Digitalización y Seguridad, motor de innovación financiero

Patrocinadores:

Digitalización y Seguridad,

motor de innovación financiero

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. La industria de los servicios financieros atraviesa por una de las etapas de transformación más profundas que se ha visto, a través de la tecnología, la banca dejará de ser un sitio físico al que los clientes van, para convertirse en algo que los clientes hacen estén donde estén.

Como el resto de los sectores, la banca española también ha experimentado la necesidad de acelerar su transformación digital a raíz de la pandemia del coronavirus. Aunque era algo en lo que se llevaba trabajando ya varios años, 2020 ha supuesto la necesidad de pisar el acelerador. Según datos de Funcas, el gasto tecnológico de las diez principales entidades bancarias españolas, las cuales concentran más del 80% de los activos

bancarios, ha alcanzado los 4.774 millones de euros en 2021, aumentando un 12,2% con respecto al año anterior. Esto supone el doble de la inversión realizada en 2015 y representa el 9,44% del total de su presupuesto. Las previsiones indican que para 2025 la cifra del gasto tecnológico del sector podría superar los 6.600 millones de euros. En la misma línea se manifiestan los propios profesionales del sector, como demuestra que el 92% asegura haber notado cierta evolución durante los últimos años en su puesto de trabajo, según se extrae del 'Informe de Adaptación Digital 2022' de la escuela de negocios IEBS.

TENDENCIAS DEL SECTOR BANCARIO

El eBook interactivo 'Top Trends in Banking 2022' elaborado por Capgemini analiza cuáles serán las principales tendencias de la banca comercial para los próximos años. Según este informe, 2022 plantea ya un escenario preparado para que las firmas comerciales pasen de la banca tradicional para empresas a un modelo más experiencial. A medida que evolucionen los pagos en tiempo real, los bancos aprovecharán la automatización que proporciona la inteligencia artificial para permitir la gestión de la tesorería en tiempo real, mejorando así la previsión del flujo de caja para sus clientes.

El siguiente paso para la banca comercial será monetizar los servicios digitalizados a través de modelos 'as-a-service'. Al mismo tiempo, las Fintech diversificarán el ecosistema de la banca de consumo mediante la colaboración con operadores tradicionales o la introducción de súper aplicaciones de ventanilla única para todas las necesidades bancarias. Además, las empresas de préstamo alternativas que han nacido apoyándose en la tecnología estarán en disposición de satisfacer las demandas de las micro, pequeñas y medianas empresas con dificultades para acceder a los préstamos bancarios tradicionales.

Por otro lado, la abundancia de datos y el acceso a las nuevas tecnologías impulsarán la transformación del back-office y de la oficina, permitiendo a los bancos optimizar sus decisiones en materia de crédito. Además, las entidades más progresistas apostarán por contratos inteligentes impulsados por blockchain, que mejorarán las funciones de negociación y liquidación en tiempo real.

UNA BANCA OMNICANAL

Para ofrecer la mejor experiencia a sus clientes, el sector bancario ha necesitado hacer una clara apuesta por la omnicanalidad. El informe 'Transición digital y transformación del negocio bancario en España impulsado por la COVID-19', elaborado por KPMG junto a la Fundación de Estudios Financieros (FEF), destaca que en 2020 la mitad de los productos financieros

fueron vendidos a través de internet, llegando incluso al 60% durante los meses más duros del confinamiento. Además, 6 de cada 10 españoles ya habrían sustituido la banca física por la digital, mientras que para la mayoría de las entidades, más de la mitad de sus clientes ya son digitales. En la misma línea se muestra PwC en el informe 'Payments 2025 & Beyond', que señala que en 2030, los pagos electrónicos a nivel global van a triplicarse hasta superar los tres billones de operaciones. Según este informe, el mayor crecimiento se experimentará entre 2020 y 2025, ya que las transacciones electrónicas crecerán un 82% pasando de un billón a 1,8 billones de operaciones, mientras que entre 2025 y 2030 este crecimiento será del 61%, hasta sobrepasar los tres billones de transacciones en todo el mundo.

LA TECNOLOGÍA AL SERVICIO DE LOS BANCOS

En pleno 2022, el camino hacia la transformación digital del sector financiero es ya un hecho. La tecnología se ha convertido en la clave de estos tiempos, y es importante estar al tanto de los últimos avances para no quedarse atrás. En su informe 'Tendencias Digitales 2022 Banca y Seguros', t2ó señala tres principales tendencias tecnológicas en Banca & Seguros en 2022: Inteligencia Artificial, Metaverso/Realidad Virtual y Cloud. Además, no hay que olvidar la importancia que está cobrando el blockchain y la analítica de datos, además de la securización que todo este cambio de paradigma conlleva. Todas estas tecnologías van a acompañar al sector financiero en su camino hacia una transformación digital efectiva y con la mente puesta en el verdadero centro de sus estrategias: el usuario.

BANCA INTELIGENTE

El informe de t2ó señala que tecnologías como la Inteligencia Artificial (IA) serán clave para optimizar y agilizar los procesos de las empresas, así como para poder ofrecer nuevos y mejorados servicios a los clientes. Un artículo del think tank europeo especializado en economía Bruegel señala que antes de la pandemia el sector bancario era el segundo sector que más invertía en IA, solo por detrás del tecnológico. La Asociación Española de Banca resalta la importancia de estas tecnologías en su informe "El uso de la Inteligencia Artificial en el sector bancario", indicando que gracias a estas tecnologías se está mejorando la experiencia del usuario, aumentando la eficiencia en los procesos internos y reforzando la seguridad, entre otros. De hecho, la encuesta 'Global AI Survey' de McKinsey señalaba que el 60% de los servicios financieros ya había integrado menos un proceso basado en inteligencia artificial, sobre todo en tres vertientes: automatización de procesos (36%), asistentes virtuales (32%) y técnicas de machine learning (25%).

El gasto tecnológico de las diez principales entidades bancarias españolas ha alcanzado los 4.774 millones de euros en 2021

DIGITALIZACIÓN Y SEGURIDAD, MOTOR DE INNOVACIÓN FINANCIERO

METAVERSO FINANCIERO

Otra de las tecnologías que va a cobrar un protagonismo importante en el sector financiero en los próximos años es el de la realidad virtual, sobre todo con el desarrollo del metaverso. Como indica el informe de t2ó, el usuario se impone como centro de todas las estrategias de marca, por lo que las empresas buscan ofrecer nuevas experiencias inmersivas y diferenciales sobre su competencia, a la vez que se busca alcanzar a nuevos públicos y clientes potenciales, para lo cual el Metaverso se muestra como una gran opción. Según el informe 'Augmented reality (AR), virtual reality (VR), and mixed reality (MR) market size worldwide in 2021 and 2028' de Statista, el mercado global de realidad aumentada, realidad virtual y realidad mixta crecerá por encima de los 250.000 millones de dólares en 2028 a nivel global. Como indica Funcas en su artículo 'El uso de la realidad virtual en el sector bancario', se tendería a una virtualización de las oficinas bancarias con el objetivo de que el cliente pudiera realizar las mismas operaciones en un entorno similar al real, pero que implicara menos costes. Paralelamente ya se están desarrollando aplicaciones de realidad virtual capaces de mostrar servicios financieros en 3D. Por otro lado, sobre todo tras el anuncio de Facebook de su apuesta por el metaverso pasando incluso a cambiar el nombre de su matriz por Meta, esta tecnología está creciendo a un ritmo imparable. De hecho, Citi señala en su informe 'Metaverse and Money: Decrypting the Future', que cuenta con un mercado objetivo de 5.000 millones de usuarios y que podría tener un volumen de entre 8 billones y 13 billones de dólares en 2030. Además, esta misma fuente indica que en base a las predicciones del Fondo Monetario Internacional (FMI), este mercado alcanzará los 128 billones de PIB para ese año.

LA NUBE, SIEMPRE LA NUBE

Uno de los pilares más importantes de esta transformación digital que están llevando a cabo empresas de todos los sectores son las plataformas y los servicios en la nube. El cloud se ha convertido en el gran protagonista de nuestro tiempo, ya que el primer paso que conlleva esta digitalización del sector es la migración de todos los activos hacia la nube, ya sean plataformas, datos, aplicaciones o cualquier proceso. Esto supone un reto para las empresas más tradicionales, sobre todo en un sector como el financiero,

> A medida que evolucionen los pagos en tiempo real, los bancos aprovecharán la automatización que proporciona la inteligencia artificial para permitir la gestión de la tesorería en tiempo real

en el que la seguridad se vuelve de importancia capital. Deloitte indica en su informe anual 'Tech Trends 2022' que en 2020, el mercado global de cloud superó en volumen por primera vez al mercado no-Cloud, en parte a causa de la pandemia. La estimación de Deloitte es que el mercado Cloud doblará en tamaño al no-Cloud para el año 2025. Por otro lado, se espera que para este año los servicios en la nube supongan ya el 40% del gasto de IT en el sector financiero, gasto que para 2028 podría ya suponer hasta el 80%, conforme a datos del estudio 'Construyendo los servicios financieros del futuro', confeccionado por IDC junto a OpenText.

BLOCKCHAIN, EL FUTURO DE LAS FINANZAS

La cadena de bloques ha emergido como una de las tecnologías que más dará que hablar en un futuro próximo. Esta tecnología, que aún se encuentra en sus primeras fases de adopción, será capaz de facilitar transacciones más rápidas y sencillas, a la par que seguras. Este artículo de The European Business Review señala que el 66% de las entidades bancarias tiene previsto implementar soluciones basadas en blockchain en los próximos tres años. Aquí también entran en juego las criptomonedas y la tokenización de activos, a debate en las últimas semanas a causa de su posible futilidad y gran incertidumbre. A pesar de ello, PwC señala en su informe 'Finanzas & Criptoactivos' que la capitalización de mercado actual de los activos tokenizados en relación a las criptomonedas y las stablecoins aún es pequeña, pero se espera que el impulso de estos activos digitales se acelere rápidamente en los próximos años. Este informe también indica que según algunas estimaciones, los volúmenes podrían alcanzar unos 24 billones de dólares para el año 2027.

EL RETO ESTÁ EN LA ANALÍTICA DE DATOS

Los datos siguen siendo uno de los activos más importantes en cualquier industria que se precie, ya que se han convertido en la clave para que empresas de todos los tipos y de todos los tamaños puedan optimizar sus flujos de trabajo y ofrecer el mejor servicio a sus clientes, aumentando así tanto productividad como beneficio. El crecimiento de esta tecnología es una realidad, como demuestra el informe de Mordor Intelligence 'Big Data Analytics In Banking Market - Growth, Trends, Covid-19 Impact, And Forecasts (2022 - 2027)', donde se apunta que se espera que el mercado de Big Data Analytics en el sector bancario registre una tasa de crecimiento anual del 22,97% durante el periodo 2021-2026. A pesar de ello, según el 'Informe Mundial de la Banca Retail 2022' de Capgemini y Efma, más del 70% de los ejecutivos bancarios indica que los bancos tradicionales carecen de capacidades de datos y análisis. Además, el 95% de los ejecutivos cree que

6 de cada 10 españoles ya habrían sustituido la banca física por la digital

sus actuales sistemas heredados y capacidades tecnológicas están obsoletos, lo que le impide optimizar completamente sus datos para las estrategias de crecimiento centradas en el cliente. Esto significa que aquí es donde está el reto del sector financiero, ya que la banca tradicional debe desarrollar capacidades y estrategias muy focalizadas en los datos para ser capaces así de impulsar la personalización de la experiencia que requiere este nuevo tipo de cliente.

