

EMPRESAS: 4 CIBERAMENAZAS QUE SERÁN TENDENCIA EN 2022

A puertas de culminar el 2021 y darle la bienvenida al 2022, los delincuentes cibernéticos continúan aprovechando el impacto de la pandemia generada por la COVID-19 para atacar a los usuarios y también a las empresas. De acuerdo al Informe sobre Predicciones Globales de Ciberseguridad 2022, elaborado por Check Point Software Technologies, para el año entrante, los cibercriminales encontrarán nuevas oportunidades de ataque con las deepfakes, las criptodivisas, los wallets, entre otros.

Cabe destacar que, según el Grupo EULEN Perú, los sectores que mayor demanda de servicios de seguridad cibernética requieren en Perú, son: Industrial (20%); Banca, Financieras, Seguros y AFP (18%); Tecnología (15%); Minería y Energía (12%); Retail (12%); Telecomunicaciones (11%) y otros (12%). “Muchas empresas todavía realizan teletrabajo o trabajo mixto, por lo tanto, es fundamental analizar qué procesos e información crítica son empleados por los usuarios, identificar las malas prácticas y corregirlas a la brevedad. La idea es generar una cultura de -trabajo seguro- basada en la prevención”, indica Santiago Barranzuela, gerente de Seguridad del Grupo EULEN Perú.

Asimismo, el experto comenta algunas ciberamenazas que se pronostica, serán tendencia en 2022:

Aumento de amenazas en la nube

El trabajo colaborativo en línea incrementó durante la pandemia, siendo la nube una herramienta vital para que las empresas pudieran garantizar la continuidad del negocio. Si bien, desde hace un tiempo las organizaciones venían migrando su información más crítica a la nube, el contexto actual aceleró dicha transición. No obstante, la falta de práctica y conocimiento sobre el proceso de configuración, llegó con nuevas amenazas de seguridad. Así es como proteger las infraestructuras en la nube de las ciberamenazas debe ser una prioridad para todas las compañías e instituciones en 2022.

Incremento de amenazas por ransomware

Un gran porcentaje de violaciones de datos tiene una motivación económica. Los cibercriminales continúan violando los servidores y bases de datos de las empresas para causar daños financieros. Es así como los ataques de ransomware, los cuales mantienen como rehén la base de datos de una empresa a cambio de algún tipo de compensación económica, han crecido a un ritmo insólito, convirtiéndose en una amenaza para miles de compañías a nivel global.

El Grupo EULEN, empresa familiar multinacional con la matriz en España, avalado por la experiencia de más de 57 años en el mercado y consolidado como líder internacional en la prestación de servicios generales a empresas y administraciones públicas, que cuenta con más de 7 000 clientes en 14 países, y emplea a más de 90 000 personas en modalidad de planilla.

En el 2002 inicia sus operaciones en Perú, contando con una oficina central en Lima y dos delegaciones en las provincias de Arequipa y Trujillo, además de oficinas administrativas en todos los departamentos del Perú. Cuenta con más de 7.500 empleados y ofrece servicios de limpieza, seguridad física, seguridad electrónica, mantenimiento, servicios auxiliares, jardinería, Facility Management, Facility Services y trabajo temporal a más de 300 clientes de primer nivel en todo el país.

¿Qué podemos hacer? Educar a los colaboradores es la mejor solución. Enseñándoles sobre cómo identificar fuentes de correo no verificadas, textos fraudulentos, etc. Recuerda que un solo archivo descargado en algún equipo o intranet de la empresa puede causar un daño crítico.

Cuidado con las Fake News y las campañas de desinformación

Durante el 2021, la difusión de noticias falsas sobre la Covid-19 y el posterior proceso de vacunación fueron tendencia. Para el año entrante, los ciberdelincuentes continuarán aprovechando el contexto para generar campañas falsas y así, ejecutar diversos ataques de phishing y estafas.

Ataques a la cadena de suministro

A pesar de que los ataques a la cadena de suministro no son los delitos cibernéticos más frecuentes, estos serán cada vez más comunes en 2022. Pueden ocurrir cuando los cibercriminales encuentran una debilidad o una serie de vulnerabilidades en el ecosistema de una empresa, especialmente a través de sistemas de terceros, debido principalmente a la masificación de la digitalización, el trabajo remoto, etc. Debido a ello, los ciberdelincuentes pueden explotar más puntos de acceso en la cadena de suministro.

“Las tendencias de ciberseguridad suelen ser un buen indicador sobre el futuro próximo que nos espera. A medida que la tecnología evoluciona y más empresas se encuentren en medio de la transformación digital, resulta inevitable encontrarnos con una serie de retos en el sector. Es esencial que las organizaciones continúen gestionando y formando a su fuerza laboral en temas de ciberseguridad, pues siempre es mejor ir un paso adelante”, concluye Barranzuela.

El Grupo EULEN, empresa familiar multinacional con la matriz en España, avalado por la experiencia de más de 57 años en el mercado y consolidado como líder internacional en la prestación de servicios generales a empresas y administraciones públicas, que cuenta con más de 7 000 clientes en 14 países, y emplea a más de 90 000 personas en modalidad de planilla.

En el 2002 inicia sus operaciones en Perú, contando con una oficina central en Lima y dos delegaciones en las provincias de Arequipa y Trujillo, además de oficinas administrativas en todos los departamentos del Perú. Cuenta con más de 7.500 empleados y ofrece servicios de limpieza, seguridad física, seguridad electrónica, mantenimiento, servicios auxiliares, jardinería, Facility Management, Facility Services y trabajo temporal a más de 300 clientes de primer nivel en todo el país.