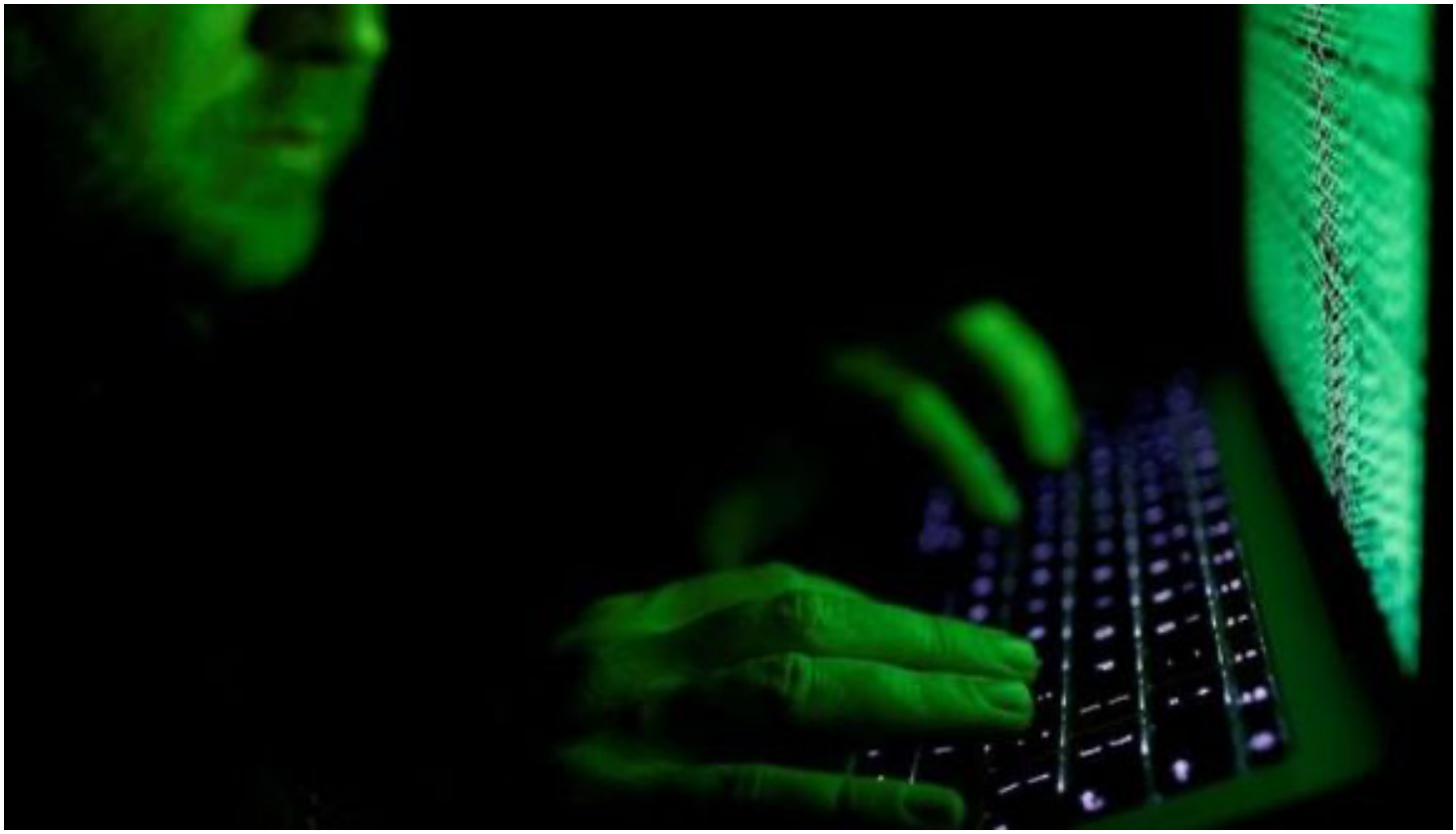
TECNOLOGÍA

Lo que están haciendo las empresas peruanas para evitar ser víctimas de ciberataques

Las empresas que se encuentran operando mediante el teletrabajo se encuentran más vulnerables a los ciberataques, por lo que deben mejorar sus prácticas de seguridad, señala Elder Cama, de EY Perú.



Los ciberataques que más afectan a las empresas tienen por objetivo la suplantación de identidad o el secuestro de información. (Foto: Reuters)

Actualizado el 21/08/2020 a las 05:53
Selene Rosales
selene.rosales@diariogestion.com.pe

Con el auge del teletrabajo, la empresas se encuentran en una situación de mayor vulnerabilidad ante los ataques cibernéticos, pues su información es almacenada en los equipos domésticos y poco protegidos de los trabajadores, desde donde circula hacia distintos puntos de la red. ¿Qué pueden hacer entonces las empresas frente a la nueva fuerza que cobran estas amenazas?

En general, los usuarios del Perú sufrieron más de 613 millones de intentos de ciberataques entre enero y junio del presente año, según la plataforma Threat Intelligence Insider Latin America de Fortinet, una herramienta que recopila y analiza este tipo de incidentes a nivel mundial.

