helpsystems

GUÍA *(Ciberseguridad)*

Desafíos de Ciberseguridad en el Sector Financiero - Estudio de Mercado

Un ciberataque contra el sector financiero puede causar daños considerables. Esto quedó muy claro en agosto 2020, cuando la bolsa de Nueva Zelanda quedó fuera de servicio por dos días seguidos por un ataque de denegación de servicio distribuido (DDoS), que se cree se originó en el extranjero.

Entre los desafíos que plantea la pandemia de Covid-19 y la aceleración de las iniciativas de Transformación Digital, la cadena de suministro es una de las vías de ataque más comunes. Un ejemplo es la tristemente célebre vulneración de Equifax en 2017, en la que los hackers expusieron datos, incluidos números de la Seguridad Social, porque la empresa no había parcheado un servidor correctamente.

Este ataque exitoso no solo afectó a Equifax: su cadena de suministro, incluidas Visa y MasterCard, envió alertas a los bancos notificándoles que 200.000 tarjetas de crédito también podrían haber estado comprometidas.

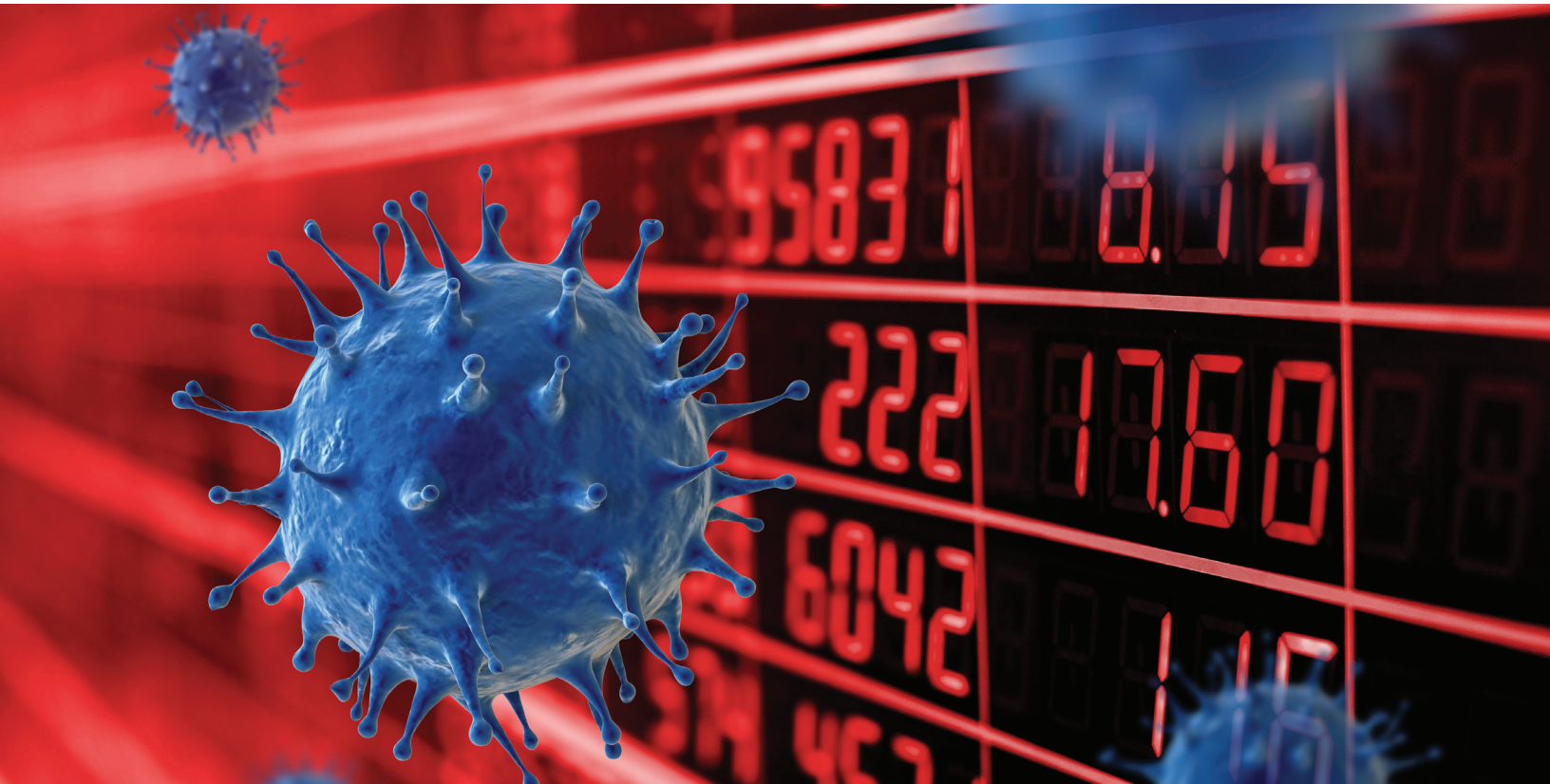
Otro ataque a la cadena de suministro fue la filtración de British Airways, en 2018, en la que los atacantes robaron los datos de pago de los clientes mediante un código malicioso implantado en un software de terceros que la aerolínea tenía en su sitio web. Y otro ataque similar afectó a la empresa de eventos Ticketmaster el mismo año. Se cree que ambos fueron perpetrados por el grupo Magecart cuyo objetivo son las empresas de comercio electrónico.

