Figuriamoci: con tutti i media che abbiamo intorno (dai CD ai DVD, con fileMP3 e film ormai divulgatori di software malevolo della peggior specie quali worm, trojan, virus, ecc.) e con quelle micidiali "chiavette USB", ed ancora iPod e macchine fotografiche digitali che circolano come strumenti da "untori moderni", spesso inconsapevoli "portatori sani"...
E poi, non scordiamoci i modem collegati ai sistemi di automazione, laggiù negli armadi in fabbrica (spesso neanche censiti e sconosciuti agli utilizzatori dei sistemi) predisposti per la manutenzione remota. Tante minacce e vulnerabilità spesso sconosciute ai più.
Qualche tempo fa Eric Byres, esperto e ricercatore, in prima linea nello studio della Cyber Security in ambiente industriale, affermava: "Le vulnerabilità di Windows e Linux sono in genere ben conosciute e capite. Le vulnerabilità di sistemi di controllo e SCADA non sono capite e percepite. E' importante scoprire eventuali falle prima che i dispositivi critici "esposti" vengano installati in campo in produzione (ove poi sarebbe costoso intervenire) e prima che "cracker" possano scoprirle ed iniziare e sfruttarle".
L'importante è non solo parlarne, ma fare: mettiamo in sicurezza reti e sistemi di controllo!
Da tempo Clusit (Associazione Italiana per la Sicurezza Informatica www.clusit.it) porta avanti un'attività di divulgazione e training per aumentare la consapevolezza sul tema: è anche stata completata la scrittura del Quaderno "La protezione di reti e sistemi di controllo ed automazione (DCS, SCADA, PLC, ecc.)" ed a fine Giugno 2007 si è tenuta la Giornata di Studio sull'argomento cyber security industriale, la terza che ANIPLA (Associazione Italiana per l'Automazione www.anipla.it) organizza in tre anni, sempre patrocinata da parte di Clusit. ◆

L'impronta digitale

INTERVISTA AL **DOTT. ANGELO ATTIANESE,**
PRESIDENTE DI XELIOS ITALIA

Che cosa si intende per riconoscimento biometrico?
Le tecnologie biometriche attualmente esistenti afferiscono a tre categorie specifiche: l'analisi comportale, l'analisi biologica e l'analisi morfologica. Di queste la più utile è la terza, in quanto studia le impronte digitali, la geometria della mano e del volto, il disegno della rete venosa dell'occhio, l'iride e la retina, perchè questi elementi permangono in un individuo in modo stabile durante tutta la vita. I sistemi di analisi delle impronte digitali hanno raggiunto negli anni la piena maturità tecnologica, infatti questa tecnica è la più utilizzata e la più affidabile nell'impiego con grandi flussi di persone e anche quella meno invasiva e più scelta dagli utenti.

Qual è secondo Lei l'importanza della biometria nel telelavoro?
In un epoca in cui il nomadismo fa parte ormai delle abitudini di vita delle persone, anche il semplice cittadino vuole poter usare in modo sicuro un portale senza lasciare le proprie impronte o password in una banca dati centralizzata. Lasciare libero accesso dall'esterno senza garantire l'identità delle persone che si collegano può compromettere le misure di protezione applicate alla rete dell'ente. Un'autenticazione multi fattore permette di preservare la sicurezza del sistema informativo garantendo l'identità degli utenti distanti e rispettando le normative vigenti. Inoltre, l'ergonomia e la sicurezza di un sistema token-biometrico non sono in discussione. Un esempio concreto di applicazione è rappresentato dall'IVA o dall'e-voting. Sono disponibili sul mercato anche soluzioni di sicurezza personale costituite da dispositivi biometrici a chiave su porta USB per autenticarsi in modo sicuro e senza depositare informazioni sul computer da cui si effettua l'accesso.

