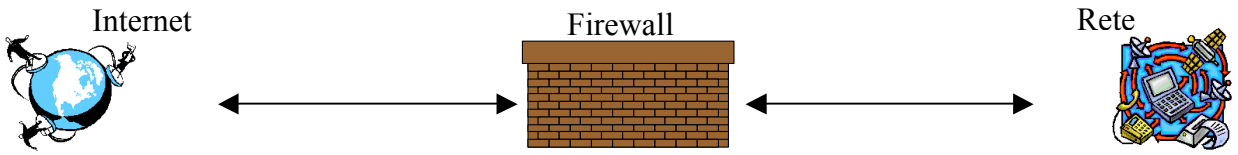
L’educazione alla sicurezza e il valore della tranquillità:

il Firewall da costo a risorsa per la Pubblica Amministrazione

Il problema della sicurezza informatica rappresenta uno degli aspetti cruciali dell'amministrazione di una rete aziendale. La sicurezza diventa di primario interesse quando l’ente connette la propria rete privata a Internet.

Un numero sempre maggiore di utenti su reti private richiede accesso ai servizi Internet come World Wide Web (WWW), Internet mail, Telnet e File Transfer Protocol (FTP). In più, l’ente deve offrire dei servizi di e-government e quindi offrire home page WWW e server FTP per l’accesso al pubblico. Gli amministratori si interessano sempre più alla sicurezza delle loro reti quando espongono i dati privati al rischio di attacchi da parte di "cracker" Internet. Per ottenere il livello richiesto di protezione, un'organizzazione ha bisogno di una politica di sicurezza per impedire agli utenti non autorizzati di accedere a risorse sulla rete privata.

Il firewall è un sistema o gruppo di sistemi che rafforzano la politica di sicurezza tra la rete di un'organizzazione ed Internet. Il firewall determina quali servizi interni possono essere accessibili dal di fuori, quali utenti esterni possono accedere ai servizi interni e quali servizi esterni possono essere accessibili da utenti interni. Affinché il firewall sia efficiente, tutto il traffico da e verso Internet deve passare attraverso di esso; in questo modo il traffico può essere ispezionato e monitorato (non si può gestire ciò che non si misura). Il monitoring e la misurazione dell’uso di internet serve per incrementare il rendimento delle risorse umane a garantire il ritorno dell’investimento. La maggior parte delle persone pensa che il compito del content filtering sia soprattutto quello di bloccare l’accesso ai contenuti proibiti o a siti potenzialmente dannosi, ed effettivamente è così, il content filtering aiuta anche le aziende a misurare e gestire l’uso del web per ottenere un maggior rendimento dei collaboratori. Questo è possibile quando un prodotto di content filtering permette di visualizzare report dei siti web visitati ed utilizzati.



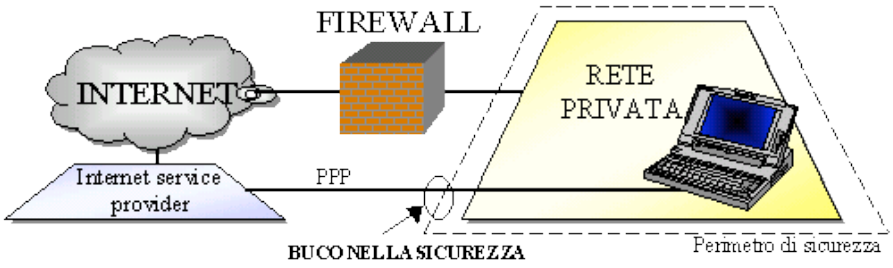

Il firewall deve permettere il passaggio solo al traffico autorizzato ed il firewall stesso deve essere immune alle penetrazioni. Sfortunatamente, un sistema firewall non può offrire alcuna protezione una volta che un hacker è entrato attraverso il firewall o lo ha raggirato. Il firewall è parte di una politica di sicurezza complessiva, un processo, che crea un perimetro di difesa progettato per proteggere le risorse informative dell'organizzazione. Questa politica di sicurezza deve includere la pubblicazione di regole per informare gli utenti delle loro responsabilità. Le politiche dell’organizzazione definiscono gli accessi alla rete, gli accessi ai servizi, l’autenticazione remota e locale dell'utente, misure di protezione dai virus ed addestramento degli utenti della rete privata. Tutti i punti potenziali di attacco della rete devono essere protetti con lo stesso livello di sicurezza. Installare un firewall senza una politica chiara di sicurezza è come mettere una porta d’acciaio su una tenda.

