

La seguridad, tanto de los datos como del entorno físico, subió a la palestra a propósito del drama del 11-S.

Seguridad en los datos, una necesidad globalizadora

Algunas empresas que estaban en las Torres Gemelas contaban con una copia de seguridad de sus datos al otro lado del río Huston. Otras perdieron todos sus documentos imprescindibles, escrituras, contratos o la relación de pedidos y clientes. Muchas sobrevivieron gracias a internet, que en todo momento fue capaz de redireccionar la información. En algunos aspectos si hay un antes y un después del 11-S en seguridad de los datos. En general, la seguridad incumbe a todo el ámbito de la empresa, pero por la dificultad de abordar algo tan complejo vamos a centrar nuestro Café de Redacción en la protección de los datos. Y como también es inabarcable en el espacio de la revista tradicional, adjun-

tamos un CD en el que se recogen sin esta limitación artículos muy interesantes que completan la información. Este es el resumen de la conversación mantenida en torno a nuestra Mesa de Redacción, en la que participan Michael Behringer, de Cisco Systems; Hector Sánchez, de Microsoft; Luis Fuertes, por Veritas e Ignacio González, Proveedor de Servicios de Internet del IIES.

Los sucesos del 11-S tuvieron efectos devastadores sobre las empresas aparte, por supuesto, de la terrible pérdida de vidas humanas. Las empresas sufrieron un ataque a su seguridad y muchas perdieron los documentos más sensibles. ¿Va a haber un antes y un después del 11-S, en seguridad de los datos?

Michael Behringer. En general, ha aumentado la preocupación por la seguridad en las empresas. Algunas de las que sufrieron el ataque, pudieron recuperar gran parte de los datos porque los tenían depositados en otras sedes, incluso al otro lado del río Huston. Otras perdieron material muy importante. En general, la seguridad es algo global, que está en todo: en los edificios, en las bases de datos, en la red, etc. Si un punto falla, repercute en todos los demás. La realidad es que dependemos de que todos los puntos estén seguros y a veces las compañías lo olvidan.

Luis Fuertes. Yo diría que el 11-S fue un día crítico para la seguridad de los datos. Por un lado, está el garantizar la inviolabilidad de los datos frente a ataques externos y desde el 11-S se piensa en la protección física frente a posibles desastres. Hemos notado en mi compañía que en las empresas hay una mayor tendencia a la protección frente al desastre, a estrategias de recuperación. Sin embargo, no creo que el 11-S haya aumentado la preocupación por los piratas de la red, por ejemplo.

Héctor Sánchez. El 11-S lo que marca es una diferencia en el nivel de concienciación de las empresas que han visto que pueden perder en un día toda la información. Muchas se preguntan si sobrevivirían ante un suceso como este. Tal reflexión reposiciona la seguridad a su justo nivel de importancia ante no solo los responsables de IT de las empresas, sino ante los decisores de negocio de las mismas.



De izda a dcha: Michael Behringer, Luis Fuertes, Héctor Sánchez, Ignacio González y César Rico, en un momento del debate.

Ignacio González. Nosotros no hemos notado desde el Centro Servidor que haya más ataques de virus y demás desde fuera, a partir del 11-S. Lo que sí hay que destacar es que es importante mantener los niveles de seguridad internos en cuanto a accesibilidad incluso física del Centro. Hay que considerar la seguridad como un todo. Hay que evitar que alguien entre en la *password* de *root*, el administrador de sistemas debe impedir los accesos no deseados. El 11-S ha servido para que se vea que no sólo hay que tener bien guardados los datos, sino además repetidos y guardados en varios lugares distintos, para prevenir un desastre como este.

Michael Behringer. Nuestra preocupación es mayor ahora, pero también el 11-S ha constatado que ante un desastre como éste, las redes móviles y fijas no funcionaban, pero internet sí funcionó. Me da cierto orgullo a mí que trabajo con internet, ver que ante un gran problema, ha sido la plataforma más útil.

Ignacio González. La propia arquitectura de la red hizo que

funcionara, si no entrabas por un lado entrabas por otro. Hubo que buscar la forma, pero la red nunca se cayó. Había cuellos de botellas, eso sí.

Michael Behringer. Es debido a la arquitectura, desde luego: la forma de estrella de las redes telefónicas les hizo caer, en cambio la red de internet sobrevivió, aunque con problemas lógicos.

