



Ciberseguridad en entornos financieros, el reto que no cesa

Patrocinadores:





El sector financiero ante el reto digital, el cliente en el centro de todo

Como una rueda que no deja de girar, el sistema financiero lleva inmerso en una transformación digital sistémica desde hace más de medio siglo. Tanto es así que este desarrollo tecnológico ha favorecido la mecanización de distintas tareas de soporte a la actividad financiera, como la dispensación automática de

efectivo, pero, también, ha marcado el movimiento hacia un negocio basado en el conocimiento y en el análisis de la información donde el cliente es el núcleo del negocio.

Así, y a lo largo de todos estos años, se han dado pasos de gigante en innovación con el desarrollo de soluciones tecnológicas destinadas

a la informatización de los sistemas de gestión (mainframes), el almacenamiento de la información, comunicaciones corporativas, ofimática y servicios web, auspiciados, estos últimos, por ese gran descubrimiento que ha sido Internet. Pero también, como decíamos, y por el deseo de evolucionar desde un sistema estático y me-

ramente transaccional, basado en la operación, hacia otro más inteligente asentado en el conocimiento del cliente y en su relación con la entidad, se ha apostado fuerte por tecnologías que permitan optimizar el servicio y la calidad ofrecida a los usuarios. En este punto, tecnologías como Big Data y Analytics, Inteligencia Artificial, Machine Learning, Blockchain o Biometría se han integrado a la perfección en las entrañas tecnológicas de los sistemas financieros, adaptándose por entero a las nuevas demandas y promoviendo una eficiencia operativa sin precedentes de

para a mantener un concepto "Open Banking" y de omnicanalidad permanente.

LIDERANDO LA TRANSFORMACIÓN DIGITAL

En este punto, y con la innovación tecnológica por bandera, el sistema financiero actual contempla una [estructura heterogénea](#) en la que convergen instituciones financieras monetarias (entidades de crédito, establecimientos financieros de crédito, entidades de pago electrónico u organismos de autoridad bancaria como el Banco Central Europeo o el Banco de España) junto a otros inter-

mediarios no financieros (Sociedades de Valores, Fondos de Capital Riesgo, Fondos de Titulación...), auxiliares financieros y empresas de seguros. Todas ellas, conviven a su vez con otras entidades que, como en el caso de las Fintech y, posteriormente, las BigTech, Neobancos y empresas de telecomunicaciones (Telecos) utilizan la tecnología para ofertar servicios financieros diferenciadores y que durante los últimos años han experimentado un auténtico boom, propiciado por una oferta disruptiva pero también por unas exigencias regulatorias mucho más livianas.

Por todo ello, el sector financiero necesita seguir avanzando como un gran bloque unido y cohesionado, y que, además, cumpliendo con los principios básicos de la protección al consumidor, estabilidad financiera e integridad del mercado, adaptar su modelo de negocio a una nueva realidad. Para ello, esta entente requiere de un entorno competitivo adecuado que le permita progresar hacia un hábitat flexible, donde se favorezca la innovación, y se limiten prácticas como la intermediación financiera no bancaria (shadow banking), que pueden suponer una amenaza potencial para la estabilidad financiera a largo plazo.

EL FARRAGOSO MUNDO DE LAS NORMATIVAS

Tras la crisis financiera global que comenzó en 2007, se produjo una revisión de los estándares regulatorios globales del sector financiero para que las entidades adoptasen una serie de políticas y estrategias para mejorar su resistencia a los

La nube se ha instaurado como una tendencia en alza en el sector financiero. Sin embargo, para mantener seguros los datos confidenciales la salvaguarda de esta información se convierte en un reto



Desde hace tiempo los ciberataques más exitosos están siendo ejecutados por redes criminales altamente profesionales

riesgos que pudiesen surgir en el ejercicio de su actividad. Dichas medidas, que fueron lideradas por el G20 y el Consejo de Estabilidad Financiera (FSB), se centran principalmente en tres aspectos básicos: solvencia (Basilea III), supervisión (MUS) y contabilidad (IFRS9).

Adicionalmente, el sector financiero tiene que lidiar también con otras leyes que marcan requisitos de liquidez y de capital más altos, como TLAC (a nivel global) y MREL (a escala europea); pruebas de resistencia internas como parte de sus procesos de gestión de riesgos, incluyendo los procesos de adecuación de capital y de liquidez (ICAAP e ILAAP) y otras relacionadas con la conducta, en materia de protección de los inversores y los clientes, como MIFID II y PRIIP.

En lo que respecta a la protección de datos, una de las [prioridades](#) que la Unión Europea se ha marcado en su haber, el Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) o la regulación europea sobre servicios de pagos electrónicos PSD2, han su-



puesto un antes y un después para un sector en el que la explotación de los datos se ha convertido en uno de sus principales activos. En este sentido, y desde la perspectiva de que la información personal y financiera de los clientes bancarios no pertenece a las entidades financieras ni a terceros, sino que es propiedad de los usuarios, estas organizaciones han tenido que avanzar en múltiples aspectos para adecuarse a una regulación estricta que sanciona cualquier brecha de seguridad.

UNA AMENAZA REAL: LOS DATOS EXPUESTOS

Llegados a este punto, no hay duda de que los datos de los usuarios son un activo de un valor incalculable.

Sin embargo, y por el alcance que representan, la actividad cibernética maliciosa supone una amenaza continuada para el sector financiero

que, en los últimos años, se ha convertido en un ansiado objetivo para los ciberdelincuentes. Tanto es así, que los incidentes de seguridad, tanto online como offline, han aumentado en número y sofisticación, y no solo por parte de ciberdelincuentes o grupos hacktivistas, sino también por parte de los Estados, según el Informe [Ciberamenazas y Tendencias 2019](#) de CCN-CERT.

A este respecto, se estima que, a nivel mundial, en 2021, el crimen cibernético tendrá un coste para las organizaciones de más de 6.000 millones de dólares anuales, frente a los 3.000 millones de dólares que supuso en 2015, según [el Informe Oficial Anual sobre Ciberdelincuencia de 2020](#) de Cybersecurity Ventures. Dicha cantidad incluye el daño y la destrucción de datos; el dinero sustraído; la pérdida de productividad; el robo de propiedad intelectual, de datos personales y de información financiera; la interrupción del curso



normal de los negocios después de un ataque o el daño a la reputación de la marca, entre otros.

Y es que, a pesar de que desde hace años las entidades financieras han incrementado sus inversiones en seguridad, inyectando de media entre el 11% (bancos) y el 10% (entidades no bancarias) de sus presupuestos, según un estudio de [Deloitte](#), la realidad evidencia que los ciberataques, sobre todo los destinados al robo o alteración de datos personales, se han incrementado.

Así, en los últimos años, el mundo de las finanzas ha quedado particularmente expuesto ante ataques dirigidos, DDoS y ransomware. Asimismo, se ha observado un fuerte aumento en el número

de usuarios infectados por troyanos bancarios (Emotet), malware móvil (open banking), phishing dirigido, ingeniería social, ataques 'watering hole' y de puertas traseras que han permitido a los delincuentes cibernéticos infiltrarse en los sistemas de información con total confidencialidad. Los ataques XSS (Cross Site Scripting) como SQL Injection que explotan las vulnerabilidades en los navegadores o servidores web, también representan una amenaza importante.

Además, en el caso de las instituciones bancarias, los cibercriminales han seguido desplegando técnicas tradicionales como la manipulación física de los cajeros automáticos (ATM), el robo de

datos de tarjetas de pago y cuentas bancarias en línea, y la clonación de tarjetas de crédito.

Ante tal proliferación de ataques, muchas empresas han movido ficha, recurriendo a soluciones perimetrales, como firewalls tradicionales para intentar frenar esta escalada de ataques. Sin embargo, ha quedado demostrado que este tipo de tecnologías, por sí mismas, no son suficientes para plantar cara a las nuevas técnicas de ataque, que requieren otra aproximación muy diferente.

Adicionalmente, la escasez de habilidades que golpea a un sector necesitado de profesionales especializados ha resultado ser también un gran desafío para los equipos de seguridad TI de las

La solución pasa por un enfoque multicapa

Desde hace tiempo, los hackers han puesto su diana en las personas, más allá de las infraestructuras. Es una simple cuestión práctica: ¿para qué perder tiempo y recursos atacando redes corporativas o endpoints si es mucho más rápido y sencillo doblegar la naturaleza humana?

A raíz de esta realidad, el mercado financiero se ha puesto manos a la obra para cerrar las brechas de vulnerabilidad y responder a las nuevas amenazas de

manera sistemática. Ser capaces de utilizar un enfoque integral de la ciberseguridad, comenzando por la identificación de los riesgos y las respuestas, se plantea como una forma de potenciar el rendimiento de estas organizaciones. Ya no basta con desplegar modelos tradicionales de seguridad estáticos basados en la detección, lo inteligente es evitar que estas amenazas afecten a los sistemas mediante técnicas de protección multicapa y proactivas. Por tanto, se hace

necesario aumentar el nivel de seguridad informática mediante una combinación de tecnología fiable (prevención de amenazas en tiempo real) inteligencia compartida y protecciones avanzadas en toda la infraestructura corporativa.

De igual modo, la nube se ha instaurado como una tendencia en alza en el sector financiero, dadas sus grandes ventajas, que la convierten en una plataforma idónea para migrar determinados procesos y ayudar a las instituciones

financieras a gestionar grandes cantidades de datos de forma rentable. Sin embargo, para mantener seguros los datos confidenciales y la salvaguarda de esta información se convierte en un reto, así como la necesidad de obtener visibilidad y control sobre miles de servicios cloud, sobre todo según las diversas regulaciones tienden a endurecer las condiciones y a exigir de las entidades mayor transparencia y niveles más altos de protección del consumidor.

empresas financieras. La buena noticia es que ya son muchos los que están trabajando en una mejor cultura en seguridad y, por supuesto, en una mayor inversión en educación, necesaria para formar a los empleados, la primera línea de defensa de cualquier corporación.

CUIDANDO LA TECNOLOGÍA, PERO TAMBIÉN EL COMPONENTE HUMANO

Las amenazas del mundo digital están en constante evolución, por lo que el entorno de seguridad corporativo debe avanzar en idéntica línea, o anticiparse, utilizando una serie de tecnologías que puedan asegurar una protección proactiva frente a estos peligros. En este sentido, los riesgos deben quedar dimensionados para tratar todas las áreas, desde la tecnológica hasta la humana.

A nivel de infraestructura tecnológica una defensa integrada, con las mejores soluciones de su clase, irá encaminada a proteger tanto el correo electrónico (spam, phishing, malware...) como la navegación web (filtrado URL, sandboxing, Ga-

En los últimos años, el mundo de las finanzas ha quedado particularmente expuesto ante ataques dirigidos, DDoS y ransomware

taway Web Seguro...) la nube (CASB, o tecnologías basadas en el nuevo concepto SASE), la red (firewalls, UTMs), o las estaciones de trabajo y los servidores, con tecnología EDR y EPP.

Otra técnica que ha demostrado su capacidad y ha permitido responder a las amenazas con mayor confianza y velocidad es la Inteligencia Artificial, y son cada vez más las empresas que recurren a ella para proteger sus infraestructuras. Sobre esta evolución, un [estudio de Capgemini](#) alude a que el 63% de las organizaciones desplegará IA en 2020 para mejorar la ciberseguridad, siendo su aplicación más popular la seguridad de la red. Adicionalmente, y además

de para proteger la red, las compañías, incluidas las entidades financieras, utilizan la IA para otros fines, como asegurar sus datos, salvar sus endpoints y desarrollar una mejor gestión de la identidad y el acceso, sin olvidar, su idoneidad para identificar y entender las intenciones del phishing y de los correos electrónicos fraudulentos.

Sin embargo, y al igual que ocurre con el Machine Learning, utilizado para monitorizar la actividad de cualquier ordenador a fin de detectar y bloquear automáticamente los procesos sospechosos antes de que ocurran, o el Deep Learning, empleado para realizar predicciones a partir del



conocimiento, estas tecnologías se han convertido en objeto de deseo para los cibercriminales más avezados. Desde hace tiempo, los ciberataques más exitosos están siendo ejecutados por redes criminales altamente profesionales que aprovechan estas tecnologías para explotar vulnerabilidades como el comportamiento de los usuarios o las brechas de seguridad, y así obtener acceso a sistemas y datos empresariales.

La biometría también se está convirtiendo en un gran aliado para la ciberseguridad. De hecho, las técnicas de autenticación biométrica como las huellas dactilares, el iris y la voz son extremadamente útiles para el reconocimiento de personas basada en rasgos de conducta o físicos.

Para proteger la información, además del uso de técnicas de análisis, aprendizaje e inteligencia de amenazas, contar con herramientas criptográficas que por medio del cifrado de los datos ayuden a garantizar la confidencialidad e integridad de la información financiera, será de gran ayuda. De hecho, estas tecnologías resultarán cruciales para cumplir con los requerimientos de seguridad en los entornos financieros y asegurar el cumplimiento, tanto a nivel normativo como de negocio. Por ello, la implantación de comandos criptográficos y de Tarjetas EMV, o la actualización de las Claves de los ATM's y el uso de la firma digital permitirán luchar contra amenazas como el phishing en el ámbito financiero. Por supuesto, tampoco

¿Te gusta este reportaje?

Compártelo en redes






hay que olvidar la tecnología de Blockchain, que emplea mecanismos criptográficos de seguridad para acceder, firmar y cifrar las transacciones, los bloques y su encadenado.

Por último, no hay que olvidar el componente humano que, como ha quedado verificado a lo largo de los años, es el eslabón más débil de la cadena y la principal causa de infracciones de datos. Y es aquí donde las compañías deben revisar sus protocolos de actuación y, por supuesto, nunca dar nada por sentado. Ninguna fuerza laboral, ni siquiera la más joven, lleva aparejada una conciencia innata de las amenazas a la ciberseguridad. ■



MÁS INFORMACIÓN

-  [Las API son ahora el objetivo de los ciberataques contra entidades financieras](#)
-  [El 41% de las familias de malware observadas en 2019 eran nuevas](#)
-  [Se disparan los ataques DDoS inteligentes centrados en la capa de aplicación](#)

**THE ART OF
CYBERSECURITY**



Presentamos el arte de proteger su nube híbrida

Cuando los entornos físicos, virtuales, cloud y de contenedores están protegidos de una manera sencilla y automatizada, la ciberseguridad puede ser una obra de arte.

Conozca cómo en www.theartofcybersecurity.com

Amenazas desconocidas detectadas
y detenidas en el tiempo por Trend Micro.
Creado con datos reales por el artista Brendan Dawes



EVA CRISTINA CAÑETE BONILLA, CISO DE UNICAJA BANCO

“Los modelos de seguridad tradicionales ya no tienen el efecto deseado”

En plena transformación digital, en un momento en que los usuarios demandamos un acceso a los servicios en todo momento y lugar, los bancos y los servicios financieros se han convertido en uno de los objetivos preferidos de los ciberdelincuentes. De los retos y amenazas a las que se enfrentan preguntamos a Eva Cristina Cañete Bonilla, CISO de Unicaja Banco.

La banca, los servicios financieros, son ahora digitales, móviles y cada vez más centrados en los clientes. A nivel de seguridad, ¿qué retos cree que está afrontando el sector financiero?

Sin duda alguna la Transformación Digital, el uso masivo de dispositivos móviles, el IoT o el Big data son retos importantes para la protección de nuestra información. Desde hace algún tiempo se nos viene demandando acceder a ella en cualquier momento y desde cualquier lugar.

