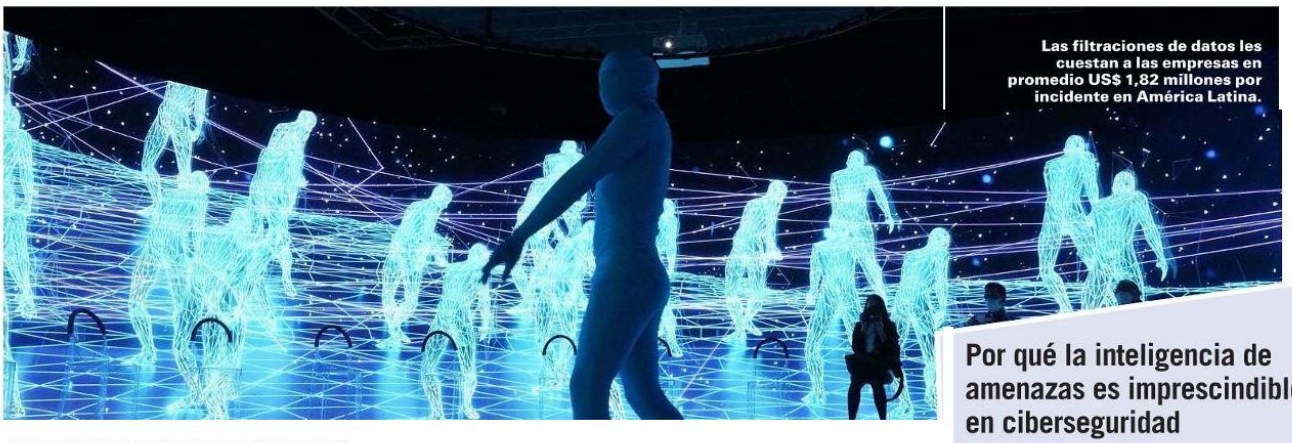
LITORALPRESS

Fecha: 23-06-2022
Medio: El Mercurio
Supl. : El Mercurio - Cuerpo B
Tipo: Ciencia y Tecnología
Título: Las acciones y prácticas de las empresas para fortalecer la ciberseguridad de los clientes

Pág. : 5
Cm2: 922,0
VPE: $ 12.111.569

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: Positiva



Las filtraciones de datos les cuestan a las empresas en promedio US$ 1,82 millones por incidente en América Latina.

ANTE MAYORES VULNERACIONES:

Las acciones y prácticas de las empresas para fortalecer la ciberseguridad de los clientes

Desde robustecer las claves mediante formatos alfanuméricos hasta fomentar la cultura preventiva son las iniciativas que llevan a cabo las firmas con el fin de dar mayor seguridad a sus usuarios.

Al adaptarse a la pandemia, las empresas debieron acelerar, rediseñar y ampliar sus entornos digitales, sentando como un imperativo la convivencia con las tecnologías con el fin de mejorar la visibilidad de su seguridad y la preparación para responder ante las amenazas en sus entornos de nube híbrida.

Pese a estos avances, uno de los flancos que quedaron al descubierto en materia de seguridad son los clientes, factor de riesgo y uno de los principales grupos vulnerables por los cuales los cibercriminales interceptan las redes. Ante este escenario, diversas son las acciones y prácticas que ponen en marcha las empresas con el fin de robustecer la ciberseguridad de cara a sus usuarios, ya sea a través de claves alfanuméricas hasta el trabajo que fomenta constantemente la cultura preventiva por parte de estos.

MEJORAS INTERNAS

Ricardo Seguel, director del Magister en Ciberseguridad de Ingeniería de la Universidad Adolfo Ibáñez, explica que las principales iniciativas que actualmente llevan a cabo las firmas son "las campañas de sensibilización sobre el uso de claves robustas (de más de 8 caracteres que combinen mayúsculas, minúsculas y números) y los peligros de los ataques de *phishing*, en los cuales los clientes, por error u omisión, son engañados para descargar y ejecutar un archivo adjunto con contenido malicioso, o para hacer clic en un *link* y acceder a sitios que lucen confiables, ingresar datos o claves, sin darse cuenta de que al hacerlo están descargando o instalando *malware* en sus dispositivos que pueden pasar desapercibidos por un antivirus", detalla Seguel.