Luis Fuertes. A raíz de lo de las Torres Gemelas, hemos visto que sobrevivieron muchas empresas situadas allí porque anteriormente habían sufrido otro atentado el año 93 en el mismo sitio. Entonces sí que hubo bajas empresariales. Pero en esta ocasión ha sido menos grave porque estaban más preparadas. El 11-S debería servir para no preocuparse tanto por la empresa que si está preparada. Lo malo es que muchas no lo están, en una encuesta reciente a 700 empresas europeas emerge un 12 por ciento sin plan de recuperación de desastres. Es un porcentaje muy alto porque se trata de grandes compañías. Se

ha despertado interés por la seguridad, pero no suficiente.

¿Ocurre igual en el caso de las empresas españolas?

Luis Fuertes. Muchas funcionan con una preocupación mínima, se limitan a hacer un "back-up" (copia) y a guardarlo en otro sitio, algunas llegan incluso a meterlo en una caja ignífuga, pero poco más. No tengo datos de España, pero en Europa en menos de un 20 por ciento de las compañías el Consejo de Administración se involucra en la Recuperación de Desastres, mientras que en EEUU, el 90 por ciento de los Consejos lo hace.

Héctor Sánchez. La recuperación de datos ante desastres constituirá un importante mercado para la Banda Ancha, mercado ávido de proporcionar contenidos y servicios. Serán fundamentales las soluciones de arquitecturas de sistemas ya probadas en origen por los diferentes fabricantes (p.e. Microsoft y CISCO) y ofrecida en la forma de solución (p.e. Microsoft Solutions Architecture)

Es una vía clara para que el integrador final implante de forma más sencilla y controlada sus soluciones de arquitectura. Esas integraciones de los equipos de los distintos fabricantes tendrán un mercado mucho más amplio por la reducción de costes y tiempo que conlleva su despliegue.

Ignacio González. Pienso que son mayoría las empresas en España, en general, no se cuida la seguridad en los sistemas lo suficiente desde la alta dirección, no se facilitan las herramientas necesarias a los administradores. Creen que es suficiente lo que hay, no invierten en seguridad ni lo consideran un capítulo imprescindible que añadir en los presupuestos anuales. Para mí, es un aspecto poco cuidado, que se confía al responsable de cada departamento sin asumir que es algo imprescindible para todos. Hacen falta herramientas que no se facilitan y eso es algo que ocurre en casi todas las empresas españolas.

Michael Behringer. Hoy en día hay muchas soluciones, internet ha cambiado el rumbo. Se puede hacer la copia y trasladarla por redes de larga distancia gracias a internet, ahí entran nuevas soluciones que interesan al mercado desde el 11-S: es *Storage Areal Networking* (SAN) (almacenamiento sectorial en red). Es una posibilidad de llevar la réplica a otra parte del mundo por internet, más fácil y más barato que con cintas.

Luis Fuertes. De todas formas, la copia en cintas no se van a poder eliminar nunca porque

una réplica de datos a larga distancia necesita un *back-up* en cinta previo, por si hay alguna pérdida de datos o algún fallo. Es necesario utilizar soluciones de banda ancha que permita enviar réplicas de un sitio a otro y disponer de un centro alternativo para recuperar los datos. Muchas empresas afectadas, el 11-S sobrevivieron por la réplica que tenían al otro lado del río, gracias a la fibra óptica tirada por debajo del agua. Pero las empresas desconfían también de que sus datos estén guardados en forma fiable y en buen sitio. Por eso hay que ofrecer soluciones de encriptación muy seguras.

En cuanto a los virus y los anti-virus que tanto aburren al usuario ¿no debería detectarlos la misma red para evitarle problemas?

Héctor Sánchez. Los códigos maliciosos, también llamados malware (virus, caballos de troya, gusanos etc.) son en efecto un constante dolor de cabeza para todo tipo de usuarios tanto particulares como empresariales.

La mejor protección pasa, por llevar a cabo dos acciones fundamentales: evitar la ejecución de códigos cuya procedencia no sea conocida o de confianza y por otro lado, mantener nuestro sistema actualizado constantemente en materia de parches y updates de seguridad. Son dos medidas muy básicas pero extremadamente eficaces. Y fáciles de implantar en la actualidad: Las Software Restriction Policies de Windows XP impiden que el usuario ejecute nada que no sea previamente aprobado por el administrador. Esta drástica medida aumenta



Michael Behringer: “La seguridad es algo global, está en los edificios, en las bases de datos, en la red. Si un punto falla, repercute en el todo”

muchos enteros el nivel de seguridad.

Por otro lado Windows Update (así como su versión para la empresa: Software Update Services), permiten que tan pronto como el fabricante saque un parche de seguridad el usuario tenga la opción inmediata de instalarlo.

