ENRIQUE DOMÍNGUEZ. DIRECTOR ESTRATÉGICO DE INNOTEC. GRUPO ENTELGY

El factor humano, la última barrera en la defensa en ciberseguridad

La masificación en el uso de los nuevos dispositivos, la hiperconectividad o la falta de concienciación sobre los riesgos y amenazas que se ciernen en el ciberespacio dejan al descubierto algunas de las más importantes brechas de seguridad en las organizaciones. En muchos de estos casos, esta situación incluye errores humanos cometidos por desconocimiento o desinformación de los propios empleados. Para invertir este escenario, la sensibilización y concienciación en ciberseguridad de todo el personal juega un papel fundamental. Es preciso que todos ellos conozcan y apliquen buenas prácticas en el uso de los dispositivos y soluciones tecnológicas y no solo en su lugar de trabajo, sino también en su ámbito personal.

Grupos organizados

El cibercrimen dejó de ser una cuestión de aficionados para convertirse en algo propio de grupos organizados hace ya algún tiempo; verdaderos profesionales que dedican su tiempo y sus recursos a explotar las vulnerabilidades de seguridad en todos los niveles. Secuestro de ordenadores (ransomware), robo de información clave; fraude online, estafas electrónicas, suplantación de identidad o ataques web contra la imagen y reputación de una firma, son delitos que afectan diariamente a las organizaciones. En ocasiones, no porque no se considere la ciberseguridad como algo fundamental, sino porque se deposita la confianza en unas medidas de protección técnicas (software o hardware), que resultan insuficientes, dejando de un lado la pieza final (y además más vulnerable) del engranaje: el factor humano.

Shutterstock / Sfio Cracho

Prueba de ello son las numerosas empresas que culpabilizan a las personas, indicando que buena parte de sus incidentes de seguridad se deben a un error humano. Bien es cierto que, debido a un entorno de control insuficiente, las personas se están convirtiendo en el blanco predilecto para los ciberdelincuentes quienes, valiéndose de diversas técnicas y modalidades de ataques, convierten a cualquier empleado en su objetivo directo o en la puerta de entrada a la organización, escalando privilegios en la red hasta alcanzar a su verdadero objetivo.

Blanco de cualquier atacante

En este contexto, nadie está exento de convertirse en el próximo blanco de cualquier tipo de atacante: desde organizaciones criminales o empresas de la competencia (ciberespionaje

industrial), hasta aquellos cuyas motivaciones se mueven por venganza (como un extrabajador resentido, por ejemplo), por activismo o por el deseo de evidenciar las debilidades de una organización. Y lo hacen de muy diversas formas. Así, por ejemplo, algunos atacantes se valen de la ingeniería social –una técnica utilizada para obtener información a través de la interacción social, la manipulación o el engaño– para lograr que la víctima le dé información sin ser consciente de ello.

Otras víctimas han caído en la trampa del phishing o del spear phishing (técnica similar a la anterior, en la que a través de un correo electrónico, aparentemente confiable, y dirigido explícitamente a una persona, se le redirige a un sitio web falso y con gran cantidad de malware).

Otros métodos muy en boga son el conocido como «Fraude del CEO» (un empleado de alto rango, o el contable de la empresa, con capacidad para hacer transferencias o acceso a datos de cuentas, recibe un correo, supuestamente de su jefe, ya sea su CEO, presidente o director de la empresa. En este mensaje le pide ayuda para una operación financiera confidencial y urgente) o criptojacking (ataques dirigidos al robo de criptomonedas).

Buenas prácticas para una cultura de la seguridad

Sea como fuere, las empresas coinciden en admitir que el uso inapropiado de los recursos por parte de los empleados (incluidos los puestos de gerencia y con grandes responsabilidades) les hace vulnerables. La falta de concienciación, a todos los niveles, se convierte entonces en una de las causas últimas de las fallas de ciberseguridad.

Frente a ello conviene implantar programas de concienciación, formación y sensibilización a todo el personal y durante un tiempo continuado para que, a modo de lluvia fina, «empape» en el comportamiento de los usuarios y lleguen a interiorizar unas buenas prácticas en ciberseguridad, tanto en el ámbito profesional como personal. Pues sólo cuando las personas son capaces de cambiar su forma de actuar en su día a día (entorno personal) cambiarán sus hábitos en su entorno laboral.


Shutterstock / Haksim Kabakou

> «Uno de los errores de los programas de concienciación en ciberseguridad es que han sido realizados por técnicos que saben más de tecnología que de personas»

Programas como Firewall Mindset™ de InnoTec, empresa de ciberseguridad del grupo Entelgy, pueden convertirse en un aliado perfecto para provocar un cambio en el modo de actuar de todos los empleados, implementando en su quehacer diario las mejores prácticas. Para ello se utilizan las capacidades de Entelgy como inductor del cambio organizacional, juntando metodologías del trabajo con personas, historias impactantes desde un punto de vista emocional o storytelling. Evitando así uno de los errores comunes de los programas de concienciación en ciberseguridad, realizados y ejecutados por técnicos, que saben más de tecnología que de personas.

Y en todo esto juega un papel fundamental los directivos y altos cargos que deben estar comprometidos completamente con la ciberseguridad.

Deben ser los primeros en implantar las medidas en su actividad diaria, aceptando que existen riesgos y que cualquier desliz puede llevar consigo una pérdida en la información de su empresa, haciendo tambalear su futuro y el de sus empleados. ●