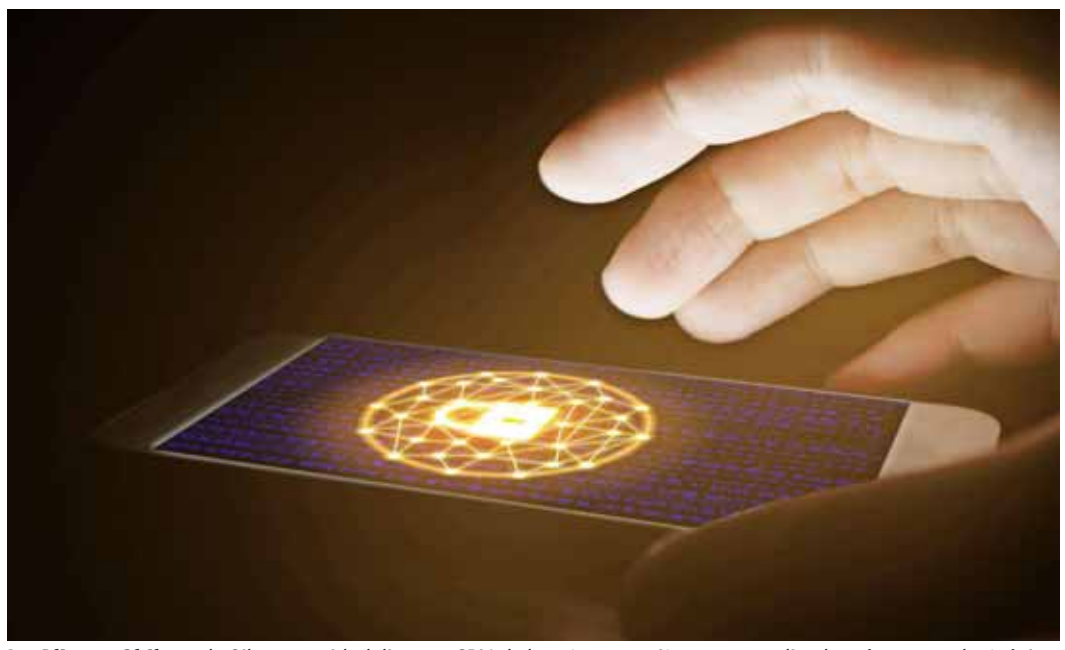
LOS MÁS COMUNES IRÁN AL ALZA:

Los siete ciberataques a los que hay que ponerles atención este 2021 en Chile

Phishing, ransomware, botnets y whaling son algunas de las vulneraciones que los expertos proponen tener bajo la lupa. ¿Cómo evitar ser víctima de un ciberfraude en tiempos de pandemia, teletrabajo y *e-commerce*? Saber qué son y cómo operan es clave para evitarlos.

DANIELA PALEO



La Alianza Chilena de Ciberseguridad dice que 91% de los ataques exitosos son realizados vía correo electrónico.

En 2020, la pandemia y las restricciones de desplazamiento generaron un incremento de interacciones en la web: un número alto de usuarios se volcaron a realizar la mayoría de sus actividades (compras, trabajo, educación, trámites y otros), por el canal *online*.

Esto, señala Alejandro Barros, investigador del Centro de Sistemas Públicos de Ingeniería Industrial de la U. de Chile, generó desafíos significativos en la escalabilidad que los sistemas tenían, ya que muchos no estaban diseñados para aumentos de usuarios y transacciones. "Además, se observaron grandes deficiencias en los niveles de usabilidad de estas plataformas y también muchos problemas asociados a la seguridad. De hecho, Google estimó un incremento de 350% de sitios considerados peligrosos", dice.

Hugo Galilea, director de la Alianza Chilena de Ciberseguridad, agrega que los ataques basados en ingeniería social proliferan en general vía *e-mails* o a través de la visita a páginas web con código malicioso. "En estos los ciberdelincuentes utilizan diferentes técnicas de manipulación psicológica para conseguir que las víctimas entreguen información confidencial y/o personal, con el fin de vulnerar un sistema", explica.

¿Qué nos depara 2021? Diego Macor, gerente de Soluciones de Ciberseguridad IBM Sudamérica, proyecta que se observen una serie de ataques informáticos similares a los de 2020. "Los ciberdelincuentes buscan la oportunidad, donde puedan encontrarnos con 'las defensas más bajas de lo normal'. Ese momento se da cuando hay cambios en el comportamiento de las personas o empresas, como trabajar en la casa o cuando una empresa cambia sus sistemas para adaptarse al trabajo remoto o mover sus cargas a la nube", indica.

