Serie Executive

Aspectos esenciales de la seguridad para los directores de Tecnologías de la Información

Aunar la innovación con la confianza

IBM

Las compañías en la actualidad reciben cada día nuevos torrentes de información, que les permiten realizar análisis instantáneos y la toma de decisiones más acertadas. Las conexiones entre empleados, clientes y contratistas se han multiplicado de forma exponencial, a través de una amplia gama de tecnologías. Sin embargo, estas extensas redes superpuestas plantean enormes dificultades en materia de seguridad. La complejidad es abrumadora, y los posibles puntos de ataque casi infinitos. Los directores de Tecnologías de la Información (CIO) se ven sumidos en una creciente frustración, y en un mar de dudas, preguntándose con frecuencia si es posible disponer de un sólido sistema de seguridad en una era hiperconectada. La respuesta es afirmativa, pero esto requiere cambios esenciales en los procesos y actitudes. IBM ha puesto en marcha su propia estrategia interna y ha definido los diez elementos esenciales para una seguridad inteligente en el siglo XXI.

Cuando amanece en Nueva York, el Vicepresidente de Ventas se levanta de la cama, revisa su smartphone y ve que ha surgido una gran oportunidad en Malasia. Esta noticia desencadena una cascada de comunicaciones. Antes del desayuno, seis miembros del equipo global celebran una teleconferencia, uno de ellos a través de una conexión de Skype desde Estocolmo. Tres contratistas llaman por los teléfonos móviles. Durante todo el día, se entrecruzan correos electrónicos por todo el mundo, aproximadamente la mitad de ellos a través de la red corporativa, otros en Gmail y Yahoo. Cuando cae la noche en Nueva York, se cierra el acuerdo. En las horas siguientes, algunos de los participantes se conectan unos a otros en LinkedIn.

El 91%

de los usuarios de smartphones de las compañías se conectan al correo electrónico de la empresa, pero sólo a uno de cada tres se le ha solicitado que instale un software de seguridad en el móvil.

Datos: Kaspersky Labs
http://usa.kaspersky.com/sites/usa.kaspersky.com/files/Enterprise%20Mobile%20Survey.pdf

No es ningún secreto que hoy en día los administradores pueden acumular conocimientos y gigabytes de datos en un instante, y utilizarlos para adoptar decisiones más rápidas y basadas en información de mejor calidad. Sin embargo, las ventajas que suponen estas redes interconectadas –su velocidad y apertura, el fácil acceso desde cualquier lugar del mundo– también crean una gran cantidad de vulnerabilidades. Y a medida que la información se vierte desde miles de dispositivos y a través de numerosos servicios públicos basados en la web, la labor de garantizar la seguridad de la red de una empresa incrementa infinitamente su complejidad. Un estudio de Kaspersky Labs nos muestra que el 91% de los usuarios de smartphones de las compañías se conecta al correo electrónico de la empresa, pero sólo a uno de cada tres se le ha solicitado que instale un software de seguridad en el móvil. Debido a ello, el acceso es muy fácil para todos los involucrados, lo que con frecuencia incluye a las organizaciones criminales.

Los delincuentes consideran en la actualidad a los ordenadores conectados a Internet y los dispositivos móviles como un lugar idóneo para actuar. Al infectar los dispositivos con malware difícil de detectar, amplían sus bases de operaciones. Para los ladrones, las redes corporativas están repletas de tesoros digitales, incluyendo contraseñas, identidades de usuarios, secretos comerciales e información personal.

Los intrusos digitales también tienen como objetivo ciertos activos estratégicos, como los ministerios públicos o las redes de comunicación. Algunos delincuentes tienen como objetivo interrumpir las operaciones empresariales. Según las estimaciones de Gartner, entre el 20 y 30 por ciento de los equipos han estado en peligro debido a ataques de botnets y malware que se pueden utilizar como infraestructura de base para las operaciones delictivas. Puesto que muchas compañías permiten la utilización en la empresa de dispositivos de propiedad privada, el potencial de infección es un problema tangible.

Entre el 20 y el 30%
de los ordenadores de los consumidores almacenan programas maliciosos y trabajan a tiempo parcial para los delincuentes.

Source: http://www.computerweekly.com/opinion/CW-Security-Think-Tank-How-to-prevent-security-breaches-from-personal-devices-in-the-workplace

Un solo ordenador infectado puede causar daños de gravedad. Uno de los ejemplos más inquietantes hasta la fecha es Stuxnet, un gusano altamente sofisticado diseñado para paralizar software y equipos industriales. En la primavera de 2009, el gusano comenzó a propagarse mediante máquinas, la mayoría de ellas en Irán. Al parecer, alguien lo había introducido a través de una memoria USB contaminada. Desarrollado para atacar máquinas que ejecutaban un programa de software Siemens, el gusano causó estragos en numerosos sistemas industriales.

