[1]

Cómo proteger tus dispositivos de ataques informáticos

Imatge:

La semana pasada hubo un ataque masivo mediante código malicioso de tipo *ransomware*, que ha afectado a un gran número de organizaciones a nivel estatal. Aunque el COAC no se ha visto afectado, informamos a los colegiados de las posibles problemáticas que el ataque puede ocasionar.

El *ransomware*, de la variante WannaCry, puede infectar a los equipos informáticos que utilizan sistema operativo **Windows**. Una vez infectado un ordenador, el virus se distribuye al resto de máquinas Windows que haya en la misma red.

Las medidas de prevención deben partir del usuario, ya que actualmente no hay un programario de desinfección o un sistema que proteja completamente de esta amenaza.

Las formas por las que un ordenador se puede infectar son las siguientes:

· Phishing mediante correo electrónico que contenga un enlace a una web o un fichero adjunto.

· Accediendo a páginas web infectadas con un navegador sin actualizar o que tenga plugins desactualizados o no seguros.

Los sistemas afectados (de los que ya hay una actualización de seguridad disponible en Microsoft), son:

· Microsoft Windows Vista SP2
· Windows Server 2008 SP2 i R2 SP1
· Windows 7
· Windows 8.1
· Windows RT 8.1
· Windows Server 2012 i R2
· Windows 10
· Windows Server 2016

Consejos y recomendaciones
El Centro de Seguridad de la Información de Catalunya (CESICAT) ha publicado los siguientes consejos:

·Actualiza el sistema operativo Windows a su última actualización para una protección adecuada frente a esta ciberamenaza.

·Asegúrate de que los archivos adjuntos son documentos que estabas esperando. En caso de que no estuvieras esperando estos ficheros, se recomienda eliminar el correo recibido y no abrirlo por precaución a infectar el ordenador.

·Mantén la versión de antivirus actualizada a la última versión, así como los complementos de seguridad y cortafuegos.

·Realiza copias de seguridad de los archivos con regularidad. Un ataque *ransomware* no supone un problema siempre que se mantenga una copia de seguridad de sus archivos.

·Utiliza un servicio antimalware eficaz. Hay herramientas de seguridad que identifican el comportamiento específico de un *ransomware* y bloquean la infección antes de que pueda causar daños.

·En caso de resultar afectado por un ataque de tipo *ransomware* se recomienda apagar el ordenador y desconectarlo de la red. Posteriormente, ponte en contacto con un técnico informático.

En **esta página web** [2] encontraréis más información y una explicación más detallada sobre

este virus.

13/05/2017

Tornar [3]

Links:
[1] http://coac.arquitectes.cat/es/apoyo/actualidad/ataque-masivo-ransomeware
[2] https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2091-ccn-cert-bp-04-16-ransomware-1/file.html
[3] http://coac.arquitectes.cat/es/javascript%3Ahistory.back%281%29