

Sicurezza ICT

soluzioni e tecnologie per proteggere l'azienda

Introduzione

Il tema della sicurezza è oggi sentito in modo prioritario dai responsabili dell'IT delle imprese e da tutte le figure chiave all'interno dell'azienda ormai consapevoli dell'importanza di una corretta politica di gestione della sicurezza.

Le aziende italiane continueranno nel prossimo futuro a investire fortemente in sicurezza, ma cercheranno di misurare questo investimento con parametri agganciati direttamente alle priorità dell'impresa: in ottica di gestione del rischio complessivo (di subire danni o frodi, di danneggiare la propria immagine verso clienti e partner, di trovarsi impreparati per particolari normative o nuovi sviluppi della tecnologia), e con valutazioni legate in ogni caso a un "livello di rischio accettabile".

Il mercato cresce in Italia, oggi più che in passato, grazie a una maggiore adozione di soluzioni che abbassano il rischio complessivo, anche se ancora molto può essere fatto per ridurre la complessità dei processi e le numerose difficoltà associate alla gestione della sicurezza ICT. Elemento di successo è e sarà quindi la capacità non solo di conoscere ma soprattutto di "anticipare" gli strumenti e i processi che caratterizzeranno una corretta politica di sicurezza aziendale sia verso l'interno sia verso l'esterno.

Agenda

Sicurezza informatica: una questione di cultura e organizzazione

- Metodologie di analisi del rischio
- Definire una politica di sicurezza aziendale
- Tipologia di attaccante
- Penetration test. Cosa sono?

Sistemi di autenticazione

- Password
- Tool di cracking locali e distribuiti
- Smart card e token come repository dei dati di autenticazione
- Sistemi biometrici
- Il sistema di autenticazione Kerberos, RADIUS, TACACS
- Panoramica sulle principali funzionalità di sicurezza dei sistemi operativi più utilizzati

Sistemi connessi: il rischio di essere in Internet

- Vulnerabilità della suite ipv4
- Le debolezze dei protocolli di rete più utilizzati
- Attacchi Eavesdropping
- IP Spoofing
- Arp poisoning
- Connection Hijacking
- Social engineering (presentazione di un caso reale)
- Attacchi guidati dai dati (data-driven): virus, malicious scripts, trojans hourses (presentazione di due caso reali)
- Pishing (presentazione di un caso reale)
- Attacchi DoS (Denial of Service)
- Hackers: anatomia di un attacco via Internet

Sistemi per la difesa dalle intrusioni via Internet: Firewall

- Firewall 2.0
- WAF - *Web Application Firewall*
- Proxying
- Circuit level proxying
- Stateful inspection
- Architetture di firewall: indicazioni per la scelta
- Panoramica su alcuni prodotti commerciali ed open maggiormente diffusi
- IDS e IPS

Lo scambio sicuro di informazioni in rete: tecniche di base

- Il problema del man-in-the-middle
- L'inizializzazione di un sistema crittografico e la sua gestione
- Perché introdurre la crittografia: soluzioni commerciali ed open attualmente disponibili
- Infrastrutture a Chiave Pubblica (PKI)
- Il ruolo dei diversi attori di una PKI (CA, RA)
- SSL, CACert (rilascio punteggi in quanto certificatore)

La sicurezza delle comunicazioni IP

- Definizioni e scenari di utilizzo
- Sicurezza e insicurezza nelle reti Wireless (esempio pratico in aula e presentazione di un caso reale)
- Protocolli per il tunneling dei dati su Internet: L2TP, PPTP
- Servizi di sicurezza per le VPN: l'architettura IPSec.
- Prodotti commerciali ed open

La sicurezza dei servizi applicativi

- Posta elettronica sicura (PGP, S/MIME, SALS, TSL, IMAPS, POP3S)
- Soluzioni anti-spamming: applicazioni e tecnologie emergenti (SPF - Sender Policy framework, Greylist, RBL)
- Accessi sicuri in emulazione di terminale (telnet sicuro tramite SSH)
- Accesso sicuro ai servizi WWW (SSL)
- Soluzioni crittografiche per la protezione dei dati residenti su PC
- Vulnerabilità dei sistemi SMTP: come sfruttare le malconfigurazioni dei server di posta
- Tecniche di spamming e nuovi vettori di attacco degli spammer
- Soluzioni anti-spamming: applicazioni e tecnologie emergenti (SPF - Sender Policy framework, Greylist, RBL)
- Policy e best practices per prevenire e mitigare il fenomeno dello spamming

L'aggiornamento sui temi della sicurezza

- Vigilanza continua: la sola tecnologia non basta
- Le mailing-list ed i siti più importanti
- I siti dei produttori del software
- Organismi ed enti di informazione
- Aspetti Normativi: legge sulla privacy 196/2003
- Certificazioni

Metodologie didattiche

Il corso si svolgerà basandosi su casi studio, simulazioni, demo di prodotti applicativi di auditing e di analisi dei rischi, discussioni sulle tecniche di difesa e sugli strumenti di prevenzione. Questo affinché sia il più concreto possibile l'approccio e la conoscenza di tematiche quali l'Analisi dei rischi e valutazione delle Vulnerabilità aziendali.

Le lezioni saranno svolte in modo tale da favorire al massimo il processo d'apprendimento. Il materiale didattico comprende il manuale del corso che integra l'intera collezione delle diapositive mostrate con note, commenti, esempi e casi di studio. Una nutrita raccolta di documentazione e programmi di utilità sarà inoltre distribuita in CD-ROM.

Ad ogni partecipante sarà rilasciato un attestato di partecipazione certificato da NCP.

Obiettivi

Il corso analizza le problematiche relative alla protezione delle reti e delle applicazioni di rete e fornisce un'ampia panoramica delle tecniche di protezione. I partecipanti, al termine del corso, saranno in grado di comprendere i rischi presenti nelle loro architetture e di approntare le soluzioni più idonee a proteggere il proprio sistema.

Destinatari

Il corso è rivolto a chi si occupa di sviluppo, gestione ed organizzazione di reti di calcolatori e di applicazioni di tipo Internet, Intranet ed Extranet..

Prerequisiti

Il corso affronta una ampia panoramica delle problematiche inerenti il mondo Internet e i suoi protocolli. E' consigliata la conoscenza degli argomenti del corso Basic IP Tutorial.