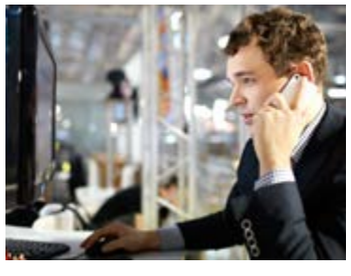
it Digital Security

La publicación electrónica sobre Seguridad Digital que necesitas

Mayo 2018 - nº 8

La seguridad está en tu mano



Las estafas de soporte técnico siguen creciendo

Quest añade capacidades UEBA a su Change Auditor

McAfee Labs Day muestra los últimos avances en seguridad

PCI DDS, la seguridad de los pagos digitales

Movilidad y BYOD, todo un mundo por securizar

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

it Digital Security

Director Rosalía Arroyo
rosalia.arroyo@itdmgroup.es

Colaboradores Hilda Gómez, Arantxa Herranz, Reyes Alonso, Javier San Juan

Diseño revistas digitales Contracorriente
Producción audiovisual Favorit Comunicación, Alberto Varet
Fotografía Ania Lewandowska

it Digital MEDIA GROUP

Juan Ramón Melara juanramon.melara@itdmgroup.es
Miguel Ángel Gómez miguelangel.gomez@itdmgroup.es
Arancha Asenjo arancha.asenjo@itdmgroup.es
Bárbara Madariaga barbara.madariaga@itdmgroup.es

Clara del Rey, 36 1º A · 28002 Madrid · Tel. 91 601 52 92

¿Te avisamos del próximo IT Digital Security?

La seguridad está en tu mano

La seguridad está en tu mano centra nuestra portada de este mes de mayo. En realidad, resulta curioso que pueda ser así, que pueda estar tan cerca, tan a mano. A veces nos complicamos la vida. Puede que sólo baste con tener un backup que funcione y nos permita recuperar lo perdido, robado o cifrado; con cifrar la información, centrarnos en securizar el endpoint, u optar por servicios gestionados de seguridad. ¿Realmente necesitamos un SIEM, controlar los accesos, contar con un SOC, hablar de inteligencia de amenazas, de machine learning de inteligencia artificial…? Un grupo de expertos en seguridad nos contado qué aspectos básicos debe afrontar una empresa para estar segura.

Un mes más seguimos con nuestros #DesayunosITDS, en esta ocasión para hablar de la seguridad de la movilidad y el BYOD. Parece claro que la movilidad está superada, que las empresas la han adoptado para ser más flexibles y más productivas, que los empleados hacen uso de sus dispositivos personales por la misma razón, ¿pero se tiene en cuenta la seguridad? Expertos de ESET, Citrix y Samsung han respondido a la gran pregunta, y propuesto algunas soluciones que nos permitan adoptar la movilidad de una manera segura.

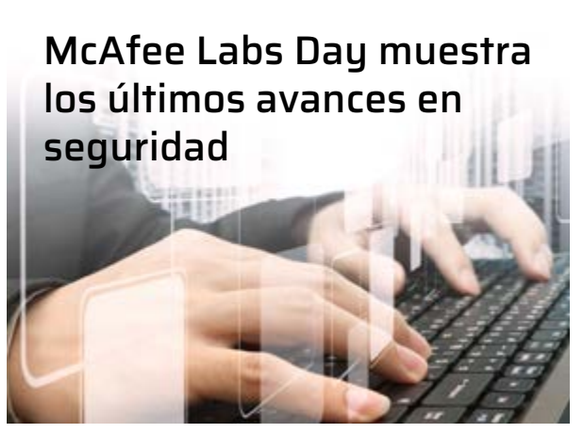
Los temas de actualidad se este número de mayo se han centrado en el McAfee Labs Day celebrado en París, en el que un grupo de periodistas se reunieron con directivos de la firma de seguridad para conocer las últimas novedades del mercado y de la compañía. Quest celebraba un evento en Madrid para anunciar mejoras en su plataforma Change Auditor. Además, nos hacemos eco del último estudio de Microsoft sobre las estafas de soporte técnico, que siguen creciendo.

También incluimos un especial, en esta ocasión de GoNetFPI y sobre PCI DSS, un estándar cuyo objetivo es asegurar que todas las compañías que procesan, almacenan o transmitan información sobre tarjetas de crédito cuenten con un entorno seguro.

¿Te interesa la seguridad? Entonces seguro que te gusta este número de IT Digital Security.

Sumario

Actualidad



McAfee Labs Day muestra los últimos avances en seguridad

Las estafas de soporte técnico siguen creciendo

Webinars ITDS

Quest añade capacidades UEBA a su Change Auditor

Índice de anunciantes

No solo IT

Protegiendo el Dato que salva Vidas

La Auditoria de ciberseguridad, ¿están mis sistemas seguros?

La amenaza del fraude online

Desayunos ITDS

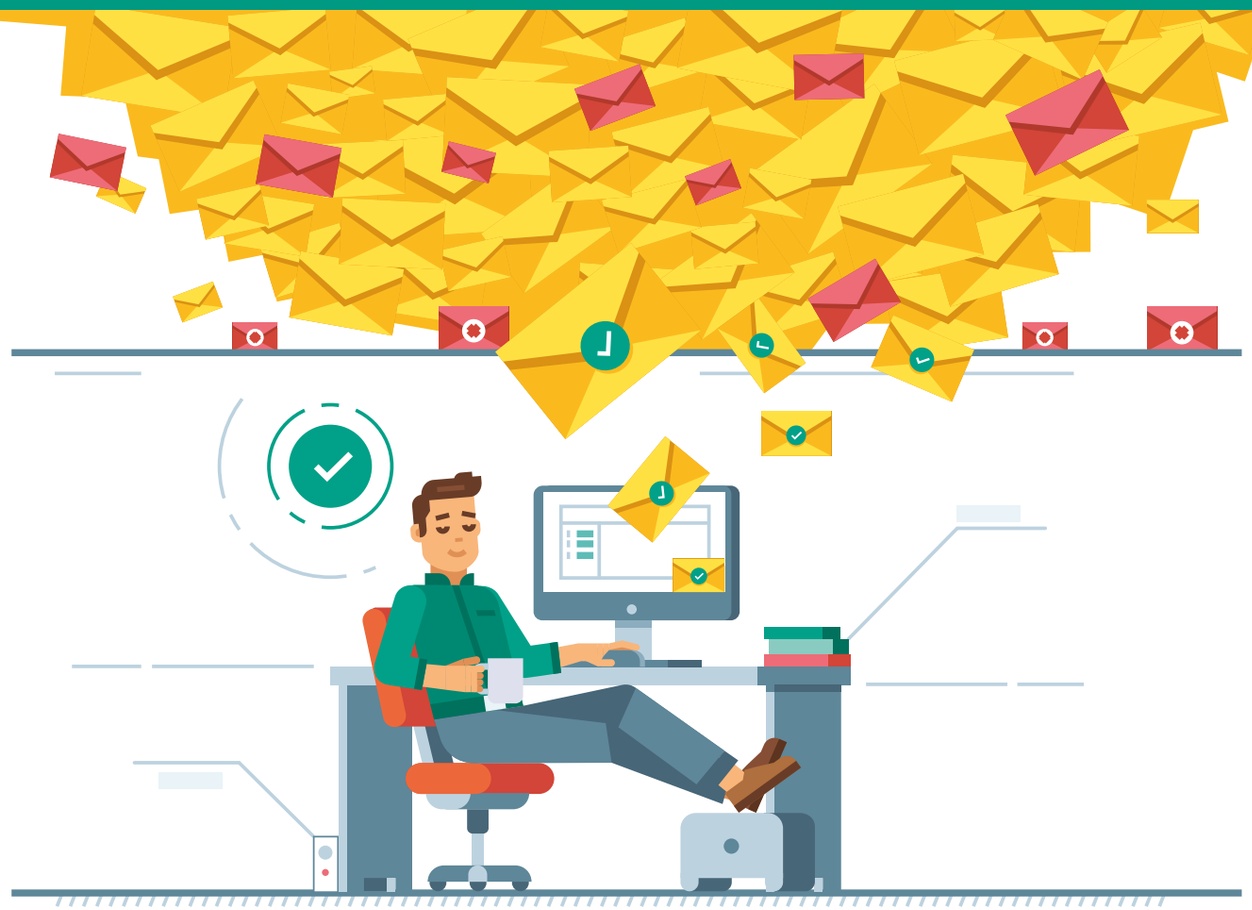
Movilidad y BYOD, todo un mundo por securizar

Especial GoNetFPI

¿Te avisamos del próximo IT Digital Security?

Kaspersky for Business

KASPERSKY lab



3,5 millones de correos electrónicos se envían cada segundo.

Evite que los más peligrosos accedan a su bandeja de entrada.

Elija la protección de correo electrónico de Kaspersky Security for Microsoft Office 365.

Kaspersky® Security for Microsoft Office 365

#TrueCybersecurity
cloud.kaspersky.com

McAfee Labs Day muestra los últimos avances en seguridad

Las amenazas se multiplican a una velocidad aterradora. Este es año del ransomware. Los buenos no son los únicos que explotan el machine learning. Vivimos de crisis en crisis. El sistema de salud está en peligro. Si tienes un problema con la propiedad de los datos, tienes un problema con la propiedad de las ideas. No tenemos ni idea de lo que los fabricantes de móviles están haciendo con nuestros datos. Blockchain redefine las relaciones y el poder del consumidor. La superficie de ataque es cada vez mayor. Hay que colaborar para que la seguridad evolucione. Esto y más es el McAfee Labs Day 2018.

La séptima edición del McAfee Labs Day se celebraba en París con la asistencia de algunos de los ejecutivos más representativos de la compañía y un invitado, Tom Cheesewright, un visionario que habló a los asistentes sobre cómo la vida digital y la conducta de los asistentes virtuales están cambiando.

La séptima edición de este evento ha estado dedicada “a proteger las cosas que importan”, decía Marc Vos, Senior Manager, Worldwide Consumer Reviews, al grupo de periodistas asistentes, a los que en esta edición se pone al día sobre las últimas soluciones del fabricante y la situación del mercado de ciberseguridad.

La primera ponencia de la jornada estuvo a cargo del carismático Raj Samani, McAfee Fellow & Chief Scientist, quién habló sobre una investigación realizada por la compañía en torno a la próxima generación de amenazas. Las áreas de investigación son cada vez más amplias, llegan hasta los hospitales y sus máquinas de electrocar-

diograma. “Todo lo que hacemos está dirigido a que nuestros clientes están seguros”, decía Samani mientras recordaba que el ransomware sigue siendo un problema, que se está convirtiendo en un servicio al que pueden acceder usuarios con cada vez menos conocimientos técnicos pero con capacidad para tener éxito.

El Chief Scientist de McAfee no sólo mencionó la Operación Bacovia llevada a cabo en Rumanía, en la que participaron autoridades de medio mundo para poner fin a una de las redes de ransomware más agresivas de los últimos tiempos utilizando CTB-Locker y Cerber, sino los ataques producidos en los Juegos Olímpicos de invierno, que para Raj Samani fueron una campaña de espionaje.

El futuro pasa por los coches conectados, por eso la compañía cuenta ya con un Automotive Research Center que analiza un mercado muy fragmentado con centenares de empresas de terceros. “En los próximos mese anunciaremos acuerdos con fabricantes”, decía Samani, para después reflexionar que “vivimos de crisis en crisis”. Ahora tenemos la GDPR, la crisis de Facebook, “pero en realidad no tenemos ni idea de lo que los fabricantes de móviles están haciendo con nuestros datos”, aseguraba el directivo.

La seguridad del humano extendido

Presentado como un “futurist speaker”, Tom Cheesewright habló sobre el futuro y sobre cómo cambiará la tecnología con una ponencia titulada “Securing the extended human” en la que planteaba dónde están las fronteras del ser humano.

Reflexionaba Cheesewright sobre la evolución habida en el control de las máquinas. Hemos pasado de instrucciones escritas en un idioma que la máquina pudiera entender al click del ratón, hasta lo táctil “cuando el nivel de intuición creció”. Ahora estamos en el momento de la voz; “los interfaces han

Aunque un 75% de empresas dicen que la seguridad del IoT es importante/prioritaria para sus empresas, el 84% de las organizaciones no están preparadas

evolucionado, y la pregunta que debemos hacernos ahora es, ¿qué es lo siguiente?".

Decía el visionario que ahora somos biónicos, y que, si la fricción con el interfaz cae mucho más, ni siquiera sabremos que están ahí; "el gap entre el humano y la máquina desaparecerá".

La inteligencia artificial está a la orden del día y sus aplicaciones nos permiten obtener respuestas antes siquiera de hacer la pregunta, "extrapolando el dato obtenido en acciones previas". El resultado es un futuro en el que la habrá una realidad mixta.

"El almacenamiento y procesamiento de nuestros datos también es un problema inevitable, lo que genera dudas sobre su propiedad y los derechos que tenemos sobre ellos", decía, Cheesewright, que prevé que el valor que tienen nuestros datos "servirá como una moneda de cambio para la provisión de servicios o la adquisición de bienes".

Cerraba su ponencia asegurando que estamos en una fase de transición "para la cual todavía no estamos preparados adecuadamente". ¿El gran desafío? prepararnos para hacer frente a una nueva realidad, aquella en la que la máquina sea la que llame a tu jefe para decirle que su procesador, el ser humano, está infectado con un virus, decía Tom Cheesewright.

OPERACIÓN BAKOVIA

CLICAR PARA VER EL VÍDEO

Raj Samani, McAfee Fellow & Chief Scientist

Secure Home Platform

Proteger las cosas que importan pasa por proteger el hogar, y hacerlo teniendo en cuenta la idiosincrasia del usuario, que busca que las cosas sean sencillas y no le lleven mucho tiempo. La mayoría de los dispositivos no están fabricados de forma segura, "y cualquier cosa que se conecte a Internet también puede conectarse a las amenazas online", decía Antonio Gaetani, Director Worldwide SHP Partner Solutions.

El planteamiento de McAfee para el hogar conectado no se basa tanto en aplicar seguridad a cada endpoint como establecer un hub al que se conecten todos. La solución es un Secure Home Platform, un router que protege de manera automática toda la red del hogar. "Sabemos que si pedimos a los usuarios que configuren un segundo dispositivo por seguridad probablemente no lo harán", por eso la compañía ha decidido asociarse con otros fabricantes para incorporar en sus soluciones toda la capacidad de su Global Threat Intelligence.

EL ESTADO DE LA SEGURIDAD ENDPOINT

Para descubrir cómo se está desmoronando exactamente la seguridad del punto final y qué están haciendo las organizaciones para solucionarlo, Ponemon Institute realizó una encuesta que indica que estamos en medio de un cambio significativo en la seguridad del punto final. La fe en las soluciones tradicionales, como los programas antivirus que se basan en el escaneo de archivos y la coincidencia de firmas, ha disminuido significativamente frente a las nuevas amenazas sin archivos. La mayoría de las organizaciones están reemplazando o aumentando estas soluciones con nuevas herramientas de seguridad diseñadas para detener ataques sin archivos, aunque muchos siguen siendo escépticos, tales ataques se pueden detener en absoluto.

"Hemos decidido asociados con partners, como D-Link o Arris, y con ISPs, como Telefónica, cuando los usuarios aceptan el router del proveedor", explicaba Gaetani. En cuanto al modelo de negocio, dependerá del partner. En el caso de Arris, se establece un bundle con un servicio basado en suscripción por tres años.

Cada router tiene un agente de McAfee que vigila a qué webs se conectan los dispositivos del hogar. Cuando se detecta un intento de acceso a un site peligroso se envía una alerta de acceso no autorizado al móvil del usuario, que podrá, desde el teléfono, autorizar o denegar dicho acceso. La plataforma también permite establecer controles parentales en todos los dispositivos de la casa, o uno a uno.

La compañía anunciaba durante el Mobile World Congress de Barcelona una nueva opción para su Secure Home Platform. Un skill de Amazon Alexa que permite a los usuarios administrar fácilmente la seguridad de red de su hogar conectado utilizando su voz.

