Reporte técnico

Galvanize

Trasladar el foco de la ciberseguridad desde el cumplimiento hacia los riesgos

Trasladar el foco de la ciberseguridad desde el cumplimiento hacia los riesgos

LAS ORGANIZACIONES MODERNAS COMPRENDEN AHORA QUE LA CIBERSEGURIDAD ES UN TEMA CRUCIAL.

Ha crecido la frecuencia y la sofisticación de los ciberataques; en la primera mitad de 2019, se reportaron 3813 filtraciones de datos, que representan un aumento del 54 % con respecto al año anterior[1]. Y a la luz de las modificaciones estructurales de la mano de obra relacionadas con la COVID-19 y el traslado no planificado hacia entornos de trabajo remoto que quizás no cuenten con la infraestructura adecuada, la vulnerabilidad de las empresas frente a los ataques aumentó en 2020.

A pesar de que las empresas saben que la protección de ciberseguridad es esencial para salvaguardar sus compañías, muchas conciben los protocolos de ciberseguridad como un enfoque basado en el cumplimiento de las normas gubernamentales y de la industria, en lugar de visualizarla desde un nivel de análisis de riesgos. Este reporte técnico presenta las principales razones para trasladar el foco hacia los riesgos y las mejores prácticas para hacerlo.

3813 filtraciones de datos reportadas en la primera mitad de 2019, que representan un aumento del 54 % con respecto al año anterior

[1] *https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report*

EVOLUCIÓN DEL PANORAMA DE LAS CIBERAMENAZAS

Aunque las empresas tienen algún tipo de actividad en línea desde hace tres décadas, en los primeros años de Internet, no había muchos intereses en juego para los ciberataques. Los ataques estaban motivados por la notoriedad, no por una ganancia financiera. Por ejemplo, en 1988, el "Gusano Morris"[2] se replicó en todo el ciberespacio y enlenteció las computadoras hasta el punto de hacerlas inutilizables; Robert Morris, el creador del gusano, dijo que intentaba descubrir el tamaño real de Internet.

En aquel momento, era raro que las organizaciones almacenaran datos confidenciales como archivos de clientes, datos financieros y de IP en línea; hoy lo hacen millones de compañías. Por eso, es mucho más probable que veamos ciberataques con consecuencias significativas para las empresas en términos de problemas operativos, responsabilidad, robo de IP y daño a la marca. Y debido al aumento de los dispositivos con integración de Internet de las cosas (como electrodomésticos inteligentes y automóviles autónomos), los ciberataques pueden afectar la infraestructura física de la cual dependemos, además de la IP que almacenamos en la nube.

El Informe de costos de las filtraciones de datos en 2020 de IBM mostró que el costo promedio actual de las filtraciones de datos es de USD 3,86 millones y que identificar y contener la filtración lleva generalmente 280 días.[3]

Muchas industrias ya han tomado medidas para determinar estándares mínimos de cumplimiento normativo con el fin de proteger los datos en línea de las empresas y los consumidores. Sin embargo, las organizaciones inteligentes van más allá e implementan un enfoque basado en los riesgos para monitorear y gestionar la ciberseguridad, en general dentro del ámbito del jefe de seguridad de la información (CISO, por sus siglas en inglés).

El rol del CISO ahora tiene mayor influencia; en la actualidad, el CISO puede reportar al departamento jurídico, a los jefes de información o de riesgos o, algunas veces, a todos ellos. Esto se debe a que la ciberseguridad está entrelazada con todos esos departamentos y no puede aislarse. Para el CISO es esencial ganar visibilidad dentro de la organización y lo logra con personas que defiendan iniciativas en los diferentes departamentos; uno de los cuales debería estar procesando el traslado hacia un enfoque de ciberseguridad basado en riesgos.

A continuación, veremos cómo se refleja en la práctica.

[2] *https://www.nato.int/docu/review/2013/cyber/timeline/en/index.htm*

[3] *https://www.ibm.com/security/data-breach*

EL VALOR DE LOS ENFOQUES BASADOS EN RIESGOS PARA LA CIBERSEGURIDAD Y LA GESTIÓN DE RIESGOS

¿Qué significa adoptar un enfoque de ciberseguridad más basado en riesgos en lugar de centrarse en el cumplimiento?

