it Digital Security

La publicación electrónica sobre Seguridad Digital que necesitas

Octubre 2017 - nº 1

¿Por qué IoT no es seguro?

Hacia la autenticación biométrica

Las brechas de seguridad más sonadas de la historia

Data Protection Officer, el nuevo superhéroe

El actual contexto europeo de ciberseguridad

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

ITDS, una apuesta segura

¿Será ITDS una apuesta segura? Pues no lo sé, vosotros como lectores y el mercado lo dirá. Nosotros hemos puesto de nuestra parte todo lo posible, la experiencia de IT Digital Media Group con propuesta como IT User o IT Reseller sirven de referencia, y la confianza en una profesional como Rosalía Arroyo porque no creo que haya muchos periodistas en España que sepan de Seguridad más que ella, así que por nuestra parte la apuesta es segura. Veremos qué os parece a vosotros. Todos los detalles en este enlace.

Y yendo al grano. Nos ponemos en marcha hablando de IoT. ¿Es segura? Pues como decía el otro, ojo al dato. Demasiados dispositivos y conectados demasiado rápido. Los dispositivos que conforman ese Internet of Things del que llevamos hablando desde hace un tiempo, suman miles de millones e invaden el mercado cada día y de una manera acelerada. Llegar el primero tiene un coste, y ése es el que estamos a punto de pagar todos, sobre todo cuando si para llegar el primero se han obviado las medidas de seguridad más básicas.

Son, además, muy diferentes entre sí, y controlar miles de millones de dispositivos a los que a veces ni siquiera se puede cambiar la contraseña por defecto, es un reto. También es un reto proteger el IoT con un modelo de seguridad que apenas ha empezado a contemplar la movilidad y el BYOD. ¿Una referencia? Nada como echarle un ojo al nacimiento de Mirai hace unos meses, una botnet utilizada para lanzar ataques de denegación de servicios distribuido (DDoS), como el que dejó sin conexión a medio internet tras el ataque a Dyn. El hecho de que empiecen a diferenciarse entre botnets y thingbots no hace sino demostrar el interés que los ciberdelincuentes tienen en la capacidad que ofrecen de miles de millones de dispositivos conectados.

Pero no todo está perdido. Echa un ojo a nuestro tema de portada y mantengamos la esperanza.

IT Digital Media Group

Juan Ramón Melara
juanramon.melara@itdm-group.es

Miguel Ángel Gómez
miguelangel.gomez@itdm-group.es

Arancha Asenjo
arancha.asenjo@itdmgroup.es

Bárbara Madariaga
barbara.madariaga@itdm-group.es

IT Digital Security
Rosalía Arroyo
rosalia.arroyo@itdmgroup.es

Colaboradores
Hilda Gómez, Arantxa Herranz, Reyes Alonso
Diseño revistas digitales
Contracorriente
Diseño proyectos especiales
Eva Herrero
Producción audiovisual
Antonio Herrero, Ismael González
Fotografía
Ania Lewandowska

IT User TECH & BUSINESS
IT Reseller TECH&CONSULTING
IT Digital Security
IT televisión

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

En Portada

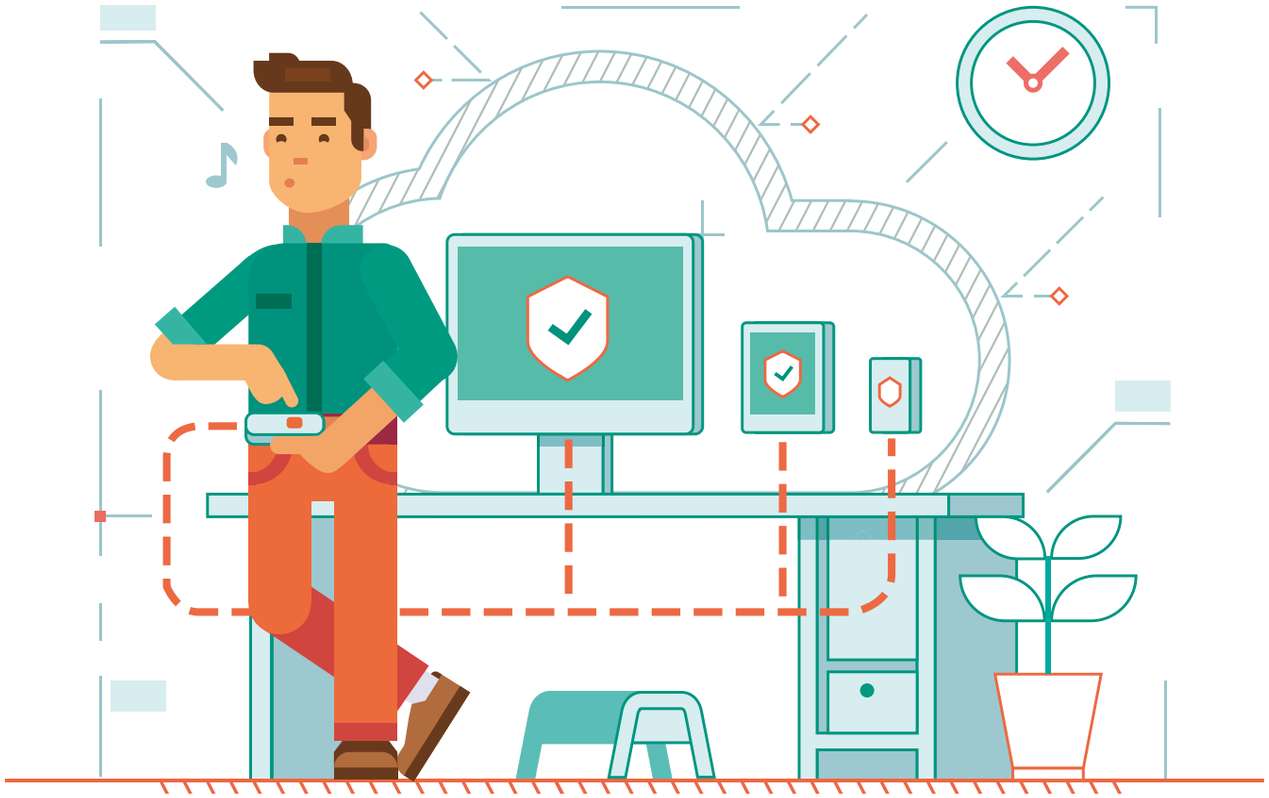
Por qué IoT no es seguro

Actualidad

No solo IT

Índice de anunciantes

¿Te avisamos del próximo IT Digital Security?



Deje que fluya su creatividad. Y aleje las ciberamenazas

Kaspersky Endpoint Security Cloud.
La seguridad que necesita con la flexibilidad que desea

El 40 % de las empresas afirma que el aumento de la complejidad de su infraestructura está llevando sus presupuestos al límite. Kaspersky Endpoint Security Cloud ayuda a las pequeñas y medianas empresas a simplificar la gestión de la seguridad, sin tener que invertir en recursos o hardware adicional. Gestione la seguridad de endpoints, dispositivos móviles y servidores de archivos Mac y Windows de forma remota, desde cualquier lugar, con nuestra consola basada en la nube.

cloud.kaspersky.com

Data Protection Officer, el nuevo superhéroe

Entre las novedades que propone la GDPR, de obligado cumplimiento a partir del próximo 25 de mayo de 2018, está la figura de un Data Protection Officer (DPO), la figura responsable de la privacidad que, con una función preventiva y proactiva, se encarga de supervisar, coordinar y trasmitir la política de protección de datos tanto dentro como fuera de la empresa. Además, se le considera como el punto de encuentro entre el responsable del fichero y/o tratamiento, el afectado y la autoridad de control, que en España será la AEPD (Agencia Española de Protección de Datos).

El 25 de mayo de 2018 el Reglamento General de Protección de Datos (GDPR), la normativa sobre protección de datos firmada hace año y medio, será de obligado cumplimiento. Pocas dudas hay sobre el impacto que tendrá en las empresas, en todas las que, independientemente de su tamaño, gestionen datos personales, de empleados o de terceros. Su objetivo es el de superar la fragmentación normativa existente y modernizar los principios de privacidad en la Unión Europea. Pero quizá la mayor novedad de la GDPR es que ha elevado la privacidad y la protección del dato a la máxima potencia. Si el big Data convirtió al dato en el petróleo del nuevo siglo, la GDPR hace que “por primera vez, la responsabilidad en cuanto al dato sí que se incorpora como una variable de decisión en cómo voy a trabajar”, decía Roland Ruiz, consultor de software de Information Builder, durante la tercera edición del Chief Data Officer Day (CDO 2017) celebrado en Madrid y en el que, por primera vez se ha desarrollado un summit dedicado al DPO (Data Protection Officer) y ciberseguridad.

La GDPR impacta sobre las empresas en distintos niveles: técnico, legal y organizativo. Sus elementos más relevantes son el derecho de los ciudadanos a la portabilidad de sus datos; la necesidad de obtener un consentimiento activo a la hora de recabar los datos; el deber de las empresas a notificar a la Agencia de Protección de Datos y a los clientes potencialmente afectados si han sufrido una intrusión; y el nuevo cargo de DPO, o Data Protection Officer, el responsable de supervisar la estrategia de protección de datos y su implementación para cumplir con la normativa.

Durante su participación en una ponencia, David Moreno, CISO de Grupo Cortefiel, aseguraba que "los retos del DPO van más allá de lo técnico, hacia lo legal. Tienen que enfrentarse a la estructura y mentalidad de la organización, a la regulación, a los departamentos de marketing –que tiene que saber cómo tratar cierta información. Es un superhéroe". Y añadía el directivo que "nadie sabe hacer eso porque hasta ayer esa figura no existía", y requiere un proceso de aprendizaje continuo.

GDPR – THE DATA PROTECTION OFFICER — CLICAR PARA VER EL VÍDEO

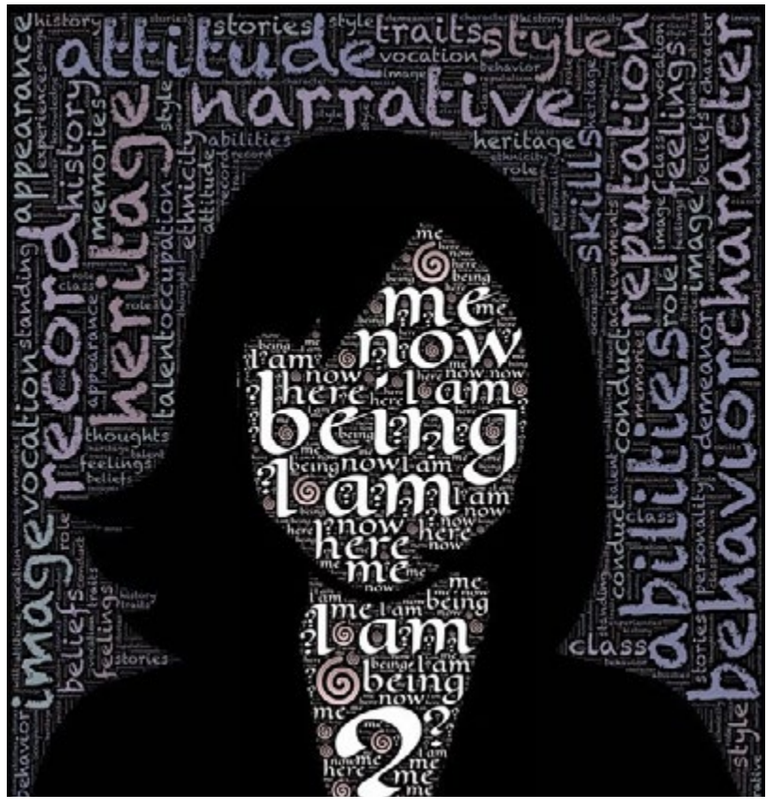
Se Busca

Responsable de protección de datos, DPO, para cumplir con la normativa GDPR, que será de obligado cumplimiento el próximo 25 de mayo de 2018, y cubrir 40.000 puestos vacantes en Europa.

Su papel será el supervisar, coordinar y transmitir la política de protección de datos tanto en el interior de la institución como desde dentro hacia el exterior.

Se requiere:

- Conocimientos legales y de TI
- Gran capacidad de negociación
- Ser pragmática y realista
- Capacidad de visión holística del negocio
- Capacidad de hacer de puente entre las diferentes áreas del negocio y las áreas técnicas



Compañera de escenario, Montserrat Valentí Vall, responsable de Asesoría Jurídica y Cumplimiento Normativo de Seguros Catalana Occidente, aseguraba que el DPO es "una figura que debe tener mucha capacidad de negociación, de poder convertir en ventaja lo que estaba en contra. Una persona pragmática y realista capaz de responder a cómo llevar a cabo una portabilidad o cómo establecer la base legal asociada a ese tratamiento". Elena Mora González, Subdirectora Marco Regulatorio de Seguridad de Mapfre, por su parte, no quiso olvidarse del papel del Data Protection Officer en cuanto a concienciar y divulgar, "porque cuando hablamos de un proyecto de adecuación hablamos de un proyecto de toda la organización. La GDPR es una obligación de toda la compañía", y advertía que el día a día de un DPO "puede ser muy diferente de una organización a otra, porque una puede ser muy tecnológica y otra más legal. Un centro médico difiere de un centro asegurador".

Los expertos hablan

Sobre el perfil del DPO y el impacto que la GDPR va a tener en las empresas hablamos con algunos de los asistentes al Chief Data Officer Day.