Y no solo empleados o proveedores, también los clientes quieren relacionarse con su banco de este modo, provocando un alto impacto en la forma de protegernos. Por todo ello, los modelos de seguridad tradicionales ya no tienen el efecto deseado. Se hace imprescindible adaptarlos a la nueva forma de ser empresa.

Esto no va solo de un cambio en la estrategia de seguridad sino de un cambio en los departamentos de seguridad, que ahora más que nunca tienen que ser ágiles, flexibles y resilientes.



Cómo hacer frente a los nuevos modelos omnicanal donde se transfieren más datos entre sistemas que nunca.

La omnicanalidad habla de fronteras, o mejor dicho habla de su desaparición. Las empresas tenemos que estar preparadas para que consuman nuestros servicios desde cualquier lugar y en cualquier momento. El intercambio de información es incesante e imparable. Esto adquiere especial relevancia si pensamos que la mayoría estamos adoptando modelos de trabajo colaborativo, amparados en la Transformación Digital.

Lo que nos lleva a basar nuestra estrategia de seguridad en la protección del dato, con independencia de donde esté, quién y cómo lo consume.

Las amenazas internas en el sector financiero no solo proceden de los empleados o la cadena de distribución, sino de miles de clientes, ¿cómo se aborda este reto?

Las entidades llevamos formando y concienciando a nuestros empleados, ya que es la forma de prevenir que sean víctimas de engaños que puedan acabar provocando incidentes de segu-

ridad. Se trata de crear cultura de seguridad corporativa que redunde también en una mejora en la concienciación de los clientes, los cuales son objetivos de los planes de seguridad, formación y concienciación. Realizar consejos sencillos de seguridad, comunicados a través de los diferentes canales de interacción con los clientes, es el mejor modo de combatir este tipo de amenazas.

Las técnicas de múltiple factor de autenticación que garantizan que la persona adecuada accede a la cuenta correcta, ¿son imprescindibles en estos entornos? ¿se está haciendo uso de la biometría?

Aunque el uso de técnicas de múltiple factor de autenticación no está generalizado, es una tendencia al alza y en mi opinión, imprescindible. En especial cuando se consumen servicios en Internet, como pueden ser servicios de almacenamiento de información, espacios de trabajo colaborativo, etc.

Por otro lado, las entidades financieras estamos preparadas para ofrecer biometría como segundo factor de autenticación en el consu-

“La aparición de normativas en materia de seguridad supone una palanca para los departamentos de seguridad de las empresas”



mo de servicios bancarios. Observamos que esta adopción va al ritmo en el que los clientes poseen dispositivos móviles con estas capacidades, como no podría ser de otro modo. Con el tiempo, y gracias al uso de este tipo de móviles, acabará imponiéndose como mecanismo de autenticación.

¿Qué impacto han tenido normativas como GDPR, PCI DSS o PSD2?

En general, la aparición de normativas en materia de seguridad supone una palanca para los departamentos de seguridad de las empresas que le ayudan a visualizar su función, al tiempo que suponen un consumo en tiempo

y recursos muy importante. Y este impacto no se puede medir solo en términos de adecuación. Hay que contabilizar el impacto que tiene mantener esos cumplimientos. Por ello, hay que buscar sinergias y elementos comunes entre las normativas que nos apliquen minimizando los esfuerzos individualizados.

El uso de los marcos de controles de seguridad o framework que analizan la seguridad desde distintas perspectivas (legal, organizativa y técnica) y capacidades o dominios (gobierno, seguridad, vigilancia y resiliencia) facilitan la adecuación a diferentes normativas. Nos permiten aunar esfuerzos y aprovechar los requisitos comunes y no comunes de todas ellas. ■

¿Te gusta este reportaje?

Compártelo en redes



MÁS INFORMACIÓN

[Unicaja Banco](#)

[Unicaja Banco refuerza sus medidas de prevención](#)

[Medidas a adoptar por la banca móvil para garantizar la seguridad de las transacciones](#)



Tendencias de seguridad en el sector financiero

Sin duda, la tecnología es un habilitador para la evolución del sector financiero. Y ahora, en un momento en el que el impacto del COVID-19 lo ha trastocado todo, la tecnología adopta si cabe mayor importancia.

El sector financiero recurre a ella para proteger sus infraestructuras, avanzar en cumplimiento y en concienciación y, en definitiva, para prosperar en su carrera hacia la transformación digital.

En los últimos años, los servicios financieros como la banca móvil o la banca online han vivido una gran explosión de popularidad. De este modo, lo que antes eran tendencias ahora son realidades, y hoy casi el 100% de los servicios financieros dependen de la tecnología. Para hablar de cómo las nuevas tecnologías y servicios han acompañado y guiado la evolución de este sector, además de tratar otras cuestiones más actuales como el impacto del COVID-19; el estado del arte de la ciberseguridad; el efecto de normativas como PCI-DSS o PSD2; el peso de las amenazas externas e internas; la importancia de la formación y la concienciación; y lo que está por venir, desde el punto de vista tecnológico y de ciberseguridad nos acompañan en esta mesa redonda telemática Miguel Ángel Rojo, CEO de Botech; Nuria Andrés, Territory Account Manager de Forcepoint; Luis Suarez, Presales Engineer



“El impacto del teletrabajo ha sido elevado, pero también la importancia de contar con estrategias de resiliencia y ciber resiliencia. El sector financiero ha demostrado ser un alumno aventajado”

NURIA ANDRÉS, TERRITORY ACCOUNT MANAGER DE FORCEPOINT

de Kaspersky; Jesús Rodríguez, CEO de Realsec; y José de la Cruz, Director Técnico de Trend Micro. Su experiencia en la gestión comercial y técnica dentro de compañías fuertemente vinculadas al sector financiero nos ofrecen distintas perspectivas del presente, pero también de las tendencias que marcarán el avance de este sector en el corto medio plazo.

LA HUELLA DEL COVID-19

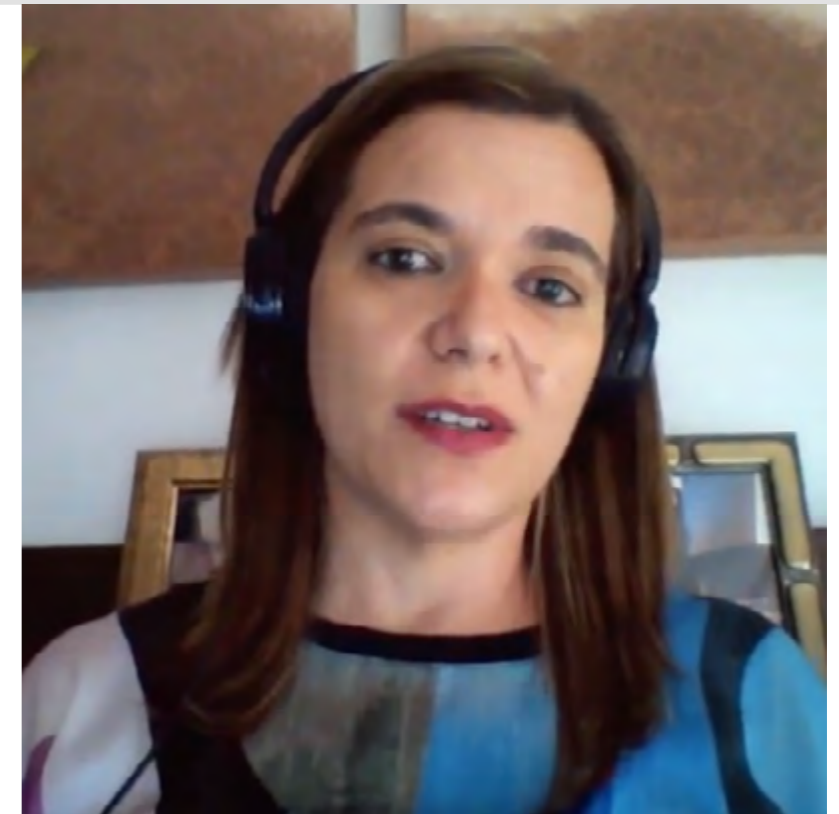
La cotidianeidad humana y empresarial ha quedado marcada por la injerencia del COVID-19, una realidad de gran alcance que ha impactado de lleno en todos los sectores, muy especialmente en el financiero.

A este respecto, Miguel Ángel Rojo reconoce que, en este tiempo, las transacciones online se han incrementado. El e-commerce ha crecido, a la par que los ataques de phishing y las campañas de malware dirigidas. “En dos meses y medio hemos realizado más análisis forenses remotos que en todo 2019”, lo que refleja una gran actividad, pero también el empleo de equipos mal securizados para trabajar. Pese a todo,

“el sector no se ha detenido; han surgido otros retos e inquietudes, dando paso a un nuevo entorno que está por llegar”.

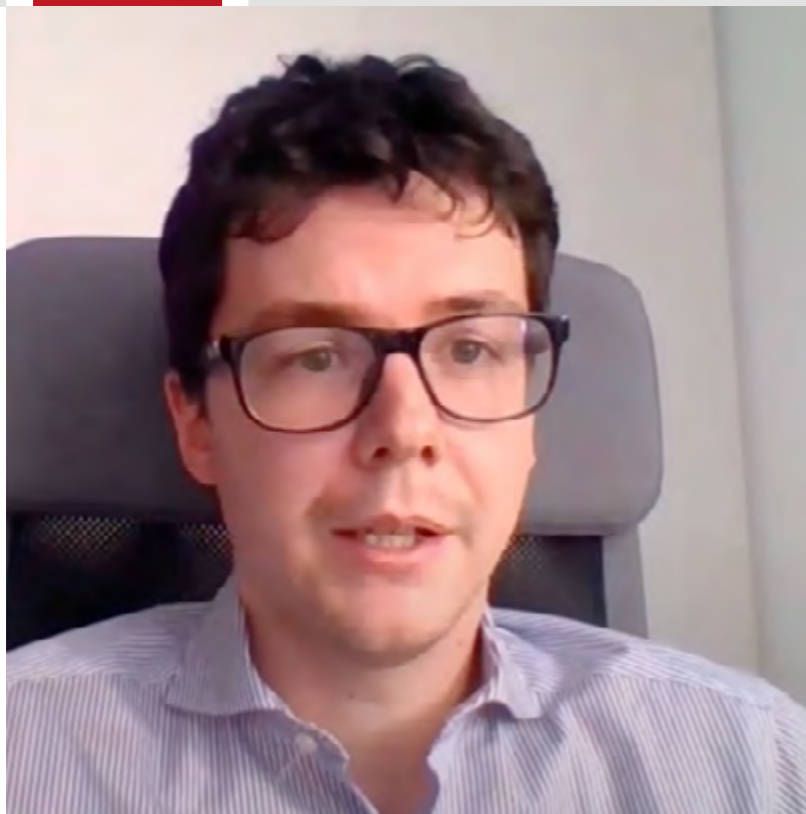
Para Nuria Andrés, el impacto del teletrabajo ha sido elevado, pero también la importancia de contar con estrategias de resiliencia y ciber resiliencia. Y aquí es “donde el sector financiero, ha demostrado ser un alumno aventajado”. No obstante, la nueva normalidad hacia la que avanzamos va a requerir acelerar la transformación digital. “En el sector bancario se va a apostar al 100% por el cloud. Esto va a conllevar que haya que repensar las estrategias de ciberseguridad, a fin de proteger el cloud desde el cloud”.

Además de la adopción del teletrabajo como principal medida asumida por las empresas, Luis Suárez destaca también la fuerte impulsión que han vivido las Fintech, “al tener los usuarios que realizar sus operaciones financieras de un modo online, a través de los aplicativos que la banca tiene disponibles”. Esta mayor dimensión digital también ha provocado un aumento de las campañas de phishing relacionadas con la pandemia, con campañas destinadas al robo de



datos, aprovechando la actualidad de los ERTES. “El hecho de que las entidades financieras hayan tenido que adoptar el teletrabajo ha derivado en un efecto llamada tanto para las organizaciones que se dedican al fraude como para los oportunistas”, expresa Jesús Rodríguez. Durante este tiempo han surgido falsas ONGs pidiendo aportaciones monetarias, supuestos doctores ofertando test sanitarios además de la concurrencia de todo tipo de mercancías fraudulentas. “El incremento del fraude, sobre todo en APPs, utilizando phishing y malware, ha estado y sigue estando a la orden del día”.

Pese a la gran tragedia que ha supuesto esta pandemia a nivel mundial, y el incremento de los ataques cibernéticos y la sobrecarga de servicios



“Las entidades financieras buscan proteger los dispositivos que interactúan externa o internamente, con tecnologías que incluyan servicios de inteligencia, herramientas de detección avanzada y otras para el cumplimiento”

LUIS SUÁREZ, PRESALES ENGINEER DE KASPERSKY

derivada del aumento de la actividad telemática, José de la Cruz, destaca, no obstante, un aspecto positivo: “Tecnológicamente, el COVID-19 se ha convertido en un habilitador, acelerando la transformación digital hacia soluciones nube, de navegación segura y, en general, hacia aquellas que permitan adoptar esta nueva realidad. Automáticamente toda la banca ha pasado a ser online”.

CIBERSEGURIDAD EN EL MUNDO FINANCIERO

El COVID-19 ha puesto de manifiesto la importancia de que las entidades financieras cuenten con una adecuada estrategia de ciberseguridad, a tenor del incremento de los ciberataques, sin embargo, ¿cuál es su grado de compromiso con la seguridad?

En comparación con otros verticales, el financiero va por delante en ciberseguridad, destaca Nuria Andrés. “Es un sector en el que pesa mucho la normativa. Además, la lucha contra ciberamenazas cada vez más sofisticadas y la obligación de proteger la información sensible de los clientes y la imagen de marca, los lleva a cuidar este aspecto”. Tras el impacto del COVID19 es de esperar que esta seguridad se acreciente, a fin de neutralizar todo tipo de amenazas y proteger la nueva superficie de ataque, que es cada vez más grande, el cloud.

Sin duda, el financiero es, para Luis Suárez, un sector concienciado con la ciberseguridad y cuyas necesidades van en línea con la situación existente. “Estas entidades buscan proteger cualquier dispositivo que tenga capacidad de interactuar, tanto a nivel interno como externo, a través de una combinación de tecnologías que incluyan servicios de inteligencia, herramientas de detección avanzada y otras destinadas a facilitar el cumplimiento. “Tener

una relación de herencia y sincronización con un servidor de gestión que esté en el cloud”.

Este alto nivel de capacitación es también destacado por Jesús Rodríguez. “Se trata de un sector que está muy bien preparado para luchar contra la ciberdelincuencia y el ciberfraude”. Los exigentes niveles de cumplimiento obligan a estas organizaciones a invertir en soluciones de seguridad que les permitan acatar normativas como PCI-DSS o PSD2, de cara a autenticar a sus clientes y evitar riesgos de suplantación de identidad. Lo mismo ocurre con otras soluciones para prevenir vulnerabilidades o luchar contra el phishing y el malware.

José de la Cruz traslada el liderazgo en seguridad del sector financiero a dos áreas principales: los servicios expuestos (banca online), que aglutinan gran parte de la inversión y están muy protegidos, y los servicios internos, importante foco de ataques y donde aún queda margen de recorrido. “COVID-19 ha acelerado la transición en algunas tecnologías. Se ha

“Cumplir con PCI DDS es complicado y costoso. No obstante, las entidades tienen que entender que se trata de proteger al usuario, salvaguardar la transacción e instaurar una marca de calidad ”

MIGUEL ÁNGEL ROJO, CEO DE BOTECH

pasado de modelos on premise a otros cloud, y también de arquitecturas de soluciones y de software monolítico a soluciones de microservicios, adoptando el modelo DevOps”.

