Ingeniería humana: ¿cómo cuidar el actuar de los empleados para evitar ciberataques?

CIUDAD DE MÉXICO. 14 de junio de 2023.- Más de la mitad de las violaciones de datos en la actualidad, según un estudio de ISACA, se deben a errores humanos y otras acciones, como descuidos y *clicks* en *links* apócrifos, realizados por los colaboradores de las empresas.

Esto despierta una importante alerta para las compañías que deben saber que, actualmente, cualquier equipo conectado a su red puede ser el detonante de un atentado de ciberseguridad a gran escala que no solo le cueste dinero a la compañía, sino que impacte negativamente en la reputación del negocio.

"La ingeniería social o humana es un aspecto fundamental en la seguridad cibernética de las organizaciones actualmente, ya que los ataques basados en engaño y manipulación de las personas son altamente efectivos y difíciles de detectar. Los profesionales de TI y de la ciberseguridad de las empresas deben prestar especial atención a este aspecto, ya que los colaboradores de una empresa pueden ser el eslabón más débil en la cadena de seguridad", señala Santiago Rosenblatt, fundador y CEO de Strike.

Los ataques que se propagan utilizando anzuelos y trampas, como el *phishing*, son muy comunes en el panorama actual de amenazas. Estos ataques consisten en la creación de correos electrónicos o mensajes falsos que aparentan ser legítimos, con el objetivo de engañar a los colaboradores para que revelen información confidencial, como contraseñas o datos de acceso.

De ese modo los empleados pueden caer en la trampa al hacer *click* en enlaces maliciosos, descargar archivos adjuntos infectados o proporcionar información sensible a través de formularios falsos. Esto puede resultar en el robo de datos, comprometer los sistemas o incluso en una gran pérdida financiera.

Entre las amenazas más comunes en cuanto a la ingeniería humana se encuentran:

1. Phishing y spear phishing: Correos electrónicos fraudulentos que imitan a empresas legítimas para obtener información confidencial.

2. Ingeniería social telefónica: Llamadas telefónicas en las que los atacantes se hacen pasar por representantes de una empresa para obtener información o acceso no autorizado. En estos casos, es común que se utilicen plataformas de Inteligencia Artificial para simular las voces de directivos y/o líderes de las empresas, para de ese modo pedir los accesos y la información a los colaboradores, evitando así que puedan negarse.

3. Ataques en redes sociales: Los atacantes utilizan información pública de las redes sociales para ganar la confianza de los colaboradores y obtener acceso a información privilegiada.

Para protegerse contra estas amenazas, Strike recomienda a las empresas que implementen una combinación de medidas técnicas y educativas:

- **Concientización y capacitación:** Es fundamental educar a los colaboradores sobre los riesgos de la ingeniería social y cómo reconocer los ataques. Se deben impartir programas de capacitación regulares y realizar simulaciones de ataques para fortalecer la seguridad.

- **Implementación de políticas de seguridad sólidas:** Las empresas deben establecer políticas claras en relación al manejo de información sensible y las prácticas de seguridad. Esto incluye el uso de contraseñas seguras, la autenticación de doble factor y la restricción del acceso a información crítica.

- **Actualizaciones y parches:** Es esencial mantener los sistemas y *softwares* actualizados con los últimos parches de seguridad para protegerse contra las vulnerabilidades utilizadas en ataques de ingeniería social.

- **Seguimiento y análisis:** Las empresas deben monitorear y analizar constantemente los intentos de ataques y las tendencias en ingeniería social para adaptar sus defensas y contramedidas.

Sumado a todo lo anterior, el *hacking* ético se presenta como un enfoque ideal para cerrar las puertas de las redes y evitar que las amenazas de ingeniería humana hagan daño a una organización.

Bajo un esquema sólido de *hacking* ético, mediante pruebas como el *pentesting*, se identifican vulnerabilidades que pueden cerrarse antes de que los ciberdelincuentes las encuentren, en el caso de que tengan éxito en alguna de sus propagaciones de contenido apócrifo.

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/

Síguenos en nuestras redes sociales:
Instagram - @strikesecurity
Twitter - @strike_secure
LinkedIn - Strike

Contacto para prensa México
another
Ahtziri Rangel | PR Expert
+ 52 1 55 1395 6970
ahtziri.rangel@another.co