Expansión

25 May, 2017

‘MustEducate’ contra ‘Wannacry’

Juan Pedro Moreno

Si como de un videojuego se tratase, y aplacada ya la bestia *Wannacry*, aplicados los antídotos y parches, cerradas las puertas, reclutados y conformadas legiones de hackers, antihackers y protohackers y realizado el recuento de bajas se podría dar casi por cerrada la última batalla de esta guerra moderna. Una batalla que –junto al terrorismo internacional y otras amenazas como el cambio climático– está llamada a ser la “nueva norma” del siglo XXI y la era digital.

Es momento de hacer balance y replantear la estrategia. Una de las primeras conclusiones es que, como en cualquier episodio bélico, el argumento se ha desarrollado entre seres humanos y no entre máquinas o entre máquinas y personas. Son seres humanos intentando aprovecharse de otros seres humanos, más desprevenidos o confiados, aprovechando sus debilidades, su ignorancia o su falta de preparación. Nada nuevo que no hayamos visto antes.

Sin menoscabar la importancia de la prevención y la rápida respuesta tecnológica, se ha demostrado que es el flanco humano –el relativo al empleado, usuario o ciudadano– el principal aliado del contagio y la posterior infección. Las personas desprevenidas se han expuesto al contagio y han contraído un virus que ha atacado a un órgano vital de la era digital: el tercer brazo tecnológico. Hoy en día ya no se puede sobrevivir sin acceso a la red, al teléfono móvil o al ordenador.

También estos días hemos visto cómo las compañías se han defendido y han superado el ataque, quedando indemnes o casi indemnes del contagio. ¿Cuál ha sido la principal razón? La cultura de prevención e involucración de todos los empleados en la protección e identificación temprana de la amenaza. Una “cultura de ciberseguridad que genere comportamientos ciberseguros” con el objetivo de fomentar entre todo el ecosistema de la compañía –empleados directos, indirectos, subcontratados, etc– una serie de principios y comportamientos ciberseguros con la máxima implicación del primer nivel de gestión de la compañía. Todo ello unido a una estrategia de utilización de soluciones tecnológicas tendentes a impedir y controlar el ataque, rodeando al empleado de fuertes muros y pantallas.

El empleado puede ser un aliado de los ciberatacantes si mantiene una actitud ingenua o desprevenida pero también puede ser el protagonista principal a la hora de combatirlos. ¿Cómo? Educando, formando y haciendo un seguimiento permanente del conocimiento y atención de las personas a esta amenaza. Con una cultura de prevención –bajo la premisa *MustEducate*– que convierta a una potencial víctima ingenua en un empleado formado y preparado para la defensa.

Para ello hay que realizar una constante inversión en concienciación y formación de la fuerza de trabajo en ciberprotección mediante un gran programa especializado. Un esquema que incluye cinco puntos básicos: comunicación, sensibilización, formación, experimentación y reconocimiento y medición.

Un programa de comunicación para que los empleados lo conozcan a todos los niveles y a través de todos los canales (información basada en vídeos orientados a comportamientos específicos del tipo *Make the Right Call*, para que toda incidencia de *Information Security* sea registrada y gestionada por los centros de operaciones de seguridad correspondientes, reconocimiento de emails sospechosos, protección de *passwords*, publicación en redes sociales...).

Concienciación

Un programa de concienciación o sensibilización destinado concienciar de las consecuencias derivadas de dar un click o conectarse a una web infectada. Programa de formación global y capacitación multicanal (compuesto de actividades de formación/concienciación mediante formatos audiovisuales atractivos). Un cuarto programa de experimentación y reconocimiento. Las evidencias nos confirman que los seres humanos cambiamos nuestros comportamientos cuando experimentamos en primera persona las consecuencias directas del resultado de nuestras acciones. El susto y el mal trago al abrir un correo de origen desconocido o pulsar un enlace de procedencia dudosa no se olvidan fácilmente. Por ello, hay que realizar pruebas reales con mensajes internos, con un proceso automatizado para reportar sospechas de *phishing* incluyendo “autoataques trampa” para identificar el grado de asimilación. Y, por último, desarrollar un modelo de medición porque medir es la única vía para conocer el punto de partida de la organización en relación a cómo son los comportamientos ciberseguros de los empleados.

En definitiva, hay que contar con una estrategia en constante evolución que se ajuste a las nuevas amenazas que puedan ir surgiendo en el futuro. Una estrategia orientada a contar con los mejores aliados de la seguridad de la información: nuestros propios profesionales. La educación y formación serán sus principales aliadas y *MustEducate* la nueva consigna.

Presidente de Accenture en España, Portugal e Israel