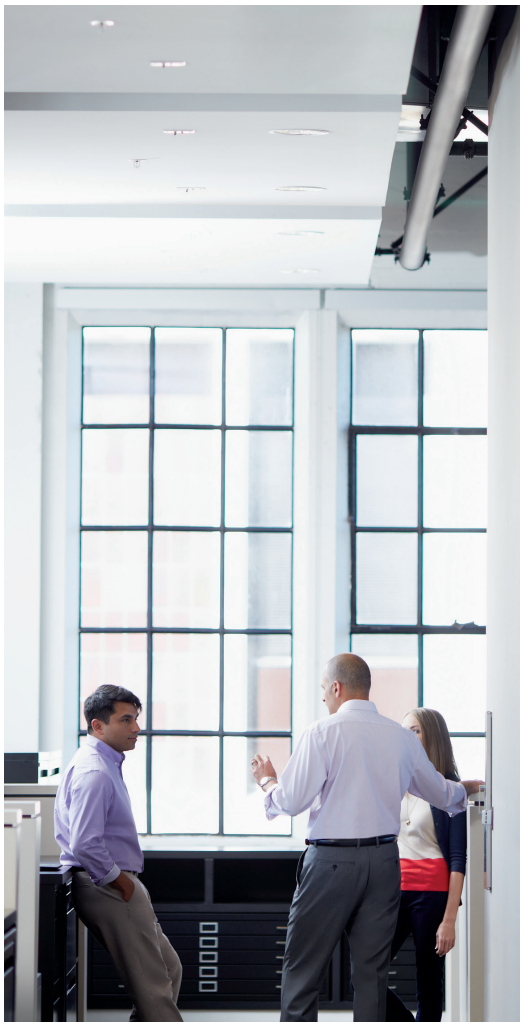
Cinco preguntas que los ejecutivos necesitan hacer a sus equipos de seguridad

Office

Microsoft



Las infracciones de datos son más que un problema de seguridad. Un ataque importante puede perjudicar a su base de clientes, a las relaciones con partners, al material administrativo, o incluso a los beneficios e ingresos. En el pasado, las infracciones de datos se cobraron empleos de ejecutivos, produjeron pérdidas de ingresos importantes y dañaron la reputación de las marcas. Según un estudio sobre la reputación de las marcas de 700 consumidores realizado en 2014 por Ponemon Institute, las infracciones de datos fueron el hecho más perjudicial para la reputación de una marca, superando a los desastres medioambientales y a un servicio de atención al cliente deficiente.[1] En un mundo donde las infracciones de datos son algo habitual, ¿qué pasos se pueden realizar para minimizar los daños?

En 2015 se produjeron 781 infracciones de seguridad, mientras que en 2014 se produjeron 783.[2]

[1] Experian: Las consecuencias de una infracción de datos
[2] Informe sobre infracciones de datos realizado por ID Theft Center en 2015

La media del coste total consolidado de una infracción de datos en 2015 fue de 3,8 millones de dólares (un aumento del 23 % desde 2013).

Estudio sobre el coste de las infracciones de datos realizado por IBM en 2015

Las infracciones de seguridad afectan a toda la organización y por este motivo, el equipo directivo necesita unir sus fuerzas con los directores de seguridad en su lucha para la seguridad empresarial.

Aunque los directores de seguridad, los directores de seguridad de la información y los analistas de seguridad son la primera línea de defensa contra los hackers, no tienen que considerarse como la última y única línea de defensa. Los directores de seguridad, que suelen ser los responsables de administrar los riesgos financieros de una corporación, tienen que preguntarse cuáles son los riesgos empresariales de la ciberseguridad. Además, aunque otros roles ejecutivos no tienen medidas de seguridad a su alcance, pueden tomar medidas para ayudar a mejorar la seguridad global de las organizaciones.

