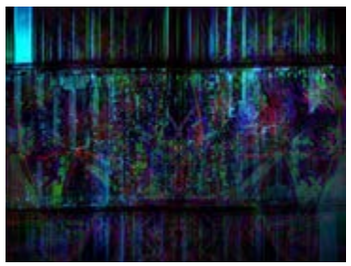
it Digital Security

La publicación electrónica sobre Seguridad Digital que necesitas

Junio 2018 - nº 9

Por qué necesitas una web segura (HTTPS)

La capa de aplicación, el lugar correcto para establecer la defensa



VPNFilter, el nuevo caos que amenaza Internet

Continúa la consolidación en el mercado de seguridad

#ITWebinars GDPR, el último empujón

#DesayunosITDS Ciberseguridad 4.0, repasamos el sector

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

Por qué necesitas una web segura

Tener una página segura es vital. Para ello, en lugar de HTTP se debe utilizar el protocolo HTTPS, algo que se identifica en la mayoría de los navegadores con un candado verde al comienzo de la URL. HTTPS no sólo garantiza que nos estamos conectando a la página a la que nos queremos conectar, sino que lo que se envía, como números de tarjetas de crédito, contraseñas o nombres de usuarios, se hace de manera cifrada y segura. En esencia, se trata de mantener una conversación privada entre las dos partes.

Además de por seguridad, utilizar HTTPS impedirá que algunos navegadores, como Google Chrome, identifique las páginas web que no estén utilizando este protocolo como inseguras, lo que no sólo impactará en la imagen de la compañía, sino que repercutirá en el posicionamiento de la página. Todo esto, junto con la manera de conseguir certificados de seguridad gratuitos, centra el tema de portada, pero hay mucho más en este número.

Volvemos a celebrar uno de nuestros #DesayunosITDS, en el que han participado expertos de SonicWall, Trend Micro, Kaspersky Lab y S21Sec, para hablar de Ciberseguridad 4.0, o lo que es lo mismo, de los problemas de seguridad avanzados, de herramientas y soluciones de seguridad vanguardistas, de tecnologías basadas en aprendizaje que puedan hacer frente al nuevo panorama de amenazas.

El 25 de mayo GDPR, el reglamento de protección de datos de la Unión Europea pasaba a ser de obligado cumplimiento. Quisimos darle un último empujón con la celebración de un webinar en el que participaron expertos de Trend Miro, ESET, Check Point, Thales e-Security, BitDefender y WatchGuard, cada uno de los cuales planteó su propuesta para cumplir con una normativa que ya forma parte de nuestro día a día.

La actualidad del mes ha estado marcada con VPNFilter, un malware que ha infectado más de medio millón de routers y sistemas NAS. Además de poder espiar el tráfico que se enruta a través de los dispositivos, los ciberdelicuentes tienen la capacidad de poder poner fin a estas máquinas, dejando a cientos de miles de personas sin acceso a internet.

También hacemos un repaso por las adquisiciones de los primeros meses del año, y hablamos con directivos de Akamai sobre cuál es el lugar correcto para establecer la defensa, y de SonicWall sobre la nueva estrategia de la compañía.

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

¿Te avisamos del próximo IT Digital Security?

En Portada

No solo IT

Infraestructuras TI definidas por software

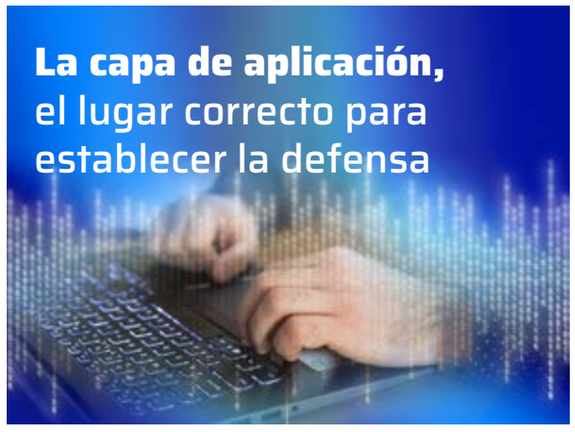
He sufrido un incidente de seguridad, ¿y ahora que hago?

La ciberseguridad y su asegurabilidad

Índice de anunciantes

¿Te avisamos del próximo IT Digital Security?

Actualidad



Webinars ITDS

Desayunos ITDS

Ciberseguridad 4.0

Webinar ITDS

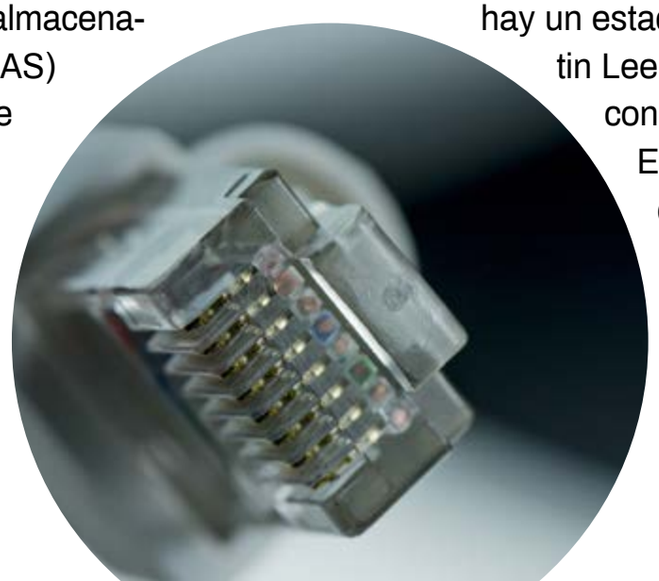
GDPR, el último empujón

VPNFilter, el nuevo caos de Internet

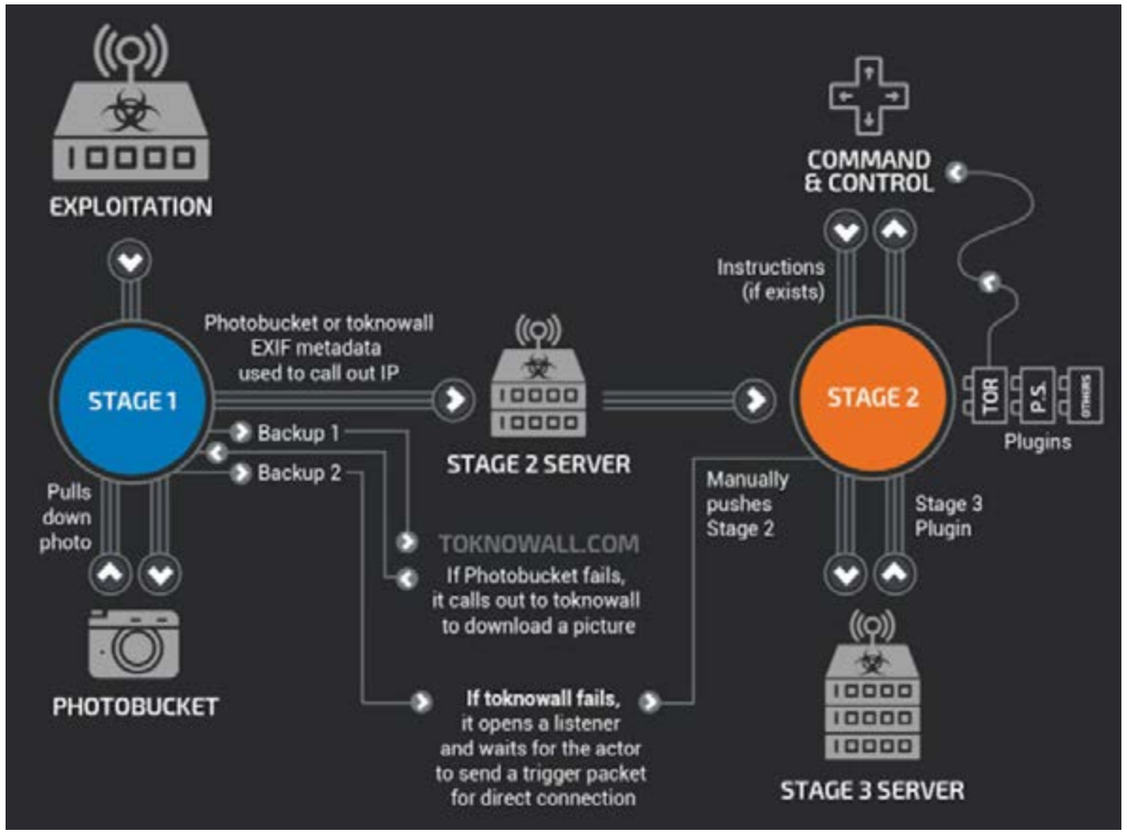
Investigadores de seguridad del grupo Cisco descubrieron una enorme botnet compuesta por más de 500.000 routers y dispositivos de almacenamiento conectado a la red (NAS). Los expertos aseguran que, además de leer el tráfico de red, el malware, bautizado como VPNFilter, es capaz de poner fin a los dispositivos afectados, dejando a cientos de miles de personas sin conexión a Internet.

"Detrás de cada ataque hay un individuo", asegura Martin Lee, Technical Lead, Threat Intelligence, Cisco Talos. Y lo dice mientras hablamos de VPNFilter, un nuevo malware que marcará un antes y un después en la historia de la seguridad, como ya lo hizo Mirai el año pasado. Tanto la escala como la capacidad del malware es lo que ha alertado y preocupado a una comunidad que está acostumbrada a trata con cientos de nuevos programas maliciosos cada día.

Se calcula que la cantidad de dispositivos infectados es de al menos 500.000 repartidos en al menos 54 países. Los dispositivos conocidos afectados por VPNFilter son los equipos de redes Linksys, MikroTik, NETGEAR y TP-Link, así como en los dispositivos de almacenamiento conectado a la red (NAS) de QNAP. La investigación de Talos, parte de la cual salió publicada en un post de la compañía, apuntó a que la actividad relacionada con el malware había aumentado en las últimas semanas y los atacantes parecían estar particularmente interesados en objetivos situados en Ucrania.



"Es casi seguro que detrás de las amenazas hay un estado nación", nos decía Martin Lee en una entrevista telefónica concedida a **IT Digital Security.** El malware "permite a los atacantes leer el tráfico de red. Además, sabemos que hay un módulo de este software que es capaz de leer un sistema SCADA, de modo que el impacto a este sistema



Etapas de VPNFilter (Fuente: Cisco Talos)

El objetivo del malware es crear una infraestructura expansiva y difícil de atribuir que se puede utilizar para satisfacer las múltiples necesidades operativas del actor de amenazas

de control industrial también le da otra dimensión a este malware".

VPNFilter es diferente a la mayoría de las otras amenazas de IoT porque es capaz de mantener una presencia persistente en un dispositivo infectado, incluso después de un reinicio. VPNFilter tiene una gama de capacidades que incluye espiar el tráfico que se enruta a través del dispositivo. Y sí, sus creadores parecen tener un interés particular en los sistemas de control industrial SCADA, creando un módulo que intercepta específicamente las comunicaciones Modbus SCADA.

Y lo que también llamó la atención de los investigadores de Talos es la capacidad destructiva de VPNFilter "que puede activarse en máquinas de víctimas individuales o en masa, y tiene el potencial de cortar el acceso a Internet a cientos de miles de víctimas en todo el mundo".

Con toda esta información Cisco ha estado trabajando "en colaboración con otras organizaciones, tanto públicas como privadas, para monitorizar las actividades del malware y desactivar los sistemas de comando y control que mantienen activa la amenaza que controla esta red de dispositivos comprometidos".

Nos explica también Martin Lee que el tipo de dispositivos a los que se dirigen los ciberdelincuentes con VPNFilter son difíciles de defender porque

habitualmente estén en el perímetro de la red, sin un sistema de prevención de intrusiones (IPS), “y sin embargo están conectados a internet, son vulnerables, los malos saben que están ahí afuera, saben que pueden verse comprometidos y saben que esto se puede usar para convertirse en parte de sus redes para causar daño”. Para colmo “la mayoría de los dispositivos tienen vulnerabilidades públicas conocidas o credenciales predeterminadas que hacen que el compromiso sea relativamente sencillo”.

VPNFILTER - BREAKING DOWN THE THREAT

CLICAR PARA VER EL VÍDEO

"Sabemos que hay un módulo de VPNFilter capaz de leer un sistema SCADA, de modo que el impacto los sistemas de control industrial también le da otra dimensión a este malware"

Para Martin Lee, una de las claves del alcance e impacto de esta nueva amenaza es que implica dispositivos simples que están conectados a Internet y a los que se no se presta atención. El hecho de que den servicio a usuarios y pequeñas oficinas es un añadido “porque la destrucción de estos dispositivos con el tamaño de esta red sería muy dañina. Por eso que pensamos que es tan importante que la gente conozca el alcance de este ataque y también por qué es tan importante trabajar con nuestros socios para desmantelarlo y evitar que se use para causar daño”.

Sobre si este tipo de ataques que llegan a los medios de comunicación generan conciencia de seguridad, dice Martin Lee que “ciertamente hace que la gente piense en la seguridad de sus dispositivos conectados a medida que nos movemos hacia un mundo de internet de cosas con pequeños dispositivos informáticos que van a estar conectados a Internet de una manera u otra”.

La amenaza del IoT no es nueva. Mirai tuvo un gran impacto y se han visto otros ejemplos con más o menos acierto, con más o menos alcance. ¿Podemos esperar un cambio de actitud por parte de las

empresas? “Bueno, necesitamos que las empresas comiencen a pensar en ello y estén al tanto de la naturaleza de las amenazas que existen. El entorno de amenaza es algo que está en constante cambio. Esta es la primera vez que hemos visto un ataque de esta naturaleza y es importante para las empresas pensar cómo sus sistemas están expuestos a Internet”.

Comentamos también con Martin Lee las conversaciones detectadas en la Dark web sobre el uso de dispositivos de IoT para hacer minería de criptodivisas. La respuesta del directivo de Cicos Talos no puede ser más clara: “Detrás de cada ataque hay un individuo, los ciberataques no ocurren por accidente. Detrás de cada ataque hay un individuo con objetivos concretos”. Todo puede ser.

"Esta es la primera vez que hemos visto un ataque de esta naturaleza y es importante para las empresas pensar cómo sus sistemas están expuestos a Internet"

¿Cómo funciona VPNFilter?

VPNFilter es malware que funciona en varias etapas. En la primera se instala y mantiene una presencia persistente en el dispositivo infectado, y se comunicará con un servidor de comando y control (C&C) para descargar más módulos.

La segunda etapa contiene la carga principal y es capaz de recopilar archivos, ejecutar comandos, extraer datos y administrar dispositivos. También tiene una capacidad destructiva y puede “bloquear” efectivamente el dispositivo si recibe un comando de los atacantes. Lo hace sobrescribiendo una sección del firmware del dispositivo y reiniciándolo, dejándolo inutilizable.

Hay varios módulos conocidos de la Etapa 3, que actúan como complementos para la Etapa 2. Estos incluyen un rastreador de paquetes para espiar el tráfico que se enruta a través del dispositivo, incluido el robo de credenciales del sitio web y la supervisión de los protocolos Modbus SCADA. Otro módulo de la Etapa 3 permite que la Etapa 2 se comunique mediante Tor.

A los usuarios con dispositivos afectados se les está recomendando que los reinicien cuanto antes.

Enlaces de interés...

- Cómo proteger los routers domésticos de ataques como VPNFilter
- El FBI recomienda reiniciar los routers para contrarrestar a VPNFilter
- Primeras medidas para detener a VPNFilter
- 500.000 routers afectados en más de 54 países por el malware VPNFilter

Compartir en RRSS

Lo que es verdaderamente importante para hacer frente a VPNFilter es aplicar los parches a los dispositivos afectados

En todo caso, si el dispositivo está infectado con VPNFilter, el reinicio eliminará la Etapa 2 y cualquier elemento de la Etapa 3 presente en el dispositivo. De forma que el reinicio eliminará, al menos temporalmente al menos el componente destructivo de VPNFilter. Sin embargo, si está infectado, la presencia continuada de la Etapa 1 significa que las Etapas 2 y 3 pueden ser reinstaladas por los atacantes.

Lo que es verdaderamente importante es aplicar los parches a los dispositivos afectados.

Quién está detrás del ataque

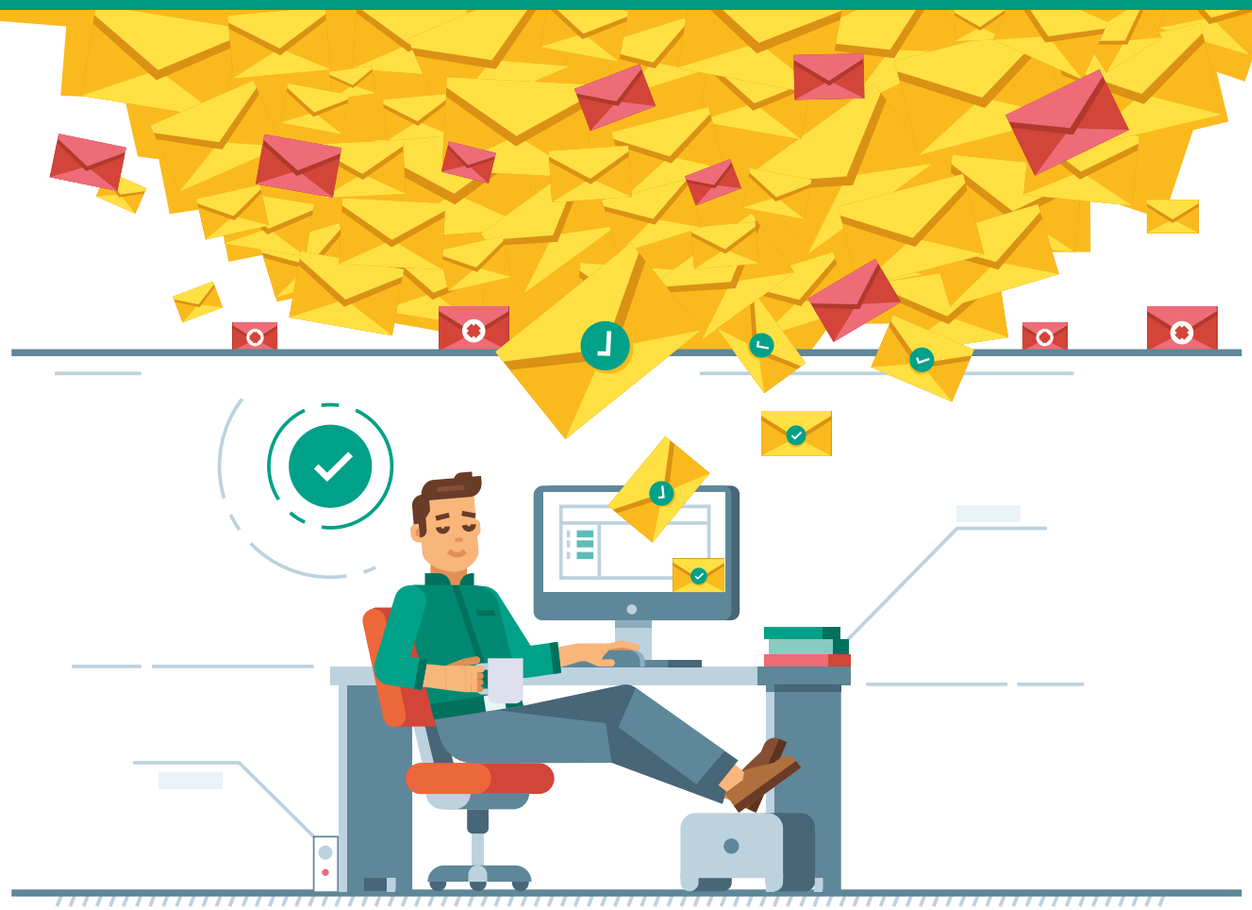
Las primeras noticias publicadas por Cisco Talos ya apuntaban a que detrás de VPNFilter estaba una nación estado. El objetivo del malware es crear una infraestructura expansiva y difícil de atribuir que se puede utilizar para satisfacer las múltiples necesidades operativas del actor de amenazas. Dado que los dispositivos afectados son legítimamente propiedad de empresas o particulares, la actividad maliciosa realizada desde los dispositivos infectados podría atribuirse por error a quienes realmente fueron víctimas del actor. Las capacidades incorporadas en las diversas etapas y complementos del malware son extremadamente versátiles y permitirían al actor aprovechar los dispositivos de múltiples maneras.