En opinión de Miguel Ángel Rojo, el sector financiero lleva tiempo haciendo significativas inversiones en tecnología. De hecho, “puede ser considerado el avanzador tecnológico, sobre todo, en España”. Muy importante también es el tema reputacional, la importancia de salvaguardar la marca, entendiendo esta como un activo más a proteger. “Es un tema de confianza pura y dura, y en este terreno el financiero va por delante de otros sectores donde aún es necesario avanzar en reputación: de la marca, de sus directivos, etc”.

LA IMPORTANCIA DEL CUMPLIMIENTO

El financiero es un sector altamente regulado, con distintas y complejas normativas como PCI-DSS o PSD2 enfocadas en proteger los datos del consumidor y las compras o pagos online. Ahora bien, ¿cómo puede la tecnología ayudar a acatar estas directrices?

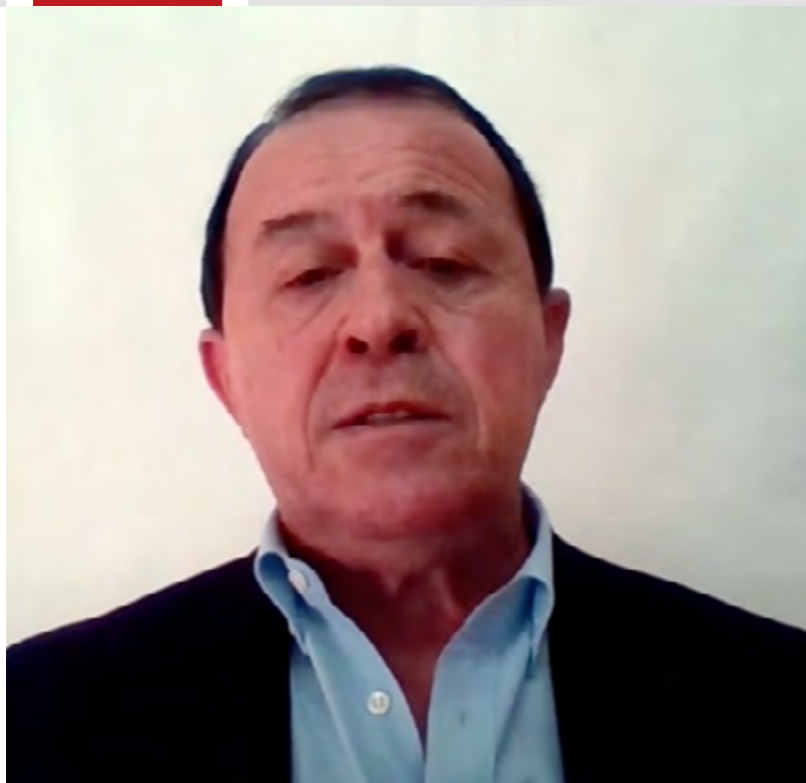
Al respecto de estas regulaciones, Luis Suárez destaca que se trata de normas dirigidas a optimizar la relación de las distintas plataformas de pago con las entidades financieras (PSD2), utilizando para ello un segundo factor de autenticación, o la monitorización de las modificaciones de ficheros con información relacionada con tarjetas de crédito (PCI-DSS). “En ambos casos deben protegerse las tecnologías, con detección temprana del fraude (telemetría) para cumplir con PSD2 y cubriendo los ATMs y realizando File Integrity Monitoring para PCI-DSS”.

“Bajo el punto de vista de la inversión, PSD2 supone un coste importante, razón que explica que vayamos por la segunda moratoria”, revela Jesús Rodríguez. No obstante, la autenticación de doble factor es totalmente necesaria para proteger tanto al usuario como a la entidad, y ya hay organizaciones que tienen implantadas soluciones para certificar a los usuarios. En lo que respecta a PCI DSS, su cumplimiento en el sector financiero es muy destacado, al contrario que en retail, donde aún queda mucho por hacer.



“Cuando se trabaja en entornos híbridos o multicloud, como es la realidad actual, destaca José de la Cruz, “una estrategia Cloud Security Posture Management ayuda a garantizar el cumplimiento tanto con regulaciones externas como con la normativa interna, y a aseverar que se siguen las mejores prácticas en cuanto a ahorro de costes, rendimiento o fiabilidad. En lo relacionado con PCI DDS, la supervisión de la integridad de los archivos (File Integrity Monitoring) permite afrontar los requisitos obligatorios de control de la seguridad.

Para Miguel Ángel Rojo, en España, el sector financiero está bastante concienciado con el cumplimiento. En el caso de PCI DDS, aunque su acatamiento es complicado y costoso, se



“Las infracciones más graves son las que se generan dentro de la propia entidad. Las organizaciones deben establecer procedimientos y soluciones para la prevención y contra la fuga de datos”

JESÚS RODRÍGUEZ, CEO DE REALSEC

avanza. “No obstante, aún queda por hacer. Las entidades deben entender que se trata de proteger al usuario, salvaguardar la transacción e instaurar una marca de calidad”. En lo que respecta a PSD2, es necesario trabajar en factores de autenticación como la biometría, que ofrezcan mayor cobertura y seguridad para evitar estafas como el carding o el autofraude.

La biometría, no solo física sino también la destinada a analizar el comportamiento del ser humano, es un concepto que también defiende Nuria Andrés. “PSD2 pone al usuario en el centro. La banca siempre ha invertido mucho tiempo y dinero en proteger sus propias infraestructuras, pero ha hecho poco foco en

el usuario”. A través del análisis del comportamiento del usuario es posible detectar situaciones de fraude en fases temprana, y así aplicar políticas de seguridad dinámicas, no estáticas.

AMENAZAS: EL USUARIO EN EL PUNTO DE MIRA

En un sector en el que la información exige un alto nivel de protección, la seguridad no es una opción. Pero, ¿de dónde provienen las principales amenazas? Las amenazas proceden tanto del exterior como del interior, y “ambas son importantes”, indica Jesús Rodríguez, no obstante, “las infracciones más graves son las que se generan dentro de la propia entidad”. En la actualidad, cuando la coyuntura actual ha obligado a dar cre-

denciales de acceso a muchos usuarios, es muy importante que las organizaciones establezcan procedimientos y soluciones para la prevención y evitar la fuga de datos, con independencia de instaurar mecanismos con otros propósitos”.

“Las entidades financieras han hecho mucho hincapié en proteger los servicios expuestos, pero no tanto los internos. Esta debilidad puede ser aprovechada por los clientes o por los usuarios internos, para lanzar ataques muy dañinos”, refleja José de la Cruz. Además, el hecho de que los ciberataques actuales sean multivector amplía la gravedad de su impacto. “Es preciso proteger todos los vectores posibles de ataque y hacerlo con una tecnología que sea capaz de adquirir inteligencia exterior y compartirla”.

“En el sector financiero se solía mirar de la muralla hacia fuera pero no de la muralla hacia dentro, cuando lo cierto es que puede haber problemas en ambos perímetros”. Con esta reflexión, Miguel Ángel Rojo incide en la importancia de no descuidar ningún recurso, dado que los vectores de ataque pueden ser múltiples. La concienciación es muy importante, también la del usuario final. “En España el usuario final es muy maduro, frente al de otros países, donde la bancarización está todavía por llegar y este se convierte en un vector de ataque”.

La amenaza interna es un factor que está creciendo. En este sentido, Nuria Andrés estima que las entidades financieras deben integrar programas y propuestas tecnológicas que permitan

“Al usuario no se le puede formar; hay que concienciarle, ayudándole entender y a diferenciar entre un ataque y lo que es el uso legítimo de una aplicación o de cualquier tipo de transacción ”

JOSÉ DE LA CRUZ, DIRECTOR TÉCNICO DE TREND MICRO

mitigarlas a través de la prevención, detección y respuesta. “Se trata de analizar el comportamiento de los usuarios internos para poder establecer políticas de seguridad dinámicas que prevengan la fuga de información. También es necesario proteger al usuario del propio usuario”.

La amenaza interna está ahí. No obstante, Luis Suárez se pregunta: ¿y qué hay de aquellos ataques que son externos, pero se camuflan o mimetizan como si fueran internos? “En el sector financiero este tipo de ataques son extremadamente peligrosos”. A este respecto, señala como ejemplo Carbanak. Diseñada para el espionaje, la extracción de datos y el control remoto, esta APT consiguió saltar la red interna de los bancos, estudiar el modo de actuar de las distintas entidades y usar dichos conocimientos para robar dinero.

CONCIENCIACIÓN Y FORMACIÓN COMO PUNTA DE LANZA

En un mercado tan sensible como el financiero, cómo de importante es la concienciación. ¿Es mayor que en otros sectores? “La concienciación es clave”, esgrime José de la Cruz. Un

usuario o un empleado concienciado puede convertirse en una medida para bloquear un ataque. A nivel interno hay que invertir en procesos de evaluación continua para comprobar que los planes de formación se cumplen y son efectivos, y en el caso de no serlo, trabajar más en esa habilitación. Al usuario, por el contrario, no se le puede formar, hay que concienciarle, ayudándole entender y a diferenciar entre un ataque y el uso legítimo de una aplicación o de cualquier tipo de transacción.

“La formación es vital para la seguridad y para el cumplimiento. La inversión en este aspecto será bien utilizada, aprovechada y de largo recorrido” considera Miguel Ángel Rojo. El concepto de la seguridad tiene que ser una máxima. Si un usuario interno ofrece información que luego es utilizada para cometer un asalto, las consecuencias económicas y de daño reputacional serán inmensas. Al usuario externo también hay que educarlo. Sufre un continuo bombardeo de información de entidades financieras que pueden confundirlo”.

Nuria Andrés señala al empleado como “la última barrera de defensa ante un ataque. Por



eso, debe estar formado, entrenado y la empresa debe constatar que de verdad está adquiriendo esos conocimientos”. Luego está el cliente. Aquí la banca tiene que contribuir a hacer partícipes a las personas de la importancia de la ciberseguridad, pero también es responsabilidad de la sociedad: “a nivel cultural, todos deberíamos ayudar en esa concienciación ante las ciberamenazas y los ciberdelincuentes”.

“La concienciación interna es básica y se está trabajando en ella”, corrobora Luis Suárez. “No se trata solo de proveer contenidos sino de ofrecer una metodología que ayude a reforzar esas habilidades”. En cuanto a la concienciación del usuario externo, esta es más complicada. El banco está limitado. Puede integrar

Principales áreas de inversión

El impacto del COVID-19 ha trastocado muchas cosas, entre ellas, la forma de trabajar. Ante este nuevo escenario, ¿cuáles van a ser las áreas fundamentales, desde el punto de vista tecnológico y de seguridad, en las que las organizaciones financieras van a invertir a corto medio plazo?

“El sector financiero va a reforzarse para adecuarse a esto que ha venido a denominarse como la nueva realidad”, opina Miguel Ángel Rojo. “De hecho, la inversión no se va a frenar; se va a reforzar”. En su opinión, será necesario realizar ajustes presupuestarios, sobre todo en lo destinado a la tecnología, pero se continuará, a fin de llegar al usuario. “El sector financiero va a seguir siendo la punta de lanza de la inversión tecnológica, como lo lleva siendo los últimos años, y el referente. Se trata de un mercado muy interesante”.

En opinión de Nuria Andrés, “ahora, más que nunca, hay usuarios por todas partes y los datos, también están en movimiento, han volado al cloud. El perímetro se ha

diluido como tal, y la nueva realidad acuñada por Gartner, SASE, alude a que el nuevo perímetro es el usuario”. En este sentido, razona Andrés, toca evolucionar para proteger la identidad del usuario, bajo un concepto de confianza cero, apostando por herramientas de seguridad as a service, y monitorizando el comportamiento del usuario para aplicar políticas de seguridad.

“Por la exposición de sus activos, una entidad financiera debe hacer un ejercicio de verificación: ver en qué punto se encuentra y definir dónde le gustaría estar”, precisa Luis Suárez. Para lograrlo debe apoyarse en soluciones tecnológicas que le permitan cubrir diferentes aspectos, desde detección avanzada hasta archivo de aplicaciones o más. No obstante, la falta de personal cualificado dificulta este hecho, por lo que debe confiar en fabricantes que ofrezcan tecnología y servicios para sacarle valor.

Cercano ya el fin de la última moratoria para cumplir con PSD2, “en los próximos meses el sector

financiero debe adecuarse para cumplir con esta normativa”, manifiesta Jesús Rodríguez, “y me consta que muchas entidades ya están trabajando en esa dirección”. Trascendental es también, bajo su parecer, poner foco en la prevención del riesgo y en la protección de la información y los datos, y, en última instancia, seguir luchando contra el phishing y el malware, “un mal contra el que llevamos años peleando y no terminamos de erradicar”.

Para finalizar, José de la Cruz señala el particular momento en el que se encuentra el sector financiero: en medio de una transformación digital (apuntando hacia modelos DevOps, de nube, multi-cloud) acelerada por la adopción de normativas y por los cambios que ha motivado la irrupción del COVID-19. “Ante todo esto, se hace necesario contar con soluciones a medida que nos ofrezcan una visibilidad de 360° sobre esta arquitectura híbrida y que pueda ser complementada con una protección de múltiple vector”, concluye.

¿Te gusta este reportaje?

Compártelo en redes



medidas de autenticación adicional, reforzar los accesos a las plataformas... sin embargo, la responsabilidad en algún punto debe recaer sobre el usuario. No podemos cargar todo el compromiso a la entidad o a los proveedores de servicios.