- Los directores de tecnología pueden asesorar a los directores de seguridad y a los directores de seguridad de la información sobre el software de seguridad implementado en su organización, pero también necesitan centrarse en las características de seguridad de toda la tecnología implementada.
- Los directores de marketing y los ejecutivos de marketing responsables dela reputación pública de sus compañías tienen queser conscientes de los riesgos para la reputación que pueden producirse debido a una infracción y desarrollar un plan ante un ataque para proteger al máximo los ingresos por ventas.
- Los departamentos de recursos humanos tienen que conocer la forma en que una infracción de información interna puede afectar a la confianza de los empleados y, por lo tanto, necesitan centrarse en proteger la información confidencial que administran.
- Los consejeros delegados y los miembros del consejo tienen que reconocer las posibles implicaciones de una ciberseguridad defectuosa en el valor de sus compañías y dar prioridad a la seguridad en el plan de desarrollo de su empresa.

En relación con la protección de los activos organizativos más importantes, ¿qué necesita preguntar el equipo directivo a sus equipos de seguridad?

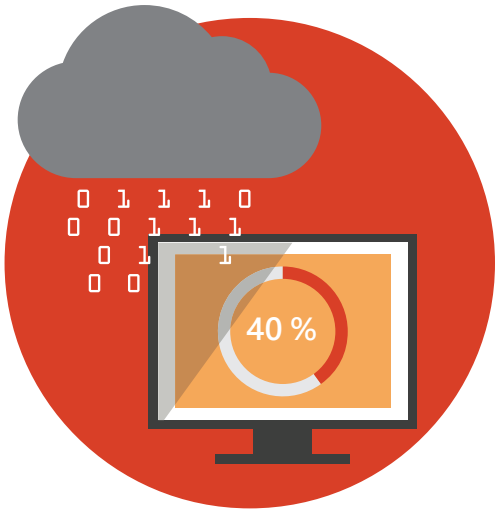
PREGUNTA 1

¿Con qué frecuencia ve que se usan servicios en la nube no autorizados?

Dropbox. Google Drive. MediaFire. Egnyte. Aunque puede que no se admitan en su organización, es probable que miembros del equipo de seguridad hayan visto cómo se usaban una o más de estas nubes privadas en alguna organización.

Las "nubes no autorizadas" (las opciones de sincronización y uso compartido de archivos privados no admitidas o protegidas por la infraestructura de TI de una empresa) se están introduciendo lentamente en las organizaciones. Según un estudio realizado en 2013 por Symantec, el 77 % de todas las empresas experimentaron situaciones de nube no autorizada.[3]

Para eliminar las nubes no autorizadas, los equipos de seguridad necesitan hablar con sus directores de tecnología sobre el servicio en la nube autorizado recomendado por la organización. Después, otros miembros del equipo directivo pueden valorar la solución que será más útil para sus empleados y socios comerciales. Consulte con sus equipos de seguridad sobre la implementación de soluciones en la nube admitidas en toda la organización. Las soluciones de nivel de empresa, como Microsoft OneDrive, permiten a los empleados guardar, compartir y colaborar en documentos sin poner en peligro la seguridad de los datos.



El 40% de las organizaciones que experimentaron situaciones en la nube no autorizada vieron expuestos sus datos confidenciales.[3]

[3] Estudio de Symantec: Evitar los costes ocultos de la nube

“El hecho de que Microsoft esté detrás de Office 365 es un factor muy importante. No tendré que volver a cambiar de proveedores en el futuro, ya que confío en que Microsoft protegerá nuestro correo electrónico y otros servicios”.

Paraic Nolan
Director de finanzas
Big Red Book

PREGUNTA 2

¿Nos estamos protegiendo contra las amenazas internas?