Los actores con amenazas avanzadas, incluidos los estados-nación, tratarán de hacer que la atribución de sus actividades cibernéticas sea extremadamente difícil, a menos que sea de su interés que se sepa abiertamente que llevaron a cabo un acto específico. Con este fin, los actores con amenazas avanzadas utilizan múltiples técnicas, incluida la infraestructura de cooptación propiedad de otra persona para llevar a cabo sus operaciones. El actor podría usar fácilmente los dispositivos infectados con este malware como puntos de salto antes de conectarse con su víctima final con el fin de ocultar su verdadero punto de origen.

En todo caso, y a pesar de algunos titulares, no se ha podido demostrar que efectivamente el gobierno ruso esté detrás del posible ataque.

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

SonicWall, la Zero Day Protection Company

No hace mucho que hablábamos de SonicWall. Coincidía con el nombramiento de Sergio Martínez como Country Manager de la región de Iberia, coincidía con el lanzamiento de nuevos productos y con el despertar de una compañía que sigue recuperando el tiempo perdido.

Nada mejor que reunir a los partners para poner las cartas sobre la mesa. Los partnes, los pulmones de las empresas para aumentar ese 'breath' con el que tantos sueñan, quieren tener claro que han apostado por caballo vencedor, que el tiempo y el esfuerzo dedicado a certificaciones no es en vano. Y parece que con la nueva SonicWall el futuro está asegurado.

Separada de Dell, la compañía está sedienta de innovación y no deja de lanzar novedades. Novedades con mayúsculas, porque no se trata sólo de mejorar productos al compás de los naturales avances de las tecnologías, sino de adentrarse en nuevos segmentos del mercado, como el mundo del endpoint o el de la virtualización.

La vida de la nueva SonicWall es un no parar y los primeros que se muestran encantados con la situación son sus valedores, Francisco Partners, uno de los fondos de inversión que rescató a SonicWall

LOS OSCUROS SECRETOS DE LOS FIREWALLS

Entre los hallazgos de la encuesta global realizada por la compañía cabe mencionar que los responsables de TI simplemente no pueden identificar casi la mitad (45%) del tráfico de red de su organización.

Estos son números asombrosos, especialmente en vista de la cantidad cada vez mayor de datos que fluyen diariamente hacia las arcas de almacenamiento de la empresa. Si no puede identificar qué tipo de datos se están ejecutando a través de la red de su sistema, su empresa tiene un serio riesgo de seguridad.

de las manos de Dell, donde la pequeña compañía languidecía a la sombra de un gigante. Y es que recientemente se anunciaba que los resultados de SonicWall habían superado sus objetivos financieros durante seis trimestres consecutivos, al tiempo que se registra una tasa de renovación de clientes de más de 90% por ciento para el primer trimestre, un aumento del 14 por ciento anual.

Los partnes de la compañía comprobaban el 23 y 24 de mayo en Barcelona y Madrid respectivamente, en sendos roadshows, el nuevo ritmo de la compañía. Nos lo ha contado Sergio Martínez, Director General de SonicWall para España y Portugal asegurando que “nunca ha habido tanta innovación en SonicWall al mismo tiempo”.

Ha habido cuatro grandes líneas de innovación. Explica Sergio Martínez que la primera se centra en la renovación de firewalls de gama media, la gama NSa (3650, 4650, 5650), dotados de más rendimiento, más capacidad…

Pero quizá más importante ha sido la entrada de SonicWall en el mundo del endpoint. Se ha presentado Capture Client y que el Product Manager de SonicWall haya venido desde California a España

indica la importancia que la compañía ofrece a este producto; Capture Client es “un endpoint conectado a nuestra nube y basado en el motor más potente que existe en el mercado de próxima generación que es SentinelOne, con quienes hemos firmado una alianza”, nos cuenta Sergio Martínez, añadiendo que mientras que el corazón late con SentinelOne, SonicWall incorpora la sincronía con los firewalls, “de forma que de manera centralizada puedes controlar todos los portátiles de la compañía junto con los firewalls , estableciendo reglas... “Es muy potente”, asegura el director general de SonicWall Iberia.

La tercera gran novedad es la entrada de la compañía en el mundo virtual. Al respecto se han presentado firewalls virtuales, que según Sergio Martínez “es una gran demanda en el mercado a pesar de que todavía el 90% del mercado es firewall

"Queremos ser la la Zero Day Protection Company. Preparar a los clientes para enfrentarse a amenazas desconocidas"

"Capture Client es un endpoint conectado a la nube y basado en uno de los motores más potentes que existe en el mercado de próxima generación que es SentinelOne"

físico". La compañía, que entra con fuerza y ya ha cerrado las primeras operaciones, ha presentado un appliance para VMware, en junio llegará el de Amazon, HyperV, Azure, y en julio llegarán más, incluido el de Google. "De forma que nos metemos de pleno con appliances de firewall en el mundo virtual", resume Sergio García.

Pero queda más, porque no contentos con todo lo que han hecho, siguen adelante y apuntan ahora hacia el mercado de firewall de aplicaciones, o WAF (Web Application Firewall). Nos explica el directivo que ya tenían incorporado un WAF en un appliance, pero que ahora lo han separado "y lo convertimos en un appliance virtual que se puede escalar de forma muy potente". Es un anuncio interesante teniendo en cuenta que parece que los ataques

contra la capa de aplicaciones no paran de crecer, algo lógico por otra parte teniendo en cuenta que hace tiempo que las aplicaciones se han ido a la nube. Lo que hace el WAF es ponerse en medio para detectar ataques contra los servidores web con la ventaja añadida, en el caso de SonicWall, de que están conectados a su Capture Cloud, la nube de la compañía donde están los motores de sandboxing y desde donde dotan de inteligencia a todos los dispositivos.

Recordar que en abril de 2018 SonicWall anunciaba Capture Cloud Platform, que integra seguridad, gestión, análisis e inteligencia de amenazas en tiempo real en toda la cartera de productos de seguridad de red, correo electrónico, móvil y en la nube de la compañía.

Enlaces de interés...

- Con Sergio Martínez, SonicWall quiere conquistar el midmarket
- SonicWall lanza Capture Cloud Platform, seguridad unificada y conectada
- Europa recibió el 37% de los ataques de ransomware lanzados en 2017
- La seguridad de las Comunicaciones
- SonicWall anuncia nuevas soluciones de seguridad de próxima generación

La tercera gran novedad es la entrada de la compañía en el mundo virtual. Ya se ha presentado un appliance para VMware, y en junio llegarán más, como el de Amazon o HyperV

No queda aquí todo, porque Sergio Martínez nos adelante que "vienen más novedades", como la próxima presentación del GSM en la nube; "le estamos dotando de mucha más información para poder conectarlo a muchas cosas". La parte pública de ese gestor es securitycenter.sonicwall.com, una web que te informa de los ataques en tiempo real que se están produciendo en todo el mundo. Tiene tres pantallas, una es el mapa del mundo que muestras las oleadas de ataques en tiempo real; otra pantalla con estadísticas mensuales de cómo evoluciona el ransomware, etc.; y la tercera pantalla con información sobre nuevas vulnerabilidades.

¿Cuál es el objetivo de tanta innovación? "Ser la Zero Day Protection Company. Preparar a los clientes para enfrentarse a amenazas desconocidas. Y eso se hace con una defensa en profundidad. Nosotros somos conocidos en el mundo del firewall, pero ahora nos metemos en el mundo del endpoint, orquestándolo todo y dotándolo de inteligencia en la nube".

¿Y cuál es el papel del partner en esa nueva SonicWall? "Vital, queremos que de un paso más y que venda servicios a sus clientes. Que con nuestra tecnología y nuestra plataforma cloud, pueda construir servicios de gestión de la seguridad a sus clientes, y se convierta en el CISO de las empresas medianas que no tienen, ni tendrán nunca, un CISO porque no tienen capacidad para ello".

'QUEREMOS IR MÁS ALLÁ DE LA SEGURIDAD PERIMETRAL' (EDUARDO BRENES, SONICWALL) CLICAR PARA VER EL VÍDEO

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

La capa de aplicación,
el lugar correcto para establecer la defensa

Continuamos viendo una tendencia de ataques que se mueven hacia la capa de aplicación desde la capa de red, haciendo que la defensa sea más complicada. Nos los contaba John Summers, Vicepresidente y CTO de Akamai, quien vino a España para intervenir en la Conferencia internacional de Seguridad que cada año organiza ISMS Forum.

John Summers llegaba a Madrid para hablar del actual panorama de amenazas de seguridad y el papel de los CISO, que tienen el desafío de detectar amenazas y mitigar los ataques maliciosos procedentes de botnets y atacantes sofisticados que buscan explotar vulnerabilidades web específicas. Su charla se tituló ¡Historias de guerra en la nube y el mayor ataque jamás visto!, donde además de lo anterior Summer habló de la plataforma inteligente desplegada globalmente de Akamai, de la enorme visibilidad que esta plataforma otorga a la compañía, de las últimas tendencias en ataques DDoS y capas de aplicaciones, del aumento de ataques en puntos finales API, de tendencias recientes en ransomware…

¿Te avisamos del próximo IT Digital Security?

"Los dispositivos de internet serán capaces de ataques significativos y peligrosos durante los próximos tres años como mínimo"

John Summers,
Vicepresidente y CTO de Akamai

Y entre unas cosas y otras conseguimos mantener un breve encuentro en el que CTO de Akamai nos aseguró que las amenazas siguen creciendo y evolucionando y que en 2018 veremos el mayor ataque que jamás hemos visto en internet. "Desde la perspectiva de DDoS, continuamos viendo un incremento de los bots, que buscan en la infraestructura de los clientes la manera de robar los datos", nos cuenta el CTO de Akamai, asegurando también que se observa "una tendencia continua de ataques hacia la capa de aplicaciones alejándose de la capa de red, lo que hace que sea más difícil para los clientes defenderse contra ellos".

Hace tiempo que se habla del fin del perímetro, a pesar de lo cual los responsables de TI siguen defendiendo sus infraestructuras de una manera tradicional. Las aplicaciones web, los sites, viven fuera del centro de datos y eso hace que esas webs y las aplicaciones basadas en cloud estén en constante riesgo de unas amenazas que se hacen cada vez más sofisticadas. Habla John Summers de controles de seguridad multicapa, de "entender a tus enemigos y sus armas" y de dos categorías generales de ataques: DDoS y los que van contra la capa de aplicaciones para robar datos.

Predice Akamai que para 2020, el ataque DDoS promedio (DDoS) generará 1,5 Tbps de tráfico de red, pero que incluso los ataques de denegación de servicio grandes y sofisticados de hoy en día pueden fácilmente saturar los recursos de TI disponibles. "Cuanto más comprenda los matices de los diferentes tipos de ataques DDoS y amenazas web, mejor podrá determinar cómo afectarán a su red".

it whitepapers

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.

GDPR, YA ESTÁ EN VIGOR!

Si su empresa maneja datos personales considerados de Alto Riesgo

En Thales podemos ayudarle

#APTOparaGDPR

THALES

MITIGAR UN ATAQUE DDOS CON AKAMAI

CLICAR PARA VER EL VÍDEO

John Summers aconseja practicar una buena higiene de aplicaciones web mediante el uso de un ciclo de vida de desarrollo de software seguro

John Summers asegura que el IoT es la fuente de los mayores ataques que hemos visto. “Desafortunadamente la mayoría de los dispositivos de consumo que se están vendiendo llegan al mercado con terribles fallos de seguridad”, dice el CTO de Akami, explicando que muchos de ellos son lanzados con contraseñas por defecto que son fáciles de adivinar; con fallos en el software y sin posibilidades de actualizar el firmware. “De forma que tenemos millones de dispositivos ahí fuera, en nuestras casas, en nuestros negocios que los hackers conocen, saben cómo conectarse a ellos, cómo explotarlos… y que pueden aprovecharse para lanzar grandes ataques”.

Planteamos a John Summers si la expansión de 5G significará un cambio importante de cada al papel que los dispositivos conectados pueden tener en un ataque. Asegura el directivo de Akamai que el hecho de que 5G traiga consigo no sólo una mayor conectividad sino un mayor ancho de banda, “por eso es cada vez más importante conseguir que la seguridad de sea la correcta”.

Preguntamos a John Summers si la seguridad debe establecerse en las cosas o en la red. Para el directivo el primer paso está en el propio dispositivo conectado. Habla de establecer estándares que obliguen, por ejemplo, a que puedan cambiarse las contraseñas por defecto de los dispositivos que llegan al mercado. “Es algo muy simple de hacer y si hubiera reglas de fabricación que indicaran que deben ser lanzados con esa capacidad, con ese tipo de requisito…. Estos tipos de reglas ayudarían a que Internet sea mucho más seguro”, y añade que también debería exigirse que los dispositivos puedan actualizarse. Todo esto, dice el CTO de Akamai, “lleva tiempo”, lo que significa que las empresas tienen que suponer

que los dispositivos de internet serán capaces de ataques significativos y peligrosos durante los próximos tres años como mínimo; “Y eso significa aumentar sus defensas y poner en su lugar las protecciones de la capa de aplicaciones frente a las aplicaciones de negocios de su empresa”.

Vuelve a comentar John Summers que deben establecerse las defensas en la capa de aplicaciones. Explica el directivo que son cada día más comunes; son ataques contra el Sistema de nombres de dominio (DNS) y ataques que roban datos. Los intentos de robo de datos suelen tomar la forma de ataques de inyección de comandos en los que un hacker inserta comandos en una aplicación vulnerable. El atacante puede ejecutar estos comandos para ver datos, eliminar datos o hacerse cargo de la máquina. El directivo tiene claro que “la capa de aplicación es el lugar correcto para establecer la defensa, y no en la capa de red”, y nos explica que en realidad los usuarios están en la nube, son trabaja-

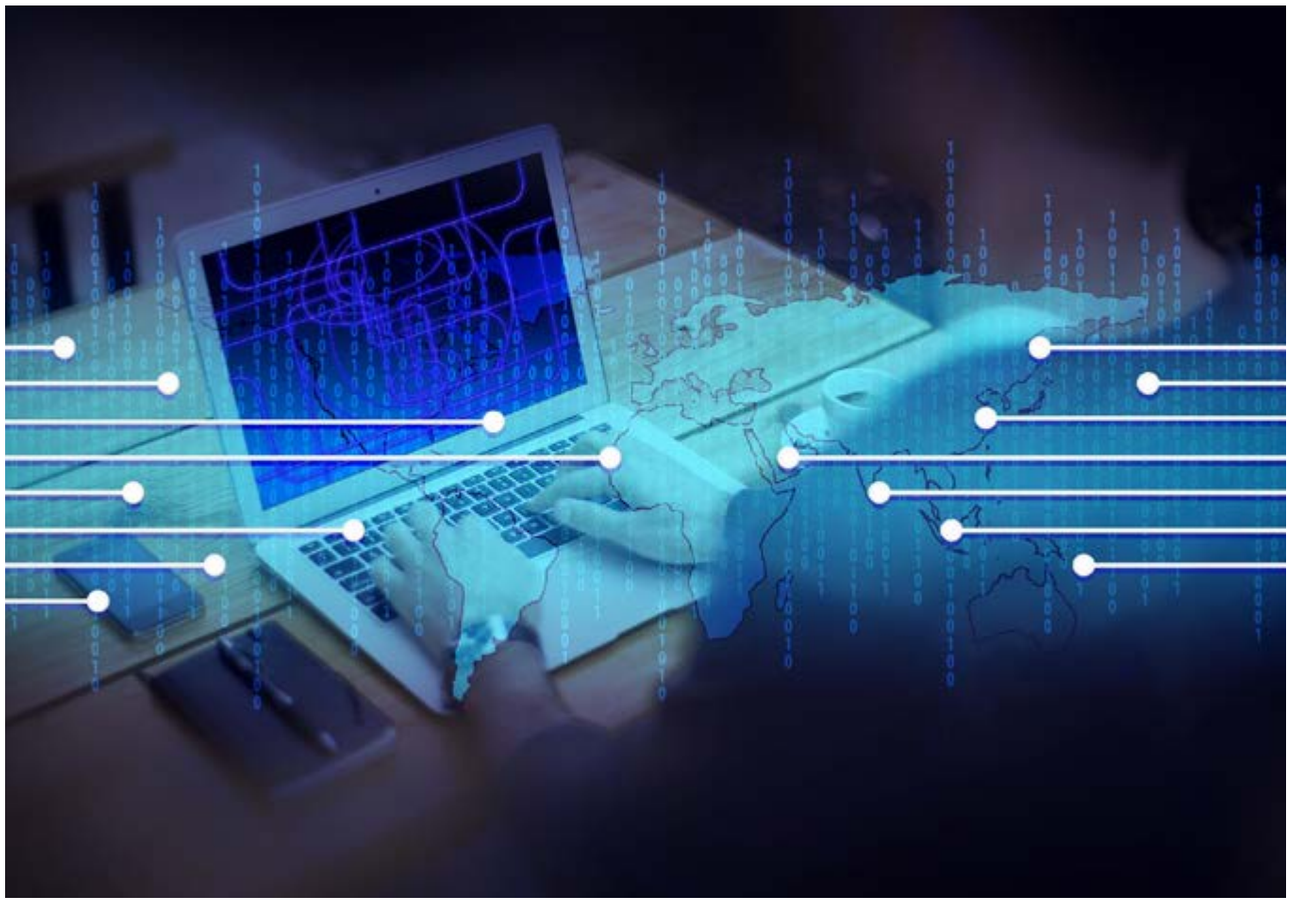
"Históricamente la gente no ha pensado mucho en la seguridad del DNS, pero esto está cambiando porque también es el lugar más rápido donde poder detectar un ataque"

dores móviles y las aplicaciones se mueven desde y hacia la nube, y eso significa que hay un usuario en la nube tratando de acceder a una aplicación de negocios que también está en la nube… “y todo esto hace que tengamos que dejar de pensar en una protección de seguridad en la capa de red y tengamos que pensar en la capa de aplicación”.

