

1. Como empresa especializada en formación, L&M Data Communications dispone de un lugar privilegiado para conocer cuáles son las últimas tendencias en el mercado de la seguridad TI. Supongo que la llegada del B2B y todos los procesos que tienen que ver con Internet debió ir acompañada de una evolución de las tecnologías de seguridad para adaptarse a los nuevos requerimientos. La explosión de movilidad y teletrabajo que estamos viviendo ha debido ser otro motor de empuje al negocio de la seguridad no sólo en términos de negocio, sino en el desarrollo de tecnología nueva. ¿Cuál es la tendencia? ¿En qué momento se encuentra el mercado de la seguridad informática y hasta qué punto todos estos cambios han hecho variar o evolucionar los conceptos o la forma de acometer los proyectos?

Tendencias tecnológicas

La movilidad y el teletrabajo ha requerido llevar la seguridad hasta un punto donde los sistemas remotos puedan entrar y autenticarse de forma segura dentro de los entornos corporativos. Sin duda alguna han sido los sistemas firewall que han extendido su capacidad para poder realizar comunicaciones cifradas tras organizaciones o bien contra usuarios individuales los que han hecho extender las posibilidades de la interconexión segura de este tipo de comunicaciones. Cada uno de estos aspectos configura los entornos de Redes Privadas Virtuales o VPNs donde el Firewall, aparte de un punto de control y filtrado, se convierte en la pieza clave para el cifrado/descifrado de la información.

En tecnologías también habría que nombrar el diseño de protocolos que incorporan dentro de sus definiciones los niveles de seguridad adecuados. Cada vez más la seguridad es un procedimiento incluido en los protocolos de transporte de las comunicaciones y del hardware específico.

Además, se produce otra interesante batalla tecnológica entre la velocidad de las redes de comunicaciones y los filtros a la información: Disponemos de dispositivos que son capaces de gestionar elevados anchos de banda para la interconexión de datos. Lo que ocurre es que, paralelamente y por problemas de seguridad, nos vemos obligados a tener que filtrar y analizar la información que entra y sale de nuestras empresas. Por un lado hemos conseguido superar sin problemas elevadas tasas de transmisión de datos pero por otro nos vemos forzados a incorporar elementos de control cada vez más sofisticados y rápidos para el análisis. Aunque ya están presentes en el mercado el futuro de la interconexión se adivina a través de electrónica de comunicaciones que directamente implemente componentes de filtrado avanzados. Por así decirlo vamos a tener una personalización de la seguridad desde el propio dispositivo que nos da servicio de red como podría ser un conmutador ATM o un concentrador de comunicaciones.

El mercado de la Seguridad

Respecto al momento en que se encuentra la seguridad informática claramente es una época donde la concienciación de las empresas y administraciones ha hecho que se implementen numerosas soluciones a medida en las organizaciones. Los productos de seguridad han proliferado en calidad y cantidad en el mercado actual y más

concretamente en los últimos cinco años de forma espectacular. Si bien no son perfectos si que han sufrido una evolución muy favorable.

La realidad también nos demuestra que las empresas se preocupan cada vez más por tener correctamente definidos planes de Seguridad corporativos en lugar de simplemente tratar de incorporar una serie de herramientas y/o sistemas específicos dedicados a la Seguridad.

La forma de acometer los Proyectos de Seguridad

Desde hace algún tiempo se comete el error de implantar la seguridad como un nivel o capa adicional con el que intentamos cubrir nuestros obsoletos o poco fiables sistemas y servicios de comunicaciones.

Con relación a la forma de acometer los proyectos de Seguridad cada vez más el cliente es consciente de que la clave del éxito de implantar un proyecto de Seguridad pasa más por una actualización de sus infraestructuras y el rediseño de su red que por incorporar complejas herramientas que le aporten seguridad.

2. ¿Cuáles son en su opinión las mayores lagunas o áreas más desprotegidas en el entorno corporativo, es decir, dónde tiene el distribuidor más oportunidad de negocio hoy en día?