Come è possibile combattere il problema del phishing con il riconoscimento biometrico? Come si garantisce ad un cittadino la dovuta mobilità rispetto a pratiche amministrative, magari di qualche ente pubblico?
Attraverso sistemi di autenticazione a distanza con un metodo multi fattore (token-bio) è possibile collegarsi senza rischio ad un sito governativo, a reti private, a siti di commercio elettronico o di banking online. Per raggiungere la massima sicurezza si sostituisce la semplice password con una procedura d'autenticazione forte. Ogni utente si vede attribuire un token biometrico che genera un codice, valido unicamente per il collegamento in corso. Quando gli è richiesto, l'utente presenta la sua impronta digitale (cio che è), e solo allora il token biometrico genera il codice unico (OTP One Time password – ciò che possiede). L'unione di questi elementi costituisce la prova dell'identità dell'utente. ◆

La nuova frontiera della sicurezza aziendale

I servizi di vigilanza degli Istituti Italiani tra tecnologia e professionalità degli operatori. Una scelta consapevole è possibile informandosi sulle risorse tecnologiche e sullo spirito di servizio.

Uno dei servizi in outsourcing più richiesto dalle aziende in questo periodo è relativo al settore vigilanza e sicurezza, perché risulta evidente che nessuna attività produttiva potrà funzionare in modo corretto se gli immobili, i macchinari, le attrezzature, il denaro contante e, non da ultime, le persone che lavorano, sono esposte alla mercè di terzi senza un adeguato livello di protezione.
La tutela dei beni è diventata una esigenza per contrastare la crescente diffusione della microcriminalità che colpisce i piccoli esercenti, e per porre un freno anche alla criminalità organizzata che, per scopi evidentemente illeciti, può sottrarre dei beni all'azienda colpita o danneggiarla gravemente. Nel caso per esempio di banche o aziende che gestiscono prodotti ad alto valore poi il problema si trasferisce direttamente alla tutela dei dipendenti della società, in quanto spesso le aggressioni a titolo di rapina sono causa di decessi e ferimenti tra il personale. L'assicurazione può intervenire per la copertura dei danni patrimoniale alle cose e alle persone, ma non potrà mai restituire una vita oppure rendere ad un clima aziendale la giusta serenità che è stata violata e compromessa.
Per intervenire contro queste spiacevoli evenienze sono nati, e sono proliferati negli ultimi tempi, numerosi istituti di vigilanza privata, sia essa armata o non armata, in grado di proporre alle aziende clienti dei servizi di controllo e sicurezza all'avanguardia.
Nel caso di aziende che trattano merci di valore ridotto, o difficilmente sottraibili per via diretta, si preferisce affidare l'incarico ad una sorveglianza non armata, che unitamente all'ausilio di strumenti elettronici e informatici di controllo, anche in collegamento con le forze dell'ordine, possa impedire una eventuale azione intrusiva o danneggiante.

Altro caso, ma nato dalle stesse premesse, è l'introduzione di un servizio di vigilanza armato in quei settori del credito, della tecnologia o dell'industria dove si teme un attacco improvviso e organizzato in grado di sottrarre beni e causare danni alle attività produttive e di ricerca (le nuove invenzioni ad esempio non hanno prezzo, e se vengono sottratte formule o piani di sviluppo il danno è irreparabile).
E' poi anche una questione d'immagine, pertanto l'azienda cliente preferisce mostrare ai proprio ospiti un grado di gestione della sicurezza avanzato, grazie a sistemi di telecontrollo e guardie giurate.
Per quanto concerne il ramo tecnologico, oggi si assiste ad uno scenario di nuovi ritrovati, utilissimi per la sorveglianza: telecamere per visione notturna con zoom in grado di identificare i particolari a centinaia di metri di distanza, sistemi antifurto perimetrali e di area molto sofisticati che agiscono tramite microonde e infrarossi, combinatori telefonici e sistemi di allarme radio con collegamento diretto ad un centro di controllo in grado di intervenire in diverse situazioni, come ad esempio ferimenti, incendi, sicurezza e problematiche di varia natura.
Il punto è che non esiste a priori una chiave magica per la soluzione di ogni problema di sicurezza e controllo, ma un buon istituto di vigilanza ha dalla sua l'esperienza e la tradizione di chi ogni giorno si confronta con le situazioni impreviste: la guardia non è un semplice strumento armato difensivo, ma quasi più una figura di riferimento per la tutela e l'integrità dello scenario al quale è stato assegnato.
Sia in postazione fissa, sia in ronda diurna e notturna, oppure in attività di pattugliamento, il servizio di sicurezza garantisce la protezione a beni e persone, scoraggiando l'azione di malviventi che trovando di fronte a sé un ostacolo obiettivamente efficace, possono desistere dal compiere azioni illecite. Il buon servizio di vigilanza, attraverso la professionalità specifica e le competenze dei propri addetti abituati alla dedizione e allo spirito di servizio, è una presenza sicura e stabile: non si fa sentire, ma c'è. ◆

