it Digital Security

La publicación electrónica sobre Seguridad Digital que necesitas

Octubre 2017 - nº 1

Guarda esta revista en tu equipo y ábrela con Adobe Acrobat Reader para aprovechar al máximo sus opciones de interactividad

PABLO FERNÁNDEZ BURGUEÑO

@Pablofb

Abogado y socio en NevTrace y Abanlex

Pablo es jurista especializado en ciberseguridad, derecho del entretenimiento y modelos de negocio basados en el uso de blockchains. Es abogado en ejercicio, fundador de Abanlex y NevTrace, un laboratorio de criptografía aplicada desde el que realiza investigaciones sobre big data contra la ciberdelincuencia.

Seguridad Informática y previsiones de futuro

para el sector financiero

El sector financiero y bancario se enfrenta principalmente a los desafíos derivados de los avances informáticos y, en especial, a los vinculados con fintech, blockchain y seguridad informática.

Las fintech son empresas que unen las finanzas y la tecnología para prestar servicios financieros a los usuarios a través del uso de sitios webs y aplicaciones móviles haciendo extraordinariamente fáciles operaciones tales como la inversión en empresas o en proyectos de terceros, el cambio de divisas, las transferencias internacionales o el envío de dinero entre personas. Sus creadores emprenden nuevos modelos de negocio basados en la automatización de procesos sobre los pilares de la informática, la posibilidad de replicar acciones y la escalabilidad del producto.

El sector financiero y bancario también se enfrenta al reto surgido del nacimiento de soluciones basadas en la tecnología blockchain. A partir de esta se derivan las monedas virtuales, como el Bitcoin o el Monero y los smart contract, que permiten la creación de sistemas monetarios alternativos y la programación del dinero, respectivamente.

Gracias a la tecnología blockchain es posible mantener un libro contable único cuyo contenido se encuentra repetido íntegramente en diferentes ordenadores conectados. En la blockchain pueden escribirse transacciones monetarias, códigos informáticos o simples cadenas de caracteres alfanuméricos.

La confianza que se deposita en las anotaciones que se escriben en la blockchain se ve reforzado por la siguiente norma: aquel ordenador que trate de editar o borrar alguna de ellas es inmediatamente expulsado de la red. Esta garantía de integridad es la que ha permitido que determinadas blockchains, como la de Bitcoin, se abriera a Internet y se mantenga de forma simultánea en decenas de

La tecnología avanza mientras el sector financiero trabaja para conseguir integrar y mantener medidas suficientes de seguridad informática para combatir los ataques constantes y masivos que sufre

miles de ordenadores no identificados alrededor del mundo. A más ordenadores conectados, mayor es la seguridad que ofrece.

La tecnología avanza mientras el sector financiero trabaja para conseguir integrar y mantener medidas suficientes de seguridad informática para combatir los ataques constantes y masivos que sufre.

Estos ataques son a veces dirigidos contra las entidades con la finalidad de sustraer grandes cantidades de dinero o, aún más valioso, de secretos comerciales o datos de carácter personal; otras veces son el resultado de infecciones aleatorias sufridas por los clientes o los propios empleados de las sucursales.

Las estafas informáticas representan casi siempre más del 80% de los delitos informáticos, según los últimos informes anuales publicados por la Fiscalía General del Estado, aunque hay otra gran variedad de acciones ilícitas que llegan a los tribunales. La implementación inmediata de medidas de seguridad técnicas específicas, para evitar las brechas de seguridad o las consecuencias de estas, es exigida por las diferentes normas que ya están en vigor como, por ejemplo, la Directiva NIS o el Reglamento General de Protección de Datos. Si bien ya están en vigor, la exigibilidad de las mismas comenzará en el año 2018, con sanciones por su incumplimiento con multas de hasta 20 millones de euros o de hasta el 4% de la facturación global del año financiero anterior, eligiéndose la cifra más alta.

Ante esta situación, las empresas del sector deben tomar decisiones estratégicas de transformación digital para aprender a convivir con la nuevas fintech, convertirse en una de ellas, comprar sus proyectos o invertir en ellos; desarrollar productos basados en blockchain, usar las monedas virtuales para optimizar los tiempos y mejorar los procesos y comenzar a programar smart contracts con el objetivo de programar el dinero; y adecuarse de manera urgente a las nuevas normas en materia de seguridad informática invirtiendo en personal legal y téc-

A partir de 2016 se obliga a un banco español a indemnizar a un usuario que sufrió un ataque informático en su ordenador

nico capaz de evaluar el impacto de los potenciales ataques, seleccionar las soluciones adecuadas e implementarlas de manera eficiente y resiliente.

