Restauracióncolectiva
El portal de referencia para los profesionales del sector

Foto portada de sección y superior: ©Depositphotos

El cibercrimen como modelo de negocio: cómo reforzar la ciberseguridad en las empresas

01-02-2023

Recientemente se ha presentado el informe 'Presente y futuro de la ciberseguridad en 2023'; un tema que nos puede sonar muy lejano y ajeno pero que tiene que ver con nuestro día a día personal y profesional, ya que todas las organizaciones (desde la pyme a la multinacional) están expuestas a cualquier tipo de ciberataque. Os dejamos en este artículo un resumen sobre los principales desafíos en ciberseguridad y los consejos principales para evitar problemas.

La creciente inestabilidad geopolítica producto del conflicto entre Rusia y Ucrania, los ataques contra la disponibilidad y la nueva ola de 'hacktivismo' y de ataques patrocinados por Estados en todo el mundo han marcado el panorama de amenazas de ciberseguridad de 2022, tal y como se desprende del Informe 'Presente y futuro de la ciberseguridad en 2023' elaborado por el equipo de Ciberseguridad de Seresco, una compañía española especializada en soluciones tecnológicas, entre las que se encuentran los servicios de ciberseguridad para empresas.

Tras un año marcado, además, por otros componentes, como el fuerte repunte del *malware*, los altos niveles de *ransomware*, la ingeniería social y el *phishing* o el riesgo para las redes industriales y de corte operativo (redes OT), los expertos de ciberseguridad apuntan que 2023 continuará siendo desafiante en la lucha contra el cibercrimen. *"Este año estará marcado por un aumento del número de intentos de ataque e intrusión, acompañando sin duda a todos los nuevos procesos de transformación digital y la adopción de nuevas tecnologías, pero que cuya base predominante de materialización será la facilidad y rapidez de éxito debido a la disposición de nuevas armas como la computación cuántica, las redes 5G, el malware como servicio, y los recursos de IA"*, explica el citado informe (al final del artículo tenéis un glosario de términos para no iniciados).

Previsiones para 2023: sofisticación de ataques y aprovechamiento de nuevas tecnologías

- **Aumento de efectos e influencias geopolíticas en la ciberdelincuencia.** A medida que aumenten las tensiones entre Oriente y Occidente, se sucederán gran cantidad de ataques contra la disponibilidad, tanto disruptivos como destructivos, a

todo tipo de Infraestructuras críticas, redes OT e instituciones gubernamentales. Los ataques de *malware* de tipo *wiper* irán en aumento, como aquellos dirigidos a la obtención de grandes cantidades de multinacionales o la Inteligencia de gobiernos.

- **Proliferación de ataques a cadenas de suministro a gran escala.** Aumentarán los ataques a proveedores de grandes servicios, como servidores de correo, alojamientos en la nube, desarrolladores de *software* o suministros digitales. Con ello, en lugar de afectar a una única víctima, los atacantes accederán a dichos proveedores para alcanzar múltiples objetivos dentro de su red.
- **Mayor volumen y sofisticación de *malware*.** Se prevé la difusión de *malware* maleable y adaptable a cada escenario, pudiendo realizar cambios de código para evadir su detección, del mismo modo que los virus biológicos mutan para pasar inadvertidos por un sistema inmunológico que estaba preparado para detectar y combatir anteriores cepas. Aparecerán alternativas de elementos maliciosos con nuevas capacidades y técnicas de evasión más avanzadas.
- **El robo de datos se centrará en la nube y en las *cookies*.** Habiendo generalizado el uso de la nube, aumentado así la superficie de ataque y relegando la seguridad a un segundo plano, es inevitable percibir aquí una tendencia mantenida al alza a corto y medio plazo. Igualmente, los ataques para capturar *cookies* se están volviendo cada vez más sofisticados, siendo un vector que permite eludir la autenticación multifactor (MFA).
- **El cibercrimen como modelo de negocio (CaaS) aumentará.** Ha demostrado ya que algunas de sus modalidades, como IAB, MaaS y RaaS, han estado realmente presentes durante este periodo. El acceso a las nuevas tecnologías facilitará la proliferación de nuevos ciberdelincuentes que podrán navegar por mercados ilícitos para hacerse con todo tipo datos, servicios o material listo para usar.
- **Cuidado con la ingeniería social, especialmente con el *phishing*.** Habrá cada vez señuelos más elaborados y la falsificación de comunicaciones y sitios oficiales (*spoofing*) será muchas veces difícilmente reconocible. El fenómeno irá dirigido, en gran medida, a comprometer las credenciales de acceso de las víctimas y a eludir los sistemas MFA.
- **Las IA jugarán un papel importante.** La calidad del código producido por una IA depende del código con la que se la alimente y de la corrección de las órdenes que se le trasladen. Por ello, el desarrollador continúa ejerciendo un papel clave, pudiendo producirse un aumento de vulnerabilidades si éste no toma la atención necesaria.
- **Pymes y administración pública regional y local: mayor vulnerabilidad percibida.** Continuarán los ataques recurrentes a la administración pública, pero con un foco aumentado en las pequeñas administraciones, tales como ayuntamientos. De modo análogo, se verá un creciente interés por empresas y negocios de menor tamaño al habitual, debido a la mayor vulnerabilidad percibida en ellas.
- **Focalización en redes OT, dispositivos móviles e IoT.**El acercamiento de redes OT a redes IT traerá consigo un gran torrente de nuevas vulnerabilidades, lo cual se verá acentuado por el gran número de controladores industriales (ICS) obsoletos en cuanto a parches de ciberseguridad se refiere. Igualmente, generalizado el uso de dispositivos móviles e IoT, y aprovechando habituales deficiencias de configuración y obsolescencia de los mismos, serán un objetivo habitualmente amenazado.
- **Avalanchas de desinformación y *deepfakes*.** Con el continuo aumento en la cantidad de datos e información que se manejan por internet, por las redes sociales y por los medios de comunicación, crecerá el número de focos de desinformación para aumentar audiencias o empujar la opinión social en determinados temas. El incremento en implementaciones de las IA y en recursos tecnológicos harán, por su parte, que los *deepfakes*sean cada vez más sofisticados, numerosos, convincentes y efectivos.