Un metro di giudizio per la certificazione

DOTT. FABIO GUASCONI
CONSULENTE SGSI.NET - SOCIO CLUSIT

La fiducia è un elemento critico per prendere decisioni, nella vita di tutti i giorni e a maggior ragione nel business. Chi ha la responsabilità di scegliere ha la necessità di percepire in breve di cosa si può fidare e di cosa no.
Le certificazioni, specie dove un forte e dinamico aspetto tecnologico rende difficile l'orientamento, mirano ad offrire un metro di valutazione uniforme, anche a livello internazionale. Per ottenere ciò entrano in gioco degli attori fidati: i cosiddetti enti o laboratori di certificazione, che prendono in carico la valutazione di un'entità, e un sistema di accreditamento che effettua attività di controllo. In questo contesto chi promuove la certificazione è il produttore o il proprietario dell'entità in esame, per dimostrare ai suoi partner e clienti le qualità della stessa.
Nell'ambito della sicurezza delle informazioni (non solo informatica dunque), questa "entità" si scinde in due categorie ben distinte: prodotti e sistemi.
Una certificazione di prodotto, normalmente condotta secondo lo standard ISO 15408 tratto dai noti "Common Criteria", viene effettuata presso un laboratorio adeguatamente attrezzato. In base alla tipologia del prodotto e al livello di sicurezza che si vuole certificare (crescente da EAL1 a EAL7), sono definite le caratteristiche di sicurezza nonché le modalità della loro verifica. In caso di superamento di tutte le verifiche stabilite viene emesso il certificato. A titolo di esempio IBM DB2 è stato certificato EAL4+.
Una certificazione di sistema segue invece la più estesa impostazione tracciata dalla ISO/IEC 27001 (nato dalla BS 7799), che consiste nell'instaurare un processo di gestione della sicurezza di tipo trasversale, orientato sia agli aspetti tecnologici sia a quelli organizzativi della sicurezza nell'azienda. Gli enti di certificazione eseguono delle visite periodiche presso l'azienda per valutare la conformità del sistema alla norma e, in caso positivo, rilasciano il certificato. Sempre per citare un esempio, Intesa SanPaolo ha certificato alcuni suoi servizi.
In Italia il mercato in questo settore sta ancora muovendo i primi passi, mentre in altri paesi quali l'Inghilterra è ben più maturo. Tale situazione concede però alle aziende che decidono di intraprendere ora questo percorso l'opportunità di ottenere un rimarcabile vantaggio d'immagine e di valore aggiunto sui competitors, oltre ai benefici derivanti da una migliore gestione degli investimenti e da un ridotto impatto degli incidenti legati alla sicurezza. ◆

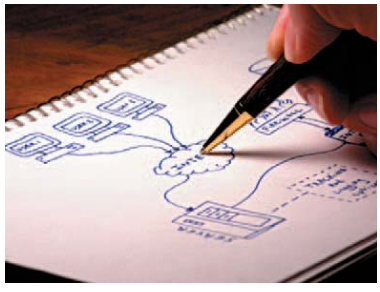
Le Certificazioni, importante strumento per il business

Le certificazioni più richieste dalle aziende sono quelle relative alla qualità, oggi considerate come un fattore determinante per valutare il grado di efficienza di una realtà produttiva.

