Acronis

10 Simples Tips para Protegerse del Ransomware

El ataque de ransomware WannaCry, que derribó cientos de miles de computadoras en 150 países, marcó el comienzo de la próxima oleada de ataques de ransomware. En tan sólo unos pasos, puede protegerse de cualquier ataque de ransomware, incluyendo WannaCry.

1

Manténgase al día con las actualizaciones del sistema operativo y las aplicaciones

Los ataques de malware como WannaCry a menudo explotan las vulnerabilidades de software que usted puede cerrar mediante la instalación del último sistema operativo y parches de aplicación, actualizaciones y releases de seguridad.

- Instale el **parche** de seguridad de Windows
- Lea la guía para clientes de **Microsoft**

2

Realice copias de seguridad periódicas

Las copias de seguridad de imagen completa periódicas son la mejor manera de mitigar los ataques de ransomware. Debería realizar una copia de seguridad de archivos críticos con regularidad, preferiblemente a un almacenamiento seguro en la nube proporcionado por su proveedor de copia de seguridad. Sin embargo, debe consultar con su proveedor para asegurarse de que su copia de seguridad en la nube está protegida contra el ransomware.

3

Habilite Acronis Active Protection™ en sus copias de seguridad

El software moderno de copia de seguridad tiene protección en tiempo real incorporada. Tecnología innovadora detecta y detiene el ransomware usando heurística de comportamiento incluso cuando su programa de anti malware no lo hace. **Acronis Active Protection** también recupera automáticamente cualquier archivo dañado en un ataque de ransomware devolviéndolo a su estado original.

4

Instale un software de antivirus y mantenga su base de datos actualizada

El software de antivirus/antimalware provee una defensa valiosa contra una variedad de virus maliciosos. Escoja su software cuidadosamente y active la actualización automática de su base de datos de firmas. Aún así, tenga en cuenta que muchas variantes nuevas de ransomware pueden evadir defensas de antivirus, así que asegúrese de hacer una copia de seguridad de sus sistemas y utilizar Acronis Active Protection.

5

Haga visibles las extensiones de archivo

Su sistema operativo puede esconder por defecto las extensiones de archivo (como .pdf para archivos de Adobe). Haga visibles las extensiones de archivos para dificultar a los atacantes camuflar archivos maliciosos como legítimos. Por ejemplo, con las extensiones de archivos visibles, usted podría fácilmente detectar un archivo de javascript (con la extensión .js) tratando de disfrazarse como un documento de Microsoft Word (.docx)

6

Tenga cuidado con los adjuntos de correo electrónico

Si recibe algo de una persona que no conoce, o algo que no espera, ¡no lo abra!. Confírmelo con el remitente y páselo por su software de antivirus. Podría necesitar hacer lo mismo incluso con correos recibidos de personas que conoce. Manténgase del lado seguro: No abra adjuntos sospechosos y no haga clic en los links, especialmente los que le piden descargar software para "leer este adjunto". Tenga cuidado: pida al remitente confirmación.

7

No habilite las macros en documentos adjuntos recibidos vía correo.

Cuando reciba un documento de Word o un libro de Excel por correo y le pida "habilitar las macros" ¡No lo haga!. El Malware se propaga de esta forma (Por ejemplo, Osiris Ransomware). Si el archivo está infectado y usted permite a las macros ejecutarse, está inadvertidamente permitiendo la instalación de ransomware y la encriptación de su información.

8

No le de a los usuarios de su computadora más privilegios de los que necesita.

Si su usuario (el login de su dispositivo) tiene privilegios de Administrador podría crear un desastre en todas las computadoras y dispositivos de su red. No apague UAC (User Account Control) en Windows tampoco: la capa extra de seguridad no está de más.

9

Use nuevas características de seguridad en sus aplicaciones de negocio

Aplicaciones esenciales de negocio, como Microsoft Office 2016, ahora incluyen una opción para "Bloquear Macros en archivos descargados de internet". Esto es útil, asegúrese que está activado en su dispositivo.

10

Prevenga que programas se ejecuten desde los folders AppData y LocalAppData

Muchos programas de Ransomware (por ejemplo, Cryptolocker) copian archivos a estos folders y se ejecutan sin detectarse, tratando en enmascararse como procesos estándar de Windows. Puede crear reglas específicas dentro de su instalación de Windows para bloquear la ejecución de archivos desde estos folders.

NO SE CONVIERTA EN PARTE DE LA ESTADÍSTICA

Muchas víctimas de ataques de ransomware piensan que nunca les pasará a ellos. Y luego, cuando pasa, estos individuos no están preparados para resistir el ataque y pagan miles de dólares en rescates. Con algunos simples pasos y protección robusta contra ransomware de compañías como Acronis, usted puede proteger su información valiosa de la forma más eficiente y rentable.

Acronis

Para más información visite **www.acronis.com**