Las amenazas internas suelen considerarse unas de las amenazas más difíciles ante las que defenderse. Con el aumento de freelancers, autónomos y empleados temporales en una empresa, defenderse contra las posibles amenazas internas parece casi imposible. En 2013, el FBI calculó que los ataques de amenazas internas por usuarios malintencionados costaron aproximadamente 412 000 dólares por incidente.[4]

Aunque no existe una solución única para defenderse contra las amenazas internas, los expertos recomiendan un enfoque múltiple en el que participen varios miembros del equipo directivo. El departamento de recursos humanos debe comprobar los antecedentes de todos los empleados y freelancers de forma exhaustiva. Además, las relaciones humanas pueden ayudar a identificar señales de advertencia en el comportamiento poco común de algunos empleados (por ejemplo, faltar al trabajo o presumir del posible daño que podrían realizar).[5] Los directores de tecnología y los directores de seguridad pueden debatir sobre la posibilidad de implementar herramientas de supervisión de comportamiento de seguridad para identificar casos en que los empleados obtengan acceso a archivos con los que no tienen ninguna relación, guarden archivos e información en una ubicación externa o se produzcan inicios de sesión de empleados en horas poco comunes.

Por suerte, si se producen sospechas de amenazas internas, existen soluciones como Microsoft Data Loss Prevention (DLP) implementada en OneDrive para la Empresa, SharePoint Online, Exchange y Office 2016, que permitirá a sus administradores de TI protegerse contra la pérdida de datos sin aumentar sus presupuestos.

Los administradores recibirán notificaciones si se intercambia información confidencial y podrán recuperar los datos y el acceso de algunos empleados. Además, con DLP, los administradores pueden revisar datos de incidentes y generar informes de incidentes para conocer exactamente desde dónde se puede haber filtrado la información.

[4] Fred Donovan, FierceITSecurity: ¿Cree que la persona que se sienta a su lado puede ser un usuario malintencionado?
[5] George Silowash, Software Engineering Institute: Guía de procedimientos recomendados para mitigar las amenazas internas: Cuarta edición

No solo necesita defenderse contra virus y malware (en el 19 % de los incidentes de seguridad están implicados usuarios internos malintencionados).

Fred Donovan, FierceITSecurity: ¿Cree que la persona que se sienta a su lado puede ser un usuario malintencionado?

PREGUNTA 3

¿Tenemos preparado un grupo de trabajo de ciberseguridad?

Los profesionales de la ciberseguridad aprenden a pensar cuándo (o no) se producirá una infracción. Planear una infracción quiere decir crear un grupo de trabajo en toda una organización que designe quién estará a cargo de informar sobre el ataque a los clientes (el director de marketing), quién será el responsable de proteger una red (el director de seguridad de la información, el director de seguridad y el director de tecnología) y quién se encargará de las ramificaciones legales de la información comprometida (responsables del departamento legal, atención al cliente y recursos humanos). Aunque crear un grupo de trabajo de ciberseguridad en una organización se considera un procedimiento recomendado, la mayoría de las organizaciones no han preparado con antelación un grupo de trabajo en absoluto.

Según una encuesta de seguridad de la información de Microsoft, el 63 % de los ejecutivos financieros de grandes empresas creen que "simplemente afrontan al día las amenazas de seguridad", el 28 % considera que están por delante de estas amenazas y el 9 % piensa que están muy por detrás.[6]

¿Quién tiene que implicarse? Una gran parte del grupo de trabajo estará formado por analistas de seguridad y por el departamento de TI. Pero no subestime la importancia del soporte legal, financiero, de los inversores y de las relaciones públicas. Cualquiera que pueda contribuir a corregir una infracción debería incluirse en un grupo de trabajo de ciberseguridad y estar preparado para tomar medidas.

[6] Estudio sobre la seguridad de la información de Microsoft, septiembre-octubre de 2015

El 84 % de las organizaciones no han implementado un grupo de trabajo de ciberseguridad.