La lección para los líderes en materia de la seguridad de las compañías está clara. Si un gusano puede diseminarse en una industria altamente protegida en Irán y en el extranjero, ¿no sería mucho más fácil encontrar una apertura entre los profesionales conectados por medio de Twitter, Facebook, mensajes de texto y Skype? Más aún, si un gusano puede desactivar equipos industriales, ¿no podría interrumpir las cadenas de suministro, desviar el tráfico, o dañar las redes eléctricas, entre otras catástrofes? Pues en una palabra, sí.

Para afrontar estos retos cada vez más acuciantes, las compañías necesitan **una nueva raza de líderes en seguridad.** Naturalmente, deben estar al día en lo relativo a innumerables amenazas tecnológicas, pero también a cuestiones estratégicas. ¿Qué información debe ser compartida en general? ¿Quién debe tener acceso a ciertas cuestiones de primera magnitud, y cómo van a ser protegidas? La combinación de los retos técnicos y de los retos estratégicos alcanza una complejidad vertiginosa. Y si bien se puede caer en la tentación de responder con soluciones igualmente complejas, los ejecutivos con visión de largo alcance se han dado cuenta de que esta escalada es insostenible, inasequible, y en última instancia, infructuosa.

La única respuesta es la de cambiar, en un nivel fundamental, los modos de funcionamiento de las compañías. Lo primero es **ampliar el ámbito de la seguridad de la empresa,** incluyendo el personal técnico y sus máquinas, y también a todos los miembros de la empresa y a todos los que hacen negocios con ella. Esto es lógico: debido a que cada persona constituye una vulnerabilidad potencial, también cada persona debe representar una parte de la solución. Al fin y al cabo, el éxito depende de crear una concienciación sólida y persistente: **una cultura consciente de los riesgos.**

Una cultura consciente de los riesgos exige mucho más que una tecnología actualizada, y va mucho más allá de las mejores prácticas. Representa una nueva forma de pensar, adoptando un enfoque pragmático de seguridad ante cada decisión y procedimiento en todos los niveles de la empresa. Debemos reconfigurar los métodos utilizados para la gestión de la información, incluyendo desde los niveles de dirección hasta los estudiantes en prácticas del verano. En esta cultura, los procedimientos seguros para los datos se deben convertir en algo cotidiano, similar a abrocharse un cinturón de seguridad o guardar las cerillas en un lugar seguro.

Representa una nueva forma de pensar, adoptando un enfoque pragmático de seguridad ante cada decisión y procedimiento en todos los niveles de la empresa.

No es una decisión que pueda posponerse. La seguridad de la empresa se está acercando rápidamente a un punto de inflexión. Consideremos los elementos de juicio: en el entorno criminal, los profesionales han sustituido ya a los aficionados, incrementándose por ello el nivel de amenaza. Al mismo tiempo, las compañías han ganado en productividad y han dado más poder a los trabajadores al difundir ampliamente un aluvión de datos digitales en operaciones, marketing, ventas y servicio al cliente. De esta forma, se ha multiplicado la vulnerabilidad. Y debido a que la casi totalidad de la actividad comercial de las compañías en la actualidad es administrada digitalmente, las consecuencias de una vulnerabilidad pueden hacer tambalearse a toda la empresa. En suma: los ladrones son más hábiles, disponen de innumerables puertas y ventanas digitales para penetrar en una empresa, y la información almacenada dentro de la misma tiene un valor incalculable.

Mientras que los riesgos son enormes, el camino hacia la seguridad puede parecer desalentador, y además, confuso. Aunque hoy en día existen numerosos productos y servicios de seguridad en el mercado, nuestros clientes nos comentan que a menudo se sienten frustrados por un mercado de seguridad que, en su opinión, va dando bandazos de titular a titular, buscando relevancia en la última crisis de seguridad o en las exigencias del cumplimiento. Muchos de ellos no saben por dónde empezar o a quién creer, y con frecuencia describen la seguridad y el cumplimiento como una inversión de valor imposible de calcular, con una dudosa rentabilidad de la inversión (ROI) y con tanto atractivo como badenes en medio de una autopista. Esta confusión a menudo conduce a la falta de decisión, o aún peor, a la decisión de renunciar a la innovación debido al miedo.

