CONSTANT SECURITY

AFFIDABILITÀ E SICUREZZA GIOCANO D'ANTICIPO

PAROLA D'ORDINE: PROTEZIONE

Proteggere i dati sensibili immagazzinati nei propri sistemi informatici è divenuto un punto fondamentale delle attività aziendali e questo vuol dire proteggere la propria rete ed essere sempre informati sulle sue debolezze.
In Italia il decreto legislativo del 30 giugno 2003 ha introdotto il Documento Programmatico sulla Sicurezza che obbliga le aziende a presentare il loro piano annuale per proteggere i dati sensibili dei loro clienti/utenti.
Il DPS recita quanto segue: "*Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico adotta [...] idonee misure tecniche e organizzative adeguate al rischio esistente, per salvaguardare la sicurezza dei suoi servizi*".

UN HACKER DALLA VOSTRA PARTE

Così come esistono figure chiamate hacker che cercano le debolezze di un software o di una rete per entrare e agire a scopo personale, esistono strumenti ed aziende che eseguono le stesse attività per verificare e migliorare la protezione dalle intrusioni.
Constant Security INRETE nasce per cercare come un hacker le difese più deboli, ma agisce per proteggere costantemente la rete aziendale.
Constant Security INRETE opera continuamente alla ricerca di vulnerabilità, eseguendo una continua scansione dei servizi accessibili e la verifica dei possibili problemi utilizzando vari database disponibili su exploit e vulnerabilità.
Tutti i server, così come tutti i segmenti della rete aziendale esposti a internet, vengono sottoposti a questo tipo di controllo in modo tale da verificare la necessità dell'aggiornamento anche di un solo componente.
Le caratteristiche di Constant Security INRETE sono:

- verifica delle vulnerabilità del sistema e confronto con eventuali situazioni simili in database di registro storico exploits e vulnerabilità
- i risultati vengono presentati secondo la prospettiva di chi si deve difendere invece di chi attacca
- il software di scanning, costantemente aggiornato, è anche in grado di generare una serie di alert automatici tramite e-mail e/o sms
- riduzione drastica del tempo di gestione della vulnerabilità.

PREVENIRE È MEGLIO CHE CURARE

La sicurezza totale è una chimera, ma utilizzando uno strumento come Constant Security INRETE è possibile tenere costantemente sotto controllo la sicurezza dei propri sistemi individuando immediatamente i punti di debolezza ed essere pronti per interventi risolutori.
Nell'istante in cui viene scoperta una falla di sicurezza nel vostro sistema, vi trovate nel cosiddetto "giorno zero" ovvero un momento di altissima vulnerabilità per la vostra azienda. Gli attacchi informatici nel periodo immediatamente successivo agli zero-days sono molto pericolosi proprio perché vengono lanciati quando ancora non è stata distribuita alcuna patch e quindi i sistemi risultano non protetti, lasciando le aziende totalmente impotenti di fronte all'attacco.
Agire con immediatezza di fronte alle emergenze di un zero-day significa poter decidere come gestire al meglio i propri servizi internet nel rispetto non solo dei vostri clienti, ma anche dell'attuale quadro legislativo in materia di protezione dei dati sensibili.
Venire a conoscenza della debolezza di un software quando qualcosa di grave è già successo è troppo tardi.
Per questo motivo il servizio Constant Security di INRETE permette di affrontare le vulnerabilità dei propri sistemi seguendo l'unica via possibile: conoscerle prima degli altri.

INRETE
Inrete Srl - Via Postiglione, 29 - 10024 Moncalieri (TO) - Tel: (+39) 011 6811590 - Fax: (+39) 011 6811603
Web: http://www.inrete.it - Email: info@inrete.it - Posta elettronica certificata: inrete@cert.inrete.it