



“En el sector bancario la concienciación de empleados y clientes es algo primordial”

Tuvimos el placer de charlar con David Matesanz, Global CISO en Santander Asset Management sobre la concienciación en seguridad cibernética tanto por parte de los clientes como de los empleados y la ciberseguridad en el sector bancario.

CyberSecurity News (CsN): Una de las piezas clave para estar protegidos de posibles ciberataques es la concienciación de los empleados, ¿En el sector bancario hay un buen plan de concienciación?

David Matesanz (DM): La concienciación en ciberseguridad es algo que me ha sorprendido muy gratamente desde mi llegada al sector bancario. Todos los empleados tienen una cultura de riesgos bastante desarrollada, conciben el riesgo ciber como algo muy relevante. Adicionalmente, hay una gran sensibilidad desde la Dirección, lo que conlleva que medidas de seguridad que, en otros sectores, son impenables en la Banca se implementan rápidamente y todo el mundo entiende que son necesarias.

Hay campañas de concienciación temáticas, cursos online, charlas, simulacros de phishing...etc., todo de una manera muy constante, lo que hace que todos los empleados tengamos la ciberseguridad muy presente y no se entienda como una “moda” pasajera.

CsN: ¿Cuál o cuáles cree que son los fallos humanos, de seguridad, en que los trabajadores caen más fácilmente? ¿Qué se puede hacer para evitarlo?

DM: Los ciberdelincuentes cambian y evolucionan, los ataques son cada vez más sofisticados pero, al final, siempre aprovechan los mismos fallos: engañar a los empleados para que pinchen en un link o revelen información, contraseñas débiles, configuraciones vulnerables por defecto y falta de parcheo...

Caemos una y otra vez en los mismos errores, emails que nos dicen que tenemos un paquete que no tenemos, o que nos piden urgentemente que hagamos algo fuera de lo normal, o que nos ofrecen algo a cambio de que pinchemos en un link.

5 consejos para la ciberseguridad: “Protege tu información y tu equipo”, “Se discreto online y en público”, “Piensa antes de hacer click o responder”, “Mantén tus contraseñas seguras” y “Si sospechas, repórtalo”.

CsN: Los bancos y los servicios financieros se han convertido en unos de los objetivos preferidos de los ciberdelincuentes, ¿Cuáles son las principales amenazas que afectan al sector financiero?

DM: Los servicios financieros han sido desde siempre uno de los principales objetivos de los ciberdelincuentes. Allí donde haya dinero habrá siempre amenazas que intentan aprovechar todas las vulnerabilidades para manipular o vulnerar los sistemas de pago, realizar ataques dirigidos a altos cargos, o personal con capacidad de realizar transacciones económicas, o “simplemente” utilizar ransomware para secuestrar la información.

CsN: Los ciberdelincuentes han aumentado tanto en número como en nivel de sofisticación sus ataques contra entidades bancarias, y además han encontrado nuevas vías que van más allá de robar los datos de los clientes. ¿En qué consisten esas nuevas vías y cómo pueden prevenirse?

DM: “Los atacantes sólo tienen que aprovechar una vulnerabilidad una vez, mientras que nosotros tenemos que defender todas las vulnerabilidades todo el tiempo”. Cada vez usamos más servicios digitales, y tenemos más dispositivos conectados. Las vías realmente las abrimos nosotros.

En cuanto a la sofisticación, la ciberdelincuencia se ha profesionalizado hasta el punto de que se ofrece como servicio al alcance de cualquiera. Existen auténticos modelos de negocio dedicados a la ciberdelincuencia. Esto es clave para entender



David Matesanz, Global CISO en Santander Asset Management

por qué el riesgo en ciberseguridad no para de crecer.

La manera de reducir este riesgo es defender todas las vulnerabilidades durante todo el tiempo o bien cerrar estas vías, y dejar de usar servicios digitales y estar hiperconectados, lo cual creo que no es una opción, o bien desarrollar toda una estrategia de ciberseguridad acompañada del soporte y el talento necesario.

CsN: Por último, ¿Cuáles son los retos del futuro que se prevén en el sector banca en cuanto a ciberseguridad?

DM: La digitalización, es el principal reto y la facilidad de uso y la velocidad son una prioridad.

El reto es estar en la cresta de la ola en todo momento, defender todas las vulnerabilidades todo el tiempo y adaptar nuestras defensas a la evolución de las amenazas y los atacantes. Se trata de una carrera de fondo y sin descanso.

No quiero terminar sin mencionar como reto, la creación y atracción de talento. Esto es un reto no solo del sector bancario sino de todo el país. Al final, no debemos olvidar que detrás de todas las tecnologías, sistemas, procesos, hay personas que requieren de una alta cualificación y que, a día de hoy, escasean. Si queremos estar a la altura de los ciberataques, debemos ser capaces de generar y atraer ese talento, y esto es algo que no se consigue a corto plazo. ■