El DPO es una figura que cuesta encontrar y en Europa hay 40.000 puestos vacantes sin cubrir

María José Pérez Guillén, Senior DSG Consultant de Informatica, dice que la GDPR impacta de una forma muy global a todas las compañías y por eso se hace necesaria la figura de un DPO que centralice todos los cambios que supone esta regulación. ¿Y cuál sería el perfil de un DPO? “Debe ser una persona que conozca muy bien la legislación, por lo tanto, tendrá que venir del departamento de legal, y a su vez tendrá que ser tecnólogo porque tendrá que ser capaz de traducir todos los cambios que trae la legislación al departamento de TI. Por tanto, es un perfil bastante complejo y bastante completo”, dice Pérez Guillén.

Dice también la ejecutiva que la del DPO es una figura que cuesta encontrar y recuerda que en Europa hay 40.000 puestos vacantes de DPO sin cubrir.

Pablo Boixeda, Sales Ingineer de Cloudera, dice que el primer impacto de la GDPR en las empresas es que “van a tener que proteger la información y van a tener que segmentar esa protección”. El control y visión de los datos será total, porque hay que tener claro cuándo han sido manipulados los datos y por quién; “en definitiva, va a tener que dar una protección de 360 grados a esos datos desde el punto de vista de acceso, que esos accesos puedan ser auditados, aplicar cifrado a esos datos para que no puedan ser extraídos y se puedan explotar desde fuera”.

Respecto al perfil que debe tener un DPO, la visión personal de Boixeda es “una persona que haga de puente entre las áreas de negocio y las áreas técnicas. Ha de entender cómo los datos han de servir al negocio, cómo pueden genera más volumen de negocio, cómo pueden ayudar al departamento de operaciones, cómo puede ayudar a recortar costes, cómo puede ayudar las tecnologías orientadas al dato a sistemas de compliance y de seguridad. Y después tiene que tener una parte más orientada a la tecnología”, ya que tiene que integrarse y tiene que conversar con los departamentos de IT tradicionales.

Ventaja de la GDPR

“Que por primera vez un porcentaje de tu ingreso pueda ser una multa anual está haciendo que todo el mundo, de verdad, vaya a tener una responsabilidad sobre la gobernanza del dato”, asegura Roland Ruiz, de Information Builder, para quién la GDPR ha hecho que “la responsabilidad sobre el dato haya pasado a ser prioritario”.

Entre las tareas del DPO, el supervisar el cumplimiento de lo dispuesto en el Reglamento, así como en otras disposiciones de protección de datos de la Unión o de los estados miembros

Ante la insinuación de que el DPO proceda del departamento legal, Ruiz asegura “si es un perfil puramente legal puede perder contacto con la realidad del negocio. Yo pondría más a una persona que tuviese visión IT y también visión de negocio. Que realmente venga de operaciones o venga de IT es una decisión de la empresa, pero que tenga una visión holística del negocio. Creo que la parte legal se la pueden aconsejar y por tanto no creo que haga falta que sea un experto en esa área”.

Julia Urío Rodríguez, responsable del portfolio de soluciones y gobierno de IBM, explica que la regulación de protección de datos que será de obligado cumplimiento el próximo 25 de mayo tiene varias dimensiones: una más organizativa, otra más de procedimientos y procesos, otra de cómo impacta a las personas de la organización, una dimensión más cercana a los datos, a cómo impacta en la información que esas empresas manejan y usan, y la última es una dimensión relacionada con los niveles de seguridad con respecto al tratamiento de esa información. “A nivel organizativo el impacto va a requerir que se cree una figura de DPO en aquellas organizaciones importantes con volumen de datos a tratar importantes”, dice la directiva.

Sobre ese DPO dice Urío que “tradicionalmente estaba el security data officer que dependía mucho del área de IT pro el hecho de que era un componente de seguridad del dato, pero el DPO está adquiriendo más un componente del negocio, muy cercano a sus departamentos legales, y sus departamentos de gestión de riesgos. Y por tanto sale del área de IT; esa figura del DPO está próxima al negocio, próxima a legal y con ciertos conocimientos tecnológicos”.

Para David Cristóbal Campanario, Pre-Sales Consultant de Talend, la GDPT trae algunos cambios importantes. El primero con respecto a la calidad, puesto que la información debe ser veraz, debe ser cierta y debe ser actualizada; el segundo está relacionado con la trazabilidad del dato, un aspecto al que hasta ahora no se le había prestado mucha atención y que ahora es de vital importancia por lo que implica la portabilidad de la información. “Más allá del borrado de la información, que es algo que se puede considerar relativamente sencillo, el tema de portabilidad de la información es algo que puede convertirse en un quebradero de cabeza para la mayor parte de las empresas”, asegura David Cristóbal.

Sobre el perfil de un Data Protection Officer, dice el ejecutiv de Talend que “en general debe ser eminentemente IT pero conocimientos legales y de las implicaciones que las regulaciones tienen”. Dice también David Cristóbal que el DPO en un perfil “muy difícil de encontrar”.

Aspectos de la regulación como el derecho al olvido o la portabilidad del dato van a tener un gran impacto en las empresas, dice Juan Julián Moreno Piedra, IM&G Pre-Sales Manager de Micro Focus. Añade el ejecutivo que “prácticamente todas las empresas grandes han nombrado un DPO y están empezando a hacer un estudio de los datos, un estudio que tiene que comenzar por hacer un inventario de tus datos, entender qué usuarios usan los datos de tu empresa y para qué los usan, y a partir de aquí establecer la estrategia”.

Respecto al perfil que debería tener un DPO, el ejecutivo de Micro Focus lo tiene claro: “Una persona completamente centrada en los datos, independiente de la parte de TI de las empresas. Un perfil absolutamente cross, presente en todos los departamentos”.

Figura legal o figura de TI, lo que parece cierto es que el DPO se está formando ahora, que es una de las piedras angulares de todo este proceso de adaptación. Que hacen falta 40.000 profesionales y que no es consistente esperar al 24 de mayo para nombra uno, porque no tendrá conocimiento de todo el proceso.

Enlaces de interés...

- W Directrices para el Data Protection Officer (DPO)
- W La GDPR en español, que no te la cuenten
- La GDPR aún no preocupa a los directivos
- Cuatro consejos para empezar a prepararte para la GDPR

MICRO FOCUS®

Discover

the New

Hacia la autenticación **biométrica**

La biometría, la ciencia de analizar características físicas o de conducta que son específicas a cada individuo con el objetivo de ser capaz de autenticar su identidad, se ha vuelto un elemento cada vez más importante en un mundo dominado por los servicios cloud. Para muchos la identidad se ha convertido en el nuevo firewall.

El mundo se ha vuelto digital y cada persona utiliza, o debería utilizar, 27 contraseñas para gestionar el acceso a todos sus servicios, desde el correo electrónico, banca online, redes sociales y todo tipo de recursos.

El momento parece el adecuado. La capacidad que aportan los smartphones junto con los avances tecnológicos, hacen que la biometría sea fácil de utilizar. Al mismo tiempo las grandes empresas, los bancos, compañías se seguros y de salud se han dado cuenta de que necesitan una mejor seguridad. El interés en la adopción de biometría para una autenticación segura está creando una industria con un tamaño de mercado que pasará de los 10.740 millones de dólares en 2015 a más de 32.000 millones para 2022. Además, según en el informe Global State of Information Security Survey 2017 de PwC, el 40% de los encuestados citaron la biometría como una prioridad para proteger a las organizaciones.

¿Y están las empresas españolas preparadas para adoptar soluciones de autenticación biométrica? Para Cristina de Sequera, directora de la unidad de negocio de Transformación Digital de Grupo CMC, está claro que sí, y si no lo están, “han de prepararse rápidamente porque los clientes están demandando soluciones más ágiles, cómodas y seguras”.

De la misma opinión es Jordi Quesada, Key Account Manager Cyber Security de G+D Mobile Security, quien asegura que “dar el salto al acceso lógico es una transición natural si lo que se persigue es mejorar la seguridad en todo tipo de accesos, ya sea a lugares como a información, sistemas, etc.”

Además, y aunque para Héctor Sánchez, director de tecnología de Microsoft Ibérica, “cada vez son más las empresas que están adoptando este tipo de tecnología para su seguridad”, para Rodrigo Chávez Rivas, responsable de IT Security Services & Solutions en Unisys, “son muchas las variables que determinan si una empresa está preparada para adoptar soluciones de autenticación basadas en biometría. Entre las más relevantes destacaría dos: la experiencia de usuario y la madurez de la tecnología”.

Las infraestructuras y recursos TI actuales deben permitir el acceso simultáneo de varios individuos, dispositivos y aplicaciones, y deben hacerlo de forma segura, con garantías. La información y recursos de una red corporativa son cruciales para la continuidad de negocio y una brecha de seguridad no sólo impide esa continuidad, sino que impacta en la reputación de la marca y su futuro crecimiento.

Hay que estudiar no sólo cuándo sino para qué debe una empresa plantearse adoptar soluciones

El paraíso de los hackers

Un buen reto es un regalo para los investigadores. Cuando parece claro que una huella dactilar es más segura que una contraseña, ¿por qué no demostrar lo contrario? Y si se hace a lo grande mejor.

Eso es lo que pensó Starbug, nombre en clave de Jan Krisller, especialista en biometría que en diciembre de 2014 demostró ser capaz de clonar la huella dactilar de la Ministra de Defensa de Alemania, Ursula von der Leyen, utilizando únicamente fotografías en alta definición que había tomado durante una rueda de prensa celebrada en octubre.

La investigación se presentó en el evento anual Chaos Communication Congress, donde Starbur explicó que trató las fotos con el software comercial de huellas digitales de Verifinger con el fin de trazar los contornos de la huella digital de la ministra.

El experto invirtió la imagen del dedo de Von der Leyen y lo imprimió en una hoja transparente con saturación de tóner.

A continuación, vertió una capa de pegamento de madera sobre la parte superior, que, al levantarse, capturó una impresión que Krisller fue capaz de utilizar para desbloquear un iPhone.

Starbug ya es conocido por sus investigaciones en seguridad biométrica. En 2013 fue capaz de falsificar los sensores TouchID de Apple 24 horas después del lanzamiento del iPhone 5S. Usando una mancha en la pantalla de un iPhone imprimió un dedo falso con pegamento de madera y grafeno pulverizable, que desbloqueó con éxito un teléfono registrado en el pulgar de otra persona. En este caso tuvo que tener acceso al terminal de donde robó la huella.

Esta historia, que no deja de ser algo más que curiosa, plantea una cuestión: Cuando una contraseña es robada se puede cambiar, ¿qué ocurre cuando una huella dactilar es copiada?

Windows Hello

Los fabricantes de ordenadores primero, y los de terminales móviles después, han normalizado el uso de la biometría para verificar la identidad del usuario. Los lectores de huellas dactilares empezaron a aparecer las PDA u en ordenadores portátiles profesionales hace bastantes años. Ahora son comunes en smartphones, y no sólo en los de gama alta.

Y en este proceso de normalización de uso de una tecnología también participa el software, en este caso Windows 10, la última versión del sistema operativo de Microsoft que llegó al mercado con Windows Hello, "una forma más personal de iniciar sesión en tus dispositivos Windows 10 con solo un vistazo o un toque", dice la compañía.

Windows Hello usa una combinación de cámaras de infrarrojos (IR) y software especial para proteger contra la suplantación de identidad.

Windows almacena los datos biométricos que se usan para implementar Windows Hello de forma segura sólo en el dispositivo local. Los datos biométricos no pasan de un dispositivo a otro ni se envían nunca a servidores o dispositivos externos. Dado que Windows Hello sólo almacena los datos de identificación biométrica en el dispositivo, no hay ningún punto de colección único que un atacante pueda poner en riesgo para robar los datos biométricos.

De cara a las empresas, las credenciales de Windows Hello se pueden enlazar con el dispositivo y el token. Además, el proveedor de identidad (por ejemplo, la cuenta Active Directory, Azure AD o Microsoft) valida la identidad del usuario y asigna la clave pública de Windows Hello a la cuenta del usuario durante el paso de registro. En función de la directiva, las claves se pueden generar en el hardware o en el software, aunque el gesto de Windows Hello no vale en otros dispositivos, ni se comparte con el servidor, sino que se almacena localmente en un dispositivo concreto.

Añadir que las cuentas personales (cuenta Microsoft) y las corporativas (Active Directory o Azure AD) usan un solo contenedor para las claves. Todas las claves están separadas por dominios de proveedores de identidad para garantizar la privacidad del usuario.

de autenticación biométrica, dice Cristina de Sequera, asegurando al mismo tiempo que "se están desarrollado muchas iniciativas de transformación digital que integran tecnologías de autenticación biométrica en el ámbito de relación con el cliente

para mejorar la experiencia de usuario en el proceso de identificación.

Para Héctor Sánchez, director de tecnología de Microsoft Ibérica, "en un mundo en el que las amenazas son cada vez más constantes, las empress

2017 USER RISK REPORT

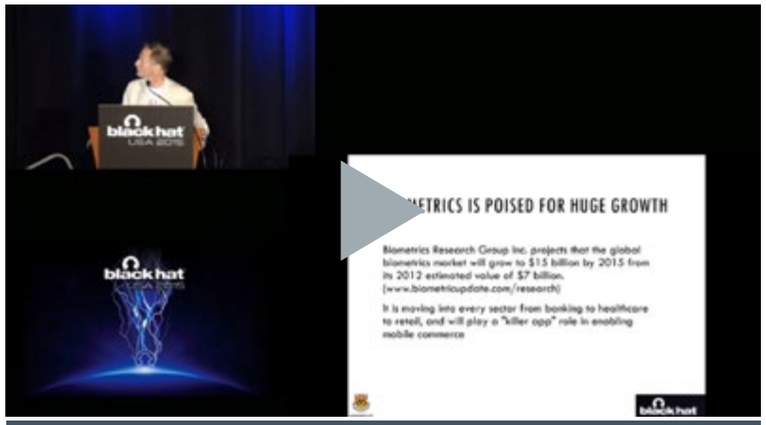
Una encuesta elaborada por Commvault entre grandes responsables de empresas recoge que el 81% se sienten extremadamente preocupados por perderse los avances del cloud. Es lo que se llama el Cloud FOMO (Fear of Missing Out).