McAfee es una compañía de 30 años con más de 400 millones de usuarios en todo el mundo y más de siete mil empleados. Lo contaba Martin Pevetta, Director WorldWide Consumer Producto Marketing, encargado de hacer un repaso por el portfolio de la compañía, que sigue viendo a los teléfono como una de las principales amenazas. Por eso en breve se lanzará una nueva versión de McAfee Mobile Security, un producto que lleva más de siete años en el mercado.

De manera un poco más específica habló Pevetta de McAfee Safe Connect, un producto diseñado

Gari Davis, Chief Security Evagelist

"para proteger tu privacidad online". Un producto "user centric" que incluye tanto privacidad wifi como capacidad de navegar por internet de manera verdaderamente anónima sin restricciones geográficas.

El futuro de la seguridad

El cierre del evento estuvo a cargo de Gary Davis, Chief Security Evangelist de McAfee, que habló de la situación del mercado y de nuevas amenazas, revisando los eventos que han generado titulares, y cómo hay podemos hablar del típico ciberdelincuente u organización que lo que quieren es ganar

Enlaces de interés...

- McAfee quiere asegurar el cloud con su CASB Connect Program
- El machine learning y el ransomware marcarán la ciberseguridad de 2018
- McAfee Secure Home Platform
- McAfee Safe Connect

El valor que tienen nuestros datos servirá como una moneda de cambio para la provisión de servicios o la adquisición de bienes

dinero, pero también de otros actores, como las naciones estado o los hacktivistas, que tienen otras motivaciones.

Es el año del ransomware, decía el evangelista de McAfee, apuntando también a que el machine learning no sólo lo utilizan los buenos, sino “los enemigos para soportar sus ataques y aprender de las respuestas defensivas, de los modelos de detección, y para detectar vulnerabilidades mucho más rápido que antes”.

El futuro también nos depara batallas entre bots, un Mirai vs Reaper, una mayor velocidad de los ataques y el riesgo de los coches conectados. Existe una realidad de negocio, decía también Davis, y es que, aunque un 75% de empresas dicen que la seguridad del IoT es importante/prioritaria para sus empresas, el 84% de las organizaciones no están preparadas.

El evangelista de McAfee llamaba a la acción “para tener la seguridad en cuenta desde el inicio, mejorar la educación, desarrollar estándares que funcionen en todos los ecosistemas y colaborar en la forma de asegurar que la seguridad evolucione”.

La sesión finalizó con Marc Vos anunciando que el próximo McAfee Labs Day que se celebre en Europa será en Portugal.

Compartir en RRSS

TREND MICRO™

POWERED BY XGen™ SECURITY

Detectar y prevenir las brechas a la velocidad del rayo

Su compañía se encuentra en el punto de mira de una variedad cada vez más compleja de amenazas: ransomware, amenazas avanzadas, ataques dirigidos, vulnerabilidades y exploits.

Solo la visibilidad completa de todo el tráfico y actividad de la red situará la seguridad de su red por delante de los actuales ataques específicamente diseñados que eluden controles tradicionales, explotan las vulnerabilidades de red y secuestran o roban datos confidenciales, comunicaciones y propiedad intelectual.

Trend Micro Network Defense detecta y evita las infracciones a la velocidad del rayo en cualquier lugar de su red para proteger sus datos críticos y su reputación.

Capacidad probada

Trend Micro Deep Discovery:
Sistema de Detección de Brechas "Recomendado" con 4 años consecutivos con tasas de detección del 100%.

Trend Micro TippingPoint:
Sistema de Prevención de Intrusiones de Última Generación "Recomendado" y 99,6% de efectividad de seguridad.

NSS LABS RECOMMENDED

Inteligencia de amenazas líder del sector

TREND MICRO SMART Protection Network™

TELUS®

Web App Digital Vaccine BY TippingPoint

ZERO DAY INITIATIVE

www.trendmicro.es

Quest añade capacidades UEBA a su Change Auditor

La detección de actividad sospechosa por usuarios deshonestos es un desafío difícil que Quest quiere afrontar con Change Auditor Threat Detection, un nuevo módulo para su Change Auditor que utiliza machine learning avanzada, analítica de conducta de entidades y usuarios (UEBA) y tecnologías de correlación.

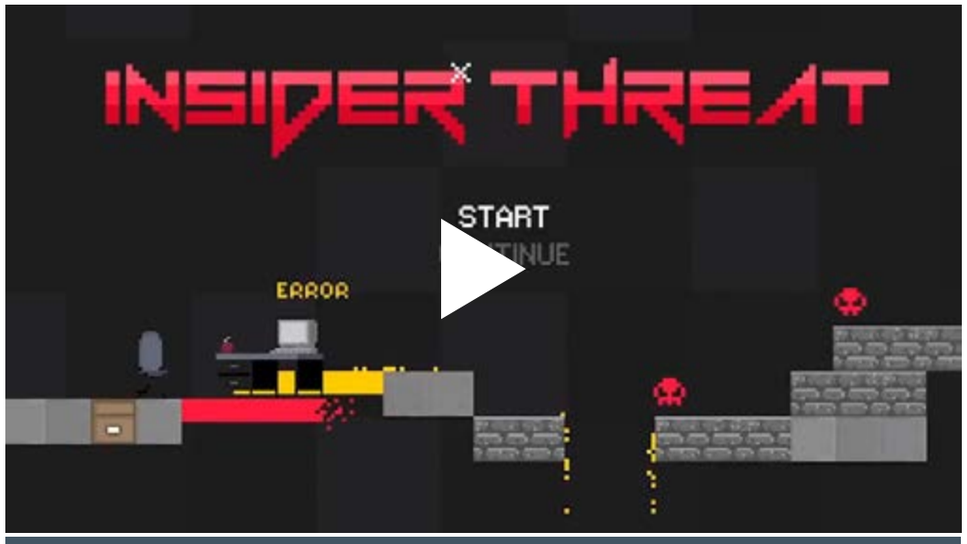
Cómo tener la mejor arquitectura para proteger mejor mi empresa y hacer frente a GDPR. Desvelar este gran secreto fue la labor de Isaac Forés, encargado además de arrancar un evento que reunía hace unas semanas en Madrid a varias decenas de profesionales de TI en torno a la propuesta del fabricante de seguridad y de GDPR.

Hacía Forés referencia a algunas cifras que aseguraba son emblemáticas, como los diez millones de ciberataques que recibe Microsoft Azure cada día; los 191 días que, de media, tardan las empre-

sas en conocer la existencia de una brecha de seguridad; y cien, un número mágico porque representa el porcentaje de crecimiento de la compañía en el último año “de lo que os vamos a enseñar”.

Las amenazas son reales, pero la mayoría proceden de dentro, por eso las soluciones de UEBA, o de comportamiento de entidades y usuarios, ganan cada vez más tracción. De igual manera que la gestión de identidades es capaz de saber quién accede a qué y con qué permisos, UEBA quiere poder detectar conductas anómalas que hagan saltar las alarmas, y no sólo sobre el comportamiento de un empleado o usuario, sino de una máquina.

En todo caso UEBA no es una novedad. La tecnología lleva circulando desde hace unos años por el mercado, pero su interés no deja de crecer.



ACABA CON LOS ‘GRANUJAS’ GRACIAS A QUEST CHANGE AUDITOR THREAT DETECTION — CLICAR PARA VER EL VÍDEO

De hecho, según Gartner las ventas de soluciones de UEBA independientes se están duplicando cada año y el año pasado ya alcanzaron los 200 millones de dólares. Se sabe además que muchos vendedores están incorporando capacidades de UEBA en otras soluciones de seguridad, como los SIEM (Security Information and Event Management), IAM (Identity and Access Management), seguridad endpoint, tráfico de red o herramientas de DLP (Data Lost Prevention). Es el caso de Quest, que presentaba durante el evento Change Auditor Threat Detection, un nuevo módulo de Change Auditor, que cuenta con otros doce, como Change Auditor for Active Directory o Change Auditor for SQL Server.

A cargo de la presentación de este nuevo módulo estuvo César Moro, Sales Consultant en Quest Software, quien aseguraba que el coste medio para las organizaciones a nivel mundial de un ciberataque es de 3,62 millones de dólares; el que 70% de los empleados tienen privilegios excesivos dentro de la organización, tanto

Quest, una vida en constante evolución

La evolución de Quest software es de libro y por poderes. La compañía cumplió 30 el año pasado, toda una vida que le ha valido para comprar un buen puñado de compañías y hacerse hueco en el mercado con una amplia oferta de soluciones y herramientas para la gestión de bases de datos –donde se inició, infraestructuras Microsoft, monitorización de servicios para el usuario final (gama de productos Foglight), gestión de aplicaciones, y gestión de entornos virtualizados tanto de servidores como de escritorios.

La compañía tardó diez años en salir del mercado norteamericano. Y a partir de ese momento fue todo correr. En 1997 abrió una oficina en Reino Unido y un año después lo hacía en Alemania y Australia, al tiempo que adquiría su primera compañía, TOAD, en 1998, tan sólo un año antes de salir a Bolsa y adquirir Stat, adentrándose en el mercado de gestión de cambio de aplicaciones.

A comienzos del 2000 Quest avanza hacia el mercado de gestión de aplicaciones con la compra de Foglight, un producto de monitorización, para seguir con su proceso de expansión en Francia y Holanda. A finales de año ya contaba con más de 1.400 empleados, ingresos de 167 millones de dólares y una nueva compra: Fastlane Technologies, que permite a la compañía adentrarse en el mercado de gestión de Microsoft y ampliar su oferta en el mercado de bases de datos más allá de Oracle con un producto para IBM DB2.

Dos años más le valen a la compañía para abrir oficina en Japón y realizar una nueva compra, Sitraka, con la que sigue ampliando su oferta de gestión de aplicaciones, esta vez hacia el mercado de aplicaciones web escritas en Java.

Los años siguientes reafirman la apuesta de Quest por el mercado de Microsoft SQL Server. No sólo es considerada por IDC como el principal referente de software de gestión de bases de datos distribuidas y uno de los principales vendedores de soluciones de gestión de aplicaciones, sino que sigue con su programa de adquisiciones: Aelita Software; Imceda Software, con la que añade capacidades de backup y recuperación a SQL Server y Vintela, para la gestión de identidades. Corre ya el año 2005 y Quest Software tiene 2.750 empleados e ingresos de 476 millones de dólares.

En 2006 la compañía entra en el mercado de SharePoint y realiza dos adquisiciones: ScriptLogic para poder acercarse a la pyme y la checa Charonware creadores de CASE Studio2, tecnología que incluyó en TOAD Data Modeler. En 2007 la compra es Provision Networks, empresa de gestión de virtualización de escritorio, y en 2008 las de Vizioncore, con la que se adentra en el mercado de virtualización de servidor, y PassGo Technologies. La adquisición de PacketTrap para la monitorización de red se produce en 2009 y un año después le siguen Voelcker, para reforzar su oferta de gestión de identidades, y Surgient para el mercado de automatización.

Sigue la pasión por las compras y en 2011, con 3.500 empleados y una facturación de 767 millones de dólares, adquiere BakBone Software, e-DMZ, RemoteScan, Symlabs, ChangeBASE, vKernel y BiTKOO.

La carrera en solitario se acaba en 2012, cuando Dell anuncia la compra de Quest, una aventura que acaba en noviembre de 2016, cuando es vendida a Francisco Partners y Elliott Management y vuelve a ser relanzada al mercado como Quest.

Mayo 2018

como para que un 55% genere más de la mitad de los ataques que sufre una organización.

Frente a estas cifras, otras casi peores, porque el número de alertas que se generan diariamente es de 50.000. “Nadie es capaz de procesar esta cantidad”, aseguraba César Moro, añadiendo que el 44% de esas alertas quedan desatendidas.

¿Te avisamos del próximo IT Digital Security?

Change Auditor y Directorio Activo

La amenaza interna contra Active Directory (AD) es real, generalizada y costosa. El predominio de AD en empresas de todo el mundo lo convierte en un blanco atractivo, por eso monitorizar los registros de eventos de AD es un comienzo, pero muchas amenazas internas se aprovechan de los even-

it whitepapers

NUEVE BUENAS PRÁCTICAS PARA LA SEGURIDAD DEL DIRECTORIO ACTIVO

Debido a que Active Directory (AD) es el principal directorio de autenticación y autorización para más del 90% de las empresas del mundo y alrededor de 500 millones de cuentas de usuario activas, es un objetivo común para los ciberataques. De hecho, más de 95 millones de cuentas de Directorio Activo están bajo ataque cibernético a diario. Aunque no existe un enfoque estricto para la seguridad del AD, las organizaciones pueden tener en cuenta algunas prácticas, como las nueve que se plantean en este documento.

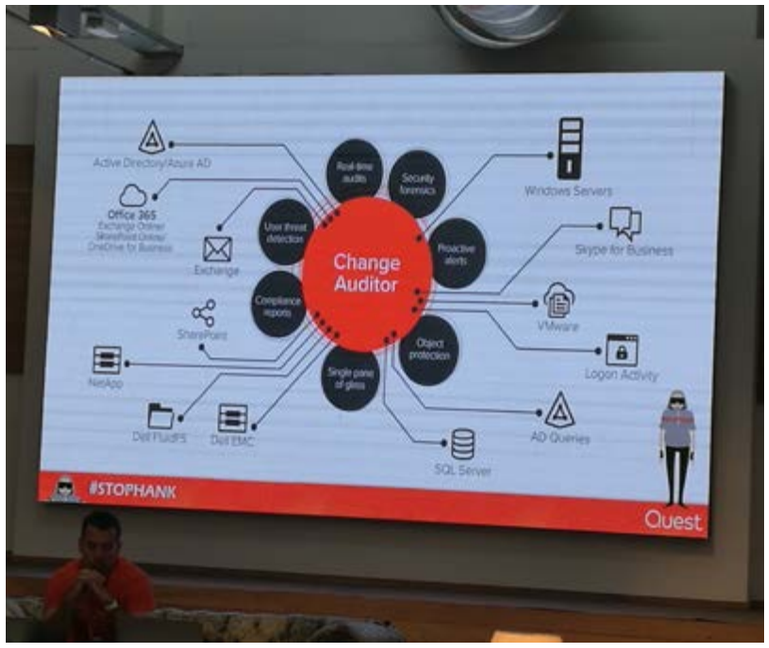
tos de AD que no se registran. Además, la lista de elementos que hay que buscar en un ataque sospechoso es larga, y no hay una forma automática de protegerse contra todos.

Change Auditor es la propuesta de Quest para la elaboración de una auditoría del área de TI en tiempo real, un análisis forense y una monitorización integral de la seguridad, incluido un seguimiento en detalle de las actividades del usuario durante los inicios de sesión, las autenticaciones y otros servicios clave de las empresas a fin de mejorar la detección de las amenazas.

> Es imposible vivir sin cuentas privilegiadas, de ahí la importancia de su gestión para minimizar el riesgo y evitar brechas de seguridad

Change Auditor Threat Detection es un nuevo módulo de la solución, capaz de analizar los logs recogidos por el resto de los módulos y que permite "detectar anomalías gracias a la correlación inteligente de eventos", explicaba César Moro, quien destacaba entre sus ventajas los marcadores de riesgo multivariados, que tiene en cuenta con sólo los marcadores del evento en sí, sino que agrupan eventos similares (marcadores de Indicador) para poder identificar anomalías durante un periodo de tiempo prolongado, además, los indicadores y eventos calificados son agregados en alertas y vueltos a calificar de nuevo teniendo en cuenta la singularidad de su composición; por últimos, alertas, categorizadas por severidad, son sumadas para formar una calificación simplificada del riesgo de usuario.

Quest Change Auditor Threat Detection utiliza Aprendizaje Automático Avanzado, análisis de comportamiento de entidades y usuarios (UEBA) y tecnología de correlación para detectar con precisión actividades anómalas e identificar a los usuarios de mayor riesgo. El resultado es contar con una herramienta capaz de identificar amenazas ya que "gracias a la correlación, sólo un conjunto de eventos lanza una alerta", lo que además reduce los falsos positivos. ¿Casos de uso de este nuevo componente? Ataques de fuerza bruta, filtración de datos, suplantación de usuarios, actividad anormal del directorio activo, elevación de privilegios…



Change Auditor Threat Detection analiza los logs recogidos por el resto de módulos de Change Auditor para detectar anomalías gracias a la correlación inteligente de eventos

Raúl Dopazo, IAM Solution Architect de One Identity, compañía perteneciente a Quest Software y experta en gestión de identidades y accesos, decía durante su intervención que el usuario sigue siendo el eslabón débil pero que al mismo tiempo "es imposible vivir sin cuentas privilegiadas", de ahí la importancia de su gestión "para minimizar el riesgo y evitar brechas de seguridad".