Con el foco en el cumplimiento, usted observará sus políticas, estándares, acuerdos contractuales, normas y mandatos legales a través de un lente específico para evaluar si cada uno de ellos satisface los estándares de cumplimiento. Por ejemplo, considere si tiene un requisito de control, por ejemplo, una protección contra malware, implementado en toda la organización. A partir de allí, debe considerar en qué medida se ha aplicado el control: ¿total, parcial o no se ha puesto en práctica?

Este enfoque tiene muchos beneficios: es fácil de seguir, fácil de comprender y se puede usar una lista de verificación para ver qué tan bueno es el desempeño de la organización. Este enfoque puede adoptarse en varios departamentos y funciona bien en un entorno relativamente estático.

Sin embargo, es difícil de actualizar para entornos dinámicos, incluidas las disciplinas como la ciberseguridad. Y su enfoque puede correr el riesgo de sobredimensionar los controles (lo cual puede acarrear costos excesivos para mitigar los riesgos) o subdimensionar los controles (lo cual puede dar lugar a inversiones insuficientes y aumentar la exposición al riesgo).

En cambio, el uso de un enfoque de análisis de riesgos permite crear el programa con una fórmula que se centre en:

+ Su perfil de riesgo: ¿Cuál es el grado de susceptibilidad de su empresa frente a los riesgos y cuáles son esos riesgos?
+ Su apetito de riesgo: ¿Qué nivel de riesgo es aceptable y cuánto está dispuesto a invertir para mitigarlo hasta ese punto?
+ Sus obligaciones de cumplimiento: ¿Qué normas de la industria debe implementar?

Poner el foco en la gestión de riesgos de ciberseguridad permite acceder a datos que aporten más información, utilidad y transparencia. Este enfoque le aportará una visión objetiva de hacia dónde debe dirigir su inversión en ciberseguridad. Comprenderá mejor sus factores de ciberriesgo y niveles de impacto, y las medidas de mitigación que debe tener en cuenta.

En cada punto, puede observar su apetito de riesgo para decidir si desea aceptar el riesgo, mitigarlo o reducirlo a un nivel aceptable. Para comprender el retorno de la inversión de sus iniciativas de mitigación de riesgos, divida el retorno financiero entre la inversión realizada.

Cuando desarrolle su proceso de gestión de riesgos, también es importante priorizar los riesgos con precisión: sea pragmático, básese en lo que sabe que su organización puede lograr en un plazo razonable. Realice una clasificación para comprender cuáles son los riesgos potenciales más costosos o con mayor impacto y luego céntrese en esas estrategias de mitigación como prioridad.

Una vez que haya determinado cuáles son todos sus riesgos, revise sus opciones. ¿Aceptará el riesgo? Esto bajará el costo pero aumentará el daño asociado. ¿O mitigará el riesgo? Lo que aumentará su nivel de inversión pero reducirá la exposición al riesgo.

Defina su respuesta en colaboración con los departamentos. Considere diferentes factores: costos, complejidad, plazo de implementación, grado de disrupción por el cambio, obstáculos empresariales, capacitación, experiencia de los usuarios finales, pruebas y aseguramiento. Al documentar cada riesgo y crear una estrategia para responder a cada uno de ellos, su organización estará mucho mejor preparada frente a potenciales vulneraciones de la ciberseguridad y otros riesgos empresariales.

¿QUÉ ES UNA "BUENA" GESTIÓN DE CIBERRIESGOS?

