Cinco consejos para prevenir un ataque de ransomware o secuestro de datos

Aunque es una de las técnicas más tradicionales, el impacto de un ciberataque por **ransomware** o **secuestro de datos es asombroso**. Pasan los años y aumenta la concienciación entre los usuarios acerca de la importancia en prevención de ciberataques, pero a lo largo del tiempo se producen campañas devastadoras.

Una de las tendencias más fuertes es que este tipo de técnicas han empezado a explotar cada vez más un formato, el del teléfono móvil inteligente. En 2018, de hecho, los ciberdelincuentes han usado cada vez más el **«ransomware»** para móviles. **El uso de este tipo de ataque, que secuestra el terminal de su víctima**, también ha crecido de forma exponencial en ordenadores. Por lo tanto, no es de extrañar que se hayan popularizado sus variantes para **smartphones** y tabletas.

A pesar que muchos de esos ataques se producen entre los usuarios, la amenaza del **ransomware** ha evolucionado, repentina y espectacularmente, dirigiéndose contra empresas de todo mundo mediante una serie de destructivos ataques y cuyo objetivo final sigue siendo desconocido. Según datos de estudio **el 26% de los ataques de ransomware se dirigieron contra las empresas.**

Un dato que aumenta exponencialmente hasta el 53% si atendemos todos los ciberataques que sufrieron, según informes recientes, a las pymes en 2017. El **malware** se ha convertido en un gran negocio para los hackers y un gran dolor de cabeza para las empresas, generando un coste anual de alrededor de 11.500 millones de dólares.

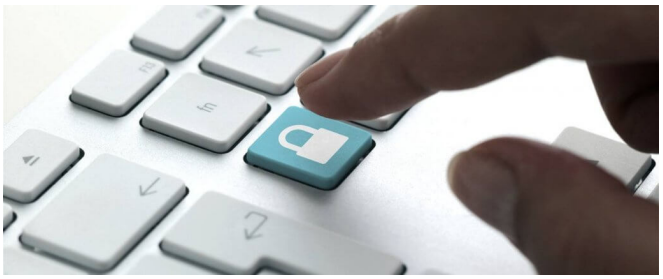
Hacer una copia de seguridad

Es algo que se debería hacer siempre que se pueda, ya sea de manera manual o, incluso, **automatizándolo gracias a algunas herramientas que se tienen a disposición**. Gracias a ello, se puede evitar la pérdida de material y datos sensibles en caso de robo del dispositivo electrónico o problemas técnicos. Pero, también, para protegerse ante posibles ciberataques como el secuestro de datos que extorsionan a los usuarios para devolverles el control de sus ordenadores. **Además de evitar**

pagar por el rescate, se recomienda por tanto realizar copias de seguridad periodicamente.
Con la llegada de redes más seguras y el almacenamiento en la nube, muchas empresas no realizan copias de seguridad de archivos y datos. Sin embargo, en caso de sufrir un ataque de "ransomware", se pueden utilizar estas copias de seguridad en lugar de pagar el rescate. **También se pueden habilitar copias de seguridad automáticas para empleados**, para que no tengan que realizarlas por su cuenta.

Educar a los usuarios a reconocer las amenazas

Un simple mensaje recibido en el correo electrónico del trabajo puede provocar un caos monumental. Los ciberdelincuentes suelen, además, aprovechar días señalados **en el calendario para cometer sus atrocidades virtuales.** Por eso hay que llevar cuidado con hacer clic en enlaces sospechosos.
Un escenario que demuestra que la educación del usuario siempre ha sido un elemento clave para evitar infecciones. Este mismo principio también se aplica al **ransomware**. Los conceptos básicos de saber de dónde provienen los archivos, **por qué el trabajador los recibe y si puede confiar en el remitente**, continúan siendo parámetros útiles **que los empleados deben usar antes de abrir archivos y correos electrónicos**, agregan las mismas fuentes, quienes subrayan que los métodos de infección más comunes utilizados siguen siendo los correos electrónicos de **spam** y **phishing**. Muy a menudo, los conocimientos del usuario pueden prevenir un ataque antes de que ocurra.



Limitar el acceso

Limitar y controlar. Ahí esta otra de las claves del asunto. Con el fin de minimizar el impacto potencial de un ataque de ransomware exitoso, la organización se tiene que asegurar de que los usuarios solo tengan acceso a la información y los recursos necesarios para ejecutar sus trabajos. **Al tomar este paso, se reduce significativamente la posibilidad** de que un ataque de ransomware se mueva lateralmente a través de su red. Abordar un ataque de ransomware en un sistema de usuario puede ser una molestia, pero las implicaciones potenciales de un ataque en toda la red pueden ser dramáticamente mayores, apuntan los expertos.

Actualizar los sistemas operativos y antivirus

Otra de las recomendaciones más fuertes es tener actualizados

los **sistemas operativos y los antivirus.** Desde el punto de vista de la ciberseguridad, siempre es beneficioso mantener los antivirus actualizados. Si bien estas protecciones por sí solas no son suficientes para detectar y **prevenir sofisticados ataques de ransomware**, cuando están diseñados para evadir las protecciones tradicionales son un componente importante para la seguridad integral. **Mantener el antivirus actualizado pueden proteger a la organización contra el malware** y aportan la seguridad de una marca reconocida.

Sistemas multicapa

Por último, otra de las recomendaciones es utilizar sistemas de seguridad multicapa con tecnologías avanzadas de prevención de amenazas. La implementación de un sistema de varias capas para la seguridad es la mejor forma de defenderse del ransomware y del daño que podría causar.

Además de las protecciones tradicionales, como antivirus e IPS, las organizaciones necesitan incorporar capas adicionales para evitar el malware nuevo y desconocido. Dos componentes clave a considerar son la extracción de amenazas (desinfección de archivos) y la emulación de amenazas (sandboxing avanzado). Cada elemento proporciona una protección distinta, pero cuando se utilizan de forma conjunta, ofrece una solución integral para la protección contra malware desconocido a nivel de red y end-point.

Fuente de información:
https://www.abc.es/