Poliziamoderna

A prova di hacking

Cnaipic - Integrità dei sistemi informatici e telematici La sempre più ampia diffusione dell'information technology e dei servizi telematici che stanno via via soppiantando le tradizionali forme di comunicazione cartacee, pone la necessità di garantire un elevato grado di affidabilità, integrità e sicurezza dei sistemi informatici e delle comunicazioni telematiche. Di fatto, negli ultimi anni e, ancor di più negli ultimi mesi, si è riscontrato un aumento esponenziale delle attività illecite poste in essere sulla rete internet mirate non soltanto a crimini economici ma anche al furto di informazioni. Basti pensare alle molteplici divulgazioni di dati sensibili sottratti, a seguito di intrusioni informatiche, all'interno di reti e server governativi e/o di grandi aziende di ogni tipo. Si ravvisa, ogni giorno di più, la necessità che gli amministratori di rete e di sistema delle varie infrastrutture informatiche elevino, anche avvalendosi di opportuni strumenti, il livello di allerta sulla sicurezza. Premettendo che la gestione della sicurezza è un processo in continua evoluzione che non può mai ritenersi evaso o esaurito, gli addetti al settore possono avvalersi di diversi strumenti sia hardware che software per agevolare i compiti di difesa delle proprie strutture informatiche. Prima di tutto, una corretta progettazione della rete intranet che preveda domini e sottodomini opportunamente separati da classi di rete differenti interfacciate tra loro, mediante l'utilizzo di firewall; un perimetro esterno della rete intranet ermetizzato il più possibile che consenta l'erogazione verso il mondo internet dei soli servizi strettamente necessari peraltro accessibili solo in zone appositamente predisposte denominate Dmz (zona demilitarizzata); l'adozione di specifici strumenti per l'analisi in tempo reale del traffico di rete come Intrusion Detection System o Intrusion Prevention System, sistemi antivirus centralizzati costantemente aggiornati, non sono che alcuni esempi di precauzioni che dovrebbero essere adottate non per garantire l'inviolabilità della propria network ma solamente per gettare le basi su cui costruire il processo della sicurezza. Infatti tutto l'hardware e il software in commercio risultano inutili se non affiancati da concrete risorse umane dedicate alla costante analisi delle evidenze e degli alert che i suddetti strumenti quotidianamente producono. Le minacce alla così detta sicurezza informatica sono in continua evoluzione, le tecniche di hacking in continuo sviluppo, metodologie sempre più elaborate e raffinate vengono adottate per scrivere worm e/o per penetrare nei sistemi informatici. Una costante manutenzione dei sistemi informatici con la tempestiva adozione di tutte le patch periodicamente rilasciate dai produttori di software e di hardware, l'adozione di opportune policy che garantiscano le misure minime di sicurezza, come la complessità e la scadenza delle password di login e delle caselle di posta, l'adozione di filtri basati su blacklist di siti malevoli e domini di spam, la crittografia dei dati sensibili residenti sui server, costituiscono dei punti essenziali su cui ogni amministratore di rete deve porre la propria attenzione. Ultima, ma non per ordine di importanza, risulta essere la formazione dei dipendenti e l'adozione, da parte loro, di adeguate policy comportamentali. Non di rado infatti si è riscontrato che l'anello debole della catena è risultato proprio l'elemento umano che ha posto in essere comportamenti incauti come, ad esempio, l'utilizzo di dispositivi di memoria usb infetti nei pc aziendali, l'apertura di file allegati ad e-mail di dubbia provenienza, ecc. oppure è caduto nei tranelli tesi dagli aggressori mediante tecniche di ingegneria sociale. **Gravi fenomeni criminali in danno dei sistemi e servizi di monetica e di home banking** La costante e continua evoluzione delle aggressioni ai sistemi di pagamento elettronico e dei servizi di home banking ha reso necessario l'affinamento di adeguate strategie di prevenzione e di repressione. Degno di rilievo, in tal senso, un protocollo d'intesa tra la polizia postale e delle comunicazioni e i principali istituti di credito, le società di emissione delle carte elettroniche di pagamento, gli intermediari e i fornitori delle infrastrutture telematiche a supporto delle transazioni finanziarie elettroniche. Il progetto, finanziato dalla Commissione Europea e ispirato a realizzare le più utili sinergie tra i settori pubblico e privato, è incentrato nell'avvio di innovative procedure di condivisione di dati per il rilevamento precoce di situazioni sospette. In merito è già in fase di sperimentazione ed avrà piena operatività nel primo semestre 2013, una piattaforma informatica di analisi sviluppata nell'ambito del progetto europeo OF2CEN – On line Fraud Cyber Centre and Expert Network, che vedrà collegati tutti gli istituti convenzionati con il Servizio polizia postale e delle comunicazioni e le sue ramificazioni periferiche. *Importanti i risultati dell'attività investigativa* Nell'anno in corso la specialità ha arrestato complessivame

...

01/03/2013