Nuevos retos de seguridad en entornos financieros

Su impacto en el modelo de negocio

Patrocinadores:

El sector financiero ante el reto de la ciberseguridad:

la digitalización abre la puerta a nuevas amenazas

Los riesgos de las TIC representan un enorme desafío para las entidades financieras y subrayan la importancia de implementar una adecuada estrategia de seguridad que abarque, desde la protección de infraestructuras hasta la seguridad de datos y usuarios. La formación y concienciación del usuario son también clave, a fin de que este se convierta en un eslabón más de la cadena en la protección.

NUEVOS RETOS DE SEGURIDAD EN ENTORNOS FINANCIEROS

A lo largo de la última década, las entidades financieras, principalmente los bancos, han acometido un importante cambio en su modelo de negocio, apostando claramente por la digitalización como motor de innovación y puntal clave en su relación con el cliente. Así las cosas, este sector ha ido avanzando desde una huella digital básica hasta un entorno basado en la omnicanalidad, con el desarrollo de nuevos productos y servicios y un mejor y mayor aprovechamiento de tecnologías disruptivas, como la inteligencia artificial, el blockchain, la analítica y las tecnologías basadas en la nube.

Sin duda, esta creciente digitalización ha favorecido importantes beneficios: el customer centric es una realidad cada vez más consolidada, pero también ha generado significativos retos y riesgos no financieros, como la dependencia de proveedores y nuevos jugadores y la proliferación de ciberataques y amenazas online, exposiciones que se han multiplicado por el aumento de dispositivos electrónicos, la migración a la nube y la apertura de puertas y ventanas que han terminado por diluir el perímetro de la red. En este sentido, datos facilitados por el Fondo Monetario Internacional (FMI) apuntan que el número de ciberataques se ha triplicado en la última década, convirtiéndose en una amenaza para la estabilidad financiera. Según esta organización, en 2020 se produjeron 1.500 casos, frente a los 400 de 2012.

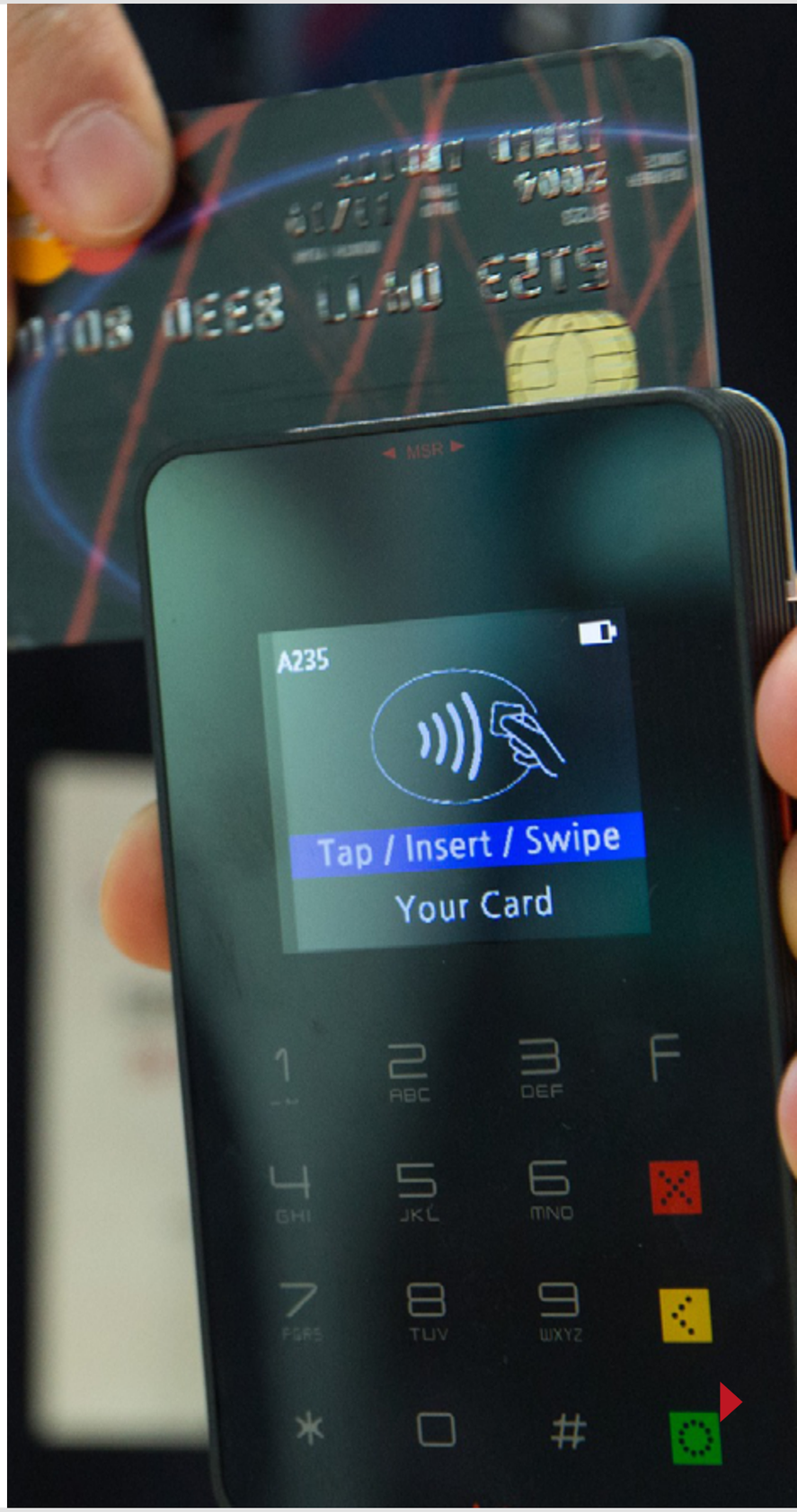
Del mismo modo, la aceleración de los planes de digitalización de estas compañías y, sobre todo, la generalización del teletrabajo a causa de la Covid-19, ha dilatado el nivel de riesgo, al abrirse nuevas vías de ataques que los ciberciminales han sabido aprovechar.

Así, este nicho ha experimentado la segunda mayor proporción de ciberataques relacionados con COVID-19, solo por detrás del sector de la salud, con un coste promedio por brecha de datos de 5.85 millones de dólares en 2020, frente a los 3.86 millones de dólares del promedio mundial, según datos de la última edición del informe anual Cost of a Data Breach Report de IBM.

EL DESAFÍO DE LA CIBERSEGURIDAD

La banca se enfrenta, por tanto, a un panorama difícil en materia de ciberseguridad, con ataques cada vez más complejos, muchos de los cuales se dirigen contra el usuario, el eslabón más débil, contra la propia infraestructura o hacia proveedores externos (ataques a la cadena de suministro). Así, a ofensivas de relleno de credenciales, fraude de apropiación de cuentas, correos electrónicos de phishing o malware (troyanos), se unen otras amenazas como el ransomware, que incluye vectores de doble extorsión y factor humano, junto con la creciente demanda de desencriptación de datos, y los ataques DDoS.

Detrás de estos ataques se esconden no solo criminales cada vez más osados, sino también estados y atacantes patrocinados por estados



que saben que por la sensibilidad de los datos que custodian, los bancos son un blanco fácil. Tanto es así, que, hoy por hoy, el ciber riesgo se encuentra en tercer lugar en el ranking de riesgos de entidades financieras, después de los lucros cesantes y el riesgo pandémico, según el 10º Barómetro de Riesgos de Allianz 2021.

Afortunadamente, y por los activos que gestionan (dinero, datos sensibles y reputación) en el sector financiero siempre ha existido una gran concienciación sobre la seguridad, tanto en la vertiente física como lógica. Se trata de un factor de confianza. Así, las entidades financieras destinaron en 2020 el 10,9% de su presupuesto a ciberseguridad, frente al 10,1% del año anterior. En términos de gasto por empleado, esto supone alrededor de 2.700 dólares, según una encuesta de Deloitte y FS-ISAC.

Ahora bien, es necesario que esta seguridad evolucione al mismo ritmo que lo hacen las tecnologías, los servicios provistos y la regulación (PSD2, Mifid2, CRD2...), sin olvidar, por supuesto, como lo hacen también la tecnología de ataque y los hackers, alumnos aventajados.

Por ello, y además de proteger infraestructuras como los ATMs, es necesario apostar por soluciones centradas en el resguardo del endpoint, la red, email, servidores o workloads en la nube, como antivirus, plataformas EDR, XDR o con capacidades de aprendizaje automático. Asimismo, estas entidades deben avanzar hacia un enfoque proactivo, que dé prioridad a la prevención, para interrumpir los ataques antes de que el malware o la amenaza maliciosa -sin archivos- pueda siquiera comenzar a ejecutarse. También, la monitorización y gestión de lo que ocurre en redes botnets o en la Deep Web ayudará a prevenir y a mejorar la seguridad, con planes de respuesta. Esto incluye la formación de los empleados en materia de concienciación sobre la seguridad, la limitación de los privilegios de los administradores y una estrategia de confianza cero que abarque la gestión de la identidad y el acceso, así como la seguridad de la red. Importante igualmente es la colaboración entre entidades y con terceros, a fin de garantizar la resiliencia operativa digital.

EL RIESGO DE LA BANCA MÓVIL

Adicionalmente, la expansión de los servicios basados en dispositivos móviles (banca móvil) y la mayor dependencia de los clientes de las aplicaciones de banca electrónica ha ampliado su vulnerabilidad, convirtiéndose estos usuarios en blancos potenciales para los actores maliciosos, que utilizan una variedad de técnicas, incluidos troyanos bancarios basados en aplicaciones bancarias falsas, para atacarles. Así, la actividad de los troyanos bancarios se ha intensificado un 15%, según un estudio de Check Point, y estos se orientan, sobre todo, a atacar el segundo factor

de autenticación, principalmente SMS, para además de robar datos de acceso o credenciales, hacerse con otros más personales.

Ante esta situación y para protegerse, los bancos deben integrar metodologías o tecnologías que ayuden a asegurar las transacciones electrónicas, como la criptografía, o que faciliten la autenticación del usuario para evitar la suplantación de identidad, como los sistemas de tokenización. Igualmente, y de cara a ser más precisos, es fundamental securizar y custodiar las claves que protegen esa información (claves de cifrado) y la gestión de su ciclo de vida, sobre todo ahora, cuando se está produciendo una clara orientación a los servicios en la nube. En este sentido, los HSMs, capaces de almacenar y proteger claves criptográficas en consonancia con las normas más rigurosas de la industria, como la Directiva Europea de Pagos PSD2, son una opción.

PROTEGER EL DATO

La progresiva implantación de modelos comerciales, como el open banking, asentado en el intercambio de datos entre bancos y terceros (Bigtech) a través de APIs, está ocasionando distintos problemas de protección, sobre todo en el ámbito de la seguridad (de usuarios y entidades) y el análisis de datos. Según McKinsey & Company, los bancos son responsables de mitigar el riesgo de fraude y deben implementar controles, que incluyan análisis avanzados (por ejemplo, para validar el origen de las llamadas entrantes a la API), modelos de

Blockchain: riesgo u oportunidad

Los bajos tipos de interés, la reducción de márgenes, y los nuevos requerimientos regulatorios están presionando a la banca para buscar nuevas fórmulas que le permitan ganar en competitividad y rentabilidad. En este contexto, tecnologías como blockchain, suenan cada vez con más fuerza, en tanto en cuanto permiten realizar directamente entre partes, transacciones seguras con el apoyo de máquinas y algoritmos.

Asociada esta tecnología a las criptomonedas, una de las formas más populares y conocidas de usar blockchain, sus capacidades van sin embargo más allá de su almacenaje e intercambio, desde transacciones en tiempo real hasta tokenización de activos, préstamos y créditos, valores, prevención del fraude e identificación de los clientes. Además, sus capacidades de seguridad, apoyadas en la descentralización de la información, así como, en la eliminación de intermediarios, y la implementación de criptografía y firma digital para asegurar las transacciones, favorecen que estas operaciones (y sus datos) tengan la mayor seguridad, privacidad y autenticidad posible.

Sin embargo, y aunque Blockchain es una tecnología bastante segura en su diseño, su incorporación en mercados y entornos regulados, como el financiero, está produciéndose lentamente. Aún se tienen que garantizar aspectos de su seguridad, muchos de ellos relacionados con la ausencia de estándares tecnológicos, la falta de interoperabilidad entre distintas plataformas de cadenas de bloques o el uso de contratos inteligentes, que puedan ser origen de fugas de datos de carácter personal, y que hace necesario incorporar metodologías de seguridad por diseño desde las primeras fases de desarrollo, para evitar riesgos como: minado de cadenas laterales o paralelas (sidechain) o ataques DDoS, entre otros.

También y en lo que tiene que ver con el sistema de autenticación de la gestión de accesos a los sistemas blockchain, y aunque la normativa europea obliga a la banca a tener sistemas de autenticación de doble o triple factor, es necesario avanzar, sobre todo, por su relación con otros sistemas de información de la empresa.

Estos aspectos podrían solucionarse con la creación segura de claves o que el proceso de firma de cada una de las transacciones que se lanzan al bloque sea invulnerable. Es necesario validar el uso de blockchain como registro fundamentado y vinculante de evidencias digitales, definiendo en qué condiciones es válido. No hay duda de que si alguien descuida la custodia de sus claves éstas podrían acabar en manos de un atacante que podría así suplantar su identidad en la aplicación correspondiente. También hay que tener en cuenta que, debido al potencial de esta tecnología, es previsible que los ciberdelincuentes busquen oportunidades para atacar cualquier vulnerabilidad, tanto humana como técnica, en el ecosistema de blockchain.

autenticación segura del cliente y herramientas sólidas para detectar ataques de fraude, de acuerdo a PSD2. Estas normas también requieren que los bancos proporcionen un "sandbox" protegido a los proveedores de servicios de pago para las pruebas y el desarrollo continuo de servicios que utilizan la interfaz del banco.

Además de involucrarse en oportunidades de negocio innovadoras y potencialmente lucrativas abiertas por PSD2, el sector financiero se ha lanzado de lleno hacia una mejora real en la eficiencia, escalabilidad y flexibilidad de la mano de la Nube, para asegurar, en tiempos de pandemia, una fuerza de trabajo a distancia y garantizar la capacidad de recuperación. De este modo, y con los usuarios, dispositivos, aplicaciones y datos fuera del centro de datos empresariales y la red, la necesidad de proteger esos activos, así como de poseer una visibilidad completa del entorno se ha hecho imperativo. A este respecto, IDC Research confirma que cualquier solución de seguridad para cloud ha de incluir tres elementos: integración nativa, protección amplia y gestión y automatización. En torno a esta premisa han surgido marcos de seguridad como SASE, que esboza una convergencia de múltiples funciones de seguridad, como acceso de red Zero Trust (ZTNA), Gateway Web Seguro (SWG) de próxima generación, Agente Seguro de Acceso a la Nube (CASB), Gestión de la Postura de Seguridad Cloud (CSPM) o Firewall como Servicio (FWaaS); entregados desde la nube.

Además de la nube, la externalización de las funciones y servicios de las TIC, que ha cobrado mayor importancia durante la actual crisis sanitaria, puede plantear también retos relacionados con la gestión del riesgo de terceros, la confidencialidad y la protección de los datos de los consumidores. Igualmente, la inclusión del aprendizaje automático y de la inteligencia artificial están acrecentando esta vulnerabilidad, cuando, por ejemplo, los datos corruptos no detectados se introducen en los algoritmos y se utilizan en la toma de decisiones, según Bank for International Settlements (BIS). Por último, y en el caso de sufrir un episodio de ransomware, la recuperación de los datos, podría tornarse muy compleja, y las dudas sobre la exactitud de la información recuperada podrían hacer que el problema se prolongue durante un largo periodo de tiempo.

