El Deber del CISO

Generando confianza en seguridad para 2023

El mundo se siente muy diferente de lo que era hace unos pocos años. El COVID cambió la forma en que abordamos el trabajo y aceleró el cambio a modelos de trabajo remotos e híbridos. En el camino, nos encontramos con una nueva ola de riesgos en ciberseguridad, contra los cuales la protección se ha convertido en una necesidad para la supervivencia para las organizaciones. Justo cuando nos estábamos poniendo al día y asegurando nuestro nuevo entorno TI, las circunstancias cambiaron una vez más a medida que las tensiones geopolíticas creaban un mundo cada vez más polarizado. De cara al futuro, vemos más cambios comerciales, económicos, tecnológicos y regulatorios, y más disrupción.

Como era de esperar, el panorama de las amenazas cibernéticas continúa evolucionando a medida que los delincuentes, tanto organizados como respaldados por Estados, buscan nuevas oportunidades para crear caos y obtener ganancias. Los ciberprofesionales, y los Responsables de Seguridad de la Información (CISO, en inglés) en particular, a menudo sienten que están trabajando duro pero progresando poco.

Creemos que el enfoque más racional para los equipos de seguridad es reconocer que nunca podrán protegerse contra todo. Este es un mensaje desafiante para comunicar a los ejecutivos. Es probable que las organizaciones siempre tengan algún grado de riesgo cibernético y, a pesar de que se tomen todas las debidas precauciones, los controles de seguridad pueden fallar, y con frecuencia así ocurre. Si las empresas tratan de protegerse contra todos los riesgos potenciales, no solo la demanda de presupuesto puede ser un lastre, sino que el costo de oportunidad puede ser oneroso dado el impacto en las operaciones y actividades comerciales.

Quizás la aspiración central de los CISOs es mantener la resiliencia de sus organizaciones a medida que aumentan los riesgos de ataques cibernéticos. Si se produce una fuga de datos o una violación de la red, ¿qué tan rápido puede la empresa detectar y contener el ataque, reanudar las operaciones y minimizar el impacto en los clientes? Esta preocupación es emblemática en la agenda de resiliencia que estamos viendo en la última ola regulaciones que están discutiéndose al respecto, en particular en torno al sector financiero, empresas de seguro y reaseguros, pensiones, casinos y juegos, entre otros. A menudo, la solución implica contar con un proceso para una detección y respuesta efectivas, una reconstrucción/restauración rápida y priorizada de los sistemas después de la interrupción y un enfoque en lo que realmente importa para el negocio. Al final, las empresas deben lograr un equilibrio entre invertir en controles preventivos y en mejorar su resiliencia.

Nuestro próximo informe anual sobre consideraciones de ciberseguridad reúne la visión de especialistas de KPMG en diferentes tópicos de la ciberseguridad a nivel mundial para explorar ocho consideraciones que los CISOs y sus equipos deben priorizar en 2023 para ayudar a mitigar el impacto de los incidentes cibernéticos y proteger el futuro de sus organizaciones. Aquí les compartimos un adelanto:

1 En tiempos inciertos, la confianza importa

La posibilidad de confiar en los sistemas digitales se está convirtiendo en un asunto que se discute a nivel de Directorio. Las personas esperan que las empresas actúen con honestidad, integridad y transparencia al maneja su información personal, y que brinden a la vez servicios digitales sólidos y seguros. En línea con el sentir de la opinión pública, los políticos y reguladores están actuando para moldear y desafiar las conductas empresariales en torno a la materia. Aprovechando nuestra reciente Encuesta de Insights sobre Confianza Cibernética, el reporte que emitiremos analizará las acciones prácticas que los CISO y sus equipos pueden tomar para ayudar a enmarcar el debate y desempeñar un papel integral en la construcción y el mantenimiento de la confianza.

2 Confía en la automatización

Nuestra Encuesta de Insights sobre Confianza Cibernética encontró que el 78 % de los ejecutivos cree que la

adopción de sofisticados sistemas de inteligencia artificial (IA) y machine learning plantea desafíos de ciberseguridad únicos, y muchos creen que también plantean cuestiones éticas más amplias. La creación de un marco para fortalecer la seguridad y la privacidad de las estructuras impulsadas por IA y, al mismo tiempo, permitir la innovación rápida y el desarrollo ágil será clave para aprovechar el potencial de estas tecnologías en desarrollo. Nuestro reporte explorará cómo los CISOs pueden lograr estos objetivos en conjunto con los equipos de privacidad y ciencia de datos y ayudar a sus empresas a prepararse para un entorno regulatorio que cambia rápidamente.

Seguridad que no obstaculiza

La seguridad a menudo se percibe como un obstáculo que agrega complejidad y costo a los sistemas y, al mismo tiempo, limita la funcionalidad. Claramente, los clientes continúan confiando en que basta con usar contraseñas, descargando públicamente su frustración cuando se bloquean sus cuentas, lo que causa desánimo. A menudo escuchamos la frase de "las personas son el eslabón más débil", pero ¿es realmente así o nuestros sistemas de seguridad son hostiles y difíciles de usar? El informe examinará cómo la seguridad se puede integrar de manera efectiva en el negocio, para que no solo no obstaculice, sino que sea intuitiva, y así entusiasmar a los empleados de toda la empresa a ser parte de un gran firewall humano.