No podemos dejar de lado el hecho de que garantizar la seguridad de una empresa es una empresa formidable, que nunca se termina. Más aún, cambiar una cultura es una tarea difícil. Pero se trata de una labor esencial. Un sólido sistema de seguridad es un coste necesario para mantenerse en el mundo de los negocios, y llegar a conseguirlo está a nuestro alcance.

En IBM nos esforzamos constantemente en hallar el equilibrio entre la innovación necesaria y la necesidad de controlar el riesgo. La respuesta integral de la compañía incluye medidas tecnológicas, de procesos y políticas. Implica diez prácticas esenciales. En los próximos meses, vamos a distribuir una serie de documentos técnicos para que pueda usted estudiarlos más detalladamente. Por el momento, este es un breve resumen:

Nuestros elementos de seguridad esenciales

1. Desarrollar una cultura consciente de los riesgos

Se trata de una idea elemental. Cualquier persona puede infectar una empresa, al hacer clic en un archivo adjunto dudoso, o al no instalar un dispositivo de seguridad en un smartphone. Por ello, el esfuerzo para crear una empresa segura debe incluir a todos los empleados. El establecimiento de una cultura del riesgo implica la definición de los riesgos y las metas y la difusión de información acerca de ellos. Pero el cambio más importante es el cambio cultural. Solo hay que pensar en la reacción automática, incluso la alarma, que muchos experimentan si ven a un padre hablando a gritos por un teléfono móvil mientras su hijo corre hacia la calle. Esa misma intolerancia debe existir, en el ámbito de la compañía, cuando los compañeros de trabajo descuidan la seguridad. Por supuesto, la dirección tiene que impulsar este cambio sin descanso desde lo alto, implementando mientras tanto las herramientas necesarias para realizar un seguimiento del progreso.

2. Gestionar los incidentes y responder a ellos

Pongamos por ejemplo que se producen dos problemas de seguridad similares, uno en Brasil y el otro en Pittsburgh. Pueden estar relacionados. Pero sin la inteligencia de seguridad necesaria para vincularlos, puede pasarnos inadvertido un patrón importante, que podría indicar un posible incidente. Es esencial realizar un esfuerzo generalizado en el ámbito de la empresa para aplicar un análisis inteligente y capacidades de respuesta automatizadas. La creación de un sistema automatizado y unificado permitirá a la empresa monitorizar sus operaciones internas y responder rápidamente a los problemas.

3. Defender el lugar de trabajo

Los ciberdelincuentes están constantemente sondeando los puntos débiles. Cualquier puesto de trabajo, ordenador portátil o smartphone ofrece una posible apertura para ataques maliciosos. La configuración de cualquier dispositivo no debe quedar en manos de individuos o de grupos autónomos. Todos deben estar sujetos a una gestión y aplicación centralizada. Asimismo, los flujos de datos dentro de una empresa tendrán que ser clasificados, cada uno con su propio perfil de riesgo, y canalizados exclusivamente a su círculo de usuarios. La seguridad del personal implica vencer el caos y reemplazarlo por la confianza.

4. La seguridad por medio del diseño

Imagínese si las compañías automovilísticas fabricasen sus coches sin cinturones de seguridad o sin airbags, y, a continuación, los añadieran más adelante, en respuesta a problemas o accidentes. Esto no tendría ningún sentido, y sería exageradamente caro. Igualmente, una de las mayores vulnerabilidades de los sistemas de información –y el mayor desperdicio de dinero– proviene de implementar en primer lugar la prestación de los servicios, y, a continuación, añadir la seguridad como idea secundaria. La única solución es la aplicación de medidas de seguridad desde el principio, y llevar a cabo de manera regular comprobaciones automáticas para determinar el cumplimiento. Esto también ahorra dinero. Si construir una función de seguridad en una aplicación cuesta 40 libras esterlinas adicionales, puede costar hasta 100 veces más –4.000 libras esterlinas– añadirla más adelante.

5. Limpieza de programas y versiones anteriores

Hablemos de un problema que sucede frecuentemente: los empleados continúan utilizando programas de software ya anticuados porque los conocen y se sienten más cómodos con ellos. Pero la administración de las actualizaciones en un conjunto de múltiples programas de software puede ser una labor imposible. Además, las compañías de software con frecuencia dejan de realizar aplicaciones de seguridad para los programas más antiguos, algo que los delincuentes cibernéticos saben muy bien. En un sistema seguro, los administradores pueden realizar un seguimiento de cada programa que se ejecuta, verificar que la versión está actualizada y disponer de un sistema exhaustivo, en lugar de instalar las actualizaciones y parches a medida que se liberan.

