Nueve prioridades para ciberseguridad en este 2022

Es una época de balances y de prioridades para lo que viene. En ese sentido, una de las áreas que creció producto del incremento de los ciberataques fue la seguridad en entornos digitales. Y aunque existe mayor concientización e inversión, falta camino por recorrer.

Hoy más que nunca es importante seguir avanzando en la preparación de los colaboradores y de los equipos de trabajo en las empresas para seguir creciendo. Es por esto que comparto nueve prioridades que deben tener en cuenta todos los Chief Information Security Officer (CISO) durante este año.

Mejorar la comunicación entre los directivos. Existe el potencial de optimizar la comunicación entre los equipos pero hasta ahora, las conversaciones no gozan de mucha estructura y a menudo no tienen una cadencia regular. De hecho, el rol de CISO es más valorado cuando hay una crisis y, por el contrario, empujado hacia abajo en la lista de prioridades cuando no está sucediendo un incidente. Esto mejorará con un modelo de gobierno estructurado con representación de alto nivel, un conjunto acordado de KPIs que reflejen los requisitos de negocio y oportunidades regulares para demostrar cómo la seguridad es un facilitador del negocio.

Garantizar que la seguridad sea resistente al cambio empresarial. La resiliencia es cada vez más importante en un sentido más amplio y, por lo tanto, es esencial que la seguridad sea resistente al cambio y pueda moverse con el negocio. Esto se puede lograr planificando las actividades de continuidad del negocio/ recuperación ante desastres (BC/DR) con anticipación y compartiendo la responsabilidad sobre ellas. Los CISOs deben incluirse en estas actividades ya que su aporte sigue siendo esencial en este proceso.

El riesgo debe ser un problema compartido. Se debe establecer la responsabilidad del riesgo y el reconocimiento de este como un problema de negocio. Para mitigar los riesgos futuros, existe una gran necesidad de identificar a varios propietarios de riesgos en el negocio y no simplemente delegar en el CISO.

Preparándose para "La Gran Renuncia". Actualmente se está escribiendo mucho sobre la "gran renuncia", que probablemente continuará interrumpiendo todas las industrias este año. Por lo que podemos decir que es probable que este problema empeore antes de mejorar. Algunos CISOs están viendo el trabajo remoto como una posible solución; los equipos distribuidos se ven como una necesidad en algunas circunstancias, pero también existe la necesidad de que los equipos se reúnan cara a cara de manera regular.

Visibilizar el "shadow IT". Para muchos CISOs, un problema creciente son las nuevas herramientas de TI adoptadas sin el conocimiento de los equipos de seguridad, incluso cuando se establecen directrices claras de no hacerlo. Con frecuencia, la velocidad y la disponibilidad tienden a prevalecer sobre los factores de seguridad. Como resultado, se enfrentan constantemente a problemas. Si no se arregla esto aumentarán a medida que más y más empresas se muevan en la nube.

Gestión de riesgos de terceros. Esto sigue siendo un problema, especialmente en las evaluaciones de terceros que a menudo son largas, en plazos cortos y en un formato no estándar. La buena noticia es que se está trabajando en marcos que garanticen una certificación estandarizada para terceros, como en el sector de servicios financieros del Reino Unido, con la Declaración de Supervisión del Banco de Inglaterra – SS2/21: Outsourcing y gestión de riesgos de terceros, que entra en vigencia el 31 de marzo de 2022. El progreso en esta área seguramente será bienvenido, dado que los CISOs necesitan confiar en procesos probados, pero aún deben asegurarse que su alcance de áreas de riesgo sea lo suficientemente amplio como para incluir a cualquier proveedor o empleado con acceso remoto a cualquier aplicación empresarial.

Más enfoque en los datos y la privacidad. Es un problema que aún no se reconozca el valor de los datos. La privacidad se está regulando cada vez más con la entrada en vigor de la regulación regional y local. En los últimos años ha habido un gran enfoque en GDPR de la UE, lo que ha revelado las áreas en las que los CISOs han estado enfocando su energía cuando se trata de datos y privacidad. En términos generales, estos incluyen verificar la identidad del usuario, verificar el estado de todos los dispositivos del usuario y asegurar el acceso a cualquier aplicación.

Gestión de la deuda de seguridad. Hay mayor conciencia sobre la deuda técnica o la deuda de seguridad. La necesidad de gestionar sistemas más antiguos mientras se adapta al nuevo entorno y el riesgo y el costo en que esto incurre es especialmente importante a considerar en el área de tecnología operativa (OT). Además, algunos sistemas OT no se pueden parchear fácilmente o **incluso no tienen herramientas de seguridad básicas como anti-malware instalado en ellos.**

Ransomware, ransomware y más ransomware. Este es el principal problema táctico que preocupa a los CISOs. Resolver con equipos especializados en la gestión, con colaboradores preparados y una sólida estrategia de ciberseguridad será clave.