Podemos simplificar el tratamiento de la seguridad en el entorno corporativo en dos grandes puntos: La seguridad por máquina, también denominada seguridad por *host*, y la seguridad por red.

La mejor forma de llevar a cabo un proyecto de seguridad corporativa es precisamente implementando la seguridad bajo la combinación de ambas aunque muchas veces resulte complicado, especialmente en las grandes organizaciones.

La seguridad por *host* incluye el conjunto de técnicas y herramientas que permiten que un ordenador se encuentre seguro: Sistema operativo correctamente configurado, políticas de backup, cifrado de ficheros, programas antivirus, programas de auditoría del propio sistema, etc. Aparte de las técnicas y herramientas criptográficas es importante recalcar que una componente muy importante para la protección de los sistemas consiste en la atención y vigilancia sistemática y continua por parte de los gestores de red.

Por otro lado, el segundo aspecto, la seguridad por red, engloba el conjunto de sistemas interconectados. Entran entonces a formar parte aspectos del tipo autenticación en red, sistemas cortafuegos o *firewalls*, programas de detección de intrusos (Intrusion Detection Systems o IDS), programas de auditoría en red, etc.

Si bien la seguridad por *host* había sido la más potenciada por el momento y marcaba claramente la tendencia de los últimos años a día de hoy es posiblemente la seguridad por red y sus productos asociados donde el distribuidor encuentra mayor número de

oportunidades. También es importante recalcar que cada vez más son los clientes que reclaman soluciones del tipo "llave en mano" para solucionar su seguridad corporativa en un momento puntual, sin tener clara la necesidad de tratar la seguridad como un proceso continuo.

También la migración de los procedimientos convencionales de transacciones de información dentro de la empresa a procedimientos telemáticos así como el desconocimiento real con respecto a la productividad que se pueda obtener hace que cualquiera de los sistemas basados en Infraestructura de Clave Pública PKI (Public Key Infrastructure) para la expedición de certificados digitales en una organización sea otro de los aspectos interesantes a desarrollar e implantar en muchas de las empresas actuales.

3. ¿Podría especificar cuáles son las áreas de mayor interés para el futuro según su conocimiento?

La seguridad, como otros muchos aspectos en las redes, tiene un enorme componente físico (seguridad de dispositivos) y lógico (políticas y servicios de seguridad de las organizaciones y empresas). Tan solo una combinación correcta de ambas permitirá aproximarnos a un modelo efectivo de seguridad en la red. La propia complejidad de las redes actuales es una dificultad para la detección y corrección de los múltiples y variados problemas de seguridad que van apareciendo. La seguridad como parte fundamental del diseño de las redes actuales habrá que especificarla correctamente a través de políticas y planes, decidir entre distribuir o concentrar así como de disponer de tecnologías y dispositivos avanzados que nos permitan una mayor efectividad en materia de seguridad de la información. Cualquiera de las áreas centradas en estos objetivos básicos son válidas e interesantes para cualquier empresa que quiera despuntar en el mundo de la seguridad.

Con respecto a las tendencias de dichas áreas deberíamos hacer la siguiente reflexión: Como ya sabemos, la seguridad es inversamente proporcional a los servicios ofertados. Los sistemas operativos actuales incluyen y requieren por parte de los usuarios mayor número de funcionalidades que, normalmente, se resuelven a través de emplear millones de líneas de código. Todo esto nos lleva a pensar que los sistemas de hoy en día puedan resultar incluso más vulnerables que aquel concepto de informática a través de sistemas monolíticos con poca flexibilidad de configuración para el usuario.