Sono molteplici le certificazioni richieste da una azienda per poter migliorare la propria struttura e potersi interrelazionare ottenendo più fiducia verso clienti, fornitori e partner.
A titolo non esaustivo sono citabili le seguenti certificazioni: marchio CE, Marcatura Europea, certificazione di attrezzature navali, certificazioni di sistema e di prodotto ISO 9000 QS9000 ISOTS16949, dell'ambiente EMAS e ISO 14001, della salute e sicurezza OHSAS 18001, della responsabilità sociale SA 8000 e Codici di Condotta, della certificazione di prodotto e agroalimentare, ecc.
Tra le certificazioni più richieste vi sono quelle relative alla qualità, essendo considerata come un fattore determinante per la valutazione del grado di efficienza di una realtà produttiva o di servizi.
Nell'ambito della qualità ne individuiamo tre fondamentali: l'ISO 9000 identifica una serie di norme e linee guida sviluppate dall'ISO, che propongono un sistema di gestione per la qualità, pensato per tenere sotto controllo i processi aziendali indirizzandoli alla soddisfazione del cliente, l'ISO 9001 per la definizione dei requisiti dei sistemi qualità e l'ISO 9004 che è una linea guida per il miglioramento delle prestazioni delle organizzazioni. Attualmente le ISO 9000 sono usate in industria come modello di riferimento per la qualificazione e la selezione dei fornitori e nei contratti tra fornitori e clienti. In particolare nei rapporti con i fornitori la ISO 10005 individua delle linee guida per il piano di qualità, che ogni fornitore dovrebbe adottare per garantire le clausole contrattuali nei confronti delle aziende clienti: il piano di qualità risulta necessario per esplicitare nei confronti del cliente le regole di comportamento del proprio sistema. In Italia e in Europa, si sta diffondendo notevolmente la richiesta di certificazioni.
Per alcuni settori, soprattutto in relazione ai concorsi pubblici (appalti e bandi), la certificazione è obbligatoria e la si ottiene attraverso un ente certificatore. ◆

Il riconoscimento delle competenze: la certificazione CISSP

La certificazione CISSP (Certified Information Systems Security Professional) è una qualifica di eccellenza a livello mondiale che permette di riconoscere chi veramente ha competenze e professionalità in materia di ICT Security e accresce il ritorno degli investimenti fatti da ogni organizzazione in ambito informatico.
Nel mondo i Professionisti certificati CISSP sono 48.598, distribuiti in 126 paesi, di cui 176 in Italia.
Dal 2004 Clusit organizza a Milano e a Roma i seminari di preparazione all'esame CISSP e gli esami.
Il prossimo seminario si terrà a Roma la settimana dal 22 al 26 ottobre e l'esame il 24 novembre.
Per un approfondimento: www.clusit.it/isc2



"Online Sicuro": un progetto di Web Security Awareness e assistenza on line per cittadini e piccole/medie imprese

Si tratta della realizzazione di un portale che illustrerà al cittadino le principali problematiche di sicurezza relative all'utilizzo di Internet: la sicurezza del proprio pc, la sicurezza delle transazioni on line, l'e-government, la tutela dei minori su Internet, i virus, la posta elettronica, la Privacy, la tutela dei diritti d'autore, lo spamming, il phishing, ecc. Alle imprese illustrerà: le misure minime di sicurezza, gli obblighi di legge, la gestione della sicurezza in azienda, la business continuity e la gestione delle crisi, la formazione e la certificazione del personale addetto ai sistemi, ecc. Ma la parte più innovativa del portale, che sarà operativo entro fine anno, consiste in un servizio di assistenza on line per il cittadino: una sorta di 113 informatico. L'iniziativa sarà promossa direttamente dalla Presidenza del Consiglio dei Ministri e vedrà il coinvolgimento delle Confederazioni Industriali, di Confcommercio e delle Associazioni dei Consumatori. Le attività saranno coordinate da Infosecurity Italia e portate avanti dal Clusit e dal CERT.IT (Computer Emergency Response Team c/o il Dipartimento di informatica e Comunicazione dell'Università degli Studi di Milano). L'operazione sarà finanziata da un gruppo di aziende private (appartenenti sia al settore IT che al mondo industriale, finanziario e dei servizi). ◆

Internet: sicuri vuole dire conoscere

Gli utenti di internet e delle nuove tecnologie informatiche sono milioni, ma sono ancora relativamente pochi coloro che hanno affrontato con attenzione uno studio connesso all'utilizzo di questi strumenti così versatili, ma anche così pericolosi.