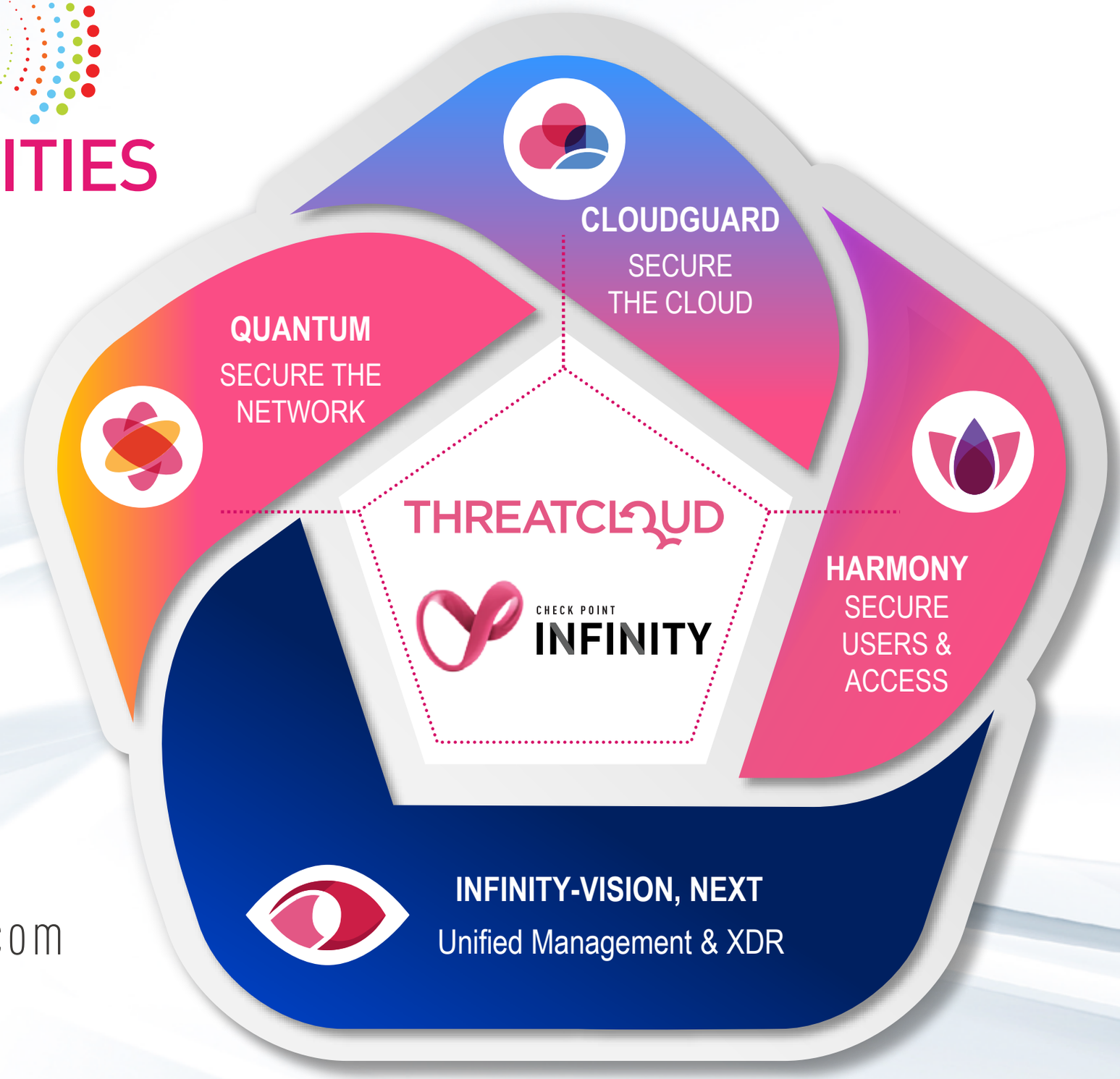
No hay duda, por tanto, que el gran volumen de datos generados por la banca requiere de la facultad de analizar y proteger dicha información, manteniendo y acatando, al mismo tiempo, las estrictas normas de la UE en materia de privacidad y protección de datos. Asimismo, el aumento de la demanda de servicios financieros en línea, y la progresiva modernización de los sistemas de pago, según el dinero en efectivo va perdiendo preponderancia, llevan a cuidar todos los aspectos de la seguridad. Cualquier incidente podría socavar la confianza del cliente, por lo que la ciberseguridad es más esencial que nunca. ■

MÁS INFORMACIÓN

- Incremento de ciberataques en la ultima década
- Ciberataques relacionados con la Covid-19
- Cost of a Data Breach Report
- 10º Barómetro de Riesgos de Allianz 2021
- Madurez en la ciberseguridad y riesgos en las instituciones financieras
- Actividad de los troyanos bancarios
- Directiva Europea de Pagos PSD2
- PSD2 y la disrupción en el open banking
- El efecto de los datos corruptos
- Bajos tipos de interés

Check Point®
SOFTWARE TECHNOLOGIES LTD

NEW WORLD
NEW OPPORTUNITIES
2021



MÁS INFORMACIÓN:

www.checkpoint.com/es

info_iberia@checkpoint.com

Nuevos retos de seguridad en entornos financieros;
su impacto en el modelo de negocio

Más tarde o más temprano las entidades financieras pueden ser víctimas de un ciberataque. Con esa idea en mente, deben prepararse para responder a las amenazas de hoy pero también a todas aquellas que van surgiendo al amparo de las nuevas tecnologías.

MESA REDONDA IT: Nuevos retos de seguridad en entornos financieros; su impacto en el modelo de negocio

El sector financiero, sobre todo la banca, lleva años sumido en una profunda transformación digital que le ha llevado a afrontar una serie de cambios, tanto en el modo de ofrecer y prestar sus servicios como en el de atender a sus clientes. Asimismo, la situación derivada de la COVID-19 ha transformado el comportamiento del consumidor, desde las preferencias de canal hasta el método de pago, y ha abierto una importante brecha en ciber-

“Las organizaciones tienen que actualizar o desarrollar sus propios sistemas de ciberseguridad según se detectan nuevos sistemas de ataque. Afortunadamente hay bastante concienciación en ciberseguridad”

EUSEBIO NIEVA,
DIRECTOR TÉCNICO DE CHECK POINT

seguridad, al incrementarse la digitalización y, por ende, la superficie de ataque. Por todo ello, ¿cuáles son los principales retos de ciberseguridad a los que se enfrentan actualmente entidades y servicios financieros? Para hablar sobre ello y conocer cómo afrontan los nuevos ataques y amenazas; su grado de concienciación al respecto de la ciberseguridad; cómo se ha adaptado este sector a tecnologías emergentes como blockchain o las nuevas normativas como PSD2; o cuál debe ser el siguiente paso en la adopción de nuevas tecnologías de seguridad, hemos contado con la participación en esta Mesa Redonda IT de Eusebio Nieva, Director Técnico de Check Point; Javier Sánchez, Territory Sales Manager de Entrust; Luis Javier Suárez, Presales Manager de Kaspersky; Jesús Rodríguez, CEO de Realsec; Igor Unanue, CTO de S21sec; Alfonso Martínez, Country Manager, Data Protection de Thales; y José de la Cruz, Director Técnico de Trend Micro Iberia.

RETOS EN CIBERSEGURIDAD

La creciente digitalización ha abierto la puerta a importantes retos en materia de ciberseguridad que, aunque extensibles a todos los verticales, en el financiero se perciben aún más. En este sector se maneja algo que todos los atacantes quieren: “dinero”, asegura Eusebio Nieva, por lo que no se debe confiar en sistemas tradicionales como protección frente a amenazas desconocidas. “Las organizaciones tienen que actualizar o desarrollar sus propios sistemas de ciberseguridad según se detectan nuevos sistemas de ataques”. Afortunadamente hay bastante concienciación en ciberseguridad.

Efectivamente, la cada vez mayor sofisticación por parte de los cibercriminales lleva a un nuevo paradigma en el que, según Luis Javier Suárez, “ya no basta con confiar en soluciones que aseguren un elevado grado de prevención, sino que se ha de plantear la hipótesis de poder estar siendo comprometido y no saberlo”. Aquí ya entra la parte de recoger ciertas métricas, telemetrías o anomalías para poder hacer un análisis y ver cómo cambian las normas del juego.

En idéntica línea, José de la Cruz recurre al planteamiento Zero Trust; “hay que asumir que

va a existir una brecha, y estar preparados para detectarla y actuar". Además, destaca dos retos que apuntan a la protección de las infraestructuras, donde hay una amalgama de tecnologías tradicionales y modernas combinadas, y a los usuarios, externos e internos. "Debemos dotarles de una seguridad que les aporte visibilidad sobre lo que ocurre en sus entornos".

Sobre estos retos, Igor Unanue considera, que, por el propio proceso de digitalización, estas organizaciones integran nuevas tecnologías, aplicaciones... que están atrayendo nuevos tipos de ataques, como los de tipo hacking, que permanecen en las redes internas largo tiempo sin ser descubiertos, causando importantes daños. "Van a seguir descubriéndose nuevas amenazas. La banca debe mantenerse alerta y estar corrigiendo para poder protegerse mejor".

UN NUEVO CONCEPTO DE BANCA

La progresiva digitalización ha marcado una senda de cambios. Se ha pasado del cliente físico al cliente móvil, de los centros de datos al cloud, ampliándose, al mismo tiempo, los vectores de ataque, lo que ha supuesto una mayor vulnerabilidad. ¿Cómo está enfocando la banca estos cambios?

Desde la perspectiva de este desarrollo, Javier Sánchez, observa que, en la actualidad, el vector de relación entre la banca y el usuario es la aplicación, por lo que hay que protegerla. "Las apps son un riesgo para los usuarios, que pueden ver comprometidos sus datos, y para los bancos, por el desprestigio para su negocio". Sobre la nube, donde cada vez residen más datos, incluso críticos, Sánchez estima que estarán seguros mientras el control de las claves que los cifran, no viaje con ellos.

Sobre este proceso de transformación, Jesús Rodríguez destaca que, a consecuencia de la pandemia, muchos desarrollos se han precipitado. "El uso del efectivo ha caído y canales que se iban a desarrollar de forma natural se han precipitado". Cada vez se hacen más operaciones utilizando dispositivos móviles y fórmulas, como el open banking, están cambiando el modo en que se utilizan los servicios bancarios. "Esto incide en la necesidad de proteger las transacciones (crip-

"Mediante la utilización de criptografía se van a proteger las transacciones, y con los sistemas de tokenización se va a autenticar a los usuarios. La suplantación de identidad es uno de los mayores riesgos para la banca"

JESÚS RODRÍGUEZ, CEO DE REALSEC

“La concienciación, incluso la formación, no dejan de ser responsabilidad del banco. El usuario tiene que ser un eslabón más de la cadena en la protección, no un habilitador de un ataque”

JOSÉ DE LA CRUZ, DIRECTOR TÉCNICO DE TREND MICRO IBERIA

tografía) y al usuario (sistemas de tokenización para evitar la suplantación de identidad).

Por su parte, Alfonso Martínez defiende la idea que con la gran evolución que ha tenido la banca en estos últimos años, esas entidades no pueden seguir protegiéndonos como hace 10 o 15 años. “Al igual que el abanico de opciones se multiplica, las amenazas también y son más sofisticadas. Los fabricantes no podemos quedarnos atrás. Tenemos que dar soluciones a las tendencias tecnológicas que van surgiendo, y ofrecer esa completa seguridad alrededor de la información”.

LA CONCIENCIACIÓN DEL USUARIO

El usuario es el centro de todo. Sin embargo, es importante encontrar un equilibrio entre la experiencia de usuario y la seguridad. ¿Cómo conseguirlo?

Para Eusebio Nieva, este equilibrio pasa porque el usuario perciba que la seguridad es útil. “Las medidas de protección pueden interferir en el usuario, en el acceso o en el dato”. Sin embargo, se debe intentar que el cliente distinga estas pautas como una ventaja, que aprecie que con estos mecanismos evita perder dinero, mientras consigue que las transacciones sean fiables y sus datos estén seguros. “A la vez que protege, la propia tecnología debe mostrar sus beneficios”.

Este componente de concienciación también es apreciado por Luis Javier Suárez, quien distingue dos desafíos para los bancos: conseguir que la experiencia del usuario no sea invasiva, mientras se recogen comportamientos y detectan anomalías que permitan tomar medidas para la detección temprana del fraude; y trabajar la concienciación, tanto dentro de la propia empresa como de cara al usuario. “Es importante trasladar las buenas costumbres adquiridas en la banca tradicional al mundo digital”.

La importancia de la concienciación, y de la formación, es destacada por José de la Cruz. “No deja de ser responsabilidad del banco proteger los activos de sus usuarios, que deben ser un eslabón más de la cadena en la protección, no un habilitador de un ataque”. Además, es clave comprender que la seguridad se ha de implementar en la fase de diseño, para que la integración sea mucho más transparente y sencilla y no interfiera en la agilidad o experiencia de usuario.

Para referirse al valor que le da el usuario a esta agilidad, Igor Unanue cita el doble factor

de autenticación, que no se implementó hasta que no fue obligatorio por ley, para no interferir en el acceso. “Es un tema de concienciación, de cultura. Cuando nos habituemos a utilizar determinadas tecnologías de seguridad también lo haremos en la banca”. No obstante, estas tecnologías han de resultar naturales para el usuario. “La seguridad debe ser cada vez más efectiva y más sencilla”.

PSD2 Y OTRAS REGULACIONES

Las entidades financieras siempre han estado a la cabeza en cuanto a modelos de transformación digital y en la adopción de medidas de seguridad, siempre han querido ir un paso por delante. Sin embargo, ha habido casos más complicados, como con la regulación PSD2. ¿Se ha logrado de una manera efectiva su adopción? Ahora, cuando ya se vislumbra el reflejo de PSD3, toca preguntarse si la banca está preparada para lo que está por venir.

Al respecto de la observancia de PSD2, Jesús Rodríguez refiere cómo las entidades se han estado preparando, primero, con el desarrollo de APIs para poner a disposición de terceros información de los clientes, y, después, con el establecimiento de un sistema de autenticación de doble factor. “En España no podemos hablar de incumplimiento, aunque la mayoría de entidades no han adoptado un sistema de tokenización; han optado por el envío de un SMS. A futuro, con la PSD3 en el horizonte, habrá que buscar otras soluciones basadas en token”.

Sobre la aceptación de estas medidas, Alfonso Martínez reconoce el gran esfuerzo realizado al abrir estas APIs para favorecer el open banking. Sin embargo, expone la importancia de implementar la seguridad desde el principio, en consonancia con PSD2, y para cumplir con otras nor-

“La seguridad debe estar habilitada desde el principio. Solo si los fabricantes ofrecemos las tecnologías adecuadas, las entidades van a poder acatar las distintas normativas y procurar los servicios (seguros) apropiados”

ALFONSO MARTÍNEZ, COUNTRY MANAGER, DATA PROTECTION DE THALES IBERIA

"A causa de las normativas, los bancos están aplicando cada vez más niveles de seguridad sobre sus accesos a la red SWIFT. Pero hay que hacer más. Si ocurren ataques es porque detrás hay una vulnerabilidad, y los atacantes saben aprovecharlo"

IGOR UNANUE, CTO DE S21SEC

mativas. En este punto el papel de los fabricantes es clave. "Debemos ofrecer las tecnologías adecuadas para que estas entidades puedan procurar los servicios (seguros) apropiados".

ATAQUES A LA RED SWIFT, UN RIESGO SISTÉMICO

Otro tema que cada vez está resultando más relevante son los ataques contra la red SWIFT, que se han multiplicado en los últimos tiempos. Ahora bien, ¿qué impacto están teniendo y en qué consisten estas ofensivas?

"Por tratarse de una red en la que fluye el negocio y circula el dinero, SWIFT es un claro objetivo para los hackers, que intentan interceptar transacciones para sacar beneficio", explica Eusebio Nieva. Para su salvaguarda, la tecnología puede ayudar muchísimo, sobre todo para el análisis de fraude y la securización de ciertos puntos que todavía son un poco débiles. "Al final se trata de aplicar la tecnología en esas transacciones. Protección y fiabilidad en todos los extremos".

Mitigar y securizar es crucial, pero antes hay que conocer cómo se producen estos ataques. En este sentido, Luis Javier Suárez, destaca que los más eficientes son los dirigidos contra la cadena de suministro. "Los atacantes manejan una cantidad abrumadora de inteligencia sobre los organismos que operan en la red SWIFT. Conocen qué vulnerabilidades pueden ser explotadas dentro de los sistemas y aprovechan esta información para saber dónde atacar y alcanzar ese objetivo".

Sobre las razones que explican los ataques a la red SWIFT, Igor Unanue revela que, por tratarse de una red externa, las medidas de seguridad son más laxas. "Sin embargo, ahora, sobre todo por las normativas, se están aplicando mayores niveles de seguridad a estos entornos, pero hay que hacer más. Si ocurren ataques es porque detrás hay una vulnerabilidad, y los atacantes la están aprovechando bien. Al final es una red de comunicación más, y como tal hay que protegerla".

La cadena de suministro es reconocida también por José de la Cruz, como el elemento más débil, y, dentro de ella, los bancos pequeños,

con medidas de seguridad menos robustas, el eslabón más frágil". No obstante, todos deben asumir que antes o después se producirá un ataque, por lo que las entidades deben dotarse de una visibilidad que les permita conocer lo que está ocurriendo, tanto en su entorno como con los flujos de información que existen con terceros.

TECNOLOGÍAS EMERGENTES

Tecnologías emergentes como blockchain, IA o IoT están empezando a impactar en los servicios financieros. ¿Cómo se están adaptando los bancos a ellas?