John Summers aconseja practicar una buena higiene de aplicaciones web mediante el uso de

un ciclo de vida de desarrollo de software seguro que incluye configuración segura, actualizaciones, parches y validación. Además, un firewall de aplicaciones web (WAF) con capacidades anti-DoS proporciona una sólida línea de defensa contra los ataques de la capa de aplicaciones, como la inyección SQL comúnmente utilizada para cubrir el robo de datos.

"La capa de aplicación es el lugar correcto para establecer la defensa, y no en la capa de red"



Por cierto, que el robo de datos a menudo se produce impunemente porque queda oculto en el tráfico cifrado. ¿Son las empresas conscientes del problema que genera el tráfico cifrado desde el punto de vista de la seguridad? “Todos saben que ven cada vez más tráfico en la red mundial va a HTTPS; ahora es más de la mitad y sigue creciendo”. Dice el directivo de Akamai que el tráfico cifrado es bueno para mantener las transacciones seguras, pero dificulta que las empresas sean capaces de hacer una inspección adecuada de dicho tráfico.

También hablamos con John Summers sobre DNS, en elemento que cada vez llama más la atención de los ciberdelincuentes, preguntándole si las empresas son conscientes de ello.

Asegurando que DNS es el primer paso para acceder a internet, que antes de que el navegador se conecte a un sitio web va al DNS a obtener una IP, asegura el directivo que la forma más eficiente de bloquear la conexión a sitios maliciosos está en el DNS.

En realidad, si el sistema de nombre de dominio, o DNS (Domain name System) no está adecuadamente protegido puede abusarse de él. Según un reciente estudio de Efficient IP, el coste medio de un ataque DNS en Estados Unidos ha crecido un 57%, respecto a datos del año pasado, hasta los 715.000 dólares en 2018. En los doce meses anteriores a la publicación del estudio las empresas se enfrentaron a una media de siete ataques DNS. Algunas de las víctimas acabaron pagando más de cinco millones de dólares en costes asociados; y una de cada cinco organizaciones (22%) sufrió una pérdida de negocio debido a un ataque de DNS:

Dice Summer que históricamente la gente no ha pensado mucho en la seguridad del DNS, pero que eso está cambiando porque también es el lugar más rápido donde poder detectar que se ha sido infectado con malware, “por eso cada vez más empresas están buscado la seguridad en la capa DNS y esa es la razón por la que verá a cada vez más proveedores de servicios ofrecer servicios de seguridad basados en DNS. Akamai tiene Enterprise Threat Protector, que

permite a los equipos de seguridad identificar, bloquear y mitigar de forma proactiva amenazas como el malware, el ransomware, el phishing y la exfiltración de datos que explotan la capa DND o de nombre de dominio (DNS) y que este verano explotarán

las capas HTTP y HTTPS “con el fin de ayudar a mantener a los clientes a salvo”.

Otro de los ataques que se está volviendo más habitual tiene que ver con el llamado crytojacking, el robo de recursos de computación para la minería de criptomonedas. Existen varios programas para hacer minería de criptodivisas, incluida Coinhive, Authedmine o Crypto-Loot; no son herramientas ilegales, pepero la falta de consentimiento por parte del usuario están haciendo que firmas de seguridad como malwarebytes las estén bloqueando.

El crypotojacking superó al ransomware como la principal amenaza de seguridad en el primer trimestre de este año. El cryptojacking es una amenaza que puede echar abajo una máquina por uso intensivo, sobrecalentando las baterías y acabar con la máquina. Una de las razones por las que se ha convertido en algo muy popular, además de por su rentabilidad, es que el ciberdelincuente sólo necesita unas pocas líneas de código para hacerlo funcionar. Según los expertos, los mineros de criptodivisas pueden poner las redes corporativas en riesgo de caída, además explotar el uso de CPU

Dice el CTO de AKamai que se está viendo un crecimiento importante de esta actividad en los últimos seis meses, pero que es fácilmente detectable poniendo controles tanto a nivel de DNS como de navegador.

El ransomware, por cierto, pierde popularidad por una serie de razones diferentes, una de ellas que el mercado empieza a estar sobrecargado de esta amenaza. Al menos es lo que dicen los expertos.

Enlaces de interés...

- Github sufre el mayor ataque DDoS hasta la fecha
- ‘Uno de los elementos principales en el coste de un ataque DDoS es el daño reputacional’ (Akamai)
- Echan el cierre al mayor marketplace de servicios DDoS del mundo
- Aumenta la demanda de soluciones de prevención y mitigación de ataques DDoS

Compartir en RRSS

Únete a la nueva experiencia en ciberseguridad

Big Data Security Analytics

CyberIntelligence Reports

Fraud Analytics

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

Continúa la consolidación en el mercado de seguridad

El de seguridad, o ciberseguridad, es uno de los mercados más fragmentados de la industria. Al mismo tiempo es uno de los más dinámicos, quizá porque las empresas que lo componen no sólo compiten entre sí, sino contra un enemigo común, el ciberdelincuente, que desde hace unos años ha profesionalizado y perfeccionado su negocio.

¿Te avisamos del próximo IT Digital Security?

PALO ALTO ANUNCIA LA COMPRA DE EVIDENT.IO

CLICAR PARA VER EL VÍDEO

Crecimiento orgánico vs crecimiento inorgánico, o lo que es lo mismo, invertir en innovación, o comprarla. El propio dinamismo del mercado de seguridad, que las amenazas sean más y más sofisticadas, está haciendo que las adquisiciones se aceleren, que haya que optar por invertir en tecnología ajena que permita mantener el ritmo. Un ejemplo sobre el que hablábamos recientemente es Quest Software, que en sus treinta años de vida ha acumulado más de 20 compras.

Y si queríamos ritmo, eso es lo que no le está faltando a este 2018, al menos en lo que respecta al mercado de seguridad. Se iniciaba el año con la noticia de Meltdown y Spectre, dos vulnerabilidades a nivel de chip que siguen de plena actualidad; se calculan unas 14 grandes brechas de seguridad contra retailers en lo que va de año y el escándalo de Cambridge Analytica y Facebook ha acabado con la primera y fijado la mirada en la segunda. Por no hablar de que, por fin, ha entrado en vigor GDPR, la nueva normativa de protección de datos que tienen que cumplir todas las empresas que gestionen datos de ciudadanos europeos.

Pero volviendo a lo que nos ocupa, las adquisiciones del mercado de seguridad han sido unas cuantas las que ya se han producido en lo que va de año. Empezaron pronto. Casi sin habernos sacudido el espumillón, el 4 de enero **Barracuda Networks** anunciaba la compra de PhishLine, y lo hacía mientras la propia compañía estaba en proceso de ser vendida a Thoma Bravo en un acuerdo de 1.600 millones de dólares anunciado meses antes. PhishLine permitía a Barracuda mejorar sus capacidades de protección del email para hacer frente al phishing, una amenaza que también estuvo tras la compara de Sookasa por parte de Barracuda en marzo de 2016.

> El 11 de enero FireEye anunciaba el cierre de un acuerdo de compra valorado en 20 millones de dólares por X15 Software

La víspera de Reyes **Verizon** confirmaba la compra de Niddel, fabricante de una solución de caza de amenazas que hace uso de Machine Learning sin que los detalles financieros fueran conocidos. Días después la consultora **KPMG** anunciaba la adquisición de la unidad de gestión de identidades y accesos (IAM) de Cyberinc, lo que le permitía sumar talento a su propia oferta, y el 11 de enero era **FireEye** quien anunciaba el cierre de un acuerdo de compra valorado en 20 millones de dólares por X15 Software, una empresa de Big Data, con objetivo de que su plataforma añada nuevas capacidades de monitorización, búsqueda y análisis de datos de seguridad generados por máquinas en entornos cloud y on-premise.

Dos días después era **Veeam Software** quien se convertía en protagonista por la compra de N2WS para reforzar la protección de datos en AWS. N2WS, por la que Veeam pagó 42,2 millones de dólares, y cuyos ingresos crecieron un 102% en 2017, operará como una compañía independiente, manteniendo su marca y convirtiéndose en “A Veeam Company”.

A mediados de enero se hacía público que **WatchGuard Technologies** compraba Percipient Networks para ayudar a mejorar la seguridad DNS. Sin des-

El 25 de enero Amazon Web Services (AWS) compraba Sqrrl, una joven empresa de seguridad cuyas capacidades de detección de amenazas potenciarán Amazon GuardDuty

velar los detalles financieros del acuerdo aseguraba la compañía que Strongarm, el producto estrella de Percipient, detiene los ataques de phishing y malware gracias a un servicio fácil de desplegar enfocado en la capa DNS (Domain Name System). Y días después se conocía que **One Identity,** una empresa perteneciente a Quest Software, había comprado Balabit, una compañía experta en gestión de accesos con privilegios.

El 22 de enero **Digi International,** un proveedor de productos y servicios de conectividad para el IoT, adquiría Accelerated Concets, un proveedor de equipos de redes móviles seguros y de categoría empresarial por 17 millones de dólares además de un pago adicional basado en el rendimiento.

El 24 de enero **Cisco Systems** anuncia planes para adquirir Skyport Systems, una compañía privada que ofrece sistemas hiperconvergentes administrados en la nube que ejecutan y protegen las aplicaciones críticas para el negocio. El equipo de Skyport Systems se unió al Data Center – Computing Systems Product Group y al Service Provider – Networking Group sin que los detalles financieros del acuerdo trascendieran. Por cierto, Cisco había sido uno de los inversores de esta empresa.

El 25 de enero se publicaba que **Amazon Web Services (AWS)** había comprado Sqrrl, una joven empresa de seguridad cuyas capacidades de detección de amenazas potenciarán Amazon GuardDuty, el servicio de detección de amenazas de que

El 14 de febrero Oracle anunciaba la compra de Zenedge para añadir a su oferta capacidades de seguridad de infraestructuras y de red basadas en cloud

Amazon lanzó el pasado mes de noviembre para proteger las cuentas y cargas de trabajo de sus clientes. Y el mismo día se sabía que Facebook, que día antes había anunciado un programa de becas para hacer que Internet sea más seguir, compraba Confirm, una joven empresa que desarrolla tecnologías de autenticación de ID que permitirá a Facebook mejorar la confirmación de identidades en su red social para proteger mejor a los usuarios.

Finalizando enero, el mismo día 30, **GitLab,** una empresa que ayuda a las organizaciones a administrar su ciclo de vida de desarrollo de software, anunciaba la adquisición de Gemnasium, un servicio que alerta a los desarrolladores de vulnerabilidades de seguridad conocidas en bibliotecas de código abierto y les ayuda a resolver esos problemas. Los términos financieros del acuerdo no fueron revelados.

Febrero

Las adquisiciones del mes de febrero arrancaban bien pronto. El día 1 **Bomgar,** un proveedor de soluciones de acceso seguro que en España está presente a través de Avansis, anunciaba la compra de Lieberman Software, un fabricante de gestión de credenciales e identidades con privilegios sin que los detalles financieros del acuerdo trascendieran.

El día 6 era **Proofpoint,** proveedor de soluciones de seguridad de correo electrónico basado en cloud, e-discovery y compliance, quien anunciaba la compra de Wombat Security. Los planes de Proofpoint pasaban por integrar sus capacidades de protección contra amenazas avanzadas con la tecnología de simulación de phishing en tiempo real y capacitación en ciberseguridad en Wombat, reconocido por Gartner en su Cuadrante Mágico para Security Awareness Computer-Based Training.

El día después y sin desvelar los detalles financieros, **Rubrik** anunciaba un acuerdo para la compra de Datos IO, experto en software de backup y recuperación para bases de datos NoSQL y sistemas de archivos de big data. La adquisición de Datos IO extenderá el alcance de Rubrik hacia aplicaciones en la nube de misión crítica y bases de datos cada vez más adoptadas por los equipos de aplicación y DevOps.

El 13 de febrero **Carbonite,** una empresa de backup y recuperación, se hacía con Mozy, un proveedor de servicios de backup seguros basados en cloud, por 145,8 millones de dólares en efectivo. Mozy era propiedad de Dell Technologies.

Un día después **Oracle** anunciaba la compra de Zenedge para añadir a su oferta capacidades de seguridad de infraestructuras y de red basadas en cloud. De manera más concreta combinación de Oracle y Zenedge equipa la oferta de Infraestructura como Servicio de Oracle con las con capaci-

El 22 de febrero Konica Minolta Business Solutions adquirió VioPoint, una firma consultora de ciberseguridad

El 15 de marzo Palo Alto Networks anunciaba la compra de Evident.io, un proveedor de servicios de seguridad cloud y automatización de cumplimiento

dades integradas de próxima generación de Web Application Firewall (WAF) y Denegación de Servicio Distribuido (DDoS) de Zenedge.

El 14 de febrero **VMware** firmaba la compra de CloudCoreo, fabricante de un producto que monitoriza los stack sde infraestructura en la nube en busca de errores, configuraciones erróneas y riesgos de seguridad en la nube. El día después era **KPMG** quien firmaba la adquisición de Cyberinc, una compañía de gestión de accesos e identidades. En ninguno de los casos se ha tenido información sobre la cuantía de las compras.

Los últimos días de febrero quedaron marcados por las compras de VioPoint, una empresa de consultoría de seguridad, por parte de **KonicaMinolta** y de PhishMe, experta en formación de ciberseguridad por una firma de inversión. Mientras que en el caso de Konica no se conocen los detalles financieros, en el de PhishMe, la adquisición tuvo u valor de 400 millones de dólares.

Marzo

Al igual que ocurría en febrero, marzo también se estrenaba pronto en adquisiciones, aunque esta vez fue sólo informativa. Y es que el día 1 **Akamai** Technologies revelaba el pago de 380 millones de dólares en 2017 por la adquisición de Soasta y Nominnum, adquisiciones que están diseñadas para mejorar el rendimiento web y las capacidades de ciberseguridad de Akamai.

El 8 de marzo **McAfee** anunciaba el cierre del acuerdo para adquirir TunnelBear, un proveedor de servicios de VPN. Los términos financieros del acuerdo no fueron revelados.

El 13 de marzo **CyberArk** anunciaba la compra de ciertos activos de Vaultive para impulsar los controles de seguridad cloud y agilizar la experiencia del usuario en lo relativo a las cuentas con privilegios y administradores cloud. Por cierto, que la de Vaultive y CyberArk era la sexta compra de una empresa con capacidades de CASB (cloud access security bróker) en los últimos años; reciente era la de Skyhigh Networks por parte de McAfee, y también se pueden mencionar la de Skyfence por parte de **Forcepoint,** la de CloudLock por parte de Cisco o la de FireLayers por Proofpoint.

También en marzo, el día 15, **Palo Alto Networks** anunciaba la compra de Evident.io, un proveedor de servicios de seguridad cloud y automatización de cumplimiento por 300 millones de dólares en efectivo. Integrando la tecnología de Evident.io, Palo Alto dijo que ayudará a sus clientes a asegurar que sus despliegues cloud son seguros y que cumplen continuamente con las normas de seguridad.

El 28 de marzo **VMware** anunciaba la adquisición de E8 Security, una compañía de análisis de com-

El 28 de marzo VMware anunciaba la adquisición de E8 Security, una compañía de análisis de comportamiento

El 2 de marzo Qualys anunciaba la compra de IMobility para mejorar la capacidad de su plataforma de cumplimiento y seguridad basada en cloud al mundo de los dispositivos móviles y el IoT

portamiento. Los términos financieros del acuerdo no fueron revelados.

Marzo se cerraba con el anuncio de que **Opaq Networks,** una empresa de seguridad en la nube de la red, adquiría FourV Systems, fabricante de GreySpark, que proporciona inteligencia empresarial para administrar las operaciones de seguridad. Los términos financieros del acuerdo no fueron revelados.

Abril

A primeros de abril, concretamente el día 3, **Qualys** anunciaba una ampliación de la capacidad de su plataforma de cumplimiento y seguridad basada en cloud al mundo de los dispositivos móviles y el IoT con la compra de 1Mobility. Los detalles financieros del acuerdo no han trascendido, pero según anunciaba la compañía la adquisición le permite ofrecer a las empresas de todos los tamaños la capacidad de crear y actualizar de manera continua un inventario de los dispositivos móviles de su entorno, ya sean Android, iOS o Windows Mobile; así como evaluar su postura de seguridad y cumplimiento.

El seis de abril **RSA** anunciaba la compra de Fortscale para ofrecer a sus clientes nuevas capacidades UEBA (user entity and behavioral analytics) a través de su plataforma RSA NetWitness SIEM. Fortscale se convertirá en parte de RSA NetWitness Platform, que ayuda a los responsables de seguridad a detectar y responder ataques, para “ofrecer la solución más completa de UEBA en el mercado”.

El 11 de abril **Palo Alto** anunciaba la compra de la firma israelí Secdo para potenciar Traps. De manera más concreta, la compra de Secdo lleva las capacidades de EDR (endpoint detection and response) de la firma israelí a Palo Alto Traps y a su Application Framework con el fin de mejorar su visibilidad y rapidez de detección, explica la compañía en un comunicado.

Mayo

El 8 de mayo **LookingGlass** anunciaba la compra de la plataforma de inteligencia de amenazas a Goldman Sachs. Competidor de IBM, Check Point o Trend Micro, LookingGlass ha adquirido Sentinel,

Enlaces de interés...

- Adquisiciones de empresas de seguridad
- Seis tecnologías que IAM debe tener en cuenta
- ¿Te enseña tu empresa cómo identificar el peligro?
- W Los principios de la protección de datos
- W El riesgo de los usuarios con privilegios
- W PCI DSS, la Seguridad de los datos de los pagos digitales a tu alcance

El 25 de mayo, y sin ofrecer información sobre los detalles financieros del acuerdo, Malwarebytes anunciaba la compra de Binisoft

la plataforma de SIEM desarrollada por la firma de servicios financieros para la gestión de la inteligencia de amenazas.

El 21 de mayo **Utimaco,** uno de los principales fabricantes de Hardware Security Modules (HSMs), anuncia su intención de adquirir a Micro Focus las líneas de negocio Atalla HSM y ESKM (enterprise secure key manager), con las que podrá estrechas las relaciones con empresas de servicios financieros y bancarios.

El 25 de mayo y sin ofrecer información sobre los detalles financieros del acuerdo, **Malwarebytes** anunciaba la compra de Binisoft, la compañía rumana responsable de Windows Firewall Control, para mejorar la gestión de los productos, y USB Flash Drives Control, para regular cómo se utilizan las memorias USB dentro de las empresas. Según las compañías, el Windows Firewall Control de Binisoft es utilizado por millones de usuarios y mejorará de manera significativa la plataforma de protección endpoint de Malwarebytes.

También el 25 de mayo **WISeKey International,** una compañía suiza experta en seguridad e IoT, anunciaba la adquisición del 15% restante de QuoVadis Holdings, una compañía líder en ciberseguridad con un fuerte enfoque en la próxima generación de infraestructura de clave pública (PKI), autoridad de certificación (CA) y servicios de firma electrónica (eID), con actividades operativas en Suiza, Alemania, los Países Bajos, Bélgica, el Reino Unido y las Bermudas.

Compartir en RRSS

GDPR, el último empujón

Aprobado en abril de 2016, el Reglamento Europeo de protección de datos es de obligado cumplimiento desde el 25 de mayo de 2018. Dos años que han sabido a poco, que han obligado a las empresas a tomar conciencia de que la seguridad no es una opción, que los datos son el activo más valioso y que la privacidad debe estar en primera línea.

