CIBERSEGURIDAD 2020: MITOS VS. REALIDAD

EL MUNDO EN EL QUE VIVIMOS

En nuestra sociedad impulsada digitalmente, la ciberseguridad es un elemento esencial para garantizar la integridad y la privacidad de los datos. Casi todas las organizaciones están atravesando alguna forma de transformación digital para mejorar el acceso a los datos, aumentar la velocidad de comercialización y reducir los gastos operativos. Desafortunadamente, también vivimos en una época de tecnología falsa extensa, fraude cibernético desenfrenado, mayor sofisticación de los ataques cibernéticos y costosas violaciones de datos cibernéticos. Muchas organizaciones están luchando por separar los hechos de la ficción (información errónea, exageraciones y noticias falsas) para comprender el valor del creciente número de software, hardware, pólizas de seguro y servicios profesionales relacionados que trabajan para mitigar el fraude cibernético demandas y daños por violación de datos. Para disipar algunos de los mitos comunes que rodean la ciberseguridad, buscamos investigación, una amplia experiencia de campo y el sentido común.

BDO®

Mito #1

La mayoría de las empresas han aumentado significativamente sus inversiones en software, hardware, pólizas de seguro y servicios profesionales relacionados en los últimos tres años para gestionar adecuadamente los riesgos cibernéticos.

Realidad

Para el 2021, se espera que el fraude cibernético global y los daños por violación de datos cibernéticos alcancen los $6 billones, aumentando de los $4 billones actuales en daños globales, según Cybersecurity Ventures. Los daños globales por el fraude cibernético y las violaciones de datos cibernéticos han ido en aumento durante los últimos diez años, en gran parte debido a una subinversión en la ciberseguridad global. Muchas empresas han aumentado modestamente su gasto en herramientas y servicios de ciberseguridad. Sin embargo, la organización promedio actualmente gasta / invierte solo del 2% al 5% de su presupuesto anual de tecnología de la información en seguridad de la información, según estudios de Forrester Research, Gartner Group y el Instituto de Ingeniería de Software (SEI) de la Universidad Carnegie Mellon (CMU).

Mito #2

Casi todas las organizaciones brindan información oportuna y detallada sobre la evolución de los riesgos de ciberataque y ciberataque a sus ejecutivos y a la Junta Directiva.

Realidad

Según la encuesta de gobernanza cibernética de BDO de 2019 (BDO's 2019 Cyber Governance Survey), menos del 30% de los directores ejecutivos y de la junta directiva encuestados afirmaron que recibieron actualizaciones trimestrales o más frecuentes sobre amenazas de ataques cibernéticos, amenazas de fraude cibernético o factores de riesgo de violación de datos cibernéticos.

Mito #3

La mayoría de las organizaciones han contratado a un director de seguridad de la información (CISO) de tiempo completo, dedicado y altamente capacitado para administrar la estrategia de seguridad de la información, las personas, las políticas, los planes, los sistemas, las herramientas y los procedimientos de su organización para mitigar eficazmente el fraude cibernético y la violación de datos cibernéticos riesgos.

Realidad

Menos del 20% de todas las organizaciones encuestadas por BDO durante los últimos tres años han contratado a un CISO. De aquellos a los que se les ha asignado el título de CISO, muchos carecen de educación, capacitación y certificación profesional en ciberseguridad adecuadas.

Mito #4

Los especialistas en ciberseguridad son capaces de gestionar eficazmente el creciente número de ciberamenazas como resultado directo de los avances tecnológicos en análisis de big data, visualización de datos, cifrado de datos, biometría, gestión de identidad y acceso, arquitectura de datos, simulaciones de ciberataques, entrenamiento basado en inteligencia artificial.

Realidad

La mayoría de las pequeñas y medianas empresas han realizado inversiones tecnológicas relativamente limitadas para mejorar la ciberseguridad, debido a razones financieras.

Mito #5

El uso de educación, capacitación, simulaciones y campañas de phishing por correo electrónico en ciberseguridad ha permitido a las organizaciones frustrar todos los ataques de phishing por correo electrónico.

Realidad

El factor humano sigue siendo el eslabón más débil de la ciberseguridad. Incluso después de realizar campañas periódicas de educación, capacitación y de concientización sobre ciberseguridad, la mayoría de las organizaciones generalmente encuentran que alrededor del 5% o más de sus empleados aún son susceptibles a ataques de phishing. Además, los ataques cibernéticos de amenazas internas humanas representan un peligro claro y presente para casi todas las organizaciones.