SEGURIDAD EN EL SECTOR BANCARIO

La transformación digital y la introducción de todas estas tecnologías va a suponer todo un reto para la securización del sector financiero, ya que esta digitalización implica un aumento exponencial de la superficie de ataque, con lo que se impondrá un modelo de seguridad en el que el modelo SASE, ZTNA y Zero Trust tomarán todo el protagonismo. Como se ha venido observando en los últimos años, el ransomware va a seguir siendo el gran enemigo también para las entidades bancarias. El informe 'Modern Bank Heists 4.0' de VMware refleja que el 63% de las entidades financieras ha admitido haber experimentado un aumento de ciberataques en el último año. Además, el 74% sufrió al menos un ataque de ransomware. Otro dato preocupante es que el 63% de ellas ha admitido que pagó el rescate para recuperar sus datos. La tensión geopolítica que Rusia está provocando a nivel global sitúa a este país como la mayor preocupación del sector. El artículo 'Ciberseguridad en el sector bancario: nuevos retos' de Funcas va en la misma línea, asegurando que el financiero es el sector que más ciberataques recibe, con cerca del 21% de todos los que se producen en el mundo. Por otro lado, la encuesta 'Digital Trust Survey 2022' de PwC apunta que los ciberataques volverán a registrar en 2022 cifras récord. Esta amenaza se ve reflejada en los presupuestos que están destinando las empresas a protegerse:

El 60% de los servicios financieros ya había integrado menos un proceso basado en inteligencia artificial

el 69% de las compañías a nivel global (el 70% en España), tiene previsto aumentar sus inversiones en ciberseguridad, frente al 55% del año pasado. Además, un 26% espera que este incremento sea del 10% o incluso mayor. Centrándonos de nuevo en el sector bancario, IBM en su estudio 'Cost of a Data Breach Report 2021' asegura que la industria financiera es la segunda que más está gastando en ciberseguridad a nivel global. Esta inversión es claramente necesaria, ya que el coste de sufrir un ataque es ampliamente superior a la inversión realizada para proteger los activos. Es por ello por lo que la concienciación sigue siendo básica no solo para los usuarios, sino también para los altos directivos de las grandes empresas, que en muchos casos todavía necesitan comprender la importancia de esta inversión. ■

Profesionales digitales para una banca digital

La pandemia y la recién estrenada nueva normalidad han traído de la mano esta necesidad de digitalización a pasos agigantados para hacer frente a las nuevas necesidades de la sociedad, que se verán solventadas gracias a estas y otras tecnologías disruptivas que, en mayor o menor medida, van a ser necesarias para que el sector continúe siendo relevante. Pero ninguna revolución se puede llevar a cabo sin las personas, por lo que, a pesar de que el papel protagonista cada vez más recae en la tecnología, sin profesionales capaces de sacar el máximo partido de ella no valdría para nada. **Según la 'Radiografía de las vacantes en el sector tecnológico 2022' de DigitalES**, hay más de 120.000 vacantes tecnológicas sin cubrir en España, sobre todo centradas en tres perfiles fundamentales: desarrolladores de software, técnicos de ciberseguridad e ingenieros de telecomunicaciones. Sin duda es el momento de apostar por una salida profesional cercana al mundo tecnológico, porque todas estas tendencias no irán sino a más en los próximos años.

MÁS INFORMACIÓN

- Funcas: ¿Cómo evoluciona el gasto tecnológico de la banca española?
- Informe de Adaptación Digital 2022 de IEBS
- eBook interactivo 'Top Trends in Banking 2022' Capgemini
- Informe Transición digital y transformación del negocio bancario en España impulsado por la COVID-19, KPMG y FEF
- 'The next normal arrives: Trends that will define 2021—and beyond', McKinsey
- 'Payments 2025 & Beyond', PwC
- Informe Tendencias Digitales 2022 Banca y Seguros, t2ó
- Artículo 'The impact of COVID-19 on artificial intelligence in banking', Bruegel
- Informe El uso de la Inteligencia Artificial en el sector bancario, Asociación Española de Banca
- 'Global AI Survey', McKinsey
- 'Augmented reality (AR), virtual reality (VR), and mixed reality (MR) market size worldwide in 2021 and 2028'. Statista
- Artículo 'El uso de la realidad virtual en el sector bancario', Funcas
- 'Metaverse and Money: Decrypting the Future', Citi
- 'Tech Trends 2022', Deloitte
- Estudio 'Construyendo los servicios financieros del futuro', IDC y OpenText
- Artículo 'Future of Blockchain: How Will It Revolutionize The World In 2022 & Beyond!', The European Business Review
- 'Finanzas & Criptoactivos', PwC
- 'Big Data Analytics In Banking Market - Growth, Trends, Covid-19 Impact, And Forecasts (2022 - 2027)', Mordor Intelligence
- 'Informe Mundial de la Banca Retail 2022', Capgemini y Efma
- 'Modern Bank Heists 4.0', VMware
- 'Digital Trust Survey 2022', PwC
- Artículo 'Ciberseguridad en el sector bancario: nuevos retos', Funcas
- 'Cost of a Data Breach Report 2021', IBM
- 'Radiografía de las vacantes en el sector tecnológico 2022', DigitalES

Síguenos en:

SOLUCIONES DE CIBERSEGURIDAD_

- HSM de Propósito General
- HSM en Cloud
- HSM Financiero
- Remote Key Load
- Soluciones de Cifrado, Firma Digital y Sellado de Tiempo
- Soluciones PKI

Ciberseguridad Blockhain&IoT

www.realsec.com

realsec by utimaco®

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

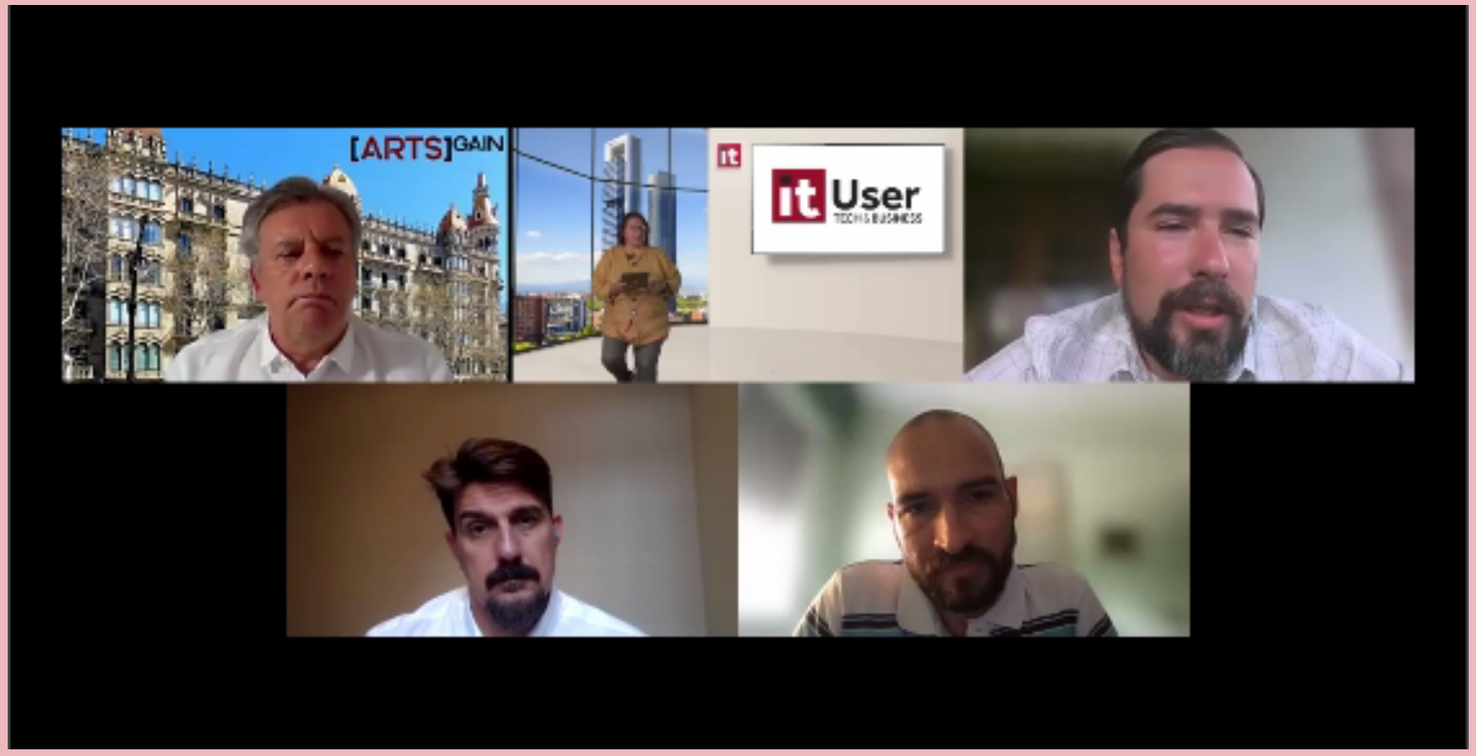
MÉXICO
Av. Jaime Balmes 8 piso M6-A,
Colonia Los Morales, Polanco, Alcaldía
Miguel Hidalgo, C.P 11510, Ciudad de México
Tfno.:+52 (55) 44 35 00 45
E-mail: infomexico@realsec.com

MESA REDONDA IT:

Retos y oportunidades de las Fintech

La digitalización y las nuevas tecnologías como el blockchain han supuesto el caldo de cultivo perfecto para la creación de nuevos modelos de negocio relacionados con el sector bancario, llamados a complementar los servicios que ofrece la banca tradicional. Estas empresas han encontrado tanto retos como oportunidades desde su nacimiento, ya sea en temas de reglamentación, seguridad o usabiidad.

La industria de los servicios financieros atraviesa un momento de cambio sin igual, tanto por la transformación digital que necesitan abordar los players más tradicionales, como por el amplio abanico de posibilidades que han abierto las nuevas tecnologías, y que se están traduciendo en nuevas empresas nativas digitales que desde el principio han colocado al cliente en el centro de sus estrategias. Para analizar cuáles son los retos y oportunidades a los que se enfrentan día a día las Fintech, qué tecnologías son clave para el crecimiento de la industria, el papel de la normativa vigente, qué estrategias de ciberseguridad llevan a cabo y cómo se relacionan con la banca tradicional, hemos contado en esta Mesa Redonda IT con la participación de Xavier Olivella, director general de ArtsGain Investments; Chema Prieto, director de innovación de Tutellus; Luis Eduardo Imbernón, CTO de Hipoo; y Víctor Tuson, CTO de Ebury.



MESA REDONDA IT: Retos y oportunidades de las Fintech

"El inversor teóricamente se siente mucho más seguro cuanto más normativas hay. Pero a la vez, esto hace que las gestoras tengan que ofrecer más capas de control, que está bien, pero a la vez hace que los costes de implantación sean más altos"

XAVIER OLIVELLA, DIRECTOR GENERAL DE ARTSGAIN INVESTMENTS

RETOS DE LAS FINTECH DESDE EL PUNTO DE VISTA TECNOLÓGICO

Como cualquier empresa, y más en un sector tan controlado como es el de los servicios financieros, las Fintech están encontrando ciertos retos a la hora de ofrecer sus servicios. Para Xavier Olivella, estos retos se engloban en tres grandes áreas. "Una es el cliente, porque es lo primero, sin clientes no haces nada, y para ello hemos utilizado bases de datos relacionales, de forma que podemos no solo captar cliente sino también tener la visión 360º de cada uno de ellos. El segundo, que es muy importante para empresas reguladas como la nuestra, es el poder hacer el onboarding del cliente de forma semiautomatizada, para cumplir con la normativa vigente y toda la parte de informes trimestrales y semestrales que hay que enviarle a la CNMV. La tercera es la gestión de los activos".

En el caso de Tutellus, Chema Prieto señala que, aunque han encontrado retos tecnológicos o en la regulación, los grandes caballos de batalla están en la adopción y la usabilidad. "Al final los retos más importantes que estamos encontrando es más temas de adopción. Vemos que el mundo cripto es algo completamente nuevo, toca temas que no son los habituales, porque es una economía descentralizada, con lo cual cambias el enfoque y eso requiere de un tiempo de adopción. Y también de usabilidad, el mundo cripto es algo muy nuevo y todavía no tienes los interfaces diseñados para el usuario medio, está diseñado para un tipo de usuario bastante avanzado, que se mete en el mundo cripto porque busca una rentabilidad importante, pero que tiene que luchar con esas barreras de usabilidad".

Luis Eduardo Imbernón resume la cuestión en tres retos principales a los que han tenido que enfrentarse en los últimos años. "El primero es la digitalización de los bancos. Es un sector tecnológicamente lento, que parece que siempre va por detrás del resto de sectores, por un tema de seguridad, de tecnología...". El segundo reto que comenta es el de la seguridad. "Hay que tener muy en cuenta que trabajamos con datos muy sensibles, datos financieros, datos económicos de personas. El tema del robo de datos está a la orden del día". Por último, el portavoz habla de conseguir la confianza de las personas. "Los bancos, y más los préstamos hipotecarios, siempre han producido mucho recelo en las personas, entonces conseguir demostrar a estas personas que Hipoo es un intermediario neutral, transparente, y que lo único que buscamos es aliarnos con ellos para acompañarles a tomar la decisión financiera tal vez más importante de su vida, es muy complicado".

CRECE LA INVERSIÓN EN TECNOLOGÍA DEL SECTOR BANCARIO

Según Funcas, la inversión en tecnología en el sector bancario se ha incrementado en más de un

60% entre 2015 y 2020. Pero, ¿este crecimiento va a continuar? Como indica Chema Prieto, "Sí que vemos un interés muy grande por parte de grandes bancos por lo que es el mundo cripto, porque ya no solamente hablamos de tecnología, es un cambio de paradigma en el cual los bancos también quieren estar y yo creo que juegan un rol muy importante. El camino de la confianza en gran parte lo tienen los bancos ya construido y creo que son conscientes que cuando la regulación que está a punto de aterrizar a nivel europeo tome ya forma y sea mucho más concreto lo que le piden a los actores que utilicen el mundo cripto, creo que van a entrar en las tecnologías cripto de una manera mucho más profunda".