Para concluir este bloque, Jesús Rodríguez también incide en el valor de la concienciación y de la formación, como las dos medidas para prevenir los posibles riesgos de seguridad dentro de cualquier empresa. “En el sector financiero llevan tiempo trabajando esta parte”, señala, “a fin de concienciar y sensibilizar al usuario interno”. Asimismo, es básico educar al usuario en aspectos como la generación de contraseñas robustas o la protección de los datos. “El ideal en formación es empezar desde abajo. Pero en este proceso de transformación digital no todo el mundo ha recibido la misma educación en materia de seguridad”. ■



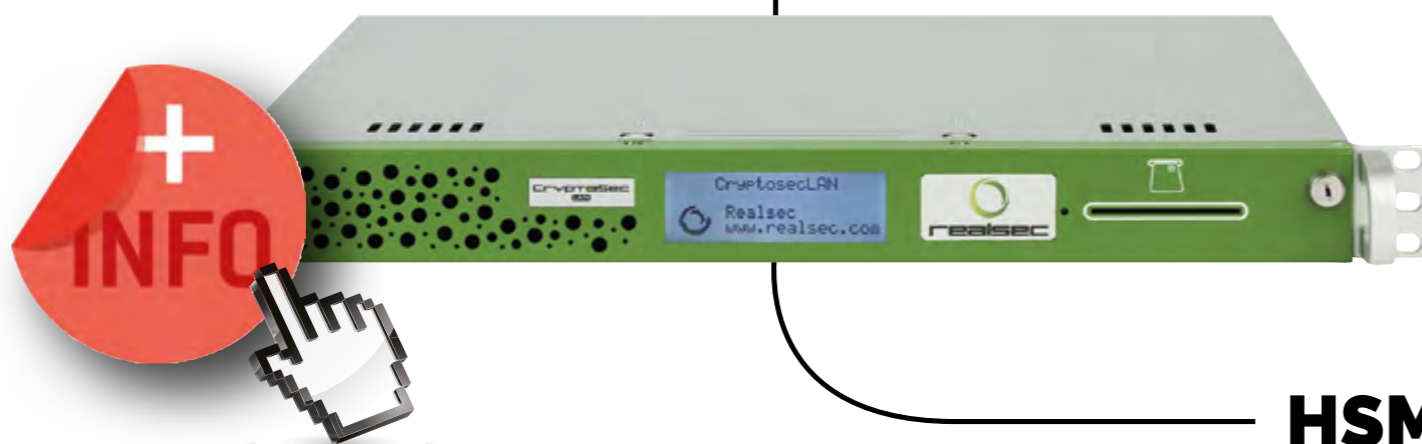
MÁS INFORMACIÓN



[Tendencias de seguridad en el sector financiero](#)

CIFRADO HARDWARE EN EL ÁMBITO FINANCIERO

CRYPTOsec LAN



HSM con el mayor rendimiento transaccional del mercado

- Incluidos todos los algoritmos de cifrado simétricos y asimétricos **(sin costes adicionales ocultos).**
- Autenticación de doble factor para cumplimiento PSD2 e integración con soluciones de Blockchain.
- Certificación FIPS 140-2 level 3 del NIST y la Certificación PCI PTS HSM v2.0. del PCI Security Standards Council.



realsec

La clave para proteger su negocio



www.realsec.com

JOSÉ DE LA CRUZ, DIRECTOR TÉCNICO, TREND MICRO IBERIA

“En la adopción de las correctas medidas de seguridad el sector financiero progresa adecuadamente”

Las instituciones financieras asumen un papel aún más activo en la creciente convergencia de la tecnología de la información (TI) y la tecnología operativa (OT). La necesidad de dar servicio a los clientes las 24 horas, los 7 días de la semana, ha llevado a la industria a adaptarse, especialmente con la adopción de dispositivos inteligentes conectados. Sobre los retos de seguridad que afrontan los servicios financieros o cómo impactan las regulaciones hablamos con José de la Cruz, Director técnico de Trend Micro.

La banca, los servicios financieros, son ahora digitales, móviles y cada vez más centrados en los clientes. A nivel de seguridad, ¿qué retos cree que está afrontando el sector financiero?

Aprecio 2 retos. Desde el punto de vista de infraestructura: el banco tiene que garantizar que

su infraestructura es segura y resistente ante ataques de robos de información, denegación de servicio, suplantación de identidad, etc. Desde el punto de vista del usuario: el banco tiene que intentar garantizar que el usuario no sea víctima de ningún tipo de estafa que esté suplantando la identidad del banco.



¿Cuán maduro es el sector financiero respecto a la adopción de las adecuadas medidas de seguridad?

Progresada adecuadamente. No estamos en el escenario ideal, pero se aprecia una fuerte inversión en ciberseguridad la cual se incrementa de manera progresiva y constante año tras año.

¿Cree que se está educando a empleados y clientes para adoptar de manera segura los nuevos entornos bancarios financieros?

Si, la concienciación es uno de los puntos clave. Como apuntaba anteriormente, el banco es indirectamente responsable de que sus usuarios sean capaces de discernir una estafa de una comunicación legítima por parte del banco.

Esto se consigue con campañas de concienciación y con una estrategia de comunicación

¿Quieres saber más?

Puedes ampliar la información de la propuesta de Trend Micro para proteger los entornos financieros en este enlace



muy clara (ej.: el banco nunca se va a dirigir por correo electrónico al usuario para pedirle datos).

Por otra parte, al igual que cualquier otra compañía que maneje datos sensibles, la concienciación, formación y evaluación continua al empleado es fundamental para conseguir

que éste represente la primera barrera de protección.

¿Qué impacto tiene el cumplimiento regulatorio de normativas como PSD2 en este mercado?

Un impacto positivo y, a mi entender, asumible por bancos y usuarios. Cuestiones como la doble autenticación son una realidad desde hace tiempo en servicios de correo o a nivel empresarial. Incluso los propios bancos las utilizaban para autenticar operaciones sensibles (ej.: Transferencia). Ahora simplemente se volverán generalizadas.

Es una normativa que va a ayudar a mejorar la seguridad y a reducir drásticamente ataques basados en robos de credenciales.

¿Qué puntos cree que tendría que mejorar el sector financiero?

Creo que debe continuar en la línea actual y quizás ser más flexible y ágil a la hora de implementar mecanismos de protección. ■

¿Cuál es la propuesta de Trend Micro?

La propuesta de Trend Micro radica en cubrir todos los vectores de ataque con una tecnología que permita colaboración (no sólo con productos del mismo fabricante) y que proporcione visibilidad y control al banco.

Adicionalmente, ponemos foco en la protección de vulnerabilidades las cuales continúan representando un foco de ataque crítico y que deben ser cubiertas tanto en sistemas soportados como en aquellos que

ya están fuera de soporte por parte del fabricante (ej.: Windows 2000, 2003 y 2008). Esto se consigue implementando la tecnología de parchado virtual tanto en el endpoint como en servidores y/o la red.



MÁS INFORMACIÓN



[Bancos bajo ataque: Tácticas y técnicas utilizadas para apuntar a organizaciones financieras](#)



[Caso de éxito: Bulgarian American Credit Bank](#)

JESÚS RODRÍGUEZ, CEO DE REALSEC

“Uno de los más importantes retos a los que se enfrenta la Banca europea es dar cumplimiento al marco normativo PSD2”

Caminamos hacia la consolidación de una sociedad y economía digitales, en la que la Banca, Entidades financieras y empresas de Medios de Pago han tenido que adaptar sus procesos de negocio hacia un entorno cada vez más digital. Sobre los retos de seguridad que afrontan los servicios financieros o cómo impactan las regulaciones hablamos con Jesus Rodríguez, CEO de Realsec.

La banca, los servicios financieros, son ahora digitales, móviles y cada vez más centrados en los clientes. A nivel de seguridad, ¿qué retos cree que está afrontando el sector financiero?

Efectivamente, en este momento estamos asistiendo a importantes cambios en la Banca, la mayoría determinados por procesos de transformación digital. Entre estos, destacamos la aparición de las empresas financieras tecnológicas o Fintechs, que apoyándose en tecnología digital están ofreciendo una amplia variedad de

servicios innovadores para el consumidor a un menor coste. Por lo que respecta a los retos, en mi opinión, uno de los más importantes retos al que se enfrenta la Banca europea, en este momento, es dar cumplimiento al marco normativo PSD2. En España, el cumplimiento de este nuevo marco normativo deberá hacerse efectivo, tal como ha establecido el Banco de España, a finales del presente año.

La Banca tiene además otros importantes retos a los que hacer frente, tales como la extracción de un mayor valor a sus datos, la lucha contra el



fraude o los ciberataques, cada vez más sofisticados, a los que se enfrenta cada día.

¿Cuán maduro es el sector financiero respecto a la adopción de las adecuadas medidas de seguridad?

La banca española siempre ha estado comprometida con la seguridad y, en muchos casos, ha sido pionera en la definición de las políticas y procedimientos y medidas de seguridad necesarias para evitar los riesgos inherentes a su operativa de negocio. En mi opinión, cuenta con un

¿Cuál es la propuesta de Realsec?

Realsec, como empresa desarrolladora de sistemas de cifrado basados en hardware (HSM), dispone de varias soluciones para proteger la operativa bancaria y de los Medios de Pago.

Una de nuestras soluciones más implantadas en la Banca de múltiples países es nuestro HSM financiero y para pagos "Cryptosec-BANKING". Se trata de un HSM que incorpora funciones y comandos criptográficos complejos, definidos para la Banca Universal por el Consorcio PCI (VISA y MASTERCARD) y que han sido desarrollados utilizando algoritmos de cifrado simétrico y asimétrico estándar. Estos comandos, protegen las transacciones bancarias y proporcionan un entorno seguro en el ámbito de los medios de pago.

Entre las funcionalidades de Cryptosec-BANKING se encuentran: la generación, validación y verificación de los códigos PIN de las Tarjetas de crédito y débito, competencia como centro autorizador de tarjetas, funciones de autenticación, generación de mensajes, tokenización, etc.

Realsec, dispone de otras soluciones basadas en hardware criptográfico para reforzar los sistemas de autenticación robusta (SCA), gestionar y proteger de forma centralizada las claves y los certificados, cifrar datos y archivos o fortalecer las nuevas plataformas de Blockchain.

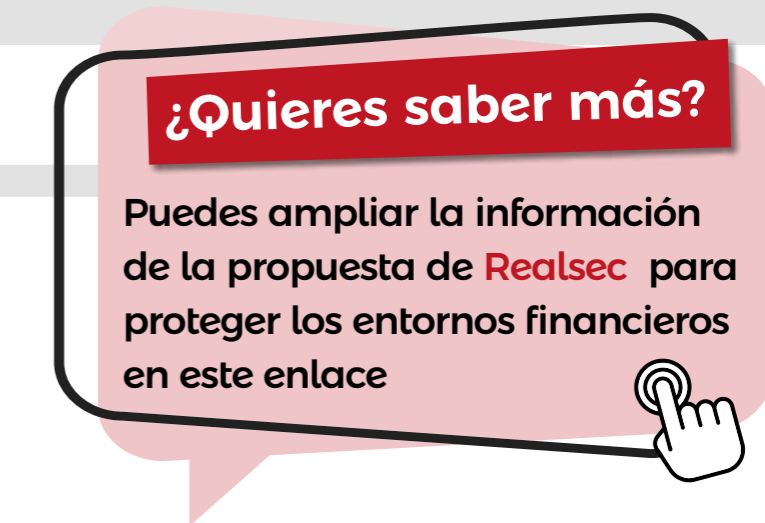
alto conocimiento, en materia de seguridad lógica y digital, así como con la capacidad suficiente para poder adoptar e implantar cualquier tipo de medida, venga o no determinada por las diversas normativas a las que está sujeta.

¿Cree que se está educando a empleados y clientes para adoptar de manera segura los nuevos entornos bancarios financieros?

Más que educar considero que la Banca está informando a sus clientes usuarios para que adopten determinadas medidas que eviten los posibles riesgos de fraude o ciberdelitos cuando éstos operan con la Banca digital.

¿Qué impacto tiene el cumplimiento regulatorio de normativas como PSD2 en este mercado?

En el caso de la normativa europea PSD2, su cumplimiento tiene un elevado coste para la Banca por cuanto está obligada a desarrollar las APIS necesarias que permitan poner a disposición de terceros los datos de sus clientes. Además, las entidades financieras están obligadas a implantar soluciones de autenticación robusta (SCA) que utilizan claves que deberían de ser generadas y custodiadas en dispositivos criptográficos. Hasta ahora, muchas de las entidades financieras han optado por salvar la situación mediante el envío de un mensaje SMS a sus clientes, con una clave de autenticación de un solo uso, pero su elevado coste por cada transacción les llevará sin duda a implantar soluciones tecnológicas de autenticación



¿Quieres saber más?

Puedes ampliar la información de la propuesta de **Realsec** para proteger los entornos financieros en este enlace



ción más eficientes y menos costosas.

¿Qué puntos cree que tendría que mejorar el sector financiero?

En materia de seguridad todo es siempre mejorable, pero podemos decir que el sector financiero, en general, está preocupado por el alto incremento del malware, cada día más sofisticado y dirigido hacia la banca móvil, así como por el incremento del phishing sobre los dispositivos móviles.

La Banca tendría que mejorar sus sistemas de autenticación implantando soluciones más robustas de doble o triple factor para lograr así una mayor protección de los sistemas de pago en la Banca Móvil; al mismo tiempo que mejora los sistemas de protección de los datos, las claves y los certificados y avanza en la usabilidad de la tecnología Blockchain para determinados procesos de negocio. ■



MÁS INFORMACIÓN



[Hardware para la encriptación de datos](#)



[Caso de éxito: Diebold](#)

MIGUEL ÁNGEL ROJO, CEO DE BOTECH

“El principal reto del sector financiero continúa siendo la protección de datos sensibles”



Cada día se realizan ingentes cantidades de operaciones financieras a través de internet, no sólo compras, sino pagos de facturas y todo tipo de transacciones bancarias. Todas estas operaciones crean una gran cantidad de datos confidenciales que se deben proteger. Sobre los retos de seguridad que afrontan los servicios financieros o cómo impactan las regulaciones hablamos con Miguel Ángel Rojo, CEO de BOTECH.

La banca, los servicios financieros, son ahora digitales, móviles y cada vez más centrados en los clientes. A nivel de seguridad, ¿qué retos cree que está afrontando el sector financiero?

El sector financiero lleva muchos años situado en el punto de mira de los ciberdelincuentes y es uno de los principales focos de ciberataques. Esto no es algo nuevo y el sector, que es muy consciente de ello, se está regulando constantemente. El principal reto del sector financiero continúa siendo la protección de datos sensibles, tanto de manera interna como externa. Por eso, cada día el estándar PCI-DSS es requerido

por más empresas ya que, si se procesa, guarda o transmite datos de tarjetas, se debe cumplir con el estándar.

La normativa PCI ha tenido un fuerte impacto en este mercado, ¿qué viene a regular y a quiénes? ¿cómo impacta en los pagos móviles?

Hemos trasladado nuestra tarjeta física a un entorno digital, que convive con muchas aplicaciones que tenemos descargadas en nuestro dispositivo. Es fundamental que todas esas aplicaciones estén desarrolladas con el estándar PA-QSA, Payment Application Qualified Security Assessor (PA-QSA), dentro de las normas de PCI Council.

Además está la variante de firma en dispositivos con tabletas o Smartphones; dentro del estándar PCI hay una norma para este tipo de aplicaciones que es PCI Pin On Glass, lo que demuestra que es un estándar vivo. Es fácil imaginar que en muy poco tiempo todas nuestras tarjetas estén incluidas en nuestro dispositivo móvil y tenemos que tener la misma seguridad que tenemos ahora en el pago con tarjeta física.

Es muy importante que seamos conscientes de que no importa tu sector de actividad, si tu organización procesa, guarda o transmite datos de tarjetas debe cumplir con el estándar PCI DSS. Para cumplir con este estándar, es necesario definir

¿Cuál es la propuesta de BOTECH?

Desde BOTECH, junto a nuestro partner 1st Secure IT, impulsamos el cumplimiento de la normativa PCI DSS. Nuestra propuesta ofrece la posibilidad de conseguir esta certificación con una metodología muy sencilla. Proponemos, en primer lugar, realizar un curso inicial de capacitación con el objetivo de abordar temas sobre conceptos generales, puntos clave para el cumplimiento y concienciar dentro de la organización. En segundo lugar, llevar a cabo un asesoramiento experto para el alcance del PCI DSS, para lo cual se realizan entrevistas, se recopila información y se revisa la documentación necesaria para identificar de manera clara los procesos, activos y proveedores involucrados que determinarán el alcance de PCI DSS. En tercer lugar, realizamos un GAP Analysis gratuito para nuevos clientes con el fin de analizar todos los procesos de seguridad existentes y determinar el nivel de cumplimiento de la organización. Y, en último lugar, se realiza una fase de revisión final donde se determina el estado de cumplimiento de PCI DSS y la posterior preparación del informe ROC (Report on Compliance) y AOC (Attestation of Compliance).

