

Esistono impianti di rivelazione anti intrusione mediante l'installazione di sensori volumetrici all'interno di un edificio, sensori sulle aperture dello stabile (porte e finestre), centraline che gestiscono sensori di temperatura, movimento, infrarossi, sistemi di notifica istantanea (sms, mail, telefonata), sistemi di gestione e visione diurna / notturna remota, registrazione audio-video remota etc. etc.

I dati aziendali, i nostri dati, rappresentano l'edificio da difendere a tutti i costi e, gli apparati a protezione, sono i firewall hardware e software che possono contenere le più svariate tecnologie di prevenzione attacchi, difesa passiva e/o attiva, notifiche immediate, antivirus a corredo, controlli a livello layer 7 (chat, instant messenger...), servizi di web filtering, gestione centralizzata e remota etc. etc.

Il classico esempio di protezione perimetrale passiva è rappresentato dal router che natto il traffico su una network interna privata che con un minimo di configurazioni di access lists, rappresenta la forma più comune di barriera logica dal mondo esterno, internet, verso la nostra azienda. Ma un intruso determinato è in grado di forzare qualsiasi struttura di "recinzione", semplicemente utilizzando dei software che si trovano sul web, sfruttando le falle del sistema operativo del router, utilizzando i servizi pubblicati, sniffando il traffico, etc. etc. Anche in presenza di un Firewall, correttamente installato ma privo di servizi (IDS, IPS, Configurazioni complete, gestione aggiornamenti, lettura log, etc. etc.), la situazione rimane pressoché invariata a quella del router.

Negli ultimi anni, si è rafforzato il concetto di protezione perimetrale, focalizzandolo sull'esterno della rete e si è giunti alla conclusione che è fondamentale rilevare l'intruso nell'istante in cui cerca di attaccare.

Qualsiasi sistema di sicurezza, che protegga una rete, deve tenere presente queste semplici regole: rilevare l'intruso istantaneamente, notificare il problema, eseguire automaticamente delle contromisure (sicurezza attiva) se necessarie, auto aggiornarsi, prevenire le minacce software, consentire gli accessi a utenti sicuramente autenticati, monitorare costantemente il traffico generato dai servizi erogati verso il web e resistere ai guasti hardware / software.

Installare uno o più sistemi di sicurezza perimetrale che soddisfino tutti questi requisiti è soprattutto un lavoro di concetto slegati dal tipo di hardware e/o software (Cisco Asa, Fortigate, Isa Server etc. etc.) acquistati. Paradossalmente è possibile spendere migliaia di euro per ottenere una protezione simile a quella offerta da un semplice router configurato con delle access lists.

Bisogna affidarsi a personale qualificato, diffidare dei "faciloni" e soprattutto rivolgersi a persone di fiducia, perché demandare la configurazione dei sistemi di protezione è come affidare le chiavi di casa al guardiano notturno.