El crecimiento de este tipo de inversiones está asegurado para Luis Eduardo Imbernón. "Las empresas digitales estamos sirviendo como palanca para que los bancos fomenten la inversión y la digitalización de los procesos y les estamos empujando hacia un nuevo sistema que realmente es mucho más rentable para todas las partes, para las entidades bancarias, intermediarios como puede ser Hipoo y sobre todo para los clientes. Esto lo están viendo los bancos. El crecimiento a medio plazo no solamente va a continuar, sino que todo apunta a que se va a ver incrementado y principalmente yo hablaría de áreas como ciberseguridad, inteligencia artificial, medios de pago y préstamos hipotecarios".

Por su parte, Víctor Tuson comenta que "los bancos están reconociendo que tienen como organizaciones unos impedimentos para innovar. Estoy viendo mucha adquisición de talento en empresas y soluciones. Inversiones como Ebury o en otras fintechs, es una cosa que se está desarrollando más, sobre todo ahora". El portavoz señala que estas inversiones no se están realizando únicamente a nivel interno, sino que también están adquiriendo compañías que les van a permitir ir más rápido a la hora de abordar ciertos servicios por temas de regulación. "Los bancos, como tienen que ofrecer servicios de todo para fidelizar a los clientes, les cuesta ir rápido por regulaciones que luego tienen que seguir. Es mejor a veces poder especializar una compañía en una solución y hacerte especialista en una solución digital, que como banco intentar abarcar todas estas cosas".

UNA EXPERIENCIA DE USUARIO ADAPTADA A LOS NUEVOS CLIENTES

El cliente está cambiando, ahora exige una experiencia mucho más personalizada, los millenials cada vez se convierten más en el grueso de ese cliente que solicita todo este abanico de servicios financieros. Por todo ello, ofrecer una buena experiencia de usuario se ha vuelto fundamental.

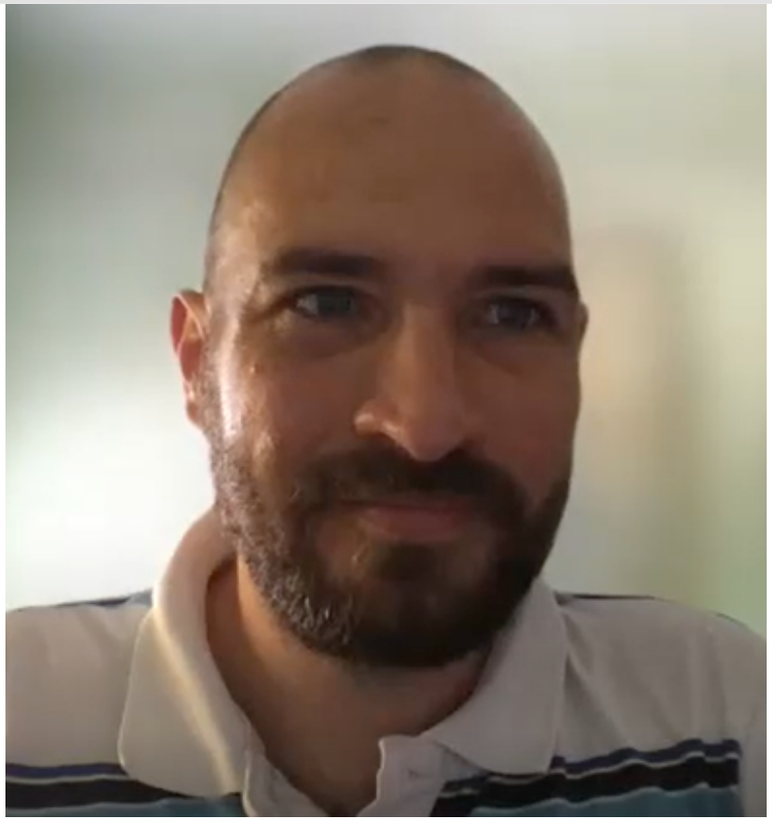
"En el caso del sector hipotecario, uno de los problemas que de forma más tradicional u online se enfrentan las personas que quieren solicitar hipotecas es el de la desconfianza. Es una barrera muy grande", señala Luis Eduardo Imbernón. Para superar este reto, el portavoz señala cuatro tecnologías que son básicas: "Tenemos por un lado la tecnología móvil. El 80% de nuestros clientes hacen uso de su móvil para acceder a nuestra

"El tema de ciberseguridad viene de serie en el mundo blockchain, porque de alguna manera externalizas esa seguridad en la red que elijas. Esa es la ventaja que te da la blockchain"

CHEMA PRIETO,
DIRECTOR DE INNOVACIÓN DE TUTELLUS

plataforma. Adaptar todo el front end, toda la experiencia de usuario a la tecnología móvil y que sea adaptativa a cualquier dispositivo, sea tablet, móvil, con distintos formatos y demás, es vital, porque está demostrado que si la experiencia de usuario en el móvil es mala, se te pueden caer las operaciones. Por otro lado, entran en juego las interfaces de comunicación vía API que permiten agilizar los tiempos de la transferencia de datos entre los bancos, los intermediadores y demás. El tercer punto clave es la inteligencia artificial. Estamos ahora mismo en un boom y está claro que nos va a permitir adaptar de forma predictiva los productos a los contextos de nuestros clientes". Por último, señala el tener un buen diseño del producto que facilite los procesos, "aunque no se trata ya de una tecnología, pero es una de las partes más olvidadas y que más efecto tiene sobre la experiencia de las personas".

Para Víctor Tuson, lo que va a transformar para bien la experiencia del usuario es el open banking. "Lo que lo que va a hacer más impacto a la experiencia de usuario es la capacidad del usuario de abrirte sus datos para ti. Los datos no son del banco, obviamente si esta persona tiene una hipoteca con un banco puede compartir esos datos, esa información y esa seguridad. La experiencia de usuario es mucho más sencilla porque ya tienes esta información". Además, menciona otra tecnología de la que se está hablando cada vez más en los últimos años: el blockchain. "Si se añade encima de una cadena distribuida pero también pública, que pueda ser revisada qué cambios se están haciendo, que añada encima de este conocimiento digital que comparten desde las distintas instituciones financieras, puede también hacer que las transferencias sean mucho más seguras, que el tiempo que tardan en darte una hipoteca o una transferencia de pagos o un fondo de inversión sea más corto, y mejorar mucho la experiencia del usuario".



"Las empresas digitales estamos sirviendo como palanca para que los bancos fomenten la inversión y la digitalización de los procesos, y les estamos empujando hacia un nuevo sistema que realmente es mucho más rentable para todas las partes"

LUIS EDUARDO IMBERNÓN, CTO DE HIPOO

De la misma forma opina Xavier Olivella, poniendo el foco en el blockchain y el Big Data: "Para nosotros blockchain es la principal por dos cosas: una, por favorecer los contratos inteligentes, y eso da una facilidad de uso para el usuario y una reducción de costes para las gestoras, y para la tokenización de las acciones, para ofrecer liquidez al inversor y que pueda vender o comprar cuando quiera. El segundo es el Big Data. Seguramente las entidades financieras hasta hace muy poco no ponían al cliente en el centro de donde tiene que estar. Desde el momento que existen las gestoras o servicios digitales como los que hay aquí hoy, han tenido que poner al cliente en el centro y eso hace que el Big Data sea ideal para poder saber cómo se comporta tu cliente".

¿CÓMO SE AFRONTA TANTA NORMATIVA?

Víctor Tuson lo tiene claro, en su opinión las normativas están ahí por muy buenas razones. Pero para cumplirla es necesario apoyarse en la tecno-

logía: “Es casi imposible cumplir con la normativa y garantizar la seguridad sin tecnología. Es más una necesidad. El problema es si estás preparado como organización en dar ese paso y sobre todo en encontrar partners adecuados”. Para Xavier Olivella, se trata de dos caras de la misma moneda. “El inversor teóricamente se siente mucho más seguro cuanto más normativas hay. Pero a la vez, esto hace que las gestoras tengan que ofrecer más capas de control, que está bien, pero a la vez hace que los costes de implantación sean más altos. Por mucho que haya una normativa e incluso la automatices, eso incrementa tu coste”.

Por su parte, Chema Prieto hace hincapié en el diseño de esas regulaciones. “Las regulaciones tienen que estar muy bien diseñadas. Cuando es una tecnología nueva, muchas veces la regulación no es capaz de estar a la última, y siempre van a cometer errores. No son rápidas a la hora de corregir esos errores, con lo cual suponen a veces un lastre. Es verdad que si hay una regulación al menos tienes algo a lo que atenerte y va a permitir que grandes entidades que están muy reguladas como los bancos puedan entrar en juego y tengan de alguna manera su rol, y que también al inversor final le puedan dar esa seguridad si la está buscando”.

EL RETO DE LA SEGURIDAD

“Nosotros utilizamos la normativa europea de doble control cuando accedes a la base de datos o a la aplicación y las herramientas que te dan las aplicaciones cloud que utilizas o que hayas podido implementar”, comenta Xavier Olivella, que añade: “Establecer una estrategia de ciberseguridad en serio solo lo afrontan los grandes, porque tienen capacidad económica y recursos de IT. En nuestro caso, la mayor parte de recursos de IT son externalizados. También es cierto que nosotros no vamos al retail, con lo cual todas las transferencias bancarias, etc, no van a través de nuestra plataforma, con lo cual se simplifica ese problema”.

Para Chema Prieto “el tema de ciberseguridad viene de serie en el mundo blockchain, porque de alguna manera externalizas esa seguridad en la red que elijas, es esa ventaja que te da la blockchain”. A pesar de ello incide en que “por supuesto tienes que diseñar bien los contratos inteligentes para que no sean manipulables. No es que alguien se los vaya a cargar, porque están en la red, pero sí que tienes que asegurar que alguien no se pueda aprovechar de un protocolo que está implementado en la red y que tenga formas de sacarle provecho como no estaba previsto o no estaba diseñado”. ■

“Es casi imposible cumplir con la normativa y garantizar la seguridad sin tecnología. Es más una necesidad. El problema es si estás preparado como organización en dar ese paso y, sobre todo, en encontrar partners adecuados”

VÍCTOR TUSON, CTO DE EBURY

MESA REDONDA IT:

Digitalización y Seguridad, motor de innovación financiero

Las entidades financieras llevan años invirtiendo recursos para que los usuarios digitales puedan operar con los más altos estándares de seguridad y de esta forma garantizar que sus transacciones en línea sean tan confiables como las que pudieran realizar a través de una sucursal.

La seguridad es uno de los aspectos más importantes que entran en juego a la hora de hablar del sector bancario. En los últimos años esta industria ha realizado una clara apuesta por la digitalización, siendo una de las que mejor se está adaptando a los nuevos tiempos. Esta carrera tecnológica lleva implícita la seguridad de los servicios, sobre todo porque se trata de uno de los sectores más atacados por la ciberdelincuencia. Para analizar cuáles son los retos

MESA REDONDA IT:
Digitalización y Seguridad, motor de innovación financiero

“El sector financiero es el sector que encabeza el número de ciberataques, es uno de los objetivos claros de las organizaciones que quieren atacarnos”

ELENA GARCÍA-MASCARAQUE, DIRECTORA DE MSSP DE WATCHGUARD

y oportunidades del sector bancario, qué tecnologías están liderando su transformación digital, cómo puede afectar a la experiencia del cliente y qué papel juega la normativa, hemos contado en esta Mesa Redonda IT con la participación de Elena García-Mascaraque, directora de MSSP de WatchGuard; Daniel Rodríguez, director general de Redtrust; Pablo Juan Mejía, director de Realsec by Utimaco para España; Daniel Howe, senior sales engineer de Fastly; Carlos Tortosa, responsable de grandes cuentas de ESET; y Álvaro Fernández, sales manager Iberia de Sophos.

DESAFÍOS DEL SECTOR BANCARIO

La digitalización está trayendo nuevos retos a los que el sector bancario debe enfrentarse. Como indica Pablo Juan Mejía, “el Covid aceleró sin lugar a dudas estos procesos, ahora los bancos se están enfrentando al manejo de datos que anteriormente no tenían de los usuarios, o no tan de la manera como la manera de la que lo hacen hoy en día”. Por ejemplo, el portavoz habla de los datos biométricos: “el tema de la digitalización y el manejo de estos datos biométricos es algo a lo que hoy en día se están enfrentando, y para lo cual solamente necesitan los métodos adecuados para poder manejarlos y garantizar la seguridad a los usuarios. En una encuesta reciente hecha en julio de este año por Utimaco, el 89% de los españoles está preocupado por su seguridad, por la seguridad precisamente de sus datos. No es un tema menor, dado que el 21% de los ciberataques que se realizan están orientados justamente al sector bancario. Dentro de estos retos de la digitalización, sin lugar a dudas la seguridad es uno de los principales a los que se está enfrentando la banca”.