Financial Executives Research Foundation: El rol del director de seguridad en la ciberseguridad

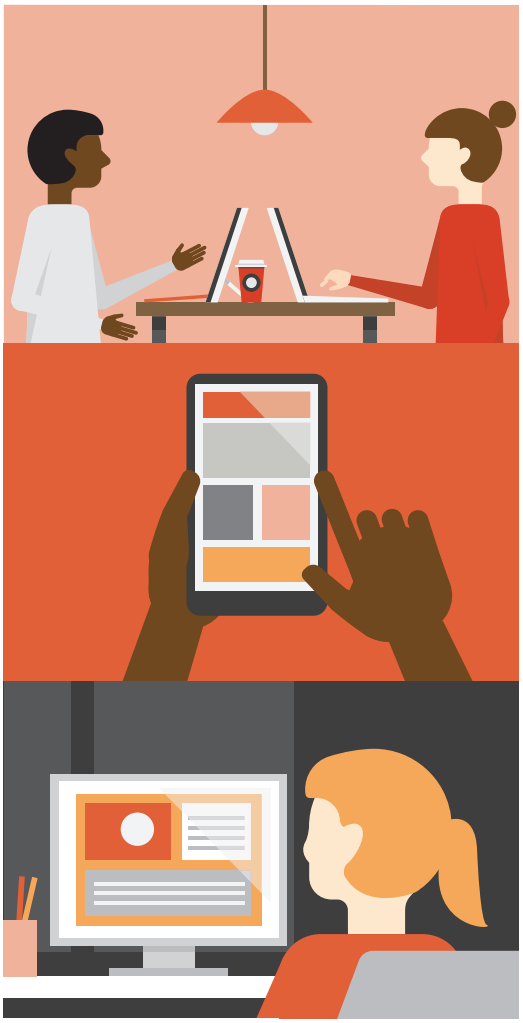
PREGUNTA 4

¿Es segura su política de BYOD?

Las políticas de BYOD aumentaron en gran medida en los últimos cinco años, lo que permite a los empleados tener acceso a los archivos de la compañía en sus propios dispositivos y en cualquier momento. Pero, según un informe realizado en 2014 por Check Point, más de la mitad de los ejecutivos de TI informaron que los incidentes de seguridad de BYOD costaron a sus organizaciones más de 250 000 dólares en un período de dos años.[7]

Es posible seguir ofreciendo soporte a las directivas de BYOD sin poner en peligro la seguridad y sin afectar a su presupuesto. Pregunte a los equipos de seguridad sobre las funciones de inicio de sesión único de las ofertas actuales y la administración de autoservicio de contraseñas. Las herramientas de administración de movilidad, como Microsoft Enterprise Mobility Suite, pueden mantener a los empleados conectados a las aplicaciones que necesitan sin poner en peligro la seguridad. En un informe realizado por Forrester sobre el impacto económico de Microsoft Office 365, el 28 % de los usuarios empresariales vieron una mejora en la seguridad de los datos móviles debido a la capacidad de Enterprise Mobility Suite de borrar datos de forma remota en los dispositivos perdidos.[8]

[7] Infosecurity Magazine: Los costes de los incidentes de seguridad de BYOD superan los 250 000 dólares
[8] Informe de Forrester: El impacto económico total (Total Economic Impact™) de Microsoft Office 365, octubre de 2014



