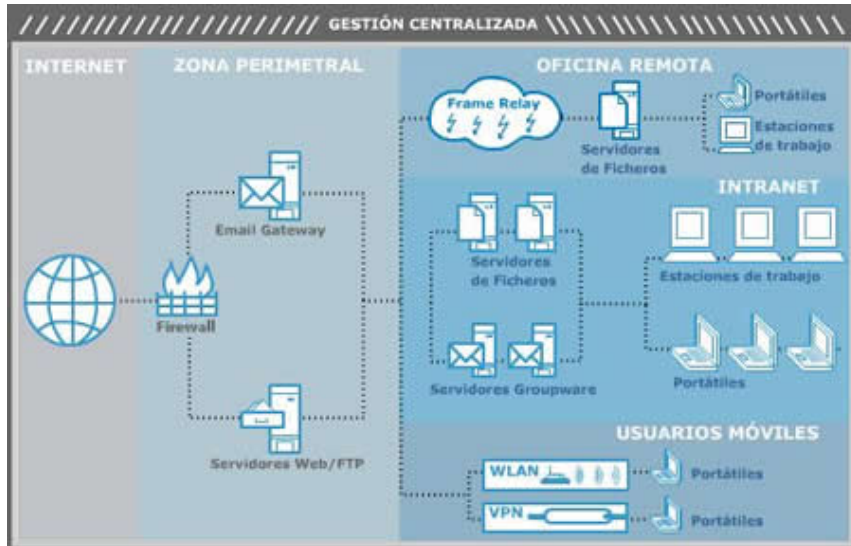


Seguridad Perimetral, Gestión Unificada Control de Amenazas.

El avance de la tecnología, ligado a amenazas cada vez más complejas, ha provocado que las soluciones de seguridad perimetral avancen a una nueva generación, cuyo exponente más destacado aparece en las distintas gamas de UTM (Unified Threat Management)



Más Noticias de Enciclopedia-Capacitación

- [Cómo saber si nuestras contraseñas son seguras.](#)
- [Manejar la privacidad en Facebook.](#)
- [Clickjacking: el engaño del clic.](#)

Tipos de protección

La seguridad adquiere progresivamente un mayor protagonismo en la infraestructura de IT de cualquier organización y es tendencia generalizada la planificación de políticas que preserven sus sistemas de información.

Dependiendo de la criticidad del entorno y de la preocupación por la seguridad de la compañía existen diferentes tipos de protección para asegurar los activos de la misma. José Manuel Crespo, director de Marketing de Producto de Panda Software, y Juan Grau, director regional de Ventas de Radware Iberia, distinguen dos tipos de seguridad: física y lógica. Por seguridad física se entiende el conjunto de elementos que constituyen el control de accesos al negocio (puertas, cámaras de vigilancia, etc.), así como el control de acceso de las personas autorizadas por medio -por ejemplo- de controles biométricos.

Por el contrario, cuando hablamos de seguridad lógica nos referimos a la relacionada con la protección de la información y el acceso a sus fuentes. Esta categoría se compone a su vez de informática personal (a nivel de usuario); seguridad de servicios comunes (servidores, red, etc.); seguridad de acceso a la información e identificación de usuarios, y seguridad perimetral, que es el tema en el que centraremos este reportaje.

Seguridad perimetral

La seguridad perimetral basa su filosofía en la protección de todo el sistema informático de una empresa desde "fuera", es decir, establecer una coraza que proteja todos los elementos sensibles frente amenazas diversas como virus, gusanos, troyanos, ataques de denegación de servicio, robo o destrucción de datos, hackeo de páginas web corporativas, etcétera.

Toda esta tipología de amenazas posibles ha fomentado una división de la protección perimetral en dos vertientes: a nivel de red, en el que podemos encontrar los riesgos que representan los ataques de hackers, las intrusiones o el robo de información en las conexiones remotas; y a nivel de contenidos, en donde se engloban las amenazas que constituyen los virus, gusanos, troyanos, spyware, phishing y demás clases de malware, el spam o correo basura y los contenidos web no apropiados para las compañías. Esta clara división unida al modo de evolución de las amenazas en los últimos años ha propiciado que el mercado de seguridad perimetral se centrara en la creación de dispositivos dedicados a uno u otro fin.