“Nosotros hacemos una encuesta todos los años y entrevistamos a cerca de 6000 empresas y de múltiples sectores, de los cuales hay 500 que son del sector financiero”, señala Álvaro Fernández. “Lo que nos comentan es que los ciberataques se están incrementando, en concreto desde el año pasado en un 55%”. Además de este aumento de ataques, también se puede observar que cada vez son más complejos, como señala el 60% de los encuestados en dicho estudio. “El sector bancario es un sector en IT bastante maduro. En ciberseguridad también es bastante maduro y obliga a los atacantes a ser mucho más elegantes o mucho más sofisticados a la hora de atacar. Luego también lo que nos transmiten es que una vez que sufren el ciberataque, el impacto que tienen es mayor al de otros años. Principalmente los retos que vemos a los que se están enfrentando es el aumento de los ataques, esa mayor sofisticación de los mismos y minimizar el impacto que estos tienen”.

Para Elena García-Mascaraque, “el sector financiero es el sector que encabeza el número de ciberataques, es uno de los objetivos claros de las organizaciones que quieren atacarnos. Vemos además que solamente en ransomware, durante el primer trimestre ya se ha duplicado el número

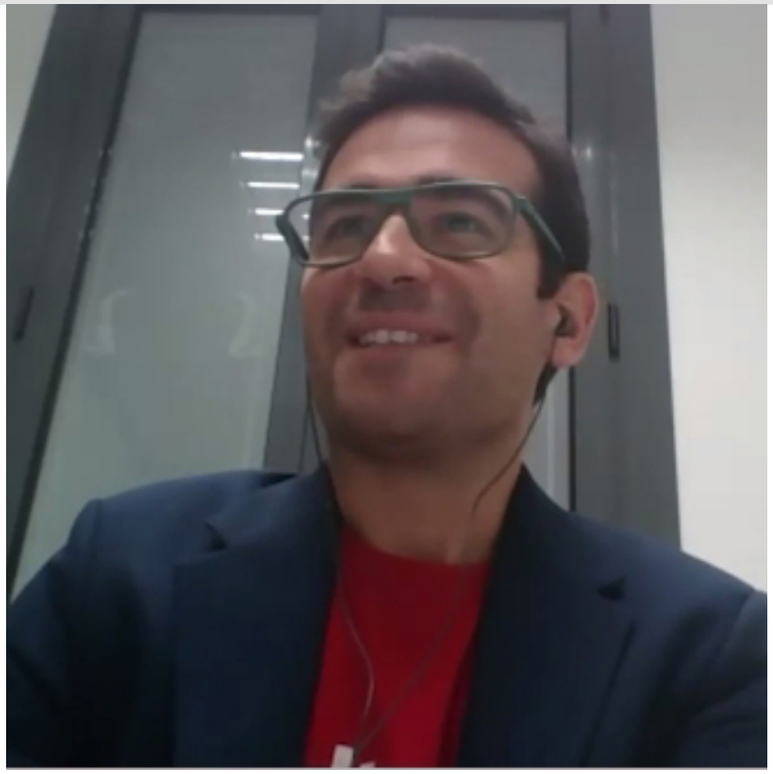
de ataques con respecto al total del año pasado, es una tendencia absolutamente fehaciente que está ocurriendo. Las entidades tradicionales financieras con el entorno regulatorio están muy preocupadas, están poniendo mucho foco en la seguridad, pero al mismo tiempo no nos olvidemos que hay una cadena de suministro bastante extensa. De hecho lo que evidenciamos es que el 87% de las empresas de finanzas y de instituciones financieras no solamente están preocupadas por su propia seguridad, sino por la de todos los proveedores o colaboradores de servicios que están accediendo también a esta información". Elena también subraya la complejidad de los nuevos ataques: "esta sofisticación hace que los ciberataques tengan una duración muy extensa, no estamos hablando de duración de días ni de semanas, el atacante puede estar en la empresa durante una media de 200 días, con lo cual tenemos que sofisticar también nuestros sistemas de investigación ante estos ataques".

TECNOLOGÍAS PARA SECURIZAR LA NUEVA BANCA DIGITAL

Para incluir la tan necesaria capa de seguridad a toda esta digitalización, el sector financiero ha tenido que apoyarse en una serie de nuevas tecnologías, aunque para Álvaro Fernández, más bien está adoptando "arquitecturas como SASE, para tener el perímetro controlado de otra forma, entendiendo que el perímetro ya ha desaparecido". "Vemos que para esa transformación, la seguri-

"Lo que a la banca, o en general, a todas las empresas les interesa saber es que la persona que está detrás de esa pantalla o dispositivo es quien dice ser"

DANIEL RODRÍGUEZ, DIRECTOR GENERAL DE REDTRUST



"Dentro de estos retos de la digitalización, sin lugar a dudas la seguridad es uno de los principales a los que se está enfrentando la banca"

PABLO JUAN MEJÍA, DIRECTOR DE REALSEC BY UTIMACO PARA ESPAÑA

dad es un habilitador, se apoyan en la seguridad para poder habilitar esa transformación. Lo que vemos que es un cambio de paradigma importante es toda la parte de detección y de respuesta. Los bancos es un sector con un componente de madurez bastante alto y además es un sector que tradicionalmente se ha hecho él mismo las cosas, es decir, han comprado diferentes productos de seguridad, los administran ellos, los gestionan ellos y luego son capaces también muchos de ellos de crear su propio SOC, atenderlo con su personal interno e ir mejorando esa seguridad conforme vayan viendo esos casos de uso", añade, y vuelve a la idea que transmitía antes sobre el crecimiento del número y de la complejidad de los ciberataques: "Ese aumento de los ataques, esa sofisticación de los mismos, lo que hace es que obliga a los bancos a ir más allá con la detección y la respuesta. Ya no hablamos solo de EDR, sino de la detección y respuesta expandida, es decir, de XDR".

De la misma forma se expresa Carlos Tortosa cuando indica que "generalmente la banca, con esa digitalización, son precisamente entidades que están al día prácticamente de cualquier información que podamos generar no únicamente nosotros, sino cualquier otro tipo de proveedores de servicios. Tiene muy claro qué necesidades tiene, hablamos de XDR, de MDR o de cualquier otra tecnología que puedan aplicar. Están generando su propio SOC o sus propios nodos de servicios para poder mantener todas estas herramientas

"Ojalá hubiera más normativa para otros sectores. Probablemente sufriríamos menos en cuanto a robo de datos y demás"

DANIEL HOWE, SENIOR SALES ENGINEER DE FASTLY

que incorporan, que son muchas y muy diversas, mantenerlas actualizadas y que realmente puedan cubrir todas sus necesidades". Después hace foco en la identificación del usuario: "cualquier usuario puede acceder desde cualquier parte, necesitamos identificar a ese usuario cuando accede y para eso se están fijando diferentes tecnologías. Los bancos en este caso están invirtiendo para poder tener claro quién accede a qué información".

También se refiere a la identidad Daniel Rodríguez, señalando que "uno de los factores más importantes es el multifactor o esa gestión de la identidad. Lo que a la banca o en general a todas las empresas les interesa saber, es la persona que está detrás de esa pantalla o dispositivo, que es quien realmente dice ser. Al final, eso libera de muchas más problemáticas futuras a la banca o a cualquier otra empresa. Tienen que adoptar aquellas tecnologías que a la vez le faciliten el uso al cliente final o incluso a los empleados. La evolución y la transformación digital de las entidades financieras tiene que ir enfocada en ese sentido".

SEGURIDAD VS. EXPERIENCIA DE USUARIO

La experiencia de cliente es, sin lugar a dudas, una de las máximas del sector bancario. ¿Cuáles son las directrices que las entidades financieras deben seguir para satisfacer las demandas de sus clientes? ¿Qué tecnologías son clave para mejorar la experiencia del cliente?

Para Elena García-Mascaraque "esta experiencia de usuario tiene que ser tanto interna como externa. Cómo combinar esa seguridad con que el usuario no rechace la seguridad y por lo tanto, no lo use". La portavoz subraya la importancia de contar con una tecnología robusta y una cultura de seguridad muy embebida

“Cualquier usuario puede acceder desde cualquier parte. Necesitamos identificar a ese usuario cuando accede y para eso se están fijando diferentes tecnologías”

CARLOS TORTOSA, RESPONSABLE DE GRANDES CUENTAS DE ESET

dentro de las organizaciones. “Cada vez somos mucho más conscientes de que la seguridad es una responsabilidad de todos, no solamente de los departamentos de sistemas, los departamentos de seguridad, sino también de los empleados y de los clientes. Afortunadamente, estos últimos años, donde el sector financiero se ha visto abocado a la digitalización por diseño, porque todos hemos tenido que hacer uso de herramientas tanto profesionalmente como personalmente, nos ha ayudado y nos ha acelerado”. Además, señala que “la seguridad debe ser parte de esos proyectos ágiles de diseño de aplicaciones, la seguridad debe estar integrada en el proceso de DevOps y la seguridad por diseño en estas nuevas aplicaciones debe ser un nuevo estándar más aparte de la usabilidad, de la escalabilidad, de la apertura hacia nuevas aplicaciones”.

“El equilibrio entre esa usabilidad y la tecnología es complejo”, señala Daniel Rodríguez. “Cuando hablamos con los departamentos de IT y de seguridad, lo que siempre nos dicen es sea lo que sea, que al usuario no haya que tocarle nada, que no tenga que cambiar su manera de hacer, porque puede ser un desastre. Ese es el mayor reto”. Además, subraya que a la hora de vender seguridad “es mejor siempre ir por el lado de la usabilidad, de la disponibilidad, de la facilidad de uso y venderle seguridad sin querer, porque al final nos beneficia a todos. Esa dualidad y ese equilibrio tiene que venir por las dos partes, tanto por la parte del proveedor que le va a dar ese servicio, como por parte de la empresa, que va a poner todo su empeño y todo su esfuerzo en formar internamente a sus empleados. También tener la responsabilidad de formar a sus propios clientes, porque muchas veces el cliente simplemente es el actor pasivo y es ahora cuando más tiene que ser activo y ver que puede estar en riesgo su seguridad, su información, su dinero, si no atiende a unas especificaciones mínimas de seguridad. Esa pedagogía que se ejerce muchas veces a nivel interno para cumplir normativas y compliance con todas las ISOs y todo lo que haga falta, también tiene que trasladarse al cliente final”.

Por su parte, Daniel Howe recalca que “el negocio banca es un negocio completamente electrónico. Son pioneros en muchas de las tecnologías, lo han sido tecnológicamente siempre, han sido capaces de adaptarse incluso cumpliendo con toda la normativa compleja que tienen, que tienen que exigir a sus colaboradores y a sus proveedores para garantizar con todo lo que se espera”. El portavoz señala que al hablar de usabilidad, “no es algo a lo que la banca tradicionalmente se haya dedicado, que es el esfuerzo a todo lo que es el UX, a todo lo que es la usabilidad de la plataforma. Todo eso ha hecho que empecemos a ver muchas veces situaciones o preocupaciones del sector bancario casi como si estuviéramos hablando de un ecommerce”. En este sentido comenta que “hay veces que es cierto que tienes conversaciones con empresas financieras y el tratamiento que les estamos dando, les estamos hablando como si fuera un portal de venta online.

Es mucho el negocio que ellos saben que tienen y tienen que ponerse a la altura de otros que están apareciendo en el mercado, que no son bancos per se, pero que realmente están empujando mucho y que pueden llegar a coger parte de su negocio".

> "Ese aumento de los ataques, y su sofisticación obliga a los bancos a ir más allá con la detección y la respuesta"
>
> ÁLVARO FERNÁNDEZ, SALES MANAGER IBERIA DE SOPHOS

UNA REGULACIÓN ROBUSTA ES MUY BIENVENIDA

Carlos Tortosa lo tiene claro, "la regulación en el sector bancario es precisamente la más robusta que podamos tener. Hay que tener en cuenta que estamos hablando tanto de una cantidad de dinero importante la que manejan los bancos, como de una exposición clara en el caso de los datos personales de cada uno de los usuarios. Partiendo de esa premisa de que en mi opinión, la regulación es la adecuada y que tiene que ser lo más robusta posible, por la parte de los bancos hay una gran parte de ellos que están yendo, ya no digo por delante de la regulación, pero sí implicándose al 100% en la misma. No se esperan a que la regulación les obligue a tomar ciertas medidas o incorporar ciertas soluciones, porque ellos ya per se lo están haciendo también. Por ejemplo, la generación de sus propios SOC o de sus propios servicios internos para protección de los datos ya nos hace pensar que su inquietud va muchas veces por encima de esta regulación".

De igual forma piensa Daniel Howe: "La normativa es buena y bienvenida sea. De hecho, ojalá hubiera más normativa para otros sectores, probablemente sufriríamos menos en cuanto a robo de datos y demás. Sí que es cierto que lo que esto hace es acompañar a todos los proveedores de la banca a estar en el mismo cajón de compliance, de PCIs y demás". Por otro lado, el portavoz hace referencia al reto que plantean los passwords: "empieza a ser muy problemático todo el compartimiento de passwords y demás. Ahí tenemos un reto importante, yo creo que la banca será un poco el que evolucione todo el tema de las credenciales, los accesos, si acabamos llegando a un mundo en el que no tengamos esas passwords malditas... Todo ese tema de la evolución o el multifactor, que también hemos visto que no es la solución porque se pueden hackear, todo eso que la banca siempre ha estado por delante, seguirá innovando y avanzando".