Cómo reforzar la ciberseguridad en las empresas

Ante este escenario, el informe de Seresco recuerda una serie de medidas básicas para favorecer la protección, tanto de particulares como de instituciones o empresas:

- Aumentar la salud de nuestras contraseñas.
- Actualizar el *software* y los dispositivos a las últimas versiones disponibles.
- Establecer una configuración DMARC en el correo electrónico.
- Formación continua en ciberseguridad.
- Configurar bien nuestras opciones de seguridad en la nube.
- Analizar concienzudamente comunicaciones, anuncios, adjuntos y enlaces.
- Extremar precauciones en las redes IT.
    - Ciberseguridad como anticipación, no como reacción.
    - Hacer copias de seguridad de absolutamente toda la información –y guardarlas correctamente–.
    - Vigilancia y monitorización continua.
    - Llevar a cabo auditorías periódicas.
- Máxima prevención en redes OT.
    - Establecer una seguridad en profundidad.
    - Favorecer la sectorización.
    - Valorar qué dispositivos necesitan conexión.

– Descarga del informe completo: ‘Presente y futuro de la ciberseguridad en 2023’.

GLOSARIO BÁSICO PARA NO INICIADOS

– CaaS. Es el denominado crimen como servicio (*Crime as a service*) que hace referencia a criminales que ofrecen sus servicios a cualquier persona/entidad que quiera pagarlos: entrar en la cuenta de Facebook de otra persona, espiar WhatsApp, insertar *malware*, obtener credenciales de acceso, interceptar correos…
– IAB.

Agentes de acceso inicial. Actores que venden el acceso a las redes empresariales a un comprador viable. En el pasado, los intermediarios de acceso inicial (IAB) solían vender principalmente el acceso de la empresa a los delincuentes que pretendían destruir los datos, o robar IPs, o datos financieros de las empresas comprometidas. Hoy se contratan a los IAB para comprometer a las empresas objetivo, de modo que la banda pueda empezar a cifrar los archivos sensibles y destruir las copias de seguridad.
– IoT. Abreviación del término en inglés*Internet of things*; en español, internet de las cosas, es un concepto que se refiere a la interconexión digital de objetos cotidianos, como relojes, cámaras de grabación, electrodomésticos, etc. mediante internet.
– Hacktivista. Ciberdelincuente que haciendo uso de sus conocimientos en materia informática y herramientas digitales los usa para promover su ideología política. Entre las acciones que realizan destacan las modificaciones de webs (*defacement*), redirecciones, ataques de denegación de servicio (DoS), robo de información privilegiada o parodias de sitios web, entre otras.
– Malware. Es un tipo de *software* que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información. Palabra que nace de la unión de los términos en inglés de *software* malintencionado: *malicious software*. Dentro de esta definición tiene cabida un amplio elenco de programas maliciosos: virus, gusanos, troyanos, etc. La nota común a todos estos programas es su carácter dañino o lesivo.
– MaaS. *Malware as a Service* permite a cualquier persona realizar un ataque de *malware* a gran escala con poco o ningún conocimiento técnico o experiencia requerida. Es un ejemplo de uno de los servicios prestados como parte de la economía de servicios del ciberdelincuente.
– Phishing. Técnica o tipo de ataque en el que alguien suplanta a una entidad/servicio mediante un correo electrónico o mensaje instantáneo para conseguir las credenciales o información de la tarjeta de crédito de un usuario. Ese correo/mensaje suele tener un enlace (o fichero que contiene ese enlace) a un sitio web que suplanta al legítimo y que usan para engañarlo.
– RaaS. El *ransomware* como servicio (*Ransomware as a service*) es un modelo de negocio en el que actores maliciosos contratan los servicios de un *ransomware* a través de un programa de afiliados y se encargan de llevar adelante los ataques. Este servicio lo ofrecen grupos de ciberdelincuentes que desarrollan este tipo de códigos maliciosos y lo ofrecen en foros clandestinos en los que buscan reclutar afiliados, que son quienes contratan el servicio.
– Ransomware. *Malware* cuya funcionalidad es ‘secuestrar’ un dispositivo (en sus inicios) o la información que contiene, de forma que si la víctima no paga el rescate, no podrá acceder a ella.
– Redes OT. Los sistemas OT ofrecen la integración de *software* y *hardware* que sirven para poder comunicar, controlar y supervisar diversos dispositivos de las redes industriales.
– Spoofing. Es una técnica de suplantación de identidad en la Red, llevada a cabo por un ciberdelincuente generalmente gracias a un proceso de investigación o con el uso de *malware*. Los ataques de seguridad en las redes usando técnicas de *spoofing* ponen en riesgo la privacidad de los usuarios, así como la integridad de sus datos.
– Wiper. Es un tipo de *software* malicioso que pone en riesgo la información personal, documentos y cualquier tipo de archivos que se tengan almacenados. Su objetivo no es otro que borrar el contenido que haya en una memoria o disco.

Notícias Relacionadas

- El 94% de las empresas prevé sufrir ataques cibernéticos y el 44% declara haberlos sufrido
- Food defense para proteger de sabotajes la producción y suministro de alimentos
- ¿Pueden las empresas indagar en las redes sociales de los candidatos?
- Rapidez, estrategia y recuperación: claves para gestionar una crisis en redes sociales