



**Concedetevi una siesta.  
Alla sicurezza pensiamo  
noi**

## AREA CULTURALE IP SECURITY

### UN MODO DIVERSO DI PARLARE DI “MINIMO LIVELLO DI SICUREZZA DELLE INFORMAZIONI”



*Esistono moltissimi parallelismi tra il mondo della sicurezza informatica e la tutela della salute dei pazienti, in fondo parliamo entrambi di virus!*

Per i produttori di soluzioni per la sicurezza informatica è facile disquisire dei motivi – per altro oggettivi – che rendono necessario investire nella tutela della privacy dei pazienti contro intrusioni o fughe di dati. È ormai una gara a chi dipinge nel modo più catastrofico le conseguenze di tali evenienze, basandosi su più che ovvi riferimenti a normative ormai consolidate su *tutela e trattamento dei dati personali o sulle misure minime di sicurezza*. Se presentare gli imperativi emergenti dal quadro legislativo non fosse sufficiente, il Vendor può far leva sul rapporto qualità/prezzo per invogliare l'IT manager a considerare sistemi IPS (prevenzione delle intrusioni) in tempo reale, dotati di tutte le funzioni di sicurezza, sciorinando nel suo “itanglish” tutte le meraviglie della tecnologia di cui sono dotati i dispositivi “tutto in uno”: antivirus, antispam, filtraggio URL, gestione dei tunnel VPN SSL e IPSec, generazioni di chiavi PKI, e quant'altro, sottolineando il risparmio notevole sui costi di gestione associato ad un solo dispositivo, senza però accorgersi che, lo stesso IT manager, immerso in un mondo che non è chiaramente quello di un produttore di sicurezza informatica, non percepisce il reale beneficio che il suo ospedale può trarre dall'impiego dell'una o l'altra tecnologia.

Eppure, se consideriamo l'infrastruttura IT come il cuore di un ospedale, si possono ricavare parallelismi interessanti. Presa in generale la

sicurezza informatica è tanto semplice e necessaria quanto la tanto decantata assunzione di fermenti lattici per incrementare le difese immunitarie contro gli agenti esterni (intrusion prevention), inutile dire che i risultati dipendono dalla qualità del prodotto. Allo stesso modo è tanto sottile ed utile quanto applicare un “reveal” sottocute che, pur essendoci, non ha impatto sulle “prestazioni” del paziente (rete), registra l'ECG in tempo reale (traffico di dati in ingresso ed uscita) per circoscrivere e diagnosticare correttamente una particolare sintomatologia (vulnerability assessment o risk management in tempo reale) e quindi condurre una terapia mirata (indicazione automatica delle patch da applicare ai PC, notebook o server della rete). Come un pace maker, che analizza le attività cardiache ed emette impulsi ove necessario, con un firewall di nuova generazione si possono creare regole di trattamento dei pacchetti, in base al loro comportamento. In questo caso è l'accuratezza dell'analisi che fa la differenza tra la vita e la morte, o tra un “denial of service” e una rete protetta.

Neanche il ritmo con cui si trasformano le minacce informatiche è differente dalle mutazioni virali a cui siamo sottoposti. Solo che i nostri dispositivi garantiscono una reattività “day-0” contro minacce non note, i vaccini invece non sempre funzionano: il sogno di qualsiasi medico.