Barros coincide en que serán más o menos semejantes a lo que vimos en 2020, ya que las condiciones ambientales se mantendrán (pandemia y operaciones a distancia). "Los ataques se darán especialmente en cuatro áreas: robo de criptomonedas, robo de credenciales y medios de pago en bancos y *retail*, *ransomware* y ataques a organismos públicos y agencias de seguridad", advierte.

E-mail, el punto débil

El **phishing**, en sus distintas versiones, dice Nicolás Corrado, socio de Deloitte experto en ciberseguridad, se ha vuelto más común y lo seguirá siendo en 2021, en gran medida porque este tipo de estafas se aprovechan de técnicas de ingeniería social. ¿En qué consiste? Erich Zschaeck, gerente de Ciberseguridad de EY, explica que son aquellos ataques que pueden ser masivos o direccionados a una persona y que apuntan a robar credenciales, contraseñas y datos personales: "Es el más frecuente en todas las industrias y uno de los principales puntos de entrada". También dice que el **ransomware** —ataque que secuestran información de las empresas y para su liberación piden un rescate en criptomonedas— se abrirá camino este año.

Ricardo Seguel, académico de Ingeniería y Ciencias de la UAI, complementa que el también llamado **malware** opera al ser descargado en un dispositivo móvil o computador y explotando una vulnerabilidad del sistema operativo que lo bloquea. Así, "antes o mientras el dispositivo está bloqueado, el *ransomware* podría robar toda la información de la víctima enviándola al sitio del atacante, por lo que el rescate a veces no es solo para liberar el dispositivo rehén, sino que también para que el atacante no divulgue o venda la información robada".

El **whaling** es otra modalidad que está adquiriendo popularidad, ya que abusando de la posición de autoridad que tienen ciertas personas al interior de una institución, por ejemplo los directores, los cibercriminales se aprovechan de ellos para direccionar sus acciones maliciosas. "Los destinatarios se ven en la obligación de proveer la información requerida, sin dudar o exigir información adicional al requirente", precisa Corrado.

Otra tendencia mundial es el **deepfake**, que consiste en la manipulación de contenido mediante el uso de herramientas de inteligencia artificial, permitiendo la simulación de personas en videos, incluso replicando sus gestos o voz.

En IBM advierten que los **botnets** podrían verse este año: una red de sistemas informáticos comprometidos que pueden realizar múltiples tareas automatizadas sin el permiso o conocimiento de los dueños de dispositivos. "Los atacantes usan los recursos informáticos de estos sistemas para ejecutar ataques a gran escala y otras actividades maliciosas mientras permanecen anónimos".

Otra forma de manipulación es el **social engineering** o campañas de ingeniería social que se llevan a cabo con el único propósito de extraer información comercial confidencial, como credenciales de inicio de sesión, registros de empleados y datos bancarios. "Generalmente se distribuye a través de correos electrónicos de *phishing* y otras formas de comunicación diseñadas para parecer inofensivas, pero en realidad canalizan información a fuentes maliciosas", dice Macor.

Por su parte, las **amenazas persistentes avanzadas** (*advanced persistent threat* o APT) se han convertido en una forma de violación de datos ampliamente utilizada, altamente efectiva y económicamente devastadora, que es difícil de detectar, y aún más, de recuperar. Usando tácticas sofisticadas y sigilosas, los atacantes obtienen acceso no autorizado a una red o sistema y pueden permanecer sin ser detectados durante meses o años.

Educar y proteger

La primera y principal recomendación para protegerse de los ataques virtuales, dice Seguel, es la educación y sensibilización de las personas sobre el uso responsable de los dispositivos, datos personales e información de sus organizaciones.

Galilea comenta que dado que el 91% de los ataques exitosos son realizados a través de un correo electrónico, lo primordial es crear conciencia en ciberseguridad, estar atentos y conocer estas técnicas. "Primero, nunca abrir un adjunto o seguir enlaces por correo, mensajería instantánea o red social, aun cuando el remitente sea conocido", explica y añade que se deben revisar exhaustivamente los remitentes en busca de *cybersquatting* (cambio de una letra por otra para confundir al receptor, como cambiar una "i" por una "l") y estar atentos a los *spoofing* (utilizar un remitente válido de manera fraudulenta para generar confianza).