Además de los riesgos en la cadena de suministro, el sector financiero se enfrenta a una estricta normativa sobre la privacidad y Seguridad de la información, lo que complica aún más las cosas. Los bancos deben cumplir con normativas como el Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI DSS, por sus siglas en inglés) y la Actualización del Reglamento General de Protección de Datos (RGPD o GDPR), en unas condiciones cada vez más difíciles debidas a la pandemia Covid-19.

Todo ello mientras se evidencia un aumento de los ciberataques a las empresas de servicios financieros. Casi dos tercios (65%) de las grandes organizaciones financieras han sufrido un ciberataque en los últimos 12 meses, según la encuesta realizada por HelpSystems, proveedor de soluciones de Seguridad de la Información, a 250 CISOs y CIOs de todo el mundo.

Desde la llegada del Covid-19, el riesgo se ha elevado aún más, y el 45% ha observado un aumento de los ataques de Ciberseguridad durante este periodo. Las amenazas se dirigen a distintos vectores a medida que el teletrabajo se convierte en la norma en el sector de los servicios financieros.

Los CISOs y CIOs financieros tendrán que trabajar los próximos tres años en medio de la incertidumbre provocada por Covid-19, lo que plantea un enorme desafío para la Ciberseguridad: ¿cómo pueden las organizaciones financieras adoptar la Transformación Digital y permitir un teletrabajo eficiente mientras siguen aumentando las ciberamenazas?



Desafíos estratégicos

Las empresas financieras se enfrentan a una gran cantidad de desafíos en materia de Ciberseguridad y protección de datos. Esto se ha acentuado durante la pandemia de Covid-19, que ha obligado a las organizaciones a acelerar la Transformación Digital mientras gestionan una fuerza de trabajo remota.

Las empresas financieras ya conocen y temen el impacto de un ciberataque. Cuando se les preguntó qué implicaciones de un Ciberataque o filtración temen más, el 51% dijo que el daño a la reputación de la marca. Mientras, el 43% teme una filtración de los datos confidenciales de los clientes, el 40% está preocupado por el tiempo de inactividad de cara al cliente, y el 34% cita como problema la interrupción de las operaciones internas.

Las amenazas son inmensas, pero el reto más preocupante y que podría causar más daño en los próximos 12 meses es la posible debilidad de la Ciberseguridad en la cadena de suministro, según casi la mitad (46%) de los CISOs/CIOs encuestados.

Le sigue de cerca el aumento del teletrabajo durante la pandemia Covid-19, seleccionada por el 36% de los encuestados como la amenaza con mayor potencial de causar daños en los próximos 12 meses.

Mientras, el 35% cita el acceso de los hackers a los sistemas centrales como lo más perjudicial, y otro 35% dice que una amenaza interna, ya sea maliciosa o accidental, tiene el potencial de causar estragos. Las filtraciones de datos (31%), los ataques de ransomware (28%) y los ciberataques y el espionaje de potencias extranjeras (24%) también son muy citados.

Dentro de tres años, el principal reto en materia de Ciberseguridad para las empresas financieras será la Transformación Digital, según afirma el 41% de los encuestados. En relación con esto, el 28% de los encuestados señala la transición al teletrabajo como otro reto con gran impacto en el futuro inmediato.