Para finalizar, en opinión de Pablo Juan Mejía, "la regulación puede ser o restrictiva o promotora del cambio o de la innovación. Estamos en un momento de inflexión, donde hoy tenemos ciertas regulaciones que son necesarias para el momento en el que estamos y la futura innovación que vendrá en los siguientes años. Dentro de este punto de inflexión, es un buen momento para que futuras regulaciones que surjan justamente promuevan esta innovación". "Confío en que todas las regulaciones estarán promoviendo esta innovación y la adopción de estas nuevas tecnologías", añade. ■

Controla los certificados digitales para una identidad digital segura en entidades **bancarias y financieras**

Controla y gestiona permisos de uso

Firma digitalmente documentos

Usa los certificados en cualquier lugar

Cumple con la normativa del sector

Descubre más sobre nuestra solución en
redtrust.com/sectores/banca-fintech

redtrust
a **KEYFACTOR** company

FERNANDO RODRÍGUEZ FERRER, STRATEGY, BUSINESS DEVELOPMENT & INNOVATION DIRECTOR DE BIZUM

“Nuestro objetivo es digitalizar cada vez más a los usuarios bancarios”

La digitalización en el sector financiero ha traído una apuesta clara por que el móvil sea el centro de toda relación que tiene el cliente con su banco. Esto implica ciertos retos a los que hay que plantar cara, ya sea en cuanto al acceso de toda la población, a nivel regulatorio o a la hora de hablar de la seguridad de las transacciones y los datos.

Como señala Fernando Rodríguez Ferrer, strategy, business development & innovation director de Bizum, no todo el mundo está preparado para afrontar este cambio digital de la misma forma y hay entidades que se están preparando para proporcionar un acceso bancario móvil más sencillo a clientes que quizás no están tan acostumbrados a trabajar en un entorno digital. Tecnologías como el machine learning o la inteligencia artificial ayudan a proporcionar una experiencia mucho más personalizada.

Bizum ha llegado para ayudar a la banca a incentivar cada vez más la digitalización de sus usuarios apostando por la omnicanalidad. Los pagos inmediatos entraron en España gracias a Bizum y es un mercado clave, como demuestra que casi la mitad de los pagos inmediatos de 2021 fueron españoles. Además, apuesta por la educación y la concienciación de los usuarios para mejorar la seguridad del sector, además de contar con restricciones en las cantidades que se pueden transferir para minimizar los daños en caso de phishing o smishing.

> Tecnologías como el machine learning o la inteligencia artificial ayudan a proporcionar una experiencia mucho más personalizada

Servicios de logística y bancos: los ganchos favoritos del smishing

JOSEP ALBORS,
director de Investigación y Concienciación de ESET España

Tras varios meses observando y analizando desde ESET España numerosas campañas de phishing enviado a través de mensajes SMS (también conocido como smishing), podríamos pensar que los delincuentes han evolucionado sus tácticas para tratar de conseguir nuevas víctimas. Sin embargo, tal y como vamos a comprobar en este artículo, vemos como los ganchos más utilizados siguen siendo los mismos que ya hemos visto desde hace tiempo.

LA BANCA ONLINE SIEMPRE ATRAE LA ATENCIÓN

Con un uso de la banca online bastante elevado por parte de los usuarios, no es de extrañar que los delincuentes suplanten constantemente a algunas de las entidades bancarias más conocidas para tratar de robar nuestros datos. Además de los clásicos correos de phishing bancario, el envío de mensajes SMS a nuestros teléfonos móviles también se ha convertido en algo habitual

Además, es bastante frecuente que los delincuentes detrás de estas campañas utilicen enlaces acortados para que los usuarios no sepan a dónde los redirigen, incluso a pesar de que se utilicen direcciones similares a las reales o que, aparentemente, tienen relación con la entidad bancaria suplantada.

PAQUETES PENDIENTES DE ENTREGA

Otra de las técnicas que ha tenido mucho éxito a la hora de conseguir nuevas víctimas desde hace unos años es la que se hace pasar por una empresa de logística y nos indica que tenemos un paquete pendiente de entrega. Con el aumento del comercio online que provocaron las restricciones impuestas para tratar de contener la pandemia, es bastante probable que varias de las personas que reciban este mensaje SMS estén realmente esperando un paquete, por lo que las probabilidades de que pulsen sobre el enlace aumentan.

PREPARACIÓN Y DURACIÓN DE CAMPAÑAS

Por experiencia, sabemos que este tipo de campañas no suelen durar muchos días antes de que sean eliminadas, pero esto no evita que los delincuentes traten de sacar el mayor provecho de ellas. Un buen ejemplo es que desde hace años se toman la molestia de conseguir certificados para sus webs fraudulentas, de forma que estas aparezcan con el candado de seguridad y el uso del protocolo HTTPS, que muchos usuarios aún piensan que significa que la web es segura cuando lo único que indican es que las comunicaciones entre nuestro dispositivo y esa web se realizan de forma cifrada.

Podríamos pensar que los delincuentes han evolucionado sus tácticas para tratar de conseguir nuevas víctimas, pero vemos cómo los ganchos más utilizados siguen siendo los mismos que ya hemos visto desde hace tiempo

CONCLUSIÓN

Con la elevada cantidad de webs fraudulentas que se utilizan actualmente en campañas de phishing, siempre es mejor acudir a la web oficial del banco o empresa que, supuestamente, nos envía un SMS para avisarnos de un problema en lugar de pulsar sobre el enlace proporcionado. ■

CARLOS TORTOSA, DIRECTOR DE GRANDES CUENTAS DE ESET

"Los principales ataques tienen al usuario como objetivo"

El sector financiero cuenta con una gran exposición ante posibles ataques de seguridad, además de manejar no solo información confidencial de sus clientes, sino también su dinero. Los retos son claros, por una parte se deben tomar las medidas de seguridad necesarias para proteger un entorno corporativo, pero añadiendo la protección del acceso del usuario que utiliza servicios.

En palabras de Carlos Tortosa, Director de Grandes Cuentas de ESET, los principales ataques tienen al usuario como objetivo, a través de grandes campañas de phishing que además suponen un problema para la reputación de la marca. Además, a nivel corporativo el ransomware sigue siendo el principal riesgo, como demuestra que un 74% de las entidades bancarias ha recibido algún ataque de este tipo, por encima de la media en España.

Estos ataques son similares a los que están recibiendo las Fintech, esos players que han entrado en el sector y que realmente son nativos digitales, por ello la manera de protegerse ante ellos es muy parecida en ambos casos. Para lograr evitar estos ataques, las entidades bancarias están apostando por la concienciación y la formación de sus usuarios, a pesar de la heterogeneidad de sus clientes objetivo, tanto en edad como en conocimientos tecnológicos.

DANIEL HOWE, SENIOR SALES ENGINEER DE FASTLY

“El sector financiero tiene el foco en la seguridad de su plataforma digital”

El sector financiero es consciente de que está evolucionando y que en el futuro la gran mayoría de sus clientes van a ser nativos digitales, que accederán a sus servicios o bien a través de su app, o de su web. Es por ello que el foco está puesto en garantizar la seguridad de estas plataformas. Asimismo, la banca necesita garantizar también que sus proveedores también estén completamente regulados.

Para Daniel Howe, Senior Sales Engineer de Fastly, el problema principal que tiene la banca es que han aparecido nuevos players en el mercado que realizan muchísimas transacciones en ecommerce. De hecho, hay bancos que están convirtiéndose un poco en ecommerces, lo que hace que estén poniendo mucho foco en la usabilidad.

A través de su plataforma Edge, Fastly ofrece una mayor potencia de computación en la nube, por encima incluso de la propia infraestructura que pueda tener cualquiera de los grandes proveedores de cloud o cualquiera de las infraestructuras propias del banco, haciendo que todas las operaciones sean mucho más ágiles. Además, gracias a su plataforma de Next Generation WAF, son capaces de ofrecer una gran visibilidad del tráfico que reciben los bancos, ayudándoles a mitigar riesgos, teniendo en cuenta que más del 50% del tráfico que se produce en Internet es tráfico generado por bots.

> La banca necesita garantizar también que sus proveedores también estén completamente regulados

PKI:
un paso más para la ciberseguridad de la banca

PABLO JUAN MEJÍA,
Country Manager de Realsec by Utimaco en España y México

Parte del éxito de la banca digital reside en la implementación de robustas soluciones de seguridad que protejan, en todo momento, los pagos y las transacciones.

Desde Realsec by Utimaco, hemos hablado sobre cómo el cifrado proporcionado por un HSM o módulo hardware de seguridad es el mejor aliado para la protección de los datos del cliente en estos procesos.

En esta ocasión, vamos a tratar por qué una PKI (PKI, Public Key Infrastructure o Infraestructura de Clave Pública) es esencial para sumar un plus de confianza en los intercambios de información en una sociedad cada vez más digital y en la que la banca está muy presente; al tiempo que proporciona certeza a la identidad digital sin comprometer los datos de sus clientes, empleados, servidores, sistemas internos, así como para la implementación de certificados de dispositivo desplegados para cajeros automáticos, entre otros.

A su vez, todos estos públicos del banco tienen la seguridad de que es el banco y no un suplantador quien se comunica y comparte información con ellos, puesto que los sistemas del banco (y opcionalmente también los usuarios) disponen de certificados electrónicos y de las correspondientes claves privadas, con lo que el banco refuerza la confianza en las comunicaciones y transacciones de datos en los medios digitales tanto con sus clientes como en sus propios sistemas.

Con la implementación de una estructura de tecnología de clave pública estamos reforzando el acceso seguro, la integridad y autenticidad de los datos a la vez que podemos verificar a gran escala la identidad digital de personas, sistemas y dispositivos y, por lo tanto, estamos creando entornos más confiables para las firmas digitales y transacciones electrónicas.

¿DE QUÉ SE COMPONE UNA PKI?

La PKI se conforma como una arquitectura de seguridad basada en software y hardware que proporciona identificación y autenticación seguras, confidencialidad, no repudio e integridad de los datos. Sobre esto además puede leer el siguiente post de nuestro blog: ¿Qué es una PKI y para qué sirve?

Aunque la PKI es escalable y podemos adaptarla según los servicios requeridos, es importante destacar que una PKI básica se compone típicamente de una CA o Autoridad de Certificación y una Autoridad de Registro o RA. La CA es el elemento principal, cuyos roles son Autoridad de Certificación Raíz y la Autoridad de Certificación Subordinada. Su misión consiste en generar los Certificados Digitales.

La Autoridad de Registro es el punto de acceso de los usuarios finales a la Autoridad de Certificación. Siendo a su vez, el instrumento en el que se generan o validan las solicitudes de certificación y las solicitudes de revocación.

Además, los módulos de seguridad o HSM serán los responsables de gestionar las claves de privadas de las CA.

> Con la implementación de una estructura de tecnología de clave pública estamos reforzando el acceso seguro, la integridad y autenticidad de los datos

En una segunda fase y con el objetivo de implementar un sistema PKI más completo, podemos incorporar una Autoridad de Validación o VA y una Autoridad de Sellado de Tiempo o TSA.

Por su parte, con la Autoridad de Validación podemos proporcionar “en todo momento” el estado de revocación actualizado de un certificado y en algunos casos aligerar el tráfico de red como consecuencia de la descarga repetitiva de las listas de certificados revocados.

A su vez, es aconsejable añadir a esta suite, una Autoridad de Sellado de Tiempo o TSA que otorga certeza y evidencia el instante (horario exacto) en el que se realizó la firma digital a través del sello de tiempo o tiempo o Time Stamping.

También sobre todo lo aquí señalado, puede encontrar información más detallada en el post de nuestro blog ¿Qué es una Infraestructura de Clave Pública o PKI?

INTERNET DE LOS PAGOS & PKI

Actualmente, ya nadie duda de que el Internet de las Cosas o IoT está presente en numerosas facetas de nuestro día a día: hogares conectados, pagos a través de monedero electrónico... pero, al mismo tiempo, se erige como un atractivo blanco para los ciberdelicuentes y es aquí donde las empresas fabricantes y/o usuarias no deben escatimar en la protección de los entornos IoT.

El Internet de los Pagos es el Internet de las Cosas aplicado al desarrollo de la Banca digital inteligente y es en este escenario donde PKI es la responsable de construir un ecosistema IoT de confianza basado en comunicaciones y transferencia segura de datos.

