SOFTENG
YOUR COMPETITIVE ADVANTAGE

La miopía en el Comité de Dirección, y el papel del CIO para prevenirla y mantener la compañía protegida y segura.

La miopía, conocida como la visión de cerca, se produce cuando vemos con claridad lo que está más próximo a nosotros, pero borroso todo aquello que está en la lejanía o a cierta distancia. En el mundo empresarial, denominamos miopía cuando el foco está puesto en el corto plazo sin ser capaces de ver lo que puede venir para estar mejor preparados.

Pues bien, en un mundo cada vez más digital y con la sofisticación actual de las ciberamenazas, la seguridad es un activo estratégico vital para el negocio, pero que requiere poder ver con claridad los beneficios a largo plazo para actuar de manera eficaz ahora en el corto plazo; y evitar verlo *todo negro* cuando el daño ya sea inevitable.

Analizamos cuál es el papel del CIO y CISO a través de 3 objetivos estratégicos y sus desafíos, partiendo de un escenario de miopía en el Comité de Dirección, con el fin de prevenirla para mantener la compañía protegida y segura.

1. Promover una cultura de confianza digital

el 87%

de los responsables de ciberseguridad creen que su organización se está quedando corta para abordar los riesgos cibernéticos, según el estudio ‘Prioridades de seguridad 2021’ de IDC Foundry.

El desafío

La digitalización ha derribado los muros físicos abriendo el perímetro corporativo por los cinco costados y dejando desprotegidas nuevas superficies de ataque.

Por ello, es esencial que todas las personas de la empresa, a todos los niveles, estén implicadas y alineadas porque la identidad - es decir, ellos literalmente -, son la primera línea de seguridad.

El objetivo

Todo cambio empieza por la cultura.

Para mentalizar a toda la empresa sobre los riesgos de seguridad y sus consecuencias, es clave promover un plan de concienciación para crear una cultura de confianza digital, que debe bajar en cascada desde la Alta Dirección a todas las áreas de negocio.

Solo con una cultura de confianza digital sólida, la empresa será capaz de abordar de manera exitosa los complejos retos de la ciberseguridad.

2. Implementar un modelo de seguridad Zero Trust

el ransomware

ha sido considerado la principal amenaza en 2020-2021, según el informe «Panorama de amenazas» de ENISA.

El desafío

Actualmente, los ataques de ransomware son una de las principales amenazas a la seguridad digital de la empresa. El Ransomware-as-a-Service (RaaS) es un modelo de negocio que facilita los ataques de ransomware independientemente del conocimiento de los ciberdelincuentes.

Pero esto es solo una muestra de entre todos los tipos de ciberamenazas y de lo fácil que puede ser lanzar un ataque malicioso.

Por ello, es vital securizar y proteger todas las superficies de ataque, y estar siempre alerta. Es importante tener en cuenta que cualquier amenaza, por leve que sea, puede impactar críticamente en cualquiera de nuestras superficies vulnerables y hacer tambalear el negocio, sufriendo la paradoja del castillo de naipes

El objetivo

Por ello, es vital securizar y proteger todas las superficies de ataque, y estar siempre alerta.

Es importante tener en cuenta que cualquier amenaza, por leve que sea, puede impactar críticamente en cualquiera de nuestras superficies vulnerables y hacer tambalear el negocio, sufriendo la paradoja del castillo de naipes.

Zero Trust genera un claro beneficio tangible en la seguridad de la empresa. Pero, además, también proporciona un alto valor intangible ayudando a consolidar una cultura de confianza digital en todos los niveles de la empresa y protegiendo el negocio.

3. Adoptar y escalar la innovación en la nube

para el 2025,

según Gartner, más de la mitad del gasto de las organizaciones en software de aplicaciones, servicios de procesos comerciales e infraestructura de sistemas se habrá trasladado a la nube.

El desafío

La adopción de nuevas tecnologías por parte de las empresas es algo que ocurre desde siempre. Innovar no es nuevo, pero hoy es imprescindible para que cualquier organización esté bien preparada, progrese y se mantenga competitiva.

Ahora bien, no hay innovación sin presupuesto.

Por ello, el desafío del CIO es consolidar la seguridad como un activo estratégico para aumentar la implicación presupuestaria que permita contar con los recursos necesarios y un entorno en la nube seguro para innovar.

El objetivo

Adoptar la nube como modelo de innovación digital es el camino para avanzar.

Y ello, pasa indudablemente por hacerlo de manera escalable y segura frente a la sofisticación de las ciberamenazas que se producen como esporas en un entorno cada vez más digital, siendo necesario estar siempre alerta.

Promover una cultura de confianza digital,
demostrar los beneficios para el negocio de una estrategia de seguridad Zero Trust
y adoptar la innovación digital en la nube de manera escalable y segura,
son tres objetivos estratégicos que deben estar subrayados en la agenda del CIO
para convertir la seguridad en un activo de alto valor para el negocio.

SOFTENG
YOUR COMPETITIVE ADVANTAGE

Te recomendamos:

- ¿Por qué la ciberseguridad es un laberinto tan complejo para las empresas?
- Cómo evitar sufrir la paradoja del castillo de naipes para garantizar la seguridad digital
- ¿Por qué tu empresa debería adoptar una estrategia de seguridad Zero Trust?

Para más información: **info@softeng.es**

Fuentes:

- Security Priorities Study 2022 • Foundry (foundryco.com)
- Informa “Panorama de amenazas” de Enisa 2021.
- Se acelera el cambio hacia la TI en la nube, artículo en IT Trends.
- Gartner Says More Than Half of Enterprise IT Spending in Key Market Segments Will Shift to the Cloud by 2025, artículo de Gartner.
- Extortion Economics | Security Insider, artícuo de Microsoft
- The Innovator's Guide to Zero Trust Security, eBook CSO y Microsoft Security.