También es muy importante recordar que, aunque la normativa PCI DSS debe completarse anualmente, al igual que la auditoría, se recomienda obtener reportes aprobados de forma trimestral.

con el comité de dirección una persona responsable dentro de la empresa. PCI DSS no es, ni mucho menos, una normativa imposible de cumplir, pero sí es necesario apoyo experto para lograr la implementación de forma eficiente.

La normativa PCI DSS consta de seis categorías, 12 requisitos, alrededor de 200 controles y 250 procedimientos de prueba con el fin de garantizar la confidencialidad de los datos de la tarjeta de pago.

Estos son los requisitos fundamentales que es necesario cumplir:

- ❖ Construir y mantener una red segura.
- ❖ Proteger los datos de los titulares de las tarjetas cifrando la transmisión de datos e información confidencial de los titulares.
- ❖ Establecer un programa de gestión de vulnerabilidades.
- ❖ Crear medidas sólidas de control de acceso.
- ❖ Monitorizar y testar regularmente las redes y mantener una política de seguridad de la información actualizada.

Se habla de PCI DSS, y también de PCI 3DS, PCI PIN, PCI ISA... ¿Qué les diferencia?

Todas estas normativas buscan garantizar la protección de datos y la seguridad en las transacciones económicas. Por ejemplo, PCI ISA (Internal Security Assessor) permite evaluar y validar el cumplimiento de PCI DSS a través de la realización de autoevaluaciones internas. El objetivo de la normativa PCI PIN es garantizar la gestión se-

¿Quieres saber más?

Puedes ampliar la información de la propuesta de **BOTECH** para proteger los entornos financieros en este enlace



gura, el procesamiento y la transmisión del número PIN en las transacciones económicas. PCI 3DS crea un marco de trabajo transversal que permite la implementación en forma masiva de este protocolo de seguridad en entornos de e-commerce y m-commerce o comercio móvil.

¿Cuál es el nivel de adopción de esta normativa en España?

Según un reporte sobre seguridad en medios de pago de la firma Verizon, 2019 Payment Security Report, 15 años después de la puesta en vigor del PCI DSS, el número de empresas que logran mantener el cumplimiento al 100% de los 12 requisitos de la normativa se redujo del 52.5 % registrado en 2018 a un mínimo de 36.7% en todo el mundo, un dato muy significativo y preocupante. ■



MÁS INFORMACIÓN



[El cumplimiento PCI cae por primera vez en seis años](#)



[BOTECH Academy](#)

LUIS SUÁREZ, PRESALES MANAGER DE KASPERSKY IBERIA

“El mercado financiero es uno de los más conscientes de la importancia de adoptar medidas de seguridad”

Los incidentes de ciberseguridad que afectan al mundo financiero no solo provocan pérdidas económicas a las entidades y a sus clientes, sino que también implican pérdida de datos, daños en la reputación corporativa, filtraciones de información confidencial, etc. Sobre los retos de seguridad que afrontan los servicios financieros o cómo impactan las regulaciones hablamos con Pedro García Villacañas, Director preventa de Kaspersky Iberia.

La banca, los servicios financieros, son ahora digitales, móviles y cada vez más centrados en los clientes. A nivel de seguridad, ¿qué retos cree que está afrontando el sector financiero?

Entre los retos a afrontar se encuentran los ataques de phishing financiero, que crecieron un 9,5% en el último trimestre de 2019.

Además, durante el pasado año los ciberdelincuentes aplicaron un nuevo método: el robo

mediante la manipulación directa de las aplicaciones bancarias utilizando los servicios de accesibilidad de las aplicaciones.

Los troyanos bancarios, que crecieron un 61% en 2019, y el malware para cajeros también son retos a los que la banca debe hacer frente.

¿Cuán maduro es el sector financiero respecto a la adopción de las adecuadas medidas de seguridad?



El mercado financiero es uno de los más conscientes de la importancia de adoptar medidas de seguridad para su negocio y clientes. De hecho, el impulso de medidas de seguridad como la biometría, la autenticación multifactor o la basada en el comportamiento, viene dado en buena parte por su adopción por el sector financiero. Eso no impide, sin embargo, que los ciberdelincuentes sigan buscando vectores de ataque para superarlos.

¿Cree que se está educando a empleados y clientes para adoptar de manera segura los nuevos entornos bancarios financieros?

La formación de empleados y clientes es uno de los puntos más importantes cuando hablamos de ciberseguridad. Los empleados sue-

len ser considerados el eslabón más débil de la cadena por lo que es importante poner a su disposición una formación continua sobre las políticas, las amenazas actuales y cómo enfrentarse a estas amenazas. Debería prestarse especial atención a la ingeniería social, que sigue siendo el vector de ataque más común y exitoso.

¿Cuál es la propuesta de Kaspersky ?

Kaspersky dispone de distintas soluciones para elevar los niveles de seguridad a través de la predicción, prevención, detección y respuesta al cibercrimen. Entre ellas:

- ❖ **KASPERSKY ENDPOINT SECURITY FOR BUSINESS.** Protección adaptativa para amenazas dirigidas a los endpoints.

- ❖ **THREAT MANAGEMENT AND DEFENSE.** Protección avanzada basada en inteligencia de amenazas.

- ❖ **IOT & EMBEDDED SECURITY.** Protección de los sistemas IoT y dispositivos integrados, reduciendo al máximo los riesgos en estos dispositivos.

- ❖ **KASPERSKY ANTI TARGETED ATTACK PLATFORM.** Una solución de seguridad unificada contra ataques dirigidos.

- ❖ **KASPERSKY ENDPOINT DETECTION AND RESPONSE.** Prevención de las interrupciones de la actividad al eliminar los riesgos de las amenazas avanzadas.

¿Qué impacto tiene el cumplimiento regulatorio de normativas como PSD2 en este mercado?


El cumplimiento de dichas normativas suele obligar a la adopción de nuevas tecnologías. Debemos entender que la inclusión de nuevas tecnologías suele ir de la mano con nuevos vectores de ataque, y es muy probable que los atacantes recurran a nuevos esquemas fraudulentos para abusar de estos nuevos mecanismos.

¿Qué puntos cree que tendría que mejorar el sector financiero?

La interconexión de los sistemas y el uso de los dispositivos móviles se encuentra muy extendido tanto para el acceso remoto como para compartir datos. Esta digitalización expone cada vez más a las organizaciones financieras a ataques tanto genéricos como dirigidos.

Por eso, además de todas las medidas que las entidades tengan en marcha, es recomendable prestar atención a los nuevos vectores de ataque que se podrían desarrollar en los próximos meses:

¿Quieres saber más?

Puedes ampliar la información de la propuesta de **Kaspersky** para proteger los entornos financieros en este enlace 

- ❖ **Ataques a Fintech.** Las apps de inversión son cada vez más populares entre los usuarios de todo el mundo, pero no todas estas aplicaciones utilizan las mejores prácticas de seguridad.

- ❖ **Nuevos troyanos para banca móvil.**

- ❖ **Acceso de pago a la infraestructura bancaria y ataques ransomware a bancos.** Los expertos de Kaspersky esperan un aumento de la actividad de los grupos especializados en la venta de accesos a la red de bancos de las regiones de África y Asia, así como de Europa del Este.

- ❖ **Magecarting 3.0:** más grupos de ciberdelincuentes se centrarán en los sistemas de procesamiento de pago online. En los últimos años, el llamado JS-skimming (el método de robo de datos de tarjetas de las tiendas online) ha ganado popularidad entre los atacantes. ■

MÁS INFORMACIÓN

 [Caso de éxito: Alfa Bank](#)

 [Machine Learning in Cybersecurity](#)

NURIA ANDRÉS, TERRITORY ACCOUNT MANAGER SPAIN&PORTUGAL DE FORCEPOINT

“Los clientes seguimos siendo la gran asignatura pendiente”

Los bancos siempre han estado a la vanguardia de la ciberseguridad empresarial. Sus enormes reservas de efectivo y datos de consumidores los han convertido en un objetivo principal para los ciberdelincuentes, y la amenaza de pérdidas financieras, consecuencias regulatorias y daños a la reputación los ha impulsado a innovar y acelerar el campo de la ciberseguridad. Sobre los retos de seguridad que afronta o cómo impactan las regulaciones hablamos con Nuria Andrés, Territory Account Manager Spain&Portugal de Forcepoint

La banca, los servicios financieros, son ahora digitales, móviles y cada vez más centrados en los clientes. A nivel de seguridad, ¿qué retos cree que está afrontando el sector financiero?

Está claro, que desde el punto de vista económico el gran reto del sector financiero es la solvencia, pero desde el punto de vista de la seguridad, sin lugar a dudas, es la protección del dato, datos de clientes o activos financieros. ¿Y por qué? Porque pueden provocar pérdidas económicas millonarias por filtraciones de información confidencial de clientes, pero

también pueden suponer una enorme pérdida reputacional, y está demostrado que la pérdida reputacional que sufren los bancos, por incidentes o brechas de seguridad, es mucho más grave que en compañías de otros sectores. Suele decirse que, “el dinero es miedoso”. También es un sector especialmente sensible a ataques de phishing o ransomware, pero contra sus clientes.

¿Cuán maduro es el sector financiero respecto a la adopción de las adecuadas medidas de seguridad?



Probablemente, el sector financiero sea uno de los sectores más regulados. Están sujetos a múltiples normativas, GDPR, MiFID II o PSD2, y eso ha ayudado a desplegar diferentes soluciones de seguridad, pero también procesos y procedimientos. Por eso, si comparamos al sector financiero frente a otros sectores, quizás sea el “alumno aventajado”.

¿Cree que se está educando a empleados y clientes para adoptar de manera segura los nuevos entornos bancarios financieros?

En banca y también en otros muchos sectores, se está “educando y concienciando” a los empleados, por ejemplo, simulando campañas de phishing,

que sigue siendo uno de los principales vectores de ataque, e impartiendo cursos con nociones, al menos, básicas de ciberseguridad, para aquellos empleados que hayan “caído en la trampa”.

Sin embargo, los clientes seguimos siendo la “gran asignatura pendiente”. En mi opinión, no sólo es una responsabilidad del sector bancario concienciar a sus clientes, nociones de ciberseguridad deberían impartirse desde la escuela, ya que vivimos en un mundo, enteramente digital, y debería estar en nuestro ADN saber que no tenemos que proporcionar nunca a nadie, nuestro usuario y nuestra password de acceso a la banca online. Nuestro banco, nunca nos la pedirá.

¿Qué impacto tiene el cumplimiento regulatorio de normativas como PSD2 en este mercado?

La implementación de la directiva PSD2 supuso un reto, desde el punto de vista tecnológico para los bancos, y sobre todo en el lado del cliente. La Banca tradicionalmente se había centrado en proteger “el host”, quiero decir, sus servidores, su propia infraestructura, sus Data Center ON-Premise, y ahora, el cliente cobra un especial protagonismo.

¿Qué puntos cree que tendría que mejorar el sector financiero?

La Banca evolucionó de políticas de seguridad centradas en la infraestructura, hacia políticas de seguridad centradas en la protección dato. Pero, sin lugar a dudas, el siguiente reto es entender

¿Quieres saber más?

Puedes ampliar la información de la propuesta de Forcepoint para proteger los entornos financieros en este enlace



que el nuevo perímetro es el propio usuario. Y en banca tenemos muchos y muy variados tipos de usuarios, desde directores de oficina, traders, operadores en un contact center, que realmente trabajan para un tercero, o por supuesto, los clientes.

Por tanto, poder analizar el comportamiento de los usuarios, y poder aplicar políticas de seguridad dinámicas, en base al comportamiento de los usuarios y la criticidad del dato, es la evolución de las políticas de seguridad, que pueden permitir la detección del fraude. ■



MÁS INFORMACIÓN



[Protección de los datos en reposo, en movimiento y en uso en entornos híbridos](#)



[Análisis de comportamiento](#)

¿Cuál es la propuesta de Forcepoint ?

La visión de la ciberseguridad de Forcepoint, tiene dos pilares, la protección del dato, allá donde esté, y el análisis del comportamiento de los usuarios. Y precisamente, datos y usuarios son clave en la protección del sector bancario.

Muchos pueden estar pensando en que, para proteger el dato, tenemos que desplegar soluciones de DLP. Sin embargo, nosotros ya no hablamos de DLP, sino de “Protección Dinámica del Dato” (DDP, Dynamic Data Protección). Es decir, analizamos el comportamiento de los usuarios y en base al riesgo de los mismos, podemos aplicar distintas políticas de seguridad de manera automatizada, y dependiendo del tipo de dato que estemos considerando.

Además, creemos firmemente en que el nuevo perímetro es el propio usuario, somos fieles seguidores de SASE. De tal modo que nuestras soluciones más tradicionales, NGFW, Proxy o Correo, las podemos desplegar tanto ON-PRE-MISE, puras CLOUD o HÍBRIDAS, precisamente, para ayudar a nuestros clientes, y en especial al sector bancario, en su viaje al CLOUD, y su proceso de transformación digital.

¿Necesitas cumplir con el estándar PCI DSS?

Si tu organización transmite, procesa o almacena datos de tarjetas de pago debes cumplir PCI DSS.



Garantiza la protección de datos y la seguridad



Minimiza el fraude y evita cuantiosas sanciones



Transmite confianza y seguridad



Implementa buenas prácticas de seguridad



“Los bancos tienen que luchar, por un lado, para que sus sistemas sean seguros, y por otro para que sus usuarios no caigan en estafas”

JOSÉ DE LA CRUZ, DIRECTOR TÉCNICO, TREND MICRO IBERIA

La seguridad ha sido una de las principales preocupaciones del sector financiero. Sin embargo, tanto los bancos y aseguradoras como sus clientes siguen siendo objetivos prioritarios de los ciberdelincuentes. Dice José de la Cruz, director técnico de Trend Micro, que hasta hace poco eran dos los tipos de ataque más habituales: los dirigidos, que tenían un trabajo previo de adquisición de información e inteligencia sobre el objetivo; y los genéricos, en los que se lanza una campaña de spam y se va infectando en masa. “Ahora no. Ahora lo que se está produciendo es una mezcla de los dos”, dice José de la Cruz.

Explica el directivo que la tendencia es lanzar un ataque genérico con Emoted y una mezcla de TrickBot y cuando se consigue infectar a la víctima se publica la infección en el mercado negro. Cuando aparece algún interesado se le venden los accesos e incluso las herramientas “y utilizando otro ransomware distinto, que es Ryuk, se cifra la información y se reclama el



```
...},c.prototype.  
and('[data-toggle="tab"]  
removeClass("in"):b.removeClass(  
ia-expanded",...e()})var g=d.  
length&&h?g.one("bsTransitionEnd",f)  
onstructor=...conflict=fl  
.data-api",...["tab"],e)  
each(function(...this),e=d  
) {this.opt...({},c.DEF  
"click.bs.affix.data-api",a.  
tion());c.VERSION="3.3  
rollTop(),f=thi
```

pago. Es decir, hay dos o tres actores involucrados en un ataque”, dice José de la Cruz.

Los bancos no sólo tienen que lidiar con la amenaza de los ciberdelincuentes, sino también con miles de usuarios, que a menudo no toman precauciones y además esperan una experiencia impecable. Dice José de la Cruz que los usuarios son muy exigentes y que una entidad financiera no se puede permitir, bajo ningún concepto, un problema de seguridad porque afecta a su línea de flotación, que es la reputación, “sobre todo si eres un banco online”. Pero también hay que tener en cuenta la protección desde dentro del propio banco, y menciona que un banco jamás envía un correo electrónico, un banco jamás le va a pedir al usuario que ponga al descubierto las credenciales, “de forma que hay que aplicar el sentido común. Y son los bancos quienes más tienen que luchar, por un lado, para que sus sistemas sean seguros, y por otro para que sus usuarios no caigan en estafas”.

