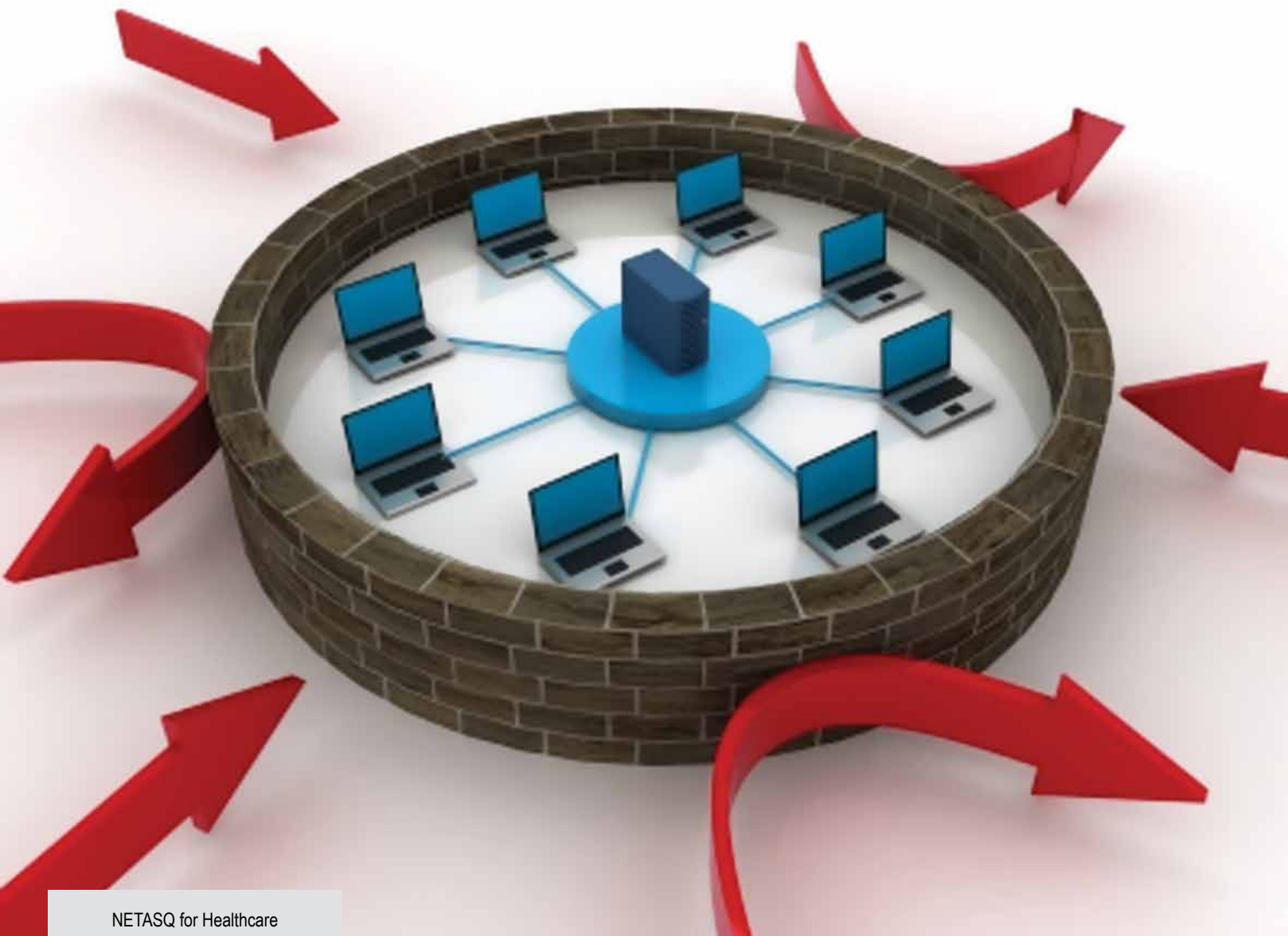


Pensi che
i tuoi pazienti
meritino

UNA SICUREZZA OTTIMALE?



Quale sicurezza per la sanità?

