PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 8 - numero 1605 di martedì 05 dicembre 2006

Minacce interne

Anche i dipendenti possono essere un pericolo per le reti informatiche aziendali. Le motivazioni, gli attacchi più frequenti.

Pubblicità

Vendetta. E' questa la motivazione più frequente che spinge dipendenti o consulenti aziendali ad attaccare, in vario modo, la rete informatica aziendale.
Il dato emerge da uno studio realizzato dal servizio segreto USA e dal CERT della Carnegie Mellon University, nel quale sono stati descritti i tratti e motivazioni più frequenti degli attacchi informatici condotti da persone di fiducia interne alle aziende, quali dipendenti e consulenti.

Le minacce "interne" risultano molto più dannose, in proporzione, rispetto agli attacchi portati da hacker esterni, in quanto dipendenti e consulenti sono considerati affidabili e, quindi meno controllati.

Attacchi più comuni portati da personale interno**.**
- **Sabotaggio**: distruzione fisica di parte dell'infrastruttura IT o dei sistemi collegati.
-**Furto di informazioni o di beni**: sottrazione di informazioni digitali, furto di documenti cartacei, furto di oggetti informativi fisici.
-**Inserimento di 'bad code'**: bombe a tempo, ossia software programmato per danneggiare un sistema in un certo momento, e le bombe logiche, che si attivano non a tempo ma secondo determinate condizioni.
- **Virus**: il portatore di virus più pericoloso è sempre l'utente disattento, ma anche gli insider usano introdurre virus nelle loro imprese.
-**Attacchi a livello di protocollo**: DNS spoofing, TCP sequence, hijacking delle sessioni TCP/IP, Denial of Service...
-**Attacchi a livello di sistema operativo** - Sono portati soprattutto da parte di utenti tecnici e con privilegi di accesso, che sanno quali vulnerabilità ci sono nei loro sistemi e quali non sono state corrette con patch.
- **Social engineering** - L'ingegneria sociale è ancora un mezzo diffuso ed efficace per carpire le informazioni necessarie ad aumentare i propri livelli di autorizzazione in rete o per raggiungere altri dati importanti.

Le **principali motivazioni** che inducono un "interno" ad agire.
-**Vendetta**: motivi di rivalsa nei confronti dell'azienda in generale o di qualche collega in particolare. Sono pericolosi perché hanno uno scopo preciso e forti motivazioni (tra i casi scoperti l'indagine ha rilevato che il 92% del campione agiva per vendetta);
-**Curiosità e sfida**: molti insider non considerano affatto ciò che fanno come un attacco all'azienda, ma piuttosto come una sfida attraverso cui dimostrare competenze e pazienza. Gli attacchi più comuni portati per questo motivo comprendono il forzare account di posta, fare penetration test
non autorizzati o arrivare a informazioni sensibili come il salario del collega;
-**Guadagno**: cresce il numero degli insider che rubano informazioni sensibili per conto di qualcuno esterno all'azienda.

Anche in Italia cresce l'attenzione nei confronti delle minacce interne alle aziende.
"Un'indagine IBM su circa 150 imprese nazionali - afferma il Clusit - ha mostrato che metà (51%) delle aziende italiane intervistate ritiene che le minacce alla sicurezza aziendale provengano oggi dall'interno delle rispettive organizzazioni. Di contro, questo pericolo è evidenziato dal 66% delle aziende a livello mondiale.
Buona parte (75%) dei responsabili IT italiani è poi convinta che il crimine organizzato dotato di competenze tecniche stia sostituendo la figura dell'hacker solitario e, in misura minore (50%) che una minaccia emergente proviene anche dai sistemi non protetti presenti nei Paesi in via di
sviluppo."

Fonte: Clusit.

Questo articolo è pubblicato sotto una Licenza Creative Commons.

I contenuti presenti sul sito PuntoSicuro non possono essere utilizzati al fine di addestrare sistemi di intelligenza artificiale.