Sobre este punto, Javier Sánchez, expresa que "están en proceso". Los bancos custodian tanto el dinero como la confianza de sus clientes por lo que tienen que tomarse su tiempo a la hora de utilizar nuevas tecnologías y que formen parte de su proceso de negocio. En el caso de una blockchain pública no hay nadie al otro lado, por lo que los bancos no pueden comprometer su confianza con una tecnología que puede no ser segura.

Ahora mismo, la banca necesita ganar en competitividad y en rentabilidad por lo que, según Jesús Rodríguez, necesita hacer uso de tecnologías innovadoras como IA, donde están más adelantados. Otras como blockchain, muy ligada a las criptomonedas, y donde se "avanzará con una regulación", también son utilizadas para cifrar bloques o firmar smart contract, pero no cuando hablamos de claves, donde el nivel de exigencia es muy alto. Otras como IoP despegarán en un futuro.

Desde la perspectiva de representar a una empresa que fabrica tecnología que ayuda o habilita para el uso de innovaciones como blockchain, Alfonso Martínez considera que falta mucha labor de comunicación. "Estas tecnologías luego hay que aplicarlas a la vida real y, en ese sentido, falta información tanto, para los usuarios finales, que tienen que saber qué es blockchain y cómo utilizarlo como para las entidades financieras, para entender cómo lo pueden monetizar.

TECNOLOGÍAS IMPRESCINDIBLES

Ante toda esta innovación, el sector financiero no puede bajar la guardia en su seguridad. ¿Cuáles son aquellas tecnologías de seguridad que puede ser consideradas imprescindibles en la actualidad? Y ¿a futuro?

"Los bancos custodian tanto el dinero como la confianza de sus clientes. Tienen que tomarse su tiempo a la hora de utilizar nuevas tecnologías y que estas formen parte de su proceso de negocio"

JAVIER SÁNCHEZ, TERRITORY SALES MANAGER DE ENTRUST

"Cualquier organización tiene que asumir que puede ser comprometida. Este paradigma nos lleva a la gestión del incidente y al gobierno de algo que se ha impulsado desde el sector financiero: la gestión de indicadores de compromiso"

LUIS JAVIER SUÁREZ, PRESALES MANAGER DE KASPERSKY

Eusebio Nieva reconoce una alta concienciación en ciberseguridad, pero recomienda no bajar la guardia. "Estas entidades deben optar por tecnologías específicas para abordar amenazas actuales, como el ransomware, los ataques a la cadena de suministro o la protección del endpoint, pero también, por enriquecer sus sistemas con diferentes soluciones que protejan contra los peligros surgidos al calor de innovaciones, como las tecnologías cloud, y que las organizaciones financieras están convirtiendo en el core de sus servicios y de sus negocios". Deben evolucionar y adaptarse según progresan sus tecnologías. La protección de la red o del endpoint era algo que había que hacer, y ahora hay que proteger las claves. En este sentido, Javier Sánchez respalda la importancia del cifrado, que ahora, además, es percibido tanto por otros fabricantes de seguridad como por las propias entidades del sector financiero como una solución necesaria para proteger la información. "Se ha producido una concienciación en torno a la importancia de securizar las claves, por lo que su adopción está ocurriendo de un modo natural en la banca".

En línea con esta innovación hay un componente de concienciación importante. A este respecto, Luis Javier Suárez valora la trascendencia de que las empresas financieras desarrollen un plan de concienciación, ya sea de forma individual o con el respaldo de una empresa especializada. "También, deben asumir que su ciberseguridad puede verse comprometida, por lo que el uso de indicadores de compromiso resulta efectivo, sobre todo para compartir con terceros la información que contienen (inteligencia y patrones de ataques) y medir la afectación". Asimismo, es esencial la explotación de inteligencia de amenazas, para ir a la par con los atacantes.

MEDIDAS PROPORCIONALES

Decidir qué solución o qué conjunto de recursos son los más adecuados para proteger las infraestructuras de las entidades financieras es complicado. "La realidad", expresa Jesús Rodríguez, es que los riesgos están ahí, y las medidas han de ser proporcionales, así como las políticas

y los procedimientos de seguridad que se establezcan. No obstante, se deben proteger los activos de negocio, los riesgos de fraude e implantar medidas contra la suplantación de identidad o el malware. Por otro lado, el despliegue de nuevos canales de pago ha promovido un mayor uso de la criptografía, mientras que el crecimiento de los datos, precisa de medidas de protección que requieren el uso del cifrado, para cumplir con normativas como PSD2 o PCI DSS.

En la misma línea, Igor Unanue reitera que allí de donde vengan las amenazas es donde la banca más tendrá que invertir en ciberseguridad. En cuanto a futuro desafíos, señala la persistencia del malware (malware bancario) y de otros procedentes de servicios cloud, por el incremento de servicios de colaboración, que derivará en muchos riesgos. "Imperativo será también proteger el endpoint y, en general, todo aquello donde la banca perciba una amenaza".

Alfonso Martínez, coincide en que hay "mucho vector que proteger y el dato debe salvaguardarse así mismo con el cifrado". El cifrado puede ser en la nube, en máquinas virtuales, incluso en movimiento o viajando de una nube a otra. Lo importante es entender que detrás de esos sistemas tan complejos existe una inteligencia real a la que hay que ayudar para que la gestión sea sencilla y la criptografía no se convierta en un dolor de cabeza. "Debemos darles las herramientas para poder gestionarlo todo de manera centralizada y correcta".

Para José de la Cruz, la banca se enfrenta a un panorama heterogéneo, con diferentes tecnologías, proveedores y entornos, que le provocan un grado de exposición muy alto. La respuesta ante eso es visibilidad y control. "Visibilidad de lo que se protege, para conocer el origen y alcance de un ataque, y control sobre aplicaciones que no han sido diseñadas con la seguridad en mente y que hay que resguardar de un modo transparente". En lo que respecta a servicios como DevOps o cloud, un enfoque Cloud Security Posture Management ayuda a dar esa capa de visibilidad, y a identificar riesgos, para mitigarlos. ■

MÁS INFORMACIÓN

- Mesa Redonda IT: Nuevos retos de seguridad en entornos financieros; su impacto en el modelo de negocio

JOSE FRANCISCO PEREIRO, GLOBAL HEAD OF PRIVACY TECH | RISK, BNP PARIBAS

“Un equipo de profesionales de seguridad capacitado y motivado es el mejor control para mitigar los riesgos”

En una situación como la que nos está tocando vivir hay que entender que el riesgo cibernético, lejos de reducirse, ha aumentado. Estamos viendo a través de los medios de comunicación como el cibercrimen está atacando multitud de empresas privadas y administraciones públicas con ataques de tipo ransomware, incluyendo infraestructuras críticas.

¿Cuáles son los principales retos de ciberseguridad a los que se enfrentan actualmente los servicios financieros?

Uno de los principales retos es gestionar el riesgo de terceras partes, la cadena de suministro se está transformando con velocidad y creciendo en volumen. Adicionalmente a la colaboración histórica con grandes multinacionales tecnológicas, es cada vez más frecuente en el sector financiero la colaboración con startups, fintech y multitud de nuevos socios. Estas organizaciones aportan sin duda innovación y nuevos modelos de negocio, pero es necesario evaluar con detenimiento los riesgos de seguridad y ayudarles a mitigarlos antes de comenzar una iniciativa conjunta.

Otro de los retos es la evolución y sofisticación de los ataques informáticos, cada vez más dirigidos y mejor ejecutados. Contra esto, además seguir trabajando en el diseño e implementación de nuevos controles técnicos para detener los ata-

ques, es fundamental entender el factor humano, puesto que muchos de estos ataques tienen como base de entrada la ingeniería social, que intenta explotar las debilidades que todos tenemos cuando somos expuestos a una situación de falso peligro o urgencia con el objetivo de influir en nuestra conducta. Por esto, ya no es suficiente con disponer de un programa formación en ciberseguridad, sino que es necesario cubrir tres dimensiones: formación, concienciación y entrenamiento. La segunda, la concienciación, hace referencia a la capacidad de crear impacto emocional para protegernos de situaciones de peligro, como muy bien se hace por ejemplo en las campañas de tráfico. La tercera, el entrenamiento, es la más importante y consiste en simular situaciones cercanas a un ataque cibernético para desarrollar las habilidades necesarias y responder adecuadamente cuando se produzca un ataque real.

El tercer reto es la captación y retención del talento en ciberseguridad. Un equipo de profesionales de seguridad capacitado y motivado es el mejor control para mitigar los riesgos, pero es necesario competir en un mercado laboral de nicho en el que cada vez hay más empresas interesadas en reclutar este tipo de profesionales. Por eso, además de desarrollar políticas de atracción para las nuevas generaciones, es necesario darse cuenta de que, muchas veces, el talento está más cerca de lo que se piensa y que una alternativa interesante es formar en ciberseguridad a profesionales que estén trabajando en otras áreas.

¿Cómo se han adaptado los servicios financieros a tecnologías emergentes como Blockchain o IoT?

Las tecnologías emergentes, como el Blockchain, IoT, AI, Big Data, Cloud y muchas otras, ofrecen sin duda una gran oportunidad para desarrollar nuevos modelos de negocio y de relación con nuestros clientes. Las ventajas de estas tecnologías suelen ser evidentes y crean un alto nivel de interés en las áreas de negocio. Sin embargo, por tratarse de tecnologías emergentes, no siempre hay experiencia en la industria que nos permita modelizar y dimensionar los riesgos de ciberseguridad de una forma estándar.

Por ejemplo, las arquitecturas Blockchain o DLT, que son reconocidas como de las más seguras en la actualidad por su base criptográfica, tienen ya algún riesgo identificado como el asociado al compromiso del 51% de los nodos de la red. Si bien ejecutar este tipo de ataque es extremadamente difícil en aplicaciones basadas en Blockchain públicos con decenas de miles de nodos, como es el caso de la criptomoneda Bitcoin, si hablamos de una implementación privada con sólo decenas de sistemas y sistemas homogéneos, el riesgo de este tipo de ataque se incrementa, por lo que es necesario de dotarlo de medidas adicionales.

Un caso particular de tecnología emergente es la computación cuántica que, cuando ésta alcance cierta escala, pondrá en riesgo la seguridad de muchos sistemas a nivel global, al poder romper el cifrado de clave pública en el que se basan muchos algoritmos criptográficos.

Por tanto, la aproximación adecuada con las tecnologías emergentes es la basada en un análisis pormenorizado de los riesgos, mediante una aproximación consultiva, dedicando profesionales de seguridad al estudio de las posibles fallas y la definición de los controles y tecnologías de seguridad necesarios, así como la realización de pruebas exhaustivas antes de su salida a producción.

¿Qué regulaciones están afectando al sector financiero y cómo se está haciendo frente a ellas?
El sector financiero es el más regulado desde hace muchos años, teniendo que cumplir con numerosos requisitos de información y reporting a agencias y bancos centrales de todo el mundo. Esto nos ha permitido disponer de una estructura empresarial y cultura organizativa que permite asimilar nuevas regulaciones con relativa ventaja a empresas de otros sectores. Dicho esto, y con relación al tema que nos ocupa, las regulaciones de privacidad que están surgiendo a lo largo del planeta, y en particular la GDPR en la zona europea, están teniendo un impacto significativo en los sistemas de información y en las medidas de ciberseguridad asociada.

Por un lado, se ha regulado el concepto de protección de datos en el diseño de nuevas aplicaciones y servicios, que tiene inherentemente asociada un componente de ciberseguridad. De esta forma, cada vez que se desarrolle un nuevo producto que procese datos de carácter personal, este deberá tener en cuenta las necesidades regulatorias y de seguridad. Además, la GDPR, en su artículo 32, establece la obligatoriedad de implementar las medidas de seguridad necesarias para proteger los datos proporcionalmente a los riesgos a los que está expuesta. La privacidad debe ser embebida en todas las arquitecturas y soluciones IT, por ejemplo, cuando antes estábamos hablando de tecnologías emergentes, la GDPR afecta en mayor o menor media en diferentes aspectos: el derecho al olvido en Blockchain, las transferencias de datos internacionales en Cloud, las decisiones automatizadas en la Inteligencia Artificial o el tratamiento masivo de datos en el Big Data.

> "Uno de los grandes retos es la evolución y sofisticación de los ataques informáticos, cada vez más dirigidos y mejor ejecutados"

Por último, la privacidad ha tenido un efecto más sutil, pero no menos influyente en el mundo de la seguridad. Hasta ahora, si una tecnología de seguridad se consideraba como buena para mitigar riesgos, se implementaba; pero tras la llegada de las regulaciones de privacidad a diversas partes del mundo es necesario asegurar que dichas tecnologías cumplen con la regulación. Por ejemplo, las tecnologías de detección de anomalías en el comportamiento de usuarios, que permitían detectar si una cuenta de usuario había sido comprometida, ya no podrán ser implementadas si no garantizan los derechos y libertades en materia de protección de datos.

Tras un año de pandemia, ¿qué han aprendido los CISOs del sector financiero?
La enseñanza fundamental es que la seguridad no se puede poner en ERTE. En una situación como la que nos está tocando vivir hay que entender que el riesgo cibernético, lejos de reducirse, ha aumentado. Estamos viendo a través de los medios de comunicación como el cibercrimen está atacando multitud de empresas privadas y administraciones públicas con ataques de tipo ransomware, incluyendo infraestructuras críticas. Además, durante esta crisis ha sido necesario tomar decisiones transcendentes en un plazo muy breve de tiempo, como la de tener que poner centenares de miles de trabajadores españoles a teletrabajar de la noche a la mañana. Estas decisiones, necesarias para la continuidad de negocio, si no son acompañadas por medidas de ciberseguridad que mitiguen los riesgos del nuevo escenario, pueden tener efectos adversos. De igual forma, los servicios bancarios online han pasado de ser una mejora a ser una necesidad, por lo que garantizar su continuidad y fiabilidad 24 horas al día frente a ataques es una de las prioridades.

Es necesario concienciar a la sociedad sobre el peligro real que supone el cibercrimen y hasta donde está dispuesto a llegar. Hemos visto como en los peores momentos de la pandemia han sido atacados los sistemas de información de algunos hospitales.

¿Qué tecnologías de seguridad considera imprescindibles para una empresa perteneciente al sector financiero?
Todas las tecnologías de prevención de fuga de datos son esenciales para evitar la filtración ac-

"El sector financiero es el más regulado desde hace muchos años, teniendo que cumplir con numerosos requisitos de información y reporting a agencias y bancos centrales de todo el mundo"

cidental o intencionada de información sensible. Es fundamental que estas estén integradas en los canales de comunicación con el exterior para monitorizar y bloquear las transferencias de datos sospechosas. Debemos asegurar que cubren todos los canales, no solo el email sino la subida de información a través de servicios web, la extracción de información a través de los puertos del ordenador e incluso también la impresión.

Dicho esto, se debe tener en cuenta que estas tecnologías son inútiles si no se definen e implementan las políticas adecuadas de identificación y bloqueo de contenidos y, para esto, el equipo de ciberseguridad no puede trabajar de forma autónoma, necesitará de la colaboración del negocio y otras áreas. Además, hay que asegurar que se dispone de un equipo de profesionales de seguridad cualificado para analizar y responder a las alertas emitidas. Sin políticas y profesionales, la tecnología DLP tendrá las mismas capacidades de mitigación del riesgo cibernético que instalar un jarrón en nuestro centro de datos, eso sí, muy caro.

Existen muchas otras que son esenciales bajo mi punto de vista, como las tecnologías y servicios para proteger frente a ataques de denegación de servicio, la protección frente al malware, el cifrado, la protección del perímetro, y los cortafuegos de aplicación y bases de datos.

¿Qué tecnologías que todavía no están ampliamente adoptadas, cree que serán imprescindibles en los próximos años?

En los últimos tiempos han aparecido nuevas posibilidades tecnológicas para la protección de los datos que deben ser exploradas por las entidades financieras para mitigar, aún más, los ciber-riesgos asociados a estos. La información es almacenada por las organizaciones en dos formatos: de forma estructurada, como por ejemplo las bases de datos; y de forma no-estructurada, como por ejemplo las hojas de cálculo.

En lo relativo a la protección de la información estructurada, a las técnicas tradicionales de anonimización y pseudo-anonimización, ampliamente empleadas como la tokenización o el masking, se unen nuevas alternativas como el uso de la encriptación homomórfica o los datos sintéticos. Es importante disponer de un portfolio amplio y contrastado de estas técnicas, puesto que no hay ninguna de ellas que, de forma individual, pueda cubrir todos los casos de uso del negocio.