La encuesta concluye que el Cloud FOMO está impulsando a los líderes empresariales a avanzar a toda velocidad en las estrategias de nube, con el 93% de los encuestados afirmando que están moviendo al menos algunos de sus procesos a la nube. Además, el 56% declaró que se han movido o tienen la intención de trasladar no sólo algunos, sino todos sus procesos a la nube.

deben ser conscientes de que deben adoptar cuanto antes medidas de seguridad que les permitan proteger su información y la de sus empleados".

"Cualquier empresa que tenga aplicaciones donde se requiera una autenticación basada en usuario y password, puede plantearse el adoptar esta tecnología", dice Jordi Quesada, añadiendo que la seguridad biométrica no debe adaptarse por seguridad que se añade, "también por una mejora de la experiencia de usuario, facilidad de uso y gestión".

Rodrigo Chávez Rivas añade el tema del coste en la ecuación al asegura que una empresa debe plantearse adoptar este tipo de tecnologías "cuando tenga casos de uso en los que el coste de su adopción se justifique, por ejemplo, cuando se necesite tecnologías de autenticación que no sólo proporcionen seguridad confiable, sino que sean además extremadamente difíciles de falsificar". Y es que hay que tener en cuenta que, si bien la relación entre los beneficios y el precio asociados a las soluciones de autenticación biométrica han mejorado significativamente durante la última década, no significa que



CÓMO EVITAR LOS RIESGOS OCULTOS DE LOS IDENTIFICADORES BIOMÉTRICOS **CLICAR PARA VER EL VÍDEO**

se deban adoptar para todos los casos, añade.

"Tradicionalmente la inclusión de soluciones de autenticación biométrica incrementaba significativamente los costes frente a las alternativas convencionales. Sin embargo, el uso masivo de dispositivos móviles por parte de los consumidores y la disponibilidad cada vez mayor de aplicaciones de autenticación biométrica han abierto una puerta a la adopción masiva de la biometría como mecanismo de autenticación para múltiples casos de uso. Por ejemplo, los sistemas de pago con móvil que usan autenticación biométrica hacen que la acción de pago sea cómoda y segura", dice también el directivo de Unisys.

"Si las empresas no están preparadas para la autenticación biométrica han de prepararse rápidamente porque los clientes están demandando soluciones más ágiles, cómodas y seguras"

Cristina de Sequera, Grupo CMC

Elementos de autenticación esenciales

Hay tres factores de autenticación, el primero basado en lo que eres (biometría), el segundo basado

THE RANSOMWARE X.

Mediante la integración de tecnologías de Machine Learning a sus mecanismos de detección, la solución **Trend Micro™ XGen ™ endpoint security** protege contra el ransomware y garantiza la integridad de sus datos.

El ransomware es sólo una parte del problema. Su vulnerabilidad, representada por la "X", también podría ser un ataque de tipo Zero Day, una amenaza debida al comportamiento de sus usuarios o cualquier actividad que comprometa la integridad de sus datos y de su reputación.

What's your X? Tren Micro™ XGen™ endpoint security es la solución.

#WhatsYourX

TREND MICRO™

trendmicro.es/xgen

Apple FaceID

A mediados de septiembre se anunciaba el lanzamiento del iPhone X. Entre sus características más destacadas el haber sustituido el TouchID por el FaceID, o lo que es lo mismo, haber sustituido la huella dactilar por el reconocimiento facial como sistema de verificación, que se utilizará no sólo para desbloquear el terminal, sino para firmar en las aplicaciones y autorizar los pagos realizados a través de Apple Pay o iTunes.

FaceIS funciona con la cámara frontal del terminal y un sistema de infrarrojos conocido como TrueDepth que proyecta una red de 30.000 puntos sobre el rostro del usuario para crear una estructura en tres dimensiones.

Esta capacidad no sólo refuerza la seguridad, sino que ayudará al FaceID a procesar todas las imágenes y reconocer el rostro del usuario independientemente del peinado, gafas, vello facial, iluminación y otros posibles cambios.

en lo que sabes (contraseña) y el tercero basado en lo que tienes (un dispositivo móvil por ejemplo), y tres elementos esenciales para asegurar el acceso a la información: Single Sign-On, gestión de contraseñas y control de accesos.

El llamado Single Sing-On, o acceso único, es un servicio que permite al usuario utilizar un conjunto de credenciales (por ejemplo, ID y contraseña) para acceder a varias aplicaciones. Este tipo de acceso mejora la experiencia del usuario porque sólo debe iniciar sesión una vez al tiempo que ayuda con el registro y la actividad del usuario en el backend.

Es una realidad que el número de servicios online a los que accedemos ponen a prueba autenticación de la identidad. Si a este inicio de sesión se le suma la biometría, el tema se simplifica. Por ejemplo, las huellas dactilares, que son bastante fáciles de integrar con la mayoría de los servicios, pueden utilizarse para el inicio de sesión único para un conjunto de aplicaciones. Se une una buena experiencia de usuarios con una mayor seguridad de la cuenta.

Los gestores de contraseñas nacieron para garantizar que los usuarios escogieran contraseñas complejas sin que tuvieran la necesidad de recordarlas. Se trata de programas que son capaces de generar, almacenar y recuperar esas contraseñas para el usuario. Actualmente son extremadamente accesibles –a veces incluso presentes en productos de seguridad de consumo, incluso como un servicio online. Las contraseñas se almacenan de manera cifrada para mantenerlas a salvo de usuarios y aplicaciones maliciosas. En ocasiones estos programas son capaces de rellenar los campos de login/password por el usuario, lo que mejora enormemente la experiencia de los usuarios.

El control de accesos tampoco es nuevo, pero ha ganado protagonismo en los últimos años. Conocida por las siglas IAM (Identity and access control), esta tecnología permite la identificación y autenticación de usuarios. También aquí la biometría puede jugar un papel fundamental a la hora de garantizar

"En materia de seguridad todo suma, y los métodos de seguridad biométrica añaden neuvas formas de asegurar nuestros equipos y la información que almacenan"

Héctor Sánchez, Microsoft Ibérica

"Actualmente pueden encontrarse soluciones de autenticación biométrica de buena calidad a precios razonables y con costes predecibles de instalación, operación y mantenimiento"

Rodrigo Chávez Rivas, Unisys

de una manera más fácil que sólo la persona correcta accede a la información correcta en el momento correcto y por las razones correctas, que es la idea que está detrás de las soluciones de gestión de identidades y accesos

Una huella dactilar no sólo elimina el riesgo asociado a un pin y una contraseña, sino que la persona que accede a los recursos es la que tiene que acceder.

Critina de Sequera va un paso más allá. Explica que la propuesta de Grupo CMC, llamada 02 Digital, se basa "por un lado, en adaptar el tipo de biometría a utilizar al proceso concreto en el que se desea utilizar y, por otro, en utilizar la biometría dentro de una combinación de factores, de forma que conseguimos elevar exponencialmente la seguridad de la autenticación. No hay biometrías buenas o malas, hay procesos que utilizan esas biometrías de forma adecuada y procesos mal diseñados".

La oferta de G+D se centra en dispositivos móviles y permite combinar diferentes opciones biométricas en función del riesgo o nivel de seguridad que queramos aplicar. Además, la solución está preparada para ir incorporando más tecnologías biométricas a medida que sean soportadas por los dispositivos móviles.

Unisys cuenta con una plataforma abierta y orientada a servicios, Stealth Identity, que permite una gestión de la identidad completa a través de la biometría y que integra todos los módulos del ciclo de vida de la identidad.

De la huella dactilar al mapa de las venas

Cuando se trata de aplicar la biometría a la autenticación se tienen en cuenta no sólo aspectos físicos que son inherentes a cada ser humano, sino los patrones. O lo que es lo mismo tecnologías biométricas fisiológicas y tecnologías biométricas de comportamiento. "Entre las fisiológicas están las que permiten el reconocimiento de huella dactilar, reconocimiento facial, de iris, de retina, de la mano, entre otras. Entre las de comportamiento están las que permiten el reconocimiento de firma, de voz, de escritura de teclado, entre otras", dice Rodrigo Chavez Rivas. Por ejemplo, en el caso de la dinámica de firmas, que no sólo tiene en cuenta la imagen de esa firma sino cómo se ha producido teniendo en cuenta diferencias en la presión y velocidad de escritura en varios puntos de la firma.

Eso mismo ocurre con los patrones de tecleo, donde no sólo se reconoce la contraseña sino los

intervalos entre cada pulsación de la tecla y la velocidad total a la que se escribe.

Sin duda una de las biometrías más conocidas es la de la huella dactilar, presente ya en muchos dispositivos de consumo como móviles o portátiles. La huella dactilar recoge dos tercios de todo el mercado de autenticación biométrica. Entre sus grandes ventajas no sólo el ser únicas, sino que el hardware de lector de huella requiere muy poco espacio físico y los datos que genera son pocos.

Pero para Chavez Rivas, es necesario explorar y desarrollar otras opciones por varias razones: “El uso mayoritario de la tecnología de huella dactilar lleva asociado un mayor número de amenazas comparado con otras tecnologías biométricas; y es necesario ofrecer alternativas a los casos de excepción. Por ejemplo, usuarios que no disponen de una huella dactilar reconocible o cuya huella se va deteriorando significativamente con el tiempo”.

Además, dice Jordi Quesada, “se puede dar el caso de que un usuario tenga una lesión en el dedo. También que intentemos usar el sistema justo después de salir de una hora de piscina. En esos casos, la biometría a través de la huella no va a funcionar. Además, por experiencia de usuario podemos querer ofrecer otras opciones o alternativas”.

Por eso, aunque el uso de la huella dactilar se haya extendido, hay que seguir avanzando. El reconocimiento facial es otro tipo de biometría que se lleva utilizando desde hace algún tiempo; se centra en diferentes rasgos, incluyendo los contornos superiores de los ojos, las áreas que hay alrededor de los pómulos, los lados de la boca o la ubicación de la nariz y boca.

El escáner de retina o de iris, el mapa de las venas de la mano, o los latidos del corazón como elementos de autenticación biométrica están siendo objeto de gran estudio. Los investigadores de seguridad consideran el cuerpo humano como la parte del cuerpo más fiable para la autenticación biométrica porque la retina y el iris no sufren cambios durante toda la vida de las personas.

"Dar el salto al acceso lógico es una transición natural si lo que se persigue es mejorar la seguridad en todo tipo de accesos, ya sea a lugares como a información o sistemas"

Jordi Quesada, G+D

Un escáner de retina iluminará los complejos vasos sanguíneos del ojo de una persona usando luz infrarroja, haciéndolos más visibles que el tejido circundante. En el caso del escáner de iris, se basa en fotos o vídeos de alta calidad de uno o ambos iris de una persona, que también son únicos para el individuo. Sin embargo, los escáneres de iris han demostrado ser fáciles de engañar simplemente usando una fotografía de alta calidad de los ojos o la cara del sujeto.

El reconocimiento de voz para asuntos de seguridad busca identifica quién habla y no lo que se dice. Para identificar al usuario un software especializado descompone las palabras en paquetes de frecuencias llamadas formantes. Estos paquetes de formantes también incluyen el tono de un usuario, y juntos forman su impresión de voz.

La disposición de las venas es única para cada persona, ni siquiera compartida en gemelos, lo que ha hecho que algunas empresas opten por este tipo de soluciones de reconocimiento y autenticación. Las venas tienen una ventaja añadida ya que son increíblemente difíciles de copiar y robar porque son visibles bajo circunstancias estrictamente controladas. Un escáner de geometría de vena iluminará las venas con luz infrarroja cercana, lo que hará que sus venas sean visibles en la imagen.

Respecto a la tecnología de autenticación que se vende más, dice Cristina de Sequera que "actualmente está implantándose mucho en el mercado la biometría facial y probablemente en los próximos meses veremos también bastante uso de biometría de voz. Otras biometrías, como la conductual o la de gestual, todavía tendrán que afinarse para que uso se haga más más extensivo".

Para Rodrigo Chavez Rivas, "la tecnología de autenticación más vendida está basada en un doble factor de autenticación que combina la autenticación de usuario/contraseña con la autenticación basada en OTP (One Time Password)".

Enlaces de interés...

