La ciberseguridad en el consejo de administración

«Hay dos tipos de empresas: las que han sido pirateadas y las que no saben que han sido pirateadas »
*- **John Chambers, CEO de Cisco Systems (1983-2015)***

Hoy en día, la mayoría del valor del mercado y de la información valiosa está en formato digital, de ahí que un ataque cibernético sea uno de los mayores peligros a los que se enfrenta una empresa. Los hackers o atacantes cuentan con la experiencia y las herramientas necesarias para desmantelar infraestructuras y sistemas complejos, y paralizar regiones enteras.

Sin embargo, cuando aparecen noticias sobre ciberataques destructivos, los profesionales de la seguridad o consejeros pueden pensar: “No creo que nuestra empresa sea un objetivo por lo que seguramente no estamos en riesgo”. Ese es el mayor riesgo, restarle valor y no saber que su empresa y/o sus empleados ya han sido comprometidos, pirateados.

¿Sabía que los documentos PDF son el tipo de archivo más común para esconder amenazas?, y que un solo usuario no autorizado puede provocar daños importantes. ¿Sabía que los dispositivos móviles son el objetivo número 1 de los atacantes?, porque son los más difíciles de defender, junto con los datos en las redes públicas y el comportamiento incorrecto de los empleados.

Usted, como parte del Consejo de Administración, ¿está dispuesto a que su empresa asuma el riesgo de sufrir un ciberataque solo por sostener el crecimiento a largo plazo? Esta es una de las preguntas que deben hacerse hoy en día los miembros del Consejo de Administración cuando analicen estratégicamente los riesgos y obstáculos a los que se puede enfrentar su empresa a corto y largo plazo.

CISCO

Diligent

Lo que está en juego es mucho más que información privada

El miedo a las brechas se debe al coste financiero de los ataques, que ya no es un número hipotético. Las brechas conllevan un daño económico significativo para las organizaciones, un daño que puede llevar años reparar. Según los encuestados del Informe de ciberseguridad anual de Cisco 2018[1], más de la mitad (53%) de todos los ataques provocaron daños financieros de más de 500.000 USD (por ataque) que incluían, entre otros, pérdida de ingresos, clientes, oportunidades y gastos extra. De hecho, el 45% de los ataques en España tuvo como consecuencia daños que superaron los 400.000€ (por ataque).

Sin embargo, el coste monetario no es el único que se debe tener en cuenta al evaluar el riesgo. La pérdida de propiedad intelectual y conocimientos sobre la competencia, o la pérdida de confianza de los clientes son costes que dañan mucho más a las empresas a largo plazo tras una brecha de ciberseguridad. Por este motivo, los consejeros deberían preparar un plan de contingencia a tales incidentes. Una estrategia que establezca cómo debe actuar la empresa si se produce una brecha de seguridad es la mejor herramienta del Consejo de Administración para mitigar los daños reputacionales que puedan surgir de un ciberataque.

¿Qué responsabilidad tienen los consejeros cuando se produce una brecha en la información confidencial de una empresa? ¿Deberían contar todos los Consejos de Administración con un experto en ciberseguridad entre sus miembros?

En este libro blanco vamos a repasar algunos aspectos que deben tenerse en cuenta para mitigar el riesgo de sufrir un ciberataque y estar preparado para actuar cuando este se produzca.

¿Por qué es tan complicado mitigar todos los riesgos relacionados con la seguridad cibernética?

El abanico de riesgos cibernéticos es demasiado amplio

Los expertos de su departamento informático pueden ver lo que está en el horizonte, pero tienen dificultades para protegerse si no actúan. Los piratas informáticos ya tienen la experiencia y las herramientas necesarias para derribar las infraestructuras y los sistemas críticos, podrían paralizar si quisieran regiones enteras. El mayor riesgo de una empresa es restarle valor a lo que parecen ser campañas contra otros, en pretender que los sistemas tradicionales de defensa siguen siendo válidos o en permitir que el caos de las batallas diarias con los hackers consuma su atención. Su protección es mucho más débil si no reconoce la velocidad y la escala a la que los atacantes están reuniendo y mejorando su ciberataques.

