PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 6 - numero 966 di martedì 23 marzo 2004

In aumento la pericolosita' degli attacchi informatici

Le "minacce a tecnica mista" rappresentano uno dei maggiori pericoli per le aziende. Nel mirino le informazioni confidenziali.

In ambito informatico si assiste ad un progressivo ridursi del tempo che intercorre tra l'individuazione di una falla di sicurezza ed il suo effettivo sfruttamento da parte degli hacker. Ne consegue che tra l'annuncio di una nuova vulnerabilità e il rilascio di un'apposita patch, le aziende sono esposte all'attività degli hacker. Una situazione che rende sempre più complesso per gli amministratori IT mantenere adeguati livelli di sicurezza.
Vulnerabilità sempre più gravi, ma che si sfruttano facilmente, mettono a repentaglio la sicurezza delle reti informatiche delle aziende e dei computer dei privati.
Questa "lotta contro il tempo" è stata messa in luce dalla quinta edizione dell'Internet Security Threat Report (ISTR), un report sulle ultime tendenze riguardanti gli attacchi Internet realizzato da Symantec.
I risultati del report si basano sull'analisi dei dati forniti da clienti Symantec e da oltre 20.000 sensori per il monitoraggio degli attacchi informatici in più di 180 Paesi.
Il report evidenzia le cause e le modalità con cui gli attacchi hanno colpito alcune aziende più gravemente di altre e si propone di fornire agli operatori e alla comunità Internet le tendenze future nelle minacce informatiche, nelle vulnerabilità identificate, nelle tipologie degli attacchi.

Attacchi.
Nella prima metà del 2003 solo un sesto delle aziende analizzate ha riportato attacchi giudicati gravi, mentre nella seconda parte tale proporzione è salita fino al 50% delle società monitorate. In particolare, le aziende che hanno segnalato attacchi informatici di rilevante serietà sono cresciute dal 17% al 45% registrando una maggiore percentuale di attacchi nei settori Sanità, Energia e Servizi finanziari.
I worm rimangono la fonte più comune di attacchi.
Quasi un terzo di tutte le tipologie di attacco ha fatto leva sulla vulnerabilità sfruttata da Blaster, worm apparso nell'agosto del 2003. Blaster ed i worm Welchia e Sobig.F hanno infettato in 12 giorni milioni di computer causando danni per 2 miliardi di dollari.
Gli attacchi a tecnica mista rappresentano uno dei maggiori pericoli affrontati dalle aziende; tali attacchi hanno utilizzato sempre più spesso le backdoor lasciate da precedenti worm. Facendo leva su backdoor preesistenti per assumere il controllo di un sistema, gli hacker possono installare una propria backdoor o utilizzare il sistema per avviare un attacco DDoS (Distributed Denial of Service).
Molti degli attacchi registrati ? in terza posizione nella classifica delle prime dieci casistiche - hanno riguardato le porte dei servizi di file sharing peer-to-peer.

Vulnerabilità.
Symantec ha documentato una media di sette vulnerabilità scoperte quotidianamente.
I risultati emersi dall'analisi dei dati raccolti indicano una stabilizzazione del tasso di rilevamento delle vulnerabilità (minore del 2%). Un dato positivo se si considera che l'incremento dal 2001 al 2002 era stato pari all'81%.
Tuttavia le nuove vulnerabilità rilevate sono sempre più gravi. Quasi l'80% delle vulnerabilità può essere sfruttato in remoto e molte di queste riguardano le applicazioni Web. Symantec ha rilevato che il 70% delle vulnerabilità scoperte nel 2003 poteva essere sfruttato senza difficoltà perché il loro accesso non richiedeva alcun codice particolare oppure tale codice era facilmente reperibile.

Minacce.
In passato le minacce a tecnica mista riguardavano le comuni vulnerabilità dei server (Web e database). Oggi l'obiettivo è rappresentato dalle vulnerabilità dei componenti base dei sistemi operativi presenti tanto sulle reti aziendali quanto su quelle

consumer.
Nel secondo semestre 2003, Symantec ha documentato più di 1.702 nuovi virus e worm per Win32: un incremento del 250% rispetto ai 687 rilevati nello stesso periodo del 2002.
Dal 2002 al 2003, il volume delle minacce alla riservatezza dei dati personali presenti nelle prime 50 segnalazioni è aumentato del 148% e addirittura del 519% nelle prime 10 segnalazioni. In precedenza, le minacce alla riservatezza e alla privacy contavano per il 22% delle prime dieci segnalazioni ricevute da Symantec. Negli ultimi sei mesi il volume di tali segnalazioni è salito al 78%.

---

www.puntosicuro.it