ESCRIBEN: Javier Oliva Posada • Sergio Sarmiento • Víctor Sánchez Baños • Guillermo Fárber • Mónica Soto • Claudia Ivett García • Sergio Pérezgrovas • Juan Pablo Delgado • Guillermo Deloya • Magú

VÉRTIGO

URGE REFORMA ELECTORAL

Consenso entre sociedad, gobierno y partidos por la libertad de expresión y acabar con el financiamiento multimillonario

Año XXI No. 1063 | 1 de agosto de 2021 | www.vertigopolitico.com | $45.00 pesos

EXHIBIR HASTA AGOSTO 29, 2021

0 74283 2 161558 01063

CIBERSEGURIDAD, CLAVE PARA NUEVOS MODELOS DE TRABAJO EN LAS EMPRESAS

Arturo Moncada
amoncadal@revistavertigo.com

Data Warden

Navarro | Soluciones tecnológicas.

Las Tecnologías de la Información y la Comunicación (TIC) incluyen aquellos medios electrónicos que almacenan, crean, recuperan y transmiten información en grandes cantidades y a gran velocidad: su permeabilidad en prácticamente todas las áreas de la sociedad se convierte en un factor de desarrollo para gobiernos, industrias, etcétera.

Dada su importancia, desde hace unas cuatro décadas las TIC trajeron consigo primero la introducción de la seguridad informática con el objetivo de proteger los sistemas tecnológicos que se utilizan; y, posteriormente, ante la vorágine del avance de internet hace unos 17 años, para proteger datos tanto personales como de entidades de gobierno y privadas.

Es de este modelo que se desprende el término ciberseguridad, ya que actualmente el objetivo se extendió no solo a proteger la información sino también a resguardar la infraestructura tecnológica que la soporta y nos hace funcionar como sociedad.

Ciberdelincuencia

Para tratar la importancia de la ciberseguridad ante el actual aumento de la ciberdelincuencia *Vértigo* entrevistó a Jesús Navarro Dorantes, director general de Data Warden.

—Diversos estudios indican que ante la actual pandemia los ataques cibernéticos aumentaron en cantidad y calidad. ¿Cómo afecta a las empresas?

—Efectivamente, derivado del tema de la pandemia hubo un crecimiento exponencial en el aumento del teletrabajo de manera forzada. Por un lado, muchos empleados tuvieron que trasladar su trabajo de forma remota; y, por otro, hubo un crecimiento muy fuerte en el paso de la capacidad de cómputo de las empresas desde métodos tradicionales hacia ambientes en la nube.

Estos cambios, puntualiza Navarro, "marcaron un crecimiento de riesgos en términos tecnológicos para las

compañías. Ante ello se debe hacer un autoestudio o diagnóstico para evaluar qué tanto se modificó la superficie de riesgo que tiene un negocio previo a la pandemia, contra lo que existe ahora en la pandemia y realizar un plan estratégico de seguridad que nos permita tener controlados los riesgos actuales".

Por otra parte, "se debe elevar el nivel de conectividad con el trabajo remoto, porque la importancia del cuidado de las redes y datos cobra mayor relevancia en la operación. Y aunque los presupuestos se han visto castigados se recomienda no reducir la adopción y mantenimiento de sistemas que permitan tener una operación cibersegura".

—En este contexto ¿qué opina sobre un gran número de empresas que consideran la ciberseguridad como un gasto y no como una inversión?

—Históricamente la ciberseguridad se ha visto como una carga operativa, como un gasto para la empresa. Desgraciadamente con la pandemia muchos negocios se vieron mermados y se puso en riesgo la continuidad de varias industrias que lo primero que hacen es recortar este tipo de gastos. En México no se observa todavía una necesidad real de adoptar una postura de ciberseguridad porque no se tiene una conciencia real de que esto es un tema serio y se sigue pensando que un ataque cibernético no le ocurrirá a la empresa. Por ende, es necesario un cambio de conciencia, de paradigma: la ciberseguridad es algo indispensable para un negocio y no un gasto superfluo. Es una pieza estratégica para el negocio en cuanto a mejoras en su servicio y mejoras en la confianza para los clientes. La empresa cumple así con las normas y prácticas de seguridad a nivel mundial.

—¿Hace falta una mayor capacitación al personal de una empresa?

—En todos los casos de temas de ciberseguridad el eslabón más débil es el usuario final. En este caso puede ser un colaborador o una persona que utilice los servicios. Entonces la clave es educar y concientizar al empleado de manera constante; hacerle ver a los colaboradores, por ejemplo, que un área de ciberseguridad no es para estar monitoreándolos o cuidándolos: es para proteger los activos de información de la compañía, para garantizar que se les dé un uso óptimo y para que se logre el mejor resultado para la compañía. Que en caso de que se registre una desviación de los sistemas o los recursos, la ciberseguridad funcione.

—Según datos sobre ciberdelincuencia la mayoría de daños o fraudes contra una empresa se realizan desde dentro de la compañía. ¿Qué puede decirnos al respecto?

—Esa es una situación real a nivel global y no solo de México. Realmente arriba de 60% de los incidentes cibernéticos —ya sean fraudes, ataques, fallas de servicio, etcétera— se ejecutan en general por usuarios internos, ya sea por un descuido, un empleado mal intencionado o alguien con un acceso más allá del que le era permitido. Es algo muy común y la gran mayoría son errores o descuidos de configuración.

> "La ciberseguridad es algo indispensable para un negocio y no un gasto superfluo".

Entonces "con más razón existe la necesidad de educar y concientizar a los usuarios en todo momento. Para evitar ese riesgo se debe tener una política de confianza cero, asegurarse de que los privilegios que se le asignan a un usuario para el acceso a los sistemas sean los mínimos necesarios que realmente requiere para ejercer su función en el negocio y esta medida aplicarla a todas las capas".

—¿Qué tipo de servicio debe ofrecer un sistema de ciberseguridad a las empresas?

—El primero es *Consultoría*. En esta línea se ayuda al cliente a tener una idea de dónde se encuentra en términos de riesgos tecnológicos, ya sea mediante un análisis de riesgo o un análisis de vulnerabilidades, de penetración, etcétera. Inclusive se realizan algunos servicios recurrentes de toma de decisiones, como puede ser un servicio de patrullaje de tipo cibernético para revisar y asegurar que la marca del negocio no se utilice para fines no adecuados o no ligados al negocio.

El segundo, explica, es el de "*Arquitectura tecnológica e implementación*. En esto lo que se hace es diseñar e implementar controles ya sea con tecnología para apoyar a las empresas a impedir riesgos en sus servicios, en sus sistemas, o para obtener mejor control de los algoritmos de su información, que se vuelvan más ágiles y más eficientes en el seguimiento de su plan de ciberseguridad. Esto tiene que ver mucho en soluciones tecnológicas con base en hardware, en software o en suscripciones en la nube".

Finalmente, "una tercera línea debe encargarse de dar *Servicios administrados* en temas de seguridad de automatización, detección y respuesta gestionada (MDR), gestión de amenazas y gestión de vulnerabilidades, con la misma visión de proveer a los clientes herramientas de identificación y reacción".

Ventajas de la ciberseguridad

- Habilita nuevas líneas de negocio de manera segura.
- Reduce la superficie de riesgo tecnológico del negocio.
- Minimiza el impacto de amenazas cibernéticas.
- Reduce el tiempo de detección y reacción ante amenazas.
- Permite contar con apoyo técnico especializado y certificado.
- Optimiza el retorno de inversiones en seguridad (ROSI).
- Contribuye a mantener una operación consistente, resiliente y confiable.

Fuente: Data Warden