Cuando hablamos de información no estructurada la situación es todavía más compleja, puesto que existen numerosos ficheros que son intercambiados diariamente como parte de la operativa normal del negocio financiero en interacciones internas y externas. Para esto es necesario implementar tecnologías que nos permitan garantizar la seguridad de los datos durante todo su ciclo de vida, siendo especialmente importantes las tecnologías de descubrimiento de la información y clasificación de los datos. Son también muy interesantes las tecnologías denominadas genéricamente como IRM, que nos van a permitir insertar las políticas de seguridad dentro del dato (control de acceso, trazabilidad, caducidad...), disponiendo de esta forma de la capacidad de proteger la información con independencia de dónde se ubique. ■

MÁS INFORMACIÓN

BNP Paribas

Más visibilidad.
Más potencia.
Más control.

¿No pensó estar preparado/a para el EDR?
Ahora lo está.

go.kaspersky.com/es_optimum

kaspersky PREPARADOS PARA EL FUTURO

Objetivos de la ciberseguridad en las entidades financieras:

protección de clientes, dispositivos y empresa ante los ataques

EUSEBIO NIEVA,
director técnico de
Check Point Software para España y Portugal

La ciberpandemia es uno de los peligros que actualmente están amenazando a cientos de compañías. Tras los meses en los que la Covid-19 ha obligado a miles de personas a extremar las precauciones para evitar el contagio y el uso del pago por móvil o la tarjeta de crédito se han instaurado como opciones masivas. Por ello, las entidades financieras se están convirtiendo en uno de los principales objetivos de los ciberataques, sobre todo, por el rédito económico que puede llegar a reportar el atacarlas.

Desde el comienzo de la pandemia, empresas de todos los sectores se han visto obligadas a implantar el teletrabajo con el consecuente incremento de los dispositivos móviles conectados a la red, aumentando considerablemente las brechas de seguridad y mejorando las oportunidades de éxito de los cibercriminales. Los frentes para los negocios se multiplican y contar una buena defensa es la única opción.

Debido a la situación, ahora se están llevando a cabo diferentes tipos de fraude y extorsión contra la banca, para de esta forma vulnerar la privacidad de estas compañías con el objetivo de llenarse los bolsillos. Así los datos respaldan la realidad del sector, ya que según Informe Global de Amenazas DNS 2020 elaborado por IDC de la mano de EfficientIP, en el 2020 cuatro de cada cinco empresas del ámbito financiero (79%) sufrieron más de diez ciberataques DNS a lo largo del año y cada uno de ellos supuso un coste de 1,16 millones de euros de media.

Uno de los mayores desafíos que tienen que afrontar las entidades financieras es la

seguridad móvil, tanto por el lado usuario como por el de sus trabajadores. Ahora más que nunca, el acceso a redes corporativas a través de móviles no securizados es un objetivo. Para ello, Check Point Harmony Mobile protege los dispositivos móviles de los empleados de todos los vectores de ataque (aplicaciones, red y sistema operativo). Este software está diseñado para reducir los gastos generales de los administradores y aumentar la adopción del usuario, escala rápidamente, evita descargas de aplicaciones maliciosas, impide el phishing en todas las aplicaciones previene ataques Man-in-the-Middle, bloquea aparatos infectados para que no accedan a aplicaciones corporativas y detecta técnicas avanzadas de jailbreaking y rooting y vulnerabilidades del sistema operativo.

En la otra cara de la moneda encontramos cómo estas entidades financieras pueden proteger a sus clientes, sus credenciales y datos personales cuando acceden a sus apps. La mejor manera de mantenerlas a salvo de los cibercriminales es contar con una protección adecuada. Impulsado por el motor de IA contextual de Check Point CloudGuard, Check Point CloudGuard AppSec es una solución que bloquea los ciberataques contra las aplicaciones, incluyendo: la desconfiguración del sitio web, la fuga de información y el robo del inicio de sesión del usuario. Para ello, es capaz de analizar cada solicitud en su contexto y asignándole una puntuación de riesgo, para una prevención precisa, eliminando los falsos positivos y evitando los más sofisticados ataques contra una aplicación, incluidos los ataques OWASP Top 10.

> “Todas las empresas pertenecientes al sector de la banca deben contar con software de protección en el total de sus emplazamientos y en todos los dispositivos que tenga conexión a su red”

Es imprescindible señalar que la banca debe contar con un software que sea capaz de proteger a la empresa de cualquier tipo de ciberataque a sus centros de datos. Esta herramienta debe mantener a salvo todos los archivos, documentación y datos pertenecientes a la propia sociedad y también de los clientes que forman parte de la misma.

Para lograr el objetivo, en Check Point Software contamos con Check Point Quantum Maestro, una solución que posibilita a las compañías ampliar fácilmente sus gateways de seguridad bajo demanda y crear nuevos servidores y recursos informáticos en la nube pública. Además, este software permite que un solo gateway se extienda hasta alcanzar la capacidad y el rendimiento de 52 en cuestión de minutos, lo que proporciona flexibilidad dinámica y un rendimiento máximo del firewall Terabit/segundo. Esta escalabilidad casi ilimitada permite soportar la alta velocidad de datos y contar con la latencia ultra baja de las redes 5G, una red que lo va a cambiar todo desde este mismo año y que será clave para todas las entidades financieras. Asimismo, hay que destacar el hecho de que llega a proteger a los entornos más extensos y con más recursos, estableciendo nuevos estándares en la seguridad de redes a hiperescala. Finalmente, es importante especificar que Check Point Quantum Maestro tiene la habilidad de extender las capacidades de seguridad Gen V de nuestra arquitectura Check Point Infinity a los entornos de hiperescala.

Si algo ha quedado claro en este último año es que todas las empresas pertenecientes al sector de la banca deben contar con software de protección en el total de sus emplazamientos y en todos los dispositivos que tengan conexión a su red para mantener a salvo todos los datos confidenciales que manejan frente a los posibles ciberataques. ■

Salvaguardar las transacciones, proteger al usuario

El financiero es uno de los sectores más afectados por los ciberataques avanzados, ahora muy enfocados en la banca móvil. Proteger al usuario frente a estas amenazas es imperativo, pero sin descuidar otros vectores, como la red SWIFT o los cajeros. La ciberseguridad de la banca debe evolucionar en la misma medida en que lo hacen los servicios.

A causa de los desafíos ligados a la pandemia el uso de la banca móvil se ha incrementado, y con ello el aumento de las ciberamenazas dirigidas contra los dispositivos móviles. Ante esta realidad, Eusebio Nieva, director técnico de Check Point, explica la importancia que tiene para estas entidades desarrollar una estrategia de ciberseguridad que englobe también este canal, con la integración de soluciones avanzadas de ciberseguridad móvil en sus apps.

En Check Point trabajan con varias entidades bancarias a las que proporcionan sus servicios de seguridad en forma de un interfaz de programación de aplicaciones (API) o de un kit de desarrollo de software (SDK) que se pueda consumir. Con esto se consigue trasladar la seguridad al dispositivo desde el cual el usuario está accediendo a los servicios, pero en vez de instalarla en dicho terminal, se pone a disposición de las entidades bancarias, de modo que cuando ellos lancen su propia aplicación de consumo o de servicios bancarios esta estará asociada a los servicios de seguridad de Check Point.

Otra consecuencia de la evolución hacia una banca más móvil, y en general más digital, es que el uso de cajeros automáticos (ATM) ha descendido, al igual que el empleo de efectivo. Hoy en día, y a causa de la pandemia, el dispositivo ubicuo que casi todo el mundo utiliza para hacer pagos es un terminal móvil o una tarjeta de crédito o débito. Sin embargo, y aunque el uso de ATM se ha reducido, lo cierto es que aún se siguen produciendo ataques contra dichas máquinas, por lo que es necesario seguir invirtiendo en su protección. Asimismo, hay que tener en cuenta que la tecnología que integra el cajero es muy antigua, por lo que es trascendental ir actualizando los servicios proporcionados por el cajero, así como la tecnología asociada a los mismos.

Además de no descuidar la defensa de los cajeros automáticos, las instituciones financieras que utilizan el sistema de pagos SWIFT también deben permanecer vigilantes. Las ofensivas contra esta red se han multiplicado en los últimos años, por lo que los bancos están implementando no solo medidas de seguridad estándar, sino también protecciones avanzadas, tecnologías de análisis de fraude, machine learning… para disuadir a los atacantes sobre su explotación, y frenar o impedir las transacciones fraudulentas o los intentos de falsificación de esas transacciones en la red de comunicaciones financieras. Nieva distingue que la tecnología de protección de las tarjetas bancarias o de los dispositivos móviles aún no está a la par con la tecnología de ataque utilizada por los ciberdelincuentes. En este sentido, sería necesario que nuevas metodologías o herramientas entraran en funcionamiento a fin de asegurar las transacciones, sobre todo desde el punto de vista del usuario que es quien las realiza. Con ello se podrían evitarse los fraudes y los ataques a dispositivos móviles con troyanos bancarios, con troyanos de tarjeta de crédito, etc. que pueden ser utilizados contra los usuarios. Por tanto, esta evolución paralela de servicios y ciberseguridad debe ser prioritaria.

Protegeré las claves, protegeré las claves, protegeré las claves…

JAVIER SANCHEZ FUERTES,
Territory Sales Manager,
Data Protections Solutions Entrust

Las empresas de servicios financieros se enfrentan a desafíos únicos en sus esfuerzos por proteger la información sensible de los clientes y cumplir con las regulaciones en evolución. El Repositorio de Confianza es fundamental aquí. La identificación y la autorización de los dispositivos, el cifrado y la verificación de los datos y las actualizaciones del software tienen algo en común, y ese denominador común es la criptografía. Y la base de la criptografía son las claves de cifrado que se necesitan para firmar y validar los certificados de los dispositivos para su identificación y autorización.

La mayoría de la infraestructura desplegada en los servicios financieros utiliza claves para el correcto desarrollo de sus funcionalidades, y en la mayoría de los casos esas claves carecen de la protección adecuada.

Por lo tanto, asegurar estas claves es fundamental, y ahí es donde entra en juego el Repositorio de Confianza para proteger y gestionar las claves de cifrado a lo largo de su ciclo de vida, completamente separadas del resto del sistema con hardware robusto y controles duales para garantizar que ningún individuo o entidad pueda subvertir las políticas establecidas para el uso de las claves.

De esta manera nuestros Hardware Security Module (HSM) nShield forman parte de esta ecuación. ¿Cómo se traduce esto en el mundo financiero?

Los certificados digitales son la forma en que las diferentes partes del ecosistema de pagos establecen la confianza entre sí. Estos certificados suelen ser emitidos por una PKI que se apoya en un Repositorio de Confianza. En la raíz de una PKI se encuentran claves criptográficas fuertes y de confianza creadas en un Hardware Security Module o HSM. Los HSM de Entrust nShield proporcionan una garantía sólida y certificada a un despliegue de PKI al tiempo que facilitan la automatización de la renovación de certificados y firmas, manteniendo las claves criptográficas privadas en un entorno seguro. Pueden desplegarse en otras áreas del nuevo ecosistema de pagos allí donde se requieran servicios criptográficos desde un entorno seguro y de confianza.

Piense en monedas virtuales, seguros, préstamos, grandes minoristas, aplicaciones bancarias móviles, etc. Los HSM de uso general pueden realizar tareas como la protección y validación del PIN, y la gestión de claves, también se despliegan como parte de las soluciones de procesamiento de pagos y puntos de venta móviles con partners de la industria. No olvidando la protección de las claves de firma y el proceso de firma de código de las Apps, el elemento de relación principal entre cliente y entidad financiera.

> “Las empresas utilizan diariamente miles de claves en sus procesos de negocio que deben protegerse de forma conveniente y evitar que sean comprometidas”

Están surgiendo nuevos servicios de pago al realizar compras en línea o a través del teléfono móvil, especialmente en Europa. El cambio puede ser un resultado directo de la PSD2, la última Directiva de Servicios de Pago. Las organizaciones de servicios financieros se enfrentan a desafíos únicos en sus esfuerzos por proteger la información sensible de los clientes y cumplir con las normativas en evolución. Merece la pena recordar que la certificación de los HSM de nShield según NIST FIPS 140-2 y Common Criteria ofrece a los clientes la garantía de que están seleccionando un producto validado según algunas de las normas de seguridad más rigurosas.

Las organizaciones financieras también siguen adoptando tecnologías nuevas y emergentes, como la nube y los contenedores, que, si bien ofrecen posibles eficiencias y reducciones de costes, amplían la huella digital de la organización. Estas organizaciones necesitan tener el control sobre las claves de cifrado que utilizan los proveedores de nube pública y de esta manera será Entrust con el cliente quienes definan las políticas y permisos asociadas a las mismas. No es una cuestión de confianza sobre los proveedores de nube pública sino de control sobre los datos y a afrontar sus retos de seguridad en la nube.

Uno de los principales obstáculos para la adopción más amplia de Blockchain es la seguridad. A medida que las organizaciones continúan encontrando nuevos e innovadores casos de uso para Blockchain, la seguridad debe incorporarse desde el principio. Entrust ayuda a abordar los desafíos de seguridad fundamentales asociados con las implementaciones de Blockchain: creación de claves, protección del proceso de firma y protección de la lógica de consenso. Debido a que se encuentra alojado dentro de los límites seguros del HSM nShield, CodeSafe ofrece protección certificada FIPS 140-2 Nivel 3 para su código más confidencial.

En definitiva, las empresas utilizan diariamente miles de claves en sus procesos de negocio que deben protegerse de forma conveniente y evitar que sean comprometidas con los consecuentes riesgos que eso significa. ■

Proteger la clave para salvaguardar el dato

Los desafíos de la regulación y el cumplimiento de la seguridad de los datos son muy altos en el entorno financiero. Por ello y a medida que evolucionan las amenazas cibernéticas, la combinación de integración tecnológica y análisis avanzado es más necesaria nunca.

Por la naturaleza de su negocio, las compañías financieras siempre han tenido que ser pioneras en cuanto al uso de medidas de seguridad, y en concreto en lo que se refiere al uso de cifrado y de Módulos de Seguridad de Hardware (HSM). Ahora, cuando la digitalización avanza rápidamente y la información fluye por distintos entornos (local, cloud, IoT) esto es más importante que nunca. Sobre ello, Javier Sánchez Fuertes, Territory Sales Manager de Entrust, observa que esa actitud pionera sigue manteniéndose, y lejos de quedarse anclada en el medio de pago, ha ido extendiéndose a otros casos de uso dentro del mundo financiero, para, por ejemplo, la protección de la infraestructura de clave pública (PKI), de los procesos de firma electrónica o de los procesos de negocio, entre otros.

Por otro lado, se habla mucho de la seguridad de los datos de manera genérica, pero hay un aspecto específico que es la seguridad de los datos en reposo que a veces pasa desapercibida. ¿Cuál es el reto en estos casos?

Sobre su importancia, Javier Sánchez cree en las empresas en general y en las financieras en particular se realizan importantes inversiones para proteger el entorno de red o el endpoint, abandonando en muchas ocasiones al dato, que por sí mismo no puede defenderse. El desafío, por tanto, pasa por identificar cuáles son los datos críticos para una entidad financiera y, sobre ellos, aplicar medidas de cifrado y por supuesto de protección de las claves. No hay que olvidar que las políticas de cifrado son tan seguras como lo son la protección de las claves.

Parece que la tecnología de cadena de bloques, Blockchain, está llamada a transformar el mundo de la banca. Sin embargo, el despliegue de servicios financieros sobre esta tecnología presenta retos en cuanto a seguridad. A este respecto, Javier Sánchez explica que la adopción de Blockchain en el mundo de la banca debe hacerse con cuidado. Los clientes depositan su dinero en un banco porque confían en dicha entidad.

En este sentido, Javier Sánchez explica que en Blockchain cada transacción que se envía a un bloque va firmada y por ese motivo lleva asociada una clave, y como hay una clave necesariamente debería haber un Módulo de Seguridad de Hardware (HSM). Desde Entrust lo que se propone es la protección de esas claves criptográficas y de esos procesos de firma, incluso de consenso, para que se realicen de forma segura mediante el uso de HSMs.

Además de trabajar en la seguridad y privacidad de Blockchain, las organizaciones financieras deben cuidar y conservar también sus claves, que están más desamparadas. En este contexto, y a raíz del crecimiento de la banca digital y móvil, el número de transacciones a través de estos medios se ha multiplicado. Por ello, Javier Sánchez incide también en lo crucial que resulta salvaguardar la clave utilizada para firmar el código de una app bancaria. Es más, teniendo en cuenta que la aplicación es, al final, el instrumento de relación entre el banco y los clientes, extremar las medidas de seguridad para resguardar esta aplicación no es baladí. De hecho, hoy por hoy, es su principal herramienta de negocio, por lo que hay que custodiarla.