Así son los ataques informáticos que sufre el sector financiero

Los ataques informáticos que sufre el sector financiero son dirigidos o aleatorios, persistentes... Debería bastar con saber que los ataques son constantes, tanto a entidades como a clientes, que muchos de ellos son exitosos y que la mayor parte de los afectados ni siquiera se dará cuenta de haberlos sufrido hasta ver las consecuencias. Con esta información, las medidas de seguridad implementadas deberían ser suficientes, pero no lo son.

Las estafas, por poner un ejemplo, representan el 80% del total de los delitos informáticos denunciados en España, alcanzando la cifra anual de 17.328 en el periodo 2014 – 2015, según publica en su Memoria Anual de 2016 la Fiscalía General del Estado. Esta sólo es la punta del iceberg o la cresta de una ola de ciberataques que convierten a España en el país más infectado del mundo en determinadas versiones de malware, como es en el caso del ransomware CryptoLocker, que exige rescates en bitcoins a los usuarios afectados.

En el ámbito de la seguridad, el Reglamento General de Protección de Datos, que entró en vigor en 2016, exige a los bancos y las empresas fintech la implantación de medidas de seguridad acordes a los resultados de un análisis de riesgo denominado Evaluación de Impacto. El cumplimiento de esta norma europea de aplicación directa será exigible a partir del 25 de mayo de 2018, por lo que es ahora el momento de adecuar los procesos a lo que ya es imperativo. El Reglamento trae algunas consecuencias interesantes para los casos de incumplimiento como son, por ejemplo, estas dos: se establece una obligación para que las empresas comuniquen, a través de un medio de comunicación social, los ataques informáticos que sufran y que hayan podido afectar a los datos de los usuarios, salvo si pueden comunicarse con ellos directamente; y las sanciones por incumplimiento podrán suponer multas de hasta 20 millones de euros o de hasta el 4% de la facturación global del año financiero anterior, eligiendo la cifra más alta.

Una novedad interesante, también en materia de ciberseguridad, es la lograda en 2016 a través de los Tribunales españoles por la cual se obliga a un

PASADO, PRESENTE Y FUTURO DEL RANSOMWARE

Puede que no sea la más peligrosa, pero no cabe dura de que el ransomware es una amenaza formidable, y lo es porque funciona, y funciona porque son muchos, demasiados, los que pagan. En cualquier caso, existe y a pesar de los esfuerzos por parte de las empresas y de la industria en general para impedir las infecciones o saber reaccionar adecuadamente cuando se produzcan, los ataques de ransomware existen... y seguirán existiendo.

según se indica en la sentencia, la entidad podía haber aplicado y no aplicó medidas de seguridad técnicas suficientes que impidiesen la consecuencia. Aquí es donde empresas como F5, Exclusive, ESET o VMware, principalmente, están apostando por ofrecer sistemas que permiten al banco analizar el dispositivo con el que se está conectando el usuario para detectar malware instalado, para cifrar los datos o, en los servidores del operador, para implementar sistemas de micro-segmentación con el objetivo de detener intrusiones o evitar consecuencias mayores.

Previsiones de futuro para el sector financiero

Estamos en un momento de la historia en la que el avance tecnológico permite la creación de sustitutos eficientes a los operadores tradicionales.

Enlaces de interés...

- La digitalización aumenta los riesgos de fraude
- Criptodivisas, el próximo gran objetivo de los hackers
- W Ciberseguridad y Servicios financieros
- W Las claves de la ciberseguridad de los servicios financieros
- V F5 y Abanlex hablan sobre la responsabilidad del ciberfraude bancario

Las entidades del sector financiero tienen la misión de aprender en poco tiempo lo que sucede a su alrededor

banco español a indemnizar a un usuario que sufrió un ataque informático en su ordenador. El cliente fue infectado con el troyano Citadel, que es un tipo de software malicioso que extrae contraseñas, gracias al cual le fueron sustraídos más de 55.000 euros de su cuenta bancaria. El juez ordenó al banco entregar dicha cantidad al cliente puesto que,

Los nuevos operadores ofrecen sistemas basados en la economía colaborativa. Se benefician de las posibilidades que abren las redes que permiten conectar personas para que, entre ellas, se transmitan todo tipo de información digital. Hasta ahora, el mensaje era texto; ahora, el mensaje puede ser dinero.

Las entidades del sector financiero tienen la misión de aprender en poco tiempo lo que sucede a su alrededor. Si siguen mejorando lo que tienen, van a ser fagocitadas en breve por las que crean algo mejor. Pueden mantenerse estáticas para analizar la situación y actuar después, como buenas fast followers. Quizá sea suficiente, aunque quizá lo recomendable sea experimentar y convertirse en lo que se demanda o comprar a las que ya han nacido convertidas.

El surgimiento de las fintech, la innovación con blockchain y la lucha por la ciberdefensa ponen de relieve una realidad: el mundo financiero ya ha cambiado.