Publicado en Madrid el 21/06/2016

Cómo disminuir el impacto de los ciberataques

Una rápida detección y respuesta es clave para minimizar las consecuencias de los ataques a los sistemas informáticos corporativos

La era digital ha permitido que compartir archivos, almacenarlos o simplemente acceder a ellos, se haya convertido en una acción completamente rutinaria, tanto que la mayoría de las veces olvidamos que tenemos información personal o confidencial almacenada en servidores o en la nube. Somos lo suficientemente confiados como para creer que estos medios de almacenamiento son tan seguros como para mantener a salvo todos nuestros datos, pero… ¿realmente lo son?

Lo cierto es que gran parte de los usuarios no tienen por costumbre pensar en el factor seguridad; el desconocimiento en este tema puede ser fuente de riesgos tanto en su entorno personal como laboral. Mientras tanto, algunos delincuentes están dedicados exclusivamente a buscar las vulnerabilidades de los sistemas e idear métodos fraudulentos para apoderarse de los datos guardados y buscar a través de ellos algún tipo de beneficio económico. En los últimos meses ha dado pintorescos titulares el robo al Banco Central de Bangladesh, una operación que gracias a una errata de los “hackers” se detectó y se pudo detener cuando ya habían sustraído casi cien millones de euros.

Javier López, experto en ciberseguridad en Ondata International, sostiene que “la conciencia sobre ciberseguridad debe cambiar; sentimos que no corremos peligro cuando cada día los ataques son más precisos y sofisticados. Una prueba de ello son las noticias, cada vez más frecuentes, sobre robo de datos, hackeo de cuentas y pérdidas de grandes sumas de dinero causadas por los ciberdelincuentes. El factor clave para minimizar el impacto de los ataques es poder detectarlos rápidamente y responder de forma inmediata, antes de que se pierdan datos críticos de forma irremediable. Es fundamental implantar soluciones como Encase Cybersecurity, que automatiza este proceso reduciendo drásticamente el tiempo de respuesta en comparación con el análisis manual del incidente”. (Ver diagrama Cronología de respuesta).

Pérdidas millonarias

En los últimos meses se han dado a conocer públicamente diversos casos de brechas de seguridad en los sistemas de almacenamiento, que han ocasionado la pérdida de millones de dólares. El más conocido es el ocurrido al Banco Central de Bangladesh, donde los hackers, aprovechando una vulnerabilidad en la seguridad del sistema de esta entidad, desplegaron malware a los servidores del banco e hicieron transacciones fraudulentas durante dos semanas sin levantar sospechas, robando aproximadamente 80 millones de dólares.

Otro método que están utilizando los ciberdelicuentes es el secuestro de información. Esta situación le ocurrió al Hospital de Kentucky, donde unos hackers accedieron a la red del hospital y encriptaron todos los archivos con los historiales médicos de los pacientes. El nivel de encriptación que suelen utilizar los hackers para este tipo de acciones es muy elevado y no puede ser resuelto por los técnicos, por lo que la única solución para recuperar los datos es pagar un “rescate”, que en el caso del hospital ascendió a 17.000 dólares.

Cómo responder a los ciberataques de forma inmediata

Los casos mencionados son sólo una muestra de las diferentes situaciones irregulares que han ocurrido recientemente, pero ¿se podrían haber minimizado las consecuencias de los ataques? Ciertamente, es muy difícil tener una red 100% protegida, pero sí se puede disminuir el impacto de un gran número de incidencias si se incrementan los niveles de seguridad de las redes de las organizaciones. Los expertos estiman que para alcanzar niveles de protección adecuados, las empresas deben destinar al menos un 15% del gasto en proteger sus sistemas.

Desde el departamento de Ciberseguridad de Ondata International, se informa de que “existen herramientas como EnCase Endpoint Security que detectan los ataques que pueden sufrir las organizaciones, los evalúan y responden a ellos. Se trata de una tecnología que automatiza el flujo de trabajo necesario para dar respuesta a los incidentes. De este modo, se puedan tomar acciones sobre las amenazas detectadas de forma inmediata”.

Las empresas suelen disponer de herramientas SIEM (Security Information and Event Management) para detectar software malicioso en la red. EnCase Endpoint Security es una solución que combina la protección de las herramientas SIEM existentes con la inteligencia de EnCase Cybersecurity y EnCase Analytics, a fin de obtener visibilidad completa de lo que ocurre en cada terminal y con el objetivo de proporcionar control a través de toda la cadena de ataque. Esto permite disminuir el tiempo de respuesta de meses a días. La plataforma es programable y provee respuesta automatizada. Permite detectar riesgos, amenazas y actividades anómalas con perfiles creados a medida para cada entorno.

La respuesta rápida ante un incidente de seguridad es un factor clave para disminuir el impacto de una acción maliciosa. Este software además permite al personal de TI de las empresas identificar rápidamente si los datos sensibles se encuentran en riesgo, de modo que se puedan priorizar aún más las acciones de respuesta y decidir los próximos pasos a seguir.

Acerca de Ondata International

Ondata International (www.ondata.es) es una empresa española especializada en informática forense, seguridad informática y recuperación de datos, que cuenta con veinte años de experiencia y con presencia en diez países de Europa y América. En el ámbito de la seguridad informática, Ondata es global partner de Guidance Software y da soporte a su plataforma EnCase Cybersecurity, utilizada por numerosas empresas y entidades gubernamentales para dar respuesta inmediata a los ataques realizados a sus sistemas, servidores y terminales de usuario.

Para más información: http://www.ondata.es/

Datos de contacto:
Carlos Sánchez
914174468

Nota de prensa publicada en: Madrid

Categorías: E-Commerce Software Ciberseguridad