Michael Behringer. Los virus muestran los problemas de los sistemas operativos de los PCs y explotan la vulnerabilidad de los equipos. Los sistemas operativos de las empresas son más restrictivos, pero en las casas es más difícil porque los usuarios no tienen por qué ser expertos y están menos defendidos.

Por otro lado, el Pc de la oficina pertenece al usuario según el concepto que mantenemos, aunque sea de la empresa. Este concepto hace que en la oficina el usuario no acepte bien que se le limite y el control se debe hacer en el interior de la red, más que en el mismo Pc.

Héctor Sánchez. Los usuarios debemos empezar a diferenciar muy bien el uso que hacemos del Pc en la empresa y en la casa. En la empresa el Pc es un activo de la empresa y debe ejecutar sólo lo que la empresa permite. Los usuarios empresariales no podemos poner en jaque una red corporativa por haber eje-

cutado un software de dudosa procedencia.

Michael Behringer. Es así, pero en muchas empresas necesitamos libertad para movernos, en la mía trabajamos con las últimas aplicaciones y las cogemos de otros sitios para estudiarlas y demás. No podríamos funcionar con un sistema restrictivo. Y pasará igual en otras.

Ignacio González. De poco sirve instalar un antivirus en un PC de un empleado si luego éste no lo actualiza adecuadamente o no tiene cuidado con los archivos adjuntos que recibe. O si ejecuta cualquier cosa que circula por la red. Es, por tanto, el propio usuario el que debe de tener el mayor cuidado con los virus y el sentido común es normalmente el mejor aliado.

¿Cómo se gestiona la calidad en seguridad, existe un manual, hay auditorías?

Héctor Sánchez. Existe normativa y procedimientos al respecto como la British Standard 17799, que define los pasos técnicos y los procedimientos correctos para implantar una política de seguridad. Tenemos en estos momentos localmente a AENOR que acaba de sacar una serie de especificaciones y normativas de seguridad muy interesantes.

La normativa o el procedimiento existe, pero la implantación no es en absoluto sencilla ni exenta de costes.

Luis Fuertes. Lo cierto es que la seguridad tiene que evolucionar hacia el control de calidad. Ahora mismo, incluso las pequeñas empresas se plante-

an que la certificación de calidad es obligatoria, lo regula el propio mercado si es que no se trata de un sector donde ya sea obligatorio. En seguridad, una empresa proveedora necesita sentirse segura al intercambiar de información con otra.

Michael Behringer. Cada empresa lleva su sistema. En Cisco existe la política de seguridad que define qué se puede hacer en la red, en el acceso remoto a la empresa o a la red corporativa. Hay normas estrictas si conectas con un laboratorio por la red, por ejemplo, para impedir que entren datos falsos, etc. La cuestión es la calidad. Nosotros hacemos incapié en la seguridad, es imprescindible crear en la empresa la conciencia de la seguridad, luego se establece el estándar, pero ello sólo no va a solucionar el problema.

Héctor Sánchez. En España tenemos ya en vigor una Ley de Protección de Datos Personales, y una Agencia de Protección de Datos, que obliga a las empresas a protegerlos por ley, con una serie de requerimientos de protección en función de la sensibilidad del dato.

La LOPD puede ser un motor para agilizar la existencia de políticas de seguridad en las empresas españolas, más allá de la protección del dato personal

Las auditorías ¿son un buen camino para controlar la propia seguridad?

Luis Fuertes. Nosotros auditamos a las empresas desde el punto de vista de la protección fiscal. Existen auditoras de seguridad, desde luego, españolas y extranjeras. Nosotros lo



Luis Fuertes: “Desde el 11-S se nota en las empresas mayor preocupación por la protección frente a desastres y la estrategia de recuperación”



Héctor Sánchez: “Los usuarios debemos empezar a diferenciar el uso que hacemos del PC en la empresa y en la casa. En la empresa el PC es un activo que debe ejecutar sólo lo que la empresa permite”

que hacemos es analizar riesgos y advertir al cliente de la probabilidad de superar los desastres físicos o lógicos, sin pérdida de datos.

Michael Behringer. Los datos de auditorías de que disponemos, hechas por equipos especializados, son muy preocupantes. Las encuestas estudian cuatro puntos sensibles: conectarse con internet, desde la línea telefónica, desde la red interna y desde los inalámbricos. Resulta que cerca de un 60 por ciento de las compañías son vulnerables por internet y no les preocupa. Además, el 100 por cien es vulnerable por internet desde dentro. Una vez enchufado en la red interna, puede pasar de todo.

