La ciberseguridad y el *home office*: *tips* para proteger tu empresa, desde casa

- **Los ciberataques en Latam crecieron un 24% durante los primeros ocho meses de 2021, según el informe Panorama de Amenazas en América Latina 2021.**

México, 28 de octubre de 2021.- El mundo empresarial y las dinámicas de trabajo han cambiado debido a la modalidad *online.* El teletrabajo y el *home office,* son realidades que han demostrado tener muchas ventajas, como la comodidad y el aumento de la productividad; pero todas las monedas tienen dos lados, y en este caso lo negativo (y a veces riesgoso) de estar en casa utilizando varios dispositivos para trabajar, es la exposición a la delincuencia cibernética, que está más que lista para el robo y mal uso de datos e información, convirtiéndose en un desafío importante en una era de mayor conexión.

another, agencia regional independiente de comunicación estratégica, ha vivido como la mayoría de las empresas, la necesidad de aplicar la virtualidad tras el inicio de la pandemia y comparte algunos datos y recomendaciones para quienes aún no le han dado la debida importancia a la seguridad *online* ahora que muchos siguen en sus casas.

A manera de referencia, tan sólo en México, en febrero de 2021 se registraron 15 millones de ataques de este tipo; mientras que Latam, en materia de seguridad informática, cuenta con estadísticas recientes de ciberseguridad dentro del informe Panorama de Amenazas en América Latina 2021, el cual reveló que **los ciberataques en la región crecieron un 24% durante los primeros ocho meses de 2021**. Justamente el *home office* y la piratería son los principales vectores de ataque, tanto para consumidores como para empresas. Las principales amenazas que acechan a la **región generan un promedio de 35 ataques por segundo, por ejemplo, la estafa *online* o la vulneración de datos.**

Otro dato curioso que reveló este reporte es que los ataques de *phishing* (mensajes fraudulentos) han disminuido. Sin embargo, varios países de la región se encuentran entre los más atacados del mundo. Considerando la proporción de usuarios atacados durante los primeros ocho meses del año, Brasil figura en el primer lugar con 15,37% de usuarios que registraron algún intento de ataque. Le siguen Ecuador (13,36%), Panamá (12,60%), Chile (11,90% y Colombia (11,09%).

Un dato importante para las empresas y su vulnerabilidad informática, es que a nivel corporativo, el reporte ESET Security Report LATAM 2020, mostró que un **60% de las empresas en Latam sufrieron al menos un incidente de seguridad** durante el 2019. La infección con códigos maliciosos también conserva su lugar, siendo el incidente más recurrente: **1 de cada 3 empresas sufrió una infección con algún código malicioso**, incluyendo ransomware.

Otro aspecto interesante que señaló el Panorama de Amenazas para América Latina fue el número de **ataques contra dispositivos móviles**. Según el informe, más de 173 mil intentos de infección a dispositivos móviles fueron registrados en la región entre enero y agosto de este año- un promedio de **casi 20 ataques por hora**. La principal amenaza son los programas de

adware que tienen como objetivo generar ganancias mostrando anuncios no deseados a sus víctimas.

Carla Mucharraz, directora de Talento Humano en **another** resalta que: *"el problema no sólo radica en el número de ataques, sino también en que hay que contar con medidas efectivas para proteger la seguridad de nuestros datos; si no lo hacemos, podríamos comprometer no sólo nuestra información, sino también la de nuestros clientes y usuarios".*

La estabilidad informática de una empresa, independientemente de su tamaño, es fundamental para adaptarse mejor a los procesos remotos de operación y cada una enfrenta este desafío de una manera diferente. Sin embargo, en general hay tres elementos destacables que **another** comparte, para establecer un buen plan de protección de datos:

- Clasificación de la información de la empresa.
- Plan de respuesta y continuidad del negocio en caso de ataques.
- Políticas de seguridad para proteger la base de datos.

Entonces… ¿Cómo protegerse?

Frente al escenario que enfrentan las empresas, como ***another,*** que han adoptado modelos híbridos de trabajo, es necesario contar con soluciones que permitan el uso de todas las herramientas sin perder seguridad, pero también a las que se pueda acceder desde, donde y cuando sea. Para ésto, la nube puede ser una alternativa gracias a su flexibilidad y escalabilidad, factores que dan mayor garantía para la protección de datos.

Ahora que estamos llegando a un periodo de cierta "normalidad", las estrategias mixtas de seguridad empresarial se concentrarán en la definición de perímetros de protección mucho más reducidos, enfocados en situaciones esenciales para una empresa, como las bases de datos, gestión de ventas, entre otros. Todo esto con la finalidad de blindar de manera más sólida el acceso a los sistemas desde cualquier lugar de conexión.

"Se sabe que, desde hace muchos años, ya no basta tener un antivirus para protegernos. Hoy, la tecnología ha avanzado a través de implementación de análisis de datos, machine learning *e inteligencia artificial para cubrir las necesidades de seguridad y combatir a los ciberdelincuentes con las mismas herramientas tecnológicas; de esta manera, podremos detectar, de manera oportuna, los comportamientos anormales en un sistema"*, comenta Mucharraz.

Para los que siguen trabajando desde casa o remotamente, another comparte estos tips para evitar a los ladrones digitales:

- **Evitar -y aconsejar evitar- el uso de redes públicas o inseguras para la conexión.**
- **Definir a los usuarios los protocolos para reportar cualquier situación anómala o sospechosa.**
- **Siempre, SIEMPRE tener un *backup* de la información importante.**
- **Asegurarse de que los equipos personales tengan cifrado de disco y validar los controles de prevención de fuga de información.**

- **Validar las capacidades de borrado y bloqueo remoto en los equipos, así como los controles remotos (actualizaciones, antivirus, etc.).**
- **Utilizar servicios remotos por protocolos seguros (HTTPS).**

Estos datos reflejan la importancia de un problema que crece a nivel regional y global. La única manera de reducir el riesgo de estos ataques es que las empresas se ocupen tomando las medidas de seguridad necesarias para evitarlos y así proteger la información y datos de la empresa y sus clientes.