Servizi di sicurezza informatica

Net inventory

Questo tipo di servizio consiste nell'effettuare un'accurata valutazione della rete intera e dei dispositivi presenti in essa.
Vengono quindi identificati tutti i componenti hardware e software installati, in modo da rafforzare gli standard contro i rischi di furto di dispositivi, l'installazione di software non autorizzato e l'adeguamento alla politica delle licenze aziendali.
Il servizio prevede la generazione di report dettagliati, grazie ai quali i dipartimenti di information technology hanno la possibilità di effettuare corrette valutazioni in relazione ai piani di sviluppo strategico e finanziario.

Hardening dei sistemi

I sistemi operativi più diffusi, Windows e Unix, sono spesso installati in modo incompleto, incongruo o con l'assegnazione di privilegi a operatori spesso non giustificati; inoltre, le case madri rilasciano periodicamente nuovi aggiornamenti del software di base a fronte dell'individuazione di vulnerabilità; tutto ciò richiede un costante monitoraggio dei sistemi operativi.
L'obiettivo dei progetti di hardening è quello di sviluppare un set di modifiche al sistema operativo di riferimento che lo rendano più sicuro.
Normalmente le operazioni di hardening vengono realizzate sui sistemi ritenuti ad alta criticità, per i quali il livello di availability e reliability deve essere alto.

Security scanning

Il security scanning è il servizio più comune offerto ed anche quello più richiesto dalle aziende; consiste nella ricerca di vulnerabilità della rete aziendale per mezzo di strumenti software avanzati.
Il security scanning viene effettuato on site e normalmente viene suddiviso in due fasi:

- vulnerability assessment;
- penetration test.

La fase di valutazione delle vulnerabilità parte solitamente da un database e consiste nella analisi di criticità note, parametri di configurazione, privilegi degli account, registry e servizi abilitati.
Il penetration test, invece, ha lo scopo di simulare tentativi non autorizzati di accesso a server o a singoli client della rete, sfruttando le più aggiornate tecniche conosciute.
Un aspetto importante dei servizi di security scanning riguarda la documentazione prodotta. Vengono prodotti report che comprendono informazioni ricavate dai tool di scansione e analisi e documenti contenenti tutti i dati sulle attività svolte, le macchine analizzate, le vulnerabilità individuate e le soluzioni da completare.

Auditing

Questo tipo di attività consiste nell'effettuare un controlo periodico e un'analisi sui file di log dei firewall o degli IDS (Intrusion Detection System) installati sulla rete.
L'analisi ha come obiettivo quello di individuare elementi significativi e tracce che consentano di risalire a tentativi d'intrusione.
Le attività di auditing prevedono la redazione di un report contenente un elenco dettagliato dei tentativi d'intrusione individuati e informazioni generali di carattere statistico sull'utilizzazione delle risorse.

Intrusion detection

Tali servizi riguardano una serie di attività di monitoraggio che vengono effettuate sui dispositivi di rete; sono condotti essenzialmente in tempo reale e permettono di individuare eventuali tentativi di intrusione, alterazioni delle configurazioni di riferimento standard secondo le policy prestabilite e, più in generale, problemi di incongruenza sistemistica.
I dispositivi utilizzati integrano procedure per la gestione delle funzioni di alerting e dispatching attraverso sistemi di messaggistica differenziata.
L'implementazione di questi strumenti consente di controllare in maniera costante eventuali tentatvi di attacco.

Incident handling analysis

Dopo un attacco informatico, è necessario effettuare un'analisi dettagliata dei sistemi dell'intero network.
L'obiettivo dell'indagine consiste nel comprendere ed individuare le cause che hanno reso possibile l'attacco, le vulnerabilità utilizzate come veicolo d'ingresso alle risorse ICT, le modifiche delle regole di accesso ai sistemi, l'individuazione di virus Internet-enabled, back-door e trojan horse.
Una volta ricostruita la tecnica utilizzata e la dinamica dell'attacco, sarà possibile introdurre le misure protettive più idonee per evitare ulteriori tentativi d'intrusione.

Remote security management

Le attività di gestione remota della sicurezza dei sistemi, siano essi server oppure workstation, vengono realizzate mediante l'installazione sul client di componenti dedicati che consentono il monitoraggio e la gestione a distanza. Il flusso dei dati fra la società di MSS e il client avviene sempre in modalità protetta attraverso l'implementazione di una VPN crittografata.