Cuando cree su enfoque de gestión de riesgos, recuerde las mejores prácticas. Estas son algunas recomendaciones para tener en cuenta:

+ **Implemente un comité directivo.** Cree un comité directivo interdisciplinario que le ayude a reportar los riesgos en toda la organización y colabore en la determinación de cuáles deben abordarse con mayor prioridad.
+ **Equilibre sus metas deseables y las alcanzables.** Cuando implemente sus planes, asegúrese de centrarse en objetivos viables, no en castillos en el aire que nunca se concretarán. Una regla de oro es considerar solo los planes que pueden implementarse en un plazo de dos años.
+ **Otorgue a su organización un período de gracia.** Las nuevas políticas y tecnologías no pueden implementarse instantáneamente; tenga en mente un período de gracia para permitir que su organización se tome tiempo para investigar las opciones y asegurar que el foco se centre en la implementación y la educación.
+ **Céntrese en los sistemas y activos de datos de misión crítica.** Realice una clasificación que use la evaluación del impacto para evaluar la criticidad de cada sistema o activo impactado desde una perspectiva de negocios cuando determine cuáles riesgos priorizar.
+ **Evalúe productos de GRC para ayudar a agilizar el proceso.** Con la elección de la pila de tecnología adecuada para sus iniciativas de GRC, puede semiautomatizar los procesos de ciberriesgos para minimizar el empleo de personal.
+ **Presente un argumento de negocios que ayude a establecer el enfoque de ciberriesgos.** Comparta con las partes interesadas un plan claro y dedicado para mejorar la postura de ciberseguridad de su negocio, que incluya las inversiones necesarias, las ganancias rápidas y las mejores prácticas.
+ **Establezca un enfoque escalonado.** No intente abarcar lo inabarcable y hacer todo de una vez. Comience con las iniciativas de mayor prioridad y desarrolle el programa a partir de allí.
+ **Extrapole la información de los riesgos a otras áreas del programa de seguridad.** Una vez que su programa de gestión de riesgos esté listo, muestre los mensajes a través de actualizaciones de la política y un programa de concientización y educación de toda la empresa.
+ **Promocione el enfoque entre sus clientes y socios.** La presentación de su enfoque estratégico de ciberseguridad puede ayudar a mejorar el posicionamiento competitivo de su empresa.

En el proceso de evaluación de riesgos empresariales, siga estos pasos:

1. Cree un perfil: comience por configurar su perfil empresarial con un inventario de los riesgos.
2. Determine el impacto empresarial: ¿qué impacto tendría cada riesgo en las finanzas o la reputación de su empresa?
3. Evalúe las amenazas: ¿cuál es la probabilidad de que la amenaza se concrete, sobre la base de los datos históricos y de la industria?
4. Evalúe las vulnerabilidades: ¿qué puntos débiles existen en su organización?
5. Determine el riesgo: evalúe cuáles son los riesgos prioritarios.
6. Trate el riesgo: sobre la base de los costos y el impacto potencial, ¿debería mitigar, evitar, transferir o aceptar cada riesgo?

Tenga presente que los ciberriesgos no deben estar compartimentados. Con frecuencia, otros departamentos necesitarán capacitación y educación sobre la forma de abordar los problemas de ciberseguridad. Por ejemplo, su departamento de RR. HH. debe implementar políticas para evitar los ataques internos, su equipo de concientización y educación corporativa debe desarrollar un seminario sobre la prevención de ataques de ingeniería social, y sus contratos de suministro deben incluir el lenguaje adecuado y los estándares mínimos que disminuyan el riesgo de una vulneración de terceros.

Al asegurarse de crear un programa integral alineado con las mejores prácticas del análisis de riesgos de ciberseguridad, puede lograr la aceptación de toda la organización y generar conciencia de la importancia del trabajo que está haciendo su equipo.

LA IMPORTANCIA DE LA AUTOMATIZACIÓN PARA LA GESTIÓN DE CIBERRIESGOS

Un proceso robusto de gestión de ciberriesgos depende de herramientas de automatización y estudios analíticos de datos que garanticen que su equipo esté al tanto del estado de los riesgos existentes en todo momento y que usted pueda implementar estrategias de mitigación de inmediato si se produce una acción disparadora. Su pila de tecnología de monitoreo de riesgos debe incluir la capacidad de establecer su apetito para cada riesgo, monitorear los riesgos, ver los riesgos en conjunto y reportar el nivel de riesgo para que tenga una clara visibilidad en toda la organización.