Durante años, Cisco ha estado advirtiendo a las empresas sobre la creciente actividad de ciberdelincuencia en todo el mundo. En el Informe de ciberseguridad anual de Cisco 2018[2] se presentan datos y análisis de los investigadores de amenazas realizado por Cisco y varios de sus socios tecnológicos sobre el comportamiento observado en los atacantes durante los últimos 12 a 18 meses:

- Los adversarios están llevando el malware a niveles de sofisticación e impacto sin precedentes.
- Los adversarios son cada vez más expertos en la evasión y en usar los servicios en la nube y otras tecnologías comunes, como son las herramientas de comunicación (el móvil, el correo electrónico o Whatsapp) para crear una brecha de seguridad.
- Los adversarios están explotando las grietas en la seguridad existentes, muchas de las cuales surgen de la expansión del uso de internet y de la confianza de nuestros empleados en los clientes o proveedores a los que suplantan la identidad.

Los riesgos cibernéticos pueden ser algo complicado de comprender o ajeno a los consejeros, sobre todo si tenemos en cuenta la media de edad de los consejeros en España que son 60,4 años[3]. La mayoría no se ha tenido que enfrentar a ataques cibernéticos durante su carrera profesional, pero deberían ser capaces de entender las consecuencias de este tipo de riesgo, ya que han tenido que lidiar con otro tipo de riesgos y con la gestión de estos. De todos modos, es responsabilidad de los miembros del Consejo de Administración estar al día e informado sobre los temas de actualidad.

---

1. *https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/reporte-anual-cisco-2018-espan.pdf*
2. *https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/reporte-anual-cisco-2018-espan.pdf*
3. *Según el informe índice Spencer Stuart de Consejos de Administración de 2017 (https://www.spencerstuart.com/~/media/pdf%20files/research%20and%20insight%20pdfs/spain-bi-2017.pdf)*

¿Cómo deberían gestionar los riesgos cibernéticos los consejeros?

Históricamente, la ciberseguridad ha sido responsabilidad del departamento informático. Una o dos veces al año la persona a cargo de dicho departamento hacía una presentación al Consejo de Administración que los dejaba boquiabiertos. Hoy en día, el Consejo de Administración debería definir la estrategia para mitigar los riesgos durante sus reuniones y comprender a la perfección cuál es la postura de la empresa en cuanto a la ciberseguridad. Ya no es suficiente que la ciberseguridad sea un asunto exclusivamente relacionado con el departamento informático. La realidad es que hay que poner la "Ciberseguridad por encima de todo".

La seguridad está formada por Personas, Tecnología y Procesos y es muy importante hacer foco en las tres áreas. Las personas construyen las empresas, las relaciones, actúan sobre los datos, los sistemas, los clientes y proveedores. Es vital influir en el comportamiento de las personas y su concienciación sobre la importancia de proteger los datos de la empresa. La concienciación debe ser un proceso que empiece desde arriba en los consejos de administración y se haga a todos los niveles en la empresa. Todos somos parte de la ciberseguridad y así se debe reflejar en las políticas de la compañía.

En una organización moderna, todos los departamentos (marketing, ventas, finanzas, recursos humanos o desarrollo de producto) tienen proveedores y usan la tecnología de formas distintas. Por este motivo, cada departamento debe identificar maneras de mitigar los riesgos cibernéticos para la empresa. Aunque para el 33% de las organizaciones españolas uno de los mayores obstáculos para la seguridad es la falta de personal especializado en ciberseguridad, son muchas las empresas que cuentan con un responsable de la seguridad de la información que se encarga de definir la estrategia de ciberseguridad y de su implementación en toda la empresa. Sin embargo, sigue siendo responsabilidad del jefe de cada departamento instaurar buenas prácticas y asegurarse de que las personas a su cargo cumplen las directivas del responsable de la seguridad de la información.