La amenaza del malware financiero

se mantiene constante en España

ALFONSO RAMÍREZ,
director general
Kaspersky Iberia

La seguridad financiera es una de las preocupaciones más comunes tanto para los usuarios finales como en el mundo empresarial. Y es que las ciberamenazas en este campo son cada vez más peligrosas, y afectan al bienestar económico de las víctimas, ya sean individuos u organizaciones.

Según señala nuestro último informe anual sobre Ciberamenazas financieras en 2020, España fue el tercer país del mundo y primer país europeo con mayor incidencia de amenazas financieras el año pasado. Los troyanos bancarios, que suelen emplear ingeniería social para engañar al usuario y que los descargue, implica que cualquiera pueda encontrarse en el buzón de entrada de su correo, su WhatsApp o su lista de SMS con mensajes maliciosos que pretenden infectarlo.

De hecho, la incidencia de los virus informáticos diseñados para robar credenciales bancarias se sitúa entre las principales amenazas que afrontan los usuarios en Internet y el correo electrónico es el vector de ataque más habitual. En el mismo los cibercriminales se hacen pasar por una empresa (banco, empresa de envíos...) o por un organismo oficial (la Agencia Tributaria, Correos, DGT...).

Otro de los enfoques habituales utilizados por los atacantes para obtener acceso a las cuentas de los usuarios incautos es asumir el papel de "rescatador", fingiendo ser expertos en seguridad. Los atacantes llaman a los clientes de los bancos haciéndose pasar por expertos de seguridad e informan de cargos o pagos sospechosos para posteriormente ofrecer su ayuda. Bajo ese disfraz, el atacante puede pedir a los clientes

“La clave reside tanto en la protección como en la concienciación, de manera que los distintos ataques a los datos financieros no lleguen a causar daños”

que verifiquen su identidad mediante un código enviado en un mensaje de texto o una notificación push, que detengan una transacción sospechosa o que transfieran dinero a una “cuenta segura”. También pueden pedir a la víctima que instale una aplicación para la gestión remota fingiendo que es necesaria para la resolución de problemas. Los estafadores suelen presentarse como empleados del mayor banco de la región de la víctima potencial y utilizan un identificador de llamadas falsificado para las llamadas entrantes para hacerse pasar por un banco real.

Un tercer caso clásico es aquel en el que los ciberdelincuentes actúan como “el inversor”. En este caso, los estafadores se hacen pasar por empleados de una empresa de inversión o por asesores de inversión de un banco. Llaman a los clientes ofreciéndoles una forma rápida de ganar dinero invirtiendo en criptomonedas o acciones directamente desde la cuenta del cliente, sin tener que personarse en una sucursal bancaria. Como requisito previo para prestar el “servicio de inversión”, el falso inversor pide a la víctima el código recibido en un mensaje de texto o en una notificación push. El objetivo final siempre es el mismo: engañar al usuario para que haga ‘clic’ y descargue el código malicioso en su equipo. A partir de ese momento, los ciberdelincuentes tienen acceso a la información.

En este tipo de ataques el objetivo principal suelen ser las credenciales bancarias, que luego se venden en la darkweb por precios realmente bajos. Datos de tarjetas de crédito, acceso a servicios bancarios y de pago electrónico son mercancía habitual en este tipo de mercados.

Ante este panorama, la clave reside tanto en la protección como en la concienciación, de manera que los distintos ataques a los datos financieros no lleguen a causar daños. Así, para ayudar a los particulares y a las empresas a estar protegidos frente a las técnicas de fraude en constante evolución, es importante adoptar una serie de medidas básicas como, por ejemplo, limitar el número de intentos para realizar una transacción, de manera que los ciberdelincuentes no pueden intentar introducir varias veces las credenciales. Otra recomendación que muchas entidades financieras ya han puesto en marcha es informar de forma periódica a sus clientes sobre los posibles trucos que pueden utilizar los ciberdelincuentes, con información para saber cómo identificar el fraude y la mejor manera de comportarse ante estas situaciones.

En cuanto a las medidas de protección, la recomendación es realizar auditorías de seguridad y pruebas de penetración anualmente con el fin de detectar problemas de seguridad en la red de la empresa, contar con un equipo de análisis de fraudes capaz de encontrar y analizar los métodos emergentes que utilizan los defraudadores, implementar la autenticación multifactor para minimizar la posibilidad del robo de cuentas e instalar una solución de prevención del fraude que pueda adaptarse rápidamente para identificar nuevos esquemas y métodos de ataque. ■

MÁS INFORMACIÓN

Todo sobre EDR y MDR

Inteligencia de amenazas para prevenir el fraude

En línea con su evolución tecnológica, el sector de los servicios financieros es un objetivo esencial para los ciberdelincuentes y soporta gran parte de sus ataques. Es por eso que las entidades financieras no deben bajar la guardia. Sobre este aspecto, Luis Javier Suárez, Presales Manager de Kaspersky Lab, destaca que se vienen observando una serie de tendencias dirigidas a integrar metodologías basadas en agile, en la constante evolución de los aplicativos, y que, aunque en ocasiones incluyen la seguridad en el punto inicial, no siempre es así. Por ello, es crucial no descuidar la protección y seguir estrategias DevSecOps que siempre tienen la seguridad en mente.

A esta problemática se unen otros asuntos como la heterogeneidad de sistemas o la persistencia de sistemas legacy, que contrastan con nuevos desarrollos y la evolución hacia otros entornos como cloud. Sobre la nube, Luis Javier Suárez cita la falta de visibilidad como un inconveniente acuciante, ya que no tener conocimiento de lo que allí ocurre puede derivar en peligros como el Shadow IT.

El ritmo de evolución de las tecnologías también tiene que ser tenido en cuenta, sobre todo, porque es bidireccional. Bajo esta premisa y para poder contrarrestar ataques cada vez más sofisticados, es importante contar con servicios o programas de inteligencia de amenazas que ayuden a identificar y analizar las ciberamenazas dirigidas contra la empresa.

Sin embargo, añadir mayor seguridad puede perjudicar la experiencia del usuario, algo que en este sector es muy importante. ¿Cómo se puede aplicar seguridad sin impactar en la experiencia de usuario?

Para Luis Javier Suárez transformar la seguridad en algo que no sea invasivo e incómodo para la experiencia del usuario es complicado, máxime cuando desde el punto de vista de gestión de proyectos se pone mucho foco en esta experiencia. En este sentido, observa que existe una tendencia en el mercado hacia la integración de plataformas o entornos que sean Secure by Design, los cuales, por otra parte, sería conveniente acompañar también de un ciclo de adopción y mantenimiento. Además, no hay que olvidar que la integración de nuevas tecnologías puede traer consigo nuevos vectores de ataque y que tanto el actual auge del comercio electrónico como la preponderancia del cliente como eje central de la experiencia (customer centric) hacen necesaria la existencia de sistemas para apoyar esa seguridad. También debe haber una capa de información (sistemas antifraude) que permita detectar posibles campañas a fin de poder actuar en la fase más temprana.

A raíz de la creciente digitalización y teniendo en cuenta la sensibilidad del activo que aquí se gestiona, el dinero, Luis Javier Suárez valora que, aunque no habrá grandes cambios en cuanto a técnicas de ataque, si se incrementarán las campañas de ransomware dirigido, ataques contra cajeros automáticos (ATMs) y otros fraudes derivados del aumento de los canales digitales. El auge del mercado cripto también traerá consigo campañas focalizadas, desde phishing a otras más sofisticadas.

Por ello, y para asegurar la protección de sus activos, Luis Javier Suárez incide en la importancia de la concienciación de empleados y usuarios, y en la resiliencia. En este contexto, recomienda la adopción de tecnologías Endpoint Detection and Response (EDR), que permiten tener una visibilidad extendida de lo que ocurre dentro del entorno, y también la implantación de un Plan de Respuesta a Incidentes para, llegado el momento, poder aplicar una serie de medidas para contrarrestar el incidente. Este plan ayudará a alcanzar un nivel mayor de resiliencia.

Pagos, transacciones y dinero digital:

una realidad que ha venido para quedarse

JESÚS RODRÍGUEZ,
CEO Realsec

Hace algo más de un año todo cambió en nuestras vidas y un claro ejemplo de ello es la diferente forma en la que hoy compramos y hacemos uso de los medios de pago, donde la transformación digital es la protagonista de esta nueva situación social y económica.

Todo esto, se evidencia en diferentes acciones como el incremento de las compras a través de los sistemas de comercio electrónico, cuyo crecimiento, durante 2020 en España, ha sido de un 67% junto con la proliferación de la banca electrónica y la banca móvil, que ha pasado de un 44% a un 57% en su ratio de uso. Así mismo, se ha multiplicado el uso de las Apps de pago sobre teléfonos móviles, lo que se conoce como Open Banking (Amazon Pay, Samsung Pay…), las tarjetas virtuales prepago, los sistemas wallets, los pagos contactless, el Internet de los Pagos (IoP) a través de dispositivos inteligentes conectados en la red de Internet de las Cosas y la tokenización de las tarjetas. Todo ello, sumado a una gran expansión de nuevos agentes financieros como las Fintechs y la consolidación de las "finanzas descentralizadas" o DeFi, donde tienen su origen las criptomonedas, los smarts contracts y las Apps construidas en tecnología Blockchain.

El número de transacciones de este nuevo ecosistema financiero digital representa un porcentaje superior a las operaciones de pago en efectivo, cuyo descenso en 2020 se cuantifica en un 45%, aunque no debemos olvidar que, para su efectividad, transparencia y confianza, es fundamental implementar una securización robusta.

“Esta nueva economía requiere avanzar hacia una situación en la convivan el dinero fiduciario y las monedas digitales en un marco regulado y ordenado por los Bancos Centrales”

El riesgo de fraude online crece, exponencialmente, asociado al crecimiento de los medios de pagos digitales; es por ello, que las entidades financieras necesitan reforzar la seguridad implementando medidas como la autenticación de doble factor en base a la Directiva PSD2 o mayor transparencia y gobernanza en el caso de utilizar tecnologías como Blockchain para realizar pagos digitales transfronterizos, operaciones de compensación bancaria o intercambio de cédulas de pago internacional. Así como en la gestión confiable de los cripto-activos o la securización de los entornos de pago asociados al Internet de las Cosas “Blockhain of Things”

Aunque hoy la tecnología disruptiva Blockchain por inmutabilidad, descentralización y transparencia puede considerarse confiable para determinados procesos de negocio, podemos robustecerla, en el ámbito financiero, con la implementación de módulos criptográficos HSM (Hardware Security Module) que fortalecen la infraestructura de la red Blockchain, ya sea ésta pública, privada o híbrida, tanto para las operaciones financieras, gestión de criptomonedas y la protección de otros procesos de negocio.

El crecimiento de los pagos digitales en más de un 30%, a nivel mundial durante el último año, junto con los nuevos canales digitales, en detrimento del uso del efectivo, sumado a la proliferación de las monedas digitales (CBDC) y criptodivisas en un mercado no regulado (salvo excepciones como el caso del e-Yuan chino, pero con anuncios y expectativas de una futura regulación por parte de muchos Bancos Centrales del mundo, como el BCE con la creación de Euro Digital) supone asumir la realidad de una nueva economía. La que muchos denominan “Cripto-economía”, puesto que aquí la criptografía desempeña un papel clave para la protección y la seguridad de los activos financieros que traerá consigo una mayor adaptación y confianza, tanto a los usuarios del nuevo espectro digital como a las entidades financieras, interesadas siempre en minimizar los riesgos de seguridad en los medios de pago, como la suplantación de la identidad o el fraude.

Sin duda, esta nueva economía requiere avanzar hacia una situación en la convivan el dinero fiduciario y las monedas digitales en un marco regulado y ordenado por los Bancos Centrales en el que las nuevas tecnología disruptivas, como el Blockchain, cumplan con los mismos o superiores niveles de exigencia, en materia de seguridad, a los exigidos por la Banca, como es el uso una criptografía robusta para proteger las transacciones financieras, avalada por un organismo acreditado internacionalmente, como la Certificación PCI HSM PTS en el ámbito de los medios de pago.

Para conocer más sobre la situación y el estado del arte de esta tecnología en España y América Latina les animamos a leer el II Informe de Blockchain de REALSEC, elaborado junto con IDC. ■

La ciberseguridad como factor de confianza

El sector financiero se enfrenta a un ambiente regulatorio estricto, con muchas normas que acatar y exigencias en cuanto a protección y seguridad muy explícitas. Tal situación, no obstante, ha favorecido que se haya convertido en uno de los nichos más avanzados en cuanto a ciberseguridad. A este respecto, Jesús Rodríguez, CEO de Realsec, destaca que, si bien antes de la pandemia la banca ya trabajaba en determinados procesos de transformación digital, el confinamiento ha acelerado extraordinariamente este desarrollo. Sin embargo, el crecimiento de la banca electrónica y móvil ha repercutido también en un incremento de los ciberataques y en un mayor riesgo de fraude, activando la demanda de soluciones y sistemas de cifrado para la protección de transacciones y de otros procesos de negocio.

No obstante, Jesús Rodríguez aclara que la banca siempre ha cuidado mucho todo lo relacionado con ciberdelincuencia. Es un factor de confianza, el mayor de todos, por lo que a medida que el nivel de ciberriesgo ha evolucionado, se han ido implantado soluciones de protección para mitigar estas amenazas. Adicionalmente, y en lo que respecta a la parte de medios o sistemas de pago, la tecnología de criptografía bancaria ha prosperado como sistema de protección, al igual que la orientada al tratamiento seguro de las transacciones electrónicas, la protección de la información y de los datos mediante el cifrado.

La usabilidad de la tecnología de blockchain también se ha extendido, y no solo para la gestión de criptoactivos, sino para otros procesos de negocio como la compensación electrónica o los pagos transfronterizos. Sin embargo, esta tecnología debe considerarse, además de por sus capacidades de eficiencia y trazabilidad, por sus características de seguridad. Los bloques pueden ser cifrados y dentro de la tecnología de blockchain se pueden utilizar contratos inteligentes (smart contract).

Aunque fue el año pasado cuando la normativa PSD2 entró en vigor, su acatamiento ha estado posponiéndose durante los últimos años a través de varias moratorias. En ese tiempo, las entidades bancarias han estado preparándose, trabajando en una doble dirección: el desarrollo de APIs, para permitir el acceso a nuevos actores en el ámbito financiero y en la autenticación de doble o triple factor para cumplir con la directiva de pagos PSD2. Al respecto de su acatamiento, y aunque no se puede decir que ningún banco español esté cumpliendo con la directiva en sí, si se puede aseverar que no todas las entidades financieras están utilizando soluciones de tokenización para su observancia. Dichas soluciones han sido reemplazadas por SMSs con una clave adjunta que el usuario utiliza para demostrar que es quién realmente dice ser durante la operación financiera.

La banca está ahora mismo viviendo una situación revuelta; una fase de adaptación. La crisis económica generada por la pandemia está obligando a sus entidades a adoptar una serie de medidas para no perder competitividad y rentabilidad. Así, y aunque los bancos llevan tiempo trabajando en la gestión de activos, en las criptomonedas, se está produciendo una tendencia creciente a cambiar activos financieros y efectivo por criptodivisas. Sobre ello, Jesús Rodríguez considera que según avance la regulación, esta realidad irá asentándose. Previsiblemente se avanzará hacia un euro digital regulado (algo en lo que está trabajando el Banco Central Europeo) y se extenderá la usabilidad del blockchain hacia otros procesos de negocio, como los arriba comentados.

Síguenos en:

SOLUCIONES DE CIBERSEGURIDAD_

- HSM de Propósito General
- HSM Financiero
- Remote Key Load
- Soluciones de Cifrado, Firma Digital y Sellado de Tiempo
- Soluciones PKI
- Ciberseguridad Blockhain&IoT

www.realsec.com

realsec
La clave para proteger su negocio

OFICINAS CENTRALES
C/ Infanta Mercedes 90. Planta 4. 28020 Madrid
Tfno.: +34 91 449 03 30 - E-mail: info@realsec.com

MÉXICO
Avda. Ejército Nacional, 1112 Despacho 404 Piso 4
Colonia Los Morales C.P. 11510. Ciudad de México
Tfno.: + 52 (55) 44 35 00 46 - E-mail: infomexico@realsec.com

USA
303 Twin Dolphin Dr Suite 600 Redwood City, CA 94065
Tfno.: +1 (650) 632 4240 - E-mail: sales@realsec.com

SINGAPUR
REALSEC Inc.12 Marina Boulevard.
MBFC Tower 3. Level 17-01. Singapore 018982
Tel. +65 6809 5001 • infoapac@realsec.com

El sector financiero, en el punto de mira de los cibercriminales

IGOR UNANUE,
CTO S21sec

La ciberdelincuencia es, desafortunadamente, un factor de riesgo para varios sectores como el sanitario, el público o el educativo, pero la industria financiera es y seguirá siendo uno de los sectores más vulnerables a los ciberataques. Desde siempre, el sector financiero ha estado expuesto al cibercrimen, ya que en el 90 por ciento de los casos la motivación de los atacantes es puramente económica. Tal y como detectamos en 2019, los ataques hacia entidades financieras aumentaron de forma notable y los cibercriminales encontraron vías muy sencillas de penetración en dichas organizaciones a través de simples ataques de ingeniería social vía correo electrónico. Desde entonces, los cibercriminales cuentan con más y mejores recursos.

