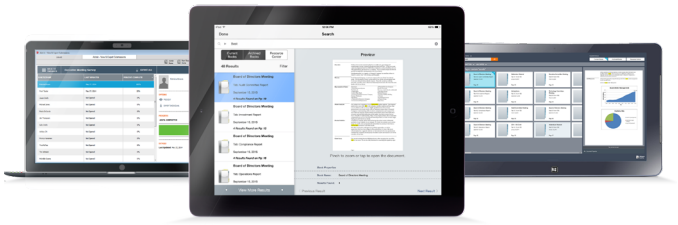
Diligent

Potenciamos el valor de la información. Con seguridad.

Diligent ayuda a las principales organizaciones del mundo a potenciar, con seguridad, el poder de la información y la colaboración, dotando a sus juntas directivas y equipos de administración de los recursos de información necesarios para tomar mejores decisiones. Más de 4.000 clientes en más de 70 países confían en Diligent para contar con acceso inmediato a la información más sensible y confidencial junto con las herramientas para revisar, discutir y colaborar en la toma de decisiones clave. Diligent Boards agiliza y simplifica la manera en que produce y se entrega el material para juntas directivas a través de iPad, dispositivos con Windows y navegadores. Al mismo tiempo, ofrece ventajas prácticas como la reducción de los costos de producción, el apoyo a las metas de sostenibilidad y el ahorro de tiempo administrativo y de TI.

Únase a los líderes. Obtenga Diligent.



Para mayor información o solicitar una demostración, contáctenos hoy mismo:

Llame: 1-973-939-9404
Correo electrónico: info@diligent.com
Visite: www.diligent.com

AICPA SOC · ISO 27001 CERTIFIED BY BRIGHTLINE · Consíguelo en el App Store · Consíguelo de Microsoft

La amenaza cibernética y la seguridad de la junta directiva: **Tres ideas erróneas que menoscaban la seguridad de la sala de reuniones de la junta directiva**

Ben Bourne
Director de relaciones públicas, EMEA

Magdalena Borcal
Directora de relaciones públicas, EMEA

Nathan Birtle
Vicepresidente de ventas y desarrollo de negocios, EMEA

El índice de ataques cibernéticos está aumentando a nivel global. Los delincuentes se vuelven cada vez más expertos en evadir los sistemas de seguridad, y con regularidad aparecen casos resonantes de infracción de seguridad en los medios de comunicación de todo el mundo. A pesar de esto, muchas juntas directivas aún ignoran la amenaza que constituye el delito informático, y en el caso de aquellas que han hecho algo al respecto, muchas han fracasado en su intento de resguardarse adecuadamente. En respuesta, hemos publicado este artículo, que está diseñado para ayudar a los directores y gerentes a tener una mejor comprensión del problema de los delitos informáticos, y al mismo tiempo, mostrarles cómo reducir los riesgos de seguridad a nivel de la junta directiva.

Existen muchos factores que afianzan el crecimiento de los delitos informáticos. La posibilidad de ser atrapado es baja si se compara con otros tipos de delitos. Los datos se pueden transmitir a través de miles de computadoras, lo que permite que los ataques sean anónimos e imposibles de rastrear. El retorno financiero que pueden esperar obtener los delincuentes informáticos es de millones de dólares. La mayor parte de estos delitos los comete el crimen organizado, cuyas actividades, según estiman los analistas, representa un costo de 455 mil millones de dólares anuales para la economía global.[1]

Un ataque exitoso puede infligirle un enorme daño a una organización. Además de las pérdidas financieras, el robo de propiedad intelectual e información puede perjudicar el comercio, la competitividad, la innovación y la reputación. Las organizaciones pueden protegerse, y al reconsiderar su manera de trabajar con datos y resguardar su información, pueden limitar su exposición a los ataques.

1 "Net Losses: Estimating the Global Cost of Cybercrime," McAfee, 2014.
http://www.mcafee.com/uk/resources/reports/ rp-economic-impact-cybercrime2-summary.pdf

Diligent

EVALUACIÓN DE SU JUNTA DIRECTIVA

Como responsables de la toma de decisiones en la organización, las juntas directivas deben comprender las amenazas que enfrenta su organización, aunque esto puede ser difícil. Muchos directores pueden no darse cuenta de cuán digital se ha vuelto el negocio. Es posible que estos no aprecien la forma en que la convergencia de la TI, la tecnología empresarial y la tecnología de operaciones han moldeado el negocio y han generado más oportunidades para que los atacantes obtengan acceso.

También hay que tener en cuenta a las estructuras jerárquicas dentro de la organización. El hecho de que la junta directiva esté ubicada "por encima" de la organización significa que los empleados responsables de la seguridad de ésta podrían no sentir suficiente confianza como para informar acerca de las inquietudes que puedan tener con respecto al esquema de seguridad de la firma. Investigaciones de Deloitte y Systemec indican que, en algunas regiones, hasta el 70 % de los encargados de la toma de decisiones de TI no confían en las políticas de seguridad de sus empresas, y concluyen que más de dos tercios de las organizaciones carecen de capacidad de protegerse a sí mismas frente a ataques.[2] De igual modo, el equipo de seguridad puede desconocer el hecho de que ocuparse de la seguridad de la junta es parte de su rol, y considerar que ésta, en cambio, se encuentra bajo el control del secretario corporativo y que no debería depender del esquema de seguridad de la organización.