Elder Cama, socio de consultoría en ciberseguridad de EY Perú, señala que si bien estos ataques son generalizados, el aumento del teletrabajo le ha facilitado a los ciberdelincuentes acceder a información de las empresas por medio de la vulneración de las computadoras de sus trabajadores.

“Lo que incrementa estos sucesos es la obligatoriedad del trabajo remoto. Cuando estabas en tu oficina, llegabas al centro de trabajo, te conectabas a la red de tu organización y, pensando en el promedio de empresas, estabas en un

entorno que podíamos llamar seguro. Allí las posibilidades de que accedan a tu información eran mucho menores. Pero ahora estás en tu casa, usando la computadora del hogar o tu laptop, que no está protegida por los mismos sistemas de seguridad", explicó a Gestion.pe.

Los principales ataques sufridos por las empresas en el Perú tienen por objetivo **la suplantación identidad -o phishing- y el secuestro de información.** En el primer caso, los ciberdelincuentes pueden acceder a las cuentas personales de uno de los trabajadores y obtener suficiente información para hacerse pasar por él, por medios virtuales, frente a su jefe u otro miembro de la organización, con el fin de concretar una estafa. Cuando se trata del secuestro de información, el atacante puede exigirle a la empresa el pago de cierta suma de dinero para devolvérsela o puede comercializar con terceros información que quizás sea confidencial.

Muchas veces estos ataques se dan a través de correos electrónicos engañosos, en los que el trabajador "cae" si se encuentra desprevenido, pero también pueden ocurrir por haber descargado una aplicación de origen dudoso que resultara ser fácilmente vulnerable.

Ante estos sucesos, estas son **las principales prácticas que están adoptando las empresas del país,** y que son recomendables, señala Cama:

- Optimizar el uso del antivirus: es necesario garantizar que las computadoras utilizadas por los trabajadores cuenten con un adecuado antivirus y evitar prácticas irresponsables, como desactivar su uso para acceder a ciertas páginas web o incrementar la rapidez de descarga.

- Adquirir nuevo software de seguridad: muchas compañías están recurriendo a distintos programas que permiten poner su información a buen resguardo. Por ejemplo, señala el especialista, algunos programas permiten que la información de una compañía compartida entre los trabajadores solo sea visible durante una cantidad determinada de horas; luego de ello esta se encripta de forma automática.

- Optimizar el hardware: los equipos antiguos pueden ser más vulnerables a ciertos ataques porque a veces no soportan nuevos sistemas de seguridad o su actualización.

- Concientizar a los trabajadores: Elder Cama destaca que se trata del punto más importante, puesto que muchos de los ataques se producen por prácticas irresponsables. En ese sentido, desaconseja compartir las contraseñas -así sea entre miembros de una misma organización- y no utilizar para el trabajo el mismo equipo que usa el resto de la familia para otros fines. Algunas compañías están recurriendo a consultores especializados para que los trabajadores tomen conciencia de las mejores prácticas.

"Como vemos, a veces la inversión adicional para mejorar la ciberseguridad de una empresa es cero, porque solo se trata de utilizar mejor los recursos que ya se tienen, pero en otras ocasiones sí se debe hacer un desembolso", comentó el especialista.

Ciberseguridad en la banca

Esta semana, la Superintendencia de Banca, Seguros y AFP (SBS) publicó un proyecto de reglamento para la gestión de seguridad de la información y ciberseguridad, que complementa al reglamento para la gestión del riesgo operacional y actualiza los requisitos exigidos en dicha materia a entidades financieras y otras vinculadas.

Al respecto, María Del Pilar Sánchez, asociada senior del estudio Rebaza, Alcázar De Las Casas, explicó que esta norma principalmente está beneficiando a los clientes de las entidades financieras, al exigirles a estas optimizar sus sistemas de ciberseguridad ante el evidente incremento de los servicios digitales durante la pandemia.

"Se está protegiendo todas las transacciones que los clientes hagan por medios digitales. Por ejemplo, si compro algo por medios digitales con mi tarjeta de crédito, con todos requerimientos que se hace la entidad financiera, será más difícil que yo sea víctima de un fraude o suplantación", explicó.

¿Qué preguntas se debe hacer durante una entrevista laboral?

¿Qué preguntas se debe hacer durante una entrevista laboral?

Este será el proceso de apertura de la cuenta DNI en el Banco de la Nación

Poder Judicial establece jornada de trabajo presencial interdiario y en horario reducido

Vacuna rusa sin ensayos completos genera temores de mutación coronavirus entre científicos

Ollanta Humala opina que el “gobierno debe definir una estrategia clara y objetivos” en lucha contra el COVID-19

Congreso crea comisión para investigar número real de muertos por COVID-19

En menos de un mes ATU retuvo 800 brevetes por incumplimiento de protocolos de bioseguridad

GESTIÓN

Director Periodístico
JULIO LIRA SEGURA

Empresa Editora Gestión