En medio de este complejo entorno, no es de extrañar que el 92% de las organizaciones del sector financiero haya aumentado su inversión en Ciberseguridad durante los últimos 12 meses, y el 26% de forma significativa. “El panorama de la Ciberseguridad en el sector de los servicios financieros es muy desafiante, y muchos CISO/CIO se centran en luchar contra las amenazas cotidianas mientras intentan alcanzar objetivos estratégicos más amplios”, afirma Kate Bolseth, CEO de HelpSystems. “Por supuesto, la tecnología es una parte clave de la Ciberseguridad, y ninguna organización estará nunca segura si no cuentan con las soluciones de Seguridad adecuadas para proteger a la organización aquí y ahora. Pero igualmente importante, sobre todo para los objetivos estratégicos a largo plazo, es asegurarse de que existan los procesos adecuados, así como de educar y capacitar a los empleados”.

Ataques a la cadena de suministro y cómo protegerse de ellos

Ha quedado claro que la gestión del riesgo en la cadena de suministro es uno de los mayores problemas para las empresas financieras. En un momento de creciente Transformación Digital que conlleva una cadena de suministro más digital, cualquier organización es solo tan fuerte como lo es su eslabón más débil.

Los hackers lo saben, y a menudo buscan puntos débiles en un proveedor externo para dar el salto a los sistemas de sus víctimas. Tanto si se trata de un ataque complejo, como el hackeo a los tokens RSA de Lockheed Martin, como de un ataque más sencillo causado por empleados “de confianza” que acceden a información que no deberían, toda la cadena de suministro está en peligro y su Seguridad debe tomarse muy en serio.

“Hay muchos casos de estudio que demuestran lo vulnerables a los riesgos que son las cadenas de suministro”, afirma Stewart Room, Responsable Global de Protección de Datos y Ciberseguridad de DWF. Cita el ejemplo del ataque de Magecart, que inyecta un código malicioso en los sitios web para robar los datos de pago. Esto ha puesto de manifiesto la vulnerabilidad de los servicios de pago ante la

debilidad de la Ciberseguridad de la cadena de suministro, afirma.

La mitigación suele ser tan sencilla como preguntar a los proveedores por sus políticas de Ciberseguridad para asegurarse de que sean sólidas. La transparencia es fundamental, incluyendo una mejor diligencia debida en las relaciones con terceros.

" La pandemia ha venido a sumarse al problema, porque ha requerido de muchos ajustes operativos que, naturalmente, implican cambios en la cadena de suministro y en la superficie de ataque que esta representa".

Desafíos normativos

El sector de los servicios financieros es uno de los más regulados en la economía. En el Reino Unido, las organizaciones financieras tienen que cumplir con normas como GDPR y la Ley de Protección de Datos del Reino Unido, PCI DSS, y otras regulaciones no específicas del sector que regulan las infraestructuras críticas.

Estas regulaciones obligan a las organizaciones a establecer medidas adecuadas para la gestión de la información, con el objetivo de mejorar la Seguridad. "No hacerlo conlleva muchos riesgos legales, con consecuencias para la reputación", explica Room.

Casi un tercio de las organizaciones encuestadas afirma que las multas como consecuencia de una Seguridad deficiente son una preocupación. Aunque es una buena idea que las organizaciones vigilen de cerca el riesgo asociado al Cumplimiento normativo, Room dice que sería un error ignorar los litigios.

"Los litigios tras una vulneración de la Seguridad son un riesgo cada vez mayor en muchas partes del mundo, especialmente cuando la vulneración afecta a los consumidores o a las relaciones entre empresas. El Reino Unido es uno de los países en los que el riesgo de litigio es mayor en este momento, pero la tendencia está creciendo también en otros países".

Mientras tanto, la mitad de los CISO/CIO financieros afirma que la visibilidad de los datos es un desafío, una preocupación importante porque es un factor integral del Cumplimiento normativo. "GDPR, que desencadenó innumerables programas de transformación de datos entre 2016 y 2018, puso la necesidad de la visibilidad de los datos en la vía legislativa rápida", dice Room. "Los reguladores europeos de la protección de datos encontrarán esta estadística alarmante".

Futuros desafíos

En un complejo panorama de ataques agravado por la pandemia Covid-19, está claro que las personas, los procesos, y la tecnología son fundamentales. Con el aumento del teletrabajo, aumenta también la amenaza interna, y dos tercios (64%) de los CISOs/CIOs encuestados citan a la Transferencia Segura de Archivos como una prioridad clave para sus inversiones. Esta una cuestión urgente que hay que resolver, pero la capacitación por sí sola no es suficiente y puede plantear desafíos. La fatiga por la Ciberseguridad interna es citada como un problema por el 28% de los CISOs/CIOs del sector financiero.

