**Ciberseguridad y 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**

El mundo empresarial y las dinámicas de trabajo cambiaron de la mano de 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 caras. En este caso, el punto 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 esta era de mayor conexión.

Estadísticas recientes de ciberseguridad del informe [Panorama de Amenazas en América Latina 2021](https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/) revelaron que los ciberataques en Latam crecieron un 24% durante los primeros ocho meses del año, **mientras que en Chile el alza fue del 19%**, siendo el home office y la piratería los principales vectores de ataque, tanto para consumidores como para empresas. Las principales amenazas que acechan a la **región, como la estafa online o la vulneración de datos, generan un promedio de 35 ataques por segundo.**

Otro dato curioso que reveló este reporte es que los ataques de *phishing* (mensajes fraudulentos) han disminuido. Sin embargo, Chile figura con un 11,9% de usuarios que registraron algún intento de ataque durante los primeros ocho meses del año.

Así mismo, el informe indica que entre enero y agosto de este año se registraron más de 173 mil intentos de infección a dispositivos móviles en Latam. Esto significa un promedio de **casi 20 ataques por hora**, siendo la principal amenaza los programas de adware que tienen como objetivo generar ganancias mostrando anuncios no deseados a sus víctimas.

**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. En este contexto, 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.

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 esto, 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.

*“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 oportunamente 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.