- La revolución de la Autenticación
- Escogiendo la mejor Autenticación biométrica
- Autenticación biométrica en la banca móvil
- Mercado de aplicaciones biométricas móviles

Check Point®
SOFTWARE TECHNOLOGIES LTD

ONE STEP AHEAD

› of the hype

LOS HECHOS:

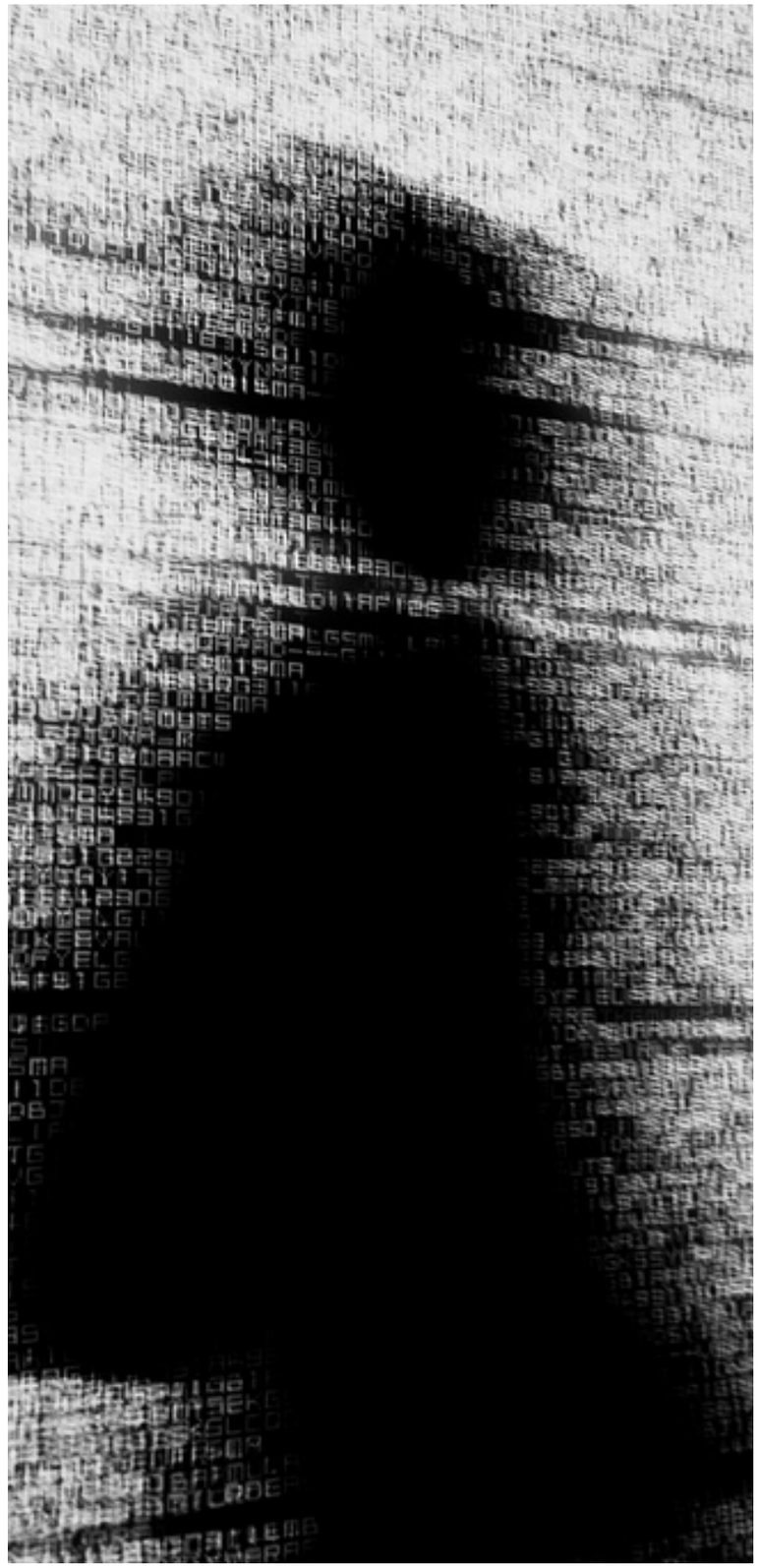
CHECK POINT THREAT PREVENTION OFRECE LA TASA DE DETECCIÓN DE MALWARE. MÁS ALTA DE LA INDUSTRIA

LGUNOS FABRICANTES EXPONEN A SUS CLIENTES AL MALWARE DURANTE 5 MINUTOS. CHECK POINT NO

CHECK POINT PROTEGE A SUS CLIENTES CONTRA EL MALWARE EN ARCHIVOS. OTROS NO

No hay segundos premios en ciberseguridad.
Contacta con nosotros. 91 799 27 14 — info_iberia@checkpoint.com

Las brechas de seguridad **más sonadas** de la historia



Se calcula que en la última década se han producido unas cinco mil brechas de seguridad. Las hay grandes y pequeñas, las más conocidas y las que han pasado desapercibidas, las que han llevado a la desaparición de la empresa que las sufrió y la que acabó, voluntaria o involuntariamente, con el que la lideraba.

Las brechas de seguridad son habituales. No en vano se habla de tres tipos de empresas: las que han sido atacadas y lo saben, las que han sido atacadas y no lo saben y las que van a ser atacadas. Es una chanza conocida en el sector, pero muy cierta. La movilidad, el cloud, el as-a-service no han hecho más que complicar la seguridad, ofrecer más opciones y puntos de entrada a los hacker. Pero las brechas se han producido desde hace más de una década, aunque las primeras fueran más el resultado de un error que de un ciberataque.

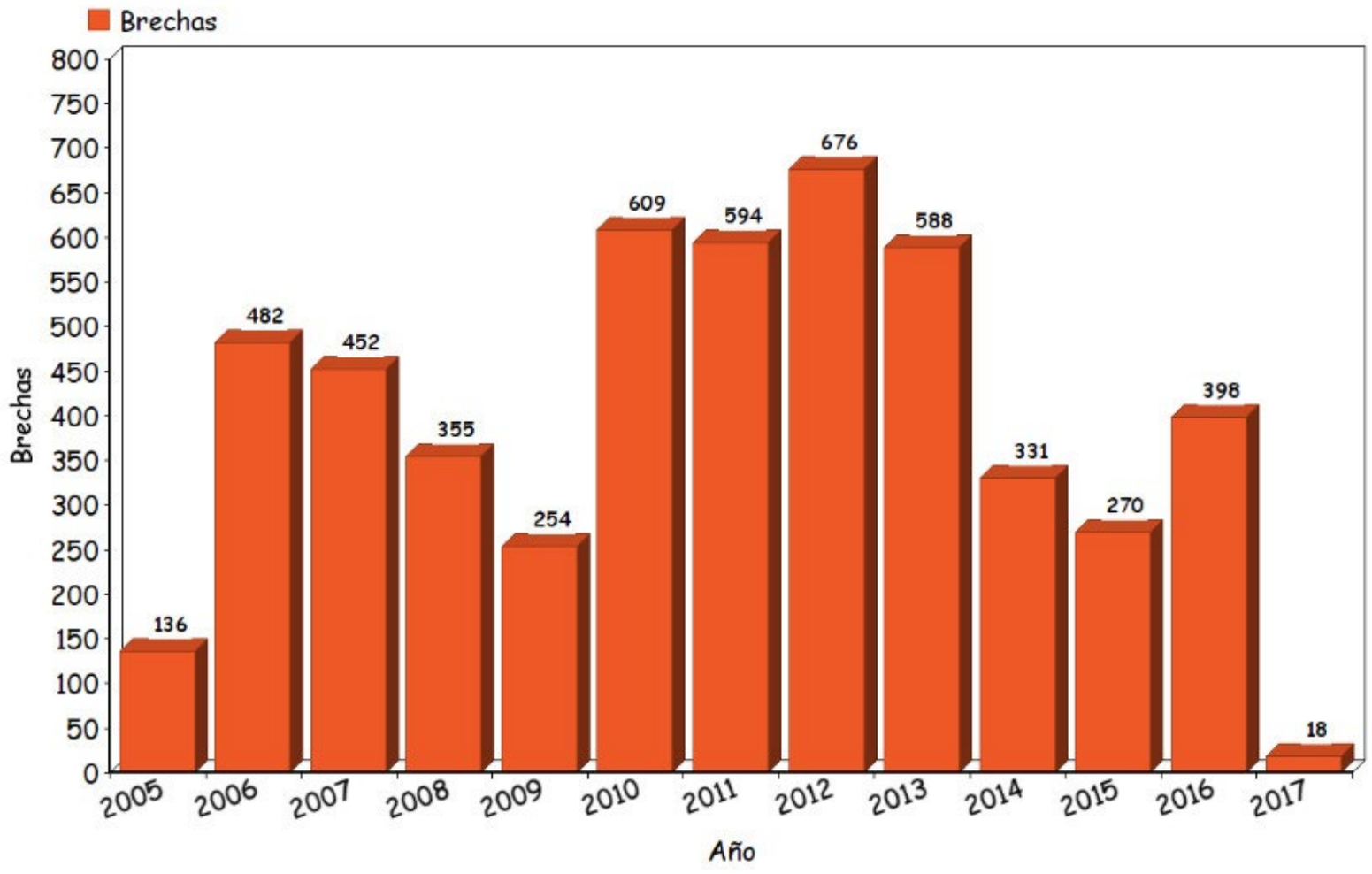
Aunque las brechas de seguridad se llevan produciendo desde antes de 2005, empezaron a tener

cierto volumen a partir de ese año, algo que se atribuye al incremento exponencial del volumen de datos, lo que dio a los cibercriminales una mayor oportunidad de exponer gran cantidad de datos en una única brecha

2017

En lo que va de año se han producido decenas de brechas de seguridad. El año se iniciaba con la de Arby's, un gigante de comida rápida que se vio afectado por un software malicioso instalado en terminales de venta de más de mil tiendas. La información robada incluye tarjetas de crédito y débito utilizadas entre el 25 de octubre de 2016 y el 19 de enero de 2017.

También a primeros de año una brecha en Dailymotion, uno de los servicios para compartir vídeos en internet más populares fue hackeado, desvelando algo más de 85,2 millones de direcciones y nombres de usuarios. Además, una quinta parte de los registros robados incluían contraseñas, aunque cifradas.



Dow Jones & Co., propietario entre otros del Wall Street Journal, anunció en julio que registros de unos 2,2 millones de suscriptores con información relacionada con sus nombres, IDs, direcciones de sus casas y trabajos, direcciones de email y los último cuatro dígitos de sus tarjetas de crédito, habían sido robados.

Unicredit, uno de los bancos más importantes de Italia, anunciaba este verano una brecha de datos que afectó a 400.000 de sus clientes cuyos números de cuenta y datos personales habían sido robados. El banco aseguró que las contraseñas no habían sido comprometidas, por lo que los ciberdelincuentes no han podido realizar transacciones no autorizadas.

Una inapropiada configuración de backup en River City Media –uno de los mayores proveedores de spam del mundo, dejó expuestas 1.370 millones de direcciones de email, algunas de las cuales iban acompañadas de direcciones IP y físicas. El fallo de seguridad también desveló la estrategia de la com-

pañía incluyendo detalles como planes de negocios, registros de Hipchat, cuentas y más.

Hasta el cierre de la revista la última gran brecha de seguridad ha sido la de Equifax, una firma crediticia que a primeros de septiembre anunciaba haber sufrido una brecha de seguridad que dejaba expuesta la información de 143 millones de consumidores en Estados Unidos. La compañía admitía que la brecha fue descubierta el 29 de Julio, cuando se detectó un acceso no autorizado al sistema. Las primeras investigaciones muestran que los hackers estuvieron accediendo a los sistemas de la compañía durante un período de más dos meses. Se investiga además la venta de dos millones de dólares en acciones por parte de dos empleados de Equifax el día después de conocerse la brecha.

2016

La brecha de seguridad más sonada de 2016 fue la de Yahoo!, no sólo por la cantidad, 500 millones de usuarios, sino porque fue detectada dos años después de haberse producido. En octubre de 2016 Weenly y Foursquare fueron las últimas compañías en anunciar sendos ciberataques que desvelaron 43,4 millones de registros en el caso de la primera y 22,5 millones de la segunda. Cada registro incluía el nombre de usuario, dirección de email, contraseña y dirección IP.

Con 32 millones de credenciales robadas, Twitter también ocupa un espacio en la lista de brechas de seguridad más importantes de 2016, aunque parece que los dos fueron robados directamente a los usuarios más que de los servidores de la red social. No fue el caso de MySpace, otra red social, que fue hackeada para el robo de 360 millones de datos de cuentas con direcciones de email y contraseñas, que posteriormente se vendieron por 2.800 dólares.

2016 también fue un mal año para la red Friend Finder Networks, compañía que está detrás de

Cómo gestionar una brecha de seguridad según la GDPR

Parece que en lo que respecta a brechas de seguridad, todo pasa en Estados Unidos. Se ven pocas empresas europeas en este listado de las brechas de seguridad más importantes de la historia, pero las cosas podrían empezar a cambiar a partir de mayo de 2018, cuando entre en vigor el nuevo Reglamento Europeo de Protección de Datos, más conocido como GDPR.

Entre las novedades más significativas la obligatoriedad de notificar las brechas de seguridad o fugas de información tanto a las autoridades como a los usuarios afectados, algo que las empresas de Estados Unidos tienen que hacer desde hace bastantes años.

Es decir que se deben notificar las incidencias de seguridad que impliquen una violación de datos personales sin demora injustificada y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella.

La diferencia respecto a la LOPD, Ley Orgánica de Protección de Datos, es que esta sólo afecta a los operadores de telecomunicaciones o proveedores de acceso a Internet. Con la GDPR cualquier empresa, independientemente de su tamaño o actividad, que maneje datos personales tendrán que informar.

Los usuarios afectados, así como la Agencia de Protección de datos, tendrán que recibir información de las posibles consecuencias de la violación de privacidad de sus datos, sobre todo si pudiera generar un problema de fraude o de usurpación de identidad, así como perjuicio a su reputación.

También habrá ocasiones en las que no se exigirá la notificación a los afectados. Si los datos extraídos estén cifrados y por tanto esa brecha de seguridad no afecte a los datos personales la notificación a los afectados no será obligatoria; tampoco la intrusión y la violación de datos no pueda afectar negativamente a los datos personales o a la intimidad del particular.