Las juntas directivas deben comprender las amenazas que enfrenta su organización, aunque esto puede ser difícil. Muchos directores pueden no darse cuenta de cuán digital se ha vuelto el negocio.

LAS TRES IDEAS ERRÓNEAS ACERCA DE LA SEGURIDAD

Las acciones de los directores son otro factor que contribuye a un mayor riesgo potencial de seguridad para la junta directiva. Al elegir acceder al material de junta directiva, almacenarlo y distribuirlo de una forma insegura pero conveniente, los directores exponen potencialmente sus datos ante terceros y pierden el control sobre ellos. Los correos electrónicos, PDF y sistemas de almacenamiento basados en la nube, por ejemplo, tienden a ser mucho menos seguros que los métodos empleados por la organización.

Los directores, así como el personal, deben ser diligentes al abordar el tema de las tecnologías de las comunicaciones. Pero incluso las más seguras prácticas laborales pueden verse menoscabadas por las ideas erróneas asociadas con la tecnología y los flujos de trabajo en uso.

Con el fin de evitar que los directores trabajen de una manera que disminuya la seguridad de su junta directiva, debe tomar en consideración las siguientes ideas erróneas:

1. El correo electrónico es seguro

Si bien el correo electrónico es conveniente, rápido y fácil de utilizar como medio para comunicar información confidencial, éste, sencillamente, no es adecuado para ese propósito. El correo electrónico no le permite restringir el reenvío de contenido. Además, anular un mensaje enviado es difícil. En la práctica, tan pronto como se envía un correo electrónico, se pierde el control sobre la información.

2. La protección mediante contraseña es sinónimo de seguridad

Aunque no deja de ser razonable suponer que agregar una contraseña a un PDF lo convierte en inaccesible para usuarios no autorizados, una sencilla exploración en cualquiera de los motores de búsqueda más populares produce millones de resultados que enseñan cómo evadir la seguridad de los PDF. Efectúe esa búsqueda en Google, y encontrará más de 2.300.000 resultados que documentan cuán terriblemente sencillo es violar este medio en apariencia seguro. La verdad es que la tecnología PDF no es segura, y que no debería confiar en ella.

3. El almacenamiento interno de información es más seguro

Quizá la idea errónea más importante que se debe tener en cuenta es la de que el almacenamiento interno de la información ofrece más seguridad que si se realiza a través de un tercero. En realidad, con frecuencia ocurre lo contrario. Un ejemplo de ello es que las soluciones internas dependen de los propios administradores de la organización para acceder a los datos y gestionarlos, pero puesto que el 55 % de los ataques cibernéticos se producen desde adentro, se ha comprobado que este acceso puede ser catastrófico.[3] Además, en términos técnicos y operativos, el programa y la infraestructura de seguridad de la organización pueden no ser suficiente para proteger los datos de las amenazas de hoy en día. Por el contrario, un proveedor de software como servicio, como es el caso de Diligent, restringe el acceso a los datos, permitiéndolo únicamente a los usuarios finales autorizados. Nuestro equipo no tiene acceso a los datos del cliente. Asimismo, hemos realizado completas auditorías de políticas y procedimientos de seguridad, con lo que hemos proporcionado funciones de respaldo de información y de recuperación de desastres, así como controles de seguridad que exceden las capacidades de la mayoría de las organizaciones.

2 Global Risk Insights, Septiembre de 2015. "globalriskinsights. com/2015/09/how-strong-are-the-middle-easts-cybersecurity-net-works/
3 "IBM 2015 Cyber Security Index" y "IBM X-Force Threat Intelligence Quarterly Q2 – 2015" https://securityintelligence.com/ the-threat-is-coming-from-inside-the-network/

EVALUACIÓN DE LA SEGURIDAD DE LA JUNTA DIRECTIVA

Los líderes que deseen evaluar las prácticas de seguridad informática de su junta directiva pueden hacerlo formulando tres sencillas preguntas:

¿Cómo se almacena la información de la junta directiva?

Una evaluación de la seguridad debería comenzar por examinar quién controla la información. No saber dónde está la información y carecer de la capacidad de controlar hacia dónde va, significa que la solución es extremadamente insegura.

Es por ello que enviar por correo electrónico documentos de junta directiva como archivos PDF no constituye una solución segura. Los archivos pueden ser reenviados accidentalmente por directores a personas que están fuera de la junta directiva, o guardados en cuentas personales de correo electrónico con mínimos niveles de seguridad en sistemas que incluso los proveedores admiten que no deberían considerarse seguros.

Esto también es válido para las soluciones basadas en la nube, en las que sus archivos podrían estar en cualquier servidor en la red para compartir archivos y usted no tiene manera alguna de saber con exactitud dónde están. El éxito de las soluciones basadas en la nube radica en el supuesto de que son seguras, cuando en realidad casos resonantes de ataques informáticos, tales como la revelación de contraseñas y de fotografías de celebridades por parte de proveedores de servicios de la nube[4], demuestran cuán falsa es esta creencia en cuanto a la seguridad.