Abbiamo osservato la crescente diffusione di sistemi informatici e di reti di telecomunicazioni, a cui è seguita la nascita di nuovi servizi e forme di comunicazione che sono oggi disponibili ed utilizzate da milioni di utenti attraverso la rete Internet.
Questa straordinaria evoluzione di tecnologia ha determinato una sostanziale modificazione nelle abitudini degli utilizzatori di certi servizi, quali quelli di informazione o di acquisto, in quanto oggi è naturale consultare un quotidiano on-line (o più quotidiani) ed effettuare degli acquisti a grande distanza senza neanche alzare il telefono.
Come è intuibile, ogni nuova tecnologia rappresenta contemporaneamente una opportunità ma anche un rischio, in quanto lo strumento è utile se risulta libero da minacce e se non risente di azioni fraudolente operate da chi sfrutta la novità tecnologica per raggiungere fini illeciti.
A volte la responsabilità è anche negli utilizzatori che hanno poca confidenza con gli strumenti informatici, vittime di un atteggiamento superficiale e di una scarsa comprensione dei rischi legati ad un uso improprio del mezzo tecnologico in un contesto di infrastruttura di rete mondiale. Ciò che viene affrontato a più riprese, in interventi formativi più o meno diretti da parte degli esperti, è il tema della "Sicurezza in Internet e nelle nuove tecnologie informatiche", perché questo ambito rappresenta una vera e propria necessità per tutti gli utilizzatori, ovvero è un elemento fondamentale per poter usufruire dei molteplici servizi oggi disponibili. Sono nate iniziative a favore della conoscenza del problema sicurezza da parte di numerose organizzazioni, commerciali e non, per introdurre una coscienza sul problema a livello sociale, determinando quindi un atteggiamento prudenziale verso un utilizzo troppo "frivolo" del mezzo informatico.
Vale la pena di ricordare che sono proprio gli utenti a inserire i dati delle proprie carte di credito o a divulgare informazioni non autorizzate circa le proprie credenziali di accesso a banche e sistemi protetti, perché non si accorgono del pericolo incombente durante la sessione di collegamento. A livello internazionale è diffusa una definizione ottimale in relazione al problema informatico evidenziando che l'atteggiamento necessario a risolvere queste imprudenze è una "cultura della sicurezza" ("Linee guida dell'OCSE sulla sicurezza dei sistemi e delle reti d'informazione: verso una cultura della sicurezza" 25 luglio 2002). Ciò che ci si aspetta da un approccio informato al discorso è trattare i cardini formativi della sicurezza sotto i profili di Internet e le reti geografiche, la sicurezza delle reti e dei servizi, i sistemi di navigazione e le autenticazioni, la cifratura dei dati e i tunnel virtuali. Queste sono le aree principali per conoscere con esattezza i problemi legati ad internet e alle nuove tecnologie informatiche. Occorre inventare un approccio formativo in un contesto flessibile in grado di arricchirsi di nuovi contributi e approfondimenti, seguendo le esigenze e la natura stessa del progetto educativo: avvicinare l'utente al concetto di sicurezza informatica per il raggiungimento di una maggiore consapevolezza nell'utilizzo di Internet e dei suoi servizi. Nel corso degli ultimi anni sono stati attivati da parte di consorzi universitari, aziende private, enti didattici accreditati, aziende e docenti, numerosi corsi di formazione e master collegati alla sicurezza informatica e all'approccio ad un utilizzo consapevole dei mezzi informatici. L'utilizzatore aziendale con l' intervento in loco del formatore o ancora meglio, attraverso internet grazie ai corsi online, è in grado di acquisire una maggiore conoscenza del settore intervenendo sulle proprie debolezze e costruendo intorno a sé una barriera contro gli attacchi di soggetti malevoli (virus, spyware, hackers e quant'altro) a vantaggio della propria sicurezza, del proprio lavoro, e del patrimonio dell'impresa nella quale opera. ◆

Soluzioni a 360°

Gruppo italiano leader nei servizi integrati con tecnologie innovative

GRUPPO VIESSE
Agenzia per il Lavoro

GRUPPO VIESSE
Facility Management

Ad Interim
Somministrazione e Staff Leasing

COMAFO
Costruzioni e Manutenzioni

ADDA
Grande Ristorazione

Ad Competence
Ricerca e Selezione

people raising
persone per progetti non profit

Ad Personam
Outplacement e Consulenza Carriera

contaplus
Persone per aziende che contano

adinterim.it | comafo.it | addaristorazione.it | gruppoviesse.it

Siamo strutturati in 9 divisioni per fornire ai nostri CLIENTI servizi specializzati con competenze e capacità che, possono agire in modo autonomo o integrato fra loro, nei settori di: **Facility Management, Global Service, Outsourcing & Problem Solving,Somministrazione e Staff Leasing, Ricerca & Selezione, Outplacement & Consulenza di Carriera.**

Numero Verde
800 029 455

GRUPPO VIESSE - Agenzia per il Lavoro - Autorizzazione Ministero del Lavoro 22.12.2004 Prot. 1235-SG