A continuación, presentamos algunas recomendaciones sobre cómo debería gestionar los riesgos cibernéticos el Consejo de Administración:

1. Proteja los activos más valiosos de su empresa.

Como con cualquier otro tipo de gestión de riesgo, es una cuestión de priorizar. No es posible proteger todos los activos, y es responsabilidad del Consejo de Administración asegurar que los directivos están protegiendo los activos más valiosos. El Consejo debería hacer un inventario de los activos digitales de la empresa y un listado de los proveedores con los que mantienen relaciones comerciales los empleados de la empresa. Para priorizar, el Consejo debería preguntarse: "¿Cuál es el activo que la empresa no puede permitirse perder?".

2. Lleve a cabo un análisis externo y aproveche los datos existentes de la industria.

Aunque cada empresa se enfrenta a riesgos distintos, comprender los riesgos que han identificado otras empresas del sector puede aportar claridad sobre dónde se debería invertir tiempo y presupuesto. Por ejemplo, la mayoría de los ciberataques del sector hospitalario están relacionados con proveedores externos cuya identidad es suplantada para conseguir los datos de pago de los clientes de las empresas del sector. En cambio, en el sector sanitario las brechas suceden normalmente por errores humanos internos.

3. No subestime el riesgo que supone el factor humano.

Solemos olvidarnos del "factor humano" en las conversaciones sobre riesgo cibernético en el Consejo de Administración. Pero debe tener en cuenta que el 91% de los ataques cibernéticos con éxito tienen su origen en un correo electrónico fraudulento (ataques de *phishing* diseñados para conseguir información relevante de los empleados). Los datos y comentarios personales y de empresa que compartimos en las redes sociales son a menudo el punto de partida para ataques dirigidos a nuestras empresas. Los Consejos de Administración deberían exigir a los directivos una presentación donde detallen qué están haciendo para formar a sus empleados.

4. Ofrezca formación continua a sus empleados.

La formación en las empresas debe ser continua, el aprendizaje nunca para. La concienciación, no puede ser una campaña, debe estar en la propia formación continua de los miembros de la empresa.

5. Siga la ley de protección de datos.

Con la GDPR (nueva ley Europea de Protección de Datos) tenemos las figuras de DPO (Data Protection Officer) y CDO (Chief Data Officer) que son los responsables del almacenamiento y tratamiento de los datos con la privacidad adecuada con respecto a las políticas de la compañía y la regulación vigente que le aplique. También estamos obligados a tratar información de clientes con obligado cumplimiento y asegurar su correcta implantación. Esta ley no solo tiene en cuenta los procesos y tecnología, sino también la capacitación, formación y concienciación de las personas.

Plan de contención en caso de brecha de seguridad

Ya hemos comentado que es muy probable que vaya a tener que enfrentarse a una brecha de seguridad, ya que el 91% de las empresas españolas admitió haber sufrido un ciberataque en 2017. Por ello es imprescindible tener un plan de contención preparado con tiempo, para reducir las consecuencias y el impacto de dicho ciberataque. El 45% de las empresas españolas tuvo que gestionar una interrupción de servicios de más de 5 horas debido a una brecha de seguridad el último año. A continuación le presentaremos algunos consejos para tener previsto un buen plan de contención en caso de brecha de seguridad.

Por qué es importante estar preparado

La pérdida de propiedad intelectual y de datos sensibles sobre los clientes afectan a los resultados de cualquier empresa. Sin embargo, es el daño a la imagen de la empresa, a su reputación y la pérdida de la confianza de los clientes lo que tiene peores repercusiones a largo plazo. A pesar de que los ciberataques son impredecibles, el Consejo de Administración tiene la posibilidad de definir e influenciar cómo responde la empresa si se produce una brecha en la seguridad. Un plan de contención efectivo empieza con una detallada preparación.