Sobre las normativas a las que están sujeto el mercado financiero, dice José de la Cruz que su impacto es grande, “aunque solo sea por las sanciones”, pero que algunas, como PCI DSS ya están bastante rodadas y otras, como GDPR, se están empezando a tomar en serio.

Destaca el directivo de Trend Micro como tecnología imprescindible para el mercado financiero la gestión de vulnerabilidades, “algo en lo que siempre insisto pero que creo que es

importante”, sobre todo ahora que ha finalizado el soporte de Windows 7 y otros sistemas operativos más antiguos en los que se siguen detectando vulnerabilidades que los ciberdelincuentes van a explotar.

Respecto a la propuesta de Trend Micro para proteger los entornos financieros, extensible por supuesto al resto de mercados, explica José de la Cruz que este año la compañía está poniendo foco en tres áreas: la nube, los sectores industriales y protección del correo electrónico.

La seguridad de la nube se articula en torno a Cloud One, que incluye tanto la parte de protección tradicional del servidor desde el punto de vista de parcheado virtual, de antimalware, gestión de contenedores, protección de la aplicación e incluso protección en los entornos de almacenamiento de nube pública como Amazon S3, Azure Block o Google Storage.

En la parte de Cloud Security Posture Management “tenemos una solución específicamente diseñada para analizar el cumplimiento normativo”, explica José de la Cruz, añadiendo que se ha integrado toda la parte de IPS dentro de la nube, “porque yo puedo tener una infraestructura IPS y un firewall maravilloso dentro de mi casa, pero cuando me voy a la nube pierdo esa capa y nosotros hemos desarrollado una solución con Tipping Point, nuestro IPS tradicional, que se puede implementar en soluciones Amazon exactamente igual que los aplicamos onpremise”. ■



“Los bancos no sólo tienen que lidiar con la amenaza de los ciberdelincuentes, sino también con miles de usuarios”



MÁS INFORMACIÓN



[Trend Micro Cloud One](#)



[Trend Micro Hybrid Cloud Security](#)

“El sector financiero en general está preocupado por el alto incremento del malware”

JESÚS RODRÍGUEZ, CEO DE REALSEC

Uno de los sectores en los que Realsec tiene mucha presencia es el de la banca. ¿Cómo habéis visto su evolución en los últimos años?

La Banca ha sufrido importantes cambios en estos últimos cinco años. Lo asegura Jesús Rodríguez, CEO de Realsec, una empresa tecnológica europea, con presencia internacional, que desarrolla soluciones de Cifrado y Firma digital para los sectores de Banca, Fintech y Medios de Pago, Gobierno, Defensa y Sector Empresarial. Asegura Jesús Rodríguez que se ha pasado de una Banca tradicional, cuyos usuarios-clientes operaban con sus Bancos de manera presencial a través de las sucursales bancarias, o haciendo uso de sus tarjetas de crédito-debito, tarjetas contactless y de la Banca electrónica; a una Banca en la que se hace uso de nuevos canales, como es la Banca Móvil o los sistemas Wallet.

“En este momento, estamos asistiendo al proceso de transformación digital que ha propiciado la aparición de las Fintechs, que, apoyándose en tecnología digital, ofrecen una amplia variedad de servicios innovadores para el consumidor a un menor coste”, añade El CEO de Realsec, asegurando que muchos bancos aún no están preparados para competir en este escenario.

Dar cumplimiento al nuevo marco normativo europeo es uno de los principales retos a los que se enfrenta la banca, dice Jesús Rodríguez. Este nuevo marco normativo europeo o PSD2, deberá de hacerse efectivo en España, tal y como ha establecido el Banco de España, a finales del presente año, e implica “la obligación de tener que compartir y poner a disposición de los nuevos actores financieros tecnológicos los datos de sus clientes. Lo que se llama “OPEN BANKING”.



Añade el CEO de Realsec que el cumplimiento de la normativa PSD2 tiene, además, un elevado coste para la banca porque “no solamente está obligada a desarrollar las APIs necesarias que permitan poner a disposición de terceros los datos de sus clientes; sino que además está obligada a implantar sistemas de autenticación robusta SCA (Strong Customer Authentication) para evitar el riesgo de suplantación de identidad en su operativa”.

Además, la Banca tiene además otros importantes retos a los que hacer frente, como la transformación digital, la extracción de un mayor valor a sus datos o la lucha contra el fraude y los ciberataques cada día más sofisticados.

Realsec cuenta con varias soluciones para proteger la operativa bancaria y de los Medios de Pago. Explica Jesús Rodríguez que una de las soluciones más vendidas e implantadas es Cryptosec-BANKING, un HSM financiero que incorpora todas las funciones y comandos criptográficos complejos, definidos por las normas ANXI x9 y por el Consorcio PCI (VISA y MASTERCARD) desarrollados mediante algoritmos de cifrado simétrico y asimétrico. “Estos comandos y funciones protegen las transacciones bancarias y proporcionan un entorno seguro en el ámbito de los medios de pago y la operativa bancaria en general”, dice el CEL de Realsec.

Entre las funcionalidades de Cryptosec-BANKING destaca la generación, validación y/o ve-

rificación de los códigos PIN de las Tarjetas de crédito o débito, las funciones para los centros autorizadores de tarjetas, la generación y custodia de claves de cifrado y autenticación, la generación mensajes, la tokenización etc.

Así mismo, Realsec cuenta con soluciones para automatizar los procesos de carga de las claves en los Cajeros y Terminales punto de venta. Sobre lo que hemos alcanzado acuerdos de integración de nuestros HSMs con terceros que tienen aplicaciones para la gestión de tarjetas, soluciones de SCA, Blockchain etc.

“En materia de seguridad podemos decir que el sector financiero en general está preocupado por el alto incremento del malware, cada día más sofisticado y dirigido hacia la banca móvil, así como por el incremento del phishing sobre los dispositivos móviles”, dice Jesús Rodríguez. Añade el directivo que la situación demanda la incorporación de herramientas y soluciones de seguridad más eficientes para la prevención y defensa contra ataques.

Añade que por lo que respecta a tecnología vinculada a Realsec como fabricante, la Banca está demandando, entre otras: soluciones para proteger sus sistemas de pago (especialmente para la Banca Móvil), para la gestión centralizada de claves y certificados, el cifrado de datos y archivos, sistemas de autenticación (SCA), HSMs para tecnología Blockchain etc. ■



“Dar cumplimiento al nuevo marco normativo PSD2 es uno de los principales retos a los que se enfrenta la banca”

MÁS INFORMACIÓN

 [Cryptosec-BANKING](#)

 [Soluciones de seguridad en banca](#)

“PCI DSS es una normativa que ayuda, que transmite confiabilidad”

MIGUEL ÁNGEL ROJO, CEO DE BOTECH FPI

Todas las empresas que procesan, transmiten o almacenan datos de tarjetas de pago deben cumplir con el estándar de seguridad PCI DSS para garantizar la protección de los datos del titular de la tarjeta y evitar el fraude. De esto hablamos con Miguel Ángel Rojo, CEO de BOTECH FPI, quien asegura que en el sector financiero se mueve mucho dinero y por tanto es muy atractivo para los ciberdelincuentes.

Explica Miguel Ángel Rojo que desde hace dos años la compañía se ha asociado con 1st SecureIT, una empresa que durante diez años ha desarrollado toda la parte de consultoría en entornos PCI en Estados Unidos y Latinoamérica, “y nosotros hemos ampliado esa cobertura a toda Europa”. Asegura el directivo que la normativa quiere dar al usuario final un marco de protección, garantizando que sus datos y los de su tarjeta van a viajar cifrados en cualquier tipo de operación.

“El principal reto es entender que es una normativa que ayuda, que transmite confiabi-



lidad”, asegura Miguel Ángel Rojo en relación a PCI DSS. Añade que una vez que entras en la rueda de la certificación PCI la tienes que estar cumplimentando año tras año, y que si bien en Europa hubo un alto grado de concienciación con la normativa en los años 2011-2012, “eso ya ha bajado bastante”. Asegura que donde más concienciación hay ahora mismo es en la región de Asia Pacífico y que en Latinoamérica es donde todavía “cuesta explicar a los negocios qué aporta la normativa, para qué sirve”. Respondiendo a alguna pregunta que le han hecho, dice Miguel Ángel Rojo que “nadie te va a multar por no cumplir con la normativa PCI DSS, pero seguramente es algo que te van a exigir las marcas de las tarjetas con las que trabajas [VISA, Mastercard, American Express...]”.

Explica el directivo de BOTECH FPI que la norma se ajusta a todo tipo de empresas que admitan la tarjeta como medio de pago, desde las que pasan ocho millones de tarjetas al año a las que pasan 87; “la normativa está adaptada a todos los tamaños de transaccionalidad”.

Sobre el proceso de implantación, asegura Miguel Ángel Rojo que “es un tema que tiene que estar liderado por la dirección”. Desde su compañía se ofrecen charlas de concienciación, se explican los beneficios, cuál debe ser el nivel de cumplimiento y se les ayuda en todo el proceso de implantación de PCI DSS. Entre las estrategias de BOTECH FPI está el empujar



La normativa PCI DSS es un estándar de seguridad que tiene como objetivo reducir el fraude relacionado con las tarjetas de crédito e incrementar la seguridad de los datos que intervienen en las transacciones online.

la normativa en el pequeño comercio para que den, hacia sus clientes, “una imagen de seguridad”, que es la que proporciona el sello de PCI Compliance. Entre las acciones que estas pequeñas empresas pueden hacer hay un formulario de autoevaluación que les permite saber cómo hacer frente a la normativa.

“Yo creo que estamos todos muy preocupados por los datos, porque no te llegue un cargo a tu cuenta bancaria, y creo que hace falta un proceso de concienciación. A veces hemos asumido que hacer procesos de calidad aportan mucho, y en este sentido yo creo que PCI aporta mucho a la industria del sector financiero”, concluye Miguel Ángel Rojo. ■



“El proceso de implantación de PCI DSS tiene que estar liderado por la dirección de las empresas”

MÁS INFORMACIÓN

 [BOTECH FPI - PCI DSS](#)

 [¿Necesitas cumplir con el estándar PCI DSS?](#)

“Los criminales saben que atacar al banco es mucho más difícil que atacar al usuario o la cadena de suministro”

LUIS SUÁREZ, PRESALES MANAGER DE KASPERSKY IBERIA

La banca, los servicios financieros, son ahora digitales, móviles y cada vez más centrados en los clientes. Las ciberamenazas en estos entornos se consideran algunas de las más peligrosas, ya que su impacto puede ocasionar pérdidas financieras directas para las víctimas. Dice Luis Suárez, Presales Manager de Kaspersky Iberia, que en estos entornos se está muy concienciado de la seguridad de sus activos; “han estado muy expuestos en sus activos físicos y al hacer el cambio hacia la digitalización de esos activos, esa madurez en la seguridad ha ido pareja”, dice el experto de seguridad.

Sobre los retos de seguridad a los que se enfrentan los servicios financieros, asegura Luis Suárez que la cadena de suministro es un tema que preocupa porque “los criminales son conscientes de que atacar al banco es mucho más difícil”. ¿Por qué soluciones están apostando para paliar este tipo de temas? “Yo hablaría de inteligencia de amenazas, del famoso Threat



Hunting, porque hay que abrazar la idea de que cualquier puede verse comprometido y de que a través de estos informes de inteligencia se pueden entender las técnicas, tácticas y procedimientos de cómo nos pueden atacar”.

No sólo es más fácil de atacar a la cadena de suministro, sino a los usuarios. Durante los últimos años los bancos han puesto un montón de servicios al alcance de los usuarios, colocando al usuario en el centro de todo; al usuario se le permite hacer casi cualquier operación sin tener que pasar por una oficina bancaria, y eso entraña unos riesgos de seguridad”, asegura Luis Suárez.

También hablamos con el Presales Manager de Kaspersky Iberia sobre fraude. Y es que uno de los productos de la compañía es [Kaspersky Fraud Prevention](#), disponible en dos versiones, “uno dedicado a la autenticación continua, que nos permite recoger una serie de telemetrías y eventos en torno a la situación del usuarios y del dispositivo”. Esto permitiría, por ejemplo, que si un usuario hace logging en los servicios de una entidad financiera de forma recurrente y periódica desde Barcelona, “y a los cinco minutos de cerrarse la sesión detecto un inicio de sesión en Corea, puedo tener una evidencia de que quizá esa transacción que se está produciendo tenga más indicios de fraude”, de forma que se puedan automatizar una serie de indicadores que puedan permitir tanto bloquear la transacción como mostrar una alerta al equipo de analistas de fraude. La solución también es

capaz de detectar el fraude cuando se hace uso de apps móviles.

La otra versión del producto está precisamente enfocado a los analistas de fraude, “para que tengan todas las herramientas y todas las métricas para que puedan analizar todos los casos de fraude”.

Explica Luis Suárez que Kaspersky Fraud Prevention “se está desarrollando teniendo muy en cuenta la normativa PSD2, que afecta a todo el mundo, pero especialmente a banca”. Añade que respecto a PSD2 hay algunas claves a destacar: por un lado lo que se busca es aunar la seguridad del usuario, y eso lleva a la inclusión de un segundo factor de autenticación; también se busca que eso no lastre la experiencia del usuario, y también que te otorgue una serie de herramientas para medir cómo estas consiguiendo estos objetivos “y Kaspersky Fraud prevention se está desarrollando con esta y otras muchas normativas en mente para poder cumplir con todas ellas”.

Además de Kaspersky Fraud Prevention, la compañía cuenta con otra serie de soluciones para proteger los entornos financieros. Menciona Luis Suárez otras opciones más orientadas a las amenazas, “tanto los servicios de inteligencia de Kaspersky, como soluciones que nos permitan sacar todo el jugo de esa inteligencia, para poder hacer un Threat Hunting efectivo, poder detectar los indicadores de compromiso y poder tener esa visibilidad, esa detección temprana antes de que se produzca la incidencia”. ■



“Al usuario se le permite hacer casi cualquier operación sin tener que pasar por una oficina bancaria, y eso entraña unos riesgos de seguridad”

MÁS INFORMACIÓN

 [Kaspersky Fraud Prevention](#)

 [Online Banking with Safe Money Technology](#)

“La seguridad tiene que ser conectada y automatizada”

NURIA ANDRÉS, TERRITORY ACCOUNT MANAGER SPAIN&PORTUGAL DE FORCEPOINT

Hace tiempo que Forcepoint apostó por una Human Centric Cybersecurity, y aseguró que las políticas de seguridad estáticas no son suficientes. Y eso mismo nos dice Nuria Andrés, Territory Account Manager Spain&Portugal de Forcepoint, a quien le preguntamos cómo se aplica la propuesta human-centric Cybersecurity de su compañía a los entornos financieros.

Nos cuenta que la estrategia tiene dos pilares: “El primero es la protección del dato, la protección de la información allá donde esté. Y el otro pilar es el análisis del comportamiento de los usuarios, porque existen muchos y muy diferentes tipos de usuarios y lo importante no es distinguir entre usuario externo e internos, sino entre usuarios maliciosos y legítimos”.