No adaptarse al nuevo reglamento supone asumir un riesgo que puede salir muy caro, pues las empresas que no lo hagan pueden enfrentarse a sanciones de hasta veinte millones de euros, frente al máximo de 600.000 de la LOPD vigente en estos momentos.

GDPR obligará a toda empresa que maneje datos de usuarios a informar sobre una brecha de seguridad 72 horas después de haberla sufrido

Penthouse, entre otras publicaciones. Un total de 412 millones de cuentas quedaron expuestas en un ciberataque que explotó una vulnerabilidad de inclusión de archivos locales, lo que permitió a los hackers acceder a todos los sitios de la red.

La conducta de VTech, el conocido fabricante de juguetes, en lo que se refiere a la ciberseguridad quedó en entredicho después de que un ciberataque consiguiera extraer información de 11,6 millones de cuentas, de las que 6,4 correspondían a niños. La información extraída incluía direcciones físicas, nombres de los padres y los niños, imágenes de los niños utilizadas como sus avatares online, contraseñas cifradas, direcciones de email e incluso preguntas secretas en texto plano.

2015

Este fue el año de una de las brechas más famosas, la que afectó a Ashley Madison. Los ciberdelincuentes extrajeron casi 100 gigabytes de datos correspondientes a más de 37 millones de clientes. Dos años después, en julio de este año, la compañía ha tenido que pagar 11,2 millones de dólares para indemnizar a las víctimas afectadas.

También sonada fue la brecha que afectó a Sony Pictures, a la que robaron entre 10 y 10,5 millones de registros con nombre, fechas de nacimiento, números de la seguridad social, direcciones de email, números de teléfono, además de información financiera como número de tarjetas de crédito.

2014

En octubre de 2014 JPMorgan desveló el que se ha convertido en del mayor robo de datos de clientes a una institución financiera en la historia de Estados Unidos. Los ciberdelincuentes consiguieron acceder a cerca de 76 millones de cuentas con nombres, direcciones postales, teléfonos y direcciones de email. El ciberataque consiguió acceder a los servidores con derechos de administrador.

RIVER CITY MEDIA HACKEADA — CLICAR PARA VER EL VÍDEO

2014 fue además un año negro para la industria del retail con brechas que afectaron a dos conocidos retailers de Estados Unidos, The Home

¿CUÁNTO CUESTA UNA BRECHA DE SEGURIDAD?

IBM ha patrocinado el 12th annual Cost of Data Breach Study elaborado por Ponemon Institute, un informe que asegura que este año el coste de medio de una brecha de seguridad o fuga de datos ha descendido un 10% respecto al año anterior. También es menor el coste de cada registro perdido o robado. Casi en compensación el tamaño de las brechas ha crecido un 1,8%. ¿Por qué una brecha es más cara cuando impacta en una empresa de Estados Unidos? ¿Qué elementos hacen que una brecha cueste más o menos?

Depot y Target. El primero sufrió dos brechas, la primera por parte de tres empleados que se cree que se llevaron 30.000 registros y la segunda en septiembre, cuando un ciberataque contra las TPV de sus más de dos mil tiendas consiguió extraer información de 56 millones de tarjetas de crédito y débito.

En el caso de Target se conoció en 2014 un ciberataque ocurrido a finales de 2013 que dejó expuesta la información de 70 millones de tarjetas de pago. Una sentencia de este año obliga a la compañía a pagar 18,7 millones de dólares.

eBay fue también protagonista en 2014 después de que un ciberataque permitiera a los hackers tener acceso a una de sus bases de datos y robar información de más de 145 millones de cuentas. Entre los datos robados contraseñas, direcciones de email, fechas de cumpleaños, direcciones de correo electrónico y otros detalles personales. No se tuvo acceso a datos financieros porque esa información se guarda cifrada de manera separada.

2013

El impacto de la brecha de seguridad sufrida por Adobe a finales de 2013 pasó rápidamente de tres millones de registros a más de 38 millones, cifras oficiales de la compañía, mientras algunos investigadores subían hasta los 150 millones. Adobe fue víctima de un ataque que expuso los ID de cliente y las contraseñas cifradas.

Evernote publicaba en marzo de 2013 un aviso informando a sus cerca de 50 millones de usuarios que había sufrido una seria violación de seguridad que permitió a los hackers robar nombres de

Consecuencias financieras de una brecha de seguridad

El incremento de las brechas de seguridad es constante. Sin embargo, su coste varía dependiendo de cada organización. En general, y según un informe de Ponemon Institute patrocinado por IBM, el coste de las brechas está descendiendo, un 10% de manera global y un 2,9% per cápita. Por otra parte, el tamaño medio de la brecha, es decir, el número de registros perdidos o robados se ha incrementado un 1,8%.

El informe también dice que las brechas son más caras en Estados Unidos o Canadá que en Brasil o India, y que varían dependiendo de las industrias. En este sentido, el coste medio de una brecha por registro perdido o robado es de 141 dólares, cifra que se eleva hasta los 245 dólares cuando hablamos del vertical de sanidad, y se reduce a los 71 dólares en el sector público.

Obvio, cuando más rápido se detecta y contiene una brecha de seguridad, menor es su coste. Los datos del 2017 Ponemon Cost of Data Breach Study indican que por tercer año consecutivo se ha detectado una relación entre cuán rápido puede una organización identificar y contener la brecha y las consecuencias financieras.

Los ciberdelicuentes causan la mayoría de las brechas de seguridad, que además tienen un coste superior que cuando es un error o negligencia.

Un equipo de respuesta ante incidentes y utilizar tecnologías de cifrado reduce el coste de registro comprometido hasta los 19 dólares.

Con 1.370 millones de registros expuestos, la sufrida por River City Media este año es la brecha de seguridad más grande de la historia

usuario, direcciones de correo electrónico asociadas y contraseñas cifradas. Los hackers, sin embargo, no fueron capaces de acceder a detalles financieros ni a las notas que los clientes habían almacenado.

2012

En 2012 Dropbox sufrió una brecha de seguridad que afectó a 68 millones de cuentas. La información no se conoció hasta 2016 cuando se descubrió online una gran cantidad de datos de usuarios del servicio de almacenamiento con información sobre nombres de usuarios y contraseñas. Dropbox confirmó años después que las credenciales habían sido robadas con los detalles de acceso robados a un empleado.

También en 2012 quedaban expuestas doce millones de Apple IDs. Un grupo de hackers llamado AntiSec y con relaciones con Anonymous aseguraba haber obtenido los datos personales de los doce millones de usuarios hackeando un ordenador del FBI. El grupo publicaba, como demostración, los datos de un millón de esas cuentas.

Blizzard, responsable de juegos tan populares como Diablo III, Starcraft II o World of Warcraft, anunciaba una brecha de seguridad con impacto en cerca de 14 millones de jugadores y que desvelaba contraseñas cifradas, direcciones de email y las respuestas a las preguntas de seguridad.

2011

Una de las brechas más sonadas de la historia se produjo este año, cuando Sony detectó una intrusión de 24,6 millones de cuentas de usuario de una base de datos de 101,6 millones. La base de datos contenía nombres, direcciones postales y de correo electrónico, fechas de nacimiento, credenciales de inicio de sesión para Playstation Network (PSN) y Qriocity. Se sospecha que los hackers también pueden tener acceso a historiales de compras, direcciones de facturación y preguntas de seguridad.

En abril de 2011 PlayStation Network tuvo que interrumpir su servicio después de detectar una intrusión externa en los servicios PlayStation Network y Qriocity, en la que los datos personales de aproximadamente 77 millones de cuentas se vieron comprometidos. El ataque ocurrió entre el 17 de abril y el 19 de abril de 2011, obligando a Sony a desactivar temporalmente PlayStation Network el 20 de abril.

Wordpress sufrió en 2011 un ataque contra varios de sus servidores que dejó expuesto el código fuente y contraseñas de 18 millones de sus usuarios.

2010

La mayor brecha de datos en 2010 generó el robo de trece millones de registros. Los hackers fueron capaces de penetrar deviantART, una de las mayores redes sociales para artistas a través de la empresa de comercialización Silverpop Systems Inc. La base de datos expuesta consistía en nombres de usuario, direcciones de correo electrónico y fechas de nacimiento de todos los usuarios de deviantART.

2009

RockYou, un fabricante de aplicaciones para redes sociales, pedía a 32,6 millones de usuarios que cambiaran sus contraseñas tras ser atacado. Un fallo de inyección SQL en su base de datos dejaba expuesta la lista entera de nombres de usuario,

Y si no cumplo la GDPR, ¿Qué?

Apenas quedan unos meses para que una de las normativas más exigentes en materia de protección de datos entre en vigor. ¿Estás seguro de cumplir con ella? ¿Qué pasaría en caso de que no fuera así?

Regístrate en este IT Webinar y conoce las principales claves de la Regulación Global de Protección de Datos, la nueva normativa europea que exige una nueva forma de gestionar y proteger la información que manejan las empresas.

direcciones de email y contraseñas, que estaban almacenadas en texto plano.

También en este año 76 millones de registros de veteranos de Estados Unidos fueron expuestos cuando un disco duro defectuoso fue enviado a reparar sin que primero se destruyeran sus datos. La unidad era parte de una matriz RAID de seis unidades que contenían una base de datos de Oracle llena de información de veteranos. La unidad se consideró irreparable y luego fue enviada a otra entidad para el reciclaje, una vez más, sin ser borrada.

Fue en 2009 cuando 130 millones de tarjetas de crédito fueron robadas en un ciberataque contra Heartland Paymant System. El problema de agravó por los retrasos a la hora de revelar la brecha y las informaciones inexactas relacionadas con la misma.

2008

No fue un ciberataque, sino el robo de información por parte de un empleado que robó información de 17 millones de cuentas lo que añadió a Countrywide Financial Corp. a la lista de 2008.

Tampoco fueron los ciberdelincuentes los culpables de que 12,5 millones de registros del Bank of New York Mellon con nombres, números de seguridad social y números de cuentas fueran expuestos. Los datos se perdieron cuando una caja de cintas de respaldo llegó a una instalación de almacenamiento con una cinta desaparecida.

Los datos de 18 millones de miembros de Auction.co.kr, una página de subastas de Corea del Sur, fueron robados por un hacker chino. Entre la información se encontraba una gran cantidad de datos financieros.

También curiosa fue la brecha de GS Caltex en 2008: En una calle de Seúl se encontraron dos CD con una lista de 11,9 millones de clientes de la compañía.

2007

En marzo de 2007 el retailer TJ MAxx sufrió una brecha de seguridad que afectó a cien millones de registros con números de tarjetas de crédito y débito, así como los registros de devolución de mercancías que contienen nombres y números de licencia de conducir, así como números de cuenta de tarjeta de crédito. El ciberdelincuente, que

¿Te avisamos del próximo IT Digital Security?

atacó los sistemas de Heartland un año después, robó los números durante un periodo de 18 meses, con un impacto económico que se calcula en 118 millones de dólares.

HM Revenue and Customs (HMRC) perdía en 2007 discos informáticos que contenían datos confidenciales de 25 millones de beneficiarios de prestaciones para niños. La organización dijo en su momento que no creía que los registros -nombres, direcciones, fechas de nacimiento y cuentas bancarias, hubieran caído en malas manos caído en manos equivocadas.

Mantener la información sensible cifrada es una manera de reducir el impacto de una brecha de seguridad

2006

Un portátil y un dispositivo de almacenamiento con datos confidenciales de 26,5 millones de veteranos de Estados Unidos fueron robados del hogar de un empleado no identificado del Department of Veterans Affairs, recuperándose casi dos meses después. La información almacenada consistía en nombres, números de seguridad social, fechas de nacimiento, números de teléfono y direcciones de todos los veteranos estadounidenses dados de alta desde 1975.

Más de 17 millones de registros de iBill, un servicio de pago online asociado con sitios de pornografía, fueron colgados en Internet con información sobre nombres, números de teléfono, direcciones de email y postales, credenciales de acceso, y cuentas de compra.

Por razones que aún se desconocen AOL publicó 20 millones de registros de 650.000 usuarios. Entre los datos expuestos, el historial de búsquedas de tres meses, así como si pincharon en un enlace. La descarga con los datos estuvo disponible durante varios días.

2005

La mayor brecha de seguridad de este año fue la sufrida por CardSystems. Un individuo no autorizado se infiltró en la red informática de un procesador de pagos de terceros y robó hasta 40 millones de números de tarjetas de crédito. El 2009 se supo que CardSystems almacenaba información sobre tarjetas de crédito sin cifrar en sus servidores.

Enlaces de interés...

- W ¿Cuánto cuesta una brecha de seguridad?
- W Fuga de información en un despacho de abogados: ¿cómo gestionarla?
- W GDPR: todas sus claves
- I Calcula el coste de una Brecha de Seguridad

NUEVO.
PERO NO NACIDO AYER.

CSC Y HPE ENTERPRISE SERVICES AHORA SON DXC TECHNOLOGY.

DXC.technology/GetItDone

DXC.technology | THRIVE ON CHANGE.

“El éxito de Netskope es una plataforma capaz de supervisar todas las aplicaciones cloud y cumplir con directivas como la GDPR”

Sanjay Beri, CEO y fundador de Netskope

En su visita a Madrid el 19 de septiembre, Sanjai Bery, CEO y fundador de Netskope, se acercó a las oficinas de IT Digital Media Group para hablar con IT Digital Security sobre cuál es la mejor manera de ofrecer seguridad y visibilidad de los servicios cloud en tiempo real, garantizando el cumplimiento de normativas y previniendo la pérdida de datos.