El firewall/VPN es el tándem histórico de seguridad perimetral y a él se han ido incorporando los sistemas IDS (Intrusión Detection Systems) e IPS (Intrusión Prevention Systems) para controlar el acceso a los sistemas de una empresa desde el exterior. En principio, el firewall o cortafuegos se necesita para controlar y monitorizar las comunicaciones. Además, se encarga de examinar las acciones de las aplicaciones que se conectan a la red y los puertos de las máquinas (comunicaciones P2P, por ejemplo). A este respecto, Natalia Gómez del Pozuelo, directora de Marketing y Distribución de Optenet, señala que "muchos protocolos presentan agujeros de seguridad que pueden comprometer la red corporativa y los datos confidenciales que ésta contiene. El bloqueo clásico de un cortafuegos se realiza a través de puertos, lo idóneo es tener una solución que permita reconocer aplicaciones independientemente de éstos".

En esta misma línea se manifiesta Eusebio Nieva, director técnico de Check Point en España y Portugal, quien además indica que el cambio principal que ha experimentado la seguridad perimetral en los últimos años ha sido "una evolución de las defensas, de ser puramente nivel 3 a inspeccionar los protocolos de aplicación, la corrección de los mismos, el contenido, el comportamiento, etcétera. Es decir, las defensas han ido evolucionando a medida que la sofisticación y peligrosidad de las amenazas lo han hecho".

Por otro lado, y con el fin de garantizar la protección a nivel de contenidos, vieron la luz los appliances basados en gestión de contenidos seguros SCM (Secure Content Management), que ofrecen una protección altamente especializada, de forma desatendida y sin influir en el rendimiento de las comunicaciones de la red corporativa.

Seguridad de contenido

Todas las organizaciones, con independencia de su tamaño y del sector al que se dediquen, están presenciando aumentos significativos en la cantidad y severidad de ciber-amenazas que van más allá de las de "tipo conexión", para convertirse en "ataques de contenido". Y es que, hoy en día, las principales amenazas provienen de este modelo de ataque, el cual no requiere de conexiones sostenidas para lograr sus objetivos.

Este tipo de amenaza se basa en el uso de contenido malicioso o agentes que, una vez introducidos en el ordenador, son capaces de actuar por sí mismos y propagarse internamente sin necesitar ningún tipo de conexión con el atacante original. El formato puede ser de virus, gusano, active web content o troyano.

El principal desafío ante amenazas basadas en contenido es que casi siempre se introducen dentro de las organizaciones por vías aparentemente inocuas, actividades tales como navegación web o intercambio de correo electrónico. Además, "todo apunta a que esta tendencia continuará en la medida en que las organizaciones precisen de comunicaciones en tiempo real -aplicaciones web y mensajería instantánea- como mecanismos competitivos en el ámbito empresarial", indica Emilio Román, director general de Fortinet.

Sin embargo, las amenazas actuales más sofisticadas utilizan combinaciones de ataques de red con los de contenido para explotar las vulnerabilidades de sistemas operativos y aplicaciones de amplia difusión, comprometiendo así a las redes en las que residen y sus recursos, con resultados en ocasiones devastadoras. Igualmente, los ataques combinados utilizan las peores características de virus, gusanos, troyanos y código maligno contra las vulnerabilidades de servidores e Internet y se transmiten y extienden a través de las redes con una velocidad sin precedentes, e implican costes ingentes para una rápida recuperación.

Nimda y Red Code fueron los primeros ataques combinados en tener éxito. Éstos utilizaron múltiples métodos y técnicas, y fueron capaces de replicarse rápidamente causando importantes daños.

