Texto
R. Contreras

ENRIQUE ÁVILA, DIRECTOR DEL CENTRO NACIONAL EXCELENCIA EN CIBERSEGURIDAD

"Apoyándonos en ecosistemas de ciberseguridad robustos podremos sobrevivir"

<< Enrique Ávila es un experto en ciberseguridad, agente activo en distintos foros profesionales. En esta ocasión acerca a Computing su punto de vista de la ciberseguridad como un asunto de interés general en el que tanto autoridades como ciudadanos somos eslabones de una cadena de contención frente al cibercrimen.

La pandemia ha traído consigo la proliferación de ataques de ransomware y phishing. ¿Está España preparada para salir bien parada de esta oleada?

España dispone de las estructuras y del conocimiento necesarios para poder enfrentarse a problemas de ciberseguridad tales como los que menciona, con cierto nivel de eficacia, pero responder a una pregunta tan directa, de forma cerrada, se me antoja imposible. Ni en relación con España, ni refiriéndonos a cualquier otro país. Al final, nos enfrentamos a acciones que pretenden la obtención de un beneficio, económico o de cualquier otro tipo, y, dependiendo de lo valioso de ese beneficio, se usarán más medios o una planificación más compleja, por parte del agresor, para maximizar sus objetivos.

Nuestra red pseudónima, en la que atribuir la responsabilidad es tan complejo, no es la más adecuada para poder luchar de manera demasiado eficaz contra el cibercrimen. Eso sí, ponemos todos los recursos disponibles para garantizar unos niveles de seguridad aceptables para la ciudadanía y las empresas de nuestro país. No está de más agradecer el enorme trabajo que, en este sentido, desarrollan Incibe, el CCN-CERT y el CNPIC, cada uno en su área de competencia, en favor de la protección de este dominio de ejercicio de nuestra soberanía.

No por ello dejaré de mencionar la necesidad de aceptar nuestra responsabilidad como ciudadanos. Hemos de aprender a aplicar ciertas medidas básicas de autoprotección en el ciberespacio, tal y como hacemos en nuestra vida analógica. Procrastinar en este asunto constituye un riesgo inaceptable, tanto individual, como colectivo.

¿Qué tipología de ataques está siendo la más frecuente?

Habitualmente, los que involucran a las personas en el desarrollo del ataque. No dejaremos de insistir en que somos los más vulnerables en la cadena de la ciberseguridad. No estamos biológicamente diseñados para operar con ventaja en el ciberespacio y solo apoyándonos en ecosistemas de ciberseguridad robustos y un mínimo de conocimiento y voluntad podremos sobrevivir en un entorno tan hostil como es este.

¿Qué acciones ha tenido que llevar a cabo el Centro Nacional de Excelencia en Ciberseguridad para gestionar esta situación?

Participamos en la formación avanzada de miembros de nuestras FCSE en materia de lucha contra el cibercrimen y análisis forense de escenarios digitales. El talento es difícil de detectar, de formar y, lo más grave y peligroso para la ciberseguridad, de retener. Más aún en un escenario en el que dicho talento muy especializado se busca en un mercado muy necesitado del mismo. La información, convertida en conocimiento e inteligencia, junto con el talento, son los dos activos de mayor valor para las organizaciones del siglo XXI. Detectarlo y retenerlo configura un enorme campo de batalla a nivel global, en el que los Estados, lamentablemente, tenemos dificultades para competir.

¿Cómo están respondiendo las empresas españolas en términos de ciberseguridad?

Depende del tamaño y del sector. Hay sectores que, ya hace años, se dieron cuenta de que su negocio dependía de la ciberseguridad. El sector financiero es un claro ejemplo. Lamentablemente, gran parte de nuestro tejido productivo se encuentra conformado por pequeñas y medianas empresas que desarrollan su actividad en sectores de bajo valor añadido, y para los que la ciberseguridad es más un gasto que una inversión. Muchas veces, ni siquiera llegan a ser conscientes de por qué, de la noche a la mañana, perdieron su cartera de clientes o qué pasó para que su información de negocio acabara en un bloque de información cifrado e inservible, sin posibilidad de recuperación y provocando el cese de la actividad. Tenemos, aún, que hacer mucha labor de concienciación en estos sectores, así como proveerles de herramientas para que puedan abordar con ciertas garantías el necesario cumplimiento normativo en esta materia.

¿La masificación del teletrabajo,cómo complica la gestión de la seguridad?

Cuantos más puntos de acceso activos tienes en un perímetro de seguridad, mayor es el riesgo de una intrusión no autorizada o de una exfiltración de información dolosa o culposa. Eso creo que es indiscutible. Los accesos a redes internas no preparadas para ello, porque estaban diseñadas poniendo el peso en el aislamiento de servicios en la intranet corporativa (muchas veces irreales), configuran en la situación actual un escenario que me atrevo a calificar de 'pesadilla'. Creo que, en un futuro próximo, seremos realmente conscientes de las pérdidas que habremos de sufrir por no haber sido previsores en este sentido. Ha llegado el momento de modificar ciertas estructuras que, aunque apoyadas en la tecnología, son ineficientes desde el punto de vista productivo y social. El teletrabajo, espero, ha llegado para quedarse y tendremos que trabajar mucho para que sea implementado de forma correcta y con las adecuadas medidas de ciberseguridad.

Las redes españolas están resistiendo al reto del confinamiento. ¿Qué acciones de protección requieren de forma adicional?

Si nos referimos a las operadoras, creo que pertenecen a ese sector para el que la ciberseguridad constituye parte de su ADN. Disponen de equipos y estructuras de mando y control especializados que, según mi opinión, configuran una potente herramienta, aunque no por ello podamos sucumbir a la tentación de considerarla invulnerable. Este juego es dinámico y afecta a un ecosistema. Y uso este término de forma consciente para que quede clara su enorme complejidad, interdependencia y dinamicidad. Si no asumimos esas tres características, tendremos un problema porque, gobernar la complejidad, es un reto al que solo podemos enfrentarnos a partir del desarrollo de capacidades prospectivas y de generación de inteligencia al más alto nivel. ■

"Hemos de aprender a aplicar ciertas medidas básicas de autoprotección en el ciberespacio, tal y como hacemos en nuestra vida analógica"