Este año, además de sufrir el típico malware financiero, el sector financiero podría ser víctima de ataques de robo de información relacionada con credenciales bancarias, datos de tarjetas de crédito o sufrir ataques Zero-Day, donde los cibercriminales se aprovechan de las vulnerabilidades y utilizan códigos maliciosos para desplegar los ataques. Muchas entidades financieras ya cuentan con sus propios sistemas de protección para hacer frente a ataques recurrentes como el phishing o el envío de información falsa mediante correo electrónico. No obstante, hay muchos nuevos software maliciosos que van surgiendo y que no son tan fáciles de identificar.

En este sentido, desde S21sec nos encargamos de monitorizar la actividad de los cibercriminales y de detectar todas las nuevas

“Toda entidad financiera debería contar con un buen sistema de detección para así identificar malware, detectar movimientos laterales o cualquier otro tipo de ataque”

amenazas que puedan afectar al sector financiero. Cada día, se identifican casi 15.000 malware diarios y la clave reside en averiguar a qué tipo de entidades afectan y qué banco en concreto está siendo víctima de dicho ataque. Nos encargamos de recuperar la información robada, además de proporcionar nuestros servicios de SOC y equipos de servicios profesionales que trabajan en proyectos de integración, consultoría o en la parte de auditoría. La consultoría en entidades financieras es muy importante debido al cumplimiento normativo que les impone implantar medidas de seguridad.

Otro aspecto a tener en cuenta es que debe haber un equilibrio entre la seguridad y la experiencia del cliente; es decir, añadir mayor seguridad puede perjudicar la experiencia del cliente, y en el sector financiero, no es fácil limitar el acceso mediante seguridad porque las entidades deben seguir funcionando. Además, la pandemia ha impulsado el teletrabajo y el uso de la banca online, con lo que es complicado imponer una seguridad total en este sentido. La única solución al respecto es estar alerta y seguir controlando la seguridad en paralelo, identificando los puntos más débiles que puedan suponer un riesgo para la compañía. En S21sec consideramos que esa es la gestión del riesgo que toda entidad y compañía financiera debe realizar, ya que imponer medidas de seguridad extremas supondría entorpecer el funcionamiento de la compañía, debiendo hacer un esfuerzo por identificar correctamente el punto de entrada más vulnerable para así implantar medidas de seguridad, como por ejemplo establecer reglas de correlación, puntos de control y sistemas preventivos.

No hay que olvidar que los cibercriminales siempre llevan a cabo sus ataques aprovechando las vulnerabilidades de los grandes fabricantes y, por ello, es imprescindible mantener los sistemas parcheados y protegidos para evitar cualquier fuga de información; es algo que el sector financiero debe tener muy claro para protegerse contra los ciberataques. Asimismo, también es importante saber que muchos de los ataques recientes han sido silenciosos y difíciles de detectar porque utilizan nuevos sistemas de ataque, de manera que los ataques son lentos y no se identifican inmediatamente.

Por ello, desde S21sec recomendamos a todo el sector financiero tener un sistema de monitorización constante y estar siempre alerta ante nuevas amenazas. Toda entidad financiera debería contar con un buen sistema de detección para así identificar malware, detectar movimientos laterales o cualquier otro tipo de ataque. Además, también es recomendable que estén al tanto de todo lo que ocurre en las redes, visualizar las vulnerabilidades y tener en cuenta que las entidades financieras estarán siempre expuestas al riesgo de los ciberataques. ■

Seguridad gestionada para mitigar los riesgos

El sector financiero siempre ha estado en el punto de mira de los cibercriminales, dado que, además, en el 90% de las ocasiones estos actores se rigen por una motivación financiera. No obstante, Igor Unanue Buenetxea, CTO de S21sec, reconoce que no es el que sufre el mayor número de ataques, aunque si al que llegan los más tradicionales, como los dirigidos contra sus clientes.

Aunque el malware financiero siempre ha existido y seguirá en activo, desde S21sec consideran que, durante 2021, tendrán mayor relevancia las vulnerabilidades Zero Day y los ataques dirigidos destinados al robo de información (credenciales, datos personales, tarjetas de crédito).

Asimismo, Unanue alerta sobre el cibercrimen bancario, el cual se está expandiendo sin pausa, y al que desde la propia empresa hacen frente a través de la monitorización de los cibercriminales, para no dejar escapar malware nuevo. En este contexto, S21sec analiza diariamente más de 15.000 muestras, lo que le permite averiguar a qué tipo de entidades afecta, incluso un banco concreto. Adicionalmente, S21sec recupera credenciales robados, monitoriza constantemente la Deep Web en busca de tarjetas de crédito e información robada a las entidades financieras (análisis en profundidad continúo). También ofrece servicios de seguridad gestionada en remoto (SOC) 24/7 y cuenta con un equipo de servicios profesionales que trabaja en proyectos de integración, auditoría y consultoría.

Sobre este último, Igor Unanue reconoce que la acción de consultoría es muy importante para este tipo de organizaciones, ya que deben implementar medidas de seguridad concretas para acatar el cumplimiento normativo. Estas, además, deben estar muy bien implantadas, ya que serán auditadas por el Banco Central Europeo (BCE).

No obstante, a veces, añadir mayor protección pueden perjudicar la experiencia del usuario; por lo que el reto está en obtener ese equilibrio para aplicar seguridad sin impactar en la experiencia de usuario

A este respecto, Igor Unanue comenta la dificultad que entraña conjugar ambos aspectos. Limitar el acceso o las comunicaciones con mecanismos de seguridad no es tan sencillo, más si cabe, ahora, con la mayor parte de las plantillas teletrabajando y los clientes operando a través de banca digital. Hay que dejar abiertas ciertas puertas para que la comunicación fluya, la economía funcione, mientras se controla la seguridad, sobre todo en los puntos de mayor riesgo. Para ello es necesario llevar a cabo una monitorización 24/7, desplegar sistemas preventivos, reglas de correlación… En definitiva, aplicar medidas de seguridad optimas sobre ese punto, para monitorizar y no siempre bloquear.

Además de desplegar una estrategia de gestión de riesgo basada en la defensa de los puntos más sensibles, desde S21sec recomiendan vigilar las vulnerabilidades Zero Day que se producen, ya que últimamente se han detectado un alto número en productos de grandes fabricantes (desplegados en organizaciones financieras). En este sentido parchear los sistemas es clave, así como mantenerlos actualizados y monitorizados. También el despliegue de un sistema de detección Endpoint Detection and Response (EDR) para poder detectar movimientos laterales, de malware y otro tipo de ataques en los puestos finales y servidores, además de monitorizar y gestionar todo lo que ocurre en las redes y que les pueda aplicar a ellos como entidades financieras. No en vano, siempre van a estar en el punto de mira de los ciberdelincuentes.

Gestión de la seguridad de los datos en tiempos de crisis para las instituciones financieras

ALFONSO MARTÍNEZ,
Country Manager Iberia, Thales Digital Identity & Security

En una crisis mundial sin precedentes como la de la COVID-19, las organizaciones que han implantado nuevas tecnologías y han elaborado un enfoque coherente de su planificación de la continuidad de la actividad y de gestión de crisis, parecen salir mucho mejor paradas.

Esto es especialmente cierto para las instituciones financieras que ahora se enfrentan a nuevos retos de ciberseguridad debido a la pandemia. Según el último informe Modern Bank Heists, la pandemia de COVID-19 se ha relacionado con un aumento del 238% en los ciberataques contra bancos de todo el mundo.

Dado que una filtración de datos puede afectar significativamente a múltiples funciones dentro de una organización, la protección de los datos debe ser responsabilidad de todos los departamentos, además del equipo ejecutivo, para garantizar la continuidad del negocio sin fisuras.

Para ilustrar esto aún más, a continuación se muestra cómo las brechas de datos pueden afectar a funciones cruciales en una institución financiera:

1. FINANZAS

Según el "Informe sobre el coste de una filtración de datos en 2019" ("2019 Cost of a Data Breach Report ") realizado por el Ponemon Institute, el coste medio de una brecha de datos se cifra en 3,92 millones de dólares a nivel mundial. Esta cifra es testimonio del importante daño financiero que cualquier in-

“La mitigación de los riesgos de los datos depende de las inversiones estratégicas en tecnologías de protección de datos y de la adopción de las mejores prácticas de ciberseguridad”

cidente de brecha de datos puede causar a una organización.

2. LEGAL

La mayoría de las normativas de protección de datos, como el Reglamento General de Protección de Datos (RGPD), el Estándar de Seguridad de Datos del Sector de las Tarjetas de Pago (PCI DSS)... obligan a seguir procesos estrictos para proteger los datos sensibles y prescriben sanciones rigurosas en caso de incumplimiento. El incumplimiento de estos mandatos legales puede costar caro a una empresa, como ha experimentado recientemente el operador de telecomunicaciones italiano TIM, que ha sido sancionado con 27,8 millones de euros por la Autoridad de Protección de Datos italiana, Garante, por incumplimiento del GDPR.

3. LÍNEA DE NEGOCIO (LOB)

Las brechas de datos pueden comprometer drásticamente las aplicaciones empresariales básicas, como los sistemas de gestión de créditos, los sistemas de gestión de las relaciones con los clientes (CRM), los sistemas de bases de datos de tarjetas de crédito/débito, etc. La indisponibilidad de estas aplicaciones críticas (que a menudo son el objetivo de los piratas informáticos) puede causar una pérdida significativa de la confianza de los clientes y del negocio.

En este contexto, es fundamental que las instituciones financieras refuercen su resistencia cibernética con herramientas y soluciones adecuadas.

La mitigación de los riesgos de los datos depende de las inversiones estratégicas en tecnologías de protección de datos y de la adopción de las mejores prácticas de ciberseguridad.

A continuación, se presentan tres mejores prácticas para construir una ciberseguridad sin fisuras para una óptima protección de los datos de la empresa.

1. Cifrar los datos sensibles

Busque en los servidores de archivos, las aplicaciones, las bases de datos y las máquinas virtuales los datos en reposo, y rastree los datos en tránsito que fluyen por la red corporativa entre ubicaciones lejanas. Una vez identificados y rastreados estos datos sensibles, es crítico cifrarlos para hacerlos inútiles a los hackers en caso de un ciberataque.

2. Almacenar y gestionar de forma segura las claves de cifrado

Las claves de cifrado pasan por múltiples etapas a lo largo de su vida: generación, distribución, rotación, archivo, almacenamiento, copia de seguridad y destrucción. Gestionar estas claves en cada etapa de su ciclo de vida a través de una solución de gestión de claves centralizada, es fundamental para la protección de los datos.

3. Implantar políticas sólidas de gestión de accesos

Implemente políticas sólidas de gestión de acceso para evitar el acceso no autorizado a los datos cifrados y a las claves de cifrado. Esto es especialmente importante en condiciones de trabajo remoto, para garantizar que sólo el personal autorizado pueda acceder a los datos sensibles en función de la necesidad de conocerlos.

Thales ha estado a la vanguardia para ayudar a las organizaciones a proteger de forma cohesiva sus datos empresariales, y continuar con la actividad habitual incluso en situaciones de crisis. Las soluciones de cifrado de datos y de gestión de claves de Thales, protegen los datos sensibles en todos los dispositivos, procesos, plataformas y entornos, cumpliendo al mismo tiempo con todos los mandatos normativos. ■

Proteger las claves y la gestión de su ciclo de vida

En un mundo cada vez más digital, el uso de certificados y claves criptográficas es imprescindible y por tanto las entidades financieras tienen que poner el foco en cómo se custodian esas claves, además de en la firma digital de las transacciones.

La banca lleva años embarcada en una evolución tecnológica orientada a la provisión de nuevos servicios de valor añadido que le permitan satisfacer las demandas y mejorar la experiencia de sus clientes, además de reducir costes. El avance de los servicios digitales es palpable, está ahí. Sin embargo, Alfonso Martínez, Country Manager España & Portugal del negocio de seguridad e identidad digital de Thales, advierte que tal desarrollo lleva aparejado un incremento de la complejidad, lo que a veces impide a estas organizaciones asegurarse de que las soluciones de seguridad de la información que implementan son realmente capaces de proteger los datos sensibles, confidenciales, que entran y salen de la entidad.

Al respecto de esta protección, Alfonso Martínez explica que las empresas financieras no deben plantearse si están cifrando bien o mal sus datos, si no, más bien, si tienen desplegada una adecuada estrategia de cifrado. De nada sirve implementar una solución de cifrado muy potente o novedosa si al final las claves criptográficas están expuestas o no están protegidas de manera conveniente. Conviene separar el tesoro de la llave, más aún cuando se está produciendo una creciente orientación a servicios en la nube. En este sentido, es primordial que los bancos mantengan la custodia y la propiedad de esas claves criptográficas con las que están cifrando datos sensibles en la nube.

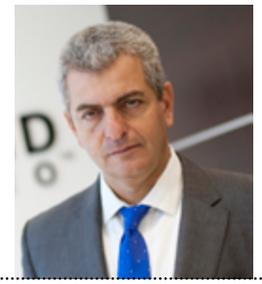
El financiero es un sector hiper-regulado, con muchas normativas a las que hacer frente: PCI DSS, P2PE, PSD2 o GDPR. Sin embargo, Alfonso Martínez explica que además de poner foco en su observancia y en la implantación de soluciones tecnológicas que, como los Módulos de Seguridad de Hardware (HSM), pueden ayudar en su cumplimiento, no hay que pasar por alto otras realidades muy en boga, como el blockchain (con las criptomonedas, los smart contract, IoT) y otras más sencillas, como las facturas electrónicas o el uso de los certificados SSL de los servidores. Al final, en este mundo digital, el uso de certificados y claves es imprescindible, por lo que es muy importante cuidar la forma en que se custodian esas claves y la firma digital de las transacciones.

Sin duda, las entidades financieras no solo se enfrentan a ciberataques, muchos problemas vienen también de las brechas de datos. Sobre ello, Alfonso Martínez especifica que se han visto casos muy cercanos de filtraciones en entidades financieras en las que no solo se han revelado datos bancarios sino también personales (nombre, DNI…). El problema aquí es claro: un número de tarjeta se puede cambiar, pero una identidad u otros datos personales asociados a una cuenta particular es imposible.

Para defender esta información, que también "viaja" a las nubes, ya sea privada, pública o híbrida, Thales propone una estrategia de seguridad que pasa primeramente por descubrir dónde reside la información sensible, por ejemplo, en qué servidores, y de qué tipo de datos se trata (una tarjeta de crédito, una dirección de correo…) para seguidamente proceder a su cifrado. No obstante, ese cifrado hay que asegurarlo poniendo el foco en la custodia de las claves criptográficas y, por supuesto, en una gestión de un ciclo de vida de esa clave para saber a quién pertenece, cuándo ha sido generada o cuando caduca. Se trata, por tanto, de proteger las claves criptográficas y la gestión de su ciclo de vida.

La industria financiera ante nuevos retos y viejas amenazas

JOSÉ BATTAT,
director general de Trend Micro Iberia



En 2020 las ciberamenazas no dieron tregua –la pandemia no ayudó–, y 2021 no está siendo diferente. El cambio de año no ha modificado las ciberamenazas de siempre, implicando que el robo de datos y el ransomware -a menudo en el mismo ataque-, así como el Business Email Compromise (BEC), los troyanos bancarios, el phishing o el malware de minado de monedas sigan copando titulares. Solo en 2020 Trend Micro detectó más de 62.600 millones de ciberamenazas, el 91% de las cuales se originaron en el email. Aunque la mayoría podrían estar vinculadas con ataques automatizados y básicos, podría decirse que son las más dirigidas y personalizadas las que suponen la mayor amenaza para los resultados y la reputación de la empresa.

Algunos sectores pueden verse más afectados que otros este año, pues los ciberdelincuentes siempre van a por el fruto más fácil: las oportunidades de generar el máximo rendimiento de los ataques. Así, aunque bancos y entidades financieras siempre han destacado que la seguridad está entre sus prioridades, el sector y sus clientes siguen estando entre los principales objetivos de los atacantes, a pesar de las nuevas normativas para reforzar aún más la ciberseguridad y la privacidad. Además de las florecientes oportunidades de negocio que han abierto las empresas de e-commerce y tecnología financiera (FinTech), la constante conectividad de los dispositivos móviles inteligentes conectados 24x7 supone para los ciberdelincuentes el acceso para estudiar y observar las lagunas de seguridad, lo que sitúa a los usuarios y a las empresas financieras como

“Los ataques online y offline amenazan constantemente al sector financiero y, a medida que el uso de la tecnología crece y se desarrolla, se presentan simultáneamente más oportunidades de negocio y de ataques”

blancos más fáciles para las transacciones fraudulentas y las brechas.

