LITORALPRESS

Fecha: 24-08-2024
Medio: La Tercera
Supl. : La Tercera - Pulso
Tipo: Noticia general
Título: Capacitación interna: la primera línea de defensa en ciberseguridad de las empresas

Pág. : 14
Cm2: 568,7
VPE: $ 5.658.383

Tiraje: 78.224
Lectoría: 253.149
Favorabilidad: Positiva

Capacitación interna: la primera línea de defensa en ciberseguridad de las empresas

"Menos del 15% de las organizaciones toma acciones de forma continua para identificar y gestionar las vulnerabilidades", afirma Kenneth Daniels, gerente general de Widefense.

BÁRBARA PEZOA

Según datos entregados por el estudio "Chile Cyber Threat Activity", realizado por la multinacional estadounidense de ciberseguridad Trellix –que anualmente investiga actos maliciosos de vulneración informática remota efectuados en diversas partes del mundo–, nuestro país fue víctima de 741.152 ataques entre enero y septiembre del año pasado.

Por otro lado, la encuesta "Chile nos habla – Ciberseguridad", realizada por la Universidad San Sebastián, revela que solo un 18,7% de las personas sondeadas admite haber recibido una capacitación o educación de ciberseguridad en su lugar de trabajo o estudios. ¿Cuán preocupante es esta modesta cifra en relación a la cantidad de ataques que recibimos?

Kenneth Daniels, gerente general de Widefense, empresa de ciberseguridad con más de 30 años de experiencia, conversó con **Pulso** sobre lo esencial que se ha vuelto hoy capacitar a los colaboradores de una empresa sobre temas de ciberseguridad.

¿Cuáles son las principales amenazas de ciberseguridad que enfrentan las empresas hoy en día?

– Más del 80% de las amenazas está relacionada con el correo electrónico. El *phishing* (engañar al usuario para que realice alguna acción como abrir un archivo o hacer clic) es el mecanismo más usado por los atacantes, en donde el robo de datos y el *ransomware* (secuestro de información) son los ciberataques más recurrentes.

Además, factores como el avance tecnológico, el uso de la IA y la mayor cantidad de dispositivos conectados, generan que las amenazas sean más recurrentes y con consecuencias más devastadoras.

¿Cómo puede una empresa desarrollar e implementar una estrategia integral de ciberseguridad?

– El primer paso es hacer un diagnóstico; es necesario definir la ruta óptima para lograr una seguridad efectividad que resguarde la continuidad operativa. La recomendación es que el enfoque sea elevar su ciberresiliencia, pues permite a las organizaciones desarrollar una estrategia centrada en su ne-

LITORALPRESS

Fecha: 24-08-2024
Medio: La Tercera
Supl. : La Tercera - Pulso
Tipo: Noticia general
Título: Capacitación interna: la primera línea de defensa en ciberseguridad de las empresas

Pág. : 15
Cm2: 384,8
VPE: $ 3.827.923

Tiraje: 78.224
Lectoría: 253.149
Favorabilidad: Positiva

gocio, que además de estar mejor protegidas, fortalece los mecanismos para defender exhaustivamente los activos que son críticos para la continuidad de su negocio.

Para implementar un marco integral de ciberresiliencia, es crucial que el diagnóstico clarifique la condición actual de madurez de su ciberseguridad, e identifique los procesos críticos del negocio. Este diagnóstico permite elaborar una estrategia personalizada y dosificada en función de cada realidad.

A grandes rasgos, una estrategia efectiva debe incorporar un diagnóstico inicial; definición de políticas y procedimientos; implementación de controles y tecnologías de seguridad, y de herramientas de monitoreo y detección; capacitación de los colaboradores; y auditorías periódicas que permitan evaluar la efectividad de las medidas implementadas.

¿Cómo se pueden identificar y mitigar las vulnerabilidades dentro de la infraestructura tecnológica de una empresa?

- Este es un tema extremadamente crítico, pues es la variable clave para reducir la exposición a ataques cibernéticos. A pesar de esto, menos del 15% de las organizaciones toma acciones de forma continua para identificar y gestionar las vulnerabilidades.