Habló el ejecutivo de One Identity Safeguard y de One Identity Unified Access Management. Sobre el primero explicó que los ciberdelincuentes buscan la manera de acceder a las cuentas privilegiadas, "ya que proporcionan acceso ilimitado a sistemas y datos" y que la gestión de Active Directory requiere control y protección contra errores humanos. "En casi todas las brechas recientes de alto perfil, se han explotado los fallos en la gestión de cuentas privilegiadas", y por eso es tan importante contar con una forma "segura, eficiente y compatible de proporcionar acceso a cuentas privilegiadas".

One Identity Safeguard es una de las propuestas, en modo appliance, lo que simplifica la implementación y la administración. Entre sus ventajas, el poder aprovechar un motor de políticas unificado y herramientas de administración para garantizar el acceso seguro a contraseñas y sesiones privilegiadas. El dispositivo Safeguard está diseñado específicamente para usar con el software Safeguard, que está preinstalado y listo para su uso inmediato. El dispositivo está reforzado para garantizar que el sistema esté asegurado en el hardware, sistema operativo y niveles de software. Este enfoque protege el software de administración privilegiado de los ataques al tiempo que simplifica la implementación y la administración.

Enlaces de interés...

- One Identity, parte de Quest, adquiere Balabit
- Desayuno ITDS - Recuperación ante desastres, ¿estás preparado?

Únete a la nueva experiencia en ciberseguridad

Solución todo en uno frente a ciberamenazas

- Amplia oferta de servicios antifraude y de ciberseguridad de vanguardia para proteger tu negocio
- Servicio personalizado a las características del cliente y 100% gestionado por un equipo experto de primer nivel
- Avalados por los resultados en clientes globales y nuestras alianzas tecnológicas con prestigiosas compañías.

GoNet

Fraud Prevention & Intelligence

Las estafas de soporte técnico siguen creciendo

¿Por qué buscar la manera de atacar un sistema, algo tecnológicamente más complicado, cuando se puede acceder a través de ingeniería social? Contar con las mejores tecnologías de seguridad y las plataformas más robustas a veces no es suficiente cuando la picaresca entra en juego.

Las estafas de soporte técnico están creciendo, al menos en lo que a Microsoft se refiere. Asegura la compañía que este tipo de actividades creció un 24% en 2017 respecto al año anterior.

Microsoft ha creado la versión más segura de su plataforma en Windows 10. Diferentes tecnologías hacen que los exploits, el malware y otras amenazas que buscan infec-

Cómo identificar una estafa de soporte técnico

- Recuerde que las empresas legítimas de atención al cliente, seguridad o soporte técnico no inician contacto no solicitado con personas.
- Tenga cuidado con los números de soporte al cliente obtenidos a través de la búsqueda de código abierto. Los números de teléfono incluidos en una sección de resultados "patrocinados" probablemente se hayan mejorado como resultado de la publicidad en el motor de búsqueda.
- Reconozca intentos fraudulentos y cese toda comunicación con el criminal.
- Resista la presión para actuar rápidamente. Los delincuentes instarán a la víctima a actuar rápidamente para proteger su dispositivo. Los delincuentes crean un sentido de urgencia para generar miedo y atraer a la víctima a una acción inmediata.
- No otorgue acceso remoto a dispositivos o cuentas a personas desconocidas o no verificadas.
- Debido a que algunas víctimas informan que su software antivirus proporcionó advertencias antes de un intento de estafa, asegúrese de que toda la protección de seguridad del ordenador esté actualizada.

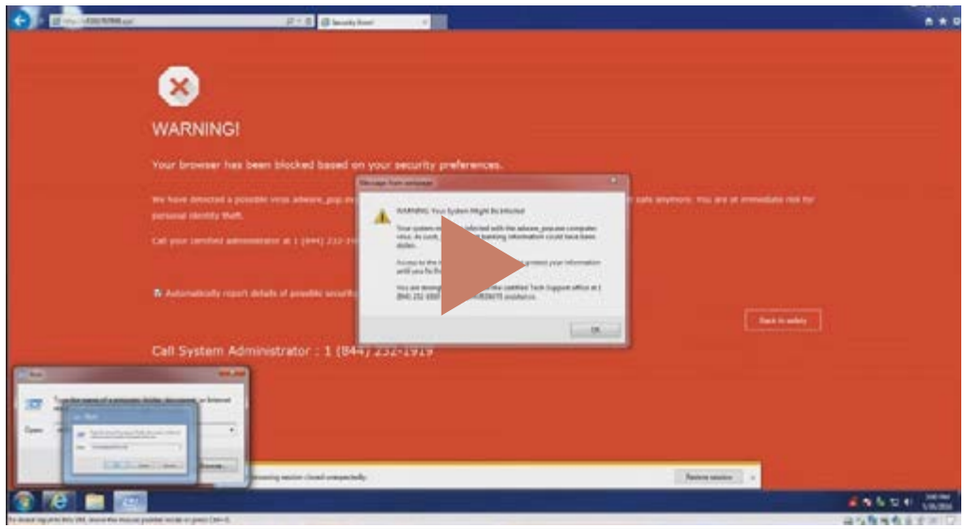
tar los dispositivos sean más difíciles de ejecutar. Cada día el machine learning y la inteligencia artificial utilizadas en Windows Defender ATP protegen millones de dispositivos de ser víctimas de ciberataques. Incluso una configuración especial hace que sólo las aplicaciones de Microsoft Store se ejecuten en Windows 10, lo que limita la cantidad de ataques que se pueden recibir.

Es decir, atacar Windows 10 es mucho más difícil desde el punto de vista técnico. "A veces puede ser más fácil convencer a los usuarios para que compartan voluntariamente sus contraseñas, información de cuenta o para instalar aplicaciones peligrosas en sus dispositivos que desarrollar malware y robar información sin que se note", dice Erik Wahlstrom Windows Defender Research Project Manager, en un post en el que habla de la guerra de las estafas del soporte técnico.

Microsoft recibió cerca de 153.000 informes de clientes que fueron víctimas de una estafa. Un 15% admitieron haber pedido dinero, entre 200 y 400 dólares de media. Un usuario holandés dijo haber perdido 89.000 euros en una estafa de soporte técnico.

> En los últimos años, los estafadores de soporte técnico han comenzado a dirigir sus actividades contra usuarios de Mac y Linux, y a hacerse pasar por representantes de todo tipo de empresas

La ingeniería social continúa siendo la clave de este tipo de actividades. Las estafas están diseñadas para engañar al usuario y hacerles creer que sus dispositivos están comprometidos o dañados, coaccionando a las víctimas para que adquieran servicios de soporte innecesarios.



ESTAFA DE UN FALSO SOPORTE TÉCNICO — CLICAR PARA VER EL VÍDEO

¿Te avisamos del próximo IT Digital Security?

Dos de cada tres encuestados han experimentado algún tipo de estafa de soporte técnico en los últimos doce meses, con casi uno de cada diez perdiendo dinero

Lógicamente las estafas de soporte técnico no son exclusivas de Microsoft. Datos del FBI Internet Crime Complaint Center (IC3) recoge más de 11.000 denuncias de este tipo de estafas, un 86% más si se compara con el año anterior. Según el FBI los estafadores lograron robar casi 15 millones de dólares en 2017.

Volviendo a Microsoft, una encuesta realizada por la compañía en 2016 desveló que dos de cada tres habían experimentado algún tipo de estafa de soporte técnico en los últimos doce meses, con casi uno de cada diez perdiendo dinero.

El plan de ataque de una estafa se inicia con una llamada telefónica que da paso a la instalación de herramientas de administración remota, la identificación de una amenaza falsa en el dispositivo de la víctima, a quien se le engaña para que compre un soporte faso. Los estafadores inician sus actividades de ingeniería social de diferentes maneras, según Erik Wahlstrom:

TRUST HACKING, LA SEGURIDAD DE INTERNET

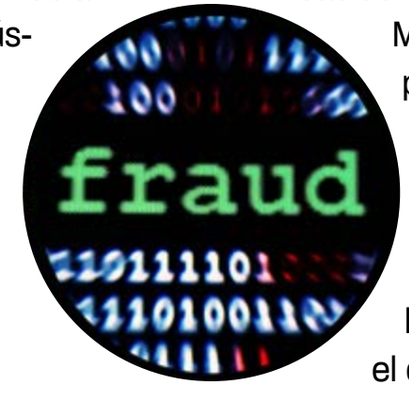
Para este informe, los investigadores de Menlo Security analizaron los principales 100.000 dominios clasificados por Alexa para comprender los riesgos inherentes al uso de los sitios web más populares del mundo, encontrando evidencias de que los ciberdelincuentes están explotando con éxito las medidas de confianza, como la reputación de un sitio en particular o la categoría en la que se incluye el sitio, para evitar la detección y aumentar la efectividad de sus ataques.

Enlaces de interés...

- La guerra contra las estafas de soporte técnico
- FBI. Tech Support Fraud
- Cómo reconocer y evitar una estafa de soporte técnico

La ingeniería social continúa siendo la clave de las estafas de soporte técnico

- **Sitios web falsos** que utilizan varias tácticas, incluido el lanzar falsas alertas y mensajes de error a pantalla completa. Los estafadores conducen a las posibles víctimas a estos sitios web a través de anuncios, resultados de búsqueda, etc.
- **Campañas de correo electrónico** que usan técnicas similares a las de phishing para engañar a los destinatarios y que hagan clic en las URL o abran archivos adjuntos maliciosos.



- **Malware** que está instalado en los ordenadores para realizar cambios en el sistema y mostrar mensajes de error falsos
- **Llamadas telefónicas no solicitadas** que pretenden ser del equipo de soporte de un proveedor.

Microsoft también señala que las estafas de soporte técnico no son un problema exclusivo de los usuarios de Windows. En los últimos años, los estafadores de soporte técnico han comenzado a dirigir sus actividades contra usuarios de Mac y Linux, y han comenzado a hacerse pasar por representantes de todo tipo de empresas, no solo fabricantes de sistemas operativos, sino fabricantes de antivirus, proveedores de servicios de Internet o empresas de telecomunicaciones.

Mientras Microsoft continúa ayudando a proteger a los clientes a través de una plataforma reforzada y con soluciones de seguridad cada vez mejores, “creemos que ya es hora de que la industria se una y ponga fin al problema de la estafa de soporte técnico”, concluye el dirctivo de la compañía.

BE SURE TO BE FREE

BLINDA TUS "SUPERCONFIDENCIAL"

#BlindaTuLibertad

Garantiza que lo que pasa en tu empresa se queda en la empresa.
Descubre lo último en ciberseguridad empresarial.

www.eset.es

ESET

ENJOY SAFER TECHNOLOGY™

PCI DSS, la seguridad de los datos de los pagos digitales a tu alcance

GoNet
Fraud Prevention & Intelligence

PCI DSS, la seguridad de los datos de los pagos digitales a tu alcance

Los sistemas de pagos online evolucionan casi a la misma velocidad que se adoptan e implementan. El uso de dispositivos móviles ha incrementado la preocupación sobre la seguridad de los pagos digitales, especialmente en lo que a la privacidad y confidencialidad de la información financiera se refiere.

Cada día se realizan ingentes cantidades de operaciones financieras a través de internet, no sólo compras, sino pagos de facturas y todo tipo de transacciones bancarias. Todas estas operaciones crean una gran cantidad de datos confidenciales que se deben proteger, por eso la implementación segura de un sistema

¿Te avisamos del próximo IT Digital Security?

PCI DSS, la seguridad de los datos de los pagos digitales a tu alcance

La normativa PDI DSS se aplica a cualquier organización, independientemente del tamaño o número de transacciones, que acepte, transmita o almacene datos de tarjetas de crédito

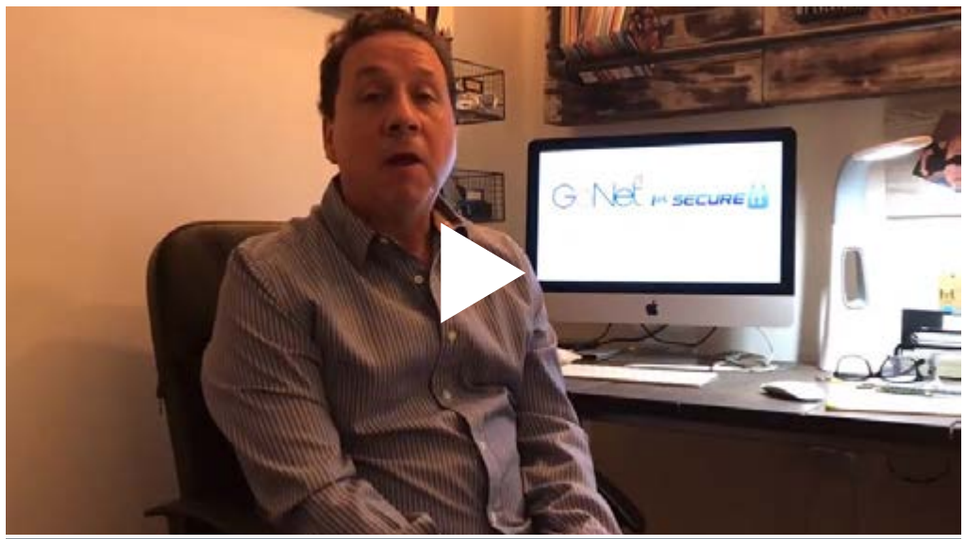
de pago de comercio electrónico debe incluir la posibilidad de identificar robos y todo tipo de fraudes online.

Precisamente el que los casos de fraude con las tarjetas de pago crecieran de forma alarmante fue lo que llevó en 2006 a las empresas de tarjetas más importantes, como American Express, Discover, JBC, Mastercard y VISA, a unirse para crear el PCI-SSC (Payment Card Industry – Security Standard Council), que sirvió para la creación del estándar conocido como PCI-DSS (Payment Card Industry – Data Security Standard), que no es otra cosa que un conjunto de requerimientos cuyo objetivo es asegurar que todas las compañías que procesan, almacenan o transmitan información sobre tarjetas de crédito cuenten con un entorno seguro.

Se entiende por información de tarjeta el número PAN completo (es el número de 16 dígitos que se encuentra al frente de la tarjeta), el nombre del propietario de la tarjeta, la fecha de expiración y el código de servicio (código de 3 o 4 dígitos que se encuentra en la banda magnética). En todo caso, adicionalmente son considerados datos sensibles el código de seguridad (CVC o CVV), la información completa de la banda magnética (o el equivalente en las tarjetas chip) y los PINs, ya que estos datos son los que se utilizan como códigos de autenticación para autorizar las transacciones de pago.

Muchos comercios creen que la implantación de sistemas de pago tokenizados, o que cumplen la norma P2PE, les exime del cumplimiento de la normativa, cuando no es así, aunque esto facilita mucho el cumplimiento. Las verticales objetivo de cumplir con PCI DSS son: Retail (online/offline); Call centers (solo aquellos que acepten pagos por teléfono o email); Banca (aquellos que trabajen con comercios); Finanzas; Agencias de viajes (obligado cumplimiento desde el 1 de marzo de 2018); Proveedores de medios de pago y afines.

PCI DSS, la seguridad de los datos de los pagos digitales a tu alcance



En todo caso, la normativa PDI DSS se aplica a cualquier organización, independientemente del tamaño o número de transacciones, que acepte, transmita o almacene datos de tarjetas de crédito. Lo que sí que varía es el modo en que el cumplimiento es auditado, en función de la cantidad de transacciones anuales que la organización realice. Se establecen cuatro niveles, siendo el primero el asociado a todas las organizaciones que procesen más de seis millones de transacciones anuales, que serían auditadas por una empresa auditora habilitada por el consorcio PCI.