Mito #6

Solo las grandes empresas multimillonarias y las agencias gubernamentales están sujetas a importantes violaciones de datos cibernéticos.

Realidad

Según un estudio reciente de Forrester Research, casi todas las industrias del mundo han sufrido importantes violaciones de datos cibernéticos y aproximadamente el 30% de todas las violaciones de datos cibernéticos notificadas se produjeron en empresas con menos de 200 empleados. Además, es importante tener en cuenta que muchos ciberataques y violaciones de datos no se informan..

Mito #7

La cobertura del seguro de responsabilidad cibernética puede garantizar que las organizaciones estén protegidas financieramente de costosos fraudes cibernéticos y violaciones de datos.

Realidad

Hay más de 100 compañías de seguros en todo el mundo que ofrecen una amplia gama de pólizas de cobertura de seguro de responsabilidad cibernética, con muy diversas limitaciones, exenciones y términos y condiciones. A la mayoría de las empresas les resulta difícil fundamentar algunos de los daños mientras preparan una reclamación por violación de datos cibernéticos y no siempre reciben el reembolso completo de las compañías de seguros por las acciones necesarias de reparación de seguridad cibernética posteriores a la violación.

Mito #8

La mayoría de los contratistas principales gestionan de forma eficaz el riesgo de ciberseguridad de su cadena de suministro a través de programas de gestión de relaciones con proveedores y auditorías cibernéticas realizadas de forma independiente.

Realidad

La mayoría de los contratistas principales confían principalmente en las autoevaluaciones de riesgo cibernético de los proveedores y no realizan auditorías de riesgos de ciberseguridad de los proveedores ni exigen auditorías de ciberseguridad específicas de la industria y certificaciones de cumplimiento de ciberseguridad de forma independiente, como ISO 27001.

Mito #9

Para detectar rápidamente las intrusiones cibernéticas y reducir el impacto de una violación de datos cibernéticos, la mayoría de las organizaciones han implementado un sistema de correo electrónico eficaz 24 x 7 x 365 y una capacidad de respuesta a incidentes, detección y monitoreo del sistema de red.

Realidad

Muchas pequeñas y medianas empresas son vulnerables a estos daños y no realizan monitoreo activo, detección y capacidad de respuesta a incidentes las 24 horas del día, los 7 días de la semana, los 365 días del año, ni internamente ni a través de proveedores de servicios de seguridad administrados (MSSP) subcontratados.

Mito #10

La mayoría de las empresas y organizaciones gubernamentales han desarrollado, documentado e implementado un programa de defensa cibernética eficaz.

Realidad

Desafortunadamente, la mayoría de las organizaciones no están implementando un programa eficaz de ciberseguridad basado en amenazas. Más bien, algunas empresas no tienen políticas, planes y procedimientos de ciberseguridad estructurados o documentados. Muchas empresas y organizaciones gubernamentales están optando por implementar un enfoque de ciberseguridad basado en la lista de verificación de cumplimiento, que está bien intencionado, pero que a menudo no logra una verdadera defensa cibernética, ya que las regulaciones no pueden seguir el ritmo de las tácticas de ciberataque, métodos y procedimientos.

RESUMEN

Con demasiada frecuencia, los altos ejecutivos toman malas decisiones de inversión en seguridad de la información basadas en información errónea, un enfoque financiero a corto plazo y una falta de conciencia sobre la seguridad cibernética, lo que deja a sus empresas vulnerables a las ramificaciones de los ataques cibernéticos. Para lograr una seguridad de la información real, una organización debe comprender los elementos clave y los conceptos erróneos que rodean el problema, tales como: los objetivos de datos del ciberatacante y los métodos sofisticados, así como la evaluación de las vulnerabilidades reales de los ataques al sistema de información de su organización.

CONTACTO

STEVEN CAUWENBERGHS
Partner - Risk Advisory
+32 (0) 497 05 12 23
steven.cauwenberghs@bdo.be

FRANCIS OOSTVOGELS
Manager - Risk Advisory
+32 (0) 474 92 08 00
francis.oostvogels@bdo.be

NICK HUYSMANS
Manager - Risk Advisory
+32 (0) 486 31 90 45
nick.huysmans@bdo.be

BDO Risk & Assurance Services, a Burg. Ven. CVBA registered in Belgium under BTW BE 0874 840 624 RPR Brussel, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name of the BDO network and for each of the BDO Member Firms.

Copyright © January 2020 BDO Risk & Assurance Services. All rights reserved.

www.bdo.be