Mientras que las defensas contra amenazas de conexión han dependido tradicionalmente de sistemas desplegados en la red, tales como cortafuegos, las primeras respuestas a ataques de contenido se basaron en software de aplicación instalado en ordenadores, como por ejemplo antivirus personales y software de detección de intrusiones basadas en host.

En opinión de Emilio Román, los fabricantes de seguridad han respondido al cada vez mayor número de amenazas desarrollando soluciones parciales. "Aunque los firewalls, VPNs e IDSs son efectivos proporcionando protección a nivel de red, no cubren las necesidades de protección actuales en los ámbitos telemáticos: miran solamente las cabeceras del paquete (no miran el interior); no pueden comprobar el contenido del paquete en tiempo real y procesarlo para identificar virus, gusanos u otras amenazas, y por lo tanto, son totalmente ineficaces contra ataques basados en el contenido; como consecuencia de lo anterior, los virus, gusanos y troyanos transmitidos por correo electrónico y tráfico http franquean fácilmente los cortafuegos y VPN pasando a menudo desapercibidos por los sistemas de detección de intrusiones". En definitiva, el directivo asegura que la defensa contra ataques combinados está más allá de la capacidad de las soluciones convencionales de seguridad de red, y que "los firewalls, servidores VPN e IDSs fallan a la hora de proporcionar protección completa, lo cual ha acelerado la necesidad de implantación de soluciones de defensa en profundidad, a nivel de contenido".

Esta misma opinión la han manifestado la mayoría de los profesionales consultados por este medio, que si bien alegan que de nada sirve la seguridad interna de la red si se descuida la perimetral, al mismo tiempo razonan que tampoco valdría de mucho tener una puerta cerrada con llave si, una vez dentro, disponemos de todos los bienes de valor al alcance de cualquiera. "La seguridad interna, la autenticación del usuario, los sistemas de encriptación de datos y un largo etcétera son igualmente necesarios, y deben complementarse sin perjudicar al flujo de trabajo con otras técnicas de seguridad perimetral", fundamenta Juan Carlos Pascual, director técnico de IpsCA.

Por tanto, se ha notado una clara evolución en el mercado desde lo que llamamos seguridad perimetral a una defensa en profundidad. Ahora hay una orientación clara hacia la integración de los sistemas de detección de intrusos en dispositivos típicamente perimetrales, como los cortafuegos o dispositivos pertenecientes a los cores de red como pueden ser los switches. De ahí el auge de soluciones conjuntas que combinan antivirus, antispam, firewall y diversos mecanismos más.

*** De la misma manera, ya no es suficiente con asegurar la red de una empresa, sino que también debemos preocuparnos porque ningún empleado introduzca ficheros infectados, o se conecte con un dispositivo móvil no seguro que ponga en peligro al resto de la red. Y es que, como advierte Andrew Bartram, director EMEA de Bluesocket, "las redes wireless LAN utilizan ondas de radio que traspasan los límites físicos de una organización, como es el caso de oficinas o edificios". Por eso, añade, "son necesarias soluciones que limiten la visibilidad, los accesos a las infraestructuras wireless de una empresa y puedan bloquear dispositivos externos de acceso a las redes corporativas o dispositivos internos de acceso a los recursos externos a lo largo de toda la red inalámbrica".***

En palabras de Juan Manuel López, director de Marketing de Mambo Technology, "el reto de los fabricantes se encuentra en la gestión eficiente de la respuesta ante los nuevos ataques que proliferan en la red de redes y en proporcionar a sus clientes firmas actualizadas y efectivas para poder controlarlos. Esto, junto con el desarrollo del hardware específico como podrían ser las plataformas basadas en ASIC para integrar los diferentes módulos de seguridad (firewall, detectores de intrusiones, antivirus...), será un factor importante dentro del mercado de este sector. Cabe destacar que en entornos extremadamente críticos también se opta por incluir HIDS, es decir detectores de intrusión, a nivel particular, de una determinada máquina para controlar de una manera exhaustiva los accesos a la máquina, sus datos y aplicaciones".

