

Virus, costante vulnerabilità dei sistemi informativi.

La produttività di un'azienda moderna è sicuramente legata alla stabilità, alla sicurezza ed alle prestazioni della propria infrastruttura informatica.

L'impiego di un Firewall permette un controllo efficace del traffico di rete, mediante il suo utilizzo si limitano attacchi informatici ai sistemi server e si impediscono accessi non autorizzati alle risorse aziendali.

Da solo, tuttavia, un firewall non è sufficiente: si è ancora vulnerabili ai virus che possono liberamente attraversare la barriera convogliati nei flussi di dati dalla navigazione web e della posta elettronica o, comunque, all'interno di qualunque file scaricato da Internet.

Per questo motivo è necessario attivare azioni preventive mediante un server dedicato in grado di intercettare, analizzare e ripulire il traffico di rete, in modo da ridurre, se non azzerare, il rischio di infezione da virus. Analogamente occorre intervenire per fermare eventuali mail infette in uscita dall'azienda: se questo si verificasse, al rischio di propagare l'infezione, si aggiungerebbe il danno dovuto alla pessima immagine che l'azienda fornirebbe del proprio sistema informativo.

Spamming, fastidiosa invasione dei sistemi di posta elettronica.

Il sistema di posta elettronica, nato in ambienti di ricerca con l'obiettivo di abbreviare i tempi di comunicazione di ricercatori appartenenti a diversi istituti, è entrato ben presto a far parte del modo di vita della società contemporanea. Superfluo ricordare i molti aspetti positivi di questo strumento di comunicazione, quali trasmissione praticamente immediata delle comunicazioni, delocalizzazione geografica del recapito, riconosciuta validità legale, etc.

L'utilizzo in azienda di uno strumento di comunicazione così potente è ormai indispensabile. La considerevole riduzione dei tempi di comunicazione introdotta dal sistema di posta elettronica aziendale ha reso possibile un sostanziale aumento della produttività complessiva.

Tuttavia tale sistema di corrispondenza è fortemente compromesso nelle proprie funzionalità dal fenomeno dello "spamming".

Che cos'è lo "spamming"? Molto semplicemente è l'invasione, se non addirittura l'intasamento, delle caselle di posta elettronica con comunicazioni pubblicitarie o di natura ancora peggiore, non autorizzate e non richieste.

Si potrebbe accostare il fenomeno dello spamming a quanto avviene con i volantini che vengono lasciati quotidianamente nelle cassette della posta tradizionali. La differenza è però apprezzabile se si pensa ai costi irrisori che questa forma di pubblicità elettronica comporta, costi che hanno portato ad una quasi esasperata diffusione del fenomeno.

Analogamente a quanto proposto per confinare i virus, anche in questo caso occorre intervenire a monte del sistema informativo aziendale mediante azioni preventive che, grazie ad un server dedicato, analizzino e rimuovano le email indesiderate dal flusso di dati in ingresso.

Confinare le epidemie virali

Per contrastare efficacemente la contaminazione da virus del sistema informativo occorre agire prima che l'infezione penetri all'interno della rete aziendale, nei server, nelle applicazioni o sui desktop.

Installato in una LAN aziendale immediatamente a valle del gateway esistente, KNK Shield crea un sistema di protezione entro il quale tutto il traffico HTTP, FTP, SMTP e POP3 viene intercettato ed eventualmente ripulito.

KNK Shield è in grado di analizzare tutto il traffico di rete alla ricerca di eventuali virus contenuti nei dati in transito nella LAN aziendale.

Intercettare lo spamming

Analogamente a quanto si fa per i virus, anche per il fenomeno dello spam è necessario intraprendere azioni di blocco prima che il flusso di dati email raggiunga l'interno della rete aziendale.

Grazie alla sua posizione, a monte della connettività aziendale, KNK Shield implementa un sistema di filtro delle email di spam basato sui più recenti algoritmi di ricerca ed intercettazione.

KNK Shield è in grado di esaminare tutte le email in transito verso la lan aziendale e stabilire con accuratezza l'origine non autorizzata delle email in ingresso.

Semplicità, Affidabilità e Trasparenza

La facilità di installazione e configurazione rende KNK Shield uno strumento di semplice inserimento nella LAN aziendale, trasparente nei confronti della struttura esistente.

La procedura di configurazione di KNK Shield, strutturata in pochi semplici passaggi, richiede pochi minuti.

KNK Shield è "trasparente", non richiede cioè nessuna riconfigurazione dei client aziendali, né, tantomeno, dei server presenti in LAN.

Gli obiettivi prioritari del team di sviluppo della soluzione KNK Shield sono stati un'ottima stabilità di sistema, una piena compatibilità con le infrastrutture di rete aziendali ed un elevato standard di sicurezza intrinseca.

Stealth Update

Non richiede gestione né manutenzione assistita da operatore.

KNK Shield implementa autonomamente servizi in grado di effettuare l'aggiornamento automatico delle definizioni dei virus e del software.

Tutti i pattern file, il motore di scansione e il software si aggiornano automaticamente: in questo modo la soluzione risulta continuamente allineata con le più recenti definizioni dei virus, difendendo al meglio la struttura informativa aziendale da nuove infezioni.

High Performance

Nessuna perdita di prestazioni della connettività di rete.

Progettata per essere una soluzione High Performance, KNK Shield implementa un algoritmo di scansione particolarmente performante che, unito ad architetture hardware dimensionate in modo da limitare al minimo l'eventuale degrado della banda passante, rendono l'intero sistema non invasivo.

L'algoritmo euristico di ricerca dei virus contenuti nei dati che transitano nella rete risulta di elevata efficienza.

Le piattaforme hardware Intel, utilizzate per la soluzione, risultano particolarmente performanti e sono dimensionate in base alle reali necessità di connettività aziendale.

High Availability

Pronto per ambienti Mission Critical, KNK Shield è predisposto per configurazioni in HA (High Availability) per sistemi ad alta affidabilità.

La configurazione HA di KNK Shield prevede la possibilità di collegare più unità e di implementare in questo modo un affidabile cluster antivirus. Mediante questo dispositivo, il sistema di protezione perimetrale KNK Shield risulta sempre operativo anche a fronte di eventuali guasti hardware che possono presentarsi sulle singole unità costituenti il cluster.