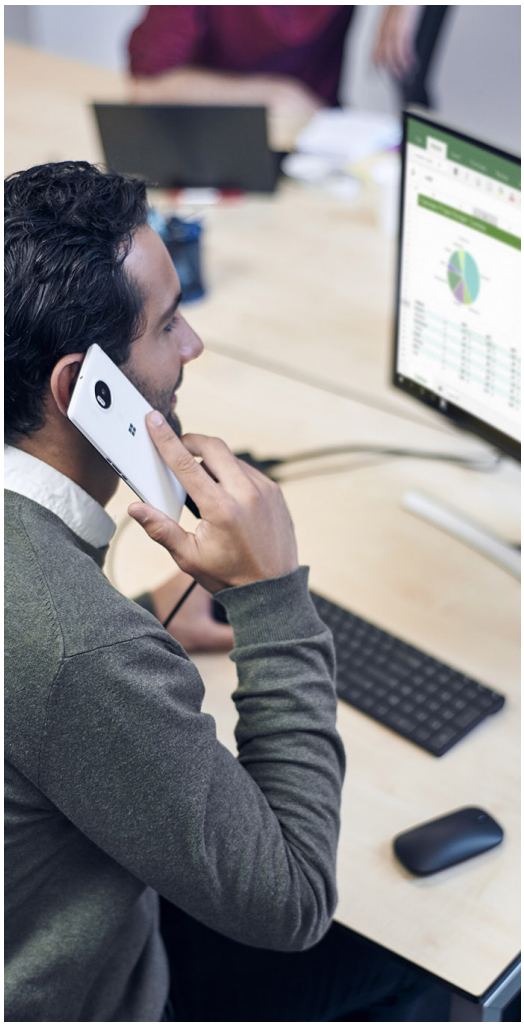
Además, la administración de dispositivos móviles (MDM) de Office 365 puede ayudar a proteger los dispositivos de su empresa desde cualquier lugar. Su equipo de TI puede administrar directivas de dispositivos móviles y realizar un borrado selectivo de los datos de Office 365 si un empleado abandona su organización, lo que ahorra tiempo y complicaciones a sus departamentos de recursos humanos, TI y seguridad.

“Necesitamos proteger y administrar los dispositivos móviles y los smartphones utilizados fuera de la red corporativa, así como los datos que contenían. Enterprise Mobility Suite proporciona estas funciones en un paquete rentable”.

Kris Mampaey
Director de TI
Willemen Groep

PREGUNTA 5

¿Se siente limitado por su presupuesto de seguridad o por el número de empleados?



Los responsables de la seguridad empresarial contratan equipos de forma continua y necesitan administrar varias soluciones de seguridad y miles de alertas al día. ¿Son razonables sus presupuestos y permisos de contratación? Al revisar la resistencia de la seguridad de una empresa, el equipo directivo necesita asegurarse de que se asigne un presupuesto generoso para un desarrollo rápido de la seguridad y evaluar si se pueden reducir otros presupuestos para adaptarse a estas necesidades.

Independientemente de si es necesario contratar más asistentes de administración o analistas, o bien aumentar el presupuesto de TI, conozca cuáles son las necesidades de su equipo de seguridad y realice los cambios necesarios para asegurarse de que puedan desempeñar su trabajo al máximo.

Por suerte, muchas de las herramientas que ya se usan en su compañía pueden complementar su plan de seguridad. Las soluciones de uso compartido y sincronización de archivos para empresas, como Microsoft SharePoint y OneDrive, pueden eliminar el uso de nubes no autorizadas por parte de los empleados, a la vez que mejoran de forma significativa la seguridad de los archivos compartidos con socios y freelancers. Preparar y comunicarse con un grupo de trabajo de ciberseguridad puede resultar más fácil con herramientas de comunicación para la oficina, como las conferencias online de Skype Empresarial y Exchange Online. Mejore la seguridad de su política de BYOD con las aplicaciones móviles disponibles para una amplia variedad de programas de Office en dispositivos Apple, Android y Windows. Lo que es aún más importante: todas estas herramientas están disponibles dentro de su presupuesto y es probable que sus empleados ya estén familiarizados con Office 365.

Es hora de hablar con su equipo de seguridad.

¿Tenemos controlado el uso de nubes no autorizadas? ☐

¿Hemos protegido nuestra política de BYOD? ☐

¿Qué estamos haciendo para protegernos frente a amenazas internas? ☐

¿Tiene el presupuesto suficiente mi equipo de seguridad? ☐

¿Hemos creado nuestro grupo de trabajo de ciberseguridad? ☐

¿Quiere más sugerencias empresariales?

Conozca las mentes de los innovadores tecnológicos y empresariales con la serie de webcasts Modern Workplace de Microsoft:

https://products.office.com/business/modern-workplace/webcast-series