Para eso, se utilizan métodos y tecnologías especializadas que permiten identificar vulnerabilidades en *software* y aplicaciones, además de verificar las configuraciones de seguridad. Adicionalmente, el aumento de desarrollos personalizados involucra a más del 50% de las organizaciones en proyectos de *software* propio. Considerando que el *software* personalizado puede ser una ventaja, debe tenerse claro que este puede ser extremadamente vulnerable y terminar siendo un perjuicio si no se implementa un proceso de desarrollo seguro. En este punto, lo importante es que el mecanismo debe ser dinámico y ágil.

¿Cuál es la importancia de la capacitación continua en ciberseguridad para los empleados de una empresa?

-En la misma línea de las vulnerabilidades, en un contexto en donde el 95% de los incidentes ocurre por falta de conocimiento, la capacitación es fundamental para que los colaboradores comprendan la importancia de su rol en la protección de la empresa, y que adquieran los conocimientos necesarios para reconocer posibles amenazas y minimizar las probabilidades de ser víctimas.

La vulnerabilidad en las personas solo puede remediarse con conocimiento y el ejercicio continuo de enfrentarse a situaciones de simulación de ataques.

Es crucial que las organizaciones, sin importar su tamaño o industria, comprendan que todos los colaboradores son clave en una estrategia efectiva de seguridad, porque son la puerta de entrada para los ataques como phishing.

¿Cuáles son los errores más comunes que cometen los empleados en temas de ciberseguridad y cómo pueden evitarse a través de la formación?

- Los errores más comunes son el uso de contraseñas débiles, clic en correos o links maliciosos, no actualizar los *software*, omitir o suspender el uso de antivirus, acceder a servicios críticos desde redes de wifi públicas, acceder a cuentas personales a través de dispositivos corporativos o viceversa, entre otros.

La formación en ciberseguridad proporciona los conocimientos adecuados para que los colaboradores conozcan los riesgos a los que se exponen ellos y su organización, y estar atentos a posibles ciberataques e incluso saber cómo actuar frente a uno.

¿Qué riesgos enfrentan las empresas que no priorizan la formación en ciberseguridad de su personal?

- El mayor riesgo es que la estrategia del negocio falle por desconocimiento de un tema que no está relacionado con el negocio. Me refiero a fallas provocadas involuntariamente en la tecnología que soporta la operación. Los atacantes se aprovechan de la buena intención y de la curiosidad de las personas para lograr sus objetivos de cometer robo, fraude, extorsión o incluso daños a la infraestructura. Sumado a ello, con las nuevas y próximas legislaciones en materia de ciberseguridad y protección de datos, las empresas se arriesgan a millonarias multas.

Las organizaciones necesitan que sus colaboradores participen activamente en el centro de su estrategia de ciberseguridad. No tener conocimientos sobre las prácticas de ciberseguridad las hace vulnerables a trampas como correos electrónicos de *phishing* o descargas de *software* malicioso.

¿Qué habilidades y conocimientos deben priorizarse en una capacitación de ciberseguridad efectiva?

- Lo primordial es que las personas estén conscientes de su papel en la ciberseguridad, es decir, posicionar la ciberseguridad como un tema crítico y explicar a los colaboradores cómo pueden contribuir individualmente debe ser primordial.

En términos generales, deben abordarse tres escenarios en donde las personas pueden ser vulneradas: primero, como individuos, es decir, deben conocer todo lo relacionado a los métodos que usan los atacantes, las condiciones de riesgo en las tecnologías que usan y su papel como garantes de esa individualidad. En segundo lugar, en el entorno colaborativo, en donde su exposición a *phishing*, ingeniería social y la responsabilidad asociada al resguardo de la privacidad e integridad de la información a la que tienen acceso y con la que trabajan. Y por último, en la interacción con el mundo exterior, cuando las personas conscientes y naturalmente separan los entornos de trabajo de los públicos o personales y pueden llegar a ser multiplicadores o embajadores de buenas prácticas.

En síntesis, el objetivo es lograr que la persona sea consciente de su rol y su responsabilidad como eslabón en la estrategia de ciberseguridad de la organización.