Tanto los nuevos modelos digitales financieros (Fintech, neobancos...) como la banca tradicional son conscientes que el desarrollo exitoso de estos pagos va ligado a la seguridad robustas de sus sistemas y es aquí donde la PKI se convierte en una aliada tecnológica imprescindible para la securización IoT, dotando de certificados digitales con claves seguras a cada uno de los dispositivos de la red de Internet de los Pagos, logrando así una identidad en línea tanto de las personas como de los objetos o dispositivos.

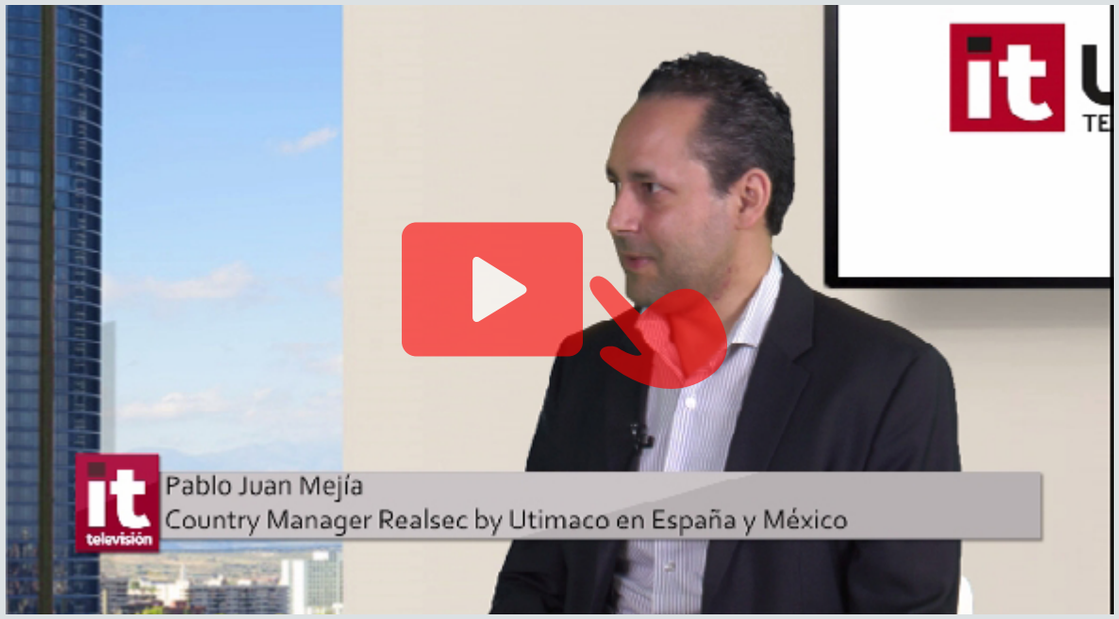
Los dispositivos IoT dependen principalmente de certificados digitales para su identifi-

cación y autenticación, siendo el Internet de las Cosas la tecnología emergente de mayor crecimiento en la actualidad que impulsa el despliegue y aplicación de PKI. Por lo tanto, si queremos alta seguridad y más en entornos tan críticos como los pagos, una PKI es clave dentro de las estrategias de ciberseguridad del sector financiero como catalizador de las aplicaciones centrales del negocio. ■

PABLO JUAN MEJÍA, COUNTRY MANAGER DE REALSEC BY UTIMACO EN ESPAÑA Y MÉXICO

"Los bancos deben evolucionar para reforzar la confianza de los usuarios"

El dinero es un activo crítico para todas las entidades financieras, por lo que siempre ha estado sujeto a diversos ataques. Anteriormente eran las personas armadas que entraban a la sucursal y robaban el dinero, hoy en día estos ataques se hacen digitalmente. La confianza de los usuarios es algo primordial, por lo que los bancos deben evolucionar para tener esa confianza frente a estos ciberataques.



Para Pablo Juan Mejía, Country Manager de Realsec by Utimaco en España y México, es indispensable que los bancos utilicen los mecanismos de protección adecuados, como son el manejo de claves criptográficas a través de dispositivos como HSMs. La banca utiliza datos cada vez de mayor sensibilidad, cuando se procesa una transacción, el banco debe asegurarse de que esa transacción es legítima, debe estar asegurada por algún procesamiento criptográfico. El sector afronta la seguridad en base a tres principios: las regulaciones, la madurez de las tecnologías y la relación entre el beneficio que les brinda y su precio. Además, si la seguridad no es funcional, no va a ser útil. Por su parte, las FinTech tienen que ir adoptando aquellas medidas de seguridad mínimas que les permitan generar confianza en los usuarios.

> Es indispensable que los bancos utilicen los mecanismos de protección adecuados, como son el manejo de claves criptográficas

Redtrust,
la herramienta de gestión y protección de la identidad digital para el sector bancario

DANIEL RODRÍGUEZ,
director general de Redtrust

El bancario es uno de los sectores más favorecidos por la digitalización. A nivel interno se han agilizado la mayoría de los procesos y securizado la comunicación con otras entidades y organismos, mientras que de forma externa se ha optimizado la experiencia del cliente gracias al asentamiento de la banca online. Sin embargo, esta madurez digital ha convertido a las organizaciones bancarias en un objetivo lucrativo para los ciberdelincuentes, que buscan un beneficio a través del robo o cifrado de datos y de técnicas como la suplantación de identidad.

Ante este paradigma, garantizar la seguridad de cualquier comunicación u operación, proteger la identidad tanto de clientes como de empleados y, por supuesto, acatar el cumplimiento normativo es prioritario. El certificado digital se ha convertido en el mecanismo de autenticación más robusto para verificar la identidad digital, por lo que sus casos de uso más comunes en la banca comprenden desde la firma digital, para acreditar la autenticidad, integridad y no repudio del contenido de documentos y archivos (PDF, macros...) hasta la autenticación, mediante la verificación de credenciales, y el cifrado de información (email o comunicaciones). A la vista de esta importancia, afianzar la seguridad de todos estos procesos es imperativo.

Por ello, la prioridad para CTO y CFO debe ser la de ejercer un total control sobre dichos certificados, para controlar, delegar y restringir su uso; y aplicar un Plan de Continuidad de Negocio que mitigue el impacto de cualquier incidencia relacionada con la seguridad digital, incorporando las herramientas de salvaguarda más adecuadas para ello.

PROTEGER EL CERTIFICADO

Como gestor corporativo de certificados digitales, Redtrust ofrece una protección proactiva para la custodia de los certificados en un servidor cifrado y centralizado, ajeno a los dispositivos de trabajo. Este control y gestión de certificados digitales a través de la centralización, asegura la protección de la identidad digital de las empresas, evita su dispersión en los distintos puestos de trabajo, así como su uso y exportación ilegítima por parte de usuarios no autorizados.

Asimismo, Redtrust permite gestionar los privilegios, controlar los accesos y la información, además de crear alertas de caducidad. Adicionalmente, y para obtener un registro detallado de todas las operaciones realizadas con los diferentes certificados digitales, es posible monitorizar las acciones en tiempo real, e, incluso, registrar todas las operaciones realizadas con los certificados gracias a auditorías detalladas.

Por último, y mediante la movilidad de los certificados, Redtrust garantiza la seguridad de los accesos en remoto de los empleados y el uso del certificado desde otros lugares de trabajo. También incrementa la protección de los accesos a los entornos empresariales al incorporar la seguri-

dad de los certificados digitales a una estrategia de gestión de identidad y accesos. La combinación de IAM y certificado ofrece un elevado grado de protección cuando este se almacena en un repositorio cifrado y centralizado.

Sin duda, la integración con Redtrust para la gestión centralizada de los certificados otorga a las firmas del sector bancario la máxima garantía de protección sobre su identidad digital. A día de hoy, más del 60% de las entidades bancarias pertenecientes al IBEX 35 confían en Redtrust para ejercer una gestión centralizada y controlada de sus certificados digitales.

Además, el 40% de los clientes de banca utilizan un HSM para custodiar sus certificados de forma segura. Estas cifras posicionan a Redtrust como la herramienta de gestión y protección de identidad digital líder en el sector bancario español. ■

DANIEL RODRÍGUEZ, DIRECTOR GENERAL DE REDTRUST

"Tecnologías como Blockchain suponen un gran reto para el sector bancario"

El mayor reto al que se está enfrentando el sector financiero es la inclusión del blockchain y demás tecnologías descentralizadas. Por otro lado, el incremento de las regulaciones a nivel europeo como PSD2, GDPR o eIDAS también va a ser importante. A nivel de seguridad, la protección de la identidad es uno de los mayores retos para el sector bancario.

El certificado digital se ha convertido en el mecanismo de autenticación más robusto para validar la identidad del usuario. Como indica Daniel Rodríguez, director general de Redtrust, es muy importante la concienciación de los usuarios finales en cuanto al uso del certificado digital, ya que el uso de ese certificado por un usuario de manera descontrolada puede llevar a graves problemas de suplantación de identidad.

En cuanto a las empresas, ha habido una evolución muy positiva del certificado digital. El mercado es muy maduro y la adopción ha sido muy rápida. A pesar de ello, no todos los bancos están adaptados a esta autenticación, que además se ha demostrado que es la más segura, debido al coste tecnológico que supone. Por ello es necesario que sector público y privado trabajen de la mano para concienciar al usuario en el uso del certificado digital, pero también haciéndoselo fácil.

El estado del ransomware en el sector de los servicios financieros 2022

ÁLVARO FERNÁNDEZ DÍEZ DE GÜEMES,
Sales Manager Iberia de Sophos

El informe El estado del ransomware en el sector de los servicios financieros 2022 de Sophos ofrece nuevas perspectivas sobre los ataques de ransomware, los costes, la recuperación y el pago de rescates que han afectado a las organizaciones de servicios financieros durante el último año.

El informe se basa en nuestro estudio anual de las experiencias reales de ransomware de los profesionales de TI, de los cuales 444 encuestados procedían del sector de los servicios financieros, y trabajaban en empresas de tamaño medio (100-5.000 empleados) en 31 países.

El estudio revela un entorno de ataque cada vez más desafiante, y la creciente carga financiera y operativa que el ransomware está suponiendo para el sector de servicios financieros. Estas son las principales conclusiones del informe:

- Los ataques de ransomware a los servicios financieros han aumentado: el 55 % de las organizaciones fueron afectadas en 2021, frente al 34 % en 2020
- Los servicios financieros reportaron la segunda tasa más baja de cifrado de datos, con un 54 %. La media mundial fue del 65 %
- El 52 % de las organizaciones de servicios financieros pagaron el rescate para restaurar los datos, lo que es más alto que el promedio global del 46%
- La cantidad de datos restaurados por los servicios financieros se ha mantenido constante en el 63 % a lo largo de 2020 y 2021, la media mundial es del 61 %. Sin embargo, el porcentaje de organizaciones de servicios financieros que recuperaron TODOS sus datos cifrados subió del 4 % en 2020 al 10 % en 2021. cuando la media mundial en 2021 fue de solo el 4%
- La tasa de pago de rescates por parte del sector en cuestión se duplicó con creces: pasó del 25 % en 2020 al 52 % en 2021. La media mundial en 2021 fue del 46 %
- El coste medio de remediación en los servicios financieros fue de 1,59 millones de dólares, lo que supera la media de 1,4 millones de dólares
- El 83 % de las organizaciones de servicios financieros informaron que tienen cobertura de ciberseguro contra el ransomware, en línea con el promedio global

❖ El ciberseguro está impulsando a los servicios financieros a mejorar las ciberdefensas: el 98 % de las organizaciones de servicios financieros han mejorado sus ciberdefensas para asegurar la cobertura

❖ Los servicios financieros tienen una de las tasas más bajas de pago de rescates por parte de las aseguradoras: 32 % en comparación con el 40 % en todos los sectores

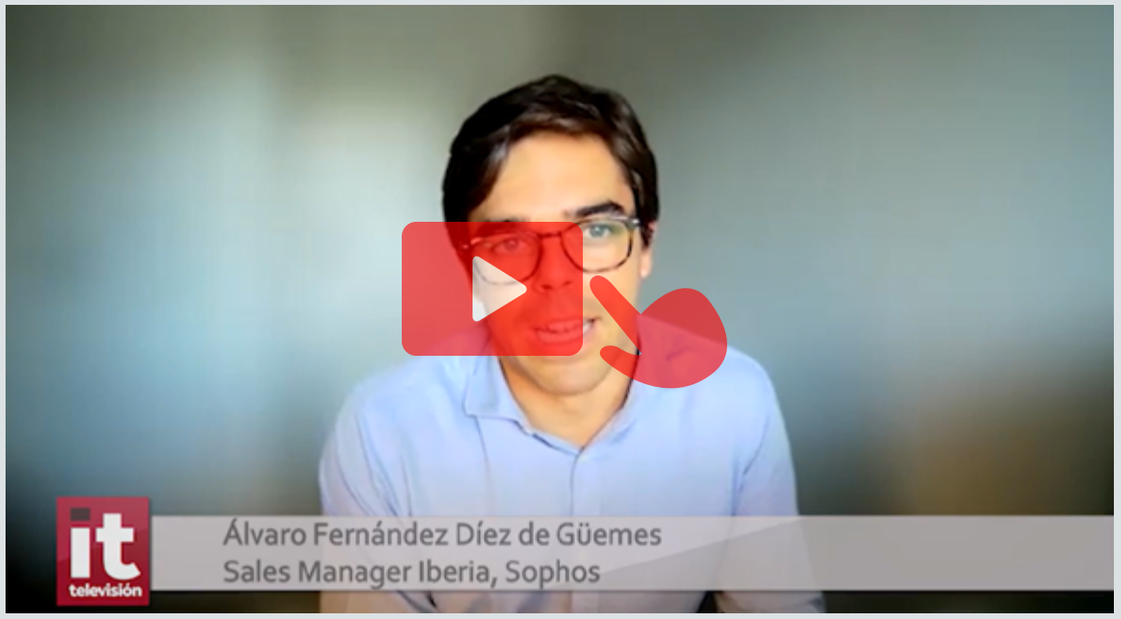
La creciente tasa de ataques de ransomware en los servicios financieros demuestra que los adversarios se han vuelto considerablemente más capaces de ejecutar ataques a escala desplegando con éxito el modelo de ransomware como servicio.