“Habilitar el cloud de una manera segura”, ese es el gran reto de la seguridad Cloud, dentro de la cual empieza a despegar CASB (Cloud Access Technology Broker), un mercado en el que Netskope es experto. El reto, continúa Sanjay Beri, CEO y fundador de Netskope, “es cómo decir sí a mis unidades de negocio, pero con garantías”. Y el gran reto técnico es tener el producto de seguridad adecuado para trabajar con la nube de una manera segura.

La clave de todo está en el CASB, una tecnología que responde al incesante uso de aplicaciones basadas en cloud y la necesidad de controlar la pérdida de datos, la monitorización en tiempo real y el cumplimiento normativo.

A su paso por Madrid, Sanjay Beri nos explica que las empresas utilizan centenares de aplicaciones basadas en cloud; “una media de 700, según un informe que hicimos hace un par de años”, especifica el directivo. Para Sanjay Beri

NETSKOPE DEMO

CLICAR PARA VER EL VÍDEO

"Cuando un departamento de TI no tiene bajo control las aplicaciones que se utilizan en sus empresas, también pierde el control sobre los datos"

está claro que “no se puede detener el avance de las aplicaciones cloud”, que “el cloud es bueno para para las empresas”, pero que, al mismo tiempo, “la seguridad cloud es un reto”, porque cuando un departamento de TI no tiene bajo control las aplicaciones que se utilizan en sus empresas, también pierde el control sobre los datos. Se dan cuenta, dice el CEO de Netskope, que sus datos están en una aplicación de la que no saben nada, ni siquiera quién está accediendo a ella.

¿Por qué se necesita una solución de Cloud Access Security Broker? Sencillamente porque el firewall se queda corto, incapaz de proporcionar la visibilidad granular que se necesite para saber qué aplicaciones se están utilizando, quién está accediendo a ellas, desde dónde y, sobre todo, si el uso de los datos en esas aplicaciones está conforme a las regulaciones.

En términos generales CASB ofrece visibilidad sobre el uso de las aplicaciones basadas en la nube, ayudando a proteger los datos corporativos de las ciberamenazas gracias a controles granulares y una mayor detección. Con CASB se acaba el Shadow IT y además se puede detectar actividad anómala y establecer políticas y controles. Por lo pronto el mercado promete: 7.510 millones de dólares para 2020, con un crecimiento medio anual del 17,6% hasta la fecha, según datos de MarketsandMarkets.

Una nueva era

Desde el punto de vista de una empresa, Internet ha cambiado mucho, asegura Sanjay Beri. No sólo se trata de que se accede desde casa, o a través de dispositivos móviles, “es que el lenguaje de Internet ha cambiado. Está basado en APIs (Application Programming Interfaces)”. Y por eso “si el lenguaje sobre el que las aplicaciones está basado cambia, si hablas en un idioma nuevo, alguien no te entenderá”. Explica el directivo que si tratas de saber lo que la gente está haciendo y gestionando la seguridad con unos dispositivos desarrollados hace diez años… “no se van a entender. Por eso nosotros construimos nuestros productos entendiendo la nueva era de Internet”.

Ya no se trata de asustar a la gente, de demostrarles que no tienen control sobre cientos de aplicaciones, sino de habilitarles a que puedan permitir el uso de esas aplicaciones en lugar de hacer esperar a los usuarios y generar el llamado Shadow IT. Esta es, según Sanjay Beri, la clave del éxito de Netskope: haber creado una plataforma capaz de supervisar todas las aplicaciones basadas en la nube que utiliza una empresa y que además “tiene la capacidad de detener el malware, el ransomware, de cumplir con la GDPR, que te habilita para utilizar dispositivos personales y acceder con ellos, de forma que finalmente puedas decir: Si”.

La plataforma de Netskope

Explica Sanjay Beri que la plataforma de seguridad pone en manos de los responsables de TI toda la información sobre el uso de la nube que se está haciendo en su empresa ya sea de manera remota o a través de un dispositivo móvil. De esta forma

"Cuando alguien dice que está adoptando Office 365 no está solo adoptando una aplicación, sino todo un ecosistema"

"se pueden comprender las actividades arriesgadas, proteger los datos confidenciales, detener las amenazas en línea y responder a los incidentes de una manera que se ajusta a la forma actual en que las personas trabajan".

Netskope es capaz de detectar todas las aplicaciones cloud que se están utilizando en una empresa, hayan sido, o no, permitidas por la empresa. La plataforma no sólo muestra qué aplicaciones cloud se utilizan más, sino, sobre cada aplicación, qué usuarios la están utilizando y desde dónde, estableciéndose además una puntuación de riesgo asociado a cada una. Además, al haber inventariado e inspeccionado cientos de archivos, la plataforma es capaz de informar sobre los datos que se están compartiendo o utilizando en cada aplicación, ofreciendo al administrador una visión clara de las posibles violaciones de políticas de seguridad gracias a Netskpope DLP.

Se trata, en definitiva, de poner fin al Shadow IT y de entender el uso que de cada aplicación hacen los empleados, estableciendo una infraestructura segura, independientemente de si se accede desde un dispositivo móvil, repite el CEO De Netskope.

Le preguntamos a Sanjay Beri de manera específica por Office 365, que ha sido una de las aplicaciones que ha impulsado el uso del cloud en las empresas. Para el directivo "es una de las muchas aplicaciones que la gente utiliza", pero lo que añade no deja de ser interesante: "de media, las empresas conectan 25 aplicaciones SaaS a Office". No se trata de aplicaciones de Microsoft, sino de terceros, como DocuSign o Box, pero el hecho es que "cuando alguien dice que está adoptando Office 365 no está sólo adoptando una aplicación, sino todo un ecosistema, y eso es muy importante porque cuando escoges una plataforma desde el punto de vista de seguridad no puede escogerse una plataforma que esté centrada sólo en Microsoft Office 365, porque vas a tener muchas aplicaciones asociadas, y necesitas una manera consistente de gestionarlas".

En todo caso, y a pesar de que Office 365 es parte importante del negocio de Netskope, "nuestro foco es cubrir todas las aplicaciones cloud con una sola plataforma enfocada a hacer fácil su configuración y gestión de las mismas".

Netskcope en España

"Estamos muy enfocados en grandes empresas y contamos con un responsable local de ventas, ingeniería de sistemas, servicios profesionales y soporte de clientes en España", asegura el directivo cuando le preguntamos por la situación de Netskope en España.

Y como España es uno de los países en los que la GDPR será de obligado cumplimiento a partir

Enlaces de interés...

- 15 Casos de uso crítico de CASB
- Tecnologías de seguridad Cloud listas para su adopción
- Market Guide for CASB

"Las mayores compañías del mundo en cada vertical son clientes de Netskope, y ahora apuntamos hacia el midmarket"

del 25 de mayo de 2018, aprovecha Sanjay Beri para decir que la plataforma de Netskope "incorpora todos los diferentes mandamientos reguladores con los que tengan que trabajar las empresas".

En España la compañía tiene un modelo de canal basado en integradores de sistemas como Telefónica o GMV, además de trabajar con Exclusive Networks.

Y las empresas españolas, ¿están adoptando soluciones de CASB? Sí, responde el CEO de Netskope, añadiendo que hace dos o tres años "la historia era muy diferente, pero que las cosas han cambiado". Explica Sanjay Beri que en este tiempo, los clientes han adoptado aplicaciones SaaS, no sólo Office, sino Salesforce, ServiceNow, y otras, y se dan cuenta de que hay miles de aplicaciones, que tienen que enfrentarse al Shadow IT, "y buscan una solución que les ayuda a gestionar todo ese problema"; "sobre todo porque una de las cosas que la GDPR va a exigirte es que sepas dónde están tus datos, los datos de tu negocio, los datos de tus clientes".

Sobre el IoT en relación con su negocio, dice el responsable de Netskope que "es sólo otro caso de uso para la nube", porque en realidad la compañía no va a construir un software para el IoT.

Para terminar Sanjay Beri resume "lo que debes saber de Netskope". En primer lugar, que no están pensando en ser absorbidos por otras empresas, que "cuando creamos la compañía lo hicimos pensando en ser autónomos y ser una 'iconic security company'", y que por tanto "estamos muy centrados en construir nuestra compañía". En segundo lugar, que "las mayores compañías del mundo en cada vertical son clientes de Netskope" y que la compañía apunta ahora hacia el midmarket. Y, en tercer lugar, que "nuestra visión es muy amplia", cubriendo no sólo Office, sino cientos de aplicaciones. "Nadie en el mercado tiene estas tres cosas", finaliza Sanjay Beri, CEO y co-fundador de Netskope.

ENJOY SAFER TECHNOLOGY™

Adapta tu empresa a la nueva normativa de protección de datos

ENDPOINT ENCRYPTION

DESCARGA GUÍA GRATUITA GDPR

http://gdpr.eset.es

Por qué IoT no es seguro

En la variedad está el gusto, aunque cuando se trata de proteger el Internet de las Cosas (IoT), habría que hablar de reto. Demasiada heterogeneidad, en los dispositivos, redes, protocolos métodos de autenticación o plataformas en la nube. El IoT, además, llega como un tsunami, con una implementación masiva que dificulta la seguridad por defecto. El resultado es un entorno donde hay millones de productos conectados en todo el mundo con bajos niveles de seguridad.

Algo importante ocurrió en 2008: el número de cosas conectadas a Internet superó la población mundial. La ratio de adopción del IoT es cinco veces más rápido que la adopción de la electricidad o la telefonía, lo que supone unos seis dispositivos conectados por cada persona que habita la Tierra. Hablamos del Internet de las Cosas, o lo que es lo mismo, decenas de miles de millones de dispositivos con sensores y capacidad de actuación, conectados entre sí y con Internet. En el mismo saco del IoT entra una pulsera de fitnes o un smartwatch, un dispositivo que controle el sistema eléctrico de un hogar o con capacidad para controlar una fábrica, un automóvil o una máquina de salud. En realidad, el mismo sensor se utiliza en todos los entornos y la seguridad no es una gran prioridad para estos dispositivos.

Cientos de miles de dispositivos de IoT se han utilizado recientemente para lanzas una de las

DIRECTRICES DE SEGURIDAD PARA EL IOT DE LA GSMA **CLICAR PARA VER EL VÍDEO**

campañas de Denegación de Servicio Distribuido (DDoS) más grandes de la historia, con un volumen de tráfico que superara el terabyte por segundo en algunos casos. La realidad es que el número de ciberataques contra dispositivos IoT vulnerables está creciendo rápidamente.

Tanto los sistemas pertenecientes a ese universo de dispositivos conectados como otros sistemas embebidos suelen fabricarse sin los mismos estándares y el mismo nivel de compromiso con la seguridad. A menudo no contemplan una forma segura de conexión remota para su gestión y actualizaciones y en algunos casos ni siquiera existe la posibilidad de ser gestionados y actualizados de forma remota. ¿Por qué? La respuesta más fácil tiene que ver con el propio coste de los dispositivos IoT. Se pueden encontrar enchufes inteligentes por 25 euros corriendo sobre un kernel de Linux, un sistema operativo completo y un sistema de archivos. Con ese precio, el margen de beneficio en un enchufe inteligente es pequeño, a lo que se suma los gastos de desarrollo inicial. Esto genera presión para mantener los costes controlados y dejar el tema de la seguridad en un segundo plano.

Todas las industrias se ven afectadas desde el momento en que, más a menudo de lo que parece, los departamentos de TI no tienen visibilidad sobre estos sistemas no tradicionales que están conectados a la red corporativa. Y de la misma manera en que se habla de Shadow IT, el Shadow IoT es un término que se utiliza cada vez más, y que no dejaremos de escuchar durante los próximos años.

Falta de concienciación

Según Gartner, aunque en 2020 más del 25% de los ataques a empresas estarán relacionados con el IoT, éstas asignarán menos del 10% de sus presupuestos de seguridad al IoT.

Por lo tanto, habría que plantearse si el mercado, las empresas, ¿están concienciadas para aplicar la seguridad al IoT? Para Eutimio Fernández, director de ciberseguridad de Cisco España, “están concienciadas, pero no preparadas”. Añade el directivo que el modelo de seguridad de red actual fue diseñado para conectar ordenadores de propósito general, y no miles de millones de dispositivos de propósito específico, y que la situación se complica aún más si no hay una verdadera integración de la arquitectura de seguridad entre las IT (Information Technologies) y las OT (Operation Technologies).

Para Pedro Pablo Pérez, CEO de ElevenPaths, la falta de seguridad del IoT “debe verse como una barrera, como un inhibidor de la adopción del IoT y, en consecuencia, de la implantación de soluciones

"El apetito que tienen ciertos fabricantes por conseguir un posicionamiento en el mercado, o simplemente por vender, está generando que muchos productos y soluciones de IoT salgan al mercado sin los mínimos controles de seguridad que deberían tener de fábrica"

Rodrigo Chávez, Responsable de IT Security Services & Solutions en Unisys

ENTREVISTA CON EXPERTOS DE SEGURIAD DEL IOT (GSMA)

CLICAR PARA VER EL VÍDEO

que se aproevechen de los enormes beneficios que esta tecnología puede traer". Y es por ello, asegura también el directivo, que la seguridad "es ya una preocupación de primer orden para el negocio y debe formar parte de cualquier solución IoT.

"Lamentablemente, aún queda mucho para que esto suceda", para que el mercado esté concienciado para aplicar seguridad al IoT, dice también Josep Albors, responsable de concienciación de ESET España.

Lo cierto es que los dispositivos conectados han sido tradicionalmente ignorados, o incluso no inventariados. Son endpoints que se han extendido por las redes empresariales, a veces sin controles o segmentación adecuados para evitar que se vean comprometidos o evitar que se utilicen en ataques contra otros sistemas corporativos. Se suma el he-

Un Jeep en manos de unos hackers

Es habitual que cuando se habla del Internet de las Cosas pensemos en sensores de tipo industrial o para el hogar, pero lo cierto es que el coche conectado lo es gracias al IoT. La principal característica de estos automóviles es que están conectados a Internet y desde ese momento son accesibles a los ciberdelincuentes.