A partir de ahí mucho que analizar, que estudiar y que tener en cuenta, seas empresa europea o no. Hay algunas preguntas que se deben saber contestar: qué ocurre con las legislaciones de los estados miembros como, en nuestro caso, la LOPD. A la hora de recoger los datos de los usuarios, ¿cambia la manera en que se debe obtener el consentimiento de los mismos? ¿Sabes cuándo o a quién hay que notificar un incidente de seguridad? ¿Sabes que debes contar con los servicios de un responsable de protección de datos, DPO?

Hay maneras de acelerar el cumplimiento. Entre ellas tener una total gestión de los datos, no sólo en cuanto a saber dónde están, imprescindible si se quiere cumplir con el Derecho al Olvido que ahora tienen los usuarios, sino quién accede a ellos mediante una gestión de identidades y accesos.

El momento ha llegado y si no estás preparado hay algunas acciones urgentes que puedes poner en marcha para acercarte a GDPR, limitar el impacto de

una brecha y reducir la cuantía de una multa. Para hablar de todo esto contamos con varios expertos de empresas líderes del sector que aclararán todos los aspectos de GDPR y cómo hacerle frente: José de la Cruz, Director Técnico de Trend Micro España y Portugal; Carlos Tostosa, Responsable de grandes cuentas y desarrollo de negocio de ESET España; Eusebio Nieva, Director Técnico Check Point España; Ignacio Berrozpe, Sales Engineer Thales e-Security; Juan Jesús Merino Torres, National Channel Country Manager de BitDefender y Carlos Vieira, Director general de WatchGuard Iberia

Trend Micro

Para José de la Cruz GDPR puede ser un habilitador más que un inconveniente para las empresas. Para ello lo primero que hay que hacer es entender la GDPR, un reglamento "que en realidad no aporta nada, sino que es un complemento a lo que había". Lo que hace GDPR, asegura el director técnico de Trend Micro, es "unificar, eliminar la inconsistencia" de las diferentes legislaciones. Además, recuerda que no sólo se aplica a las empresas europeas, sino a cualquiera que manipule datos de ciudadanos de la Unión Europea.

Explica José de la Cruz, que GDPR exige que se implemente seguridad por diseño y pensar de manera espcífica en la seguridad del dato, en segundo lugar un procesamiento seguir de datos para que no haya fugas de información o corrupción de los datos, además las fugas tienen que ser notificadas no sólo a la autoridad competentes, sino al propietario de los datos; finalmente se establece una evaluación continua de las normativa que garantice que se está cumpliendo.

"El gran habilitador de GDPR son las sanciones económicas", dice José de la Cruz, además de restricción en el uso de la información y el impacto en la imagen de la empresa.

Fundamental es identificar los datos que han de protegerse, además de ser capaces de evaluar si tenemos la seguridad adecuada para saber si tenemos la seguridad adecuada. Desde el punto de vista técnico, dice el director técnico de Trend Micro, esto implica una serie de retos, como la protección del dato y de la infraestructura que lo aloja; "no vale una protección genérica, sino adaptada a nuestro negocio".

Aplicar las mejores prácticas pasa por saber qué información estoy manipulando, por dónde puedo perderla e implementar un programa de gestión de filtraciones. La propuesta de Trend Micro es una protección inteligente que combina tecnologías intergeneracionales que protegen cualquier entorno y plataforma con el menor impacto posible, proporcionando al mismo tiempo Seguridad Conectada, "que es ofrecer la misma seguridad en todos los vectores de ataque de la organización".

Continúa José de la Cruz hablando de DLP (Data Lost Prevention) como una medida específica para proteger el dato. La solución de la compañía cuenta

"Lo más difícil es identificar el dato que tenemos que proteger. Es un punto clave en el que las compañías deben invertir la mayor cantidad de tiempo posible"

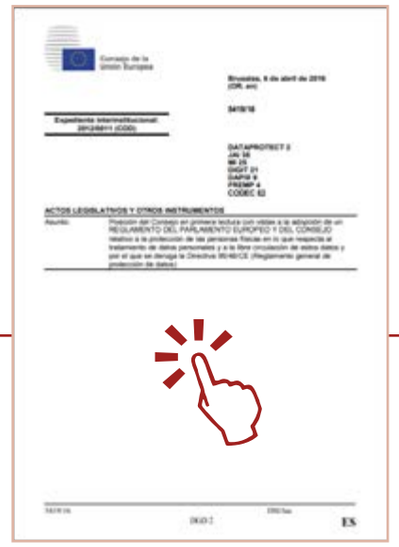
José de la Cruz, Director Técnico de Trend Micro

¿Te avisamos del próximo IT Digital Security?

LA GDPR EN ESPAÑOL, QUE NO TE LA CUENTEN

Hay mil y un documentos sobre la GDPR, la General Data Protection Regulation, la mayoría de los cuales destacan los cambios más importantes de la normativa, los artículos que más impacto pueden tener en las cuentas de la compañía, o qué pasos se deben seguir en caso de detectarse una brecha de seguridad.

Pero si no quieres que te la cuenten, aquí la tienes, en español.



"GDPR está obligando a las compañías a tomar medias y adecuar la formación a los empleados, que estamos más concienciados con la importancia de la seguridad de los datos"

Carlos Tortosa,
Responsable de grandes cuentas de ESET España

con unas 250 platillas predefinidas, muchas de ellas relacionadas directamente con GDPR. Otra de las medidas específicas es el cifrado de los datos, o mecanismos de protección continua, como la solución de parcheado virtual, así como las soluciones de protección de la nube y de la red.

"El camino más corto para proteger GDPR sería seguir con las recomendaciones: detectar los datos a proteger, implementar los mecanismos más adecuados que nos permitan proteger el dato y la infraestructura", concluye José de la Cruz.

ESET

"La información que tenemos nos dice que realmente no estamos preparados para GDPR", dice Carlos Tortosa, responsable de grandes cuentas en ESET España, añadiendo que no existen prórrogas a GDPR, y que entre las novedades de la normativa está que protege los datos de cualquier ciudadano y la obligatoriedad de notificar las brechas de seguridad, no sólo a la agencia estatal de protección de datos sino a la persona propietaria de los datos afectados.

Otras novedades mencionadas por Carlos Tortosa es que las sanciones pueden alcanzar entre el 2% y 4% la facturación de la empresa del año anterior y la necesidad de contar con un DPO (Data Protec-

tion Office). Recordaba el directivo de ESET que no hace mucho la agencia estatal de protección de datos revelaba que por el momento había tenido una comunicación de 1.300 DPO, una cifra a todas luces muy baja, lo que pone de manifiesto lo lejos que se está de cumplimiento con la normativa.

"La encriptación y la pseudoanonimización son otros elementos clave a tener en cuenta para el cumplimiento de GDPR"

Eusebio Nieva, Director Técnico de Check Point

"También es una diferencia sustancia el tema de la formación del empleado, porque todos somos conscientes de que los datos de la empresa deben estar protegidos pero esa concienciación no tiene formación", añade Carlos Tortosa. Un aspecto además muy importante si se tiene en cuenta que muchas brechas de seguridad se generar desde dentro de las propias empresas, "bien sea por mala fe o por descuido"

Asegura también Carlos Tortosa que ESET ha buscado ser práctico, no sólo proporcionando consejos para que la gente se informe, sino que las empresas hagan uso de herramientas que ha lanzado la agencia española de protección de datos, como la herramienta Facilita, y por último proponer una serie de medidas seguridad que ayuden a cumplir con la normativa, y que son medidas organizativas, medidas técnicas y medidas a nivel de datos.

La protección de la información se aborda desde ESET con ESET Deslock Encryption y ESET Secure Authentication, o lo que es lo mismo, con cifrado y con doble factor de autenticación, "dos herramientas explícitas para el nuevo reglamento de protección de datos", dice Tortosa. Explica el directivo que necesitamos tener controlada la información y tener controlado el acceso porque un 40% de empleaos consideran lícito llevarse información de una empresa de la que se van a la empresa nueva.

Además, cuenta ESET con Sagetica, una herramienta de gestión que complementa las dos mencionados antes para evitar brechas de seguridad, que permite aplicar políticas de BYOD, gestionar dispositivos extraíbles, etc.

Check Point

Para Check Point GDPR es parecida a otras normativas, pero difiere porque no se sabe a ciencia cierta cómo se aplican las medidas. "Hay que tener claro que con GDPR es un armazón de lo que hay que hacer. GDPR es, en esencia, privacidad para los usuarios" dice Eusebio Nieva, director Técnico de Check Point, quien añade que la normativa es también más dinámica en tanto en cuando se tienen que demostrar que, efectivamente, se han puesto las medidas adecuadas, que no vale con tener una solución de seguridad.

La norma dice que tienen que establecerse una protección por diseño, desde el principio, además de una aproximación basada en el riesgo, "y tercero, y eso sí es novedad, la notificación de brechas; si alguien no lo hace y se descubre la brecha va a tener un problema mucho más grave".

Una de las cosas que se tienen que tener muy en cuenta en relación a GDPR es la preparación

de los empleados, la creación de puestos específicos, así como la clasificación y la auditoría de los datos, sobre todo cuando son confidenciales o que afecten a los usuarios. Los logs van a ser también fundamentales, dice Nieva; por una parte, para la detección de una brecha de seguridad, y segundo para la demostración de que se tenían puestos los controles adecuados

Añade el director técnico de Check Point que en GDPR "tenemos también que tener en cuenta el cifrado y pseudoanonimización de los datos, es decir que los datos no se puedan ligar entre sí. La integridad de los sistemas de proceso tiene que están muy bien cuidado".

Preguntado el directivo por los puntos destacados de GDPR, las señales que nos pueden ayudar a cumplir con la normativa, habla de cosas tan básicas como la segmentación de la red, pero también de la clasificación de los datos, de la gestión de cambio de configuración y configuraciones seguras, así como de control de accesos, prevención de fugas de información o ataques DDoS, monitorización de la actividad del usuarios, gestión de vulnerabilidades o recuperación ante desastres. Y como guinda no sólo establecer todos estos controles, sino "verificar que se están aplicando, que se están viendo las cosas que pasan por la red y en los sistemas".

"Implementar cifrado es sencillo, pero gestionar la llave de cifrado de una manera segura es vital. Es la clave de bóveda de todo el edificio"

Ignacio Berrozpe,
Sales Engineer Thales e-Security

Thales e-Security

Ignacio Berrozpe, Sales Engineer Thales e-Security, dice que la adopción de GDPR hay que ponerla en el contexto de la Transformación digital y que lo que pide es que se protejan los datos de privados de los usuarios. "El reglamento pone un marco de multas, con límites máximos, de forma que no sólo hay que proteger los datos, sino que las empresas que no lo hagan tienen que ser multadas y los usuarios afectados tienen derecho a ser compensados si los datos han sido manipulados", explica el ejecutivo.

De cara a cumplir con GDPR Thales e-Secuity se centra en tres puntos distintos: cifrado de datos, gestión de identidades y control de accesos de los individuos a los datos y sistemas de gestión de cifrado.

Para Ignacio Berrozpe, "el cifrado es la mejor manera de empezar un plan de implementación de cumplimiento de GDPR". Y para poder cifrar los datos es clave saber dónde los tienes. Desde Thales e-Security intentan cubrir de una manera flexible el número máximo de casos de uso de protección, ya sea en bases de datos, en datos no estructurados con ficheros, ya sea en sistema de almacenamiento… por al "cuanto más completa la política y estrategia de protección de datos, mejor", dice Berrozpe.

Pero los datos no sólo han de ser cifrados y protegidos, sino que se debe proteger y gestionar el acceso a los mismos, quién puede acceder a ellos, algo que según Ignacio Berrozpe "tiene que ir de la mano del cifrado". Para Thales e-Security la clave está en Vormetric, una solución que permiten definir el control de acceso ligada a la protección de los datos.

Por último, la protección de las claves de cifrado. Explica Ignacio Berrozpe que el cifrado son algoritmos estándares, públicos y fácilmente implemen-

tables. Pero si bien implementar cifrado es sencillo, "gestionar la clave de una manera segura es más complicado", y el origen de Thales e-Security es precisamente los hardware security modules, lo que les hace ser "un referente en protección de llaves".

Y hace referencia también el ejecutivo a los servicios de auditoría de la compañía, que les da "una visibilidad muy grande de lo que se está haciendo en el mercado".

"A todas las empresas nos queda una oportunidad de mejora importante en lo que respecta a seguridad, y GDPR no hace sino incidir en esa oportunidad"

Juan Jesús Merino Torres, National Channel Country Manager de BitDefender

BitDefender

Juan Jesús Merino Torres, National Channel Country Manager de BitDefender, tiene claro que "nos queda una oportunidad de mejora importante en seguridad y que GDPR no hace sino incidir en esa mejora", y añade que trabajar en que los procedimientos de seguridad se conviertan en elementos competitivos que nos diferencien "es la forma correcta de verlo".

Explica el directivo de BitDefender que GDPR establece muchos puntos, pero que una de las novedades es la comunicación de una brecha de seguridad, y que para cumplir con eses punto "se hace indispensable el proceso de respuesta ante incidentes porque sin ello difícilmente podemos saber qué ocurrió, cómo ocurrió y cómo lo hemos solventado".

Hace Juan Jesús Merino referencia a la brecha de seguridad de Equifax para asegurar que generalmente los ciberdelincuentes utilizan ataques muy sofisticados, "y frente a esos ataques es importante contar con soluciones como EDR (endpoint detection and response) para poder actuar cuando se produce un ataque con éxito en la organización".

La cadena de cualquier ataque del mercado sugiere unas fases que son siempre las mismas, explica el directivo de BitDefender: primero se estudia el objetivo para detectar los débiles, y crean un malware a medida que va a explotar las deficiencias. En una tercera fase empiezan la instalación y luego la explotación. "Digamos que hasta aquí la mayoría de los ataques son detenidos por las soluciones de seguridad, pero basta con que uno pase a la fase de explotación para que entremos en un terreno en el que ya están dentro de nuestra organización, por eso la quinta fase de la cadena sería la instalación en más sistemas, en la sexta fase reciben las órdenes del servidor de C&C y finalmente llevan a cabo las acciones y objetivos que les están diciendo., ya sea extraer información, cifrarla, captar credenciales…".

GDPR, EL ÚLTIMO EMPUJÓN — CLICAR PARA VER EL VÍDEO

Dice Juan Jesús Merino que pasada la fase hay que empezar a buscar soluciones que correlacionen eventos, investiguen sobre ellos y se tomen medidas para parar al ataque. Y aprender de lo que ha ocurrido

Frente a las propuestas del mercado que proponen la utilización de un conjunto de soluciones que no sólo incrementan el coste sino que complican la gestión, la propuesta de BitDefender es GravityZone Ultra, una solución de endpoint de última generación y que integra en la misma solución un EDR, “con la ventaja de que no tiene ese coste de instalación tan alto”, dice el directivo de BitDefender, añadiendo que la solución trabaja en la fase de prevención, detección, correlación, investigación y respuesta ante incidentes.

WatchGuard

“Hay un camino muy, muy largo de recorrer para el cumplimiento de GDPR”, dice Carlos Vieira, director general de WatchGuard para España Y Portugal. Dice también que las empresas españolas estamos más avanzados gracias a la LOPD, pero que aun así “GDPR es una reglamentación que debe preocuparnos, tanto como el aumento del número de amenazas”.

Recuerda el directivo que las empresas tienen 72 horas para notificar que tienen una brecha, a pesar de que a veces se tardan meses en saber que se ha tenido”. Para Carlos Vieira el tráfico cifrado, que alcanzará el 75% en 2019 es otro problema que complica la detección de una brecha de seguridad, si no se tiene la solución adecuada; “y eso hace que las empresas tengan que actualizarse e imple-

"El número de incidentes de seguridad aumentan y se tardan meses desde que se sufre una brecha de seguridad hasta que se sabe"

Carlos Vieira, director general de WatchGuard Iberia

mentar dispositivos de seguridad capaces de analizar el tráfico cifrado", como las soluciones lanzadas recientemente por la compañía.

Experto en sus comienzos en seguridad perimetral WatchGuard ha ido evolucionando, añadiendo seguridad WiFi hace dos años y preparándose en un futuro cercano para adentrarse en el mercado de gestión de identidades, "un área importante para que las empresas cumplan con GDPR".

La propuesta del fabricante es Total Security, que integra un conjunto de servicios que seguridad que ayudan a las empresas a cumplir con la normativa europea de protección de datos.

Hace referencia Carlos Vieira a su servicio de TDR (Threat Prevention and Response), una solución de correlación de información endpint - perimetral que da visibilidad y responde de forma automática a las amenazas y que recientemente se ha integrado esta solución con Cloud Sandboxing.

Otra área importante de GDPR, y también de WartchGuard, es la visibilidad; "las empresas tienen que tener soluciones que aporten visibilidad de lo que está pasando en la red. Lo que hemos implementado es una nueva funcionalidad que es la anonimización de información, donde transformamos nombres en secuencias de caracteres que no permiten la identificación de la persona". Y tampoco hay que olvidar la importancia de un DLP (Data Lost Prevention) para controlar la salida o fuga de información de la empresa.

"Hoy la mejor solución de seguridad que las empresas pueden tener es un UTM", dice Carlos Vieira. "Con un UTM las empresas están seguras por un precio asumible en el que conviven múltiples capas de seguridad y múltiples servicios activos".

Sobre si los servicios gestionados serán fundamentales para la adopción de GDPR en empresas pequeñas, el director general de WatchGuard asegura estar totalmente de acuerdo. "Todos los estudios dicen que las empresas van a delegar la seguridad en partnes MSSP; 40% del negocio de las pymes en seguridad estará en manos de este tipo de partners", concluye el directivo.

Enlaces de interés...

- 'En GDPR el primero que no ha hecho su labor es el Gobierno' (Mario García, Check Point)
- GDPR vs Blockchain: tecnología vs la ley
- GDPR/RGPD, DPO o DPIA? ¿Qué son y para qué sirven?
- El 59% de las empresas le han dado a GDPR una alta prioridad
- Error de enfoque: las empresas no han aprovechado GDPR como oportunidad
- ¿Cómo se protege nuestra huella digital con GDPR?

Compartir en RRSS

S21SEC

Your Cybersecurity Company

+280 EXPERTOS

SERVICIOS DE SEGURIDAD GESTIONADOS SOC

100% ENFOCADOS A LA CIBERSEGURIDAD

24X7 COMBATIENDO EL CIBERCRIMEN

3 PAÍSES ESPAÑA | PORTUGAL | MÉXICO

WWW.S21SEC.COM

Ciberseguridad 4.0

Los ciberataques en general y los de phishing, DDoS o BEC en particular están evolucionando. Pero la industria no permanece impasible. Reacciona con técnicas revolucionarias, dotadas de inteligencia, basadas en aprendizaje que puedan hacer frente a esos ataques avanzados y dirigidos que ponen a prueba las soluciones de seguridad.

Hay que estar a la vanguardia y con una posición proactiva. Hacer uso del cifrado, del pentesting, ganar visibilidad de red para saber qué ocurre y jugar con todo ello como lo haría un equilibrista, orquestando y automatizando las soluciones para no desbordarnos.