Cumplir con los estándares de seguridad PCI puede parecer una tarea desalentadora, pero el cumplimiento es cada vez más importante y puede no ser tan problemático si se cuenta con las herramientas y, por supuesto, con los socios y los asesores adecuados. Además, el coste de no cumplir con la normativa se ha disparado y puede suponer una cantidad muy elevada. Un reciente estudio elaborado por Ponemon Institute y titulado The True Cost of Compliance with Data Protection Regulations, recoge que los costes en los que puede incurrir una empresa que no cumpla con normativas relacionadas con la protección de datos ha crecido un 45% respecto a 2011, alcanzando los 14,82 millones de dólares anuales. Por otra parte, y aunque la mayoría de encuestados hicieron referencia a GDPR, un 55% consideró que el Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago es un desafío.

Adoptar PCI DSS no sólo evita problemas de incumplimiento normativo, sino que ofrece una serie de ventajas:

- La primera y principal es que los sistemas son seguros y los clientes pueden confiar la empresa.
- Mitigar los riesgos asociados a un posible compromiso de la información de cuentas o titulares de tarjetas, reduciendo los costes legales y el impacto negativo en la imagen.

El número de españoles con al menos una tarjeta en su posesión alcanzó en 2017 al 82% de la población

PCI DSS, la seguridad de los datos de los pagos digitales a tu alcance

¿Qué preocupa a los clientes?

Los tres problemas a los que se enfrentan los clientes a la hora de cumplir con la normativa PCI DSS y que la solución de GoNetFPI y 1st Secure IT resuelve son:

- MINIMIZAR EL ALCANCE DE LA NORMATIVA PARA SU ENTORNO IT, lo que implica reducir tanto económica como temporalmente el proceso de certificación.
- MINIMIZAR LA EXPOSICIÓN A POSIBLES BRECHAS DE SEGURIDAD, lo que reduce significactivamente el riesgo de aparecer en medios de comunicación y por tanto la erosión de su imagen en el mercado.
- POSIBLES SANCIONES POR EL INCUMPLIMIENTO DE LA NORMA por parte de las marcas y tarjetas (VISA, Mastercard, JCB, Discover y AMEX).

- El cumplimiento de PCI mejora su reputación no sólo de cara a los compradores, sino a las marcas de pago.
- El cumplimiento de PCI es un proceso continuo que ayuda a prevenir las violaciones de seguridad y el robo de tarjetas de pago, ahora y en el futuro.
- Seguir los estándares de PCI DDS ayuda también a estar cerca de cumplir con otras regulaciones adicionales, como HIPAA o SOX.
- El cumplimiento de PCI contribuye a las estrategias de seguridad corporativas.
- El cumplimiento de PCI probablemente conduzca a mejorar la eficiencia de la infraestructura de TI.
- En el caso de los proveedores de servicios, el cumplimento de PCI DSS constituye un elemento diferenciador que puede suponer una ventaja competitiva en el mercado.
- La implementación de buenas prácticas de seguridad en la compañía recogidas en la norma.

Los grandes retos de PCI DSS

Aunque todos los comerciantes y proveedores de servicios que almacenan, procesan o transmiten datos de titulares de tarjetas deben cumplir con el estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS), la realidad es que muchos no lo hacen. De hecho, los datos muestran que las empresas inicialmente cumplen entre el 18% a 24% de la norma.

A veces el problema está en el alcance de la propia norma. El estándar tiene 243 requisitos numerados y 330 requisitos de prueba que todos los comerciantes deben cumplir. La mayoría de las organizaciones que admite IT Governance están clasificadas como Visa o MasterCard Nivel 3 o Nivel 4 para fines de informes. Estas organizaciones generalmente informan de su cumplimiento mediante un cuestionario de autoevaluación (SAQ). Si bien el objetivo de los SAQ es simplificar el proceso de notificación de cumplimiento, a menudo las compañías tienen dificultades para cumplimentarlo. También suelen subestimar qué partes de su entorno deben cumplir y cómo proteger esos sistemas.

Otro de los principales problemas es la conciencia de seguridad continuada. La protección de datos no se trata solo de usar cifrado, firewalls y software antivirus. También se trata de un proceso continuo de monitorización, de mantenimiento y gestión de la configuración, de administración de identidades, registro, escaneo y pruebas continuas. Lo que queremos decir con esto, es que muchas organizaciones no cumplen con los requisitos porque no reconocen la importancia de realizar pruebas regulares. Y hay que recordar que el requisito 11 de PCI DSS descri-

PCI DSS, la seguridad de los datos de los pagos digitales a tu alcance

be la necesidad de llevar a cabo pruebas periódicas para identificar problemas de seguridad no abordados.

Otro de los retos de la normativa es la necesidad de realizar una revisión diaria de los eventos y registros de seguridad, como pueden ser las cuentas y actividad de las personas asociadas con la información de la red, establecido en el requisito 10.6.1. Mantener soluciones de registro puede hacer que el porcentaje de cumplimiento con PCI de una organización se reduzca, ya sea por restricciones técnicas, presupuestarias o de recursos humanos. En todo caso, no significa que el estándar pueda ser ignorado, entre otras cosas porque las organizaciones que no cumplen con los requisitos podrían incurrir en fuertes multas. Para evitar esto, las organizaciones deben reconocer los desafíos de cumplir con las PCI DSS y encontrar la manera de superarlas.

> Muchos comercios creen que la implantación de sistemas de pago tokenizados, o que cumplen la norma P2PE, les exime del cumplimiento de la normativa, cuando no es así

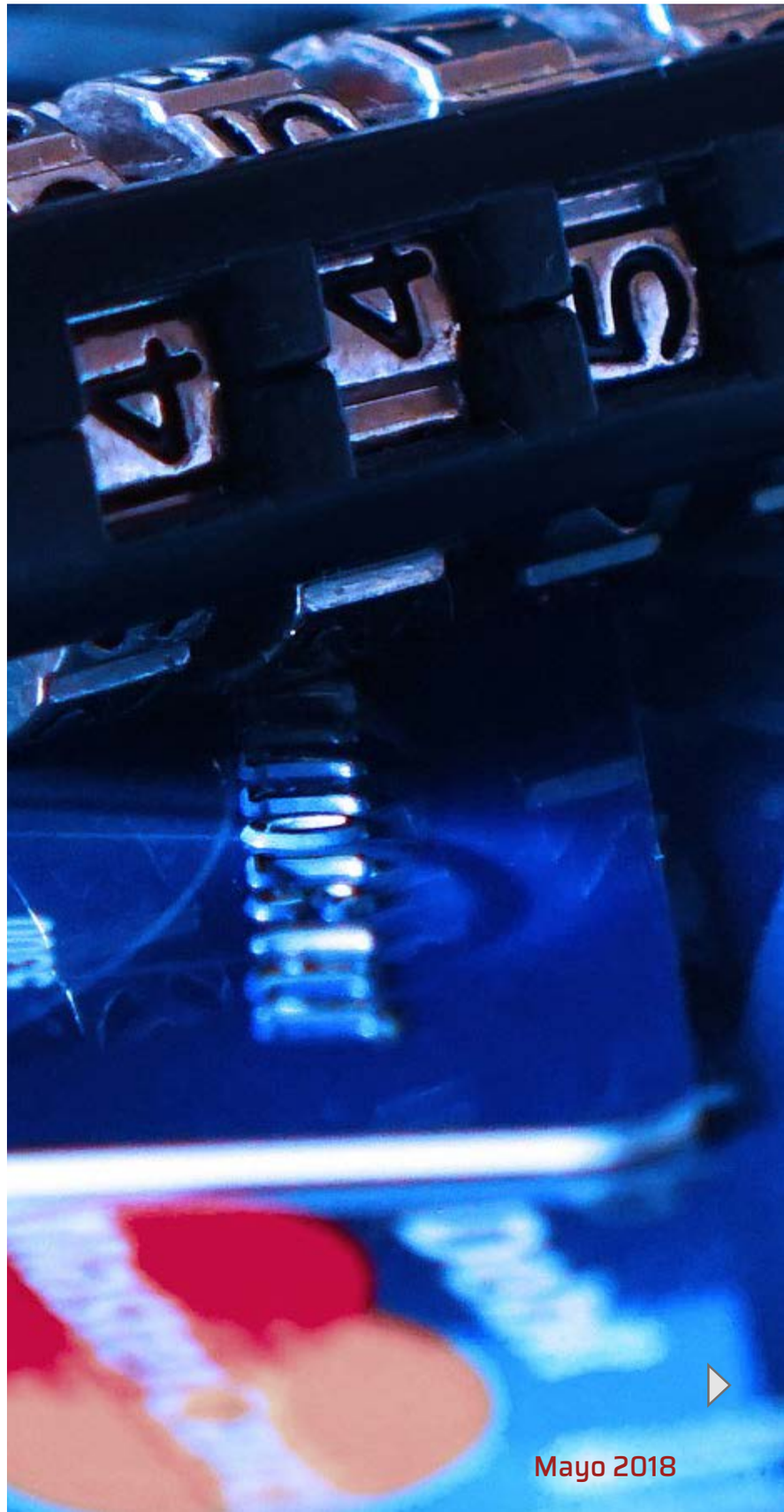
Proteger los datos almacenados de las tarjetas es otro gran reto para muchas empresas. Decíamos que, como mínimo, el estándar requiere que el número de cuenta principal (PAN) se vuelva ilegible en cualquier lugar donde esté almacenado, incluidos medios digitales portátiles, medios de respaldo y registros.

Hay que tener en cuenta además que las aplicaciones normalmente son propiedad del banco que exige el cumplimiento, lo que hace responsable a los comercios y Service Providers de desarrollo de Normativa de Seguridad, identificación y autenticación de usuarios, gestión de pistas de auditoría, identificación de vulnerabilidades y gestión de actualizaciones y pruebas de intrusión.

Alianza GoNetFPI y 1st Secure IT

GoNetFPI y 1st Secure IT se unen para luchar contra el fraude en medios de pago en el mercado ibérico mediante una alianza que permite ofrecer la máxima seguridad a sus clientes que operen con medios de pago tanto en el mercado ibérico como en el europeo y latinoamericano. Para ello, la alianza cuenta con un equipo dedicado en exclusiva a esta actividad y que está apoyado en todo momento por un grupo con más de 20 expertos auditores internacionales certificados como QSA por el PCI Council.

El número de españoles con al menos una tarjeta en su posesión alcanzó en 2017 al 82% de la población, lo que se tradujo en un aumento de ocho puntos porcentuales en relación al dato registrado un año antes y supone el dato más alto de toda la serie histórica desde hace 30 años, según una encuesta



PCI DSS, la seguridad de los datos de los pagos digitales a tu alcance

Compartir en RRSS

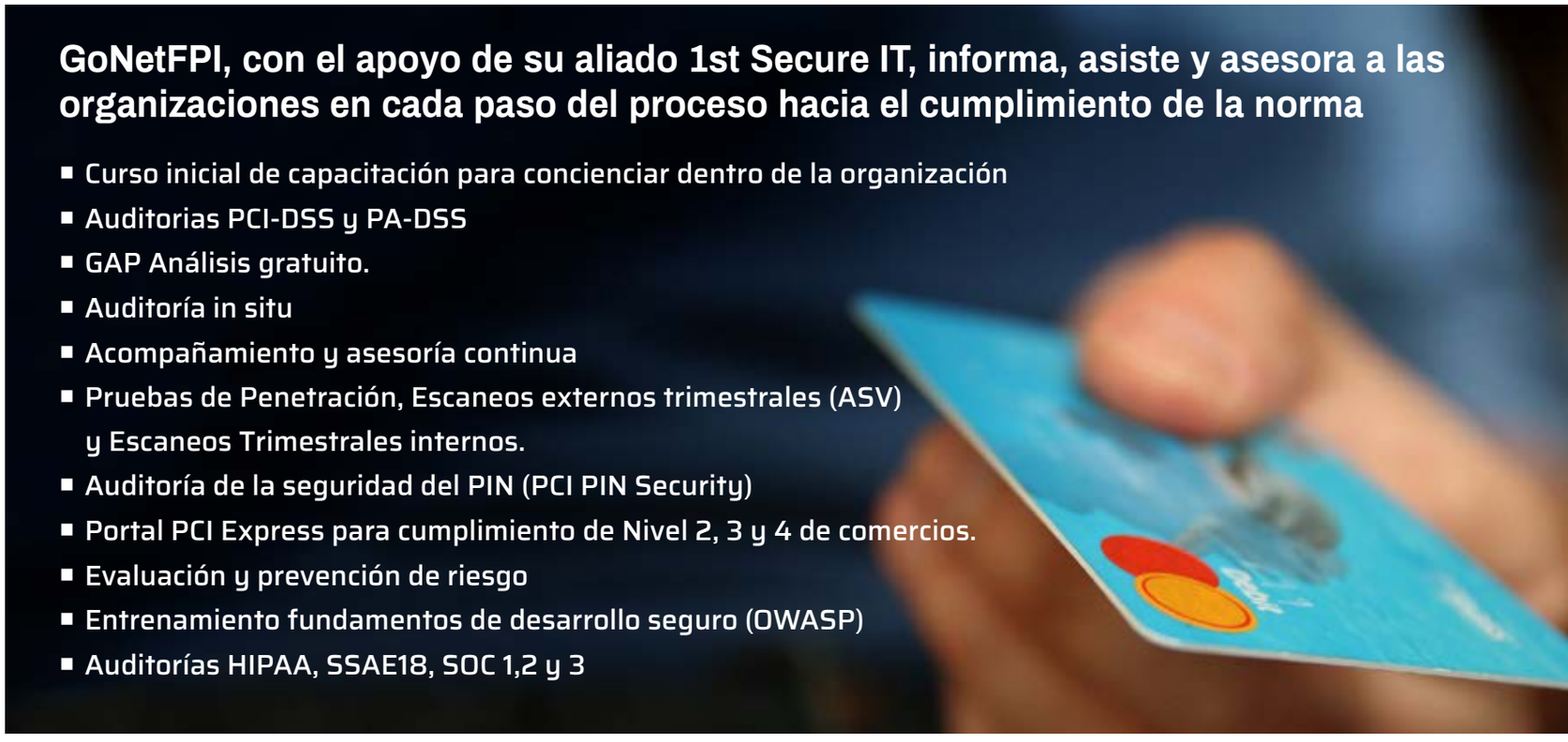
realizada por Mastercard. Actualmente en el mercado ibérico hay más tarjetas que habitantes de ahí que sean uno de los focos de los ciberdelincuentes y la necesidad de proteger las operaciones que se realizan con las mismas. La ciberdelincuencia ha encontrado uno de sus nichos y de ahí la importancia de ofrecer los servicios más completos y seguros para proteger los medios de pago de posibles ataques.

El objetivo de esta colaboración entre GoNetFPI y 1st Secure IT es atender a cualquier tipología de clientes que opere con medios de pago, desde comercios electrónicos, agencias de viajes hasta agregadores, procesadoras o entidades financieras, ya sean emisoras o adquirentes, cubriendo todas sus necesidades desde la certificación PCI, hasta el análisis de negocio y la gestión de riesgos.

GoNetFPI y 1st Secure IT ofrecerán sus capacidades en la certificación de PCI (Payment Card Industry) en el mercado europeo, con un primer foco de entrada en España y Portugal, donde el uso de tarjetas para realizar los diferentes pagos es la práctica más habitual.

1st Secure IT destaca en el sector de la ciberseguridad por realizar certificaciones PCI-DSS desde hace más de una década en Estados Unidos y Latinoamérica, entornos que han cambiado mucho en los últimos años. La compañía, con oficinas en Florida, Massachusetts, Brasil y México D.F., apoya a las instituciones, convirtiéndose en su aliado durante todo el proceso, para mejorar su seguridad en el procesamiento de datos y lograr cumplir con el estándar PCI-DSS de una manera práctica, sencilla y eficiente.