Cada vez es más difícil para las organizaciones, especialmente en el sector de los servicios financieros, asegurar la cobertura. Esto ha llevado a casi todas las organizaciones de servicios financieros a realizar cambios en sus ciberdefensas para mejorar su posición en los ciberseguros. ■

ÁLVARO FERNÁNDEZ DÍEZ DE GÜEMES, SALES MANAGER IBERIA DE SOPHOS

"El sector financiero es de los más maduros, tecnológicamente hablando"

Los retos a los que se enfrenta el sector financiero son similares al del resto de organizaciones, a pesar de la fuerte regulación establecida y de que se trata de una de las industrias más maduras tecnológicamente hablando y también en cuanto a la seguridad. Los ciberataques han aumentado un 55% con respecto al pasado año y se trata de amenazas mucho más sofisticadas.



El ataque por excelencia es el ransomware. Como indica Álvaro Fernández Díez de Güemes, Sales Manager Iberia de Sophos, alrededor del 50% de las organizaciones han sufrido un ataque de tipo ransomware. De ese 50%, en algo más de la mitad los atacantes han logrado cifrar datos, ya sea parcialmente o en su totalidad lo que supone un coste económico y reputacional. La mitad de esas organizaciones afectadas ha llegado a pagar el rescate, cuando el rescate medio ronda los 300.000 euros. Además, el coste medio de recuperarse de un ataque de este tipo está en torno al millón y medio de euros.

Para abordar esta problemática, el sector financiero sobre todo demanda servicios de operativa de seguridad y de respuesta ante incidentes. También son muy solicitados los servicios de monitorización desde un punto de vista más reactivo, para ir mejorando las políticas de seguridad. Dada la creciente complejidad de los ataques, el futuro implica la necesidad de equipos de headhunters especializados dedicados a buscar amenazas dentro de la red.

Maximizar inversión y seguridad van de la mano en el sector financiero

ELENA GARCÍA-MASCARAQUE,
security service providers director, WatchGuard-Cytomic

Hoy en día observamos una enorme variedad de innovaciones alrededor del concepto y modelo de negocio "FinTech" (Tecnología en Servicios Financieros) que han revolucionado el mercado. Ante estos progresos, muchas instituciones financieras anhelan seguir esta tendencia para ofrecer a los clientes nuevas opciones bancarias. Pero mantenerse al día con las tendencias no es sencillo, bien por lo que implica en ciberseguridad o por los estándares regulatorios, y muchos de esos desafíos han caído en manos del departamento de TI para su resolución.

Veamos algunos de los retos más importantes que afectan a las organizaciones financieras, y también los pasos clave que estas pueden dar para contar con una ciberseguridad más sólida. Así, entre los principales desafíos, encontramos estos:

❖ **Asociación con empresas FinTech para ofrecer experiencias bancarias digitales:** aunque la industria evoluciona con rapidez, está claro que las instituciones financieras establecidas y las nuevas empresas de FinTech deben trabajar juntas para seguir impulsando la innovación y satisfaciendo la demanda de los consumidores. A pesar de que la mayoría de los bancos admite que las alianzas son necesarias, un 71% se preocupa también por los ciberriesgos de estas asociaciones. Esto es en parte porque las empresas jóvenes de FinTech, por lo general, tienen menos recursos para invertir en seguridad o para atender otros requisitos de regulaciones.

❖ **Presiones similares de las expectativas del consumidor y las regulaciones de cumplimiento:** cumplir con la regulación es un objetivo diario para las instituciones financieras, no existe otra opción, pues el coste del incumplimiento es mucho más alto en términos económicos y de reputación. En cuanto al consumidor, los clientes esperan más canales y servicios, y mayores capacidades de sus cuentas online, sin comprometer la seguridad de sus datos.

❖ **Aumento del riesgo por parte de terceros:** las relaciones con terceros incluyen productos y servicios externalizados, uso de consultores externos, configuración de redes, servicios de procesamientos de pago, servicios ofrecidos por filiales y subsidiarias y otros acuerdos comerciales en los que un banco tiene una relación permanente con un tercero o puede ser responsable por los registros asociados. La Oficina del Controlador de Moneda (OCC) sostiene que el uso de terceros no reduce la responsabilidad que tiene un banco de asegurar que las funciones con terceros se lleven a cabo de manera segura. Lamentablemente, una empresa es tan fuerte como su partner más débil. Si un partner sufre un ataque, esa vulnerabilidad creará problemas significativos para su organización.

Ante estos desafíos, los servicios de ciberseguridad que son los más demandados en el sector financiero están relacionados con la implantación de un enfoque zero-trust y servicios MDR 24x7.

Asimismo, desde WatchGuard recomendamos también tener en cuenta los siguientes aspectos:

1. Seguridad Endpoint Security con capacidades de EPDR, es realmente importante contar con un agente único que recoja al menos un año de telemetría dado que las investigaciones requieren al menos de 238 días.

2. Autenticación multifactor: una política MFA hará muy difícil que los actores de amenazas comprometan las credenciales privilegiadas.

3. Servicio de Theat Hunting Avanzado para adelantarnos a las amenazas, así como su integración en un Servicio de SOC 24*7

4. Firewall: un firewall actualizado regularmente es capaz de detectar y bloquear intentos de inyección de malware.

5. Gestión de la superficie de ataque: una solución de gestión de la superficie de ataque capaz de detectar fugas de datos reducirá significativamente las posibilidades de que se produzca una filtración de datos, tanto a nivel interno como en la red del proveedor.

6. Gestión de riesgos de terceros (TPRM): un programa de gestión de riesgos de terceros identificará las vulnerabilidades de seguridad de todos los servicios en la nube de terceros para prevenir los ataques a la cadena de suministro.

La industria financiera afronta nuevos desafíos en los últimos años, muchos de ellos derivados de los impactos de la evolución hacia un mercado cada vez más digitalizado. Con WatchGuard, pueden aprovechar de forma segura el poder de estas nuevas tecnologías con soluciones sólidas y seguras que se pueden utilizar en el banco. ■

ELENA GARCÍA-MASCARAQUE, SECURITY SERVICE PROVIDERS DIRECTOR, WATCHGUARD-CYTOMIC

“La bancaria es una industria especialmente expuesta a los ciberataques”

Entre las principales amenazas que apuntan a la banca, Elena García-Mascaraque, security service providers director, WatchGuard-Cytomic, destaca el ransomware. Según sus estudios, solamente en el primer trimestre de 2022 ya se han duplicado el número de ataques de ransomware de todo el año pasado, sobre todo en EMEA, debido a la situación geopolítica de la región. Además, el phishing, los ataques de denegación de servicio y los ataques a la cadena de suministro y entrega de software, también suponen un reto para el sector. La hibridación de los procesos y las formas de trabajo está haciendo que el perímetro de seguridad se diluya, por lo que se hace necesario volver a los principios del Zero Trust, que comienzan con un endpoint no solamente protegido, sino también prevenido. El doble factor de autenticación se ha convertido en uno de los elementos clave de la seguridad, así como contar con un servicio 24x7, servicios de investigación y poner mucho énfasis en el *security by design*.

WatchGuard | CYTOMIC

WatchGuard for SOC – Eficiencia y proactividad

Anticípate a las ciberamenazas en constante evolución

Threat Hunting

Ciber Resiliencia

Detección, investigación y respuesta

SEGURIDAD ENDPOINT AVANZADA

AUTENTIFICACIÓN MULTIFACTOR

NUBE SEGURA WI-FI

SEGURIDAD DE RED

WatchGuard for SOC se basa en la combinación de soluciones de seguridad avanzada y plataforma de threat hunting para buscar, detectar y responder de manera eficiente a amenazas que hayan logrado evadir otras protecciones en endpoints, servidores, entornos virtuales y dispositivos móviles.

Contacto: **900 840 407** **strategic.accounts@watchguard.com** **www.watchguard.com**

Ciberseguridad Realsec by Utimaco

La propuesta tecnológica de Realsec by Ultimaco comprende una serie de soluciones que abarcan diversos aspectos de la ciberseguridad de las empresas, una propuesta que se adapta perfectamente a las empresas del sector financiero.

La gama de soluciones incluye:

❖ **HSM de Propósito General/ Cryptosec LAN.** Servidor criptográfico en red, de altas prestaciones y seguridad, diseñado para servicios de cifrado y aplicaciones de firma digital, independientemente del sistema operativo donde estas residan. 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.

❖ **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.

❖ **Autoridad de 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.

❖ **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.

❖ **Soluciones Ciberseguridad Blockchain & IoT.** Realsec, de la mano de su empresa matriz, Utimaco, pone a su disposición el catálogo de soluciones de ciberseguridad para entornos Blockchain & iOT: (Block-safe, Administración de Llaves Universales; KeyBRIDGE (UKM) Almacenamiento seguro de sus claves y datos confidenciales en una única ubicación centralizada y Gestor seguro de claves de empresa (ESKM).

❖ **Block-safe**. Protección de Identidades, Claves y Datos Confidenciales en Plataformas Informáticas de Tecnología Ledger Distribuida (DLT) Diseñado para soluciones basadas en blockchain.

❖ **ESKM.** Gestor seguro, interoperable e integrado de las claves de la empresa. Capacidad para gestionar más de 2 millones de claves, más de 25.000 clientes y miles de dispositivos virtuales o hardware ESKM.

❖ **KeyBridge (UKM).** Almacenamiento seguro de sus claves y datos confidenciales en una única ubicación centralizada. Plataforma capaz de custodiar de forma integral las claves y datos confidenciales de toda una organización. ■

La propuesta tecnológica de Realsec by Utimaco comprende una serie de soluciones que abarcan diversos aspectos de la ciberseguridad de las empresas, una propuesta que se adapta perfectamente a las empresas del sector financiero

Redtrust: autenticación, cifrado y firma segura

Redtrust es la solución autocontenida para todo tipo de empresas y, por supuesto, para organizaciones financieras que desean gestionar su identidad digital y asegurar el control total de los certificados digitales, custodiándolos de forma centralizada en un repositorio único, seguro y cifrado.

Redtrust permite a estas empresas crear políticas para limitar los usos de los certificados a los empleados; auditar para saber quién, cuándo y para qué se han utilizado e incluso controlar el ciclo de vida completo de cada certificado. Con su gestor especializado, las compañías financieras pueden garantizar la seguridad de estos usuarios al autenticarse, firmar digitalmente o cifrar información y comunicaciones, entre otros casos de uso.

Redtrust es, por tanto, una herramienta imprescindible. Por eso, cada vez más entidades financieras confían en ella para gestionar y proteger su identidad digital y ejercer un mayor control sobre el uso que cada empleado hace de los certificados, sin importar el número de usuarios y/o certificados.

Redtrust es la solución autocontenida para todo tipo de empresas que desean gestionar su identidad digital y asegurar el control total de los certificados digitales, custodiándolos de forma centralizada en un repositorio único, seguro y cifrado

EMISIÓN DE CERTIFICADOS DIGITALES CON REDTRUST

El auge de las gestiones y trámites telemáticos ha llevado a las entidades del sector financiero a emplear el certificado digital para garantizar la seguridad de sus comunicaciones. En la actualidad, las empresas pueden identificarse y verificar su identidad para la emisión de certificados mediante dos vías: presencial u online.

Redtrust se integra con Autoridades de Certificación tanto públicas como privadas para la emisión de certificados digitales mediante verificación presencial u online. Los certificados digitales nacen directamente dentro del servidor cifrado de Redtrust, por lo que las empresas financieras pueden emitir, renovar o revocar sus certificados sin abandonar la consola de administración.

En cuanto a la custodia de los certificados digitales, esta, tiene lugar en el repositorio de Redtrust, lo que garantiza a estas entidades su seguridad a la hora de autenticarse, firmar digitalmente o realizar trámites online con otras entidades y organismos públicos, pudiendo ejercer un total control sobre ellos gracias a la gestión de su ciclo de vida, la creación de políticas de uso o la monitorización de cualquier acción llevada a cabo con los certificados.