¿Cómo hacer frente a los problemas de seguridad básicos y avanzados? ¿cuáles son las herramientas y soluciones de seguridad más vanguardistas? ¿qué técnicas pueden significar detener un ataque, o no? ¿qué plataformas pueden simplificar la gestión?

Todas estas cuestiones son las que se han planteado durante uno de nuestros #DesayunosITDS

Compartir en RRSS

¿Te avisamos del próximo IT Digital Security?

"El papel que la automatización y la orquestación tienen dentro de una estrategia de seguridad no es el que debería"

Bosco Espinosa de los Monteros, Preventa de Kaspersky Lab Iberia

que bajo el título Ciberseguridad 4.0 ha reunido un grupo de expertos de empresas líderes del sector, empezando por Sergio Martínez, director general de SonicWall Iberia; José de la Cruz, Director Técnico de Trend Micro; Bosco Espinosa de los Monteros, Preventa para Europa de Kaspersky Lab y Francisco Luis de Andrés, Analista de Seguridad Estratégica de S21Sec.

Iniciamos el debate hablando sobre la situación actual del mercado, un panorama que Sergio Martínez calificaba de "dantesca". Hacía referencia el directivo a Securitycenter.sonicwall.com, una plataforma de la compañía que ofrece datos en tiempo real sobre los ataques que se están produciendo, y la situación es: el 70% del tráfico ya está encriptado, lo que quiere decir que gran parte de las amenazas pasan por delante de nuestras narices y no se ven; el segundo dato es que el malware ha crecido un 151% en Q1 de 2018 respecto al mismo periodo del año anterior; el tercer dato es que de este malware, el ransomware ha crecido un 220% y que el 50% de las empresas que pagaron para liberar sus datos no los recuperaron. "Si a esto le añadimos que estamos desplegando millones de dispositivo os nuevos y que el tráfico ya es de Giga y eso lo complica todo un poco más, hace que el escenario realmente divertido y para empezar a pensar en un nuevo modelo de defensa".

José de la Cruz identificaba como "persistente" el escenario de amenazas actual. Dice el director técnico de Trend Micro que a la hora de adoptar estrategias de ciberseguridad las compañías tienen que implementar sobre todo automatismos para simplificar; "hay que implementar mecanismos que nos permitan estar protegidos de manera continua y desatendida".

Bosco Espinosa de los Monteros define la situación como "interesante o curiosa". Ascendido a una posición europea, el ejecutivo de Kaspersky Lab dice que las amenazas son persistentes, que continuamente están evolucionando, pero que al mismo tiempo "se siguen cometiendo los mismos errores, los mismos fallos de seguridad, la misma dejadez". El 90% de las amenazas no son avanzadas y con un buen planteamiento de seguridad muchísimas empresas podrían estar a salvo de ellas.

Francisco Luis de Andrés menciona algunos riesgos que están creciendo en el panorama de amenazas, como son los ataques fileless (sin fichero), que están atacando los sistemas en memoria o que

los indicadores de compromiso simples, como se han conocido hasta ahora, son insuficientes, y que se va complicando muchísimo el escenario necesitando de recursos muy avanzados para poder defenderte o detectar las amenazas una vez que se han producido. “Las estadísticas hablan de más de 470 días a nivel europeo para detectar un ataque persiste”, recuerda el analista de seguridad estratégica de S21Sec.

Medidas mínimas de seguridad

Estrategia de defensa en profundidad es una de las claves de la propuesta de SonicWall. Su director general para España y Portugal asocia este concepto con los estudios que en las academias militares de hace de la defensa en profundidad que los rusos construyeron ante los alemanes en el verano de 1943 en el mayor ataque concebido con tanques contra una infraestructura fija, que es la batalla de Kursk, la última gran ofensiva de la Alemania nazi contra Rusia. Explica Sergio Martinez que los rusos, precavidos de este gran ataque, construyeron una defensa de 200 kilómetros de trincheras con un montón de líneas y defensas móviles que pudieran parar la ofensiva, “y lo consiguieron por esa defensa en profundidad de diferentes tecnologías”. Trasladado esto al mundo IT, la defensa en profundidad es combinar diferentes tecnologías, como el firewall hasta el endpoint, poniendo diferentes tecnologías en medio, “todo combinado y dirigido con una inteligencia activa”.

Coincide José de la Cruz en ese planteamiento multicapa, haciendo referencia a motores tradicionales válidos para determinadas amenazas combinado con otra serie de motores y capas que permiten bloquear los ataques: motores de sandboxing, machine learning, análisis de comportamiento… Y dado que tenemos múltiples vectores de ataques, también es fundamental, en opinión del director técnico de Trend Micro, compartir esa inteligencia, es decir “la inteligencia que he adquirido ante un ataque, conocido o desconocido, apliquémosla en todos los vectores, en el correo electrónico, en la navegación, en el endpoit…”.

"Al final el cloud hay que asumirlo, incorporarlo dentro de la infraestructura y aplicar la seguridad en profundidad"

Sergio Martínez, director general de SonicWall España

"Yo unificaría las dos cosas que se han dicho. Por un lado, la defensa en profundidad, pero esa compartición de información de los vectores es fundamental, sobre todo cuando hablamos de más de 400 días de detección de una amenaza", dice Bosco Espinosa de los Monteros, añadiendo que hoy en día necesitamos saber qué es lo que está ocurriendo dentro de nuestra red, tener una capacidad de reacción en base a un saber lo que ha pasado, tener un histórico.

Francisco Luis de Andrés destaca el servicio Threat Hunting de S21Sec como fundamental para garantizar la seguridad una brecha cuando se ha producido o para hacer acciones de prevención. Se trata de un servicio "para el que se analiza de forma regular una serie de indicadores de compromiso y, combinando acciones de inteligencia y analizando los activos de forma periódica vamos dotando de inteligencia a todos los sistemas de detección de amenazas", explica.

Automatización y orquestación

Se entiende que la automatización orquestación juegan un papel cada vez más importante en la detección avanzada de amenazas. "Dotar de inteligencia y orquestación a toda la infraestructura es clave, desde el firewall al endpoint a todos los appliances", dice Sergio Martínez. En todo caso, entendiendo que la automatización está superada, ¿el paso a la orquestación está en proceso? "Estamos en ello, estamos construyendo diferentes plataformas y uno de los grandes problemas es porque el mundo es multifabricante, y eso te lleva a que necesites plataformas para orquestar que se entiendan con varios fabricantes", añade el directivo de SonicWall. Hay que intentar facilitar la vida a los que están construyendo esas plataformas y en ese sentido, dice Martínez, la apuesta de la compañía se llama SonicCore que está basado en tecnologías Linux y con muchas APIs "abrirnos al mundo para que cualquiera pueda construir plataformas".

Hay en este punto de orquestación un llamamiento para el MSSP, el proveedor de servicios gestionados de seguridad. "Nosotros creemos que el canal va a mutar y que de ser integradores o deployers, van a empezar a gestionar la seguridad de los clientes porque cada vez es más complejo y es imposible que dentro de las organizaciones haya gente preparada y al día para hacer frente a todas las amenazas…".

CIBERSEGURIDAD 4.0 **CLICAR PARA VER EL VÍDEO**

Para José de la Cruz automatización y orquestación son dos conceptos que van muy de la mano. "La automatización es fundamental porque las compañías no tienen recursos para hacer frente a esta heterogeneidad que tenemos hoy en día, y lo que quieren es implementar un sistema de seguridad que de manera autónoma trabaje para proteger los sistemas", explica el directivo. Sobre la orquestación dice José de la Cruz que está relacionado con los servicios que se despliegan en la nube y para lo que se quiere contar con un sistema de seguridad;en este caso los clientes "cuentan ya con un sistema de orquestación de sistemas en el que van creando recursos y con escalabilidad y quieren que eso esté relacionado también con la seguridad, y por tanto que nuestra seguridad se adapte también a las nuevas tecnologías del mercado".

El papel que la automatización y la orquestación tiene dentro de una estrategia de seguridad "no es el que debería", asegura Bosco Espinosa de los Monteros. Hay quejas en los clientes y el canal de que las empresas de seguridad van por detrás de los ciberdelincuentes "y en muchos casos tenemos tecnologías e implementaciones que pueden facilitarles la vida, pero no se implementan, o se implementan tarde y mal". De forma clara estaba planteando Bosco Espinosa de los Monteros que hay que tener la tecnología, pero además "saber utilizarla, saber implementarla y saber escuchar".

La visión del analista de seguridad estratégica de S21Sec sobre el tema de la automatización y la orquestación consiste "en incorporar una tecnología muy madura que existe en el mundo empresarial como es la notación de modelados de proceso de negocio (BPMN) dentro de lo que es el mundo de la ciberseguridad, permitiendo interactuar entre distintas herramientas y en base a una lógica de negocio se vaya haciendo una decisión automatizada por parte de la herramienta, de forma que igual que ahora estamos recibiendo múltiples fuentes a través de SIEM y otros elementos, podamos tomar decisiones de forma inteligente, y esa orquestación permita también desencadenar eventos en una herramienta de ticketing o por ejemplo interactuar con herramientas de recursos humanos si se viera necesario". En todo caso y en lo referente a la orquestación, dice Francisco Luis de Andrés que lo que ha mencionado aún no se ha visto, de forma que tendremos que esperar para que este tipo de

> El 70% del tráfico ya está cifrado, lo que quiere decir que gran parte de las amenazas pasan por delante de nuestras narices y no se ven

herramientas, llamadas a facilitar la cifrada y hacer que los sistemas sean más inteligentes terminen por implantarse. Todo tendría que “por la utilización de una nomenclatura estandarizada y por una serie de fuentes estandarizadas para poder interactuar entre los distintos silos, igual que ha pasado en el mundo empresarial con el BPMN.

Seguridad cloud

Parece que, igual que ocurre con la automatización, la seguridad en la nube debería estar superada, y

¿Te avisamos del próximo IT Digital Security?

> "Hay que implementar mecanismos que nos permitan estar protegidos de manera continua y desatendida"
>
> José de la Cruz,
> Director Técnico de Trend Micro

sin embargo no parece que sea así. Coincide Sergio Martínez en el planteamiento, y asegura que, aunque el 90% de las empresas están empezando a subir cosas la nube, y a externalizar cosas, y tenemos la nube está presente en el mapa de sistemas de todas las compañías, y al fin y al cabo es una pieza más en el puzle que tiene que integrarse en toda esta estrategia en seguridad porque a mí me da igual tener un firewall físico que virtual , o un appliance que protege el correo electrónico o un firewall de aplicación –que será uno de los grandes tema que vamos a ver evolucionar en los próximos meses… Es decir, que al final el cloud “hay que asumirlo, incorporarlo dentro de la infraestructura y aplicar la seguridad en profundidad”, dice Sergio Martínez.

Recuerda por su parte José de la Cruz que el perímetro se ha perdido y que ya existen un único ente en el que todas las aplicaciones y sistemas empresariales, “independientemente de que estén en la nube, on-premise… tenemos que trata de igual manera, aplicando la solución adecuada a cada caso”.

¿Nos vamos olvidando del on-premise? Dice Bosco Espinosa de los Monteros que hubo un momento en que todo el mundo se fue a la nube, pero que ha habido una reacción cuando se han planteado cuestiones como: ¿has preguntado a tu proveedor qué medidas de seguridad te está dando? Y a pesar de que se de por hecho, no es verdad. “Cuidado, porque si pones las mismas medidas de seguridad que están poniendo on-premise, o no las pones y luego las quieres poner, te va a salir mucho más caro. Y a veces no puedes poner lo que quieras”, dice el preventa europeo de Kaspersky Lab.

El tema de la nube se ha ido complicando poco a poco, confirma Francisco Luis de Andrés, añadiendo que determinados servicios críticos son inviables o bastantes complicados en la nube. Habla también el directivo, de los tres niveles: Clod, Fog y Edge. “El trabajo con el Fog va a generar nuevos niveles de exposición; todo el trabajo de crear un nivel intermedio para acceder a los niveles de computación

de cloud va a generar mayores niveles de exposición y ahora muchas empresas están trabajando en crear sus propias pasarelas para acceder a la nube evitando problemas de latencia, creando un nivel fog entre el nivel de dispositivos y el nivel de computación", explica al analista de S21Sec.

IoT

Silencio en la sala ante el planteamiento de si hay previsiones de poder securizar el IoT a corto plazo. "No. El IoT viene de haber hecho mal las cosas durante todos los años anteriores, millones de dispositivos comprometidos con contraseñas por detecto, con vulnerabilidades conocidas…", dice Sergio Martinez, añadiendo que IoT va a ser una herramienta que van a utilizar los hacker, y lo que hay que estar es estar preparado para ello.

"IoT es un problema de diseño", asegura José de la Cruz. Existen multitud de dispositivos que no se han diseñado pensando en la seguridad y que no se pueden proteger, y eso es un problema de raíz.

Propuestas de seguridad de última generación

Al finalizar el debate, pedimos a nuestros invitados que nos hablen sobre sus propuestas más avanzadas para hacer frente a las amenazas de seguridad.

SonicWall. Nos autodefinidos como la Zero Day Protection Company, la compañía que se enfrenta a amenazas desconocidas y para ello planteamos una defensa en profundidad que empieza en el firewall de nueva generación que es capaz de detectar anomalías en el tráfico que pasa dentro de él. Hay que mirar el tráfico encriptado y dotar de inteligencia a nuestra plataforma cloud además de mirar el perímetro, pero seguir profundizando y utilizar diferentes tecnologías como sandboxing. Recientemente se ha firmado un acuerdo con SentinelOne para desplegar tecnología en el endpoint todo sincronizado y orquestado desde la plataforma cloud. Son diferentes capas de seguridad incorporando también lo último en protección también de correo electrónico.

Trend Micro. El planteamiento de Trebd Micro se basa en proporcionar a nuestros clientes visibilidad y control. Visibilidad para poder reaccionar ante un incidente de seguridad y control a través de mecanismos tradicionales y otros de nueva generación como sandboxing, machine learning y demás para proporciona esa seguridad lo más robusta posible. Hay una tecnología que quería destacar que es muy interesante que es la parte de parcheado virtual. Nosotros tenemos un programa que es el Zero Day Initiative que está específicamente oriento a la detección y publicación de vulnerabilidades con el ánimo de proteger sistemas de nuestros clientes frente a vulnerabilidades Zero Day. Por lo tanto, proporcionando todas esas tecnologías ofrece la seguridad más robusta.

Kaspersky Lab. Nosotros por un lado hablamos de protección, pero también de visibilidad porque es fundamental saber lo que está ocurriendo. Nos ayuda por supuesto la parte de sandboxing que es fundamental, la parte de machine learning, pero consideramos que machine learning no es la bala de plata, creemos que está muy bien alimentar los servicios pero que haber un equipo por detrás que nos oriente y nos haga búsquedas de amenazas avanzadas. La protección tradicional tiene que seguir ahí, pero hay que ir un paso más allá, la parte de visión de todo lo que ocurre, poder hacer un análisis, hacer un sandboxing… No nos olvidemos también de comprobar certificados, que antes se daban por supuestos, pero ahora hay que aunar tecnologías y también servicios.

S21Sec. Nosotros tenemos servicios muy avanzados, muy sofisticados, pero de vital importancia es la concienciación por parte de las empresas de que tienen que hacer diagnósticos sobre la seguridad, que tienen que realizar análisis y planes de seguridad a largo plazo marcando una serie de requisitos que quieren conseguir y un nivel de riesgo que quieren asumir, y en base a eso implementar medidas o adoptar servicios o soluciones de seguridad gestionadas, como podríamos hacer nosotros.

"En relación a la automatización y la orquestación hay que incorporar una tecnología muy madura que existe en el mundo empresarial como es la notación de modelados de proceso de negocio (BPMN) dentro del mundo de la ciberseguridad"

Francisco Luis de Andrés, Analista de Seguridad Estratégica de S2lSec

Explica el director técnico de Trend Micro que su compañía colabora con empresas grandes para ayudarles a implementar la seguridad de factor desde el principio; y que cuentan con soluciones para proteger entornos industriales, para proteger el perímetro, el entorno donde estén trabajando ese tipo de sistemas controlando ese tipo de comunicaciones.

Se diferencia entre IoT y OT como diferencia entre el mundo de dispositivos como neveras, cámaras, smartwatch… y la industria. "La frase más conocida en OT es: 'Si funciona no lo toques', pero eso ya no vale", dice Bosco Espinosa de los Monteros, porque los equipos legacy, las comunicaciones hay que protegerlas de alguna manera. Hay que ir trabajando en la protección y se está haciendo, pero despacito, dice también el ejecutivo.

Además de la complicación del mantenimiento del legacy en los entornos industriales, añade Francisco Luis de Andrés, el asunto de protocolos de IoT, como el mqtt, "que es un protocolo que incorpora medidas de seguridad adicionales. Y respecto al tema de la industria está claro que se mantiene dispositivos que no se pueden actualidad sobre sistemas que no se pueden actualizar y luego protocolos antiguos que están pasando datos en texto plano y que no se pueden tocar. Y entonces hay que entrar en soluciones de virtual patching, una buena segmentación de red, pero complica mucho la gestión".

Enlaces de interés...

- Una vulnerabilidad en Z-Wave expone 100 millones de dispositivos IoT
- Los profesionales de seguridad de TI sufren cada vez más presión
- ¿Qué acecha en tu red?
- PCI DSS, la seguridad de los datos de los pagos digitales a tu alcance
- Cambios de paradigma

¿Te avisamos del próximo IT Digital Security?

SONICWALL®

Para más información, póngase en contacto con nosotros

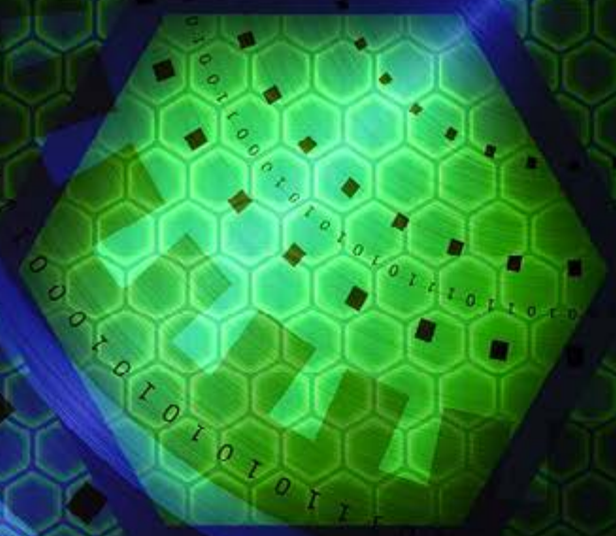
935 480 400 - spain@sonicwall.com - SonicWall.com

CAPTURE MORE.
FEAR-LESS.

¿No preferiría trabajar con el proveedor de seguridad que bloqueó el ataque de ransomware WannaCry con semanas de antelación? Con SonicWall, tema menos y concéntrese más en lo que hace mejor.

Por qué necesitas una web segura

HTTPS, o Hyper Text Transfer Protocol Secure, es la versión segura de HTTP, que es el protocolo por el que se envían los datos entre el navegador y la página web que se visita cuando se está conectado. La 'S' de Secure, significa que todas las comunicaciones entre el navegador y la web están cifradas.