Uno de los grandes retos a los que ha tenido que hacer frente el mercado financiero, quizá más que otros por la tremenda regu-



“LA SEGURIDAD TIENE QUE SER CONECTADA Y AUTOMATIZADA” - Nuria Andrés, Territory Account Manager Spain&Portugal de Forcepoint

lación a la que está sujeto, es la adopción del cloud. Recuerda Nuria Andrés que el perímetro ya no existe; “en el sector financiero hemos protegido el perímetro con mucho ahínco. Sin embargo, hemos llevado los datos al cloud y el perímetro se ha diluido”, explica, añadiendo que el nuevo perímetro es la identidad de los usuario, “y dependiendo de esa identidad nosotros en tiempo real podemos provisionar desde el cloud diferentes soluciones de seguridad (firewall-as-a-service, DLP as a Service...)”.

Lo diferencial de Forcepoint, asegura Nuria Andrés, es el análisis del comportamiento de los usuarios mientras se monitorizan las conexiones online, lo que permite “pasar de políticas de seguridad estáticas a políticas de seguridad dinámicas”.

Otro de los retos a los que se enfrenta de manera especial el sector financiero es que debe tratar con diferentes tipos de usuarios. No sólo tiene que articular ciberdefensas en torno a sus empleados, y a la cadena de suministro, sino a miles de clientes que acceden a sus servicios, desde diferentes dispositivos, la mayoría de las veces sin las mínimas precauciones y exigiendo siempre la misma experiencia de usuario. Asegura Nuria Andrés que el cliente es la última barrera de defensa y que es muy importante educar y concienciar a los usuarios. Con Forcepoint

Insider Threat se analiza el comportamiento de los usuarios de forma que se pueda detectar una exfiltración de datos.

“It’s time for Human Centric Cybersecurity”, responde la directiva de Forcepoint al preguntarle por la propuesta de su compañía para proteger el sector financiero. Añade que además de tener en cuenta el factor humano, “la seguridad tiene que ser conectada y automatizada. Hemos invertido mucho en soluciones de seguridad y hemos montado auténticos silos, y es muy importante conectar y automatizar la seguridad; y eso con el amplio portfolio que tenemos en Forcepoint lo podemos hacer”.

Destaca Nuria Andres tres áreas en el portfolio de Forcepoint. Por un lado la parte de Dynamic User Protection, que hace referencia a todo el análisis del comportamiento de los usuarios; Dynamic Data Protection (DDP), que es todo lo relacionado a aplicar todo el análisis del comportamiento de los usuarios a la protección del dato; y la parte de Dynamic Edge Protection, que es la que aglutina las soluciones más tradicionales (proxy, seguridad para el correo electrónico, CASB...). “Tenemos soluciones tanto on premise, cloud, y también híbridas, para ayudar a nuestros clientes precisamente en esa transformación digital y en ese viaje al cloud”, concluye Nuria Andrés. ■



“Lo diferencial de Forcepoint es el análisis del comportamiento de los usuarios mientras se monitorizan las conexiones online”

MÁS INFORMACIÓN

 [Forcepoint Dynamic Data Protection \(DDP\)](#)

 [Forcepoint Converged Security Platform](#)



Incrementemente su ciberseguridad sin aumentar los recursos

Las tecnologías de ciberseguridad, con EDR en el núcleo, han sido aclamadas por el sector y por los clientes, y le permiten detectar y evitar ataques evasivos a gran velocidad, sin que su equipo tenga que realizar ningún esfuerzo adicional.



Kaspersky
Endpoint Security

kaspersky BRING ON
THE FUTURE

kaspersky.es



Dinero móvil: ¿cómo asegurar las aplicaciones bancarias?

Las aplicaciones de banca móvil que ayudan a los usuarios a comprobar los saldos de sus cuentas, transferir dinero o pagar facturas se están convirtiendo rápidamente en productos estándar de las instituciones financieras establecidas. Los bancos están añadiendo servicios y funciones más sofisticadas, permitiendo a los usuarios realizar transacciones más rápidas y eficientes. Y las opciones alternativas de pago online, como la app Venmo de PayPal o Cash de Square, también están ganando popularidad rápidamente. Muchos usuarios aprecian las transacciones rápidas e informales que ofrecen estas aplicaciones.

Pero a medida que estas aplicaciones ganan terreno en el panorama bancario, los ciberdelincuentes no se quedan atrás. Los atacantes pueden utilizar diferentes métodos para

poner en peligro a los usuarios de la banca móvil -desde aplicaciones falsas y de espionaje, hasta ataques a través de conexiones de red maliciosas y el abuso de credenciales de cuentas robadas- y ese no es el final. Los troyanos bancarios se han vuelto más avanzados y sofisticados en 2019. El malware Aunbis, por ejemplo, se ha actualizado continuamente desde que apareció por primera vez en 2018. En 2019, adoptó [sensores basados en movimiento](#) para eludir el análisis de sandbox y las superposiciones para robar información personal identificable. Este agosto también vimos que el [malware bancario Trickbot](#) lanzó una campaña que difundió correos electrónicos de spam con archivos adjuntos maliciosos. Más recientemente, se descubrieron apps falsificadas que impulsaban al [troyano Ginp](#), que roba

la información de acceso del usuario y de la tarjeta de crédito.

Dado que las apps financieras están todas tan estrechamente conectadas o directamente ligadas a las finanzas de un usuario, lo que las convierte en objetivos atractivos para los cibercriminales, la seguridad debería ser una prioridad máxima. A continuación ofrecemos consejos y directrices para asegurar las aplicaciones de banca móvil y añadir capas de defensa para ayudar a evitar las amenazas digitales.

APLICACIONES SEGURAS DE BANCA MÓVIL

- ❖ Descargar desde fuentes confiables y legítimas para minimizar la exposición a apps falsas.
- ❖ Actualizar lo antes posible: la versión más actual de una app tendrá correcciones para las últimas vulnerabilidades conocidas.

JOSÉ BATTAT,
director general
de Trend Micro Iberia



“Dado que las apps financieras están todas tan estrechamente conectadas o directamente ligadas a las finanzas de un usuario, la seguridad debería ser una prioridad máxima”

❖ Habilitar cualquier característica de seguridad incorporada en las apps de banca. Éstas pueden incluir tiempos de inactividad, que requieren que los usuarios vuelvan a iniciar sesión después de cada transacción o transcurrido un período de tiempo.

❖ Eliminar el correo basura y los mensajes con regularidad para reducir las posibilidades de hacer clic en un enlace malicioso, y no abrir ningún archivo adjunto en correos electrónicos no solicitados de remitentes desconocidos.

Establecer conexiones de red seguras

❖ No realizar operaciones bancarias mientras se esté conectado a redes Wi-Fi no seguras en lugares públicos; o bien, utilizar una VPN para cifrar las transacciones.

❖ En un navegador móvil, solo acceder a sitios web bancarios o financieros que utilicen direcciones https y muestren un icono de un candado, indicando que el sitio emplea comunicaciones cifradas.

❖ Cuando se utilicen apps bancarias en un lugar público, utilizarlas a través de 3G, 4G o LTE. Además, hay que desactivar el Wi-Fi y el Bluetooth para evitar el espionaje.

PROTEGER LAS CUENTAS FINANCIERAS ONLINE

★ Habilitar la autenticación de doble factor en todas las apps financieras e instalar apps de autenticación si están disponibles. Los códigos, que se requieren para iniciar la sesión, se suelen enviar por SMS o al autenticador registrado.

★ Deshabilitar la función de autocompletar en las apps financieras o en los inicios de sesión del navegador, y asegurarse de no almacenar las contraseñas en el navegador.

★ No responder a ningún texto o correo electrónico que solicite su PIN, número de cuenta o cualquier número de tarjeta de débito o crédito.

★ Utilizar una contraseña fuerte y única para cada aplicación financiera y asegurarse de cerrar la sesión después de las transacciones.

★ Supervisar las cuentas para poder detectar rápidamente cualquier actividad sospechosa.

HERRAMIENTAS PARA MEJORAR LA SEGURIDAD MÓVIL

Los fabricantes de aplicaciones móviles y las instituciones financieras generalmente res-

ponden a las amenazas y mejoran constantemente sus productos y servicios. Pero, aparte de la aplicación de parches y actualizaciones constantes, hay otras formas de mantener la seguridad de la banca móvil.

Trend Micro Mobile Security for Android e iOS proporciona un completo sistema de seguridad para endpoints de dispositivos móviles, incluida protección frente a las amenazas de seguridad del navegador, la web, los archivos y las apps. La protección Wi-Fi de Trend Micro para Android e iOS proporciona una VPN para hotspots Wi-Fi públicos mediante los servidores de nube seguros de Trend Micro, que cifra la conexión Wi-Fi y evita el secuestro mediante ataques de tipo "man-in-the-middle". Trend Micro HouseCall for Home Networks for Android e iOS (así como Windows y Mac) analiza todos los dispositivos de la red doméstica en busca de fugas de privacidad y otras infecciones de la red, ya que muchos dispositivos de la red doméstica tienen problemas de seguridad que los atacantes pueden utilizar para controlarlos a ellos o a la propia red. ■



Hardware Criptográfico para soluciones PSD2 y Aplicaciones Blockchain en el ámbito financiero

JESÚS RODRÍGUEZ CABRERO,
Fundador / Presidente
y CEO de REALSEC



Hoy nadie duda que la Banca Digital ya no es una opción y que el éxito de su desarrollo exige el cumplimiento, por parte de las entidades financieras, de las normativas de seguridad. Además de aportar múltiples beneficios, en términos de optimización y confianza, a los usuarios finales.

En el nuevo escenario financiero, donde conviven la banca tradicional, las Fintechs y otros modelos de Open Banking, tales como las transacciones efectuadas a través de plataformas como Amazon o Google, entre otras, la seguridad en los medios de pago, además de una necesidad es un requerimiento a cumplir.

Por lo tanto, las entidades financieras deben securizar sus transacciones financieras en línea a los estándares definidos por el consor-

cio PCI (VISA y Mastercard) y para ello, es de obligado cumplimiento la implementación de un hardware criptográfico, cuyo valor y credibilidad reside en que éste cuente con la certificación PCI HSM PTS v2.0 o superior, conforme al PCI Security Standards Council; o en ciertos casos, con la certificación FIPS 140-2 Level 3 por el NIST, según los requerimientos exigibles o recomendados en cada proceso de negocio.

CUMPLIMIENTO NORMATIVA DE PAGO PSD2

La entrada en vigor de la nueva Directiva Europea de Servicios de Pago PSD2, obliga a las entidades financieras a poner a disposición de terceros, actores en el ámbito financiero, los datos de sus clientes y a implantar soluciones de autenticación de doble factor (SCA), o au-

tenticación robusta (identificación y validación de la identidad), para evitar así los problemas de fraude derivados de la suplantación de identidad.

Dichas soluciones de autenticación robusta, utilizan claves que deberían de ser generadas y custodiadas en dispositivos criptográficos (HSMs) para dotar al proceso de autenticación de las máximas garantías de seguridad y confianza.

Muchas entidades financieras que no tienen implantadas soluciones de autenticación robusta, han optado por el envío de un mensaje SMS a sus clientes, con el uso de una clave de autenticación para validar las transacciones realizadas a través de medios digitales. Pero el elevado coste de los SMS por operación, les

“El objetivo de la normativa PSD2 no es otro que proteger, mediante una autenticación reforzada, de doble o triple factor, tanto al cliente como a la propia entidad”

predispone a implantar soluciones tecnológicas de autenticación robusta SCA más eficientes y seguras.

El objetivo de la normativa PSD2 no es otro que proteger, mediante una autenticación reforzada, de doble o triple factor, tanto al cliente como a la propia entidad, frente al riesgo de fraude por robo y suplantación de la identidad.

BLOCKCHAIN EN EL ÁMBITO FINANCIERO.

El auge experimentado por la tecnología Blockchain en el último año está poniendo su foco en diversos sectores, entre otros en el sector financiero, siendo cada vez mayor el número de entidades y organismos vinculados al sector financiero, que ya están trabajando en proyectos, en muchos casos piloto, con tecnología “open source” como es el caso de Corda o Hyperledger.

El dinero utilizado por la tecnología Blockchain son los tokens, objetos similares a las monedas, pero sin valor de curso legal negociable o fungible. Sin embargo, la tecnología de Blockchain va más allá de la propia gestión de activos (criptomonedas), y puede ser utilizada

en otros muchos procesos de negocio no solo en el ámbito financiero.

Tomando como punto de partida un “Smart Contract”, es posible registrar en bloque, de forma distribuida y compartida entre las diferentes partes, cualquier tipo de información o transacción con el consenso y aprobación de sus partícipes.

Dicho consenso, permite la eliminación de intermediarios, proporcionando confianza y solidez a la cadena de bloques, cuya inalterabilidad y robustez la proporciona el cifrado y conjunción de cada uno de los bloques, mediante el uso de una función criptográfica tipo resumen denominada “hash”.

Sin embargo, como ocurre con cualquier algoritmo o función criptográfica, un “hash” o función resumen puede realizarse por software, o bien haciendo uso de una plataforma de hardware criptográfico (HSM) para reforzar la seguridad, y así tener la certeza de que las claves privadas utilizadas en el proceso de la firma digital de las transacciones, no estén expuestas, y se encuentren almacenadas y custodiadas en un dispositivo seguro y aislado.



Si además el HSM cuenta con el nivel de certificación adecuado otorgado por un organismo de confianza, estaremos reforzando la seguridad de procesos y transacciones, garantizando la inalterabilidad de lo cifrado o firmado digitalmente.

Actualmente, existen en el mercado plataformas hardware y software para nodos de Blockchain, los cuales permiten la incorporación de aplicaciones de forma virtualizada, y que para reforzar la seguridad incorporan un HSM que realiza las funciones criptográficas necesarias, permitiendo hacer uso de un “hash” y de otros algoritmos de criptografía asimétrica, eje central de la firma digital, como es el caso del algoritmo de curvas elípticas (ECDSA).

En definitiva, el objetivo perseguido por las entidades financieras, en cuanto a la seguridad de las transacciones que hacen uso de la tecnología de Blockchain, es que la información replicada sea inmutable y que no pueda ser manipulada ni alterada. ■

PCI DSS, el nuevo reto de seguridad en los servicios de pago digitales

MIGUEL ÁNGEL ROJO,
CEO en BOTECH



La sociedad se encuentra inmersa en un proceso de mejora continua en materia de seguridad que no se puede detener ni un solo minuto, ya que el cibercrimen innova a velocidad de vértigo. Si procesas, guardas o transmites datos de tarjetas de pago, para garantizar un exhaustivo control de estos datos, es necesario cumplir con la certificación PCI-DSS. Este estándar de seguridad de referencia en la industria de las tarjetas de pago acredita que el tratamiento de la información confidencial que se maneja se ejecuta con el máximo nivel de protección y seguridad. Este modelo de seguridad, que otorga el PCI SSC (Payment Card Industry Security Standards Council), persigue, y consigue, reducir y evitar el fraude en este ámbito.

El método de pago más extendido entre los consumidores continúa siendo la tarjeta de

crédito y de débito. De hecho, según los últimos datos del Banco de España, las tarjetas de crédito alcanzaron su cifra récord el año pasado y el número de tarjetas de pago en circulación se situó en torno a los 85 millones. Una tendencia alcista que obliga a actualizar constantemente las normativas para regular su uso y velar por la seguridad en los servicios de pago. La normativa 'estrella' cuando se habla de tarjetas de pago es la denominada PCI DSS, una gran conocida por el sector financiero e imprescindible en cualquier negocio que opere con ellas, sin importar su tipo de actividad. Ya que, si una organización procesa, guarda o transmite datos de tarjetas debe cumplir con el estándar PCI DSS, porque si no corre el riesgo de perder su permiso para procesar tarjetas, puede enfrentarse a rigurosas auditorías e

incluso ser sancionada con el pago de cuantiosas multas. Una normativa que permite minimizar el fraude e implementar buenas prácticas de seguridad.

