

Sicurezza dati: la scadenza è molto vicina

Dal 1° aprile tutte le aziende dovranno dotarsi di strumenti di sicurezza

Sono stati accordati altri tre mesi (la scadenza era precedentemente fissata al 31 dicembre 2005) a tutti coloro che devono adottare le misure minime di sicurezza dei dati e predisporre il documento programmatico sulla sicurezza (DPS), previsti dal D.Lgs. 196/2003, il cosiddetto Codice della Privacy. Dal 1° aprile 2006 tutti i soggetti, pubblici e privati, saranno tenuti a operare nel rispetto di precise regole nei riguardi della sicurezza delle informazioni e della protezione dei dati personali.

Le soluzioni Firewall di TWT, in aggiunta a un'adeguata documentazione e implementazione di sicurezza sulla rete interna da parte dell'azienda, assicurano la conformità alle nuove norme di sicurezza imposte dal Codice della Privacy, da adottare entro il 31 marzo 2006. Per non perdere l'appuntamento con quest'ultima scadenza, Trans World Telecommunications consiglia fin da oggi l'adozione all'interno dei sistemi informativi aziendali di misure di sicurezza tali da ridurre al minimo i rischi di distruzione o perdita di dati personali, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta.

L'Allegato B al Testo Unico della Privacy, intitolato Disciplinare tecnico in materia di misure minime di sicurezza, definisce le misure minime da applicare. Particolare attenzione va dedicata ai programmi Antivirus/Antispyware e ai Firewall: l'aggiornamento del database dei virus noti deve essere fatto ogni qual volta ne esiste

uno disponibile, poiché questi aggiornamenti fanno parte di un corretto funzionamento del programma stesso.

La soluzione TWT

TWT propone soluzioni chiavi in mano per garantire la gestione delle politiche di sicurezza aziendale.

Le soluzioni di sicurezza TWT comprendono:

- Consulenza nella definizione delle politiche di sicurezza del Firewall
- Setup e configurazione del Firewall
- Prova di intrusione iniziale e a seguito di ogni modifica (i tentativi di intrusione sono effettuati su tutte le vulnerabilità note, cercando di esaminare dati, causare disservizi o effettuare qualsiasi altro genere di attività non autorizzata)
- Report finale della configurazione
- Aggiornamenti del firmware del Firewall
- Filtering di Porte/Protocolli e Indirizzi IP, con State full inspection (filtri d'accesso sui protocolli IP, basati su differenti criteri - indirizzi, protocolli, porte - che possono essere configurati per bloccare o limitare l'accesso a gruppi d'utenti. Tramite l'utilizzo di State full inspection, il Firewall è in grado di rilevare sequenze anomale e bloccarle)
- Intrusion Detection (sistema di controllo sull'attività di frontiera, in grado di rilevare i tentativi di intrusione non autorizzati ed eventualmente di bloccarli prima che abbiano successo)
- Antivirus sui protocolli HTTP, FTP, SMTP, POP3, IMAP e disponibilità di una porta DMZ.

- Content filtering: gestione del traffico basato su url e/o parole chiave (permette di controllare e limitare il traffico verso alcuni siti Internet)

- Attestato di Conformità al Disciplinare Tecnico allegato al D.Lgs n.196/2003 (contestualmente al servizio, TWT fornirà un Attestato di Conformità alle disposizioni del Disciplinare Tecnico, come previsto dallo stesso all'art.25)

Le soluzioni Firewall di TWT, in aggiunta a un'adeguata documentazione e implementazione di sicurezza sulla rete interna da parte del cliente (DPS, antivirus, utilizzo di password, backup...), assicurano la conformità alle nuove norme di sicurezza imposte dal Codice della Privacy.

Non un semplice Firewall

TWT offre Firewall centralizzati di ultima generazione, in grado di fare da antivirus e di bloccare i worm, con in più la possibilità di configurazione delle policy dei contenuti.

In questo modo è possibile migliorare la sicurezza delle reti aziendali, eliminando sprechi ed eventuali abusi, e assicurando contemporaneamente un utilizzo ottimale delle risorse di comunicazione. I sistemi di protezione convenzionali spesso risultano troppo lenti e lasciano la rete pericolosamente esposta agli attacchi esterni. Le piattaforme implementate da TWT, d'altro canto, utilizzano un chip che consente di individuare virus, worm e ogni sorta di codice invasivo senza mai compromettere le prestazioni del vostro server.