Aunque con el tiempo se amplió a todo tipo de uso, inicialmente HTTPS estuvo dedicado a la protección de las transacciones online. Navegadores como Internet Explorer, Firefox o Chrome suelen mostrar un candado en la barra de direcciones para indicar que la página que se está visitando utiliza una conexión HTTPS segura.

Pero empecemos por el principio, por el concepto mismo de la World Wide Web, y un Tim Berners-Lee enumerando los retos que tenía que cumplir el nuevo protocolo: contar con la funcionalidad de transferencia de archivos; tener la capacidad de solicitar una búsqueda de índice en un archivo de hipertexto, negociación de formatos, la capacidad de derivar al cliente a otro servidor, y finalmente que implementara un pequeño subconjunto de funcionalidades.

Con la evolución de internet las soluciones para proteger las páginas web han evolucionado. Durante años empresas como Google han estado trabajando para animar a los propietarios de las páginas web a utilizar el protocolo HTTPS, que como hemos dicho es que el que asegura que los datos enviados entre el ordenador al site al que

navegas están cifrados y se transmiten de manera segura.

Las medidas se van a hacer más rigurosas porque el lanzamiento, el próximo mes de julio de Chrome 68, conllevará que Google marcará todos los sotes que no hayan adoptado HTTPS como no seguros. El resto seguirán marcados durante un tiempo con un candado, que significa que están asegurados por un certificado SSL.

¿Qué es un certificado SSL?

Acrónimo de Secure Sockets Layer, SSL es la tecnología que autentifica la identidad de un sitio web y además cifra la información que se envía al servidor. Es utilizada por millones de negocios online y usuarios para reducir el riesgo de que información sensible como números de tarjetas de crédito, contraseñas o nombres de usuarios pueden ser robados o interceptados por los ciberdelincuentes.

Let's Encrypt,
la revolución de los certificados digitales

El 12 de abril de 2016 se puso en marcha Let's Encrypt, una autoridad que proporciona certificados gratuitos para el cifrado de Seguridad de nivel de transporte (TLS) a través de un proceso automatizado que está diseñado para eliminar el complejo proceso creación manual, validación, firma, instalación y renovación de los certificados de sitios web seguros.

El proyecto tiene como objetivo hacer que las conexiones entre los servidores de todo Internet estén cifradas. Es decir, se trata de conseguir la que las conexiones cifradas lo sean por defecto. No sólo elimina el pago, la configuración del servidor web, la gestión de correo electrónico de validación y las tareas de renovación del certificado, sino que está destinado a reducir significativamente la complejidad de la configuración y el mantenimiento de cifrado TLS. Por ejemple, en un servidor web Linux, la ejecución de dos comandos es suficiente para configurar el cifrado HTTPS y adquirir e instalar certificados en el plazo de 20 a 30 segundos.

Los principios clave detrás de Let's Encrypt son:

- GRATIS: Cualquier persona que posea un nombre de dominio puede usar Let's Encrypt para obtener un certificado confiable a costo cero.
- AUTOMÁTICO: el software que se ejecuta en un servidor web puede interactuar con Let's Encrypt para obtener sin problemas un certificado, configurarlo de forma segura para su uso y automáticamente ocuparse de la renovación.
- SEGURO: Let's Encrypt servirá como una plataforma para avanzar en las mejores prácticas de seguridad de TLS, tanto desde el lado de la CA como ayudando a los operadores del sitio a proteger adecuadamente sus servidores.
- TRANSPARENTE: todos los certificados emitidos o revocados se registrarán públicamente y estarán disponibles para que cualquier persona pueda inspeccionarlos.
- ABIERTO: el protocolo de emisión y renovación automática se publicará como un estándar abierto que otros pueden adoptar.
- COOPERATIVO: al igual que los protocolos subyacentes de Internet, Let's Encrypt es un esfuerzo conjunto para beneficiar a la comunidad, más allá del control de cualquier organización.

Let´s Encrypt es un servicio ofrecido por el Internet Security Research Group (ISRG), una organización pública y benéfica. Entre sus mayores patrocinadores destacan The Mozilla Foundation, OVH, Akamai y Cisco Systems.

PROTOCOLOS PARA LA COMUNICACIÓN SEGURA: SSL/TLS

CLICAR PARA VER EL VÍDEO

SSL es la tecnología que autentifica la identidad de un sitio web y además cifra la información que se envía al servidor

En esencia lo que se produce es una conversación privada entre las dos partes.

Para la creación de una conexión segura se necesita que un certificado SSL, también conocido como certificado Digital, esté instalado en un servidor web y que realice dos funciones: por un lado, que autentifique la identidad de la página web, y por otro lado que cifre los datos que se están transmitiendo entre las partes.

Hace 20 años que los certificados digitales están en uso, pero a pesar de su importancia son muchos los que retrasaron su adopción debido a su precio y complejidad de adaptación. Hoy, sin embargo, contar con un certificado SSL es mucho más fácil, porque además de que existen iniciativas que los ofrecen gratis, su instalación es muy sencilla.

¿Por qué necesito tener un certificado SSL/TSL?

Hay toda una serie de razones por las que se debe contar con un certificado SSL. La primera y principal es que incrementa la seguridad del site al proteger la información sensible que se transmite, pero es que además se pueden proteger los subdominios con un único certificado SSL, algo que es extremadamente útil si se tienen que mantener sitios web complejos.

No hay que olvidarse de la credibilidad y confianza de los clientes, que ven con mejores ojos los sites que están acompañados por un candado o señal que indica que la conexión es segura y la web se toma en serie todo lo relacionado con la privacidad.

Y si la credibilidad es importante, hay que saber también que contar con un certificado SSL instalado mejora el tema de SEO, o posicionamiento en internet. De hecho, a través de la iniciativa HTTPS Everywhere, Google concede a los sites que utilicen en conexiones cifradas mejor puntuación.

Como se desprende de lo anterior, cualquier organización que utilice, reciba, procese recoja, almacena o muestre información sensible, que incluye contraseñas, información financiera o legal, datos personales, listas de clientes o incluso información médica está llamada a utilizar un certificado SSL/TSL.

La manera más habitual se acceder a un certificado SSL/TSL es preguntar al proveedor de hosting. Hasta hace poco lo normal era pagar por los certificados digitales, pero ahora hay cada vez más las compañías que los ofrecen de manera gratuita, como es el caso de Symantec o Let's Encrypt.

SSL vs TSL

Cuando se habla de HTTPS lleva asociado normalmente otras siglas, como son SSL/TSL. La primera es el acrónimo de Secure Sockets Layer, la segunda de Trasnport Layer Security, y ambas son hacen referencia a protocolos que permiten que los datos sean transferidos de manera privada y segura entre el servidor y el navegador. Aunque suele hablarse de ellos como sinónimos lo cierto es que uno es el predecesor del otro. TSL es el cifrado que se utiliza hoy en día, y que SSL está anticuado. En realidad,

Los certificados digitales de Symantec

En los últimos meses hemos visto un tira y afloja entre Google y Symantec por la confianza en los certificados digitales de la empresa de seguridad que, aunque muy conocida por sus soluciones de seguridad endpoint, también ha sido una de los mayores Autoridades de Certificación, (CA por sus siglas en inglés).

En marzo de 2017 ingenieros de Google y Mozilla detectaron que Symantec había emitido 127 certificados SSL de manera incorrecta, una cifra que posteriormente ascendió a 30.000. Siendo Internet el negocio base de Google, fue esta la compañía que primero mostró su descontento con los procedimientos de emisión de SSL de Symantec, anunciando pocos días después que tenía la intención de eliminar gradualmente el soporte para los certificados de Symantec de su navegador, Chrome.

La investigación se prolongó durante algunos meses y aunque Google fuera la voz cantante otras empresas como Mozilla, Microsoft o Apple también estuvieron muy pendientes del curso de los acontecimientos.

Por la parte de Symantec negaron cualquier irregularidad y calificaron los resultados de exagerados, a pesar de lo cual se sentaron en la mesa de negociación. Llegaron a algunos acuerdos, como el hecho de que Symantec se asociara con otra CA que emitiría certificados SSL con el nombre de Symantec, lo que convertiría a esta última, en términos técnicos, en una Autoridad de certificación subordinada (SubCA). Google propuso esta medida en la primavera de 2017, Symantec la reconoció en junio y la aprobó a mediados de julio. Se trataba de un paso crucial porque permitía a Symantec seguir siendo reconocida como Autoridad de certificación válida y emitir nuevos certificados SSL.

En todo caso, en agosto Symantec decidió acabar de golpe con las disputas con la venta de su negocio de certificados SSL/TSL a DigiCert por 950 millones de dólares y una participación del 30% en la compañía más pequeña, y dejando así que DigiCert implementara los planes para corregir los procedimientos de emisión de Symantec.

Comparado con Symantec, DigiCert es un jugador pequeño en el mercado de los certificados digitales, con una cuota del 2,2% frente al 14% de Symantec, según datos de W3Techs.

cuando alguien quiere decir SSL, en realidad está hablando de TLS.

Si nos adentramos en la parte técnicas, TLS tiene dos partes, por un lado, el TLS handshake layer, que gestiona qué algoritmo de cifrado se utilizará, la autenticación (usando un certificado específico para su nombre de dominio y organización) y el intercambio de claves (basado en el par de claves públicas y privadas del certificado). El proceso de handshake se realiza solo una vez para establecer una conexión de red segura para ambas partes.

> Let's Encrypt es una autoridad que proporciona certificados gratuitos para el cifrado de Seguridad de nivel de transporte (TLS)

La segunda parte es la TSL record layer, que es la que consigue los datos de las aplicaciones del usuario, las cifra, las fragmenta a un tamaño apropiado –determinado por el algoritmo de cifrado, y lo envía a la capa de transporte de red.

TSL establece un túnel de red cifrado y bidireccional para que los datos arbitrarios viajen entre dos hosts. TLS no sólo se utiliza con HTTP sino otros protocolos de internet como SSH (Secure Shell), que se utiliza para acceder a servidores privados a

través de Internet o FTPS, que sirve para la transferencia segura de ficheros a través de internet.

Durante su tiempo de vida se han lanzado varias versiones de SSL y TSL:

- **1995.** Netscape lanzó SSL v2
- **1996.** Llega SSL v.3, que solucionaba varios fallos de seguridad de la versión anterior. En todo caso, en 2004 SSL v.3 se consideró inseguro a consecuencia del ataque POODLE.
- **1999.** Se lanza TLS v.1.0 con un mecanismo que le hace ser compatible con SSL.
- **2006.** Llega la versión de TSL v1.1
- **2008.** TLS v1.2 es en estos momentos la versión más utilizada del protocolo

Actualmente se trabaja en TSL 1.3, una versión que quiere que el protocolo sea más rápido, más seguro y más fácil de implementar.

CONSIGUE TU PROPIO CERTIFICADO HTTPS GRATIS CON LET'S ENCRYPT

CLICAR PARA VER EL VÍDEO

Hay toda una serie de razones por las que se debe contar con un certificado SSL. La primera y principal es que incrementa la seguridad del site al proteger la información sensible que se transmite

Heartbleed, el caos

Y es que, hablando de las implementaciones, una incorrecta implementación es siempre un gran problema, y el tema que nos ocupa no es una excepción. Sólo hay que recordar a Heartbleed, un agujero de seguridad de software que ha pasado a la historia como uno de los fallos más terribles y graves de Internet. Descubierta en 2014 la vulnerabilidad (CVE-2014-0160) es un fallo de implementación en OpenSSL, una de las librerías de cifrado de código abierto, escrito en C, más populares. Dejar claro que el error está en la biblioteca OpenSSL, no en los protocolos SSL/TLS.

Cuando fue detectada, la vulnerabilidad existía en todas las versiones de OpenSSL desde marzo de 2012. Entre los productos que utilizaban OpenSSL destacaban Apache, IIS, Nginx, Cisco AnyConecct, la mayoría de los routers… en realidad era casi más fácil hacer una lista de productos web que no utilizan OpenSSL.

Heartbleed permite a los ciberdelincuentes un acceso sin precedentes a información sensible. Para entender el fallo hay que entender cómo operan los protocolos SSL/TLS y cómo almacenan los ordenadores la información en la memoria. Una parte importante de los protocolos es lo que se llama heartbeat, o latido del corazón, que es la que es la manera en la que dos ordenadores que se comunican entre sí se hacen saber que todavía están conectadas, incluso si el usuario no está descargando o cargando nada en el momento; una de las máquinas envía una parte cifrada de datos, llamada heartbeat request, a la otra, que responderá con la misma información cifrada, lo que demuestra que la conexión aún está en su lugar. Algo crucial es que esa solicitud incluye información sobre el tamaño del mensaje (p.e. 40KB).

La vulnerabilidad tiene que ver con la forma de comprobar esa longitud. Es decir, que si una solicitud decía que tenía 40KB pero en realidad solo tenía 20KB, la computadora receptora apartaría 40 KB de memoria intermedia, luego almacenaría los

20KB que en realidad recibió, y luego devolvería esos 20 KB más lo que sea que esté en los siguientes20 KB de memoria. Ese extra de 20 KB de datos es información que el atacante ahora ha extraído del servidor web.

En definitiva, la vulnerabilidad permite leer la memoria de los sistemas protegidos por versiones vulnerables de OpenSSL. Información sensible como identificadores de sesión, nombres de usuario, tokens, e incluso y en casos extremos las claves de cifrado privasas del servidor pueden ser extraídos de la memoria.

Uno de los mayores problemas de esta vulnerabilidad es que no deja evidencia aparente en los archivos de registro, lo que hace que sea extremadamente complicado saber si una máquina ha sido comprometida.

Investigaciones posteriores determinaron que un ataque permitía leer 64KB de memoria en un único mensaje de Heartbeat, peor que no existe un límite en la cantidad de memoria que puede leerse desde un servidor vulnerable. Y lo peor es que un atacante podría estar reconectando y solicitando un número arbitrario de segmentos de 64 kilobytes

EL SERVIDOR SEGURO HTTPS SSL

CLICAR PARA VER EL VÍDEO

Detectado en 2014 POODLE (CVE-2014-3566) es una grave vulnerabilidad que afecta al protocolo de comunicación SSL 3.0 que permite que los datos puedan ser interceptados y descifrados

para revelar secretos (contraseñas, claves secretas, números de tarjetas de crédito, etc.) almacenados en la memoria.

Aunque la vulnerabilidad se detectó en 2014, lo cierto es que se remota a la versión OpenSSL 1.0.1 lanzada el 14 de marzo de 2012, por lo que en su momento se calculó que había afectado a dos tercios de todo internet. El fallo se reparó en la versión OpenSSL 1.0.1f, pero hoy, años después de su descubrimiento, sigue explotándose. En enero de 2017 Heartbleed aún persistía en unos 200.000 servidores.

POODLE Attack

Ya hemos dicho que HeartBleed no es un fallo relacionado directamente con los protocolos de cifrado, pero el conocido como POODLE sí que afecta a uno de ellos. Curioso que también se detectara en 2014 y que afectara a los propios cimientos de los sistemas y protocolos de comunicaciones de la actual Internet.

POODLE (CVE-2014-3566) es una grave vulnerabilidad que afecta al protocolo de comunicación SSL 3.0. Descubierto por investigadores de Google, el fallo permite que los datos cifrados enviados entre los ordenadores y los servidores puedan ser interceptados y descifrados.

Como explicaba Josep Albors, responsable de investigación y concienciación de ESET España en WeLiveSecurity.com, el blog de la compañía, la vulnerabilidad en SSL 3.0 afecta a la parte cliente (navegadores de Internet, clientes de correo, etc.), lo que la hace menos grave y fácil de solucionar que Heartbleed.

Básicamente consiste en aprovecharse de una característica que hace que, cuando un intento de conexión segura falla, se proceda a intentar realizar de nuevo esa conexión, pero con un protocolo de comunicación más antiguo. De esa forma, un atacante podría ocasionar intencionadamente errores de conexión en protocolos seguros como TLS 1.2, 1.1 y 1.0 y forzar así el uso de SSL 3.0 para aprovechar la nueva vulnerabilidad.

"Podríamos decir que Poodle no está orientado a comprometer el sistema, sino a obtener la información que antes se enviaba cifrada y un atacante no podía descifrar", explica Josep Albors, para después añadir que se trata de un ataque en dos tiempos: Primero se fuerza el uso de un protocolo no seguro y luego se aprovecha una vulnerabilidad en él. No obstante, para poder realizar este ataque se han de cumplir una serie de condiciones, y es que el atacante ha de estar conectado a la misma red que la víctima y que JavaScript se esté ejecutando en el navegador, "algo bastante común pero que puede desactivarse fácilmente".

Josep Albors cerraba su post diciendo: "Esta vulnerabilidad en SSL 3.0 debería servir como una llamada de atención para dejar de utilizar un protocolo obsoleto que se desarrolló hace 15 años y que no está pensado para hacer frente a los desafíos de seguridad de hoy en día. Es por eso que, espe-

A partir de septiembre desaparecerá de Google Chrome el candado verde que identifica las páginas web seguras HTTPS y protegidas con cifrado SSL

ramos una rápida reacción por parte de los desarrolladores de aplicaciones que todavía hacen uso de SSL 3.0 y que implementen el uso exclusivo de TLS, algo que solucionaría este problema de forma efectiva y sencilla".

Let's Encrypt, cifrando Internet

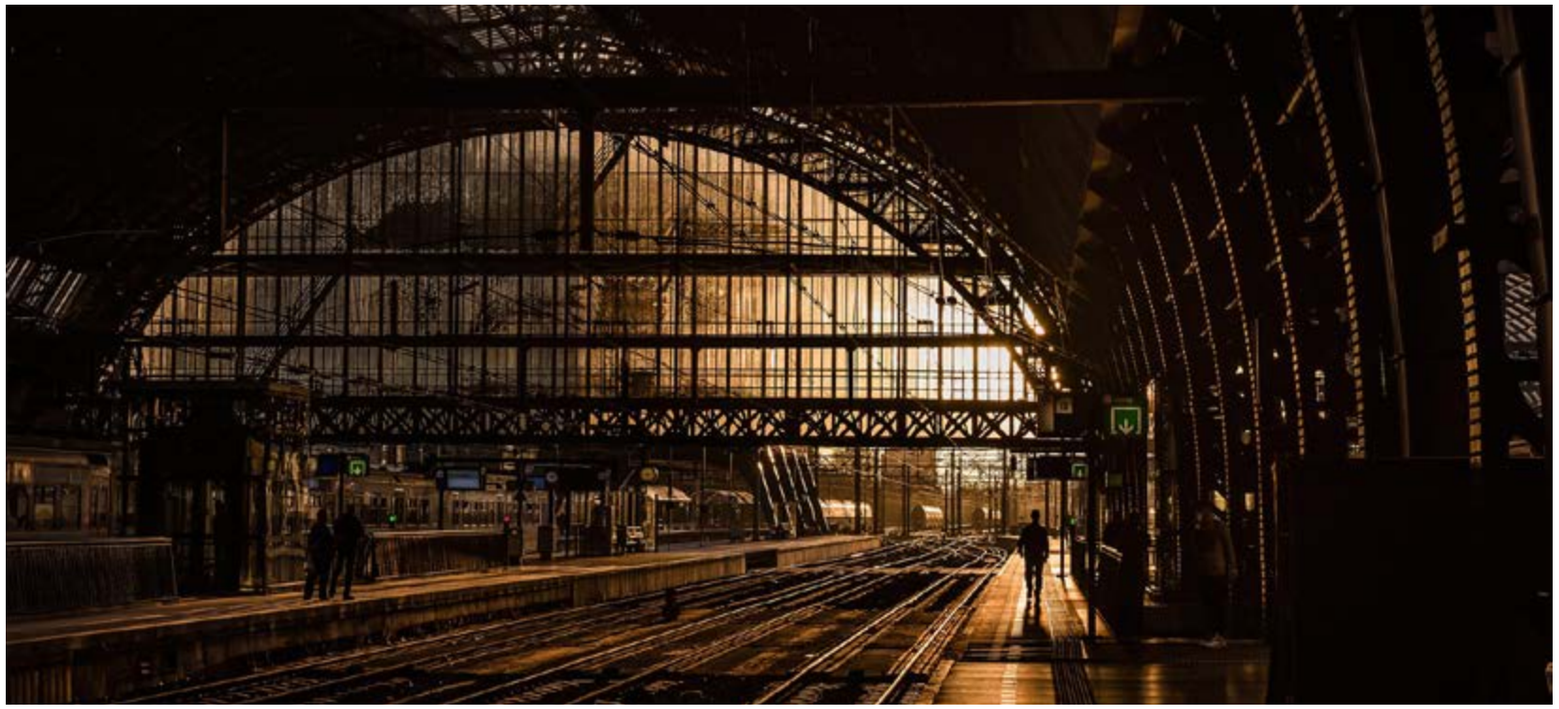
Dedicamos un recuadro para hablar de Let's Encrypt, lo que no contamos en ese espacio es que Let's Encrypt es uno de los efectos de las filtraciones de Edward Snowden. En realidad, la industria ya era consciente de la de necesidad de abandonar HTTP por HTTPS, pero este último protocolo, más seguro, requiere el uso de certificados digitales para la autenticación por los que hay que pagar.