API SERVICIOS WEB

Cada vez son más las empresas que utilizan APIs de terceros en sus sistemas internos, a fin de simplificar y automatizar procesos y acelerar el ritmo de trabajo.

Con la API de Servicios Web de Redtrust las organizaciones financieras pueden integrar sus aplicaciones corporativas con total compatibilidad y controlar cada acción desde una única consola de administración, manteniendo así la identidad corporativa. Redtrust se adapta a las necesidades de estas empresas garantizando la seguridad y control en los procesos de autenticación, firma digital y cifrado.

Con la API de Redtrust es posible firmar documentos, cumpliendo con el estándar DSS, y con total seguridad, ya que la clave privada de los certificados permanece custodiada en su servidor cifrado.

Asimismo, las entidades pueden personalizar el espacio de trabajo y configurar la herramienta acorde a sus necesidades para permitir a los usuarios gestionar sus propios certificados digitales y a través de la API, realizar firmas desde cualquier dispositivo. Las organizaciones obtienen un registro de todas las acciones que estos realizan con cada certificado. Adicionalmente, y al integrar Redtrust en los procesos, los servidores corporativos pueden utilizar la API para automatizar procesos, gestionar usuarios desde el Active Directory o subir documentos, entre otros. ■

MÁS INFORMACIÓN

- Firmar documentos PDF con certificado digital de forma controlada
- Redtrust: Gestión de certificados digitales
- El nuevo papel del certificado digital en la estrategia de ciberseguridad
- Claves del CTO y CFO para una correcta gestión de la identidad digital en banca

Seguridad integrada

Impulsado por el threat intelligence, IA y machine learning de SophosLabs y SophosAI, Sophos ofrece un catálogo de productos y servicios avanzados para proteger a los usuarios, las redes los servidores y los endpoints contra el ransomware, malware, exploits, el phishing y la amplia gama de ciberataques que se encuentran hoy en día. Sophos proporciona una única consola cloud de gestión integrada, Sophos Central, como pieza central de un ecosistema de ciberseguridad adaptativo que cuenta con un lago de datos centralizado que aprovecha un extenso conjunto de API abiertas disponibles para clientes, partners, desarrolladores y otros fabricantes de ciberseguridad.

Las soluciones para el sector financiero incluyen:

❖ **Sophos Intercept X EDR/XDR.** Un sistema de protección endpoint que engloba la protección tradicional (firmas), junto con protección "next-gen" (Inteligencia Artificial, anti exploit, análisis de comportamiento, anti ransomware y anti hacking) así como protecciones complementarias (control web, control de aplicaciones, cifrado, DLP...) y, por supuesto, EDR o, a día de hoy, XDR gracias a la integración cruzada de datos sus firewalls, el servicio de correo, UEM para la gestión de los dispositivos móviles y los sistemas de protección cloud. Su gestión se realiza a través de Sophos Central, lo que permite la interacción con otros productos de Sophos y gracias a su API, con cualquier fabricante.

❖ **Sophos MDR y Rapid Response.** Sophos Managed Detection and Response (MDR), es un servicio gestionado de respuesta frente a amenazas, que ofrece a las empresas funciones de búsqueda, detección y respuesta ante posibles amenazas 24/7. Formado por un equipo de detección de amenazas y profesionales expertos en investigaciones avanzadas es capaz de dar respuesta a los ciberataques tomando medidas para neutralizar incluso, las amenazas más sofisticadas. Sophos puede dar respuesta, apoyándose en el agente de Sophos para realizar las acciones oportunas para la detección y la mitigación de la amenaza. Además, nuestro servicio, incluye la capacidad de prestar servicios MDR de Sophos utilizando fuentes de datos de terceros (no de Sophos). Cualquier empresa que esté sufriendo un ataque activo puede recurrir a Sophos Rapid Response, que es capaz de realizar un despliegue rápido del producto y su equipo de expertos en ciberseguridad son capaces de ver cuál es la situación dentro de

la compañía, detener el ataque y, si es posible, detectar por dónde ha venido, a quién ha afectado y limpiar todo lo que haya sido dañado para que pueda volver a la normalidad lo antes posible.

❖ **Sophos Firewall.** La seguridad de red desde la compra de Astaro en 2008 por Sophos ha seguido evolucionando hasta llegar a los modernos Sophos Firewall. Los firewalls son gestionados de forma centralizada desde Sophos Central, que es capaz de integrarse con el Endpoint y con el servicio MDR, así como de hidratar el lago de datos, englobándose dentro de la estrategia XDR. La arquitectura de Xstream con doble procesador de Sophos Firewall protege la red de las amenazas más recientes al tiempo que acelera el tráfico importante de SaaS, SD-WAN, IPSec VPN y aplicaciones en la nube.

❖ **Sophos Zero Trust:** Sophos ZTNA se basa en los principios de Zero Trust: no confiar en nada y verificarlo todo. Los usuarios y dispositivos se convierten en su propio perímetro microsegmentado, con lo que se validan y verifican constantemente. Con Zero Trust, los usuarios ya no se encuentran "en la red" con la confianza y el acceso implícito que habitualmente conlleva. Sophos ZTNA es la única solución Zero Trust Network Access que se integra perfectamente con un producto para endpoints Next-Gen: Sophos Intercept X, realizando un despliegue conjunto como un único agente y administrándose de forma sencilla desde Sophos Central. Sophos ZTNA e Intercept X comparten constantemente información de estado y seguridad para aislar automáticamente los sistemas comprometidos a fin de impedir que las amenazas se propaguen o roben datos.

❖ **Sophos Email.** Seguridad del correo electrónico más inteligente con IA. Las actuales amenazas para el correo electrónico evolucionan rápidamente, y las empresas en expansión necesitan una seguridad predictiva para el email, es decir, que combata las amenazas de hoy día sin perder de vista el mañana. La protección multicapa de Sophos se sirve de la información sobre amenazas, análisis de reputación y comportamientos, y Machine Learning de vanguardia para evitar que el malware y las URL maliciosas lleguen siquiera a la bandeja de entrada. Además, la seguridad del correo electrónico basada en API gracias a la integración con Microsoft 365, evita la necesidad de redirigir el correo electrónico a través de la puerta de enlace de Sophos Email, lo que garantiza una configuración y un procesamiento del correo más rápidos aumentando la eficiencia en los flujos de correo.

❖ **Sophos Cloud Native Security (CNS):** Conscientes de que cada vez más, la infraestructura de TI está migrándose a la nube, Sophos fue uno de los primeros fabricantes en hablar de CSWP y CSPM gracias, tanto al agente para servidores, como en nuestro CNS, el cual audita los recursos que tengamos sobre proveedores de nube pública como AWS, Azure, Google Cloud y Kubernetes, asegura el cumplimiento de las normas internacionales de seguridad y evita el despliegue de software vulnerable en DevOps. Además, se integra con XDR y con el servicio MDR, lo que proporciona más visibilidad e información que será recogida en nuestro lago de datos.

❖ **Sophos Switch.** La serie Sophos Switch ofrece un acceso Ethernet seguro y escalable para sus dispositivos cableados e inalámbricos y le otorga un control total sobre su conectividad LAN. La serie Sophos Switch ofrece una gama de switches de capa de acceso de red para conectar y alimentar los dispositivos que se conectan a la red de área local (LAN), al tiempo que añaden controles de seguridad y segmentación en el perímetro de la LAN ofreciendo velocidades de conexión de hasta 2.5 G. Los switches de Sophos están pensados para oficinas remotas, pequeñas y medianas empresas, establecimientos comerciales y sucursales y están disponibles con distintas densidades de puertos para satisfacer las necesidades de conectividad de la mayoría de las organizaciones. ■

MÁS INFORMACIÓN

Sophos

Seguridad Inteligente

WatchGuard Technologies cuenta con un catálogo que combina tanto hardware como software, permitiendo crear un sólido escudo de defensa en las organizaciones gracias a una propuesta integral que abarca desde la seguridad de red hasta la protección avanzada para el endpoint e inteligencia de red, así como la seguridad Wi-Fi y autenticación multifactor (MFA).

La máxima de WatchGuard es "hacer que la seguridad de nivel empresarial sea accesible a las organizaciones de todos los sectores y tamaños, a través de la simplicidad, ofreciendo seguridad inteligente y eficaz bajo la fórmula de soluciones fáciles de desplegar y gestionar".

La oferta de seguridad de WatchGuard abarca desde los servicios de seguridad de red tradicionales hasta los más innovadores como protección contra malware avanzado, ransomware y pérdida de datos confidenciales, o servicios Zero-Trust.

Por áreas, la propuesta para el sector financiero se estructura de la siguiente manera:

❖ **Seguridad endpoint:** WatchGuard Advanced EDR y EPDR ofrecen las tecnologías necesarias para automatizar la prevención, la detección, la contención y la respuesta relacionadas con cualquier amenaza avanzada, malware de día cero, ransomware, suplantación de identidad, vulnerabilidad en la memoria o ataque sin malware y sin archivo, dentro y fuera de la red corporativa. A diferencia de otras soluciones, combina la más amplia variedad de tecnologías de protección de endpoints (EPP) con capacidades automatizadas de detección y respuesta (EDR). También cuenta con servicios administrados por expertos de WatchGuard, que se brindan como una funcionalidad de la solución como Servicio Zero-Trust de Aplicaciones: clasificación del 100% de las aplicacio-

La máxima de WatchGuard es “hacer que la seguridad de nivel empresarial sea accesible a las organizaciones de todos los sectores y tamaños, a través de la simplicidad, ofreciendo seguridad inteligente y eficaz bajo la fórmula de soluciones fáciles de desplegar y gestionar”

nes y servicio de Threat Hunting: detección de hackers e intrusos.

Adicionalmente englobado en su seguridad endpoint cuenta con WatchGuard Orion, plataforma en la nube multi-tenant e integral que permite a los SOCs acelerar y ser más eficientes en sus operaciones de hunting, detección y respuesta de ciberamenazas desconocidas y sofisticadas. Permitiendo a los profesionales del SOC, mediante visibilidad 365 días de la actividad en los endpoints, analítica de comportamiento automatizado, y numerosas herramientas especializadas, descubrir, investigar y remediar eficientemente las amenazas ocultas en los endpoints que han conseguido evadir otros controles de seguridad.

❖ **Protección de identidades:** la solución de MFA, WatchGuard AuthPoint, aporta la seguridad necesaria para proteger activos, cuentas e información, permitiendo que las empresas y sus trabajadores accedan de forma segura y sin preocupaciones a las aplicaciones corporativas desde cualquier lugar. Sencilla de manejar, se administra de forma centralizada desde WatchGuard Cloud.

❖ **Seguridad de red:** todos los servicios de seguridad de WatchGuard se ofrecen como una solución integrada en un dispositivo Firebox rentable y fácil de manejar, tanto en entornos físicos como virtuales. Los Firebox destacan por su escalabilidad y están preparados para brindar el portfolio completo de servicios de seguridad, junto con un conjunto de herramientas de visibilidad y gestión que permiten estar un paso por delante del panorama de amenazas.

❖ **Wi-Fi seguro con gestión en cloud:** con Secure Wi-Fi se ofrece conectividad Wi-Fi y seguridad patentada que incrementa la productividad y la satisfacción de los clientes. Implementando un punto de acceso WatchGuard con Wi-Fi Cloud habilitado y una licencia de Secure Wi-Fi o Total Wi-Fi, se despliega todo el potencial de los puntos de acceso WatchGuard mediante un potente Sistema de Prevención de Intrusiones Inalámbricas (WIPS). Asimismo, WIPS garantiza la protección que cada usuario necesita, defiende el espacio aéreo 24x7 contra equipos no autorizados, ataques MitM y DoS, AP no autorizados y el resto de amenazas que acechan a los entornos Wi-Fi.

❖ También proponen una plataforma de seguridad unificada, **Unified Security Platform (USP)**, que ofrece servicios de seguridad eficientes y potentes con mayor escalabilidad y velocidad, y aportando eficiencias operativas. Diseñada por y para MSP, USP unifica tanto perímetro como endpoint, conexiones inalámbricas y gestión de accesos en una única plataforma aportando una visión simultanea global y agilizando las operaciones de ciberseguridad para mejorar la práctica de provisión de seguridad moderna. ■

MÁS INFORMACIÓN

WatchGuard Endpoint Security SOC

MFA

El 55% de las organizaciones de servicios financieros fueron afectadas por el ransomware en 2021

Tome medidas contra las amenazas con un equipo de expertos en respuesta

Con Sophos MDR, su empresa cuenta con el respaldo de un equipo de expertos que ofrece un servicio totalmente gestionado con funciones de búsqueda, detección y respuesta ante amenazas las 24 horas.

www.sophos.com/es-es

SOPHOS
Cybersecurity delivered.