Cyril Deleare, gerente de la Unidad de Ciberseguridad de Entel Ocean, comenta que otro factor relevante en este cometido es contar con las tecnologías adecuadas que eviten este tipo de ataques.

"Por ejemplo, invertir en ciertos sistemas y dispositivos, dependiendo de las necesidades de la compañía, permitiría identificar *insiders* maliciosos o eventuales amenazas que están esperando la oportunidad para atacar. Otro consejo relevante es mantener las actualizaciones de redes y sitios web al día", acota Deleare.

Por su parte, Diego Macor, gerente de Ciberseguridad de IBM Sudamérica, agrega a lo anterior la implementación de modelos de confianza cero en las empresas. "Estas conexiones pueden ser de los empleados, socios, clientes, contratistas u otros usuarios. Lo anterior se hace necesario porque vivimos cada vez más en un mundo sin fronteras donde la interconexión está presente en nuestra vida diaria principalmente por la nube, pero conforme el espacio entre nosotros y el resto del mundo disminuye, también lo hace nuestra distancia de los cibercriminales", detalla el ejecutivo.

Según el Cost of a Data Breach Report 2021, realizado por el Ponemon Institute e IBM Security, las filtraciones de datos les cuestan a las empresas en promedio US$ 1,82 millones por incidente en América Latina, un 30% más que el informe anterior. Esto se debe principalmente a los cambios operativos drásticos que tuvieron lugar durante la pandemia y a la complejidad tecnológica de las organizaciones que agravaron los desafíos en materia de seguridad.

Sin embargo, estas repercusiones no solo se limitan a costos económicos, sino que también están visadas por las normativas que regulan las responsabilidades de las firmas ante incidentes que vulneren los datos y/o privacidad de las personas.

En el caso de Chile, la Ley de Protección de Datos Personales aún no opera, y la normativa de delitos informáticos –a juicio de los expertos– es muy débil para perseguir a los ciberdelincuentes y bandas de cibercrimen.

MAYOR CONCIENCIA

No obstante, desde 2017 a la fecha, gracias a la Política Nacional de Ciberseguridad (PNCS), las organizaciones chilenas han tomado mayor conciencia respecto a esta temática.

De hecho, algunos sectores se han visto forzados a hacerlo a partir de experiencias críticas, como los ataques a la banca en 2018 y 2020, y las mismas regulaciones internacionales que los auditan.

También, se han creado nuevos roles en organismos públicos que tienen la responsabilidad de regular, auditar, fiscalizar y sancionar cuando corresponda, trabajo que ha sido coordinado por la División de Redes y Seguridad Informática del Ministerio del Interior. Esta División tiene dentro de sus áreas y funciones al CSIRT de Gobierno, que por un lado se encarga de la seguridad del Estado y por otro se hace cargo de estos roles en el sector privado.

"No hay solo una tecnología para prevenir fraudes en el ciberespacio, es una combinación de tecnologías, procesos y procedimientos que deben ser definidos y llevados a la práctica, y las acciones de sensibilización y educación de clientes y colaboradores, que incluso trascienda a sus hogares y familias", finaliza Seguel.

INICIATIVAS Y ALIANZAS LOCALES

Ante las mayores vulnerabilidades, hoy las empresas han debido reforzar sus sistemas, consultando a expertos y gestionando alianzas que vayan en esta línea con el fin de entregar y contar con servicios más seguros en un ecosistema altamente amenazado.

Por ejemplo, Entel Ocean, la unidad digital de IoT, Cloud y Ciberseguridad de Entel está trabajando con IBM para extender las capacidades de su Centro de Operaciones de Ciberseguridad (SOC) a través de la integración de IBM QRadar SIEM, permitiéndole al equipo de especialistas avanzar rápidamente en la investigación de amenazas, el monitoreo proactivo, el análisis y la respuesta avanzada ante ciberataques. Asimismo, automatizar, orquestar y colaborar entre herramientas y equipos, lo que les permite reforzar la ciberseguridad y entregar más valor a sus clientes.