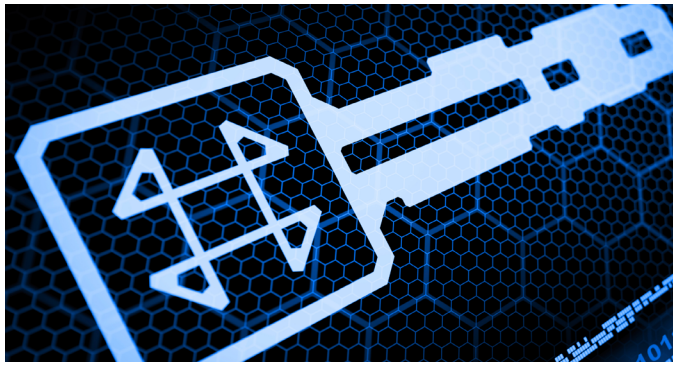
Si bien los software para juntas directivas hospedados parecieran formar parte de la nube, y frecuentemente se les denomina de manera errónea "almacenamiento basado en la nube", existen grandes diferencias. Los software para juntas directivas hospedados controlan cuidadosamente dónde se almacenan sus datos y mantienen segregada la información de cada organización. Conocer la ubicación de los datos y cómo son protegidos, permite tener mayor control y seguridad sobre quién tiene acceso a la información.

¿Qué tan potentes son las defensas?

Si bien conocer la ubicación donde residen los datos es clave, igual lo es garantizar que sólo los usuarios autorizados puedan tener acceso a ellos. Esto se puede lograr mediante el cifrado de los datos, es decir, convirtiéndolos en una serie de números 0 y 1 sin ningún significado que solo pueden descifrar quienes posean la clave digital correcta.

Las carpetas de documentos para juntas directivas no tienen clave digital alguna; quienes posean una copia, podrán leer la información. Si bien pudiera ser cierto que los PDF enviados por correo electrónico o almacenados en sistemas para compartir archivos pueden cifrarse y estar protegidos mediante contraseñas, la verdad es que toda la responsabilidad de administrar los protocolos de contraseña recae sobre quien distribuye y recibe el material. Incluso así, los documentos PDF siguen siendo vulnerables a los ataques perpetrados mediante "fuerza bruta" a través de productos de software fácilmente accesibles.

Las soluciones para juntas directivas de mayor calidad por lo general utilizan un cifrado de 256 bits, y debido a que el número de combinaciones



posibles es mayor que la cantidad de estrellas que tiene el universo, con seguridad se puede afirmar que incluso los delincuentes informáticos más avezados, utilizando la más avanzada tecnología, tardarían una eternidad en descifrar el código.

¿Quién controla las claves?

No obstante, independientemente de cuán fuerte sea el sistema de cifrado, cualquiera con la clave correcta puede tener acceso a la información; quien posea la contraseña de un PDF protegido mediante contraseña, virtualmente se apropiará del documento. Contraseñas robadas se traduce en documentos robados.

Sin embargo, un software potente nunca pierde el control de los documentos. Una contraseña tiene límites debido a que el control de las claves de cifrado residen dentro del sistema. La persona que inicie sesión solo podrá ver lo que tenga permitido, y si una contraseña es robada, el administrador solo puede denegar el acceso de esa contraseña.

En el caso de usuarios autorizados, los administradores pueden limitar el acceso a documentos específicos, así como asignar el acceso y la visibilidad de los documentos a un grupo de usuarios. Por ejemplo, un comité de compensación puede preferir negarse a compartir su información con la totalidad de la junta directiva.

El administrador de un software para junta directiva hospedado también puede controlar el acceso de dispositivos, restringiendo el acceso de los directores desde dispositivos personales y menos seguros y exigiendo el acceso a través de sistemas de propiedad de la empresa. Además, cuando ya no son necesarios los documentos confidenciales, el administrador puede realizar "una depuración virtual", bloqueando el acceso de los usuarios que intenten acceder a dichos archivos. Del mismo modo, se puede restringir el acceso según el usuario o el dispositivo, lo cual es útil en el caso de que un director salga de la junta directiva y sea necesario recuperar materiales o si una contraseña ha sido robada.

SEA UN EJEMPLO DE SEGURIDAD

La seguridad informática, específicamente la seguridad de la información y los datos de la junta directiva, debe considerarse algo fundamental. Contar con una solución para juntas directivas intuitiva y segura para manejar toda la información, las comunicaciones y la colaboración de la junta directiva favorece la existencia de una mayor seguridad y de mejores prácticas laborales en la junta directiva.

La imposibilidad por parte de una junta directiva de mantener altos estándares de seguridad puede socavar el esquema de seguridad de la organización en su totalidad, mientras que una junta directiva que lidere dando el ejemplo, incrementa la eficacia de la seguridad de la organización y la coloca en una posición firme ante las crecientes amenazas.

4 BBC News, http://www.bbc.co.uk/news/technology-29011850