Han pasado ya dos años desde que Charlie Miller, director de investigación en Twitter, y Chris Valasek, responsable de Vehicle Security Research en IOActive, fueron capaces de hackear el sistema de entretenimiento de un Jeep Cherokee. Aprovechando una vulnerabilidad en Uconnect, el software que permite a los vehículos de Chrysler conectartse a Internet, además de controlar el sistema de entretenimiento y funciones de navegación, los investigadores pudieron acceder a las funciones más críticas del coche y controlarlo de manera remota.

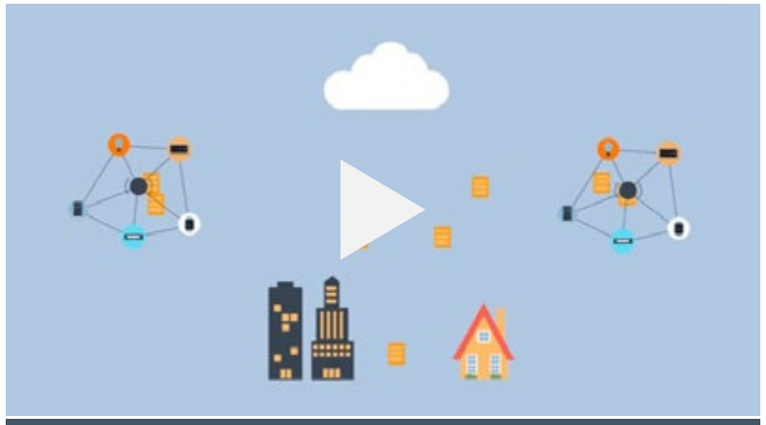
Mientras el coche circulaba a 112km/hora, el conductor pudo sentir cómo el aire acondicionado se ponía a funcionar a máxima potencia, ver fotos en la pantalla de control, escuchar música a todo volumen y activarse los limpiaparabrisas. Todo ello de repente y sin que el conductor tuviera control alguno sobre ello. Finalmente, el motor se apagó de repente.

Al mando del volante el periodista Andy Greenberg, que narró su experiencia en Wired. Estaba avisado, sabía que iba a pasar: "Recuerda Andy, pase lo que pase, no entres en pánico", fue el consejo que le dieron los dos investigadores que, a 16 kilómetros y sentados en un sofá con dos ordenadores, jugaban con el coche. El impacto para Chrysler fue tener que retirar 1,4 millones de vehículos.

Quizá el del Jeep ha sido el más conocido, pero desde luego no ha sido el último. Dieter Spaar, experto de seguridad alemán, descubrió vulnerabilidades en BMW ConnectedDrive, que permite a un hacker abrir el coche de forma remota, además de hacer un seguimiento de la localización y velocidad del vehículo en tiempo real o leer los emails enviados y recibidos a través de BMW Online.

La vulnerabilidad ya fue solucionada, pero es cuestión de tiempo que se detecte alguna más.

La seguridad del IoT se vuelve de vital importancia en determinados escenarios, y los coches conectados son uno de ellos, sobre todo con los enormes avances que se están consiguiendo en torno a los coches autónomos.



"Se han utilizado dispositivos del IoT para realizar ataques de denegación de servicio, minar criptomonedas o robar información confidencial, por poner solo tres ejemplos"

Josep Albors, responsable de concienciación de ESET España

cho de que, además, el ciclo de vida para reemplazar estos sistemas puede ser mucho más largo que con los sistemas informáticos tradicionales.

Está claro que las empresas, la industria en general, se enfrenta a una serie de retos a la hora de integrar la seguridad en el ecosistema del Internet de las Cosas. Para Eutimio Fernández existen dos retos principales; "en primer lugar, la mayoría de los dispositivos IoT no pueden protegerse a sí mismos, creando una gran oportunidad para que los atacantes exploten las vulnerabilidades y obtengan acceso a la red corporativa. El segundo reto es la implementación a escala o masiva, ya que las organizaciones conectarán cientos de miles de dispositivos en los próximos años".

Rodrigo Chávez Rivas, responsable de IT Security Services & Solutions de Unisys, habla del "apetito" de ciertos fabricantes por conseguir un posicionamiento en el mercado, como algo que impacta negativamente en la seguridad del IoT. "Si describimos los desafíos considerando el proceso que hay desde la fabricación hasta llegar al consumidor final, probablemente el primer reto sea conseguir que todos fabricantes de IoT prioricen la seguridad antes que el 'Time to market'", dice Chávez. El resultado es que muchos productos y soluciones llegan al mercado sin los mínimos controles de seguridad

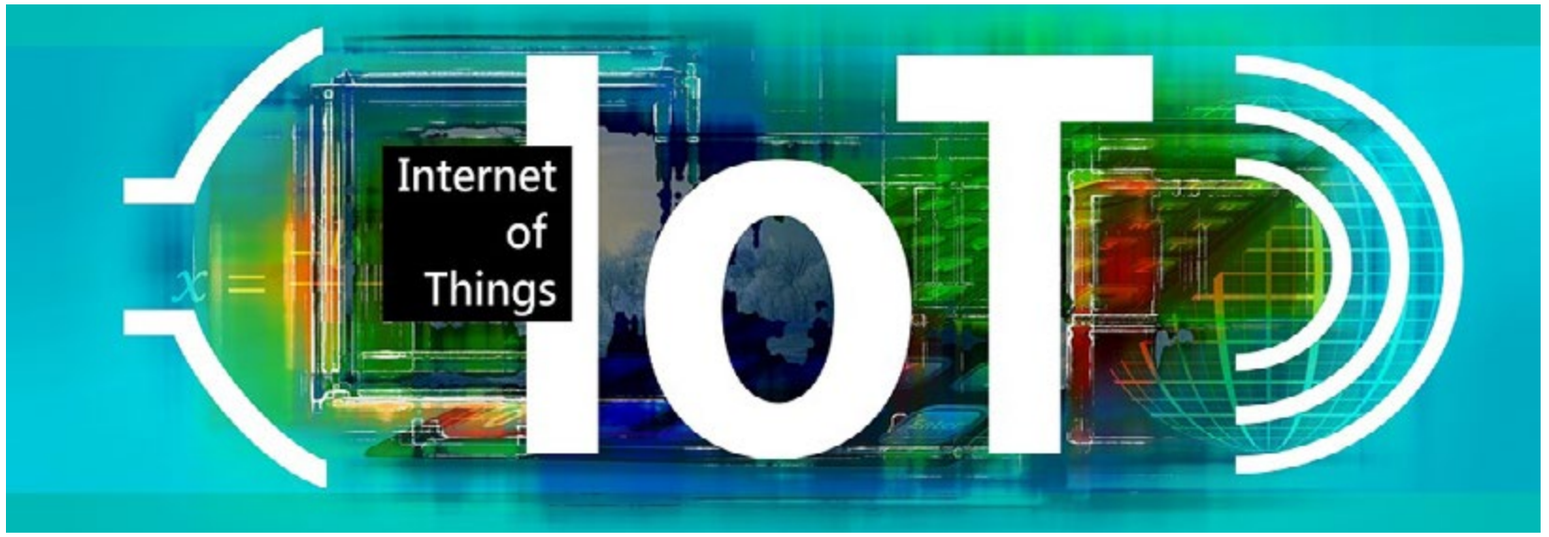
Josep Albors añade que la rapidez con la que se mueve el mercado y con la se añaden nuevas funcionalidades hace que muchos fabricantes se centren en nuevas versiones de productos sin preocuparse por ofrecer soporte de los modelos antiguos, que se quedan obsoletos.

Al preguntarse sobre los retos a la hora de integrar seguridad en el Internet de las Cosas, Pedro Pablo Pérez, CEO de ElevenPaths, enumera algunos retos que afectan principalmente a los dispositivos. Uno de ellos es la heterogeneidad de redes, dispositivos, protocolos, métodos de autenticación y plataformas en la nube; una heterogeneidad que impiden que las soluciones de seguridad puedan generalizarse. Hace referencia también Pablo Pérez a la gestión de la identidad y el acceso de los propios dispositivos, así como de los vínculos con sus propietarios y otros dispositivos, y finaliza hablando de la forma de operar los propios dispositivos, "incluyendo la gestión remota y la actualización del software y su monitorización continua para la detección de incidentes", como retos que dificultan aplicar seguridad el IoT.

Todos estos retos se acrecientan "cuando los dispositivos IoT son además implementados para controlar infraestructuras, como operaciones de fábrica y cadenas de suministro", dice Ricardo Lizarralde, Director Southern Europe Middle East and Africa, AT&T. "A fin de velar por que la integración y aplicación de la seguridad de IoT sea lo más fluida posible, las organizaciones necesitan inyectar los requerimientos y consideraciones de seguridad desde la fase inicial del proceso, para que los dis-

"El mercado está concienciado para aplicar seguridad al IoT, pero no está preparado. El modelo de seguridad de red actual fue diseñado para conectar ordenadores de propósito general, y no miles de millones de dispositivos de propósito específico"

Eutimio Fernández, director de ciberseguridad en Cisco España



positivos IoT sean diseñados con una arquitectura segura por defecto", dice Lizarralde.

En todo caso, los dispositivos de IoT necesitan dos acciones críticas por parte de us administradores para incrementar su seguridad, dice Rodrigo Chávez. Por un lado, una adecuada configuración inicial, que implica un cambio de calves de fábrica, y un adecuado mantenimiento, como es la actualización de parches de seguridad. "Finalmente, y ya en el lado del consumidor final, el reto probablemente consista en proteger cualquier dato tratado en los dispositivos de IoT y cualquier infraestructura conectada al dispositivo IoT", añade el directivo.

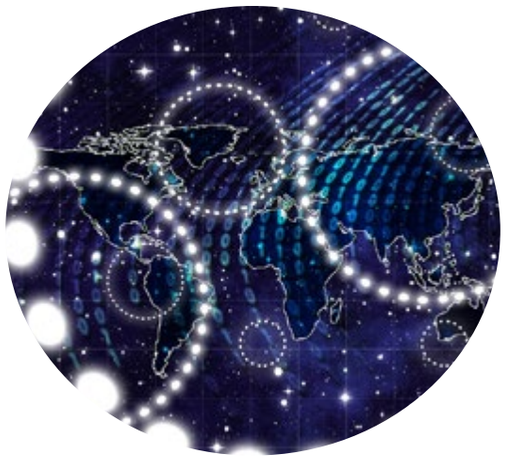
Tecnologías para securizar el IoT

Ni se va a conseguir de la noche a la mañana, ni será una tecnología única la que garantice la seguridad del IoT. Forrester elaboró en el primer trimestre de este año un documento en el que enumera lo que en su opinión son las tecnologías más importantes para proteger el IoT, para securizar el ecosistema de dispositivos conectados.

Proteger la red y los sistemas backend del IoT es una manera de empezar. Explican los expertos que proteger una red de dispositivos conectados es algo más complicado que proteger una red tradicional porque hay más protocolos de comunicación, más estándares y tipos de dispositivos, lo que plantea una mayor complejidad. Se propone asegurar el endpoint mediante soluciones antivirus y antimalware, así como firewalls y sistemas de prevención y detección de intrusiones.

La autenticación puede convertirse en un elemento imprescindible. Proporcionar a los usuarios la capacidad de autenticar un dispositivo IoT, incluso la gestión de varios usuarios para un mismo dispositivo a través de una contraseña o, mejor aún, mecanismos de autenticación de doble factor o incluso biometría. La tarea no es baladí si se tiene en cuenta que la mayoría de los escenarios del IoT contemplan comu-

De las Botnets a los Thingbots



Las Botnets son redes de ordenadores infectados que se utilizan para fines maliciosos. A veces sólo para enviar spam, otras para lanzar ataques de denegación de servicio distribuido, o DDoS, contra determinados objetivos. Actualmente las botnets con capacidades DDoS son un negocio que está disponible en la Darkweb.

Debido a su ubicuidad y al hecho de que normalmente están conectadas directamente a Internet, los routers y módems inalámbricos son uno de los principales objetivos de las thingbots, junto con las cámaras de red. La mayoría de estos dispositivos utilizan Linux como su sistema operativo, lo que permite a los atacantes utilizan un malware diseñado para este sistema operativo y compilarlo para dirigirlo contra arquitecturas específicas en las quer el dispositivo se esté ejecutando.

Lo que ha cambiado en los últimos tiempos en el Internet de las Cosas, el uso de esos miles de millones de dispositivos conectados para crear redes de Thingbots capaces de participar en un ataque DDoS. Es lo que el IBM X-Force ha definido como The Weaponization of IoT Devices en un informe.

Entre los ejemplos más alarmantes, la botnet Mirai. Capaz de infectar cientos de miles de dispositivos de IoT, especialmente cámaras de seguridad, utilizando las contraseñas por defecto para el acceso a Telnet, Mirai se ha convertido en uno de los mayores ejemplos de lo que está por llegar.

Mirai es un tipo de malware que detecta de manera automática dispositivos de IoT para infectarlos e incorporarlos a la red. En solo dos semanas la Thingbot fue capaz de interrumpir el servicio de más de 900.000 clientes de Deutsche Telekom en Alemania o infectar casi 2.500 routers en Reino Unido. En poco tiempo se hizo público que más de 80 modelos de cámaras Sony eran vulnerables a Mirai.

