¿Qué riesgos cibernéticos enfrentan las empresas?

Cada vez más las empresas están destinando más inversión en ciberseguridad ante el incremento de ataques. El aumento se ha dado sobre todo durante esta pandemia, no solo para reducir los riesgos de robos, sabotajes y defraudaciones, etc, sino para la detección de delitos cibernéticos.

La mayoría de los riesgos cibernéticos para las empresas están ligados a casos de phishing, que se distribuyen a través del correo electrónico, y ransomware, ataque a través del cual los ciberdelincuentes secuestran información de la empresa para luego pedir un rescate en efectivo o Bitcoins.

El gerente general de ESET Perú, Jorge Zeballos, destacó que en el 2020, en el Perú se dio el 20% de los ataques de ransomware de toda la región. Según la herramienta ESET Virus Radar, nuestro país registró el mayor nivel de infección con 11,69%.

“Estos resultados nos alertan sobre la situación vulnerable en que vivimos y nos motivan a concientizar a las empresas y usuarios sobre la importancia de la ciberseguridad y el uso de las herramientas de prevención”, aseveró Zeballos.

Phishing

Cabe señalar que, durante los meses de cuarentena, de mayo a julio 2020, se observó un incremento en la actividad de phishing, con casi 2.500 detecciones diarias. En los primeros meses del año los registros oscilaban en alrededor de 2.000.

“En un ataque ransomware, el costo es difícil de calcular, porque esta en función de cuanto daño podría producir la publicación de dicha información secuestrada. Ello implica no solo las multas por infringir las normas de protección de datos personales, que pueden ser sumas de hasta S/ 540.000, sino hasta la pérdida de reputación y cierre de la compañía”, detalló Zeballos.

Controles de seguridad

Según el reciente ESET Security Report (2020), los principales controles de seguridad implementados en las empresas son las soluciones antimalware (86%), firewalls (75%), soluciones de respaldo de información (68%), y el uso de soluciones de doble factor de autenticación (22%).

Por ello, Zeballos aseguró que las empresas también deberían implementar soluciones de seguridad en smartphones o tablets, sobre todo porque en el teletrabajo estos son muy utilizados para actividades laborales y personales, y pueden ser la puerta de entrada a la información sensible de la empresa.

Inversión

Asimismo, **Zeballos refirió que la mayor inversión en ciberseguridad ha sido para hardware, donde muchas empresas han privilegiado la adquisición de equipos portátiles para sus empleados con la intención de controlarlos mejor.**

“También han invertido en sistemas de autenticación (claves de una sola vez), sistemas de prevención de fuga de datos y medición de uso/ acceso a los sistemas, y licenciamiento de software de seguridad para las computadoras destinadas al home office. Estas ‘nuevas’ inversiones han requerido que la seguridad de la información y acceso a sistemas claves sea incrementado en un promedio de 30%”, indica.