La fatiga es una parte del problema porque los empleados están sometidos a la presión de tener que capacitarse de forma continua especialmente cuando se comunican por vídeo, y la Seguridad suele ser un obstáculo para su trabajo diario.

La tecnología puede ayudar a aliviar esta presión, por ejemplo, ofreciendo una mayor automatización dentro de la empresa. Es cierto que el ser humano siempre cometerá errores por mucha capacitación que tenga, y es buena idea quitarle parte de esta responsabilidad —y del riesgo.

Al mismo tiempo, la encuesta reveló que una cuarta parte de los CISOs/CIOs financieros están preocupados por el hecho de que haya demasiados procesos manuales en su empresa. Los CISOs/CIOs afirman que esto ha aumentado durante la pandemia y que ahora hay una mayor necesidad de automatización para liberar al personal de IT de las tareas manuales.

Es fundamental contar con la tecnología adecuada para respaldar a las personas y los procesos. A la hora de seleccionar un proveedor, es importante buscar una buena relación calidad-precio, y asegurarse de que las herramientas funcionen eficazmente y se integren bien.

Proteger los servicios financieros no es fácil. En condiciones extremadamente difíciles, agravadas por el virus Covid-19, no hay ningún cambio que pueda garantizar la Seguridad por sí solo. En general, es importante ser flexible y adoptar un enfoque basado en el riesgo.

Bolseth describe el desafío: "Las organizaciones necesitan hacer la transición a lo digital, cumplir con las exigencias de Cumplimiento normativo, proteger a una fuerza de trabajo remota de los retos que presenta Covid-19, y proteger a la organización contra las amenazas cotidianas, como el ransomware. No hay una bala de plata, solo una evolución constante ante el cambiante panorama de las amenazas".

Conclusión:

El sector financiero está bajo presión y esta no hizo más que aumentar durante la pandemia Covid-19. Los desafíos son numerosos, pero quizá el mayor tema en los próximos tres años será la Transformación Digital. Esta iniciativa se ha acelerado durante la pandemia, y es el telón de fondo del aumento del riesgo en la cadena de suministro.

Para hacer frente a estos retos, se necesita una combinación de personas, procesos y tecnologías. Room aconseja adoptar un enfoque holístico de la Seguridad que tenga en cuenta las preocupaciones de la IT en la sombra, provocadas por la aceleración de la Transformación Digital debida al Covid-19, el entorno de regulaciones de Cumplimiento, y el riesgo en la cadena de suministro.

La educación y la capacitación son fundamentales, pero no basta con capacitar a los usuarios para que reconozcan un correo electrónico sospechoso y lo denuncien. "Es suficiente que una persona abra accidentalmente un documento o haga click en una URL para que el malware consiga entrar", afirma Bolseth. "En la siguiente capa de defensa, las organizaciones necesitan aumentar su tecnología de Seguridad del correo electrónico para eliminar los archivos infectados y neutralizar las URL antes de que lleguen a las bandejas de entrada de las personas".

Dado que las empresas del sector financiero se enfrentan a complejos problemas de Seguridad bajo una presión continua para innovar, la planificación es lo más importante. "Desde la perspectiva de la gestión de riesgos, los ejercicios de transformación siempre plantean desafíos para la Seguridad, debido al ritmo, el alcance y el enfoque del cambio", afirma Bolseth. "Si la transformación abarca todos estos aspectos, los riesgos son elevados y, por ese motivo, es fundamental una planificación adecuada".

Covid-19: Desafíos de Ciberseguridad en el sector financiero

La pandemia Covid-19 ha presionado a todas las industrias, sin olvidar el sector financiero, altamente regulado y cada vez más digital. Por lo tanto, no es de extrañar que haya influido en la estrategia de casi todas las empresas financieras.

Casi la mitad de los encuestados considera que Covid-19 ha acelerado los cambios relacionados con la Transformación Digital que ya estaban sobre la mesa, como el paso a Office365.

Según la encuesta, el 42% de las empresas del sector financiero afirma que la Seguridad de los teletrabajadores se ha convertido en uno de los principales objetivos de la Ciberseguridad, mientras que el 47% ha aumentado la inversión en herramientas de colaboración seguras.

El rápido paso al teletrabajo también ha hecho que los empleados envíen más correos electrónicos y compartan más documentos desde sus dispositivos personales que nunca. Las cuestiones que esto plantea para la Ciberseguridad ha llevado a un aumento en el uso soluciones de Transferencia Segura de Archivos como tecnología clave en los últimos meses, según el 64% de los encuestados.