UNA NORMATIVA EXIGENTE QUE TRANSMITE CONFIANZA Y SEGURIDAD

Pero ¿qué es PCI DSS? Es una normativa que busca garantizar la protección de datos y la seguridad en las transacciones económicas. Cumplir con esta regulación es muy importante, no sólo para poder seguir con la actividad de un negocio, sino porque con ella también se transmite confianza y seguridad a los consumidores. La peculiaridad de esta normativa es que consta de seis categorías, 12 requisitos, alrededor de 200 controles y 250 procedimientos de prueba con el fin de garantizar la confidencialidad de

“La peculiaridad de la normativa PCI DSS es que consta de seis categorías, 12 requisitos, alrededor de 200 controles y 250 procedimientos de prueba”

los datos. Sin duda, una normativa muy exigente que necesita una persona responsable dentro de la compañía dedicada a ello.

Además, el principal reto del sector financiero continúa siendo la protección de datos sensibles, tanto de manera interna como externa. Por eso, el estándar PCI-DSS es cada vez más requerido por las empresas, sobre todo por temas relacionadas con el negocio, como son las grandes marcas Visa, Master Card o American Express (Amex).

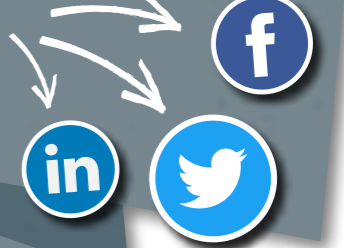
Los requisitos fundamentales que es necesario cumplir para conseguir la certificación son varios. Por un lado, es necesario construir y mantener una red segura, a través de la instalación y mantenimiento de una configuración firewall para proteger los datos y evitar el uso de contraseñas o valores predeterminados suministrados por los proveedores. Por otro lado, se protegen los datos de los titulares de las tarjetas cifrando la transmisión de datos e información confidencial de los titulares a través de redes públicas abiertas. Además, se

debe establecer un programa de gestión de vulnerabilidades y crear medidas sólidas de control de acceso, limitando el acceso a la información únicamente a las empresas que lo necesiten, asignando una identificación única a cada persona con acceso al sistema y restringiendo el acceso físico a los datos solo a los propietarios de la tarjeta. Y, por último, se deben monitorizar y testar regularmente las redes y mantener una política de seguridad de la información siempre actualizada.

Aunque pueda parecer complicado, se puede cumplir con PCI DSS, no es imposible. Solo es necesario contar con un apoyo experto para lograr su implementación de forma eficiente. Desde BOTECH, compañía española especializada en ci-

¿Te gusta este reportaje?

Compártelo
en redes



berseguridad, junto a nuestro partner 1st Secure IT referente mundial en certificaciones PCI-DSS desde hace más de una década en EEUU y Latinoamérica, impulsamos el cumplimiento de la normativa para ayudar a nuestros clientes, para que puedan garantizar la protección de datos y la seguridad en las transacciones económicas online, minimizar el fraude y al mismo tiempo que evitar cuantiosas sanciones por el incumplimiento de PCI DSS. ■



El sector financiero, uno de los principales objetivos de los ataques dirigidos digitales

El atractivo del dinero convierte al sector de los servicios financieros en el objetivo principal de algunos de los cibercriminales más peligrosos. El hecho de que los sistemas estén interconectados, y que el uso de los dispositivos móviles se encuentre muy extendido tanto para el acceso remoto como para compartir datos convierte a las organizaciones financieras en foco de ataques tanto genéricos como dirigidos.

Además, resulta cada vez más evidente que, debido a los avances en las tecnologías fraudulentas, los cibercriminales están desviando su atención de los clientes «fáciles» y la están centrando en objetivos más difíciles, pero de los que pueden obtener mayores beneficios, como son los proveedores de servicios en sí mismos, es decir, las entidades financieras de todo tipo, tanto grandes bancos como empresas Fintech.

EL SECTOR FINANCIERO, UNO DE LOS MÁS PERJUDICADOS

Si nos fijamos en los datos sobre el coste de estos ataques, y de acuerdo con el último [informe de la consultora Accenture sobre el coste del cibercrimen](#), las entidades financieras aparecen como las más perjudicadas en comparación con el resto de sectores. Según dicho estudio, el coste medio anual del cibercrimen en el mundo financiero creció un 11% desde los 16,6 millones de dólares de 2017 a los 18,4 millones en 2018.

A esto hay que sumar que 2019 ha sido testigo de varios de los desarrollos más significativos en la industria del malware, algunos de los cuales ya anticiparon nuestros especialistas de investigación de Kaspersky. Entre ellos se cuenta el surgimiento de nuevos grupos de cibercriminales y

nuevas geografías en los ataques de grupos de ciberdelincuentes, que se centran en los datos para ayudar a eludir los sistemas antifraude en sus ataques, así como el incremento en el número de datos de comportamiento y biométricos a la venta en el mercado del cibercrimen.

PREVENIR, DETECTAR, RESPONDER Y PREDECIR

La ciberseguridad debe ser un proceso constante, que aborda las amenazas de forma integral. No se trata solo de prevenir los incidentes, sino también de predecir, detectar y responder de forma eficaz, flexible y fiable.

Los productos de seguridad basados en la prevención pueden ofrecer una protección muy eficaz frente a amenazas comunes, como el malware, los ataques de red y la filtración de

ALFONSO RAMÍREZ,
Director General
Kaspersky Iberia



“La ciberseguridad debe ser un proceso constante, que aborda las amenazas de forma integral”

datos. Pero incluso estas tecnologías no bastan por sí mismas para proteger a una empresa de ataques dirigidos o más sofisticados. Las tecnologías de seguridad convencionales basadas en la prevención pueden detectar ciertos incidentes, pero suelen fallar a la hora de determinar si los incidentes aislados forman parte de un ataque mucho más complejo y peligroso que podría estar causando graves daños a su empresa y que seguirá infringiéndolos a largo plazo. Dicho esto, las tecnologías basadas en la prevención a varios niveles siguen siendo un elemento fundamental de este nuevo enfoque proactivo para la protección contra ataques.

Cuanto antes se detecte un ataque, menores serán las pérdidas financieras y el tiempo de interrupción del negocio. De ahí la importancia de una adecuada tecnología de detección. Muchos ataques son complejos y compuestos, por lo que su detección exige un profundo conocimiento sobre cómo funcionan. Se necesitan tecnologías de detección capaces de acceder a los datos de inteligencia de amenazas en tiempo real, capaces de realizar análisis detallados de comportamientos

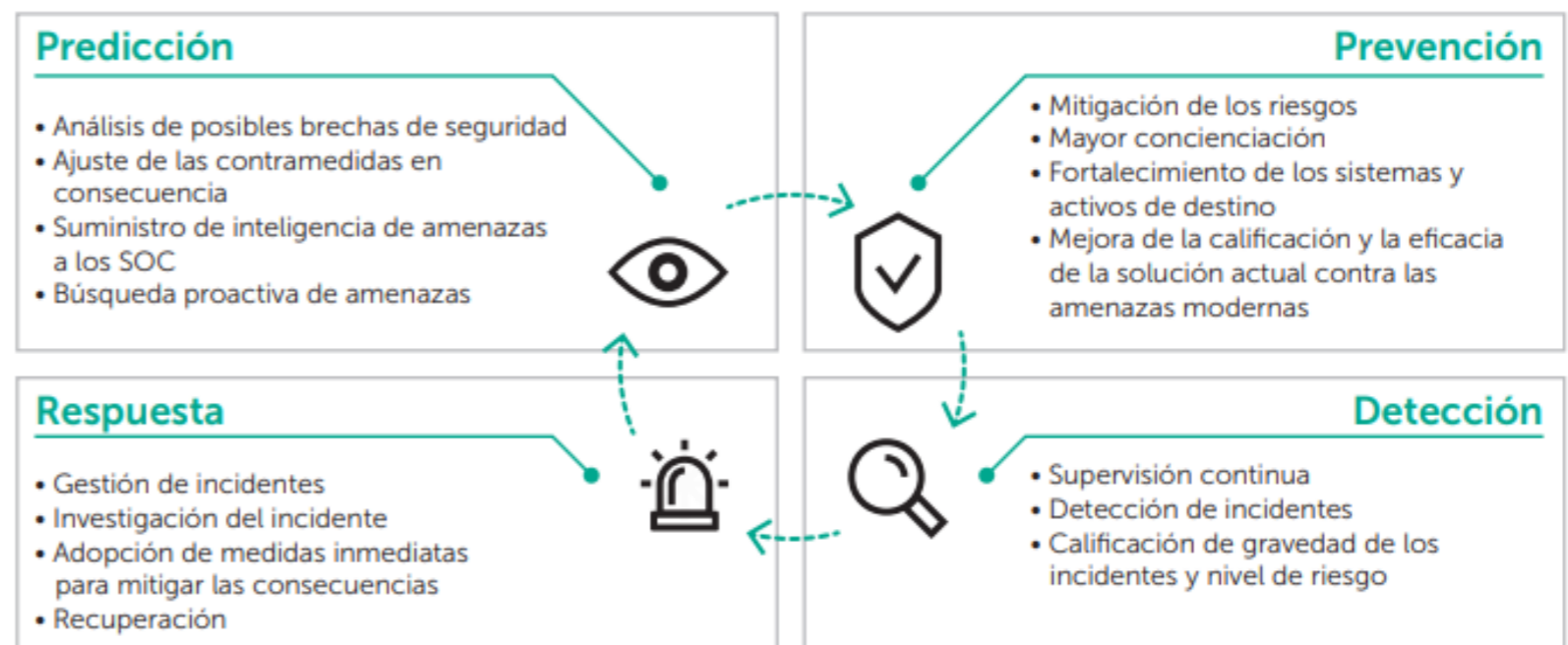
sospechosos que pueden estar ocurriendo en diferentes niveles de la red.

Como es lógico, de poco vale la detección de una amenaza si no estamos en condiciones de responder a ella de manera ágil. Después de detectar un ataque se requieren expertos de seguridad con habilidades y experiencia que ayuden a evaluar y rectificar el daño, que sean capaces de recuperar rápidamente sus operaciones, recibir información inteligente de la acción a llevar a cabo después del proceso de investigación de incidentes, y que además sea capaz de planificar acciones que impidan que el ataque vuelva a repetirse.

Por último, aunque no menos importante, y dado el panorama de amenazas en constante cambio, la predicción es un elemento clave en



toda estrategia de seguridad. Dicha estrategia debe evolucionar constantemente para hacer frente a los nuevos retos. La seguridad no es una “actividad puntual”, es un proceso constante que pasa por la evaluación continua de: las últimas amenazas y la eficacia de las medidas de seguridad para que una empresa pueda adaptarse a los nuevos riesgos y las exigencias cambiantes. ■



La revolución digital del sector financiero

NURIA ANDRÉS,
Territory Account Manager
Spain&Portugal de
Forcepoint



El sector financiero, además de ser uno de los sectores más regulados, desde el punto de vista de la seguridad, por la gran cantidad de normativas a las que está sujeto (GDPR, MiFID II, PSD2,...), está inmerso en la 4ª Revolución Industrial, la Revolución Digital. Y sin lugar a dudas, el gran reto de la transformación digital es también la Ciberseguridad.

Entre los principales retos a los que tiene que hacer frente este sector, encontramos “el viaje” al Cloud, pero también la gran cantidad y los distintos tipos de usuarios a los que hacer frente. Desde Traders, a directores de oficina, pasando por operadores en un call center externalizado o, por supuesto, nosotros, los clientes. Es por esto que, en este tipo de

entornos, es primordial discernir, donde está realmente la amenaza, porque no será solo externa, sino también puede ser interna, el llamado “insider threat”.

Es decir, en este entorno es clave proteger la información, allá donde esté, pero también saber discernir entre usuarios legítimos y usuarios maliciosos. Y precisamente, la visión de la ciberseguridad de Forcepoint tiene estos dos pilares: la protección de los datos, estén en Data Centers onpremise, o en el Cloud (0365, AWS, SFDC,..) y el análisis del comportamiento de los usuarios.

Esto también está totalmente alineado con el “viaje” al CLOUD. El perímetro que hemos conocido, hasta no hace demasiado tiempo,

ya no existe. Precisamente, en el sector financiero este perímetro se ha protegido con mucho ahínco. Hemos desplegado NGFWs de Front-End, de Back-End, hemos apostado por la microsegmentación dentro del Data Center, soluciones de Sandboxing....pero ya lo dice Gartner, “el futuro de la seguridad de Red, está en el Cloud”. Incluso han acuñado un nuevo termino, SASE (Secure Access Service Edge).

Es decir, el nuevo perímetro es el propio usuario, la identidad del usuario. Y en función de la identidad del usuario, se proporcionarán, desde el Cloud, en tiempo-real, políticas de seguridad de red (NGFWaaS, Threat PreventionaaS, ProxyaaS, DLPaaS, ..y tantos otros servicios de seguridad). Se monitorizarán continuamente

“Es hora de evolucionar las estrategias de seguridad centradas en la infraestructura, en aproximaciones centradas en el análisis del comportamiento de los usuarios”

las conexiones, e incluso, en Forcepoint, y esto es lo que nos hace diferentes, en base al comportamiento de los usuarios, en tiempo real, se podrán aplicar distintas políticas de seguridad. Es decir, proponemos migrar de políticas de seguridad estáticas, a políticas de seguridad dinámicas, en base al comportamiento de los usuarios.

Pero también es hora de apostar por la seguridad, conectada y automatizada. Tenemos que dejar de seguir montando silos de soluciones de seguridad, y poder desplegar políticas de seguridad desde el Endpoint al Cloud. Y el amplio portafolio de soluciones de seguridad de Forcepoint, también lo permite. De hecho, nuestras soluciones se pueden aglutinar en tres grandes bloques:

¿Te gusta este reportaje?

Compártelo en redes



❖ **DUP-Dynamic User Protection (Protección dinámica de los usuarios):** Son soluciones que analizan el comportamiento de los usuarios. Por ejemplo, tenemos soluciones específicas para detectar Insiders Threats, que encajan muy bien en entornos de Trading.

❖ **DDP - Dynamic Data Protection (Protección dinámica del dato):** Aplicamos el análisis del comportamiento de los usuarios, a la protección del dato. Es lo que podríamos llamar Next-Generation DLP. De hecho, Gartner ya no habla de DLP, sino de “Data Lifecycle Protection”, la protección del ciclo de vida del dato.

❖ **DEP - Dynamic Edge Protection:** Aglutina las soluciones, quizás más tradicionales, como son nuestros NGFW, Proxy, Correo (sigue siendo uno de los principales vectores de ataque) o CASB, pero con el “matiz” SASE. Nuestras soluciones pueden ser On-Premise, CLOUD o Híbridas, para permitir precisamente ese viaje al CLOUD, y llevar a cabo la transformación digital que está llevando a cabo todo el sector financiero. ■



Forcepoint

Human-Centric Cybersecurity

Los humanos son el nuevo perímetro

Forcepoint protege sus datos y usuarios dondequiera que estén

[Solicite una demo](#)

www.forcepoint.com/es



Protección del usuario



Protección del dato



Protección del edge