21/11/22

¿Seguridad? ¿A mí quién me va a atacar?

En la actualidad está existiendo una mayor acogida a securizar los sistemas informáticos de las empresas e instituciones públicas, sobre todo después de la gran noticia del *ransomware* de **Wannacry** en mayo de 2017. Sin embargo, esta acogida no es total, y muchas empresas y gente de a pie sigue reticente a ello y se hace la misma pregunta: «¿A mí quién me va a atacar?».

Desde que *Wannacry* se hizo público, en mayo del 2017, las empresas empezaron a ser más conscientes de la necesidad de la implantación de un sistema seguro en sus equipos y servicios pero, sin embargo, todavía hay muchas instituciones que no han implantado este tipo de sistemas y que, si lo han hecho, no han instaurado unas correctas políticas de seguridad.

¿Por qué no se toman medidas?

Hay varias razones por las que las empresas y las personas de a pie no toman las suficientes medidas al respecto, pero la mayoría de ellas se resumen en una sola palabra: desinformación.

Los medios de noticias, en su mayoría, exponen ataques realizados contra grandes empresas o instituciones ya que estas noticias van a tener un gran impacto y, además, una empresa pequeña es más complicado que se exponga públicamente. Además, la información mostrada en los medios de noticias va a estar sesgada por lo que le cuente la empresa.

Una gran empresa, por ejemplo, va a contar a un entrevistador que está lidiando con un nuevo *ransomware*, con un virus malicioso, o que han conseguido filtrar sus datos. Sin embargo, normalmente no va a contar el cómo ha ocurrido o cuál ha sido el **vector de entrada del atacante**, excepto a una autoridad de ciberseguridad (**NIST**, **CSIRT**, **Kaspersky**, etc.).

Phishing y vishing

Además es posible que, debido al tipo de noticias sobre ataques que aparecen en los medios de comunicación, cuando pensemos en un ataque pensemos en *malware*, *ransomware*, virus…

Pero sin embargo, no solemos pensar en ataques de *phishing* o de *vishing*, propios de ingeniería social.

Un *phishing* es el delito de engañar a alguien para que nos compartan información confidencial como contraseñas o tarjetas de crédito a través de un enlace enviado a través de un correo o un SMS, haciéndose pasar por una entidad que no es.
El *vishing* también consiste en engañar al usuario para que comparta información pero a través de una llamada de correo, no necesitando conocimientos informáticos para realizar este ciberataque.

Este tipo de ataques son muy comunes actualmente, además de que conforman un gran vector de entrada al sistema y con un poco de concienciación es posible mitigarlo.

¿Qué problemas conlleva?

Esto provoca dos grandes problemas:

- Si los ataques mostrados solamente son aquellos ocurridos a grandes empresas o instituciones, las personas piensan que, si no entran dentro de estos miembros, no les van a atacar. Por tanto, las **PYMES** y personas de a pie no se van a preocupar por securizar sus sistemas.
- Si, además, en estas noticias no incluyen los vectores de entrada de los atacantes, es muy probable que no se tengan en cuenta en aquellos sistemas que se quieran securizar.

- **Por ejemplo,** un elemento fundamental a la hora de dar seguridad un sistema es la concienciación, ya que un *malware* puede entrar a través de un *phishing* o los datos pueden haber sido sustraídos a través de un simple *vishing*.

¿Y por qué las pequeñas empresas no informan de los ataques recibidos públicamente?

Cuando se produce un ataque a una empresa pequeña, pueden ocurrir dos cosas principalmente:

- Si el ataque no es potente y sobreviven al mismo, ellos mismos no van a exponerse en los medios públicos, porque estarían exponiendo que sus sistemas no son seguros. Una gran empresa tiene su público ya afianzado, pero una **PYME** no, por lo que perdería oportunidades de mercado y, por tanto, podría ir a la quiebra fácilmente.
- Si el ataque es potente y la empresa no sobrevive al mismo, son los responsables de seguridad los que perderían dichas oportunidades de mercado y, posiblemente, las posibilidades de trabajar en el sector de nuevo.

- Por todo esto, la desinformación que existe sobre este tema es tan grande. Sin embargo, existen elementos, como los revisados en este artículo, que nos permiten comprobar que, efectivamente, **PYMES** y particulares somos también atacados.

Y entonces, ¿qué nos muestran al respecto?

- Fuera de los métodos de noticias convencionales, existen páginas web y elementos que nos muestran este tipo de información de una forma más detallada, como por ejemplo los análisis de **IBM** o **Kaspersky**.

- Estas páginas nos muestran las últimas vulnerabilidades encontradas en los sistemas informáticos, así como estadísticas de los ataques más comunes y dónde se han realizado dichos ataques. Por ejemplo, aquí **Kaspersky** nos muestra estadísticas de las ciberamenazas financieras en 2021.

- En dichas estadísticas podemos contemplar cómo se realizaron bastantes campañas de *phishing* (un 8.2%), siendo mayormente *phishing* destinado a comercio electrónico. Además, estos ataques eran mayormente destinados a pasarelas de pago como **Paypal** o **Mastercard**, que son métodos de pago muy utilizados por la población en general.

- También nos muestra las plataformas por las que más se hacen pasar los atacantes, como son **Apple**, **Amazon**, **eBay** o **Alibaba**, páginas web donde solemos comprar un gran número de artículos a todas horas y que, si nos atacan, debemos estar preparados para que no nos roben la cartera.

Conclusión

- Hoy en día mucha gente no se preocupa en exceso de darle protección a sus datos en la red o de proporcionar un servicio totalmente seguro. Estos piensan, debido a los medios de comunicación, que a ellos no les va a pasar nada y no tienen en mente que precisamente son los más fácilmente atacables.

- Si una persona es capaz de robarte en la vida real sin ser de una gran empresa, ¿por qué no sería capaz de robarte en Internet? Y, si pones alarmas, perros guardianes y sistemas de vigilancia en la puerta de tu casa, ¿por qué no las vas a poner en tus sistemas virtuales?

- O más simple aún: si cierras la puerta de tu casa con llave cada vez que sales a pesar de no trabajar en una multinacional, ¿por qué no hacerlo en la web?

Fuentes

- Kaspersky – Ciberamenazas financieras en 2021: https://securelist.lat/financial-cyberthreats-in-2021/96250/
- Kaspersky – Security Bulletin 2021. Statistics: https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2021_eng.pdf
- IBM – Cost of data breach 2022: https://www.ibm.com/reports/data-breach
- IBM – X-Force Threat Intelligence Index 2022: https://www.ibm.com/reports/threat-intelligence/
- INCIBE – Phishing: https://www.incibe.es/aprendeciberseguridad/phishing
- INCIBE – Vishing: https://www.incibe.es/aprendeciberseguridad/vishing