También implementaron IBM Cloud Pak for Security como la moderna plataforma de seguridad de su SOC, con el objetivo de mantener la continuidad del negocio de sus clientes corporativos.

Diego Macor, gerente de Ciberseguridad de IBM Sudamérica, comenta que a medida que las organizaciones modernizan su infraestructura digital a través de la nube híbrida para alcanzar mayores niveles de agilidad y velocidad, es esencial que también modernicen su seguridad. "Confiar plenamente en herramientas de seguridad anticuadas o estrategias de seguridad caducadas aumenta la complejidad de la ciberseguridad. Entre más compleja sea la arquitectura de la seguridad, más cantidad de 'puntos ciegos' habrá para los equipos de seguridad", detalla Macor.

Por qué la inteligencia de amenazas es imprescindible en ciberseguridad

Latinoamérica recibió 289 mil millones de intentos de ataques informáticos en 2021, con un ranking encabezado por phishing, malware y ransomware. Vemos que los ataques son cada vez más sofisticados en los mecanismos utilizados para detectar y atacar objetivos, y son más eficientes en tamaño, velocidad, impacto y efectividad.

PÍA SALAS, COUNTRY MANAGER DE FORTINET CHILE

Además, últimamente los ciberdelincuentes están apelando cada vez más al uso de inteligencia artificial para realizar ataques dirigidos más efectivos. La inteligencia artificial permite a los atacantes realizar un mayor número de tareas de forma automática y tomar decisiones en tiempo real para ajustar las amenazas, evadir las defensas y aprender tanto de errores como de aciertos.

Frente a este panorama dinámico y complejo, cuyos datos surgen de la organización de investigación e inteligencia de amenazas de Fortinet, FortiGuard Labs, toma relevancia el concepto de "Inteligencia de Amenazas".

Para que esta tarea sea exitosa es necesario cumplir con cuatro requisitos clave:

1. Procesos adecuados y maduros que permitan la adquisición amplia pero también el procesamiento ágil y certero de la información recabada. La capacidad de intercambiar información en organizaciones de la industria también resulta relevante.

2. Personas calificadas con entrenamiento adecuado que se mantengan actualizadas con el dinamismo que exige la velocidad con la que nuevos modelos de ataque aparecen a nivel local, pero también con la conciencia del impacto al negocio y a la sociedad.

3. Tecnologías correctas e innovadoras como Sandboxing para descubrir códigos maliciosos desconocidos hasta ese momento (ataques día cero), integradas con herramientas de análisis para correlacionamiento (SIEM) y respuesta orquestada (SOAR) que permitan operaciones de ciberseguridad realmente integradas, automatizadas e impulsadas por Inteligencia Artificial.

4. Base instalada de amplia envergadura para obtener una muestra importante dentro del universo de ataques. En este sentido, Fortinet es la compañía con la mayor cantidad de dispositivos de seguridad instalados en América Latina, con el 53%, según la consultora IDC. Esto implica que más de la mitad del equipamiento de ciberseguridad en las redes corporativas de la región es Fortinet, lo cual entrega capilaridad y músculo mayores que cualquier otra infraestructura de adquisición de datos. La ciberseguridad ha pasado de ser competencia exclusiva de las áreas tecnológicas, para ser relevante en las áreas de negocio debido a su posibilidad de acelerarlo y mitigar riesgos. La ciberseguridad impacta en los tiempos de respuesta y capacidades de atención, las posibilidades de aprovechar analítica y movilidad, así como la percepción de confiabilidad de un negocio hacia sus clientes. En este contexto, la Inteligencia de Amenazas proporciona alertas en tiempo real sobre amenazas y cambios en los riesgos, brindándoles a las organizaciones las herramientas que necesitan para estar lo más protegidas posible.