Su solución debe tener estas características claves:

+ Estar respaldada por las mejores prácticas de la industria
+ Utilizar fuentes de datos en tiempo real para analizar nuevas amenazas
+ Compartir en forma anónima información clave de incidentes y amenazas
+ Ser intuitiva para los usuarios sin capacitación especializada en la industria
+ Proporcionar datos relacionados con la industria para las evaluaciones de riesgos
+ Proporcionar cifras de la inversión en relación con el impacto para el seguimiento del ROI
+ Ofrecer opciones flexibles de generación de reportes

Su solución debe conectarse a diferentes orígenes de datos para el análisis de amenazas en tiempo real y el seguimiento de la vulnerabilidad. También debe integrarse con sus marcos de riesgos y normativos para que usted pueda seguir con facilidad el apetito de riesgo y verificar el cumplimiento. Mediante la automatización del monitoreo de los niveles riesgo o las normativas cambiantes, puede eliminar la carga operativa de la supervisión manual. Los analistas de ciberriesgos deben recibir alertas automatizadas de las situaciones que necesitan acciones posteriores y reservar su tiempo para los asuntos que requieren análisis estratégico.

Trasladarse a una plataforma automatizada de evaluación de riesgos le permitirá optimizar su estrategia de gestión de ciberriesgos y tener en todo momento una visibilidad clara de sus principales riesgos y de los factores externos que quizás puedan crear vulnerabilidades potenciales. Eso habilitará a su equipo para priorizar la mitigación de riesgos y corregir las vulnerabilidades con rapidez, en lugar de esperar meses para descubrir las fallas que hayan ocurrido.

CONCLUSIÓN

Como demostraron los repentinos cambios de la cultura de trabajo que provocó la COVID-19, es importante estar al tanto de los potenciales riesgos y vulnerabilidades. Así, podrá priorizar el monitoreo y la mitigación cuando ocurra lo inesperado, en lugar de precipitarse para crear un plan en el momento.

Crear un programa de ciberseguridad centrado en la gestión de riesgos en lugar de abordar simplemente los asuntos de cumplimiento le brinda a su organización un mayor grado de conciencia que permite dar una respuesta rápida y predecible a las amenazas que surgen y subsanar las vulnerabilidades en cuanto ocurren. Un proceso de detección de amenazas y análisis de riesgos automatizado y basado en datos proporcionará la información que su organización necesita para mantener un entorno de trabajo protegido y seguro en cualquier circunstancia, incluso frente a sucesos sorpresivos y de gran impacto como la pandemia de COVID-19.

70 % **de los CISO de EE. UU. entrevistados en una encuesta de Optiv Security dijeron que la directiva de la empresa los alentó a priorizar la ciberseguridad frente a todas las demás iniciativas de negocios.**

El trabajo proactivo para identificar, monitorear, gestionar y mitigar sus riesgos como organización le permitirá reducir el riesgo de vulneraciones importantes que podrían afectar gravemente las operaciones, el rendimiento financiero y la reputación de su empresa.

Las empresas de primer nivel saben que invertir en un plan sólido para proteger la ciberseguridad y monitorear los riesgos dará dividendos en términos de desempeño. De hecho, el 70 % de los CISO de EE. UU. entrevistados en una encuesta de Optiv Security dijeron que la directiva de la empresa los alentó a priorizar la ciberseguridad frente a todas las demás iniciativas de negocios.[4]

La ciberseguridad abarca todas las unidades de negocios y una vulneración puede tener un enorme impacto negativo en toda la organización.

Mediante la creación de un plan viable y la inversión en tecnología automatizada para monitorear y gestionar los ciberriesgos de su organización, logrará una ventaja frente a sus competidores que se centran únicamente en las iniciativas de cumplimiento y contará con los datos y análisis que le ayudarán a elegir las estrategias mejores y más rentables para mitigar cualquier problema que pueda surgir.

[4] *https://www.optiv.com/sites/default/files/2019-09/Brand_CISO-ResearchStudy_Report_091719.pdf*