Per rispondere a questa domanda non basta disquisire degli imperativi posti dalle normative del Garante sulle misure minime di sicurezza per la tutela dei dati sensibili. Sebbene tali norme comportino obblighi ben definiti, rappresentano spesso una spina nel fianco dell'IT manager che vede un costante decremento dei budget per l'infrastruttura IT a fronte di una crescente digitalizzazione di cartelle, referti, documenti amministrativi, informazioni sulle procedure... La prevenzione contro l'accesso indesiderato a tali dati è solo una parte della problematica con cui deve confrontarsi l'IT manager di ASL o strutture ospedaliere quando deve selezionare le tecnologie di sicurezza più adatte alle proprie esigenze.

Elencare gli ormai altrettanto noti vantaggi di soluzioni per la gestione unificata delle minacce (UTM), come i nostri firewall IPS, sottolineando il risparmio notevole sui costi di gestione associato ad un solo dispositivo che presenta tutte le funzioni di sicurezza avanzata out-of-the-box senza dover acquistare moduli aggiuntivi, può forse favorire la percezione dei benefici di cui una struttura sanitaria può fruire impiegando l'una o l'altra tecnologia, ma non fornisce una risposta concreta a questa domanda.

Sfide reali

In un ecosistema particolarmente informatizzato, come il mondo della sanità, ove telemedicina, sistemi informativi ospedalieri e sanitari anche geograficamente distribuiti, home-care e personal-care, diagnosi e consultazioni remote, servizi ambulatoriali remotizzati, comunicazione tra e con i laboratori diagnostici in tempo reale sono all'ordine del giorno, la sfida è molteplice: non c'è solo il problema dell'accesso arbitrario a sistemi ed in informazioni riservate; esistono anche problemi più generali riguardanti il controllo del dato in rete, la tracciabilità forense delle attività e la necessità di garantire la massima disponibilità dei servizi e delle tecnologie trasmissive. Inoltre, con l'avvento di strumenti che favoriscono la mobilità del personale anche all'interno della struttura ospedaliera, è necessario assicurare che tali dispositivi siano protetti da eventuali falle potenzialmente dannose per l'intera rete.

Disponibilità dei servizi

La disponibilità dei servizi di rete e delle tecnologie trasmissive è essenziale, se consideriamo le potenziali conseguenze di un ritardo dell'applicazione in uso o di un'interruzione del servizio in un caso d'emergenza. I firewall NETASQ integrano un'ampia gamma di funzioni per garantire la continuità del servizio. Analizzando lo stato dei link di rete cinque volte al secondo, i dispositivi sono in grado di effettuare il failover in meno di un secondo ripristinando tutte le connessioni (VPN, VoIP, FTP, streaming audio e video) in modo del tutto impercettibile all'utente, che continua a svolgere i suoi compiti senza alcuna interruzione. Le soluzioni offrono altresì strumenti avanzati per la gestione della qualità del servizio (QoS) e per la prioritizzazione del traffico, oltre che per il bilanciamento del carico tra i dispositivi, evitando in modo efficace eventuali colli di bottiglia.

Sicurezza IT = collo di bottiglia?

Con una velocità di trasferimento dati di fino a 8,5 Gbps con il motore IPS (intrusion prevention) attivato, NETASQ offre protezione in tempo reale e performance senza pari rispetto agli standard di mercato. Tale throughput è reso possibile dal motore IPS NETASQ, che non è un modulo aggiuntivo, la cui attivazione cagiona una caduta libera delle prestazioni del dispositivo, ma rappresenta il cuore dell'appliance. Integrato nel kernel del sistema operativo, il nostro IPS si basa su una combinazione brevettata di diverse tipologie di analisi protocollari, comportamentali ed euristiche del flus-



so di dati, ricorrendo solo alla fine del processo a controlli basati su signature inerenti allo specifico contesto del pacchetto da analizzare. In tale modo scansiamo in tempo reale l'intero flusso di dati bloccando a priori comportamenti "anomali" ed offriamo quindi una reale protezione day-0 contro falle ed attacchi informatici noti e non noti senza generare alcun collo di bottiglia in rete. Le minacce identificate a livello industriale solo quest'anno venivano già bloccate da NETASQ nel 2003 grazie a questa imbattibile combinazione di tecniche d'analisi.