Conocer las obligaciones regulatorias

Antes de redactar un plan de contención a una brecha de seguridad, el Consejo de Administración y el equipo directivo deben conocer las regulaciones y los requisitos que rigen los territorios donde tiene presencia la empresa. Hay que tener en cuenta que estos suelen variar según regiones y regulaciones. Por ejemplo, las empresas que controlan y procesan datos de ciudadanos europeos deben cumplir lo dictado en el Reglamento General de Protección de Datos. El RGPD, en vigor desde el 25 de mayo de 2018, no solo afecta el modus operandi de muchas empresas en todo el mundo, sino que además establece un precedente mundial en términos de protección de datos. Los miembros del Consejo de Administración deberían conocer y leer lo que establece el RGPD y la "Guía para la gestión y notificación de brechas de seguridad" de la Agencia española de protección de datos[4].

Definir un plan de notificación y comunicación

En cualquier plan estratégico de contención en caso de brecha de seguridad, es imprescindible definir el orden y las personas a las que se les va a comunicar y notificar el ataque cibernético. El plan debe responder a cuestiones como: ¿Cuándo se le va a notificar el incidente al Consejo? ¿Cuál es el plan de la empresa para informar a los reguladores? ¿Cómo y cuándo se va a informar a aquellos cuya información haya sido robada/suplantada? ¿Quién es el encargado de informar a cada uno de los grupos mencionados?

Contratar los recursos necesarios antes de que suceda la brecha

Horas después de que se haya producido una brecha en la seguridad de su empresa no es el momento adecuado para encontrar a un nuevo bufete de abogados, o a una agencia de RRPP para gestionar el incidente. El Consejo de Administración y el equipo directivo deberían contratar con tiempo a aquellos recursos externos que puedan necesitar en el caso de una brecha en la seguridad. Si se encontrase su empresa en esa situación, podrá necesitar los siguientes proveedores: un bufete de abogados, una agencia de RRPP, algún contacto del sistema judicial, entre otros. El plan de contención debe indicar: (a) cuando se debe notificar a estos proveedores (b) cuál es su responsabilidad.

Riesgos cibernéticos en la comunicación del Consejo de Administración

En general, no solemos pensar que el Consejo de Administración pueda poner en riesgo la seguridad de la empresa a través de sus comunicaciones. Pero estamos bastante equivocados. El Consejo de Administración y los directivos suelen tener a su alcance la información más sensible de la empresa, por lo que son el blanco más atractivo para los hackers y cibercriminales. Por ello, creemos que es importante destacar dos prácticas bastante extendidas entre los miembros del Consejo de Administración que pueden provocar un ataque cibernético.

1. Usar el correo electrónico personal.

El uso del correo electrónico personal para comunicaciones del Consejo de Administración supone un riesgo ingente, porque aunque las conversaciones o información que tienen los consejeros en el correo electrónico no sean confidenciales, el correo electrónico personal suele ser la puerta digital para muchas otras aplicaciones y herramientas en las que sí puede haber información confidencial. Por ello recomendamos la utilización de herramientas que puedan asegurar la privacidad y seguridad de la información.

2. Obviar las implicaciones y su responsabilidad legal

Cuando los consejeros usan el correo electrónico o el Whatsapp para comunicarse con otros miembros del Consejo sobre asuntos confidenciales, no son conscientes de las implicaciones que esas conversaciones podrían tener para la empresa en un juicio. La secretaría del Consejo de Administración tiene que establecer las buenas prácticas y exigir que las comunicaciones relacionadas con el Consejo de Administración se lleven a cabo con herramientas seguras. También es tarea de la secretaría concienciar a los miembros del Consejo sobre el riesgo que supone compartir documentos o información del Consejo fuera del portal para el Consejo de Administración.

4. *https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/reporte-anual-cisco-2018-espan.pdf*

Diligent

¿CÓMO PUEDE AYUDARLE DILIGENT?

La seguridad cibernética, concretamente la seguridad de la propia información y los datos del Consejo de Administración, es un asunto clave y prioritario para una empresa; disponer de un portal para el Consejo de Administración seguro e intuitivo para almacenar y compartir dicha información, no solo optimiza la gestión de la documentación y fomenta la colaboración, sino que además asegura la seguridad de los documentos del Consejo. El Consejo de Administración debe predicar con el ejemplo y ser el primero en adoptar mejores prácticas.

