Segundo trimestre 2017

http://www.redseguridad.com/actualidad/editoriales/lecciones-bien-aprendidas

¿Lecciones bien aprendidas?

Es momento de reflexionar y sacar conclusiones que ayuden a evitar una situación similar a la producida por WannaCry

El pasado 12 de mayo hizo su aparición en todo el mundo una nueva variante de ransonware, bajo el nombre de WannaCry, que puso en jaque a los expertos y profesionales de ciberseguridad del planeta. Por el camino dejó un reguero de **más de 350.000 equipos infectados de cerca de 180 países,** y un impacto para las empresas españolas cuantificable, según las estimaciones de la asociación ISMS Forum, en cinco millones de euros, con un coste por equipo afectado de unos 500 euros.

Ante este panorama, es momento de reflexionar y sacar conclusiones que nos ayuden a evitar una situación similar a la vivida hace unas semanas. Lo primero que conviene resaltar es que las grandes compañías han de revisar planes y protocolos de seguridad porque, aunque los que existen sirvieron para atenuar la situación y evitar un impacto mayor, lo cierto es que hay aspectos que mejorar. Por otro lado, el ataque también puso de manifiesto que muchas otras empresas no tienen implementado ningún plan de seguridad, ni medidas de control que eviten que estas amenazas pongan en riesgo su información, con el consiguiente daño que esto puede suponer para su negocio.

Por ello, se debe valorar, especialmente entre las pymes, que son las más vulnerables, **la implantación de un plan de seguridad apoyado en profesionales de TI y herramientas tecnológicas que ayuden a anticiparse y mitigar estas amenazas.**

En segundo lugar, es fundamental que las compañías actualicen sus sistemas con los últimos parches de seguridad que los fabricantes de software ponen a su disposición y los desplieguen lo antes posible en todos sus sistemas, incluidos los dispositivos móviles. La complejidad a la hora de aplicar esta medida cuando se trata de múltiples equipos o tecnologías complejas no debe ser una excusa para mantener vulnerabilidades.

Pero nada de esto tiene sentido si el eslabón más débil de la cadena de seguridad, el factor humano, comete el error de ejecutar el malware. Precisamente, la masiva expansión de WannaCry fue debido a este hecho. Hay que seguir insistiendo en la necesidad de formar a los empleados en cuestiones básicas relacionadas con la ciberseguridad, como no abrir archivos adjuntos de remitentes desconocidos o sospechosos.

Todo ello conduce a un concepto que desde estas páginas defendemos desde hace años. Se trata de fomentar la seguridad integral en las organizaciones, uniendo tanto la física como la lógica bajo una misma estructura. Para seguir insistiendo en este mensaje, **las revistas RED SEGURIDAD y SEGURITECNIA organizan IX Encuentro de la Seguridad Integral (Seg2),** un foro que arrancó en 2009 y que se ha convertido en el encuentro de referencia para la convergencia de la seguridad en nuestro país. En esta ocasión, la cita se centrará en la encrucijada normativa actual de trasposiciones y reformas, como las del Reglamento de Protección de Datos, la Ley PIC, el futuro Reglamento de Seguridad Privada o la Directiva NIS. Además, durante el evento se entregará la **novena edición de los Trofeos de la Seguridad TIC.**

Medidas como las comentadas son las que pueden y deben poner en marcha las organizaciones internamente para anticiparse a los ataques, **pero también es crucial fomentar la cooperación con las Administraciones y organismos públicos**. Afortunadamente, la prueba de fuego que fue la propagación del WannaCry en nuestro país también puso de relieve el buen funcionamiento de esta relación.