Demanda corporativa

Cada vez más, las empresas Argentinas y españolas se están concienciando de lo necesario que resulta una correcta inversión en seguridad y sí se percibe una apertura del mercado provocada por la aparición de amenazas más generalistas que afectan a todas las compañías por igual, sin distinguir tipos, sectores ni tamaños, y que implican unos costes operativos importantes. Además, el entorno regulatorio ha contribuido a este efecto positivo -como ha ocurrido con la Ley de Protección de Datos Personales-, y el control y el seguimiento de los datos ya no es sólo una práctica de negocio aconsejable, sino obligatoria.

Frente a este panorama, ¿qué servicios y soluciones de seguridad perimetral podríamos decir que son los más demandados? Para responder correctamente a esta pregunta tenemos que volver a distinguir entre grandes y pequeñas corporaciones.

Xavier García, ingeniero de Sistemas de Symantec Iberia, afirma que la gran mayoría de las compañías demandan, sobre todo, soluciones antivirus y protección del correo electrónico, "aunque se están empezando a solicitar cada vez más soluciones de protección para mensajería instantánea". Asimismo, expone que los servicios de monitorización de seguridad también están teniendo mucha aceptación. "Se trata de sistemas que monitorizan todo lo que sucede en las redes y sistemas de sus clientes y en cuanto detectan una anomalía en el sistema envían una alerta para que se inicien los procesos de respuesta más adecuados".

Por su parte, Alfonso Martínez Montero, director técnico de Stonesoft España, apunta que en las grandes cuentas predominan las soluciones integradas que permitan la convergencia de la seguridad con el networking y las comunicaciones. "Se requiere conectividad y acceso seguro desde cualquier punto, disponibilidad permanente y una defensa proactiva que proteja los activos de las empresas", defiende el directivo.

En las empresas pequeñas la situación es diferente. Al no disponer ni de personal dedicado a seguridad TI ni de una partida presupuestaria asignada a tal efecto las pymes tienden a la implantación de sistemas UTM (Unified Threat Management) que garantizan una gestión unificada de las amenazas al incorporar en un solo dispositivo protección anti-malware, anti-spam, anti-phishing, filtrado de contenidos web y además incluyen el Hardening adecuado, (cortafuegos y VPN preconfigurados) para que una empresa de estas características pueda funcionar.

Precisamente, la consultora especializada en tecnologías de la información IDC, revela que el segmento UTM del mercado de seguridad de los dispositivos dedicados es el que más rápido crece dentro del mercado de appliances de seguridad. Además, la organización estima que en 2008 los sistemas de seguridad UTM

habrán alcanzado un 32 por ciento de cuota de mercado, dejando atrás la tradicional autonomía de las appliances firewall/VPN, con un 50 por ciento de la cuota global.

Una solución UTM representa protección completa de las redes, tanto a nivel de conexión como de aplicación; menor coste total de propiedad (TCO) no sólo en infraestructura, sino también el asociado a servicios de soporte; mantenimiento y formación del personal de TI; gestión desde plataforma única y centralizada", el director regional de Ventas de Radware Iberia considera que estas herramientas son "a todas luces insuficientes para una gran empresa, donde se requiere la utilización de herramientas específicas y de alto rendimiento en cada área de seguridad, utilizando dispositivos de balanceo como elementos aglutinadores de todas las soluciones".

Por su parte, Eduardo Martín, responsable de Seguridad de Dimension Data, justifica ambas opiniones: "las soluciones integradas simplifican la gestión y operación diarias, además de permitir la concesión de cierta inteligencia a las infraestructuras de seguridad gracias a la interacción y entendimiento entre distintos componentes. En cualquier caso, y obviando los condicionantes operativos, existen escenarios en los que soluciones más específicas se pueden ajustar mejor a las necesidades concretas y por tanto no se puede afirmar directamente que las soluciones integradas sean la panacea para la protección de las grandes empresas".

Resumen de texto fuente:

Nuria Rabadán