Benefici di un Internet Firewall

Un firewall gestisce l'accesso tra Internet e la rete privata dell'ente. Senza un firewall, ciascun calcolatore sulla rete dell'ente è esposto agli attacchi da altri calcolatori sulla rete esterna. Il firewall permette all'amministratore della rete di definire un "punto di soffocamento" (choke point) centralizzato che trattiene gli utenti non autorizzati come gli hacker, i cracker e le spie; esso proibisce ai servizi potenzialmente dannosi di entrare o uscire dalla rete protetta e provvede alla protezione dai vari attacchi. Un firewall semplifica la gestione della sicurezza perché la sicurezza della rete è consolidata sul sistema firewall piuttosto che essere distribuita su ogni singolo pc della rete dell'ente. Il Firewall costituisce un punto conveniente dove la sicurezza di rete può essere esaminata e dove possono generarsi allarmi. Un firewall è il punto perfetto per monitorare o filtrare l'uso di Internet. Questo permette anche all'amministratore della rete di giustificare la spesa del collegamento a Internet, di determinare con precisione i potenziali colli di bottiglia e di provvedere a un rimodellamento del modello comportamentale dei dipendenti dell'ente. Il firewall è l'ubicazione ideale per allocare WWW e FTP server, in questo caso, lo stesso può essere configurato per permettere l'accesso a questi servizi da Internet e contemporaneamente proibisce l'accesso esterno verso altri sistemi sulla rete protetta. Qualcuno potrebbe pensare che un firewall rappresenti un punto molto delicato ma dovrebbe essere intuitivo il fatto che se il collegamento a Internet fallisce, la rete dell'ente continua a funzionare senza generare un'interruzione di servizio e solo l'accesso a Internet è perduto. Se ci sono punti multipli di accesso (nel caso di sedi distaccate), ciascuno di questi diviene un punto potenziale di attacco che l'amministratore della rete deve munire di firewall ed esaminare regolarmente.

Limiti di un Internet Firewall

Un firewall non protegge contro gli attacchi che non passano attraverso di lui. Per esempio, se è permesso di accedere dall'interno della rete protetta all'esterno, senza restrizioni, gli utenti interni possono fare una connessione diretta PPP ad Internet poiché vogliono evitare le autenticazioni addizionali richieste dal firewall e sono tentati a raggirare il sistema di sicurezza. Questi tipi di collegamenti diretti bypassano la sicurezza assicurata anche dal miglior firewall in commercio, creando anche una potenziale porta secondaria per attacchi ugualmente significativi.




Gli utenti, quindi, devono essere consapevoli che questi tipi di collegamenti non sono permessi per la sicurezza complessiva dell'organizzazione. I firewall non possono proteggere contro le minacce delle "talpe" o degli utenti inconsapevoli, infatti non possono proibire a questi di copiarsi i dati nei floppy disk o di rimuovere da un calcolatore la scheda di rete. Gli impiegati devono essere informati sui vari tipi di attacchi e del bisogno di proteggersi cambiando periodicamente la loro password.

I moderni firewall

I sistemi firewall più evoluti sono in grado di proteggere contro il trasferimento di files infetti da virus sia durante la navigazione sia durante l'utilizzo della posta elettronica. Naturalmente è comunque necessario installare dei software anti-virus su ciascun desktop della rete interna. I moderni firewall sono in grado di proteggere anche dagli attacchi rivolti ai dati. Ciò avviene quando dati apparentemente innocui vengono spediti o copiati in un host interno e poi usati per lanciare un attacco. Per esempio un tale attacco può consistere nel modificare i file che gestiscono la sicurezza, rendendo più facile per un intruso ottenere l'accesso al sistema. In

questo caso si può ipotizzare la perdita totale o parziale dei dati del sistema informatico. È evidente quindi, che l'introduzione di un firewall, non solo tutela il sistema informatico da attacchi esterni, ma va anche considerato che, la perdita totale o parziale del patrimonio informatico dell'ente, porterebbe alla inevitabile interruzione di servizio per tempi prolungati e ad uno sforzo notevole per il ripristino di tutti i dati.

Lo Studio Consulenza e Formazione per pubbliche amministrazioni del Dott. Alberto Ponti, nell'intento di assicurare agli enti locali una quanto più ampia ed articolata assistenza nell'espletamento dei loro compiti istituzionali vuole fornire agli stessi, in aggiunta a quella già garantita, una consulenza più specializzata in materia di sicurezza informatica, tutela del dato e formazione del personale incaricato del trattamento del dato.

Lo Studio è a Vs. disposizione per qualsiasi necessità o chiarimento in merito:

alberto.ponti@consulentilocali.it