Héctor Sánchez. Hay empresas que buscan la ayuda de *hackers* para que les desvelen sus puntos débiles en seguridad. Muchas grandes entidades financieras o de telecomunicaciones buscan este tipo de ayuda, denominada con frecuencia como “Hacking ético”.

Ignacio González. Hay otro aspecto preocupante y es que en la misma red hay programitas que enseñan o dirigen a cualquiera para introducirse en un sitio, sin necesidad de tener grandes conocimientos. Ya no se trata de un pirata que tenga un objetivo concreto y sepa por dónde anda, sino que hay un *software-kivi* que cualquier chavalín por jugar puede emplear y hacer daño sin prever las consecuencias. Es necesario estar protegido contra este tipo de ataques que van contra elementos tan sensibles como la clave de acceso, por ejemplo. Y en la dirección de las empresas, como decía

Café de redacción

antes, no hay suficiente preocupación por aportar los medios que garanticen la seguridad a un buen nivel. Y es que siempre pueden entrar por el puerto del http, aunque se busque la forma de cerrar el hueco de acceso.

Michael Behringer. Es cierto, lo que pasa es que están descubriendo vulnerabilidades específicas, aunque su gran mayoría no puede pasar a través de un cortafuegos (firewalls). Esta amenaza es mucho más peligrosa dentro de una empresa que entrando por internet. La relación de intrusos es mucho mayor desde dentro de la red interna de la empresa. Por eso se ponen cada vez más *firewalls*, se separan departamentos, se ponen claves.

El panorama resulta aterrador si pensamos que ahora las conexiones van a ser cada vez más abiertas, por ADSL, inalámbricas ¿qué soluciones hay?

Michael Behringer. Personalmente, creo que se puede confiar en las soluciones que tenemos, uso la banca por internet y confío en los mecanismos de defensa. No diría que las redes sean cien por cien seguros, pero nada lo es. Por lo general el riesgo es lo suficientemente bajo con las medidas habituales para poder aprovechar las ventajas de internet.

Héctor Sánchez. Hay que acercar al usuario medio las medidas de protección básicas. Por eso, es importante que el fabricante proporcione configuraciones por defecto más seguras, accesibles no solo a los usuarios avanzados.



Ignacio González: “En España, en general, no se cuida la seguridad en los sistemas lo suficiente desde la alta dirección, no se facilitan las herramientas necesarias a los administradores”

Tanto en el mundo de los servidores como en el del desktop, en Microsoft tenemos iniciativas en marcha a ese respecto (Secure by Default) para que los sistemas instalados por personal sin experiencia tengan mayores grados de seguridad. Como ejemplo, el actual windows XP tiene un Firewall personal de conexión a Internet con todas las

garantías (certificado por ICSA, inspección de estados), pero no es la opción habilitada por defecto.

En futuras releases del sistema de Desktop esa será la opción habilitada por defecto. Medidas como esta incorporan bajo el paraguas de la mayor seguridad a todo tipo de usuarios, y no solo a los más experimentados.

Para los sistemas de radio ¿el encriptado va a ser la protección común?

Michael Behringer. Los inalámbricos son un tema aparte. El estándar de encriptación era bastante vulnerable. Las empresas que hacen estos equipos han encontrado una manera de evitarlo ellos dicen que, si necesitas protección, hazlo en el ordenador. En mi empresa usamos una versión segura, la red que utilizamos está cifrada con su propia clave, cada paquete tiene otra clave. Así es completamente seguro. Si no hay cifrado de red en el wireless (inalámbrico) todavía se puede usar el WPClients que corre en el Pc y que conecta con la empresa. Es un cifrado a otro nivel, las soluciones existen, se puede trabajar en casa como en la oficina, con la misma seguridad, y cada día las medidas son más fáciles de implementar.

Héctor Sánchez. En nuestra compañía hay un trabajo muy avanzado del departamento de investigación sobre una arquitectura básica de Pc que incluye altos estándares de seguridad. Digamos que trata de incluirla desde el principio en el mismo diseño del ordenador. Encripta los distintos elementos que lo componen y su relación entre uno y otro: el mismo teclado, la pantalla, la cpu. Se encriptan con parámetros propios de la máquina, con chips diferentes en los procesos más críticos del sistema.

Muchas fases de este programa están en periodo de decisión pero responderá a las necesidades de seguridad que hoy en día y en un futuro cercano tendremos. 