¿Cuánto costó el cibercrimen en 2022?

XXXXX. XX de diciembre de 2022.- La ciberdelincuencia es un problema que las empresas deben considerar como una amenaza latente, que se encuentra en constante evolución y cada día es más difícil de contrarrestar de forma efectiva.

Este año se vio marcado por una alta incidencia de eventos, principalmente por el *ransomware*, el cual atacó a un alto número de compañías a nivel global.

Es por eso que Strike, plataforma global de ciberseguridad que previene los ataques informáticos mediante el *hacking* ético, hace un recuento de cómo se propagaron las principales amenazas cibernéticas y cuál fue el costo de no proteger a los sistemas de forma correcta a través de análisis periódicos:

- El costo del cibercrimen

Las cifras varían de acuerdo a diversas fuentes. Por ejemplo, el Informe Anual de Amenazas de Unit 42 indica que los costos de rescate de información comprometida se incrementan 144% al año.

Por su parte, el reporte Cost of a Data Breach 2021 de IBM, indica que a nivel global el cibercrimen le costó a las empresas hasta USD $4.35 millones anuales.

Asimismo, un estudio de Veeam indica que el 76% de las organizaciones latinoamericanas experimentan al menos un ataque durante el año; de esa cifra, el 24% no pudieron recuperar los datos cifrados ni siquiera mediante el pago de un rescate, lo que nos hace pensar que el costo de un ataque no solo radica en lo económico.

- Ransomware, la principal amenaza

El *ransomware*, o secuestro de datos, fue el principal problema de ciberseguridad para las compañías en 2022. Este tipo de amenaza se vio potenciada por el surgimiento de nuevos métodos como la doble extorsión, que consiste en expandir el ataque más allá del cifrado de datos y pasar a la filtración de información sensible, como forma de exigir un rescate.

➢ Ransomware on demand

También destacan los modelos de afiliados, en los que los *hackers*, tras obtener acceso al sistema de una compañía, optan por no robar los datos directamente: por el contrario deciden, en lugar de atacar, ofrecer esos accesos a otros grupos para que estos obtengan la data que

deseen. Para ello se utilizaron *crypters* como HCrypt y Snip3 con los que los criminales entregaban varios troyanos de acceso remoto, así como el *software* Qbot.

➢ Ataques simultáneos

También este año se vio marcado por los ataques simultáneos. Durante este 2022 se presentaron casos como en el que los grupos cibercriminales Hive, LockBit y BlackCat atacaban a un mismo sistema de forma simultánea.

➢ Nacimiento de nuevos grupos

Los equipos de ciberseguridad también debieron lidiar con el nacimiento de nuevos grupos emergentes de *ransomware*. 'Familias' como BlackByte, Grief, Hive, Yanluowang, Vice Society y CryptoLocker/Phoenix Locker hicieron su aparición este año, mostrando similitudes cercanas con otros grupos que (en apariencia) desaparecieron. Esto lleva a los especialistas a considerar la posibilidad de que únicamente se trate de los mismos adversarios, operando bajo un nuevo nombre.

● ¿Cómo protegerse?

Luego de un 2022 lleno de incidencias y de cara al 2023 es importante exhortar a las empresas a anticiparse a los movimientos de los *hackers*, tratando de pensar como uno de ellos.

Para cumplir con ese objetivo, el *pentesting* se destaca como el método ideal. Se trata de un proceso en el que un '*hacker* ético' ingresa a los sistemas de una compañía, tal y como lo haría un cibercriminal, pero con el objetivo de encontrar posibles vulnerabilidades que un pirata informático podría explotar.

Como resultado, confeccionan un reporte que se actualiza continuamente con todas las vulnerabilidades halladas, las cuales son categorizadas por criticidad para que la empresa que contrató el *pentest* pueda arreglarlas en el periodo que considere apropiado.

La ciberdelincuencia no deja de evolucionar y es un problema latente que las empresas deben atender de forma periódica. La ciberseguridad no es algo de una única vez, es decir, no tiene un final. Por el contrario, debe realizarse continuamente ya que no se sabe en qué momento las organizaciones pueden, sin darse cuenta, abrir la puerta a entes maliciosos que podrían causar mucho daño.

-o0o-

Sobre Strike

Strike es la plataforma de ciberseguridad en Latinoamérica. Su principal misión es ayudar a que las compañías estén protegidas a través de la detección y resolución de vulnerabilidades en sus sistemas.

Esto se realiza a través de tests de penetración - o pentests - llevados a cabo por su red global de hackers éticos, conocidos como “Strikers”, una comunidad global que reúne a los mejores expertos de ciberseguridad con reconocimientos y certificaciones internacionales. Su objetivo es impulsar una cultura de ciberseguridad de calidad y accesible, en la que la misma sea parte del ciclo de vida de las empresas y no algo estanco o independiente. Más información en: https://strike.sh/