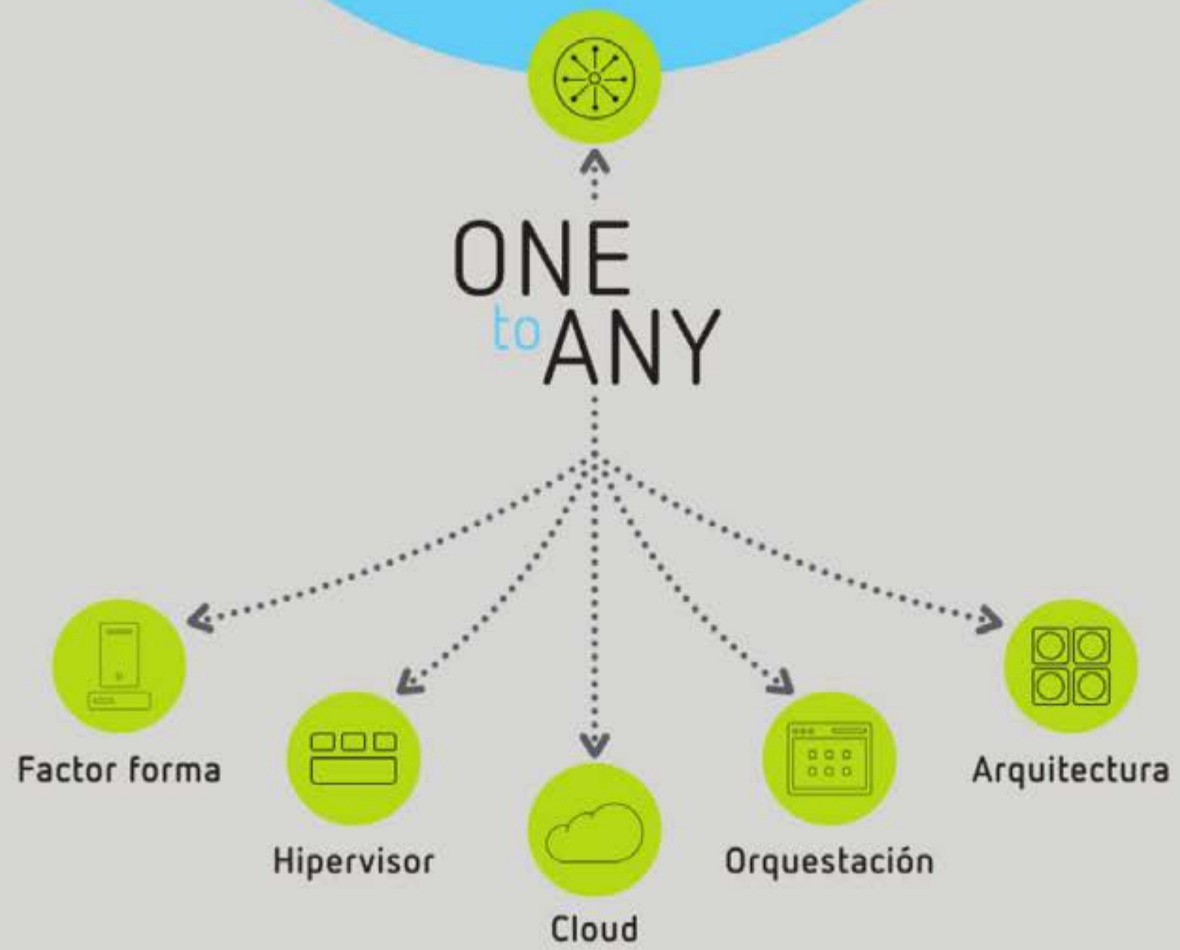
Tanto en España, como en Europa y a nivel mundial, la oferta de GoNetFPI y 1st Secure IT se diferencia de la competencia por la realización de GAP Analysis gratuito para nuevas contrataciones del servicio; mínima presencia on-site de los asesores de la compañía utilizando herramientas colaborativas y contar con más de 20 asesores a nivel mundial.



Enlaces de interés...

- GoNetFPI
- PCI-DSS Compliance
- GoNetFPI y 1st Secure IT se unen en la lucha contra el fraude en medios de pago

Mismo API
Mismo código base
Mismas funcionalidades
Mismo sistema de gestión
Para cualquier entorno



Más información en citrix.es/Netscaler

NetScaler®

CITRIX®

Hace mucho que la movilidad y el BYOD llegaron a las empresas, pero parece que su adopción no ha ido de la mano de la seguridad. Los últimos datos que manejan algunos estudios hablan de un mercado que alcanzará los 367.000 millones de dólares para 2022, frente a los 30.000 de 2014 y que el 87% de las empresas confían en el uso de los dispositivos personales para acceder a las aplicaciones empresariales.

Movilidad y BYOD, todo un mundo por securizar

Demasiados dispositivos, muchas veces sin control, acceden a las redes, recursos y datos de las empresas. La movilidad se ha convertido en un reto que hay que saber afrontar. En torno a esta temática, a cómo adoptar la movilidad y el BYOD (Bring Your Own Device) de una manera segura, hemos celebrado una nueva edición de nuestros #DesayunosITDS en el que hemos contado con la presencia de Mar García Maroto, directora de Pre-venta de Citrix

"Hay gente que piensa que el teléfono móvil no hace falta securizarlo, ni controlarlo, ni gestionarlo, ni separar la parte profesional de la personal"

Josep Albors, responsable de investigación y concienciación de ESET Iberia

Iberia; César Garro, Ingeniero especialista en Samsung KNOX y Josep Albors, responsable de investigación y concienciación de ESET Iberia.

La primera pregunta que plateábamos a nuestros invitados es si la apuesta por la movilidad ha ido acompañada de seguridad. “Los empleados son cada vez más móviles, pero no hay una concienciación de cómo se debe tratar la información empresarial en sus equipos”, aseguraba César Garro. De hecho, el número de usuarios de teléfonos móviles superará los 5.000 millones para 2019, y un año después, el 2020 el 42% de la fuerza laborar será móvil.

Mar García Maroto aseguraba que “trabajamos como vivimos, con el móvil”, y que, ya que las empresas nos permiten utilizarlo, lo que hay que hacer es “garantizar la seguridad”.

El uso de dispositivos móviles en las empresas sin su adecuada supervisión y securización les convierte, decía Josep Albors, en una puerta enorme para que los atacantes puedan acceder a recursos que hasta no hace mucho estaban un poco más escondidos; “por desgracia, ese BYOD no ha venido acompañado con concienciación”, decía el ejecutivo de ESET.

Continuando con el tema de la concienciación, Mar García Maroto aseguraba durante el desayuno que muchas compañías no son conscientes de que tienen un proyecto de movilidad; te dicen que no tienen BYOD y cuando se les pregunta si dejan a sus usuarios acceder al correo desde sus teléfonos móviles te dicen que sí, “no se están dando cuenta que eso es un proyecto de BYOD sin gobernar”. Por eso continuaba diciendo la directiva de Citrix que hay que anticiparse, ser conscientes de que el proyecto existe, que existen herramientas, que se va a mantener un entorno personal, “pero garantizar en todo momento que si estás en el entorno laboral está securizado”.

¿Te avisamos del próximo IT Digital Security?

#DESAYUNOSITDS. MOVILIDAD Y BYOD

CLICAR PARA VER EL VÍDEO

Coincidía César Garro con Mar García al dice que "lo que ocurre en las empresas españolas es que no saben lo que es el BYOD", y a partir de ahí se tiene que diferenciar lo que es información personal y empresarial en el terminal. También apuntaba el especialista en Samsung Knox que en España también se está dando el fenómeno CYOD, o Choose Your Own Device, por el que la compañía paga una parte del teléfono de una lista de opciones y el usuario aporta el resto en función de sus gustos, "lo que elimina la problemática de que el teléfono personal sea mejor que el profesional".

"Lo que se busca con la movilidad es la disponibilidad", decía Josep Albors, y se dirigía a sus compañeros de debate asegurando tener "una visión mayor de la pyme y ese catálogo de dispositivos no se da y muchos no pueden, por desgracia, adquirir soluciones como la vuestra, la de Samsung porque no les importa mezclar la vida personal con la profesional". El problema es de concienciación, y muchas veces no se toman medidas hasta que hay un problema y te das cuenta de que el empleado estaba compartiendo información confidencias desde un teléfono personal.

Adopción del BYOD y la movilidad

"Muchas empresas no reaccionan hasta que han tenido un problema o han viso que un competidor directo lo ha tenido", decía Josep Albors, añadiendo que ni siquiera consideran que son un endpoint a securizar; "hay gente que piensa que el teléfono móvil no hace falta securizarlo, ni controlarlo, ni gestionarlo, ni separar la parte profesional de la personal". Lamentablemente la industria lleva demostrando desde hacer años que los dispositivos móviles sirven incluso como vector de ataque a redes corporativas.

Hablar de movilidad y BYOD es hablar de smartphones, pero también de tabletas, de las que se utilizan para tomar nota de las reuniones con una aplicación que se ha descargar desde la tienda; "y estoy tomando las notas con contenido confidencial sin saber dónde se están guardando esas notas", aseguraba Mar García Maroto. Apuntaba también la directora de Pre-venta de Citrix Iberia que hay que ponerse al servicio del usuario, y si quiere una aplicación para tomar notas dársela, pero que esté aislada de los juegos de su hijo; "y si quiere el correo lo mismo, voy a generar en entorno de seguridad dentro de este dispositivo que está aislado

"Los empleados son cada vez más móviles, pero no hay una concienciación de cómo se debe tratar la información empresarial en sus equipos"

César Garro, Ingeniero especialista en Samsung KNOX

Al finalizar el debate, pedimos a nuestros invitados que nos hablen sobre sus propuestas para securizar la movilidad y que el BYOD:

Samsung. Nosotros nos encargamos de que lo que ocurra en el terminal esté seguro. Tenemos un ecosistema de soluciones que se llama KNOX y una gama de terminales Samsung Enterprise Edition, de forma que cuando una compañía adquiera uno de ellos incluye todo lo necesario para mantener ese dispositivo y lo que incorpore a salvo. El mensaje es: Cómprate un terminal Enterprise Edition y tendrás acceso a las soluciones de seguridad de Knox.

Citrix. La visión es permitir el Secure Mobile Workspace, un espacio de trabajo securizado que se adapte a todas esas posibilidades que hemos visto hasta llegar al Unified Endpoint Management, una única consola que nos permita controlar todos los endpoints de una manera centralizada y garantizar eses BYOD. Además, puedo adaptarme a otros dispositivos, como el PC que tengo en mi casa, permitiendo que el usuario trabaje en un entorno totalmente aislado.

ESET. En ESET estamos centrados en proteger lo que es el endpoint, y nos es indiferente que sean smartpones, PC, tablets, televisores... porque al final es el sitio en el que vas a estar operando, tanto en modo personal como profesional. Se trata de evitar que una amenaza entre en el dispositivo y acceda posteriormente a la red corporativa, de evitar la pérdida de datos y contar con un sistema de alerta para que en el caso de robo o pérdida podamos eliminar toda información. En el ámbito de la gestión disponemos de una consola centralizada para gestionar todos los tipos de endpoint, que además permite tener un control de lo que se hace con un dispositivo, una especial de control parental, para que no se instalen aplicaciones que no estén aprobadas.

del entorno personal. Y podemos dar un paso más, porque puedo transformar una tableta en un puesto productivo, un escritorio de trabajo que se comporte como un televisor. Así garantizo la seguridad y la productividad".

"Trabajamos como vivimos, con el móvil, y ya que las empresas nos permiten utilizarlo, lo que hay que hacer es garantizar su seguridad"

Mar García Maroto, directora de Pre-venta de Citrix Iberia

LA SEGURIDAD EN UN MUNDO DE ACCESOS REMOTOS

Los negocios actuales, cada vez más distribuidos, no solo están incrementando las necesidades de ancho de banda, sino disolviendo los perímetros de la red, lo que a su vez incrementa las amenazas de seguridad. Muchos ejecutivos de TI esperan que sus demandas de ancho de banda superen los 10 Gbps en 2020. Esta es solo una de las conclusiones del informe Security in a Remote Access World de iboss, que recoge que la conversación en torno a empresas distribuidas va más allá del simple fortalecimiento de la infraestructura de red y un mayor y presupuesto para hardware de TI.

Para César Garro, si te vas a grandes cuentas en España "te encuentras de todo, algunas muy avanzadas en cuanto a políticas de seguridad y otras con muchas deficiencias".

Responsabilidad de los empleados

Preguntamos a nuestros invitados si cuando se habla de movilidad y BYOD los empleados son proactivos, si entienden que las empresas deban establecer unos controles mínimos en torno a sus dispositivos personales si los quieren utilizar en el entorno corporativo. Para César Garro, "no haya que coartar la libertad del empleado y la empresa no pueda tener una intromisión en el dispositivo del empleado", y hay muchas formas de hacer eso de forma profesional.

"Yo creo que la concienciación es fundamental. Hay una parte que reside siempre en que el usuario entienda lo que está ocurriendo. Y si hablamos de BYOD el dueño es el usuario, que debe entender que si te bajas una aplicación que quiere acceder a tus contactos y a tu posicionamiento y es una linterna a lo mejor deberían plantearte para qué. Y ahí es donde estamos un poco más cojos", decía Mar García Maroto.

Por su parte, Josep Albors aseguraba que empleados hay de todo tipo, los que aplican muchas más medidas de seguridad que las que le aplican en la empresa, y otros que no hacen nada. "Hay que intentar un equilibrio, educando y concienciando. Pero no sólo se trata de darles una charla y unos folletos informativos, como hacen muchas empresas, y hacer recaer toda la responsabilidad en el empleado. Las soluciones que propone Mar de un acceso remoto a todo, cifrado, securizado, con doble factor de autenticación, a día de hoy sería una de las más destacables", apuntaba el responsable de investigación y concienciación de ESET.

Plateábamos durante el debate quién sería el responsable último del dispositivo, de mantenerlo actualizado, de aplicar las medidas de seguridad, etc. Para Josep Albors, depende de las condiciones que el empleado tenga con la empresa, de cómo se

El 87% de las empresas confían en el uso de los dispositivos personales para acceder a las aplicaciones empresariales

haya establecido este tema con los responsables de sistemas. En todo caso, “si a mí me han dado el terminal, recae en ellos”, decía el ejecutivo de ESET España.

Para Mar García los modelos son tan variados como las empresas. Las hay que entregan el móvil corporativo y se responsabilizan de todo; también se da el caso en el que t lo dan y habilitan una parte personal, y modelos de BYOD con una responsabilidad compartida. “Cuando una compañía tiene un proyecto de movilidad planificado, organizado, con perfiles de usuario… está claro quién es el responsable del acceso, de la securización del dispositivo”.

El Ingeniero especialista en Samsung KNOX asegura por su parte que “el responsable de la información corporativa es la empresa”, se encuentre donde se encuentre esa información.

Smartwatches y Pulseras

Si a la seguridad de la movilidad y el BYOD le queda mucho camino por recorrer, hablar de cómo se están gestionando los relojes inteligentes y las pulseras es casi tontería. No es que vayas a ser productivo con este tipo de dispositivos, pero preguntamos para ver si en las empresas se ha puesto sobre la mesa cómo gestionar esta movilidad tan particular.

Josep Albors recuerda el incidente ocurrido con las pulseras de fitness que el ministerio de defensa americano regaló a un grupo de soldados, cuya actividad fue monitorizada y llevó al descubrimiento de bases secretas. “Se debería hacer, pero se está viendo que no” se está planteando el uso de este tipo de dispositivos en entornos corporativos.

Para Mar García Maroto es fundamental entender para qué se está utilizando, dónde se está almacenando la información. De nuevo volvemos a la concienciación y si a ti, como individuo, “te preocupa que tu localización sea conocida y en qué condiciones”.

Asegurando que nadie, o casi nadie, se lee los términos y condiciones de los dispositivos que adquirimos, recuerda César Garro el incidente de BlueBorne, una vulnerabilidad que permitía controlar dispositivos a través de bluetooth. “En ese caso los teléfonos no eran la principal preocupación, porque es mucho más fácil atacar a un wearable. Y un wearable se va a conectar a la red corporativa, a la televisión, a tu casa…”.

Enlaces de interés...

- ¿BYOD en mi empresa? Si, pero de forma segura
- Más de la mitad de las empresas sospechan que sus trabajadores móviles han sido hackeados
- Samsung Knox
- Citrix Movilidad
- ESET Empresas

Compartir en RRSS

¿Te avisamos del próximo IT Digital Security?

