Ciberseguridad: recomendaciones para que los emprendedores eviten los hackeos o estafas

Cada año los ataques cibernéticos se incrementan en el **Perú.** Así, cuanto más aumente el nivel de transformación digital de las empresas y de la sociedad peruana, mayores serán también las amenazas que intentarán atacar las infraestructuras críticas que facilitan funciones y servicios esenciales para los ciudadanos en salud, seguridad, bienestar social, financiero y económico.

Lee también: Internet Seguro: Cuatro tips para evitar ser víctima de phishing

Según el **Índice de Ciberseguridad Nacional**, el Perú mejoró su capacidad de protección de servicios digitales y de respuesta a incidentes del 2019 al 2022. Sin embargo, en nuestro país existen varios casos de ataques de ciberdelincuentes que vulneraron la seguridad de información de entidades públicas y privadas.

En 2018, el **Banco de Crédito del Perú (BCP)** sufrió un ciberataque por una falla de seguridad en sus sistemas que filtró datos de millones de sus clientes. Recién en 2019 se supo sobre este incidente, porque los datos de los clientes del BCP fueron publicados en la *darknet o* red oscura. Más adelante, en 2020, ocurrió la filtración de millones de registros de clientes de **Cineplanet**; entre los datos sustraídos, se encontraban números de tarjetas de crédito o débito e información personal.

Luego, en 2022, se materializó un ataque de *ransomware* contra la **Dirección General de Inteligencia (Digimin)**, por el que se filtraron 9 gigabytes de datos en la *darknet*. Y, recientemente, este jueves 19 de octubre, el portal del **Estado Peruano** fue atacado por ciberdelincuentes. Estos reemplazaron páginas de su sitio web, con fotografías y enlaces sospechosos.

Frente a esta problemática, **Raúl Díaz y Carlos Torres,** docentes de la carrera de Ingeniería de Sistemas de la Universidad de Lima, coincidieron en señalar que, aunque la implementación de un sistema de ciberseguridad adecuado requiere de una importante inversión, debe quedar claro que no contar con estos programas de protección digital puede generar costos mayores por diversos conceptos.

En ese sentido, los especialistas indicaron que, en el caso de un **ciberataque**, conocido como *ransomware*, en el que se "secuestra" la información de una organización, que se cifra en sus mismos lugares de almacenamiento y que no se "libera" sino hasta que se produzca el "rescate" mediante un pago en *bitcoins,* se incurre en una serie de costos.

> *"Las empresas u organizaciones incurren en costos de indisponibilidad de operación, de recuperación de información, de incumplimiento legal, de pérdida de reputación y de pérdida de clientes. De acuerdo a Ponemon Institute (2023), el costo promedio por un ataque de ransomware puede llegar a ser de US$ 5 millones", comentaron los expertos en ciberseguridad.*

Ciberdelitos más comunes

En cuanto a los delitos informáticos más comunes en nuestro país, **Raúl Díaz**, catedrático de la Universidad de Lima, informó que son el *phishing*, el robo de credenciales, la explotación de vulnerabilidades de día cero, la mala

configuración de soluciones *cloud*, el SIM *swapping* y el robo de dispositivos móviles.

> *"Los ciberdelincuentes se especializan cada vez más en ataques de phishing muy personalizados para que las personas ingresen a páginas falsas y hagan operaciones financieras no autorizadas. Un ataque que ocurría hasta el año pasado y que disminuyó considerablemente era el de SIM swapping, que consistía en que el ciberdelincuente suplantaba tu identidad ante la empresa de telecomunicaciones y compraba un chip a tu nombre", expresó.*

Agregó que el delincuente obtenía las credenciales de banco de su víctima por *phishing* y, con esta información, el nuevo SIM, bloqueaba su celular y procedía a realizar varias transferencias de dinero, debido a que el *token* SMS ahora llegaba al teléfono móvil con el SIM que había obtenido el ciberdelincuente.

Otro caso es el de robo de celulares. Los ciberdelincuentes han aprendido a ingresar de manera no autorizada a las aplicaciones bancarias con el acceso físico al dispositivo móvil de la víctima.

Lee también: Cinco consejos clave para no ser víctima de ciberataques

Consejos y recomendaciones

Ante la vulnerabilidad de los datos de emprendedores y de los ciudadanos, en general, especialistas de la Asociación de Bancos del Perú (Asbanc), en el V Foro de Seguridad Ciudadana y Empresarial, organizado por la Comisión de Seguridad Ciudadana y Empresarial de la Cámara de Comercio de Lima (CCL), realizado el último 28 de septiembre, resaltaron que muchos de los **ciberdelitos** se pueden evitar con mecanismos de

prevención.