6. Controlar el acceso a la red

Consideremos la delincuencia urbana. El control del orden público sería mucho más fácil si cada uno de los vehículos que circulan por la ciudad llevase una identificación de radio única y viajase a lo largo de un cierto número de avenidas principales, cada una de ellas equipada con sensores. Lo mismo ocurre con los datos. Las compañías que canalizan los datos registrados mediante puntos de acceso monitorizados tendrán mucho más fácil detectar y aislar el malware.

7. Seguridad en la nube

La computación en nube promete enormes ventajas. Sin embargo, puede implicar ciertos riesgos. Si una empresa realiza la migración de algunos servicios de TI a la nube, estará en una estrecha vecindad con muchas otras personas, posiblemente incluyendo a profesionales de la estafa. En ese sentido, una nube es como un hotel en el que un determinado porcentaje de los clientes ha contraído la peste bubónica. Para sobrevivir en este entorno, los huéspedes deben disponer de herramientas y procedimientos para aislarse de los demás y vigilar posibles amenazas.

8. Patrullar el barrio

Pongamos que un contratista necesita acceso al sistema. ¿Cómo puede asegurarse de que dispone de las contraseñas adecuadas? ¿Se las envía a la agenda electrónica? ¿Se las envía por medio de un mensaje de texto? Tal improvisación tiene sus riesgos. La cultura de seguridad de la empresa debe extenderse más allá de sus muros, y debe establecer las mejores prácticas entre sus proveedores y contratistas. Este es un proceso similar al del interés por el control de calidad hace una generación. La lógica es la misma: la seguridad, como la excelencia, debe infundirse a través de todo el ecosistema. Los efectos devastadores de la negligencia en una compañía pueden convulsionar a sectores enteros de la sociedad.

9. Proteger los activos más valiosos de la compañía

En algún lugar de la cámara del tesoro están depositados los activos esenciales de la empresa, como por ejemplo sus datos científicos y técnicos, tal vez algunos documentos sobre posibles fusiones y adquisiciones, o la información financiera confidencial de los clientes. Cada empresa debe llevar a cabo un inventario, y los datos críticos deben recibir un trato especial. Cualquier elemento prioritario debe ser custodiado, vigilado y encriptado como si la supervivencia de la empresa dependiera de ello. De hecho, en algunos casos, puede que sea así.

10. Seguimiento individualizado

Pongamos el caso de una persona que trabaja para una empresa a tiempo completo. Transcurren seis meses y consigue un ascenso. Un año más tarde, aparece un competidor y contrata sus servicios, dejando la compañía. ¿Cómo trata el sistema a esta persona a lo largo del tiempo? En primer lugar, debe facilitarle un acceso limitado a los datos, y a continuación, se le abren más puertas, antes de que finalmente se le restrinja el acceso. Se trata de la gestión del ciclo de vida de las identidades. Es un elemento de vital importancia. Las compañías que administran este ciclo de forma incorrecta están operando a ciegas y pueden ser vulnerables a intrusiones. Este riesgo puede resolverse mediante la aplicación de sistemas meticulosos para identificar a las personas, gestionar sus permisos y revocarlos tan pronto como dejan la empresa.

¿Cómo podemos aunar la innovación con la confianza?

El equilibrio entre la gestión del riesgo y la habilitación de la innovación

Unirse a la conversación

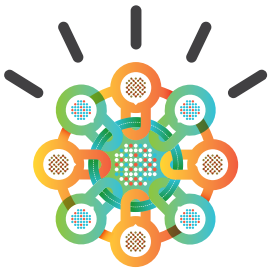
Para leer otros artículos, obtener más información o compartir sus opiniones con otros líderes en seguridad, únase a nosotros en **ibm.com/smarter/cai/security**.

Acerca de la autora

Kristin Lovejoy es Vicepresidente de Riesgos TI, Oficina del CIO, IBM. Correo electrónico de contacto: **klovejoy@us.ibm.com**.

Sobre el IBM Centre for Applied Insights

El IBM Centre for Applied Insights combina la profundidad en los contenidos y la experiencia analítica, a fin de ayudar a localizar nuevo valor añadido para los clientes. El Centro realiza actividades de investigación y genera activos y herramientas con una orientación pragmática para promover a las organizaciones a actuar.



IBM España
Santa Hortensia, 26-28
28002 Madrid
España

CIE03116-ESES-00