Como bien enuncia la ingeniería del software, los errores no se especifican, simplemente aparecen. Ahí está la clave. Por mucho que intentemos desarrollar aplicaciones estables, son demasiados factores los que entran en juego: Podemos disponer de un hardware mal diseñado, un sistema operativo con errores o mal configurado, e incluso el lenguaje de programación sobre el que estamos desarrollando nuestro código posiblemente incluya problemas de seguridad. Aparte de eso los propios protocolos que utilizamos para la comunicación pueden adolecer del mismo tipo de errores. El tiempo nos ha demostrado que, efectivamente, los problemas de inseguridad telemática son inherentes al propio diseño y, como tales, deberemos

seguir adaptándonos y configurando nuestros sistemas para aproximarnos a un modelo efectivo de seguridad.

Las técnicas de ataques cambian, los sistemas operativos se siguen desarrollando y las aplicaciones son cada vez más flexibles. De hecho es práctica habitual no sólo modificar las técnicas de ataque a los sistemas sino utilizarlas de forma combinada para que a los sistemas les sea cada vez más complicado detectarlos. También es cierto que hoy en día nos hemos acostumbrado a pagar la falta de depuración de los códigos de los programas a base de incrementar los recursos en nuestras máquinas: Añadir memoria, disco o más velocidad de CPU suele ser la forma habitual de solucionar los problemas asociados al rendimiento o la falta de depuración de los códigos de programación.

En cualquier caso saltar la seguridad de los sistemas seguirá siendo sólo cuestión de tiempo: El tiempo necesario para encontrar un fallo o para disponer de potencia de cálculo suficiente que nos permita descubrir o romper una determinada clave. Como casi siempre la solución será intentar que ese tiempo sea lo más amplio posible. Tampoco creo que debamos ser excesivamente pesimistas sobre el tema de la seguridad y la privacidad en la Red: La seguridad es un proceso continuo y un fenómeno que, como tal, deberemos aprender a saber vivir con él para intentar mejorarlo día a día.

4. Como empresa formadora, ¿actúa cómo centro de certificación oficial de algún fabricante de soluciones de seguridad?

Una de nuestras señas de identidad más importante es la independencia, por lo que no impartimos este tipo de cursos. Pero, además, querría hacer constar la aberración que supone el que sea admitido como normal que un fabricante pueda hacer "certificaciones oficiales". No quiere esto decir que los fabricantes no puedan impartir formación, ni mucho menos, pues ellos deben ser los que ofrezcan formación en sus productos. A lo que me quiero referir es a que, hoy en día, los usuarios consideran que los cursos de fabricantes son de tecnología, y así se planifica en muchos casos la formación. Como la enseñanza está necesariamente orientada a unos determinados productos, los asistentes a los cursos reciben información "viciada" que consideran como fiable. Es lo que podríamos denominar "formación con orejeras", pues limita el horizonte a lo que al fabricante le interesa.

Lo más lamentable es que, según las últimas estadísticas a las que hemos tenido acceso, nuestro país es el segundo del mundo en este tipo de formación, solamente superado por Estados Unidos. Si nos atenemos a la población o a la cifra de negocio en el sector, tendría que estar entre el vigésimo y el duodécimo. Esto es simplemente un indicador de la colonización tecnológica de que disfrutamos.

5. ¿Cuántos alumnos pasan por sus aulas anualmente para mejorar sus conocimientos en seguridad informática? ¿Cuántos de ellos son distribuidores de informática?

Por nuestras aulas pasan actualmente más de mil quinientos profesionales, de los que el número de distribuidores de informática es muy bajo. Desde nuestro punto de vista, la razón es la colonización tecnológica mencionada en la cuestión anterior.

6. ¿Qué porcentaje de su facturación está relacionado con los cursos de esta disciplina?

Los cursos específicos de seguridad son los que corresponden al "Programa Superior de Seguridad Avanzada en Redes IP e Internet" (<http://www.lmdata.es/psseg.htm>), pero el tema de seguridad se trata también en muchos otros apartados de los cuatro Programas Superiores, tres Cursos superiores y múltiples Cursos Monográficos que componen nuestras Áreas de Formación (<http://www.lmdata.es/areas.htm>). Por esta razón, es imposible saber exactamente el porcentaje de facturación relacionada con la seguridad, pero lo que sí podemos decir es que corresponde a una parte importante del total.