SAMSUNG

Secured by Knox

Galaxy S9 | S9+

Seguridad integrada para trobalar como, cuando y donde quieras

Para consultar la lista completa de las certificaciones Knox, por favor visita www.samsungknox.com

La seguridad está en tu mano

La seguridad está en tu mano. En realidad, resulta curioso que pueda ser así, que pueda estar tan cerca, tan a mano. A veces nos complicamos la vida. Puede que sólo baste con tener un backup que funcione y nos permita recuperar lo perdido, robado o cifrado; incluso que con cifrar la información evitáramos las multas y que información valiosa escape de nuestro control; quizá lo más inteligente sea centrarnos en securizar el endpoint, u optar por servicios gestionados de seguridad. ¿Realmente necesitamos un SIEM, controlar los accesos, contar con un SOC, hablar de inteligencia de amenazas, de machine learning o de inteligencia artificial…?

El 77% de los CISO, los responsables de seguridad de las empresas, están preocupados porque sus empresas no están preparadas para luchar contra las amenazas actuales y, además, la gran mayoría de las infraestructuras de seguridad de las organizaciones están anticuadas. Son datos recientes, del Security Report de Check Point publicado en abril en el que la compañía de seguridad habla de los ataques Gen V, una nueva generación de ciberataque que hacen uso de tecnologías que roban a los propios estados. Los ataques Gen V son multivectoriales, de rápida difusión y funcionan a gran escala.

Pero quizá no haya que irse a ataques tan sofisticados, a tecnologías inalcanzables. Y es que según otro estudio, en este caso de Positive Technologies, la ingeniería social sigue estando detrás de demasiados ataques, y eso es porque sigue dando grandes frutos. Para elaborar su informe la compañía envió 3.332 mensajes, y según sus resultados, si esos simulacros de hubieran sido reales, el 17% de estos mensajes habrían comprometido el ordenador del empleado y, en última instancia, toda la infraestructura corporativa.

De forma que volvemos al comienzo, a preguntarnos su necesitamos grandes, complejas y costosas soluciones o la seguridad está más a mano de lo que nos parece. Claro que todo depende del tamaño de la empresa, de los empleados y recursos a proteger, pero hemos pedido a unas cuantas empresas de seguridad que nos digan cuáles son los

"El futuro de la ciberseguridad no consistirá en el desarrollo de nuevas técnicas de detección, sino en nuestra capacidad de predicción"

Miguel Ángel Rojo, CEO de GoNetFPI

¿Te avisamos del próximo IT Digital Security?

"Todo el esfuerzo debe ir encaminado a minimizar riesgos, con una defensa multicapa que vaya desde el endpoint hasta el firewall perimetral"

Sergio Martínez Hernández, Iberia Regional Manager de Sonicwall

aspectos más básicos de seguridad que las empresas deben tener en cuenta. Ese 'must have' que lleve a contar con la seguridad correcta, eso mínimos sin los que ninguna empresa debería estar.

Visibilidad

Los enfoques tradicionales de administración de seguridad de múltiples productos, de procesos de cambio manuales y políticas monolíticas y silos de datos ya no funcionan. La seguridad debe ser ágil, eficiente y anticipar futuras amenazas. Y para ello la visibilidad es clave.

De hecho, la visibilidad es uno de los aspectos que han identificado como básicos los expertos consultados. La tarea es tan complicada como necesaria. Hablar de visibilidad es hablar de tener una imagen completa de la postura de seguridad de una empresa, de saber qué dispositivos y usuarios están accediendo a qué, de cualquier ataque en proceso o a punto de suceder, si se están incumpliendo políticas, etc.

Tanto los responsables de la seguridad de las empresas como los administradores de sistemas, necesitan entender qué está ocurriendo para poder dar una respuesta de incidencia más rápida y evitar las amenazas.

Otro aspecto importante de la visibilidad en la administración de seguridad es que monitoriza la actividad

"Las premisas que una empresa debe considerar a la hora de diseñar su estrategia de ciberseguridad son la visibilidad y el control"

José de la Cruz, director técnico de Trend Micro

diaria para crear puntos de referencia de lo que se considera un comportamiento normal en la organización. Añadir correlación de eventos para identificar patrones de ataque e inteligencia de amenazas para ayudar en la respuesta al incidente permite a las empresas ser proactivas en lugar de reactivas.

Relacionado con la visibilidad: un panel de control también nos ayuda a conseguir una visibilidad completa de la seguridad de nuestra red, lo que nos ayuda a controlar el estado de los puntos de cumplimiento y, de nuevo, estar alerta ante posibles amenazas.

Seguridad multicapa

La Seguridad Multicapa, o Defensa en Capas, incluso Seguridad en Profundidad, es una práctica adoptada hace ya bastantes años que consiste en combinar diferentes mecanismos y tecnologías de seguridad para proteger los datos y los recursos.

Es decir, que la estrategia de seguridad debe incluir medidas que ofrezcan protección para cada una de las capas, la de aplicaciones, la de red… No parece existir una aproximación genérica, sino que cada fabricante propone un listado de capas de seguridad a proteger. Unos hablan de Capa de

"Lo importante es desarrollar una estrategia de seguridad adaptativa para reducir significativamente el riesgo de ataques y los daños que éstos pueden ocasionar"

Alfonso Ramírez, director general de Kaspersky Lab Iberia

Aplicación, Capa de Transportes, Capa de Red, Capa de Enlace y Capa física, mientras otros establecen la capa de seguridad a nivel de sistema, a nivel de red; a nivel de aplicaciones y a nivel de transmisión.

Lo que parece estar claro es que establecer una estrategia que asegure una completa protección empresarial, y que debe tener en cuenta políticas de seguridad, la protección de los sistemas de red, que cuente con sistemas de detección de intrusiones y de gestión de accesos, que proteja los datos con soluciones de backup, cifrado y continuidad, que sea capaz de gestionar los certificados digitales, el email, las vulnerabilidades, y además establecer controles de privacidad y monitorizar todo.

Backup, el gran olvidado

Mencionan también nuestros expertos el backup. Es el gran olvidado. La mayoría de las veces se tiene, pero ni siquiera se comprueba de manera periódica. Que esté evolucionando hacia la continuidad de negocio está mejorando la situación de muchas empresas, algunas de las cuales –más de lo que sería conveniente, se han visto atrapadas en ataques de ransomware.

El backup está llegando a la nube. La enorme cantidad de datos que se generan, la adopción del

La opinión de los expertos

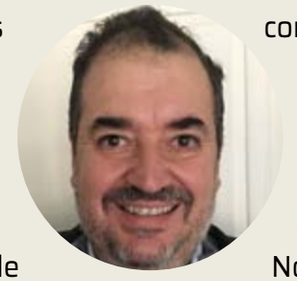
Como decíamos al comienzo del artículo, pedimos a algunas empresas que nos respondieran a una pregunta: ¿Qué aspectos básicos debe afrontar una empresa para estar segura? Aquí tienen sus respuestas, por riguroso orden de recepción de las mismas

MIGUEL ÁNGEL ROJO,
CEO DE GONETFPI

Está claro que la seguridad 100% no existe y eso es un hecho, pero sí tenemos en nuestra mano una serie de actitudes que pueden mantener más segura nuestra organización y minimizar, incluso evitar, pérdidas tanto económicas como de prestigio reputacional y de marca en cualquier sector global.

La predicción de incidentes de seguridad es una de las claves. No se trata sólo de mitigar los incidentes que pueda sufrir nuestra compañía sino de anticiparnos a ellos y evitar que lleguen a producirse. El futuro de la ciberseguridad no consistirá en el desarrollo de nuevas técnicas de detección, sino en nuestra capacidad de predicción. El futuro próximo de la ciberseguridad abandonará la línea actual basada en la detección y mitigación de los ciberataques, entrando en convergencia a través del desarrollo de técnicas basadas en la predicción de los mismos.

En línea con esta teoría de la predicción debemos destacar la concienciación y la continua monitorización. El contar con una plantilla concienciada en temas de ciberseguridad se convierte en un arma muy importante para la protección de la compañía y que, en ocasiones, los incidentes se desencadenan gracias a errores internos como descarga de archivos infectados. La continua monitorización también se convierte en un factor clave que nos permitirá detectar comportamientos 'sospechosos' y adelantarnos a determinados ataques. Por lo tanto, si tuviésemos que destacar 3 aspectos para que una empresa aumente su seguridad, desde GoNetFPI apuntamos a la predicción, la concienciación y la monitorización continua."



SERGIO MARTÍNEZ HERNÁNDEZ,
IBERIA REGIONAL MANAGER DE SONICWALL.

No existe la seguridad 100% como sabemos. Todo el esfuerzo de cualquier organización debe ir encaminado a minimizar riesgos, con una defensa multicapa que vaya desde el endpoint hasta el firewall perimetral, con un foco especial en implantar cultura de seguridad a todos los niveles, con auditorías periódicas para detectar y subsanar carencias, y con una actitud de mejora continua, ya que, como decía al principio, las amenazas cambian, mutan, y hacen muy compleja nuestra tarea en las organizaciones sea cuál sea su tamaño.

JOSÉ DE LA CRUZ, DIRECTOR TÉCNICO DE TREND MICRO

Desde Trend Micro consideramos que las premisas que una empresa debe considerar a la hora de diseñar su estrategia de ciberseguridad son la visibilidad y el control.

La primera, la visibilidad, nos debe aportar la posibilidad de detectar cualquier amenaza ya sea conocida o desconocida que tenga lugar en nuestra infraestructura y obtener toda la información posible en relación a la misma.

La segunda, el control, debe permitir bloquear o mitigar el alcance de estas amenazas, implementando mecanismos de bloqueo y limitando la propagación.

En ambos casos resulta imprescindible cubrir todos los posibles vectores de ataque (web, correo, endpoints, cloud, etc.) existentes en la organización. Y esto se consigue con desplegando una seguridad multicapa.

ALFONSO RAMÍREZ, DIRECTOR GENERAL DE KASPERSKY LAB IBERIA

WannaCry, Expetr o Bad Rabbit son solo unos ejemplos de lo devastadores que pueden llegar a ser los ciberataques.

Estas amenazas marcaron un antes y un

Continúa en la página siguiente

La opinión de los expertos

después en el mundo de la ciberseguridad. Ahora, ninguna empresa está a salvo pues las ciberamenazas evolucionan y se hacen cada vez más complejas y persistentes.
De las innumerables consecuencias, las que más afectan a las organizaciones son la fuga de datos y el impacto económico que supone recuperarse de un incidente, algo que afecta gravemente a la reputación de la compañía. Por ello, es necesario contar con una protección holística, adaptativa y multinivel en cada elemento de la infraestructura TI para evitar ataques masivos y dirigidos
Lo importante es desarrollar una estrategia de seguridad adaptativa para reducir significativamente el riesgo de ataques y los daños que éstos pueden ocasionar mediante una estrategia basada en cuatro pilares básicos: prevenir, detectar, responder y predecir. En este sentido, desde Kaspersky Lab nos encontramos trabajando en un enfoque que permite prevenir y reducir el número de amenazas avanzadas y ataques dirigidos; detectar todas aquellas actividades sospechosas que puedan poner en riesgo la infraestructura corporativa; responder, reduciendo las brechas de seguridad y realizar una investigación exhausta de los ataques, y predecir futuros ataques.
Por último, y para mantener una estrategia de seguridad fuerte y robusta, es necesario un plan de formación en materia de ciberseguridad para todos los empleados de la compañía, sea cual sea su nivel profesional. Es importante combinar herramientas adecuadas con las prácticas adecuadas. Se debe incluir también a RRHH y a la alta dirección para motivar y animar a los empleados a que tomen precauciones y soliciten ayuda en el caso de incidentes.
La formación sobre seguridad a los empleados, aportando unas claras instrucciones en lugar de unos documentos voluminosos, la construcción de habilidades y la motivación junto con la creación de la atmósfera adecuada, son los primeros pasos que toda organización debe tomar. En definitiva, creemos que es necesario mantener una cultura corporativa para protegerse de los posibles riesgos que puedan afectar a la estructura de la organización.

DARRAGH KELLY, RESPONSABLE DE PRODUCTO DE OPEN CLOUD FACTORY

Si las empresas no conocen al 100% lo que está conectado a su red, ¿Cómo lo puedan controlar o asegurar? Para nosotros todo comienza con visibilidad. Visibilidad automática de todo lo que conecta a la red vía Wi-Fi, cable o VPN, y de manera continuada.
Una vez que las empresas tengan visibilidad completa, ya podrán aplicar el control en función de los dispositivos y usuarios conectados a sus redes corporativas, pudiendo permitir, denegar o limitar el acceso a la red, esto irá vinculado a la criticidad del dispositivo. Las empresas también deberían poder categorizar aquellos dispositivos conectados, En definitiva, entendemos la seguridad desde la conexión, “siendo esta la primera línea de defensa”.
Otro aspecto que entendemos, las compañías deben de valorar el pago por la seguridad que consumen. Cada vez son más las empresas que invierten en productos de seguridad no sacando el máximo partido a lo que compran, nosotros entendemos que hay que simplificar la seguridad en el mundo empresarial.
Y el último punto es la encriptación, siendo de carácter critico en todo relacionado con el GDRP pero… ¿Cómo consigues que se use? Las empresas deben de establecer una base mínima de seguridad para los Endpoints y no dejar, o al menos limitar, el acceso a los equipos que no cumplen con su política.

JOSEP ALBORS, RESPONSABLE DE INVESTIGACIÓN Y CONCIENCIACIÓN DE ESET ESPAÑA

Yo empezaría por el endpoint, una solución de seguridad que sea fácil de administrar para la empresa, independientemente de que sean mucho o pocos equipos. Hay soluciones que te dejan tener una consola de administración y si quieres la usas y si no, no, a partir de cinco equipos. Esto es importante porque te genera una primera capa de seguridad.
Luego es necesario tener una copia de seguridad para poder restaurar de forma rápida si hay algún incidente, por ejemplo, si hay un ransomware. Y también tener esa copia de seguridad para responder a ese tipo de incidencias que ni siquiera están relacionadas con el malware, como puede

Continúa en la página siguiente

ser una inundación, un incendio... Una copia de seguridad bien respaldada te permite poder empezar a trabajar de forma rápida

Añadiría el tema de cifrado, muy importante para poder cumplir con el tema de GDPR. Hay soluciones de todo tipo para todos los bolsillos y para todo tipo de empresas. Es importante tener los datos confidenciales, tanto nuestros como de nuestros clientes, cifrados de manera que si alguien accede y consigue robarlos no pueda tener nada de esa información.

Y por último, la formación del usuario. A nivel de todas las empresas existen cursos formativos online, gratuitos, proporcionados por el Incibe, por empresas de seguridad, que son básicos y que son fundamentales, sobre todo para hacer frente a las amenazas. No hace hace falta que sean ataques avanzados, ni dirigidos, ni de ningún otro tipo, suficiente tenemos con los ataques más básicos, que siguen funcionando igual de bien a día de hoy como para que una empresa pequeña se preocupe de más.

IGNACIO GILART IGLESIAS,
CEO WHITEBEARSOLUTIONS

Los planes de recuperación de desastres (DRP) son la última línea de defensa de la infraestructura IT de una organización. Desastres naturales, accidentes, problemas técnicos y, por supuesto, ataques informáticos amenazan la conservación de los datos críticos del negocio.

Desgraciadamente, aún hoy en día, las organizaciones no se toman suficientemente en serio estos riesgos y, aunque pueda parecer alarmista, la infraestructura IT de una organización está permanentemente amenazada, tanto desde el punto de vista interno, como externo. Por ello, desde WhiteBearSolutions, siempre insistimos en la importancia que tiene contar con plan eficaz de actuación ante estas situaciones.

Asimismo, la adopción del cloud en los entornos corporativos como acelerador de la transformación digital, es hoy una realidad. Este tipo de tecnología presenta numerosas ventajas en términos de ahorro de costes y de acceso ubicuo. No obstante, también se plantean una serie de riesgos y retos en términos de seguridad. Algo que, si bien no debe ser tomado a la ligera, tampoco debería convertirse en un limitador en el uso y explotación del cloud. La implantación de una solución de gestión de identidades y accesos (IAM) nos permitirá mitigar un gran conjunto de riesgos, garantizando la normalización de identidades y sus accesos a la información corporativa, permitiendo establecer flujos de validación (lo cual facilita esta importante tarea) al tiempo que se respetan y garantizan las Políticas de Seguridad Corporativa.

