Texto
Cristina López Albarrán

GIANLUCA D'ANTONIO, MASTER EN CIBERSECURITY DEL IE Y CIO DE FCC

"Welcome to the Digital Jungle"

Las ciberamenazas persisten y son cada vez más sofisticadas y numerosas, y las empresas -al igual que los usuarios- deben estar prevenidos. Gianluca D'Antonio, Master en Cibersecurity del IE y CIO de FCC, dio inicio al Foro Ransomware refiriéndose a la "necesidad de aprender a vivir en la jungla digital que nosotros mismos hemos creado", y para ello debemos tomarnos "muy en serio la seguridad", tan en serio como que "es un negocio que mueve cantidades ingentes de dinero en todo el mundo". La mejor prueba de ello es que "la cotización de los bitcoins subió 600 dólares tan solo una semana después del ataque de WannaCry". El ransomware se ha convertido en un modelo de negocio millonario.

También hizo hincapié el CIO en el imperativo de hacer de la ciberseguridad un terreno atractivo para los jóvenes. En su opinión, las nuevas generaciones no quieren estudiar ciberseguridad. Para estos jóvenes, no es suficiente con tener conocimientos y experiencia, hay que fomentar aptitudes: dedicación, escepticismo, protección, colaboración, resolución de problemas y orientación a negocio. Muchas empresas a día de hoy buscan un CISO que no sea un técnico.

Pero no nos equivoquemos, esta falta de formación no afecta solo a los jóvenes, los mismos directivos de las empresas no están versados en la materia. Basta con analizar el reciente ataque a Equifax, del que se ha sabido que acceder a los datos críticos de la compañía era muy sencillo. "Y si la tercera empresa mundial de renting financiero funciona así.... Imaginaros qué está sucediendo en el resto de empresas", advertía. Por un lado se van anunciando nuevas alertas y por otro existe una inercia en el mundo empresarial hacia la desidia, es decir, una cierta dejadez a tener en cuenta estos riesgos. "Menos de 200 empresas en España tienen un responsable de seguridad", argumentaba. Ante este panorama veremos a ver qué pasa con los 'data breach' y GDPR. El plazo para adaptarse con obligatoriedad a la nueva normativa llega a su fin el 25 de mayo de 2018 y pocos han hecho los deberes. "En España muchas compañías no saben si tienen que tener un DPO o no, y faltan menos de ocho meses para que llegue el nuevo régimen regulador".

> **"La ciberseguridad requiere que toda la empresa se involucre"**

Buenas prácticas

Estamos viviendo en la jungla digital, un entorno en el que existe muy poca legislación pero en el que tenemos una dependencia creciente de los entornos TI y en el que vivimos una inmadurez en ciberseguridad y privacidad. En este escenario, muchos factores son gestionables o 'semigestionables' -como esa falta de regulación-, pero nos encontramos con otros que no se pueden controlar como las ciberarmas y el cibercrimen. ¿Tiene mi empresa la capacidad de resistirse al ciberataque de un país? La respuesta es no. Y menos aún si ha de enfrentarse sola a él. Por ello, D'Antonio mencionaba buenas prácticas para sobrevivir en esta selva, como abordar la ciberseguridad como una responsabilidad compartida, tener en mente el data governance y mejorar la gestión de cibercrisis reteniendo los servicios mínimos on premise. Todo ello siendo conscientes de que nuevas variantes de ransomware aparecerán con regularidad dando lugar al Ransomware-as-a-Service; hay que prepararse para el desastre y el data breach porque sucederán.

En definitiva, la ciberseguridad tiene ante sí varios retos como suplir esa falta de profesionales y capacidades; priorizar el asunto en la agenda política, económica y social; acoplar el nuevo horizonte digital con el riesgo tecnológico y vencer ese tabú que supone hablar de este tema. La seguridad ha de tenerse en cuenta, hemos de acostumbrarnos a que somos vulnerables a un ataque y afrontarlo de otra manera, al igual que cuando cruzamos una calle y miramos hacia los lados. ■