Las revelaciones de Snowden dejaron al descubierto que las agencias de inteligencia habían subvertido el cifrado desde varias direcciones, no sólo colocando escuchas telefónicas dentro de las redes de compañías como Google, en lugares donde la protección HTTPS estaba ausente, sino que obligaban o convencían a las empresas para que entregasen los datos. De forma que las empresas se dieron cuenta de que HTTPS podría ser una buena forma de que su tráfico se mantuviera a salvo de espías, una protección contra la vigilancia incluso de actores tan fuertes como NSA.

De forma que Let's Encrypt obtuvieron mucha más tracción a raíz de las filtraciones de Snowden. En octubre de 2017 un informe de Google indicó que la mitad del tráfico de internet ya es cifrado, es decir que ya viaja a través de HTTPS. Con apenas una semana de diferencia desde Mozilla aseguraban que el volumen de tráfico cifrado ya había superado el volumen de tráfico sin cifrar.

Google y HTTPS

Durante los últimos años, la industria en general ha promovido la existencia de una web más segura al recomendar que los sitios adopten el cifrado HTTPS. Google ha sido una de las compañías que



más encarecidamente lo ha potenciado, ayudando a los usuarios a comprender que los sitios HTTP no son seguros al marcar gradualmente un subconjunto más grande de páginas HTTP como “no seguro”. A partir de julio de 2018 con el lanzamiento de Chrome 68, Chrome marcará todos los sitios HTTP como “no seguros”.

A partir de septiembre desaparecerá el candado verde que identifica las páginas web seguras HTTPS y protegidas con cifrado SSL, según ha dicho Google. ¿Quiere esto decir que ya no tendremos una forma de comprobar si estamos en riesgo y que estaremos más inseguras que nunca? No, simplemente cambia el planteamiento y esto ocurrirá con la versión 69.

Según el nuevo enfoque, los sitios que antes eran señalizados con el candado verde desaparecerán ya que se entiende que todos los sites son seguros por defecto. Sin embargo, si Chrome interpreta que una web a la que el usuario está accediendo no es segura y no cumple con los requisitos que exige, mostrará la advertencia en rojo de sitio no seguro cuando los usuarios vayan a introducir sus datos.

Por tanto, Google dejará de marcar con indicadores positivos las páginas seguras para empezar y empezará a identificar como no seguras a todas las páginas HTTP. Además, penalizará a nivel de SEO las páginas que no utilicen el protocolo HTTPS.

Esa advertencia al usuario puede ser un incentivo para que los propietarios adopten las medidas necesarias para mejorar la seguridad de sus sitios web y migren a certificados HTTPS. En todo caso, según datos de Google aportados a comienzos de este año más del 68% del tráfico de Chrome en Android y Windows ahora está protegido; más del 78% del tráfico de Chrome en Chrome OS y Mac ahora está protegido y 81 de los 100 mejores sitios en la web usan HTTPS por defecto.

Enlaces de interés...

- Google se lo pondrá difícil a las webs no seguras: ¿por qué hay que migrar a HTTPS ya?
- DigiCert cierra la compra del negocio SSL de Symantec
- Oracle apuesta por mejorar la seguridad de OpenSSL
- Chrome etiquetará las páginas HTTP como Inseguras
- Aprobado el protocolo TLS 1.3 para mejorar la seguridad de internet
- Las conexiones sin cifrar HTTP están llegando a su fin
- ¿Qué acecha en tu red?

Compartir en RRSS

Próximos #ITWebinars

Seguridad y Cloud, ¿qué nos queda por aprender?

28 JUNIO

Registro

Claves para escoger las mejores soluciones de gestión empresarial para una pyme

26 JUNIO

Registro

Resolviendo los retos de IoT

JULIO

Registro

www.ittelevision.es

it televisión

IGNACIO COBISA

ANALISTA SENIOR DE IDC

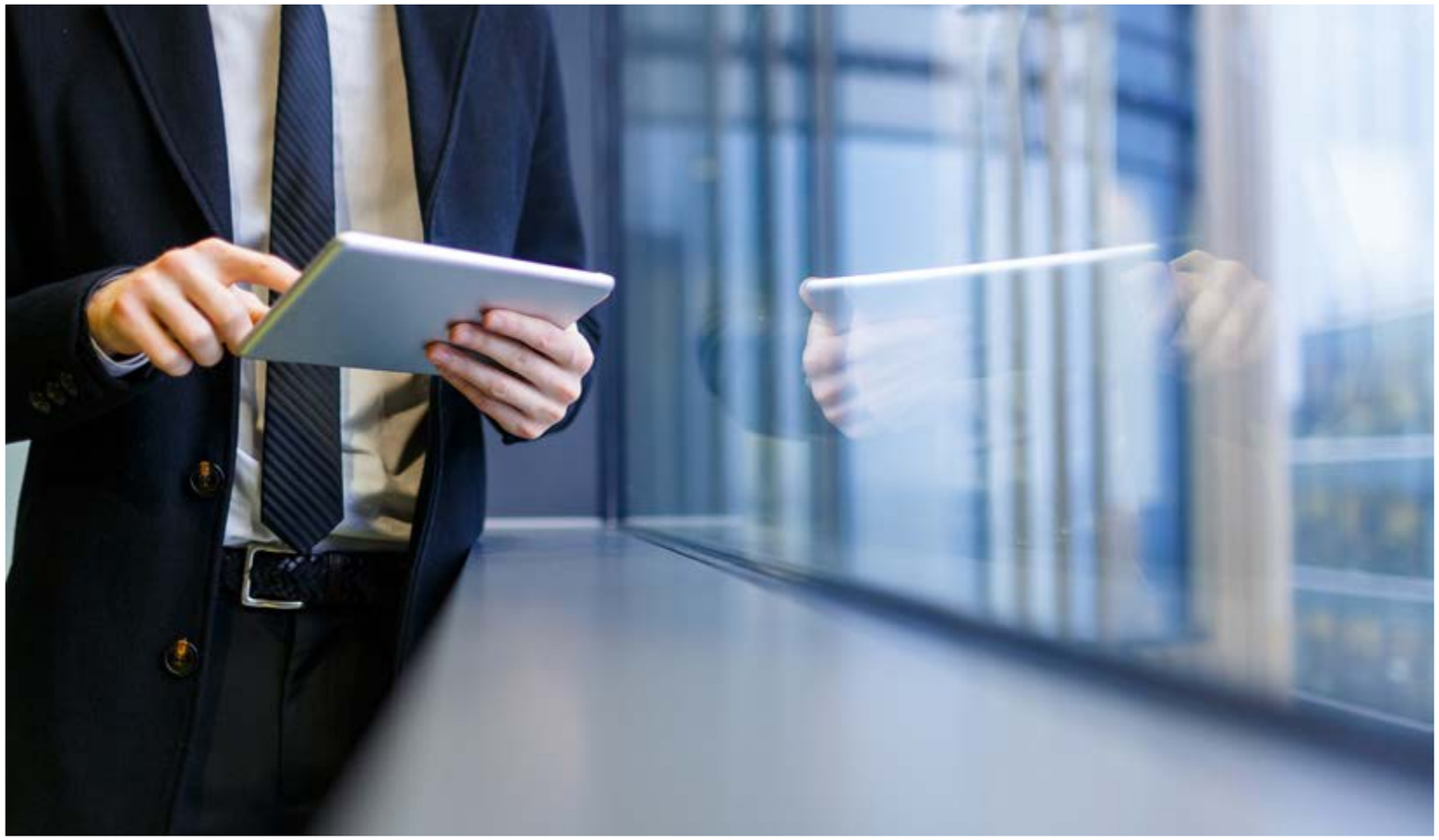
Ignacio Cobisa es analista sénior de investigación en IDC. Con más de 15 años de experiencia en el mercado de TI y telecomunicaciones, antes de unirse a IDC trabajó en diferentes puestos en el Grupo Telefónica, el último como consultor interno en la Oficina del Presidente de Telefónica. Anteriormente estuvo a cargo de Customer Relationship en Ya.com (ISP español de Deutsche Telekom Group). Ignacio es Licenciado en Economía en Complutense (Madrid) y Diplomado en Finanzas en la Universidad de Berkeley.

Infraestructuras TI definidas **por software**

Las Infraestructuras TI definidas por software tienen la capacidad de mejorar el control, el rendimiento y en definitiva conseguir la optimización de los activos del centro de procesamiento de datos.

Comenzando con las redes definidas por software o SDN por sus siglas inglesas, es importante recordar que SDN es un medio para un fin, no un fin en sí mismo. La red existe para satisfacer las necesidades de las aplicaciones y datos que operan sobre ella y, por extensión, los usuarios de esas aplicaciones y datos. SDN es esencialmente un modelo de arquitectura tecnológica que ayuda a alinear mejor la infraestructura de red con las necesidades de cargas de trabajo de aplicaciones, aprovisionamiento automatizado o integración directa con plataformas de orquestación en la nube. Esto se traduce en importantes ahorros operacionales al tiempo que permiten a las organizaciones liberar recursos para generar valor.

Dicho de otra manera, SDN puede ayudar a posicionar la red del centro de datos como un habilitador de negocios, facilitando los resultados relacionados con aplicaciones cada vez más críticas. También

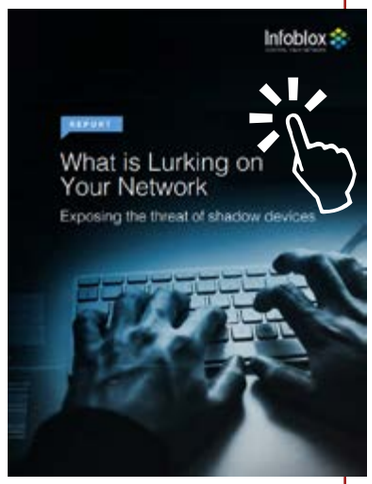


puede ayudar a los operadores de red a ser percibidos como transformadores digitales con un foco cada vez mayor en servicio y menor en producto.

Si bien la virtualización inicialmente expuso las limitaciones de las redes tradicionales, la computación en la nube ha hecho que esas limitaciones cada vez sean menores. En este contexto se puede ver a las redes definidas por software como un enfoque de arquitectura adecuado para las redes de centros de datos en la era cloud. Estudios de IDC confirman esta visión al indicar que la agilidad de la red para admitir aplicaciones virtualizadas, la

Si bien la virtualización inicialmente expuso las limitaciones de las redes tradicionales, la computación en la nube ha hecho que esas limitaciones cada vez sean menores

QUÉ ACECHA TU RED



Ha habido una gran explosión en la cantidad y tipos de dispositivos que se conectan a redes empresariales. Más de tres cuartas partes de todas las organizaciones tienen más de 1.000 dispositivos conectadas a la red de la empresa en un día normal. Incluso las empresas más pequeñas, con entre 10 y 49 empleados, tienen un número significativos de dispositivos conectados; de hecho, un 25% aseguran tener más de 1.000 cada día.

Ya sea por negligencia o por ignorancia, está claro que las organizaciones no pueden confiar en que los empleados sigan su política de seguridad para los dispositivos conectados. Los profesionales de redes y seguridad deben administrar activamente la amenaza introducida por el shadow IT.

La tendencia en el mundo TI hacia las infraestructuras definidas por software no está siendo ajena ni al mundo del almacenamiento ni al de las redes

necesidad de automatización de red para soportar la nube privada y la necesidad de respaldar las medidas de seguridad en el centro de datos, son las tres principales motivaciones para considerar o implementar tecnologías SDN.

Si nos centramos en el almacenamiento definido por software o SDS por sus siglas inglesas, podemos destacar que sus principales ventajas son:

- **Mayores cuotas de flexibilidad e interoperabilidad, lo que implica un menor lock-in, o dependencia de un fabricante**
- **Reducción de costes gracias a una mejor economía de almacenamiento**
- **Administración más fácil e intuitiva**

Los datos de IDC indican que el mercado global de almacenamiento definido por software, generará unos 13.000 millones de euros en ingresos en el año 2021 con un crecimiento anual compuesto del 13,5 % en el periodo 2017 - 2021. Muy por encima del mercado global de almacenamiento que tiene un crecimiento anual previsto para el mismo periodo en torno al 2%

SDS al igual que decíamos antes de SDN, se está viendo afectado por la tendencia de operar en la nube. De este modo, aunque SDS va a crecer tanto en modo cloud como TI tradicional, el almacenamiento definido por software en la nube va a ir ganado peso, pasando de significar el 27% del total del mercado en 2016 al 41% en 2021.

Los resultados de un estudio de IDC sobre los beneficios conseguidos tras implementar soluciones SDS nos dicen que la reducción de costes conjuntos de OPEX y CAPEX es el principal motivo expresado por las empresas para implementar soluciones de almacenamiento definidas por software. Por otra parte, la reducción de tiempos de provisión destaca por ser el aspecto que supone un mayor beneficio para las empresas en comparación con las expectativas antes de comenzar el proyecto.

Podemos concluir diciendo que la tendencia en el mundo TI hacia las infraestructuras definidas por software no está siendo ajena ni al mundo del almacenamiento ni al de las redes. De hecho, podemos afirmar que tanto el almacenamiento como las redes definidas por software se están posicionado como soluciones que van a ayudar a las organizaciones a superar los retos que se están planteando.

Enlaces de interés...

- Cambios de Paradigma
- Privacidad y protección de datos en aplicaciones móviles
- PCI-DSS la seguridad de los datos de los pagos digitales a tu alcance
- Análisis de riesgos en tiempo real, el papel de los escáneres de vulnerabilidades

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

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

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.

He sufrido un incidente de Seguridad, ¿y ahora qué hago?

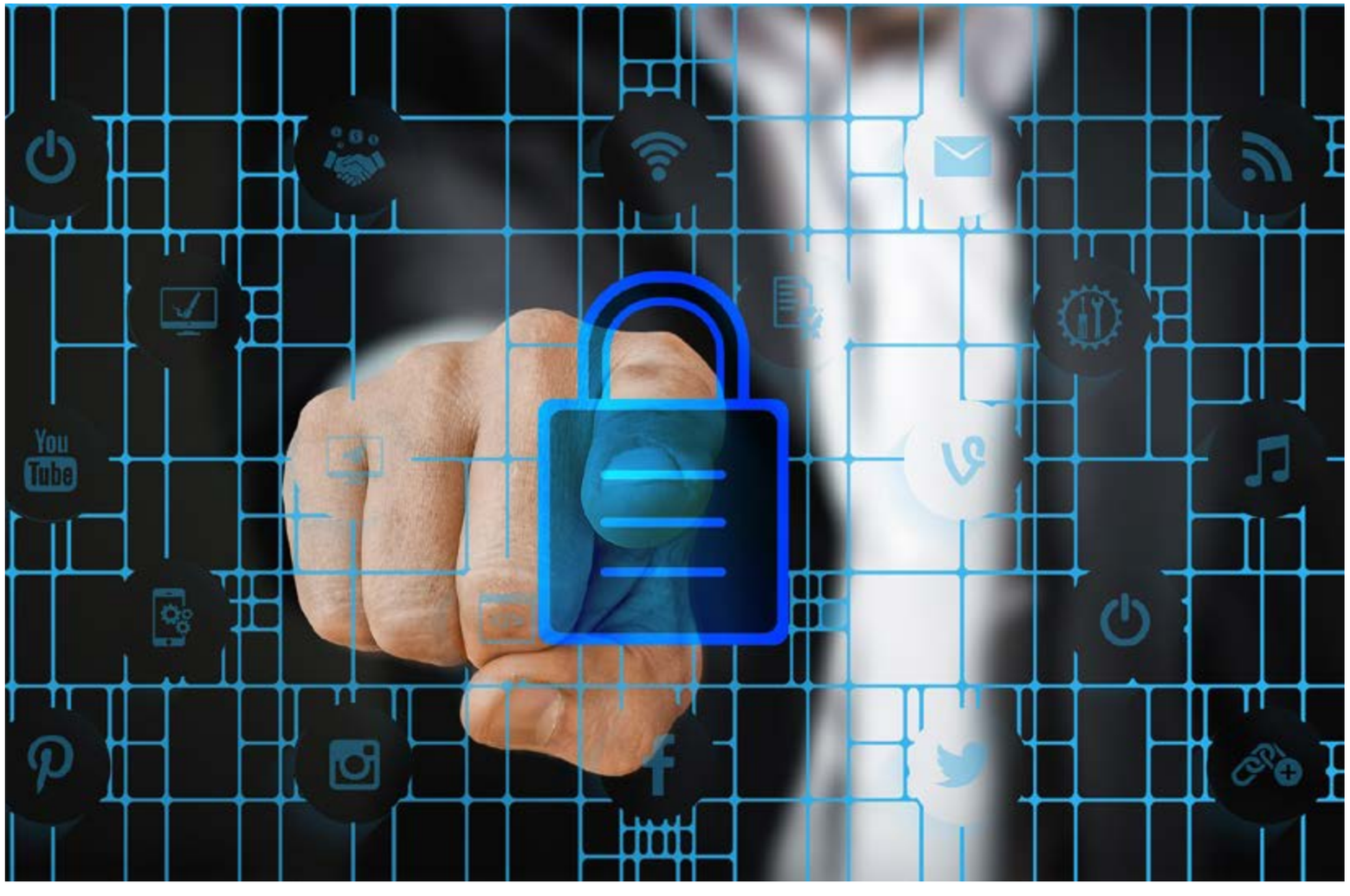
Los momentos inmediatamente posteriores a la detección de un incidente de seguridad son especialmente críticos. Una adecuada gestión en las primeras fases puede suponer una reducción del impacto en nuestra empresa.

