OPINIÓN

OPINIÓN

Un año después: ¿vulnerables ante los ciberataques?

¿Dónde son más vulnerables los usuarios? ¿cómo monitorear el acceso privilegiado a datos para evitar daños a los sistemas y otros recursos? son algunas de las interrogantes que deben responderse los responsables de la ciberseguridad.

Ciberataques. (Foto: Difusión)

Actualizado el 05/12/2021 05:11 a.m.

Sara Ugarte

Gerente de Ciberseguridad en Seidor Perú

Nunca antes las personas y las empresas se vieron más vulnerables ante los ciberdelincuentes, la pandemia trajo consigo cambios profundos en los entornos

de trabajo, educación y hábitos de compra, con un interés centrado en las noticias del **COVID**, se abrieron muchas puertas que facilitaron los **ataques digitales.**

Con la premisa de que los usuarios, y no la tecnología, constituye la variable más crítica de las ciberamenazas actuales ya que el objetivo de los ciberdelincuentes son las personas; un estudio sobre el factor humano de Proofpoint revela cuan vulnerables hemos sido durante el 2020 y cuáles fueron los ataques más efectivos y peligrosos.

La vulnerabilidad de los usuarios empieza por su comportamiento digital, el teletrabajo, el acceso al correo electrónico de la empresa desde sus propios dispositivos, el almacenamiento en la nube, instalaciones de aplicaciones de terceros son algunos puntos vulnerables que son aprovechados por los ciberdelincuentes.

En el 2021, las empresas iniciaron sus procesos camino a la normalidad, sin embargo, muchas han optado por un trabajo hibrido; en ese sentido será crucial contar con una estrategia de ciberseguridad que considere todos los ámbitos de comunicaciones de sus colaboradores y no poner en riesgo la seguridad de las organizaciones.

¿Dónde son más vulnerables los usuarios? ¿cómo monitorear el acceso privilegiado a datos para evitar daños a los sistemas y otros recursos? son algunas de las interrogantes que deben responderse los responsables de la ciberseguridad.

Un estudio global desarrollado por Proofpoint analizó diariamente por 365 días, más de 2,200 millones de mensajes de correo electrónico, 35,000 millones de URL, 200 millones de adjuntos, 35 millones de cuentas cloud, etc., es decir billones de puntos de datos en todos los canales digitales relevantes para identificar cuáles fueron los ataques más efectivos y frecuentes durante el 2020.

El estudio arrojó importantes hallazgos para tomar en cuenta en el futuro por ejemplo las técnicas de ataque de mayor éxito fueron también las más dirigidas, utilizándose en campañas a través de mensajes de correo electrónico.

Los ciberdelincuentes se aprovecharon de los nuevos intereses de las personas para lanzar todo el tiempo señuelos en los correos electrónicos, enfocados en las noticias de la pandemia, disfrazados de anuncios de los gobiernos sobre el estado de la vacunación, el OMS etc., desde los remitentes de spam hasta los usuarios de Malware comercial, ciberdelincuentes a gran escala y amenazas persistentes avanzadas (APT), casi 250 millones de mensajes dirigidos estuvieron asociados a la COVID-19, y miles de millones más de spam y ataques más generalizados.

Aquí algunos indicadores de los ataques más dañinos y del impacto que tuvieron en los usuarios:

• Hubieron más de 48 millones de mensajes con malware capaces de ser utilizados como punto de entrada para ataques de ransomware.

• Más de 1 de cada 3 personas fueron víctimas de campañas de ataques que utilizan esteganografía (código malicioso en fotografías y otros tipos de archivos) hicieron clic en el mensaje malicioso, la mayor tasa de éxito de todas las tácticas de ataque.

• Los ataques que utilizan técnicas CAPTCHA (crucigramas visuales para distinguir personas de las máquinas) superaron en más de 50 veces el número de clics conseguidos en el 2020 frente al año anterior.

• Casi el 25% de todas las campañas de ataque ocultaban malware en archivos ejecutables comprimidos, que solo se ejecutaban tras la interacción de los destinatarios.

• El phishing de credenciales, contra usuarios o empresas, fui el método más habitual de ataque, siendo responsable de casi dos tercios de todos los mensajes maliciosos, superando al resto de ataques juntos. Este ataca las cuentas, puede utilizarse para lanzar otros ataques, incluido el robo de datos y las estafas Business email compromise (BEC).

El cambio histórico que estamos viviendo, ha transformado el panorama de las amenazas. en todo el mundo, una defensa centrada en las personas puede hacer a los usuarios más resilientes y mitigar los ataques.

Las amenazas actuales requieren una estrategia centrada en las personas que permita garantizar la seguridad de los usuarios, los tiempos cambiaron y las organizaciones deberán estar preparadas para afrontar los desafíos de ciberseguridad.

NO TE PIERDAS

Contenido de **Gestión**

PetroTal anuncia solución pacífica a protesta cerca de su muelle de carga

Jefes de inversión de bancos miran con cautela a China y los mercados emergentes

Minsa plantea darle estabilidad a los trabajadores contratados por la emergencia: los CAS COVID

¿En qué invertir los S/1,200 millones del Powerball? Así podrías ganarlo antes que acabe el año

Navidad 2021: se ofertarán 1.6 millones de pavos en las fiestas de fin de año

Diez casos comunes a tomar en cuenta para el pago a trabajadores por feriado del 8 de diciembre

GESTIÓN

Director Periodístico
JULIO LIRA SEGURA

Empresa Editora Gestión
Jorge Salazar Araoz N° 171, La Victoria, Lima.

Cargando siguiente...

Los intangibles: su valor y deducibilidad