IVAN LASTRA, RESPONSABLE DE CIBERSEGURIDAD DE VECTOR ITC GROUP

Ante la inminente implantación total del RGPD, las empresas tienen ante sí el reto de afianzar los aspectos básicos que permitan garantizar la seguridad de los datos que almacenan. Según Vector, los pilares básicos para una estrategia integral de ciberseguridad son:

- Concienciación: es la base sobre la que sustentar una buena estrategia de ciberseguridad. Es necesario invertir tanto en la formación de los empleados como en implantar nuevas y mejores soluciones y servicios tecnológicos. Conviene poner en práctica una mentalidad de “confianza cero” para que las medidas de seguridad se ajusten a las preferencias del usuario, aunque esto suponga medidas de autenticación más estrictas para verificar la identidad de los usuarios.
- Tecnología: contar con plataformas de vigilancia y protección. Hoy en día ya hay sistemas que permiten predecir, prevenir, detectar y responder ante cualquier imprevisto de ciberseguridad antes de que éste suponga un problema de gravedad.

Al margen de estas herramientas y la formación de los empleados en este campo, también es necesario tomar una serie de medidas de prevención, comenzando por las más básicas, como extremar la precaución a la hora de abrir enlaces externos, sobre todo que provengan de correos desconocidos; utilizar software de seguridad, antivirus o cortafuegos; limitar la superficie de exposición a las amenazas; cifrar la información sensible; realizar copias de seguridad periódicas y mantener actualizada las aplicaciones, sistemas operativos, permisos y configuración de la seguridad.

"Para nosotros todo comienza con visibilidad automática de todo lo que conecta a la red vía Wi-Fi, cable o VPN, y de manera continuada"

Darragh Kelly,
Responsable de producto de Open Cloud Factory

Las opciones de copia de seguridad actuales son más flexibles y variadas, no sólo hay soluciones para todas las necesidades y presupuestos, incluida una amplia oferta de soluciones basadas en la nube. Apuntar a que la recuperación de desastres basada en la nube ofrece ventajas adicionales, incluida la capacidad de utilizar un modelo de pago por uso, capacidad de almacenamiento casi ilimitada y flexibilidad.

modelo de software-as-a-service, la caída de los precios… está haciendo que este mercado esté creciendo una media del 26% anual entre 2016 y 2023.

Este segmento de mercado ha sufrido un proceso evolutivo constante desde que las primeras copias de seguridad en cinta y cintas magnéticas de la década de los 60 hasta nuestros días. En lo físico se ha pasado de esas cintas magnéticas a los discos duros, CDs y DVDs, almacenamiento Flash y, en última instancia, el cloud. Sin embargo, la importancia de la copia de seguridad para las empresas no ha cambiado. Todas las empresas necesitan una copia de seguridad eficiente y confiable, así como un plan de recuperación de desastres viable.

Las empresas han invertido mucho en software y hardware de copia de seguridad en cinta debido a su eficiencia de costos y para garantizar la retención de datos a largo plazo. El paso a la nube ha sido lento por el temor a perder el control de sus datos, pero el proceso de recuperación de los datos de las copias de seguridad en cinta puede ser un proceso lento.

¿Te avisamos del próximo IT Digital Security?

Cifrado

El cifrado está más de moda que nunca. Tuvo un fuerte repunte después del escándalo de la NSA. ¿Se acuerdan? En junio del 2013, Edward Snowden, consultor tecnológico estadounidense y antiguo empleado de la CIA (Agencia Central de Inteligencia) y de la NSA (Agencia de Seguridad Nacional) hizo públicos documentos clasificados como alto secreto sobre varios programas de la NSA, incluyendo los programas de vigilancia masiva PRISM y XKeyscore. PRISM se dedicaba a la recogida masiva de comunicaciones procedentes de al menos nueve grandes compañías estadounidenses de Internet, mientras que XKeyscore era un sistema informático secreto utilizado por la agencia para la búsqueda y análisis de datos en Internet.

El caso es que después de desvelarse que la agencia nacional de seguridad de Estados Unidos estaba espiando las comunicaciones de medio mundo, la pasión por el cifrado empezó a crecer

animados por movimientos como Let´s Encryp, un movimiento que buscaba la emisión de certificados digitales a coste cero.

El cifrado tiene también un interesante papel con la llegad de GDPR, es que el cifrar la información corporativa no sólo brinda a la compañía una capa más de seguridad, sino que la ampara en caso de incumplimiento del sistema. Es decir, hay menos pro-

"Después de proteger el endoint es necesario tener una copia de seguridad para poder restaurar de forma rápida si hay algún incidente"

Josep Albors, responsable de investigación y concienciación de ESET España

"Los planes de recuperación de desastres (DRP) son la última línea de defensa de la infraestructura IT de una organización"

Ignacio Gilart Iglesias, CEO WhiteBearSolutions

Enlaces de interés...

- Los cibercriminales prefieren explotar el factor humano para lanzar ataques
- Las empresas reconocen como retos de seguridad cloud la falta de visibilidad y el cumplimiento
- El fraude de identidad crece
- W Kaspersky Threat Management and Defense
- W Phishing, el secreto de su éxito y por qué no puedes detenerlo
- W Economía de la inseguridad
- W Informe sobre la seguridad de las infraestructuras

babilidades de que el ente regulador considere tales incidentes como una falla de cumplimiento, dado que los datos se encuentran correctamente cifrados.

Formación y concienciación

Una de las mejores capas de defensa con las que puede contar una empresa es con los propios empleados. Un usuario bien formado detectará un phishing, una web maliciosa, una aplicación sospechosa, no se conectará a redes WiFi abiertas, no será víctima de un fraude de servicio técnico, no aceptará un USB, o al menos no lo pinchará en el eordenador corporativo…

Las amenazas son cada vez más sofisticadas y la ingeniería social más acertada, por eso que los empleados y usuarios aprendan a detectar el peligro y se conviertan en firewalls humanos cobra cada vez más importancia.

Son muchas las empresas que ofrecen cursos de concienciación, algunas a través de juegos y otras de manera más tradicional, pero lo cierto es que es un mercado que ha crecido y seguirá creciendo.

Compartir en RRSS

¿Te avisamos del próximo IT Digital Security?

Próximos #ITWebinars

Estrategias para lograr una experiencia de cliente satisfactoria

GDPR, el último empujón

Seguridad y cloud, ¿qué nos queda por aprender?

www.ittelevision.es

it televisión

EMILIO CASTELLOTE

IDC SENIOR RESEARCH ANALYST

Con 20 años de experiencia en las áreas de TI, telecomunicaciones y ciberseguridad, en los últimos dos Emilio Castellote años ha estado trabajando en el desarrollo de Startups, dirigiendo las áreas de estrategia de Marketing y Ventas en compañías como Genetsis Solutions o Hdiv Security.

Anteriormente ocupó cargos como Director de Canal, Director de Marketing de Producto, Director de Pres Venta y Gerente de Producto en Panda Security; Profesor asociado de la Escuela de Ingeniería y Sistemas de Telecomunicación de la Universidad Politécnica de Madrid y Profesor de diversos Masters de Ciberseguridad impartidos por la Universidad Pontificia de Salamanca y la Universidad Europea de Madrid.

Protegiendo el Dato que salva Vidas

Aplicando GDPR en el Sector Salud

Cada vez es mayor el instrumental médico que procesa la información de forma digital (pruebas diagnósticas, historiales médicos, análisis clínicos,…) y por extensión la penetración de los sistemas de gestión de pacientes con los datos de las personas asociados se incrementan elevando el riesgo.

Los procesos de transformación digital avanzan indiscutiblemente haciéndose hueco en todas las áreas de la nueva sociedad digital, y estos procesos giran en torno a dos factores fundamentales:

- Las personas
- Los datos

Las personas y los datos se funden continuamente hasta el punto de empezar a vislumbrar una nueva entidad (digital) que identifica y perfila con todo

detalle a las personas dentro del nuevo ecosistema digital. Son multitud los datos que giran alrededor de estas nuevas entidades digitales, pero hay muchos que empiezan a ser críticos por los niveles de confidencialidad que suponen para las personas.

Uno de los sectores que mayor número de datos de elevada confidencialidad maneja es el Sector Salud. Pocos sectores están escapando a la adopción de los procesos de transformación digital y el Sector Salud no puede ser menos en esta carrera digital.

Según IDC, en 2021 la inversión en seguridad IT por los proveedores del sector salud en la zona Europa occidental alcanzará una inversión de 249 millones de euros.

Cada vez es mayor el instrumental médico que procesa la información de forma digital (pruebas diagnósticas, historiales médicos, análisis clínicos,…) y por extensión la penetración de los sistemas de gestión de pacientes con los datos de las personas asociados se incrementan elevando el riesgo.

Según IDC, en España, la partida de inversión asociada a la seguridad y gestión del riesgo del dato de los proveedores del sector salud será la que obtenga un mayor crecimiento porcentual con un 4% (CAGR entre 2018-2021), alcanzando una previsión de inversión total de 25,4M€ en el periodo 2018-2021.

Este es uno de los muchos escenarios de datos confidenciales que encontramos en la actualidad, donde garantizar esa confidencialidad y la seguridad del dato se convierten en necesidades imperiosas para el éxito de cualquier acción digital.

> Una gran preocupación para los proveedores de servicios de salud en Europa es cómo implementar el derecho del paciente a acceder a sus propios datos como paciente

A pocos días de la implantación del Reglamento General de Protección de Datos (GDPR), vivimos momentos de tensión, en el lado de la empresa o la administración pública, para readaptar los procesos de gestión de la información en aras de una mayor protección del dato, pero también vivimos del lado de las personas un progresivo aumento de sus derechos en términos de confidencialidad y control del dato que identifica a las personas.

Para comprender el impacto que GDPR acabará teniendo en el Sector Salud, debemos definir cuáles son las tres características asociadas a la seguridad de un dato que debe ser protegido por el nuevo Reglamento General de Protección de Datos:

1. Confidencialidad significa que la información está protegida contra el acceso o la exposición a personas no autorizadas. Significa que un ciudadano debe poder confiar en que no se accede a la información personal confidencial por personas que no tienen derechos y un propósito concreto para ver la información. Debido a la información sensible en aplicaciones clínicas y la cantidad de datos compartidos en el ecosistema de la salud, la confidencialidad se convierte en un pilar clave.
2. Integridad significa que la información no puede ser cambiada sin autorización. Los ciudadanos y

los profesionales de la salud deben confiar en que los datos a los que tienen acceso son precisos y completos para garantizar un régimen de tratamiento adecuado. Esto es particularmente importante en el cuidado de la salud, ya que el fallo en la integridad de los datos puede ocasionar serios errores médicos. Una confusión en la información del paciente, un registro de manera incorrecta o el tratamiento previo en los diagnósticos que puedan mezclan los datos de otros pacientes, puede tener implicaciones a largo plazo para los pacientes (y el personal) involucrados.

3. La disponibilidad implica que la información es accesible para las personas autorizadas donde sea relevante. Se trata de dar acceso a la información cuando es necesaria, a menudo en un entorno basado en el contexto. Cuando el tratamiento se basa en una gran cantidad de datos y la fuerza laboral clínica es a menudo móvil, entonces el acceso a los datos se vuelve crucial, no solo en entornos críticos como el de las urgencias, sino también cuando un médico especializado supervisa a otro pabellón, cuando el personal clínico está visitando al paciente en su hogar o tratando al paciente con equipo de telemedicina.

Además de la seguridad, las tres áreas destacables que en GDPR son cada vez más importantes y relevantes para los proveedores de atención médica en el área de los derechos personales son: privacidad, consentimiento y portabilidad de datos.

La privacidad y el consentimiento dentro del cuidado de la salud tratan sobre la protección de la información y solo la comparten con las partes interesadas relevantes con el consentimiento del paciente. Los pacientes deben confiar en que los proveedores de atención médica tengan la información relevante cuando sea necesario para tomar decisiones sobre su tratamiento. Al mismo tiempo, los pacientes deben tener confianza en que la seguridad de su información personal de salud se maneja de acuerdo con la legislación vigente y las mejores prácticas. Cuando los datos y los procesos se digitalizan, compartir e integrar los datos se convierte en una realidad y, por lo tanto, se convierte en una herramienta clave en un sector de la salud moderno y sólido orientado a la calidad.

Para que el procesamiento de los datos del paciente sea legítimo, a menudo debe haber un consentimiento del paciente. Cuando se trata de tratamiento de datos personales comunes, el consentimiento debe ser libre, específico, informado e inequívoco. Lo nuevo en GDPR es que el consen-

¿Te avisamos del próximo IT Digital Security?

¿ESTÁS RECOGIENDO DATOS DE FORMA SEGURA?

Si bien hay muchos aspectos de la administración del ciclo de vida de los datos de los clientes, todo comienza con la recopilación. Para organizaciones con una gran presencia digital, identificar todos los lugares donde se almacena información personal puede ser complicado, incluso aunque el nuevo Reglamento General de Protección de Datos (GDPR) establecido por la Unión Europea (UE), lo exija.

Las empresas, ¿Son capaces de identificar y supervisar todos los sitios web que recopilan información personal en nombre de una empresa? ¿Son esos puntos de recolección seguros? ¿Están acompañados por declaraciones y controles de cumplimiento?

> Confidencialidad, integridad y disponibilidad son las tres características asociadas a la seguridad de un dato que debe ser protegido por el nuevo Reglamento General de Protección de Datos, GDPR

timiento debe ser inequívoco: el consentimiento no es ambiguo cuando la persona registrada realiza una acción afirmativa, lo que indica que la persona registrada acepta el uso de datos personales para el propósito específico. Los ejemplos de dicho consentimiento incluyen que el paciente dé su consentimiento de manera activa haciendo clic en un cuadro en una página web. El administrador de los datos está obligado a demostrar que se otorgó el consentimiento. Al procesar datos personales confidenciales, el consentimiento debe ser explícito, a menos que el procesamiento se base en otros motivos legales como se establece en el artículo 9.

Señalar que gestionar el consentimiento siempre ha sido un desafío para el sector de la salud, con las organizaciones proveedoras tratando de encontrar un equilibrio, proporcionando información clara a los pacientes que sea útil y respalde su privacidad de sus datos, sin molestarlos con documentos legales densos al ingresar a un centro de salud para recibir servicios de atención. Debido a que el paciente se encuentra en una variedad de contextos dentro de la vía de tratamiento, es relevante analizar cuándo se necesita el consentimiento. Los datos se usan en varios escenarios de casos de uso alrededor del paciente, y los proveedores de atención médica deben determinar si se requiere o no el consentimiento del paciente.

El derecho a ser olvidado y obtener información sobre los propios datos y la portabilidad de datos

Una gran preocupación para los proveedores de servicios de salud en Europa es cómo implementar

el derecho del paciente a acceder a sus propios datos como paciente. Los datos del paciente se deben recopilar y entregar cuando los pacientes soliciten acceso. Por ejemplo, la regulación introduce un nuevo derecho: portabilidad de datos. Los ciudadanos tendrán derecho a obtener sus datos en un "formato estructurado y comúnmente utilizado y legible". Esto permite que los pacientes reciban sus datos para que puedan elegir ir a otro proveedor de atención o recibir atención en otro país europeo. No es el proceso o el gobierno de hacerlo lo que más preocupa a los proveedores, sino la perspectiva del repositorio de TI. Para que los proveedores puedan distribuir todos los datos, necesitan saber exactamente dónde se guardan los datos de cualquier paciente: en qué aplicación o equipo. La mayoría de los proveedores de servicios de salud tienen 50-100 aplicaciones clínicas principales y probablemente 300-900 sistemas de TI locales adicionales para especialidades específicas. Además de eso, los equipos médicos como resonancias magnéticas o escáneres de ultrasonido también almacenan datos del paciente. Implementar procesos en torno al derecho de acceso es difícil, pero establecer puntos de vista de manera estandarizada en todos los repositorios de datos de pacientes en todos los sistemas / plataformas / equipos es una gran tarea que debe ser administrada.

Con referencia al derecho a ser olvidado, el artículo 17 establece que no se aplica al registro de salud de un individuo para atención médica, propósitos de salud pública o investigación (en los casos de uso identificados en las secciones H e I del artículo 9).

El Sector Salud incorpora así las garantías necesarias para trasladar unos niveles de usabilidad y confianza a las personas (pacientes) que tienen que percibir la entrada en vigor de la nueva legislación en materia de protección de datos (GDPR) como un refuerzo de sus derechos fundamentales en materia de privacidad de su identidad digital.