Francisco Rodríguez, especialista en ciberseguridad ITQ Latam, recomienda realizar las correspondientes auditorías de seguridad de todos los servicios expuestos por la entidad hacia internet; uso de equipos corporativos para la realización del teletrabajo con todas las medidas de seguridad; formación y concientización para los empleados en materia de ciberseguridad; simulación de ataques llevada a cabo contra los empleados corporativos, y contraseñas robustas para el acceso a servicios corporativos o un segundo factor de autentificación.

Gustavo Arijón, *senior manager* de Consultoría y Asesoría Empresarial de PwC Chile, añade que las compañías deben crear políticas basadas en la seguridad lógica y en la nube, así como un plan de respuesta a incidentes que cubra todo el perímetro de sus operaciones. "Deben abstenerse de confiar implícitamente en los activos o cuentas de los usuarios. Además, es recomendable mantener sistemas y equipos actualizados y parcheados", concluye.

DAVID ALARCON KRITZLER

"Nadie esperaba lo que significó la pandemia en términos de transformación tecnológica para todas las empresas", afirma Julio Pertuzé.

SUBSECRETARÍA DE ECONOMÍA:

25% de las pymes se digitalizaron en 2020 a través de programas estatales

Casi 248 mil pequeñas y mediadas empresas pudieron digitalizarse al acceder a la estrategia de transformación tecnológica.

DANIELA PALEO

Uno de los balances positivos que dejó 2020 es el impulso acelerado que la pandemia dio a la transformación tecnológica de las empresas. El distanciamiento provocó cambios en los patrones de consumo y diversificación de los canales de venta, aumentando el uso de plataformas de comercio electrónico y transacciones a través de redes sociales, cambios frente a los cuales las pymes no quedaron ajenas.

En ese sentido, Julio Pertuzé, subsecretario de Economía, explica que la estrategia Digitaliza Tu Pyme, lanzada en 2019, va en esa dirección y hoy está reportando resultados que superan con creces las expectativas. El objetivo en 2019 era lograr que 20 mil pequeñas y medianas firmas se volcaran al canal digital, "objetivo que se cumplió, pero nadie esperaba lo que significó la pandemia en términos de transformación tecnológica para todas las empresas: se dieron cuenta que debían empezar a abrir nuevos canales de comunicación con sus clientes, nuevos canales de negocios". Así, revela, se lograron 247.740 digitalizaciones en 2020, cifra que representa 12 veces la meta de 2019.

Este volumen representa un cuarto del universo total de las pymes registradas en el Ministerio de Economía, que suman 1.005.366 a diciembre de 2020.

Sobre las proyecciones para 2021, Pertuzé dice que hay 20 mil pymes que participan en proyectos de capacitación mensualmente, pero mientras siga la situación actual, la cifra continuará aumentando.

80% en nivel básico

De acuerdo con la "Encuesta de acceso y uso de TIC en empresas 2020" de Economía, el 99% de las grandes empresas y el 91% de las pymes cuentan con internet. Sin embargo, existen otros aspectos en que las firmas chilenas presentan brechas en materia de digitalización. Por ejemplo, cuatro de cada cinco grandes empresas dicen tener un sitio web, mientras que dos de cinco pymes cuentan con una plataforma.

"Los siete programas que engloba la estrategia de digitalización buscan ayudar a las pymes a saber cómo a través de la tecnología pueden reinventarse y crear nuevos modelos de negocios y procesos", precisa Peturzé, y añade que para estar digitalizado no es suficiente tener una página web, sino también saber usarla para lograr buenos resultados; alza en ventas y alcance de clientes.

Además, el 80% de las pymes se concentran en los niveles más básicos de madurez digital, de acuerdo con los resultados del catastro realizado a partir de las más de 4 mil pymes que han pasado por el programa Chequeo Digital, que revela que muchas no utilizan herramientas de gestión en sus negocios, no realizan análisis de resultados de sus ventas y desconocen la importancia de aplicar seguridad en la base de datos de sus clientes.

Incluso, al profundizar en los niveles de digitalización, los resultados muestran que hay mucho camino por recorrer: solo 2% está en un nivel experto. En tanto, un 50% se ubicó en el nivel más básico (inicial), y un 30% en el segundo más básico (novato).

40%

de las grandes empresas usa redes sociales, frente al 24% de las pymes, según la Encuesta de Acceso y Uso TIC en Empresas 2020 de Economía.

32,8%

de las más de 4 mil pymes que han realizado el Chequeo Digital son de la Región Metropolitana. Además, el 18% corresponde a firmas del rubro comercio; 13%, a actividades de servicio, y 11%, de turismo.