Vulnerabilità applicative

A fronte del crescente impiego di banche dati centralizzate per la condivisione delle cartelle cliniche, accessibili da remoto, l'IT Manager deve anche valutare come proteggere tale flusso di dati sensibili. I dispositivi NETASQ vengono spesso impiegati come concentratori di VPN poichè integrano la connettività cifrata IPsec ed SSL e montano un acceleratore ASIC ad esclusivo supporto di tali connessioni, il flusso di dati all'interno dei tunnel viene decodificato, analizzato e ricodificato in tempo reale. Un ulteriore aspetto da vagliare è la gestione delle falle applicative presenti sia sui server, sia sui dispositivi mobili, che possono eventualmente minare la sicurezza dell'intera infrastruttura. Con il modulo di risk management NETASQ SEISMO, l'IT Manager può monitorare tutte le vulnerabilità a livello applicativo, di servizio e di rete presenti nell'intera infrastruttura e porvi immediatamente rimedio evidenziando e risolvendo con facilità le problematiche alle quali è soggetta quotidianamente l'infrastruttura di rete, che viene completamente mappata in tempo reale durante le regolari attività di analisi del flusso di dati che passa per il firewall.

Tracciabilità forense

Con il NETASQ Event Analyzer mettiamo a disposizione uno strumento di business intelligence per la valutazione approfondita degli eventi e delle attività condotte in rete. Questo strumento consente sia di tracciare qualsiasi attività, lecita o illecita, generata all'interno della rete o condotta dall'esterno. Attacchi da remoto o fuga / furto di dati dall'interno vengono quindi monitorati e registrati in modo tale da consentirne la tracciabilità, anche forense.

Un occhio al budget

Indipendentemente dal settore di appartenenza, quando si rende necessario investire nella sicurezza IT le organizzazioni devono poter trarre il massimo beneficio dai propri investimenti. Le soluzioni NETASQ apportano

un contributo pratico e concreto alla garanzia di continuità del servizio, alla protezione day-0 delle informazioni scambiate attraverso qualsivoglia strumento di comunicazione, alla visibilità di eventuali applicazioni che scavalcano le policy di sicurezza o rappresentano una minaccia per l'intera infrastruttura.

Pur essendo noti per l'eccellente rapporto prezzo / prestazioni delle nostre soluzioni, siamo sempre molto attenti alle necessità di aziende o enti che desiderano impiegare tecnologie allo stato dell'arte, ma che devono fronteggiare tagli di budget sempre più congrui. Per questo motivo abbiamo dato vita ad un **programma "healthcare"** specifico per istituti ospedalieri e/o istituzioni della sanità. Il programma prevede sconti di sicuro interesse su dispositivi e servizi di manutenzione.

Non esiti ad avvalersene!

NETASQ merita la Sua fiducia!

1 Fondata nel 1998, l'azienda conta oltre 75.000 installazioni realizzate attraverso una rete di 750 partner in tutto il mondo.

2 Le soluzioni NETASQ sono le uniche sul mercato certificate EAL4+ secondo la nuova versione dei Common Criteria (v3.1) e hanno ottenuto la piena fiducia di NATO e UE, ratificata con le certificazioni "NATO-Restricted" e "EU Restricted".

3 GARTNER premia lo spirito innovativo dell'azienda da ormai quattro anni consecutivi.

4 Lo scorso anno NETASQ ha ricevuto il riconoscimento FAST 50 di Deloitte come una delle aziende con il più alto tasso di crescita in Francia.

UNIFIED THREAT
MANAGEMENT



www.netasq.com

NETASQ ITALIA – MILANO

Via Leone XII, 10 - 20145 MILANO - ITALIA

Telefono +39 02 - 72.537.249

email italia@netasq.com

NETASQ UFFICI INTERNAZIONALI

. BENELUX e SCANDINAVIA . Antwerpen . +32 3 242 88 10 . benelux@netasq.com

. FRANCIA . Parigi . +33 1 46 21 82 30 . france@netasq.com

. GERMANIA . Monaco . +49 8065 90903 . deutschland@netasq.com

. SPAGNA . Madrid . +34 91 761 0290 . iberia@netasq.com

. REGNO UNITO . Bracknell . +44 1344 401591 . uk@netasq.com

