Ciberseguridad, un desafío para cualquier empresa

- El trabajo en casa llegó para quedarse, y el intercambio de información desde los dispositivos para el *home office* ha obligado a que las empresas pongan atención especial en la ciberseguridad.
- Una solución a la medida pemite detectar vulnerabilidades, resolverlas y capacitar a la organización para evitarlas en el futuro; garantizando así la continuidad de la operación y reduciendo el riesgo de pérdidas.

Ciudad de México, 24 de marzo de 2021.- La **ciberseguridad** es un concepto que, aunque a veces parece lejano a nuestra vida diaria, las empresas de cualquier tamaño deben considerar al momento de plantear su estrategia de negocio y la seguridad de su información.

En el sentido amplio, la ciberseguridad implica la protección de los sistemas y redes informáticos. **Víctor Santos, especialista en Innovación y Diseño de soluciones en ciberseguridad de *Ácumen Telecomunicaciones,*** una de las empresas especializadas en soluciones integrales de ciberseguridad en México que tiene comos socios a especialistas en tecnología*,* comenta que *"el uso de herramientas y procedimientos para protegerse de cualquier tipo de ataque, amenaza o vulnerabilidad en cuanto a algún equipo o dispositivo conectado a una red de información, puede considerarse como ciberseguridad".*

¿Por qué es importante que las empresas pongan especial atención a la ciberseguridad de su información?

Dado que cada vez más personas están haciendo trabajo desde casa, los ciberataques se han vuelto más frecuentes y sofisticados; van desde los virus alojados en documentos hasta procesos de ingeniería social que buscan retener información confidencial o altamente sensible sobre los negocios y afectar no sólo de manera virtual su operación.

Las vulnerabilidades en la información de una empresa pueden afectar su reputación, pero también equivaler a multas millonarias dependiendo del ramo de la compañía, por ejemplo, si ésta se dedica a almacenar datos personales sensibles de sus clientes.

Santos comenta que los ataques pueden ser perfilados a ciertos tipos de dispositivos y de personas. Los ataques a la ciberseguridad pueden ir desde extraer un número telefónico confidencial para realizar extorsiones, hasta el robo y secuestro de información corporativa e industrial.

La aceleración del nuevo modelo de trabajo a distancia a raíz de la pandemia de COVID-19 ha promovido un **aumento en los ciberataques alrededor del mundo**. Por ejemplo,

en junio de 2020 Fortinet indicó[1] que 9 de cada 10 organizaciones reportaron al menos una intrusión en sus sistemas tecnológicos durante el año, un incremento del 19% respecto a 2019. Y parece que eso sólo era el principio.

Un smartphone, una bocina inteligente y hasta una impresora pueden ser el punto de entrada para un ataque cibernético

De acuerdo a Víctor Santos, **ningún dispositivo está exento de ser blanco de un ataque**; se han reportado casos que se intervienen teléfonos, conexiones a sistemas de sonido o bocinas con asistentes virtuales, y hasta por medio de impresoras que están conectadas a redes abiertas, que permiten el intercambio continuo de información dentro y fuera de las mismas.

"En cuanto a los dispositivos y gadgets, los conectamos a internet en cualquier red, pero no nos imaginamos qué es lo que está pasando detrás de esas comunicaciones.", comenta el especialista de Ácumen Telecomunicaciones.

Es por ello que cualquier empresa que tenga un equipo celular o de cómputo debe estar interesada en la ciberseguridad, ya sea en sus instalaciones, sus diferentes espacios de trabajo en campo o en la casa de sus colaboradores.

Seguridad de la información como medida preventiva en las empresas

En la medida que las empresas y organizaciones protegen su información, su operación se vuelve más segura y se eliminan factores de riesgo asociados a la tecnología.

Y, aunque existen muchas prácticas y métodos, se debe tener una visión de 360 grados para prevenir los ataques y no esperar a resolverlos una vez que han sucedido. Al respecto, **Julio Olivares, Director en Innovación y Diseño de soluciones**, comenta que en ***Ácumen Telecomunicaciones*** trabajan con un enfoque en 4 grandes etapas:

1. **Diagnóstico.** En dónde se realiza la auditoria y pruebas en redes, servidores, aplicaciones, y hasta en los procesos existentes en materia de seguridad de la información, así como los usuarios asociados a la empresa; con la finalidad de detectar los puntos débiles.
2. **Remediación**. Una consultoría para ayudar a cubrir las necesidades del cliente con las soluciones más adecuadas para mantener su operación.
3. **Educación**. Para que los empleados esten mas concientes y aprendan a detectar vulnerabilidades en su operación sobre aplicaciones, sus redes y comunicaciones, reduciendo los riesgos para la empresa y ayudándolos a obtener las certificaciones necesarias para cumplir las normas oficiales.

[1]https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-state-of-operational-technology.pdf

4. **Monitoreo**. se mantiene como una medida preventiva y de seguimiento para evitar ataques, identificar y mitigar futuras vulnerabilidades.

Pero no todas las medidas son idénticas para todas las empresas, es por ello que el equipo de ***Ácumen Telecomunicaciones*** trabaja desde hace más de 10 años diseñando **soluciones de seguridad informática y ciberseguridad a la medida** que responden a las necesidades de cada organización, tomando en cuenta su modelo de negocio, plantilla de trabajo y tecnología, garantizando la seguridad de la información.

Para conocer más sobre Ácumen Telecomunicaciones y sus soluciones integradas de ciberseguridad a la medida visite www.Acumen.mx

KRISTINA VELFU
contacto@kristinavelfu.com
5532000727