Diligent ofrece varias herramientas de colaboración y comunicación seguras para el Consejo de Administración. Diligent es consciente de que cualquier fallo por parte del Consejo de Administración para mantener los estándares de seguridad puede minimizar los planes de seguridad de la empresa en su totalidad. Por ello la tecnología de Diligent tiene un cifrado muy sólido y cuenta con la certificación ISO 27001. A diferencia del correo electrónico personal o del correo electrónico corporativo de un tercero, Diligent tiene herramientas que solo permiten el acceso a usuarios autorizados y aprobados. Por lo tanto, toda la información se mantendrá dentro del perímetro de seguridad de Diligent. Los consejeros y usuarios pueden usar tranquilamente el sistema y asegurarse de que no se leerán ninguna de sus comunicaciones y de que no se revelará la información en una auditoría.

Los datos sensibles de su Consejo de Administración estarán protegidos y a salvo con Diligent. Más de 4.000 clientes en más de 70 países confían en Diligent para un acceso inmediato a la información más urgente y confidencial.

Descubra más sobre Diligent en www.diligent.com/es.

Para obtener más información o solicitar una demostración, póngase en contacto con nosotros a través de:

Teléfono: +34 91 781 70 48
Correo electrónico: info@diligent.com
Entre en: diligent.com/es

CISCO

¿CÓMO PUEDE AYUDARLE CISCO?

Las últimas innovaciones de Cisco están reconfigurando el mundo de la seguridad. En un mundo con más datos, más usuarios y más servicios, hay más que proteger. Mientras tanto, las ciberamenazas evolucionan constantemente, haciéndose más inteligentes y sofisticadas. Es fundamental situar la "Ciberseguridad por encima de todo" y Cisco es capaz de hacerlo. Cisco ofrece múltiples tecnologías integradas que además se comunican entre sí para ofrecer "Ciberseguridad por encima de todo". Cisco le ofrece el alcance, la escala y las capacidades para mantenerse al día con la complejidad y el volumen de las amenazas. Poner la seguridad por encima de todo le ayuda a innovar al mismo tiempo que mantiene sus activos seguros. Cisco da prioridad a la seguridad en todo lo que hacemos. Solo con Cisco puede lograr la Seguridad en la Red, por donde pasa todo el tráfico de todas las aplicaciones, de forma que puede hacer frente a las amenazas del futuro. Cisco es la empresa de Ciberseguridad líder en la industria que ofrece una amplia cartera de productos integrados entre sí y una inteligencia global contra las amenazas.

Los investigadores de amenazas del ecosistema de Inteligencia Colectiva de Seguridad de Cisco (CSI) reúnen, bajo un solo paraguas, la inteligencia de amenazas líder de la industria usando telemetría obtenida de la vasta huella de dispositivos y sensores, fuentes públicas, privadas y la comunidad de código abierto. Esto equivale a una entrada diaria de miles de millones de solicitudes web y millones de correos electrónicos, muestras de malware e intrusiones en la red.

Nuestra sofisticada infraestructura y sistemas consumen esta telemetría, ayudando a los sistemas de machine learning e investigadores a rastrear amenazas en redes, centros de datos, puntos finales, dispositivos móviles, sistemas virtuales, web y correo electrónico. Y desde la nube, para identificar las causas de raíz y el alcance de los brotes. La inteligencia resultante se traduce en protecciones en tiempo real para todos nuestros clientes que cuentan con los productos y servicios de Cyberseguridad de Cisco.

Para obtener más información sobre nuestro enfoque de seguridad centrado en las amenazas, visite:

https://www.cisco.com/c/es_es/products/security/index.html

Consíguelo en el App Store · Consíguelo de Microsoft · DISPONIBLE EN Google Play · AICPA SOC · ISO 27001 CERTIFIED BY BRIGHTLINE