LA ESTRATEGIA DE SEGURIDAD COMIENZA AQUÍ

Si aún no lo ha hecho, evalúe los ciberriesgos para averiguar cuáles son sus puntos débiles y elabore un plan para solucionarlos.

El enfoque por adoptar dependerá de la predisposición al riesgo de la organización, del sector al que pertenezca y de la madurez de su posición actual de seguridad. Sin embargo, cualquier iniciativa debe incluir formación y concienciación de los usuarios; actividad que debe ser continua e incluir simulaciones de phishing y BEC del mundo real, y debe comunicarse regularmente al personal en pequeños fragmentos. Adapte las sesiones de formación a las últimas campañas de phishing y asegúrese de que sus herramientas ofrecen información detallada sobre las personas para centrarse en los empleados más débiles. Recuerde que todos los empleados, desde el director general hasta el último trabajador, deben asistir, incluidos los trabajadores temporales y los contratistas. Solo hace falta un clic erróneo para meter a la organización en problemas.

Otro enfoque que está ganando en popularidad es el de zero-trust. En un mundo de trabajo distribuido, dispositivos móviles y aplicaciones SaaS, la máxima de “nunca confiar, siempre verificar” se impone. Centre sus esfuerzos en la autenticación de los usuarios con herramientas multifactor (MFA), y despliegue la microsegmentación de red para restringir el acceso a recursos. Este enfoque también se relaciona muy bien con las herramientas SASE basadas en la nube para dar a los equipos de seguridad visibilidad de todo el tráfico entrante y saliente.

Los riesgos asociados a una plantilla distribuida también exigen herramientas de seguridad y gestión de endpoints basadas en la nube para obtener la máxima flexibilidad, visibilidad y control. La detección y respuesta a amenazas adquiere especial importancia, sobre todo las soluciones que incorporan IA para ayudar a los equipos de seguridad a priorizar la forma de hacer frente a los sofisticados ataques entrantes. De hecho, la IA seguirá facilitando la vida de los profesionales de la seguridad al detectar patrones sospechosos en el tráfico de red que los humanos podrían pasar por alto, detectando estilos de escritura anómalos en los emails de BEC y añadiendo automatización a la detección y repuesta.

En definitiva, los ataques online y offline amenazan constantemente al sector financiero y, a medida que el uso de la tecnología crece y se desarrolla, se presentan simultáneamente más oportunidades de negocio y de ataques. Como parte de la “vieja guardia” que se ve obligada por la tecnología a innovar y seguir desarrollándose, la concienciación en seguridad, la vigilancia, la formación y la integridad siguen siendo constantes sólidas en el sector en todo momento. ■

Protección y visibilidad de todos los vectores de ataque

Una mayor conectividad por parte de los usuarios y una evolución hacia una banca cada vez más digital han servido como reclamo para los ciberdelincuentes, que han incrementado el ritmo y la dureza de sus embestidas contra este mercado. Bajo esta situación, José de la Cruz, Director Técnico de Trend Micro, explica cómo la evolución de los ataques y amenazas contra este sector debe ser evaluada desde una doble dimensión.

Desde el punto de vista de TI, con empleados y usuarios interactuando permanentemente con aplicaciones, se aprecia cómo el ransomware ha cobrado una nueva dimensión, con campañas masivas para infectar al mayor número de compañías posible y la subasta de la información sustraída en la Dark Web. Estos ataques son cada vez más diversificados, sobre todo, en cuanto a la tecnología que utilizan para propagarse, y los vectores han cambiado. Así, y aunque el correo electrónico sigue siendo el más utilizado para iniciar un ataque, una vez emprendido este, otros vectores se involucran en el proceso, desde la comunicación a través de las distintas redes hasta la propagación desde endpoints a servidores, cloud, etc.

En lo que respecta específicamente a la banca, las amenazas se dirigen principalmente a tres elementos: infraestructuras, aplicaciones bancarias, y empresas de terceros.

Los cajeros automáticos (ATM) son las infraestructuras más atacadas, y aunque si bien es una tendencia descendente en España, no se debe bajar la guardia. Distinto es cuando se trata de aplicaciones bancarias, con ataques que se dirigen a aplicaciones de uso móvil, y donde el objetivo es el segundo factor de autenticación; y los destinados a los servicios de la entidad expuestos en Internet, aplicaciones y APIs. Por último, destacan las agresiones a la cadena de suministro, donde hay proveedores que interactúan con el banco y que, en muchos casos, no cuentan con las mismas medidas de seguridad.

Además de prepararse para luchar contra estas amenazas, la banca tiene que lidiar también con reglamentaciones como la PSD2, o incluso la futura PSD3. Sobre ello, José de la Cruz confirma que, si bien la PSD2 empezó con brío, por su orientación a fomentar la integración y el pago colaborativo, está empezando a quedarse obsoleta. Y es que, aunque los criterios de colaboración con los que fue creada sí se están cumpliendo, no se puede considerar que exista una homogenización en cuanto a estándares, APIs o modos de colaboración con terceros. En este punto, se espera que la PSD3 establezca una estandarización a nivel de API, lo que implicará además unas condiciones de seguridad más robustas.

A la luz de cómo están evolucionando los ataques y amenazas contra el sector financiero, es vital contar con una visibilidad total de la red, para luchar contra el ransomware; implementar mecanismos de control de dispositivos, de supervisión de integridad, para salvaguardar los ATMs; y optar por un segundo factor de autenticación mucho más robusto, y que no dependa de los SMS, para proteger las aplicaciones móviles.

De igual modo, sería recomendable contemplar el enforcement de políticas de seguridad, a fin de que los usuarios acaten unos requisitos mínimos cuando se conecten con el banco; proteger aplicaciones y containers; y, cuando se trate de cloud, vigilar el CSPM (Cloud Security Posture Management) para el cumplimiento de normativas. Por último, y para defender la cadena de suministro, es clave implementar mecanismos para proteger no solo a la entidad sino también a terceros.

S21 SEC

DFIR

Digital Forensics & Incident Response

¿Sabes cómo enfrentar un incidente grave de seguridad?

No serás juzgado por el incidente, sino por la velocidad en resolverlo.

¡Contáctanos ahora para obtener más información!

marketing@s21sec.com

www.s21sec.com/es/dfir-incidentes-seguridad/

Permitir la productividad en Internet con el más alto nivel de seguridad

La misión de Check Point es "proporcionar a cualquier organización la capacidad de realizar su trabajo en Internet con el más alto nivel de seguridad". Abordan las necesidades de ciberseguridad más inminentes de las organizaciones basándonos en tres principios básicos:

1. Enfoque de prevención en primer lugar: implementar protecciones de usuario preventivas para eliminar las amenazas antes de que lleguen a los usuarios.

2. Gestión Gold Standard: panel único para gestionar todo el patrimonio de seguridad.

3. Solución consolidada: obtenga una protección preventiva completa contra las amenazas más avanzadas mientras logra una mejor eficiencia operativa.

SECURE YOUR EVERYTHING CON CHECK POINT INFINITY

En esta nueva normalidad, permiten a los clientes mantener la productividad mientras permanecen protegidos en todo lo que hacen. Dondequiera que se conecte, a lo que se conecte y como quiera que se conecte: su hogar, sus dispositivos, su privacidad y los datos de su organización deben estar seguros y protegidos de cualquier amenaza cibernética. Para hacer realidad su visión, en 2021 han recalibrado su oferta de productos Infinity para enfocarlas hacia aquellas tecnologías y capacidades que brindarán seguridad sin concesiones basada en estos tres principios básicos.

Check Point consolida más de 80 productos y tecnologías y los ha organizado en tres pilares principales: Harmony, CloudGuard y Quantum, con Infinity-Vision como base.

HARMONY: EL MÁS ALTO NIVEL DE SEGURIDAD PARA USUARIOS REMOTOS

Check Point Harmony protege a los empleados remotos, los dispositivos y la conectividad a Internet de ataques maliciosos, al tiempo que garantiza un acceso remoto seguro y de confianza cero a cualquier escala y en cualquier aplicación corporativa. Check Point Harmony proporciona conectividad segura y de punto final (SASE), como una solución consolidada y unificada basada en la nube que incluye acceso remoto fácil y seguro (basado en la adquisición de Odo), navegación segura por Internet, punto final y seguridad mó-

vil y seguridad del correo electrónico. La solución ofrece la cobertura más amplia de vectores de ataque con la prevención de amenazas impulsada con Inteligencia Artificial.

Harmony presenta tecnologías que admiten entornos híbridos seguros de trabajo desde cualquier lugar (WFA). Asegurar a los empleados en el domicilio se ha convertido en una de las principales prioridades de las organizaciones de todo el mundo. La nueva familia de productos Harmony reúne más de siete categorías de productos para proporcionar una protección preventiva completa para los usuarios remotos. Incluye conectividad segura desde cualquier lugar y un entorno de trabajo seguro en cualquier dispositivo, incluidos los dispositivos móviles, personales y administrados por la empresa, tanto cliente como sin cliente.

CLOUDGUARD: NUBE SEGURA DE FORMA AUTOMÁTICA

CloudGuard optimiza la protección de las cargas de trabajo críticas en la nube, tanto públicas como privadas. Ofrece gestión de la postura en la nube, seguridad serverless y una nueva generación de firewalls de aplicaciones web con tecnología de Inteligencia Artificial contextual que protege las API, las aplicaciones web y los servidores web alojados y on-premise.

CloudGuard proporciona seguridad consolidada y prevención de amenazas en todos los entornos, activos y cargas de trabajo de la nube. Alineado con la naturaleza ágil del desarrollo y la implementación en la nube, CloudGuard ofrece una solución tanto para los profesionales de la seguridad en la nube como para las DevOps en la nube, desde la fase inicial de DevSecOps, pasando por la seguridad de la red en la nube hasta la seguridad de las aplicaciones en la nube (WAAP), así como la protección de contenedores y funciones sin servidor.

QUANTUM: SEGURIDAD DE LA RED EMPRESARIAL PARA EL PERÍMETRO Y EL DATACENTER

En 2021, la compañía seguirá aprovechando Maestro, su solución de rendimiento escalable única y disruptiva. Acelerarán la innovación en el firewall del centro de datos con la introducción de un gateway de firewall súper rápido con un rendimiento de firewall de 200 Gbps y una latencia de menos de 3 microsegundos.

Quantum refleja la solución de seguridad de red más completa para cada organización, perímetro y centro de datos, que abarca IoT Nano-Security hasta superredes Terabit y ofrece los más altos niveles de seguridad y rendimiento para administrar entornos de centros de datos.

Las puertas de enlace de seguridad de Check Point Quantum brindan una seguridad superior más allá de cualquier firewall de próxima generación (NGFW) y están diseñadas para administrar los requisitos de políticas más complejos. Con más de 60 servicios de seguridad, estos gateways previenen la quinta generación de ciberataques.

Además, tienen previsto el lanzamiento de una nueva serie de dispositivos para sucursales y oficinas dirigidos a las pequeñas y medianas empresas: Quantum SPARK.

INFINITY-VISION

Pensada para lograr una gestión de seguridad unificada y un 100% de prevención de brechas de seguridad. Permite la administración todo el patrimonio de seguridad con Check Point Infinity Portal, una gestión de seguridad como servicio (SMaaS) basada en la nube. Entregue políticas, supervisión e inteligencia unificadas desde un solo punto. Exponga, investigue y bloquee los ataques más rápido, con una precisión del 99,9% con las capacidades SOC y XDR utilizadas por Check Point Research. ■

MÁS INFORMACIÓN

- Quantum
- Harmony
- CloudGuard
- Infitiny Vision

Entrust ayuda a las empresas de servicios financieros a mejorar la seguridad de sus datos y el cumplimiento de la normativa

Empresas de servicios financieros de todo el mundo confían en Entrust para abordar sus desafíos de seguridad. Entrust cuenta con una gama de soluciones de hardware y software para ayudar a las empresas a reducir el riesgo, cumplir los distintos reglamentos y mejorar la agilidad mientras persiguen objetivos estratégicos en torno a tecnologías emergentes de pago y transacciones:

- Sólida administración de claves.
- Entorno de ejecución seguro.
- Alineación con los estándares regulatorios y de cumplimiento global en varios entornos.
- Listo para aplicaciones de Blockchain.

LA FAMILIA DE PRODUCTOS NSHIELD DE ENTRUST

Los módulos de seguridad de hardware (HSMs) nShield de Entrust son dispositivos reforzados y resistentes a manipulaciones indebidas que protegen los datos más confidenciales de su empresa. Estos módulos con certificación FIPS 140-2 realizan funciones criptográficas como la generación, administración, protección de claves y proceso de firma seguro, así como la ejecución de las funciones sensibles dentro de sus límites protegidos.

Para adecuarlos con su entorno específico, la familia de productos de HSM nShield incluye los siguientes modelos:

- **nShield Connect:** dispositivos conectados a la red
- **nShield Edge:** Módulo portatil con conexión USB
- **nShield Solo:** Tarjetas PCIe para integrar en dispositivos o servidores
- **nShield as a Service:** Solución por suscripción para acceder a HSM nShield en la nube

FUNCIONALIDADES DE LA FAMILIA DE PRODUCTOS NSHIELD DE ENTRUST

Interfaces de servicios web compatible con la nube

El nShield Web Services Option Pack optimiza la interfaz entre sus aplicaciones y HSM al ejecutar comandos a través de llamadas de servicio web.

Soporte contenerizado en instalaciones o en la nube

El nShield Container Option Pack proporciona un conjunto de scripts preempaquetados que simplifican en gran medida la integración de los HSM nShield y de esa manera proveed servicios

de criptografía a las aplicaciones desplegadas en contenedores.

*** Administración de claves para sus datos en la nube con nShield BYOK**

nShield BYOK (Bring Your Own Key) le permite generar claves robustas en el HSM nShield ubicado en las instalaciones y exportarlas de forma segura a sus aplicaciones en la nube, ya sea si utiliza Amazon Web Services, Google Cloud Platform, Microsoft Azure, o las tres.

*** Optimización de operaciones utilizando Administración y Monitorización remota**

nShield Monitor y nShield Remote Administration, disponibles para los HSM nShield Solo y Connect, le ayudan a reducir los costos operativos a la vez que se mantiene informado y en control 24x7 de sus estados de HSM.

*** Configuración remota**

Los modelos nShield Connect XC ofrecen una opción de consola en serie simplificando la instalación física del HSM para alinear, cablear y aplicar potencia. Esto facilita la implementación y la reimplementación sin necesidad de revisitar el centro de datos.

*** Arquitectura altamente flexible de Security World**

La arquitectura de Security World de nShield admite HSM nShield de Entrust mediante la creación de un entorno de administración de claves flexible y exclusivo. Con Security World de nShield, usted puede combinar diferentes modelos de HSM nShield para construir un ecosistema unificado que ofrece escalabilidad, perfecta tolerancia a fallos y balance de carga.

SOLUCIONES DE CIFRADO DE WORKLOAD, GESTIÓN DE CLAVES INTEGRADA PARA ENTORNOS MULTI-NUBE

Gestión universal de claves para workload cifrados

Entrust KeyControl es un servidor KMIP certificado por VMware, escalable y con muchas funciones, que simplifica la gestión de claves para los workload cifrados. Sirve como KMS para los clientes encriptados de VMware vSphere y vSAN, así como para otros productos compatibles con KMIP.

Cifrado de datos, gestión de claves multi-nube y seguridad del workload

Entrust DataControl asegura las workloads multi-nube a lo largo de su ciclo de vida y reduce la complejidad de proteger las cargas de trabajo a través de múltiples plataformas de nube. Funciona en las instalaciones y con las principales plataformas de nube pública, así como con soluciones de hiperconvergencia y almacenamiento. DataControl incluye el servidor de gestión de claves (KMS) de Entrust KeyControl, certificado por VMware.

ALIANZAS CON LÍDERES DE LA INDUSTRIA

Entrust a través del programa de sus socios tecnológicos, colabora para integrar los HSM nShield en una variedad de soluciones de seguridad incluyendo la creación de credenciales y PKI, seguridad de base de datos, firma de códigos, firmas administración, gestión de cuentas privilegiadas, entrega de aplicaciones, inteligencia en la nube y los big data. ■

MÁS INFORMACIÓN

- Uno de los diez bancos más importantes del mundo implementa los HSMs de Entrust para ofrecer servicios fiables y de confianza a sus clientes y colaboradores
- Protección de Blockchain
- Estudio Global de Tendencias de Cifrado 2021
- Protección de claves en entornos híbridos

cpl.thalesgroup.com

THALES
Building a future we can all trust

CipherTrust Data Security Platform

Localice, proteja y controle los datos sensibles de su organización en cualquier lugar gracias a la protección de datos unificada de última generación.

