Tendencias de ciberseguridad para 2019.

a ciberseguridad seguirá siendo un tema candente en 2019. Criptojacking, ransomware, aplicaciones móviles maliciosas o la seguridad en IoT e IA continuarán en el punto de mira de los expertos en seguridad este año.

La ciberseguridad ha estado presente en los medios durante todo 2018. Uno de los casos más sonados fue el de **Facebook y la polémica con Cambridge Analytica**, el mayor escándalo en protección de datos hasta ahora. El **auge de las criptomonedas** aumenta la probabilidad de sufrir ataques virtuales como el **criptojacking**, el secuestro de dispositivos informáticos para minar las monedas digitales.

El departamento de expertos en ciberseguridad Entelgy Innotec Cybersecurity propone **10 tendencias** que serán el foco de los ciberdelincuentes en 2019:

1. La irrupción de los criptomineros

Las criptomonedas se utilizan para realizar **envíos de dinero virtual constantemente**. Para registrar estas transacciones, es necesario que alguien compruebe y confirme los pagos. Los

mineros son los encargados de escribir estos datos dentro de la cadena de bloques (blockchain).

Cuando se realiza una transacción de criptomonedas, el minero que confirma y registra el pago se lleva **una pequeña comisión**. La posibilidad de enriquecerse con la minería ha creado el **criptojacking**, mineros que utilizan software malintencionado **para apropiarse de las monedas de forma ilegal**.

Durante las XII Jornadas STIC del CCN-CERT se habló de los últimos datos publicados en **el informe sobre cryptojacking**, donde el número de muestras de este tipo de minería dañina rondaba en enero de 2018 las 94.000, mientras que 3 meses más tarde, la cifra incrementó un 74% (127.000 muestras).

2. Inteligencia Artificial: nuevo punto de ataque

La IA se integra cada vez más en **ámbitos profesionales**. El hecho de que las grandes empresas utilicen IA para optimizar la toma de decisiones y la ejecución de acciones supondrá **una puerta para los ciberdelincuentes** que podrán acceder a datos sensibles de dichas empresas. **Es fundamental que los datos se protejan desde todos los puntos en los que sean accesibles**, evitando dejar cabos sueltos que supongan una amenaza para la privacidad de la empresa.

3. Aumento de la preocupación sobre la privacidad de los datos personales

La entrada en vigor del Reglamento General de Protección de Datos (RGPD) supuso una revolución en la protección de datos, llevó a muchas empresas a implantar medidas de seguridad para evitar fugas de información. Las grandes empresas se adaptaron

rápidamente a el RGPD, no tanto las **pymes** que, en su mayoría, **siguen sin disponer de las medidas de protección de datos necesarias**. Haber subestimado a los **ciberdelincuentes podrá salirles caro a las pequeñas y medianas empresas**.

4. Ransomware: bajará el uso del malware más rentable

El ransomware es un programa dañino que **restringe el acceso a determinados archivos o partes del sistema** y pide un rescate a cambio de eliminar este bloqueo. Aunque el ransomware seguirá utilizándose, se prevé que **su uso será cada vez menor** y los ataques descenderán durante 2019. El criptojacking, probablemente, será el nuevo sustituto del ransomware.

6. Aplicaciones móviles maliciosas

Los usuarios acostumbran a pensar que las apps maliciosas solo se encuentran en **lugares de descarga no oficiales**. Esto es un gran error, ya que **Google Play y App Store** alojan aplicaciones troyanas que son capaces de robar las credenciales de los usuarios. En su apariencia de aplicación inofensiva, estos softwares pueden interceptar mensajes de texto e incluso introducir criptomineros ocultos.

8. Más puntos de ataque con la incorporación del Internet de las Cosas (IoT)

El **IoT** no para de multiplicar los dispositivos y sistemas que pueden ser conectados a Internet. Al igual que la **Inteligencia Artificial (IA)**, estos dispositivos vinculados a la red **son puntos vulnerables de los sistemas de seguridad**. El crecimiento del IoT supone que cada vez hay más objetivos que atacar por los cibercriminales y, por tanto, **más dispositivos**

que proteger.

9. Foco en infraestructuras críticas y Operadores de Tecnología (OT)

La nueva directiva NIS obliga a todos los operadores de infraestructuras críticas y a los OT a proteger sus sistemas y redes. Esta nueva directiva también les obliga a **reportar cualquier incidente que ocurra**, lo que hará que ocupe un lugar importante durante la agenda de ciberseguridad de 2019.

10. El espionaje seguirá a la orden del día

Son muchos los dispositivos que **incorporan software malicioso de fábrica**. Dicho software puede acceder a la cámara, micrófono o información almacenada del gadget, **recopilando información muy sensible sin permiso del usuario**. Las **auditorías de seguridad** de los dispositivos serán los encargados de tratar de solucionar este gran problema, que seguirá estando a la orden del día en 2019.

Fuente: https://blogthinkbig.com