Como medida de prevención, **Giovanni Pichling**, gerente de Seguridad Estratégica de Asbanc, sugirió a la ciudadanía que no ingresen a códigos QR sospechosos, ya que los ciberdelincuentes, a través de ellos, pueden acceder a información privada.

> *"Esta es una de las estrategias que usan los criminales para poder orientar nuestra navegación y hacer que bajemos software a nuestros teléfonos y computadoras a fin de entrar ilegalmente a nuestras bases de datos personales. Esto se puede ver, por ejemplo, en menús de restaurantes y otros negocios", comentó el especialista en ciberseguridad.*

Campaña de sensibilización

En tanto, **Maurice Frayssinet**, jefe de ciberseguridad y fraude de ASBANC, sostuvo que el *malware* es una pieza de código que se utiliza para extraer información sin que el usuario se dé cuenta.

> *"Este software malicioso, desde un mensaje SMS del celular, hace que se haga clic para reenviar al usuario a una página web sospechosa; sin embargo, la disfrazan sin que nadie la detecte y roban información".*

En este aspecto, el especialista recomendó colocar un **antivirus al teléfono celular** para evitar ataques de *malware.*

> *"Las personas solo colocan antivirus a sus computadoras, pero no lo hacen con el celular; y cuando empiezan a realizar transacciones desde el móvil, corren el riesgo de que sus cuentas bancarias sean hackeadas".*

Frayssinet también recomendó a los gremios empresariales unirse para compartir información y conocimiento sobre las

nuevas modalidades de vulneración de los sistemas de seguridad, así como realizar campañas de educación en escuelas y universidades.

Además, el especialista reveló que cada día se crean millones de *malware*, que afectan a los **bancos y a todo el sistema financiero.**

> *"Los ciberdelincuentes exponen los procesos de seguridad de las organizaciones y cada vez se sofistican más, lo cual es peligroso", anotó.*

Por su parte, **Carlos Torres**, docente de la Carrera de Ingeniería de Sistemas de la Universidad de Lima, expresó que la concientización es una pieza fundamental de la ciberseguridad.

> *"Esta concientización debe ser capaz de prevenir a la población sobre el uso de Internet y los peligros potenciales que esto conlleva. Además, se debe educar sobre cuál es el buen uso de los canales digitales y cómo responder ante los ciberataques más comunes".*

Remarcó que esta tarea es significativa y debe iniciarse desde edades muy tempranas, ya que los **niños y jóvenes emplean dispositivos digitales** y pasan a estar expuestos prontamente.

"Del mismo modo, debe seguirse esta tarea para el caso de los adultos mayores, que no son nativos digitales y que tienen dificultades para familiarizarse y operar dispositivos digitales y sistemas informáticos", dijo.

Lee también: Conoce los mejores tips para protegerte de ataques cibernéticos

Open Banking y sus riesgos

Si bien el *Open Banking* es una tendencia que se viene expandiendo y permite que los consumidores puedan compartir sus **datos bancarios** (previa autorización) con otros proveedores de servicios financieros como las *fintechs* y otros **bancos**, también puede dar lugar a nuevos riesgos y retos, entre los que se encuentran los relacionados con la **seguridad de la información**, pues el incremento en el volumen de flujos de datos puede incidir en un aumento de fraude, filtración o uso indebido de la información, afectando la privacidad de los clientes.

Frente a ello, el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (Indecopi) remarcó que resulta relevante la incorporación de estándares de **protección de la información**, así como contar con mecanismos adecuados para la atención de consultas, solución de controversias de los usuarios y una clara delimitación de responsabilidades frente a transacciones erróneas o fraudulentas.

A ellos se pueden sumar otros tipos de riesgos como la ciberseguridad, privacidad y protección de los datos personales de los clientes. De esta manera, si las interfaces de programación de aplicaciones (API) no se gestionan de forma segura o no se supervisan adecuadamente, ello puede dar lugar a nuevos riesgos, poniendo en peligro la estabilidad de la estructura del mercado.

> *“Desde una perspectiva de protección del consumidor, el aumento del intercambio de datos y de los procesos de iniciación de pagos en el marco de un modelo de Open Banking también puede incrementar los riesgos de transacciones no autorizadas”, dijo la entidad.*

Datos:

– Según la División de Investigación de Delitos de Alta Tecnología (Divindat) de la Policía Nacional del Perú (PNP), en el país se registran más de 300 denuncias de delitos informáticos cada mes.

– De acuerdo a la PNP, en 2022 se denunciaron 2 382 casos de fraude informático, el delito informático más reportado en el Perú durante 2021.

– Según el Ponemon Institute (2023), el tiempo de identificación promedio de un incidente es de 204 días y el tiempo de contención después de la identificación es de 73 días. Los fraudes más importantes del Perú no se alejan de estos promedios.

LEER MÁS:

Seis recomendaciones para protegernos de ciberataques