¿Y ahora qué hago? Esta es la primera pregunta que nos planteamos y se plantean muchas empresas cuando hemos sufrido un incidente de seguridad.

A continuación, y en base a experiencias propia en este tipo de situaciones y en la de los clientes que han solicitado mis servicios, propongo unas “Guide Lines “para que sirvan de referencia, tanto para la gestión técnica del incidente como la gestión legal y operativa del mismo, con el objetivo de resolver y mitigar el daño sufrido tras el incidente, así como la posible fuga de información de nuestros sistemas.

Hay que definir, y esto es muy importante, el origen de las amenazas que provocan la fuga de información, ya que pueden ser tanto externas como internas

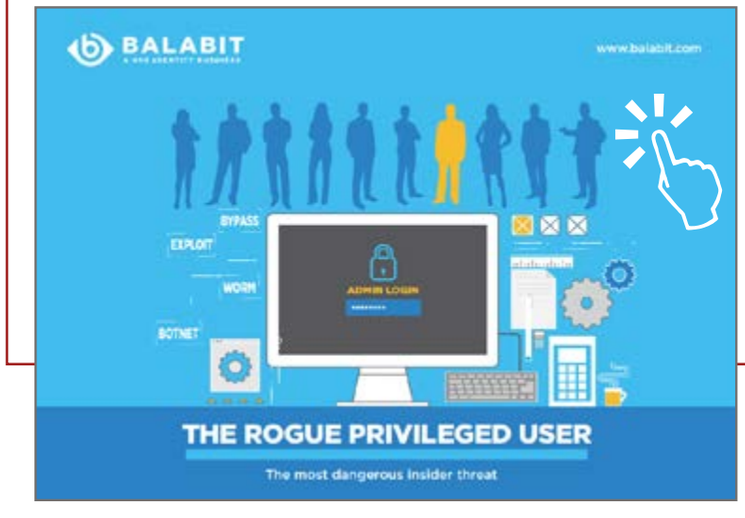
También hay que definir y, esto es muy importante, el origen de las amenazas que provocan la fuga de información, ya que pueden ser tanto externas como internas. Por origen interno se entienden las fugas de información ocasionadas por empleados propios de la empresa, ya sea de forma inadvertida (por desconocimiento o por error) o también a propósito. En el segundo caso los motivos "intencionados" que pueden estar detrás de este tipo de incidentes son muy variados y podrían ser porque el empleado esté



EL RIESGO DE LOS USUARIOS CON PRIVILEGIOS

En las brechas de seguridad, las cuentas privilegiadas juegan un papel importante. Si bien solo uno de cada diez empleados tiene acceso a estas cuentas administrativas, están involucrados en el 44% de las infracciones de datos. El 59% de las cuentas privilegiadas pertenecen a personas que no son empleados, como proveedores y contratistas externos. Un usuario deshonesto con acceso a cuentas privilegiadas puede robar información y datos confidenciales, sabotear sistemas críticos e invadir la privacidad de clientes y compañeros de trabajo.

Este documento no sólo ofrece información sobre los riesgos de las cuentas privilegiadas sino las motivaciones de los empleados que utilizan mal sus derechos de acceso así como la manera de protegerse contra amenazas internas.



descontento con la empresa, la venganza, la venta de secretos industriales o información privilegiada para la obtención de un beneficio económico particular, el daño a la imagen corporativa o la creación de una nueva empresa por parte del empleado con parte de los activos de información. Los principales orígenes externos de la fuga de información abarcan desde organizaciones criminales hasta activistas en internet. Sus principales motivaciones pueden ser desde la obtención de un beneficio económico con la venta de la información sustraída, la obtención de información específica (planos, proyectos, patentes), hasta dañar la imagen de la empresa o llevar a cabo acciones reivindicativas.

Así que lo primero que debe hacerse si hemos sido víctimas de un incidente de Seguridad es:

Los momentos inmediatamente posteriores a la detección de un incidente de seguridad son especialmente críticos

1º. Localizar el incidente.
2º. Reunión del gabinete de crisis.
3º. Informe inicial de situación.
4º. Aislar y poner en cuarentena los sistemas informáticos infectados de la infraestructura tecnológica de la empresa.
5º. Desconexión en el peor de los casos, de los elementos de acceso a internet de la empresa para que ningún equipo tenga acceso a internet y pueda volver a infectarnos de nuevo.
6º. Comunicar a los cuerpos de seguridad del estado en el plazo de 24 horas, que se ha sufrido un incidente de ciberseguridad, para ello actualmente el INCIBE (Instituto Nacional de Ciberseguridad), cuenta con un equipo de especialistas que además de recibir los incidentes reportados a través de los buzones de correo electrónico destinados para ello, emplea técnicas de anticipación y detección temprana de incidentes, esto permite por una parte elaborar alertas y avi-

Uno de los mayores retos a los que se enfrentan las empresas es conseguir la detección temprana del incidente

sos sobre campañas para mejorar la protección frente a ciberamenazas. Por otra parte, en el caso de la detección temprana de incidentes, se procede a la notificación del afectado y mantiene contacto con los proveedores de servicios de internet y otros centros de datos si fuera necesario.

5º. Notificar a la AEPD (Agencia española de protección de datos) el incidente ocurrido ya que, el 25 de mayo de 2018, entró en vigor la GDPR (Reglamento europeo de protección de datos), que obliga a todas las empresas y profesionales que hayan sufrido un incidente de seguridad y vean comprometidos sus datos, comunicar a este organismo en el plazo de 48 horas dichos incidentes y fugas de información.

Los momentos inmediatamente posteriores a la detección de un incidente de seguridad son especialmente críticos. Una adecuada gestión en las primeras fases puede suponer una reducción del impacto en nuestra empresa. Excepto en el caso de pérdida de dispositivos móviles, (Tablets, Smartphones) el principal problema en la mayoría de las ocasiones es que no es detectado hasta que su filtración se hace pública bien a través de los medios de comunicación o Internet, bien a través de algún tipo de notificación por parte del ciberdelincuente responsable del hecho. Por este motivo, uno de los mayores retos a los que se enfrentan las empresas es conseguir la detección temprana del incidente, si es posible, a través de medios internos, además realizar una constante labor de monitorización de cualquier publicación sobre nuestra entidad, se recomienda para ello, el uso de dispositivos SIEM, para tomar el control de la situación lo antes posible.

La prevención de incidentes de seguridad se basa en implantar políticas de uso y medidas técnicas eficaces en nuestra empresa, sin estas medidas quedaremos expuestos a los ataques de estos ciberdelincuentes.

Enlaces de interés...

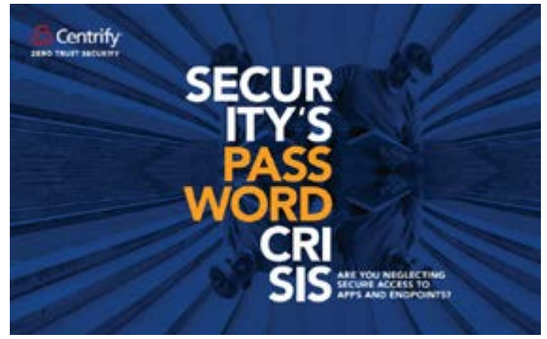
- Todo lo que necesitas saber sobre GDPR
- Crecen las brechas provocadas por amenazas internas
- Las organizaciones son más rápidas en identificar brechas
- Los principios de la protección de datos
- Por qué necesitas un sistema de identificación de emergencias

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

SONNIA MILENA CABIELES GARCÍA

ABOGADA/MASTER EN RESPONSABILIDAD CIVIL EXTRACONTRACTUAL

Sonnia Milena Cabieles García tiene una amplia experiencia sustancial y procesal en Derecho de Seguros, Mercantil, Laboral y Civil, en el sector público y privado. Con gran facilidad de adaptación a los cambios normativos, ha sido responsable del departamento Legal de Rodasoft. También ha trabajado en QBE Insurance como analista jurídica sobre la viabilidad o no del pago de los siniestros, proyección de respuestas a acciones de tutela, derechos de petición, objeciones de todos los ramos (Vida, R.C. Hogar, Property, Soat, etc) de la Compañía.

La ciberseguridad y su asegurabilidad

En los últimos meses, las siglas RGPD (Nuevo Reglamento General de Protección de Datos) se han vuelto el tema de "moda" en los sectores tecnológico, jurídico y económico en España. Y no es para menos, si tenemos en cuenta que se trata de una directiva de la U.E. que tiene relación directa con la protección de algunos de los derechos y principios fundamentales más relevantes que contempla el Art. 18 de la Constitución Española como lo son: el Derecho al honor, a la intimidad personal y familiar, y la propia imagen.

De ahí, el interés de la Unión Europea en que todos sus piases miembros adopten y adapten sus normativas internas a los nuevos reglamentos creados para la protección de datos de carácter personal con el fin de brindar cada vez más y mejores herramientas de tipo de legal, que vayan de la mano con las nuevas tecnologías y los diferentes sistemas de comunicación y almacenamiento de Datos personales

Según la AEPD, el tratamiento de datos de carácter personal debe sujetarse a una serie de princi-

Se requiere un conocimiento sobre la responsabilidad civil derivada de la puesta en marcha del nuevo RGDP, el aseguramiento de su ciberseguridad y sus posibles riesgos

pios fundamentales como: la calidad de los datos, el Derecho de información, el consentimiento, la seguridad de los datos, deber de secreto, el Derecho de acceso, el Derecho de rectificación, el Derecho de cancelación, el Derecho de oposición, el Derecho de consulta, el Derecho a revocar el consentimiento y el Derecho de indemnización. Esto con el fin, no solo de dar cumplimiento a la normativa, sino, de estimular y fomentar entre la sociedad el buen uso de los datos de carácter personal, el manejo seguro y confiable de la información y la concientización sobre su vital importancia.

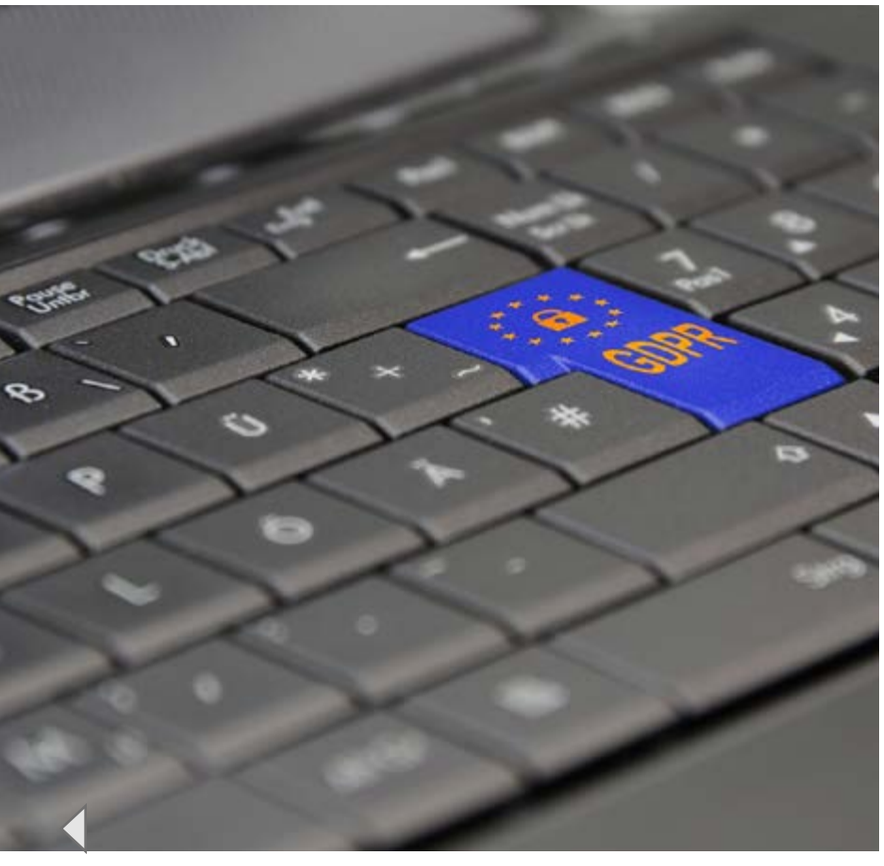
El nuevo RGDP fue aprobado en abril de 2016 por la U. E., y entró en vigencia en España el pasado 25 de mayo de 2016. La mayoría de empresas Españolas públicas y privadas involucradas en el manejo, uso y libre circulación de datos personales, sin importar su objeto social, se han interesado por conocer y saber sobre las medidas tecnológicas y legales que deben adoptar para evitar las elevadísimas multas y sanciones económicas que trae el reglamento, pero pocas se han preguntado e interesado por la Responsabilidad Civil que se deriva de dicho incumplimiento.

Al respecto, es preciso señalar que según el Régimen General de la Responsabilidad Civil Español contenido en su Código Civil - Capítulo II “de las obligaciones que nacen de culpa o negligencia, articulo 1.902” se establece que: “…El que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado…”.

En lo que a la Responsabilidad Civil se refiere, el nuevo RGDP introduce varios cambios significativos a la legislación española respecto de la LOPD, entre los más relevantes me permito señalar los siguientes;

- El nuevo RGPD, introduce a la normativa vigente dos nuevos derechos: Derecho al olvido (Art. 17 RGPD) y el derecho de la portabilidad de los datos (Art. 20 RGPD). Según la U.E. Estos dos nuevos derechos tienen por finalidad aumentar la facultad de decisión y control de los ciudada-

El nuevo RGPD establece un gran y significativo cambio en lo referente al régimen de la Responsabilidad Civil al introducir en su artículo 79 como parte o sujeto responsable a los "encargados del tratamiento de datos"



nos sobre sus datos personales que facilitan a terceros.

- El nuevo RGPD establece un gran y significativo cambio en lo referente al régimen de la Responsabilidad Civil al introducir en su artículo 79 como parte o sujeto responsable a los "encargados del tratamiento de datos". Esta situación no se encontraba contemplada en la LOPD. De ahí se destaca la importancia que, a partir del 25 de mayo de 2018, tiene el encargado del tratamiento de datos en cada empresa.
- En lo referente al Daño, el nuevo reglamento RGPD en su artículo 82, por primera vez reconoce de forma expresa el derecho a la indemnización de los daños y perjuicios de tipo inmaterial (daño moral); situación que tampoco se contemplaba en la LOPD.
- La necesidad del consentimiento claro y afirmativo, es decir, expreso de la persona concernida al tratamiento de sus datos personales.
- El derecho a presentar una reclamación ante las autoridades de control, con la regulación de su procedimiento a seguir.

A su vez, la AEPD, resalta dos elementos de carácter general que trae el nuevo reglamento y que constituyen la mayor innovación del RGPD para los responsables y se proyectan sobre todas las obligaciones de las organizaciones, y son:

- **Principio de Responsabilidad Proactiva:** Según la AEPD, el nuevo RGPD, describe este principio como la necesidad de que "… el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas, a fin de garantizar y poder

LOS PRINCIPIOS DE LA PROTECCIÓN DE DATOS

GDPR es la revisión más importante sorbe la privacidad de datos en 20 años. En este documento podrá saber cómo preparar los datos de su organización para el cumplimiento de la normativa. Para ello, DXC estableció un equipo de respuesta a GDPR en 2014 para desarrollar una estrategia de cumplimiento para uso interno y una propuesta de servicio para los clientes, estableciéndose un enfoque basado en tres perspectivas diferentes: Como controlador de datos, como procesador de daos y como consumidor de servicios de datos.

El nuevo RGPD, introduce a la normativa vigente dos nuevos derechos: Derecho al olvido (Art. 17 RGPD) y el derecho de la portabilidad de los datos (Art. 20 RGPD)

demostrar que el tratamiento es conforme con el Reglamento…". En síntesis, este principio exige una actitud consciente, diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que lleven a cabo.

- **El Enfoque de Riesgo:** Según la AEPD, el nuevo RGPD señala que las medidas dirigidas a garantizar su cumplimiento, deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas.

Una vez resaltados algunos de los elementos estructurales del régimen de la Responsabilidad Civil contenidos e introducidos en la normativa Española con el nuevo RGDP (acción, omisión, responsabilidad, daño etc.), así como los algunos de los elementos estructurales del contrato de seguro (Art 73,1 LCS) contenidos en el reglamento (reclamación, víctima, responsable, sanción etc.) se hace necesario resaltar qué; la entrada en vigencia en España de esta nueva normativa ha generado una nueva e importante línea y/o oportunidad de negocio al sector asegurador español y de toda la E.U.

En síntesis, la tecnología nos ofrece beneficios incalculables, pero, a su vez, nos conlleva a la inevitable exposición a los diferentes riesgos propios de su uso, manejo e implementación; de los cuales se pueden derivar múltiples acciones u omisiones "dañosas" contra nosotros mismos ó contra terceros. Y es en este escenario donde entra a jugar un papel muy importante el sector asegurador con la puesta en marcha de diferentes tipos de productos y/o pólizas de seguro que garanticen el pago de las posibles indemnizaciones derivadas de este tipo de riesgos.

Hoy día, compañías aseguradoras de gran impacto y reconocimiento en el mercado asegurador español ofrecen en sus portafolios de servicios varios tipos de seguros destinados a cubrir la Responsabilidad Civil por los daños a terceros y los daños propios derivados de este tipo de riesgos cibernéticos.

Entre las coberturas más habituales en el mercado asegurador están:

Responsabilidad Civil:

- **Responsabilidad por vulneración de privacidad.**
- **Responsabilidad en materia de seguridad de la red.**

Enlaces de interés...

- Todo lo que necesitas saber sobre GDPR
- 'En GDPR el primero que no ha hecho su labor es el gobierno' (Mario García, Check Point)
- GDPR vs Blockchain: tecnología vs la ley
- Checklist: controla si cumples con el principio de responsabilidad proactiva de GDPR
- ¿Cómo se protege nuestra huella digital con GDPR?

- **Responsabilidad por actividades en medios.**
- **Extorsión cibernética** pérdida de activos de datos pérdida de beneficios.
- **Responsabilidad por publicación de datos** en multimedia y publicidad.
- **Gastos de defensa, fianzas y conflictos de intereses.** Cubierto por la póliza.

Daños Propios:

- **Daños a los sistemas informáticos:** Derivados de un acto informático doloso, malware, robo de datos o denegación de servicio.
- **Interrupción del negocio:** Cubre la pérdida de beneficios como consecuencia de un fallo en los sistemas informáticos, derivado de un ciberataque.
- **Amenaza de extorsión cibernética:** Gastos realizados para proteger los sistemas informáticos y aminorar las consecuencias de una amenaza de extorsión cibernética.
- **Protección de datos:** Multas y sanciones por vulneración de la normativa de protección de datos.
- **Gastos derivados de notificación por violación de la privacidad.**

Gastos de restitución de imagen por sanciones de la Agencia de Protección de Datos.

Quiero terminar este artículo, con una invitación extensa a todos los sectores (públicos y privados) involucrados en el manejo, uso y libre circulación de datos de carácter personal a orientarse y enfocarse más hacia el conocimiento de la responsabilidad civil derivada de la puesta en marcha del nuevo RGDP, el aseguramiento de su ciberseguridad y sus posibles riesgos. it

¿Te avisamos del próximo IT Digital Security?