Asegurar un futuro sin perímetro definido

Hasta cierto punto, era posible decir que existía un perímetro digital para una empresa. Sin embargo, el COVID eliminó esa ilusión, obligando a las organizaciones a adaptarse a modelos de trabajo remotos e híbridos. Las empresas globales de hoy, las 24 horas del día y los 7 días de la semana, necesitan ayuda para definir realmente el perímetro de acción de sus planes de ciberseguridad, ya que han llegado a depender de un complejo ecosistema compartido con socios y proveedores, vinculados por plataformas computacionales en la nube. En esta nueva realidad, ¿cómo pueden las empresas otorgar seguridad a un modelo de negocio tan altamente distribuido?

El informe profundizará en los aspectos prácticos de implementar nuevos paradigmas y ambientes de confianza, alineados de mejor manera con los modelos de trabajo del mañana.

Seguridad también debe cambiar

Puede ser fácil ignorar la necesidad de un cambio en la función de seguridad en sí misma, pero hacerlo sería ingenuo. Los equipos de seguridad están asumiendo roles muy diferentes hoy en día. El modelo de responsabilidad compartida trae nuevas alianzas con proveedores de servicios en la nube; los cambios a procesos de desarrollo operacional ágiles nos llevan a repensar cómo incorporar seguridad desde el diseño; y la seguridad de la empresa y de los clientes y socios comerciales ahora abarca una gama mucho más amplia de sistemas y activos, a menudo fuera del control directo del CISO.

Nuestro informe revisará nuevos modelos de seguridad, que tratan la seguridad como un hilo conductor que conecta todas las áreas de la empresa y su red ampliada de colaboradores, y la consiguiente necesidad de contar con nuevas habilidades.

Seguridad inteligente para un mundo Smart

Nuestro mundo se está volviendo más inteligente a medida que los dispositivos conectados están integrados en todos los aspectos de nuestras vidas, particularmente en la infraestructura que respalda los ámbitos digital y físico. Hoy contamos con tecnología operativa (OT) sofisticada, sensores ubicuos y hasta sistemas y robots autónomos, con lo que los entornos operativos y de desarrollo son muy diferentes a cómo era el panorama de TI empresarial clásico. Sin embargo, posiblemente, la seguridad importa aún más con estas nuevas estructuras y la división tradicional entre TI y OT se está desvaneciendo.

Nuestro reporte profundizará en cómo las empresas pueden incorporar un enfoque de seguridad en estos diferentes entornos y qué esperarán los reguladores de las empresas para habilitar la seguridad de la infraestructura y los productos en el futuro.

Contrarrestar adversarios ágiles

Hace unos años, una semana era mucho tiempo en ciberseguridad. Hoy, un día puede parecer una eternidad cuando se trata de un atacante ágil y sofisticado. Como comunidad de seguridad, hemos mejorado mucho en la detección y el bloqueo de nuevas tácticas de ciberataque, trabajando con socios tecnológicos para acabar con la infraestructura que respalda el ataque e implementando medidas de defensa activa a nivel nacional. Pero eso requiere operaciones de seguridad que puedan responder en minutos en lugar de días, para detectar rápidamente comportamientos anómalos y maliciosos, aplicar medidas de contención y expulsar a un atacante de la red. El informe que divulgaremos proporcionará una evaluación de cómo podría ser en el futuro un centro de operaciones de seguridad y la gestión de un servicio de detección y respuesta, así como el papel del machine learning, así como una visión sobre cómo evolucionará el modelo de vinculación con la nueva comunidad más amplia de actores que participan en la red digital colaborativa que están teniendo las empresas.

Ser resiliente cuánto y dónde importa

A pesar de desplegar los mejores esfuerzos, lo peor siempre puede suceder. De hecho, es probable que sea inevitable. La resiliencia es fundamentalmente una discusión a nivel empresa, no solo una aspiración del área de seguridad, y los CISO deben resistir la tentación de asumir la responsabilidad de la seguridad organizacional como un problema exclusivo de ellos. Más bien, los CISOs

y sus equipos pueden funcionar como convocantes, animadores y catalizadores de ese diálogo que debe darse en toda la organización. Los CISOs aportan una perspectiva valiosa a estas discusiones, ya que buscan contrarrestar la intención de los adversarios maliciosos de interrumpir la organización.

En el reporte, intentaremos entrar en esa perspectiva analizando los desafíos de la resiliencia frente a un ciberataque y cómo las organizaciones pueden prepararse mejor.

A medida que avanza el 2023, nuestro mundo sigue fluyendo de forma acelerada, desafiante y cambiante. Otorgar seguridad a una empresa sigue siendo tan relevante como siempre, pero los CISOs y sus equipos deben estar preparados para adaptarse a los nuevos desafíos. Al hacerlo, el hilo conductor de la ciberseguridad deberá tejerse en torno a todo el negocio, tocando todos los aspectos de la planificación estratégica y operativa del futuro.

Contactos

Akhilesh Tuteja
Global Cyber Security Leader
KPMG International and Partner
KPMG en India

E: atuteja@kpmg.com

Kyle Kappel
Principal, Cyber Security Services
Network Leader
KPMG en Estados Unidos

E: kylekappel@kpmg.com

Erick Palencia
Managing Director - Consulting y
Líder de Ciberseguridad
KPMG en Chile

E: erickpalencia@kpmg.com

Diseñado por Evalueserve.
Nombre de la publicación: The CISO´s imperative | Número de publicación: 138468-G | Fecha de publicación: diciembre de 2022