Localizar Proteger Controlar

Empiece a localizar, proteger y controlar sus datos hoy mismo

Protección para entornos financieros

RealSec dispone de una serie de soluciones de seguridad, tanto de propósito general como orientadas al segmento financiero. Aquí repasamos algunas de ellas.

SOLUCIONES DE CIBERSEGURIDAD

❖ **HSM de Propósito General/ Cryptosec LAN**

Se trata de un servidor criptográfico en red, de altas prestaciones y seguridad, diseñado para servicios de cifrado y aplicaciones de firma digital, independientemente del sistema operativo dónde éstas residan. Ofrece generación, almacenamiento y custodia de claves y certificados capaces de integrarse con aplicaciones de firma electrónica, PKI, cifrado de archivos y BBDD, blockchain...

❖ **HSM Financiero / Cryptosec Banking**

HSM financiero para pagos en red, de muy alto rendimiento, que proporciona toda la operativa y funcionalidad criptográfica específica para el ámbito de Banca, Fintech y la industria de los Medios de Pago. Cumple con todos los requerimientos y estándares definidos por el consorcio PCI (VISA, MASTERCARD...).

❖ **Remote Key Load / Cryptosec RKL**

Automatización de la carga de Claves en los ATM utilizando cifrado asimétrico, en sustitución del antiguo proceso de carga manual, tan costoso como ineficiente. Es la solución del mercado más avanzada, madura y eficiente que ofrece servicio multiempresa y está homologada por las marcas más importantes y reconocidas de ATM internacionales, cumpliendo con los requerimientos definidos por el consorcio PCI.

SOLUCIONES CIFRADO Y FIRMA DIGITAL

❖ **Servidor de firma digital/ CryptoSign Server**

Servidor Integrado de Firma Digital que incluye en un único dispositivo (hardware y software) los elementos necesarios para que, en un entorno de red, se pueda realizar cualquier proceso de firma con las mayores garantías de seguridad y gestionar los certificados digitales.

❖ **Autoridad de Sellado de Tiempo/ Cryptosec Openkey TSA**

La Firma Digital asegura quien ha realizado una determinada acción, pero no es válida para certificar que la acción se ha producido en un determinado instante de tiempo. Para ello, se requiere de una Autoridad de Sellado que afirme y certifique que los documentos electrónicos firmados han existido desde un determinado momento, y que son válidos desde ese instante.

❖ **Servidor de cifrado y firma digital de correo electrónico/ Cryptosec Mail**

Sistema centralizado de firma digital y/o cifrado del correo electrónico capaz de alma-

cenar y administrar, de forma segura, las claves de los certificados ya que está orientada a minimizar los riesgos del «Phishing» y a conseguir la total confidencialidad del contenido de los correos mediante su encriptación.

❖ **Autoridad de Validación/ Cryptosec Openkey VA**

Con la Autoridad de Validación podemos conocer el estado de revocación de los certificados digitales emitidos bajo una determinada infraestructura. ■

AUTORIDAD DE SOLUCIONES PKI

❖ **Certificación/ Cryptosec Openkey CA**

La Autoridad de Certificación es el elemento más importante y al que más hay que proteger en una infraestructura de clave pública (PKI). Es el componente de confianza emisor de los certificados y que determina su validez en el tiempo.

❖ **Autoridad de Registro/ Cryptosec Openkey RA**

La Autoridad de Registro es el punto de acceso de los usuarios finales a la Autoridad de Certificación. Al mismo tiempo que es el instrumento en el que se generan las solicitudes de certificación y las solicitudes de revocación.

MÁS INFORMACIÓN

- Segundo Informe Blockchain
- Cifrado y Firma Digital para Organizaciones Inteligentes
- Fintech y Banca. Tendencias de seguridad & HSM

Cobertura completa de riesgos de ciberseguridad en los procesos de negocio

El desarrollo de un mundo cada vez más hiperconectado, en el que las empresas enfrentan complejos procesos de transformación digital y dependen de un mayor de dispositivos conectados a Internet, resulta clave proteger los datos de las organizaciones, así como la operatividad de sus sistemas y cumplimiento con el RGPD.

S21sec es, tal y como se define a sí misma, "la compañía pure-player de ciberseguridad más grande de Iberia con una dilatada experiencia en el sector, lo que le permite ofrecer una cobertura completa de riesgos de ciberseguridad en los procesos de negocio de las organizaciones".

Una plantilla de más de 500 expertos refleja las capacidades de S21sec para investigar, detectar y prevenir amenazas; piezas clave para reaccionar con mayor rapidez ante cualquier ataque e identificar, diagnosticar y remediar eventuales incidentes en el menor tiempo posible.

Perteneciente al grupo Sonae, S21sec está entre las cinco principales compañías de ciberseguridad de Europa, con la aspiración de liderar el mercado europeo a medio plazo.

Además, cuenta con el primer SOC de España, convertido ahora en un multiSOC

global distribuido en cuatro localizaciones, garantizando la integridad de múltiples organizaciones en España, Portugal y México.

S21sec se guía por una serie de valores clave a la hora de desarrollar e implementar sus soluciones con éxito:

Una plantilla de más de 500 expertos re-fleja las capacidades de S21sec para inves-tigar, detectar y prevenir amenazas

- **Transparencia:** se pone a disposición la información necesaria para la colaboración y la toma de decisiones colectivas.
- **Excelencia:** se persigue ofrecer la más alta calidad gracias a encontrarse en un continuo proceso de aprendizaje.
- **Trabajo en equipo:** se dedica esfuerzo para encontrar la mejor forma de ayudarse entre sí, poniendo el rendimiento de la compañía por encima del rendimiento individual.
- **Innovación:** se busca la diferenciación a través de implementar cambios que mejoran su eficiencia y ventaja competitiva.
- **Confianza:** se construyen relaciones con las personas y las organizaciones basadas en la confianza y la honestidad.
- **Pasión:** se disfruta del trabajo porque siempre se busca de manera proactiva diferenciarse.

PROPUESTA DE SOLUCIONES

S21sec aúna soluciones diferentes de manera transversal y está diseñado en torno a cinco necesidades:

1. **Identificar:** análisis de riesgos y plan general de ciberseguridad, cumplimiento regulatorio, ciberseguridad en la nube y programas de transformación y Red Team.
2. **Proteger:** diseño y despliegue de arquitecturas y tecnologías, servicios de formación y concienciación, gestión de dispositivos de seguridad, seguridad de la información y seguridad ATM.

3. **Detectar:** SOC gestionado y SIEM como servicio, Unidad de Inteligencia de Ciberamenazas, EDR - Detección y respuesta End Point.
4. **Responder:** CSIRT - Gestión de incidentes de ciberseguridad 24x7, DFIR - Análisis forense digital y respuesta ante incidentes, plataforma de respuesta ante incidentes, SOAR - Automatización, Remediación y Orquestación de la Ciberseguridad y amenazas emergentes - evaluación y perfilación.
5. **Recuperar:** Continuidad de negocio y planes de respuesta ante ciber-desastres. ■

MÁS INFORMACIÓN

- Threat landscape report
- Test autoevaluación cyberGRC

Soluciones de cumplimiento y seguridad de datos para la banca y servicios financieros

Los proveedores de servicios financieros de todo tipo están ampliando sus ofertas para competir a escala global, ahorrar costes y mejorar la experiencia del cliente con servicios de valor añadido. Pero a medida que evolucionan los servicios financieros, deben asegurarse de que sus soluciones de seguridad TI sean realmente capaces de proteger los datos confidenciales que se adquieren y transmiten.

Thales ofrece soluciones integrales de gestión de acceso y protección de datos que aseguran los datos en dispositivos, procesos y plataformas in situ y en la nube. Estas soluciones ayudan a las organizaciones a cumplir con los requisitos de cumplimiento de los servicios financieros, facilitan la auditoría de seguridad, protegen a sus clientes y evitan el daño a su reputación causado por brechas de datos.

En cuanto a seguridad, el sector financiero se enfrenta a varios desafíos:

- **Cubrir los requisitos de cumplimiento de los servicios financieros.** El cumplimiento normativo puede llegar a ser abrumador para los servicios financieros. Las normativas que abarcan requisitos de seguridad de datos incluyen PCI DSS para información relacionada con tarjetas de crédito, el RGPD y PSD2 en la UE, SOX/J-SOX, leyes de notificación de brechas de datos y de residencia locales, y muchas más en todo el mundo.
- **La protección de los datos.** Para evitar multas costosas y proteger su reputación, las empresas del sector bancario y financiero y sus ejecutivos deben salvaguardar los datos financieros confidenciales contra la exposición accidental, información privilegiada deshonesta, APT y otras amenazas conocidas y desconocidas. Y no solo deben existir procedimientos para proteger los datos, sino también para identificar y alertar a la organización cuando se produce un acceso no autorizado.

¿CÓMO THALES LES PUEDE AYUDAR?

Thales cuenta con una oferta de soluciones en diferentes áreas que incluyen:

✱ **Soluciones de cifrado.** Las soluciones de protección de datos CipherTrust Transparent Encryption y CipherTrust Application Data Protection , incluídas en la solución CipherTrust Data Security Platform de Thales, proporcionan un único marco extensible para proteger los datos en reposo bajo los diversos requisitos de la industria de servicios bancarios y financieros en la más amplia gama de plataformas de sistemas operativos, bases de datos, entornos de nube e implementaciones de Big Data. El resultado es un bajo costo total de propiedad, así como una implementación y operación simples y eficientes.

✱ **Administración de claves robusta.** Las soluciones de administración de claves de Thales, permiten la gestión centralizada de claves de cifrado para otros entornos y dispositivos, incluido el hardware compatible con KMIP, claves maestras TDE de Oracle, SQL Server...

✱ **Protección de datos de pago.** Las soluciones de Thales están diseñadas específicamente para aplicaciones de pago. El módulo payShield 10K, la quinta generación de HSM de pago de Thales, ofrece un conjunto de funciones de seguridad de pagos comprobadas en entornos críticos y que incluyen el procesamiento de transacciones, protección de datos confidenciales, emisión de credenciales de pago, aceptación de tarjetas móviles y tokenización de pagos. payShield 10K de Thales atiende lo último en requisitos de seguridad obligatorios y en mejores prácticas para una amplia gama de organizaciones que incluyen EMVCo, PCI SSC, GlobalPlatform, Multos, ANSI, así como las varias marcas y redes de pago globales y regionales.

Por otro lado, CipherTrust Tokenization with Dynamic Data Masking permite a los administradores establecer políticas para devolver un campo completo tokenizado o enmascarar dinámicamente partes de un campo. Con las capacidades de tokenización de la solución que preservan el formato, los administradores pueden restringir el acceso a activos confidenciales y, al mismo tiempo, formatear los datos protegidos de una manera que les permita a muchos usuarios hacer su trabajo.

VENTAJAS DE LAS SOLUCIONES THALES

Las soluciones de Thales ofrecen:

❖ **Cumplir las obligaciones reglamentarias.** Con sus productos de Data Security, la industria bancaria puede cumplir con los estándares regulatorios y de seguridad de datos en reposo mientras protege la información de brechas de datos en toda la empresa, en la nube y en entornos de Big Data.

❖ **Rápida de instalar.** Thales puede instalar las soluciones de seguridad de datos CipherTrust en semanas en lugar de meses. Las soluciones de Thales funcionan con la mayoría de los principales sistemas operativos, incluidos los servidores Linux, UNIX y Windows en entornos físicos, virtuales, en entornos de datos de titulares de tarjetas (CDE) de la nube y Big Data.

❖ **Fácil de usar.** Su oferta CipherTrust Data Security Platform simplifica la resolución de problemas de seguridad y cumplimiento al proteger simultáneamente los datos en bases de datos, archivos y nodos de Big Data, en nubes públicas, privadas, híbridas e infraestructuras tradicionales. La administración centralizada de toda la plataforma de seguridad de datos, facilita la ampliación de la protección de seguridad de los datos, y la satisfacción de los requisitos de cumplimiento en toda la empresa, creciendo según sea necesario, sin agregar nuevo hardware ni aumentar las cargas operativas. ■

MÁS INFORMACIÓN

- Cifrado Total
- The Key Pillars for Protecting Sensitive Data
- payShield Brochure

Soluciones más robustas gracias a la inteligencia de amenazas compartida

Trend Micro trabaja para ayudar a que el mundo sea seguro para el intercambio de información digital. Aprovechando los más de 30 años de experiencia en seguridad, investigación de amenazas globales e innovación continua, la firma permite la resiliencia de las empresas, gobiernos y consumidores con soluciones conectadas a través de cargas de trabajo en la nube, endpoints, correo electrónico, IIoT y redes.

Su estrategia de seguridad XGen impulsa sus soluciones con una combinación intergeneracional de técnicas de defensa frente a amenazas que están optimizadas para los entornos clave y aprovecha la inteligencia de amenazas compartida para una mejor y más rápida protección.

SOLUCIONES Y PRODUCTOS

Trend Micro ha innovado para adaptar su oferta a la evolución de las amenazas y a las necesidades de empresas y usuarios. Cuentan con un amplio catálogo de productos que permiten ofrecer protección en cualquier entorno, ya sea físico, virtual, en la nube y en contenedores.

El catálogo de Trend Micro ofrece una mayor cobertura, pues busca cubrir todos los vectores de ataque posibles (endpoint, cloud, navegación, email, entornos colaborativos, redes privadas/cloud, OT...), y por tecnología, ya que combinan tecnología de última generación junto con la experiencia que les aporta su trayectoria en el mercado.

Un ejemplo de esta evolución es la Tecnología XDR, introducida en el mercado por Trend Micro, que aprovecha la información recabada por los distintos vectores (endpoint, servidores, correo, red...). XDR extiende las capacidades del EDR tradicional aportando contexto a los ya citados ataques multivector, permitiendo a los clientes identificarlos y bloquearlos de manera prematura.

Por otro lado, Trend Micro estructura su oferta en torno a los siguientes ejes:

❖ **Solución Hybrid Cloud Security:** agrupa seguridad cloud simplificada gracias a la plataforma de servicios Trend Micro Cloud One. Protege entornos físicos, virtuales, en la nube y en contenedores con control y visibilidad centralizados; proporciona un conjunto completo de prestaciones de seguridad; reduce el número de herramientas de seguridad necesarias para proteger entornos híbridos y satisfacer los requisitos de cumplimiento; ahorra recursos y reduce los costes con una seguridad optimizada del entorno y políticas automatizadas. Disponible como software, como servicio, o en los marketplaces de AWS y Microsoft Azure, cuenta con tecnología de seguridad XGen, que ofrece un conjunto intergeneracional de controles de seguridad optimizados para entornos líderes.

❖ **Network Defense Solution:** área desde el que ofrece protección contra amenazas conocidas, desconocidas y ocultas, es decir, aquellas vulnerabilidades de las que no se tiene visibilidad y que residen en la red. Mediante la integración de las soluciones de Intrusion Prevention (IPS) y Advanced Threat Protection (incluido sandboxing), Trend Micro proporciona una combinación de técnicas intergeneracionales y de detección de defensas avanzadas para aumentar al máximo la protección e ir más allá de lo conocido y desconocido, ofreciendo protección más inteligente, logrando tiempos de reacción más rápido, mayor rendimiento y protección automatizada que se adapta a entornos híbridos.

❖ **User Protection Solution:** brinda protección avanzada e inteligente a los usuarios con la técnica adecuada en el momento adecuado, en cualquier dispositivo, aplicación y lugar. Se trata de una seguridad conectada y que utiliza varias capas para detener las amenazas emergentes y reducir los gastos de gestión. Seguridad optimizada para funcionar en su entorno por un proveedor de confianza y con visión de futuro que siempre trabaja en una nueva generación de seguridad. Gracias a Smart Protection Suite, son capaces de proteger a los usuarios desde el gateway hasta el endpoint.

Este catálogo de soluciones, que también abarca el segmento de la pyme, se ve complementado con servicios de soporte al cliente para garantizar un funcionamiento sin problemas y una asistencia superior. ■

MÁS INFORMACIÓN

- The Banking and Finance Industry Under Cybercriminal Siege: An Overview
- Banks Under Attack
- Mobile Banking Trojan

TREND MICRO™

THE ART OF CYBERSECURITY

Trend Micro Vision One™

Mayor visibilidad para una respuesta más rápida

Una plataforma especialmente diseñada para la defensa contra amenazas que va más allá que otras soluciones XDR

Más información en:
www.trendmicro.com