Uno de los sectores que mayor número de datos de elevada confidencialidad maneja es el Sector Salud, que invertirá en seguridad 249 millones de euros en 2021

Enlaces de interés...

- Más del 10% de las compañías no tienen un plan de preparación para GDPR
- El cifrado, medida a tener en cuenta para cumplir con GDPR
- Sanidad y ciberseguridad, un tándem difícil de gestionar
- Lo que las organizaciones sanitarias necesitan saber sobre GDPR

¿CUÁLES SON LAS **VENTAJAS** DEL SOFTWARE DE GESTIÓN EMPRESARIAL EN CLOUD?

Descarga este **documento ejecutivo** de it User RESEARCH

La Auditoria de Ciberseguridad, ¿Están mis sistemas seguros?

Cada vez somos más conscientes del riesgo al que estamos expuestos. Tarde o temprano nuestros sistemas informáticos pueden verse comprometidos y necesitamos conocer de primera mano a qué nos podemos enfrentar; por todo ello, muchas empresas se preguntan: ¿Están mis sistemas seguros?

DAVID JIMÉNEZ FERNÁNDEZ

CONSULTOR DE SEGURIDAD IT
PERITO JUDICIAL INFORMÁTICO

David Jiménez Fernández acumula más de 20 años de experiencia en el sector IT como consultor de seguridad informática, perito judicial informático/forense y responsable de preventas Técnicas de productos y soluciones de ciberseguridad. David Jimenez es también auditor de seguridad de la información y consultor en GDPR, la normativa de protección de datos que será de obligado cumplimiento a partir del 25 de mayo de 2018.

La respuesta a esta pregunta conlleva una auditoria de ciberseguridad a nuestra infraestructura tecnológica realizada por un experto o expertos cualificados en esta materia. Muchas veces no somos conscientes ni conocedores de las diferentes vulnerabilidades en seguridad de la información y en el manejo de datos de especial protección a los que nos enfrentamos día a día, hasta que somos las víctimas de un incidente de seguridad, ya sea externo o interno de nuestra red.

Las empresas y sus responsables no suelen conocer que posiblemente sus sistemas están permanentemente expuestos o comprometidos a importantes brechas de seguridad. Algunas de ellas son tan graves que pueden, incluso, atentar o afectar al principal valor de nuestra empresa; como lo son la información y los datos; ya sean de propiedad de

de algo. La auditoría, en el terreno de la ciberseguridad informática consiste en el análisis y examen detallado de la plataforma sistemática y electrónica de una empresa y sus contenidos, por parte de expertos en el tema, mediante el uso de unas herramientas específicas para obtener la mayor información posible, su estado real y actual de seguridad o vulnerabilidad y las posibles brechas a las que se encuentra permanentemente expuesta esa información.
El tiempo estimado para la realización de este tipo de auditorías, depende del número de elementos (equipos, redes, archivos etc.) a examinar. En ella se detectan los puertos de comunicaciones abiertos, programas y aplicaciones que necesitan de parches de actualización, y también los accesos a los sistemas por parte de los propios usuarios o terceras personas. Solo gracias a este tipo de auditorías se pueden conocer con detalle el grado de seguridad y madurez que tiene nuestra empresa a nivel de seguridad informática y adoptar las medidas necesarias para proteger nuestra información como uno de los activos más importantes de la empresa; prevenir no solo la fuga de información, sino, el inadecuado uso y manejo de datos; y mitigar, detectar y contrarrestar cualquier tipo de ciberataque.

El tiempo estimado para la realización de una Auditoría de Seguridad depende del número de elementos (equipos, redes, archivos etc.) a examinar

la misma empresa o aquellos datos de propiedad de los terceros que pueden tener y/o haber tenido algún tipo de relación comercial o contractual con la empresa, los cuales pueden estar en peligro o riesgo sin nosotros saberlo.

¿Qué es, y que hace una Auditoria de ciberseguridad?
El Verbo “Auditar”, clásicamente, se define como un examen minucioso y detallado sobre el estado real

DEMASIADA INFORMACIÓN

En este estudio de Digital Shadows podrás conocer el alcance de la exposición de datos en todo el mundo sólo en los tres primeros meses de 2018; las geografías más afectadas; la fuente de estos datos expuestos en los segmentos de Amazon S3, rsync, SMB, Servidores FTP, sitios web mal configurados y dispositivos Network Attach Storage (NAS); ¿Qué porcentaje de esta información era información personal del empleado o del cliente?; cómo los adversarios pueden usar estos datos para explotar tu negocio y tus clientes; qué pueden hacer las organizaciones para identificar qué información está expuesta y cómo mitigar el riesgo.

Por otra parte, la Auditoria de Ciberseguridad es, no solo muy importante, sino también muy necesaria en la actualidad, ya que gracias a la información que arrojen sus resultados podemos conocer y adoptar las medidas necesarias para mitigar el riesgo de sufrir un ataque informático. Actualmente, las empresas del sector bancario son las más propensas a sufrir este tipo de ataques, por ello, en el año 2006 se creó el estándar PCI-DDS, que regula la industria de pagos bancarios. A raíz de la creación de este estándar, las entidades bancarias deben realizar obligatoriamente auditorías de ciberseguridad cada tres meses. Este estándar proporciona un conjunto de reglas que establecen los requisitos técnicos y organizativos que deben cumplir las empresas dedicadas al desarrollo de software seguro, que desplieguen aplicaciones estándar para la industria de pagos, y estas a su vez, venden o licencian a proveedores de servicios, adquirentes, comerciantes y otras entidades de pagos.

Los conocidos ataques malware de tipo ransomware a nivel mundial como Wannacry o Petya han causado millonarios efectos dañinos a empresas y también a particulares. Este tipo de desafortunados eventos, han alertado a muchas empresas, y tanto pequeñas como grandes corporaciones se han planteado, a día de hoy en contratar los servicios de auditoria en ciberseguridad, y las que ya disponen de este tipo de servicio de auditoria a aumentar el número de realizaciones de estos.

Finalmente, podemos concluir que la seguridad a nivel de la información no es 100% efectiva; quien diga que sus equipos informáticos son 100% seguros, miente, ningún software ya sea antivirus, antispan, etc., garantizan ese porcentaje. Pero frente a todo esto, los peritos y consultores son los que deben adoptar e implementar medidas de seguridad para evitar ataque con el consiguiente perjuicio económico o pérdida de credibilidad, de reputación y la confianza en los clientes de las empresas.

Enlaces de interés...

- Las auditorías, claves para el cumplimiento e GDPR
- Gestión de Vulnerabilidades
- Y mientras GDPR acecha... se detectan más de 1,5 billones de datos corporativos expuestos

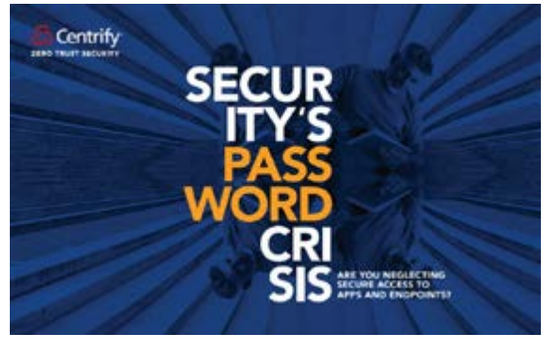
¿Te avisamos del próximo IT Digital Security?

Utilizar el engaño para una detección efectiva de malware

Para cubrir la creciente brecha de seguridad entre la infección y la detección, se requiere un plan integral de protección de datos, repleto de estrategias y herramientas nuevas y más inteligentes.
Con la actual limitación de recursos, la evaluación adecuada de las soluciones de detección requiere tener en cuenta algunos aspectos:

1. Informes precisos de incidentes reales manteniendo las falsas alertas falsas al mínimo
2. Información completa sobre el historial del ataque
3. Una GUI intuitiva que proporciona al analista un acceso rápido a todos los datos relevantes
4. Despliegue fácil y rápido con configuración automatizada
5. Mantenimiento mínimo.

Security Password Crisis



En un mundo cloud y móvil los responsables de TI tienen menos visibilidad y control sobre los usuarios que inician sesión en aplicaciones empresariales que alojan datos confidenciales de una organización. Sistemas y herramientas de autenticación poco robustas impiden a veces que los de TI distingan entre un empleado y un atacante que utiliza una contraseña robada. En este documento se exploran los desafíos de proteger el acceso a las aplicaciones empresariales y el creciente número de dispositivos que tienen acceso a ellas.

Mobile Security Index 2018

Aunque las empresas están preocupadas por las amenazas que los dispositivos móviles representan tanto para sus datos como para las operaciones comerciales, muchas de ellas no han tomado las precauciones más básicas para protegerlos. En este informe, se incluyen recomendaciones que pueden ayudar a reforzar la seguridad móvil de una organización. Verizon ofrece un marco flexible que incluye medidas de seguridad para la red, dispositivos, aplicaciones y personas.

Global deduplication for encrypted data

La deduplicación global de datos proporciona importantes ventajas sobre los procesos de deduplicación tradicionales porque elimina los datos redundantes a través de toda la empresa y no sólo de dispositivos individuales. La deduplicación global aumenta la relación de deduplicación de datos: el tamaño de los datos originales medidos con respecto al tamaño del almacén de datos una vez que se eliminan las redundancias.

La Seguridad TIC a un solo clic

it Digital MEDIA GROUP

it whitepapers

ALBERTO CORRELL

GERENTE DE RISK ADVISORY DE DELOITTE

Alberto Correl acumula diez años de experiencia en consultoría, gestionando y desarrollando proyectos relacionados con modelos de negocio y gestión de riesgos; particularmente en los ámbitos estratégico, operativo y táctico; principalmente en los sectores financiero, industrial, servicios y sector público.

La amenaza del fraude online

Cada vez son más los consumidores que encuentran en Internet una plataforma rápida, cómoda y barata para realizar todo tipo de compras. Aunque en algunos sectores, como la Alimentación, es aún un mercado incipiente en nuestro país, lo cierto es que hoy en día hay familias de productos para los que la mayoría de las transacciones ocurren online. Es el caso, por ejemplo, de videojuegos, películas y música. Según el último Estudio de Consumo Navideño elaborado por Deloitte, el canal preferido por más de un 70% de los consumidores para la adquisición de estos artículos durante la pasada campaña era Internet, y fundamentalmente las páginas web. Es más, el canal online soportaba el mayor porcentaje de crecimiento en intención de gasto.

Con el incremento en el número de transacciones y, por consiguiente, el volumen de dinero que se mueve en el comercio online, hemos visto también cómo el fraude online crece cada año. Y aunque en España no alcanza cifras preocupantes, es necesario que las compañías conozcan los riesgos a los que están expuestas y, por supuesto, las soluciones que están al alcance de su mano.

Según los últimos datos, menos del 4% de los pedidos que llegan a una tienda virtual son de origen fraudulento, lo que supone un porcentaje muy bajo

PREGUNTAS FRECUENTES SOBRE PSD2

Este documento elaborado por la Comisión Europea trata de responder las preguntas más frecuentes en torno a la Directiva de Servicios de Pago de la Unión Europea 2 (PSD2 por sus siglas en inglés), activa desde el 13 de enero de 2018.

Entre las preguntas:

. ¿Qué es la directiva de servicios de Pago

. ¿Por qué se propuso la revisión de esta directiva?

. ¿Cuáles son los principales objetivos de la directiva revisada?

. ¿Cuáles son las principales diferencias entre PSD1 y PSD2?

. ¿Qué beneficios trae a los usuarios esta directiva?

Con el incremento en el número de transacciones y, por consiguiente, el volumen de dinero que se mueve en el comercio online, hemos visto también cómo el fraude online crece cada año

en el total de transacciones. Sin embargo, según la Memoria Anual sobre la Vigilancia de los Sistemas de Pago que publica el Banco de España, las últimas cifras disponibles (de 2016) reflejan un incremento de las operaciones fraudulentas con tarjetas emitidas en España, que pasaron de 687.000 en 2015 a 888.000 en 2016. El importe de las mismas ascendió de 52 a 56 millones de euros, lo que, teniendo en cuenta el número de tarjetas en circulación en España arroja un promedio algo superior a

Según los últimos datos, menos del 4% de los pedidos que llegan a una tienda virtual son de origen fraudulento, lo que supone un porcentaje muy bajo en el total de transacciones

una operación fraudulenta al año, por un importe de 63 euros, por cada 100 tarjetas.

Aunque es importante recordar que el fraude con tarjetas también incluye usos fraudulentos de las mismas en canales convencionales; por ejemplo, compras en tienda física con tarjetas clonadas o, directamente, robadas, estas cifras, que suponen unas tasas de fraude del 0,021 % en número de operaciones y del 0,022 % en términos de importes, son, en efecto, muy bajas si las comparamos con datos de otros países. Es más, según datos de Nilson Report las pérdidas mundiales por fraude con tarjetas se elevaron a más de 21.000 millones de dólares en 2015 (unos 17.000 millones de euros), lo que hace que el porcentaje con el que contribuye España sea del 0,3%.

Sin embargo, lo que deben tener siempre presente las compañías de ecommerce es que, del total de las operaciones detectadas en España, el 69 % corresponde a la operativa a distancia, lo que incluye comercio online, operaciones a través de email y telefónicas. En términos de importe, el fraude en las compras a distancia supone un 64 %, aunque se ha observado un descenso en la tasa de fraude en términos de importe (del 0,329 % en 2015 al 0,287 % en 2016).

Una vez más, las cifras no son preocupantes en su conjunto, pero tampoco pueden ser desdeñadas por los minoristas debido a la tendencia creciente de las mismas. Si no en porcentaje, al menos sí en volumen (€). A las pérdidas económicas directas que supone este tipo fraude, por ser pérdida desconocida que impacta en los márgenes, se le puede sumar el impacto reputacional que supone entre los clientes, las posibles multas de las entidades emisoras de tarjetas si no se establecen las necesarias salvaguardas, o la pérdida de operatividad asociada. Todos ellos son efectos secundarios

A las pérdidas económicas directas de este tipo fraude se le puede sumar el impacto reputacional, las posibles multas de las entidades emisoras de tarjetas o la pérdida de operatividad asociada

indeseados cuya repercusión puede ser mayor de lo que creemos.

Y ante este panorama, ¿cómo podemos prepararnos para luchar contra el fraude en el comercio online? ¿Qué medidas deben tomar las compañías para minimizar su impacto? Una de las medidas más recomendadas, y que será obligatoria una vez sea efectiva la trasposición de la nueva Directiva sobre Servicios de Pago, es la implantación de sistemas de verificación de la identidad en dos pasos a través del envío de una clave aleatoria a través de SMS al teléfono del titular de la tarjeta.

Gracias al crecimiento exponencial de datos de todo tipo que hoy en día somos capaces de almacenar, y que de hecho guardamos en multitud de bases de datos de todo tipo, hoy día contamos con otros mecanismos que nos facilitan el proceso de toma de decisiones. Estamos hablando, por supuesto, del Big Data, los algoritmos de Machine Learning y las soluciones de monitorización transaccional para la prevención de fraude, que están obteniendo muy buenos resultados en las empresas en las que se están implantando. Gracias a la combinación de estas herramientas, es posible detectar, de forma automática, la aparición de anomalías en el comportamiento de una red o comunidad determinada.

En los últimos tiempos se han puesto en marcha distintas iniciativas en este ámbito, que arrojan resultados muy positivos: en la mayoría de los casos, el uso de herramientas de inteligencia artificial logró una reducción del 10% del fraude en tarjetas de crédito. Además, se triplica la eficiencia de cualquier sistema ya puesto en marcha y reduce el número de comprobaciones y, por ende, investigaciones finales, lo que acaba redundando en una optimización de los costes asociados.

Estamos, pues, en un momento clave de la lucha contra el fraude. Se abren ante nosotros oportunidades con las que hace unos años no podíamos ni soñar. Saber aprovechar estas nuevas capacidades se ha convertido en una necesidad para las compañías que saben lo que se juegan.

Enlaces de interés...

- Los principios de la protección de datos
- España, por encima de la media en fraude
- GoNetFPI y 1st Secure IT se unen en la lucha contra el fraude en medios de pago
- ¿Está tu empresa preparada para evitar el fraude?
- Haciendo frente a PSD2

¿Te avisamos del próximo IT Digital Security?