Compartir archivos fuera de una organización puede exponerla a la pérdida de datos y al ransomware, porque los hackers se aprovechan rápidamente de cualquier punto débil del sistema.

Hay muchas soluciones para abordar este desafío, pero la mayoría de ellas bloquean la colaboración en el origen. Aunque esta es una acción segura, también limita las operaciones diarias en gran medida. Esperar a que llegue un archivo importante es frustrante y puede hacer que se pierdan plazos de entrega de proyectos y oportunidades.

Durante la pandemia Covid-19, y en el futuro una vez superada, es importante que las empresas aborden esta cuestión, y que permitan que los empleados puedan colaborar y trabajar de la forma más segura posible.

COVID-19 DESAFÍOS DE CIBERSEGURIDAD EN LA INDUSTRIA DE SERVICIOS FINANCIEROS

Hemos preguntado a los CISOs/CIOs que trabajan en grandes organizaciones de servicios financieros de todo el mundo sobre el impacto que la actual pandemia ha tenido en sus estrategias de Ciberseguridad.

50% Aumentamos la necesidad de automatización para liberar al personal de IT de las tareas manuales

45% Hemos tenido que aumentar la Ciberseguridad con el mismo presupuesto, tecnología y recursos

49% Se aceleraron cambios que ya estaban sobre la mesa, como el paso a Microsoft 365

44% La Seguridad de los teletrabajadores se ha convertido en uno de los principales objetivos de la Ciberseguridad

47% Hemos aumentado la inversión en herramientas de colaboración seguras

36% Las herramientas de Ciberseguridad que teníamos no pudieron adaptarse al cambio en los patrones de trabajo

46% Tuvimos que reevaluar nuestra capacitación y políticas de Ciberseguridad para que reflejaran mejor el aumento del teletrabajo

35% Hemos actualizado nuestras mejores prácticas referidas a cumplir normativas

45% Hemos observado más incidentes de Ciberseguridad desde el aumento del teletrabajo

Acerca de la investigación

Esta investigación fue realizada por la empresa de investigación tecnológica Vanson Bourne, para Clearswift, en agosto y septiembre 2020. Se encuestó a un total de 250 responsables de Ciberseguridad e IT (209 CISOs, 41 CIOs) de grandes organizaciones globales de servicios financieros, 50 en cada uno de estos países: Alemania, Australia, Estados Unidos, Países Bajos y Reino Unido.

REFERENCIAS:

Equifax Hack: Keep Your Friends Close, but Your Supply Chain Closer
https://www.securityweek.com/equifax-hack-keep-your-friends-close-your-supply-chain-closer

British Airways breach: How did hackers get in?
https://www.bbc.co.uk/news/technology-45446529

New Zealand stock exchange halted by cyber-attack
https://www.bbc.co.uk/news/53918580

Magecart: Group behind BA and Ticketmaster breaches is targeting hundreds of sites
https://tech.newstatesman.com/security/magecart-ba-ticketmaster

PCI Security Standards Council
https://www.pcisecuritystandards.org/pci_security/

Stolen data is tracked to hacking at Lockheed
https://www.nytimes.com/2011/06/04/technology/04security.html

5 cybersecurity threats you didn't know you should be threatened by
https://www.clearswift.com/blog/2019/10/21/5-cyber-security-threats-you-didn%E2%80%99t-know-you-should-be-threatened

5 ways to tighten cybersecurity working from home
https://www.goanywhere.com/blog/5-ways-to-tighten-cybersecurity-working-from-home

How to protect your organization from advanced persistent threats
https://www.clearswift.com/blog/2020/09/03/how-protect-your-organization-advanced-persistent-threats

File transfer solutions emerge as key technology for the age of collaboration
https://www.clearswift.com/blog/2020/06/18/file-transfer-solutions-emerge-key-technology-age-collaboration

ICO guide to GDPR
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

helpsystems

www.helpsystems.com

Acerca de HelpSystems

HelpSystems es una compañía de software con foco en las personas, que tiene como objetivo ayudar a las organizaciones a desarrollar una mejor IT. Nuestra suite integral de soluciones de Seguridad y Automatización permite crear una IT más sencilla, inteligente y potente. Organizaciones de más de 100 países y de todos los sectores confían en HelpSystems. Más información en www.helpsystems.com