Entre las ventajas de Mirai es que ha probado ser extremadamente flexible y adaptable, lo que permite a los ciberdelincuentes desarrollar variantes capaces de atentar contra otras clases de dispositivos IoT, engrosando la botnet.

En lo que va de año han llegado al mercado 98 millones de cámaras IP, según IHS. Y la mayoría de ellas utilizan nombres y contraseñas por defecto

nicaciones machine to machine, por lo que en este caso el proceso de autenticación debe poder realizarse a través de máquinas mediante algún tipo de certificado digital y sin intervención humana.

El cifrado es otro elemento que puede jugar un papel fundamental en la seguridad del IoT. Cifrar los datos y las comunicaciones entre dispositivos y sistemas de back-end mediante algoritmos estándar ayuda a mantener la integridad de los datos y evitar que los hackers detecten los datos.

Mencionábamos antes la posibilidad de utilizar certificados digitales. Aunque las especificaciones de hardware de algunos dispositivos del IoT pueden limitar o impedir el uso de PKI, los certificados digitales podrán cargarse de forma segura en el momento de fabricación del dispositivo para después habilitarse o activarse mediante PKI de terceros. Como es lógico también sería posible instalar los certificados después de la fabricación.

La analítica de conducta podría llegar también al IoT de forma que monitorizando las actividades se detecten las sospechosas. Este tipo de soluciones, que incorporan tecnologías de machine learning, big data e inteligencia artificial permiten detectar anomalías pero son muy nuevas. Por el momento quizá deberíamos conformarnos con que la capacidad de análisis del IoT se limite a poder detectar ataques o intrusiones específicas que soluciones de red tradicionales como los firewalls no pudieran identificar.

La seguridad de las API será esencial para proteger la integridad de los datos que se mueven entre los dispositivos del borde de la red y los sistemas de back-end para asegurar que sólo los dispositivos, desarrolladores y aplicaciones autorizados se comunican con las APIs. De forma que otra de las medidas propuestas de Forrester para asegurar el internet de las cosas habla de proporcionar la capacidad de autenticar y autorizar el movimiento de datos entre dispositivos IoT, sistemas back-end y aplicaciones que utilizan APIs basadas en REST documentadas.

RIESGOS DE IOT EN LAS EMPRESAS

La proliferación y ubicuidad de los dispositivos IoT en las empresas está generando una mayor superficie de ataque y sencillos puntos de entrada que permiten a los hackers acceder a la red. Este estudio de ForeScout se ha centrado en siete dispositivos conectados a Internet comunes en las empresas y ha detectado lo fácil que es atacarlos, además de lo complicado que es implementar seguridad en ellos por sus propias tecnologías, métodos de desarrollo y producción.

IoT, la nueva arma de los ciberdelincuentes

Las posibilidades que el IoT ofrece a los delincuentes "son bastante amplias y llevamos años viendo ejemplos", dice Josep Albors, quien recuerda que ya se han utilizado dispositivos del IoT para realizar ataques de denegación de servicio, minar criptomonedas o robar información confidencial, por poner solo tres ejemplos. "El problema es que el futuro no pinta nada esperanzador si no hacemos algo al respecto", asegura.

Ricardo Lizarralde, de AT&T, recuerda que casa vez es más difícil detectar amenazas y que "los cibercriminales están desarrollando continuamente nuevas formas de abrir brechas en los sistemas de datos". La innovación camina del lado de los ciberdelincuentes; "utilizar 100,000 dispositivos IoT para lanzar un ataque DDoS ya no es sólo una teoría; esta es la última prueba de que la innovación en el cybercrimen está prosperando", recuerda.

Precisamente Eutimio Fernández habla de ataques de denegación de servicios (DDoS) que utilizan botnets de objetos conectados para colapsar servidores con tráfico procedente de múltiples fuentes como uno de los usos que los ciberdelincuentes harán del Internet de las cosas. El gran desafío, dice el responsable del negocio de seguridad de Cisco, es que "esos ataques pueden detener servicios básicos como el suministro de electricidad, gas o agua. Y es que el tamaño medio de los ataques DDoS se ha incrementado un 22% hasta los 1,2 Gbps, suficiente para dejar completamente 'offline' a la mayoría de organizaciones; e incluso provocar un ataque de enormes dimensiones o derivar en ataques de destrucción de servicio (DeOS, Destruction of Service), capaces de eliminar las redes seguras y de backup que utilizan las organizaciones para restaurar sus sistemas y datos tras un incidente de ciber-seguridad".

Para Chávez el IoT se está convirtiendo en un "interesante objetivo de ataque". Ser un entorno relativamente nuevo donde existe un enorme volumen de dispositivos pobremente configurados y peor mantenidos es una gran oportunidad para, en

"La diversidad de dispositivos personales, de fabricantes y su falta de estandarización en cuestiones de seguridad, hacen que muchos de ellos vengan de fábrica con vulnerabilidades fácilmente explotables"

Pedro Pablo Pérez, CEO de ElevenPaths

Proteger el dato, no el dispositivo

IoT por Internet of Things, pero también por Internet of Troubles o Internet of Threats. Es una chanza habitual en el sector. Se dice con convicción. Y es que la adopción masiva y acelerada del IoT no deja tiempo para casi nada y la seguridad, como casi siempre, queda por detrás de la operatividad.

La seguridad del IoT es un reto enorme. Hay propuestas que combinan segmentación, inteligencia de amenazas, automatización, filtrado de tráfico, pentesting persistente, control de accesos... y un sinfín de tecnologías para hacer frente a una amenaza.

Ante la variedad de dispositivos, hay quienes prefieren proteger el dato. No es un tema baladí. Según un informe de Cisco los miles de millones de dispositivos que formarán parte del Internet de las Cosas generan miles de billones de datos para 2018; cerca de 400 zettabyttes al año. Y esos datos deben protegerse. Asegurarlos pasas por identificarlos, autenticarlos y cifrarlos, de forma que se conviertan en datos íntegros y confidenciales.

Identificación y autenticación van de la mano. Su objetivo es asegurar que la información se está comunicando al dispositivo correcto y que la fuente es de confianza. Si no se hiciera uso de la autenticación un hacker podría comunicarse directamente con un sistema de alarma para desactivarlo o desbloquear una puerta y acceder a una casa.

La autenticación e identificación son, por tanto, necesarias, pero además de estar seguros de que nos conectamos con el dispositivo adecuado, conviene evitar escuchas, saber que no hay nadie espiando esas comunicaciones entre dispositivos o incluso pueda manipular esas conversaciones. Por eso el cifrado es la otra capa de protección importante para el IoT. Algoritmos de cifrado como AES pueden hacer que el dato sea inútil para los ciberdelincuentes

Pero el cifrado también debe aplicarse cuando el dato está en reposo. Y esto significa que los datos no sean modificados, y que no puedan ser leídos o entendidos por nadie sin las claves adecuadas.

primer lugar, acceder a datos fáciles de monetizar, y en segundo y mucho más peligroso, acceder a infraestructuras críticas.

Pablo Pérez, de ElevenPaths, dice que se puede clasificar los ataques al IoT en función del objetivo que persiguen, bien sea utilizar los dispositivos conectados como medio para atacar otro objetivo, o atacar al IoT en sí mismo. “Los ataques del segundo tipo seguramente serán menos frecuentes, pues es de esperar que se hayan concebido con la seguridad como propiedad fundamental, pero su impacto puede ser mayor, ya que uno de los objetivos puede ser las infraestructuras críticas de un país”, dice el ejecutivo.

Un perfecto caso de lo que los ciberdelincuentes pueden hacer con el IoT es Mirai, la botnet que el pasado otoño hackeo millones de cámaras para crear un ataque de DDoS. Lo que hizo único aquel ataque, que marcó un antes y un después, es la capacidad del gusano de extenderse rápidamente entre dispositivos conectados que se han desplegado sin ningún tipo de seguridad.

Pero Mirai fue sólo un ejemplo al que siguieron los ataques de Haijme y Devil Ivi, que no sólo utilizaban el mismo tipo de mecanismo para atacar dispositivos del IoT, sino que añadía herramientas que les permitían identificar diferentes dispositivos, seleccionar las contraseñas conocidas y explotar las vulnerabilidades adecuadas, comprometer el dispositivo y después utilizar su protocolo de comunicación para extender la infección a otros dispositivos.

Recomendaciones básicas de seguridad

Está claro que Interconectar dispositivos IoT y redes que utilizan diferentes grupos de especificaciones no solo genera ineficiencias, sino que incrementa los puntos en los que las vulnerabilidades de seguridad pueden existir. También ha quedado claro que en lo que respecta a la seguridad, el Internet de las cosas tiene mucho que evolucionar.

A veces nada más fácil que aplicar las mismas recomendaciones que para otros dispositivos. Ese parece ser el caso de Ricardo Lizarralde, de AT&T,

que habla de una necesaria actualización del software/firmware de los dispositivos conectados, seguido de contar con una formad e restablecer su estado original o no utilizar contraseñas predeterminadas. Además, “un dispositivo no debería ofrecer ningún servicio a la red que no sea necesario para soportar sus funciones principales; no debe tener puntos de entrada ocultos o conocidos que puedan ser atacados por el fabricante u otros y los fabricantes deberían proporcionar acceso online a los manuales de los operadores, así como acceso a las instrucciones de actualización. La información de soporte debería incluir una explicación clara de su mantenimiento a lo largo del ciclo de vida del producto”.

“Establecer la seguridad desde el diseño y concretar una normativa que obligue a los fabricantes a cumplir unas condiciones mínimas. Luego se tendrá que concienciar y educar a los usuarios para que hagan uso de esas características de seguridad incluidas y se preocupen de actualizar los dispositivos”, dice Josep Albors, de Eset.

Parecida es la opinión de Rodrigo Chávez, que apuesta por: Comprar dispositivos IoT que cumplan de fábrica con los requisitos de seguridad recomendados para el escenario al que vayan a estar expuestos; realizar configuraciones de seguridad adecuadas (cambio de contraseñas de fábrica como mínimo) y tomar las acciones recomendadas por los fabricantes; y restringir el acceso a los dispositivos IoT sólo a quienes sea estrictamente necesario, como las principales recomendaciones de seguridad.

"Utilizar 100,000 dispositivos IoT para lanzar un ataque DDoS ya no es solo una teoría; esta es la última prueba de que la innovación en el cibercrimen está prosperando"

Ricardo Lizarralde, Director Southern Europe Middle East and Africa, AT&T

La propuesta de Cisco es también muy clara. Para Eutimio Fernández, nada mejor que segmentar el tráfico IoT y el tráfico habitual de la red de TI; adoptar una arquitectura de seguridad integrada, que abarque las IT, OT y la nube, capaz de establecer políticas de seguridad una vez e implementarlas en múltiples ámbitos; automatizar. Nadie podrá gestionar los miles de dispositivos conectados a la red corporativa de forma manual, salvo con herramientas automatizadas (con funcionalidades de autoprotección y auto-reparación), inteligentes (basadas en políticas) y escalables; mantener actualizados los sistemas, implementar firewalls y sistemas IDS/IPS y aplicar ciber-inteligencia de extremo a extremo, utilizando la red como sensor para bloquear los ataques y como reforzador de las políticas de defensa; unificar los estándares, insistiendo a los proveedores para que los utilicen; convertir la seguridad en elemento básico de las implementaciones IoT desde el principio; si los dispositivos resultan comprometidos, activar procesos de respuesta frente a incidentes con tolerancia a fallos para proteger el negocio.

Junto con las recomendaciones de seguridad que se deben seguir, hay que tener en cuenta el uso de estándares, que permite no sólo una mejor interrelación entre productos, protocolos, formatos y especificaciones, sino menores riesgos de seguridad.

La primera de las cinco iniciativas más importantes en lo que respecta a estándares del IoT, según AT&T, es oneM2M, un consorcio de cerca de 230 vendedores, asociaciones industriales y agencias gubernamentales que desarrollan especificaciones

Enlaces de interés...

- TechRadar: Internet Of Things Security, Q1 2017
- Estudio 2017 sobre la seguridad de la movilidad y el IoT
- WP. Riesgos de IoT en las empresas
- Seguridad en el Internet de las Cosas

para una capa de middleware distribuido (dispositivo, pasarela, nube) que proporcione gestión de dispositivos y otros servicios comunes a todas las aplicaciones M2M.

Allseen Alliance agrupa a cerca de 185 miembros y promueve el Open Source AllJoyn Framework (inicialmente promovido por Qualcomm y ahora gestionado por la Fundación Linux), cuyo objetivo es permitir a los dispositivos descubrirse y comunicarse entre sí, y dar a los desarrolladores herramientas para crear aplicaciones IoT compatibles.

Open Internet Consortium es un consorcio de cerca de cien vendedores que promueven el IoTivity Project, un marco de código abierto (también alojado por la Fundación Linux) destinado a permitir la conectividad perfecta de dispositivo a dispositivo.

El Industrial Internet Consortium es una organización global de asociaciones público-privadas administrada por el Object Management Group. Cuenta con más de 200 miembros y fue creado para acelerar el desarrollo, adopción y uso generalizado de máquinas y dispositivos interconectados, analítica inteligente y personas en el trabajo.

Por último, la 3rd Generation Partnership Project (3GPP). Se trata de una iniciativa global que une a siete organizaciones de desarrollo de estándares de telecomunicaciones que desarrollan especificaciones que cubren tecnologías de redes celulares, incluyendo estándares de acceso por radio. Lanzado en 1998, el 3GPP se está moviendo ahora para abordar las cuestiones de telecomunicaciones, incluida la seguridad.

netskope

¿Cuántos servicios Cloud está utilizando su compañia?

¿Está seguro?

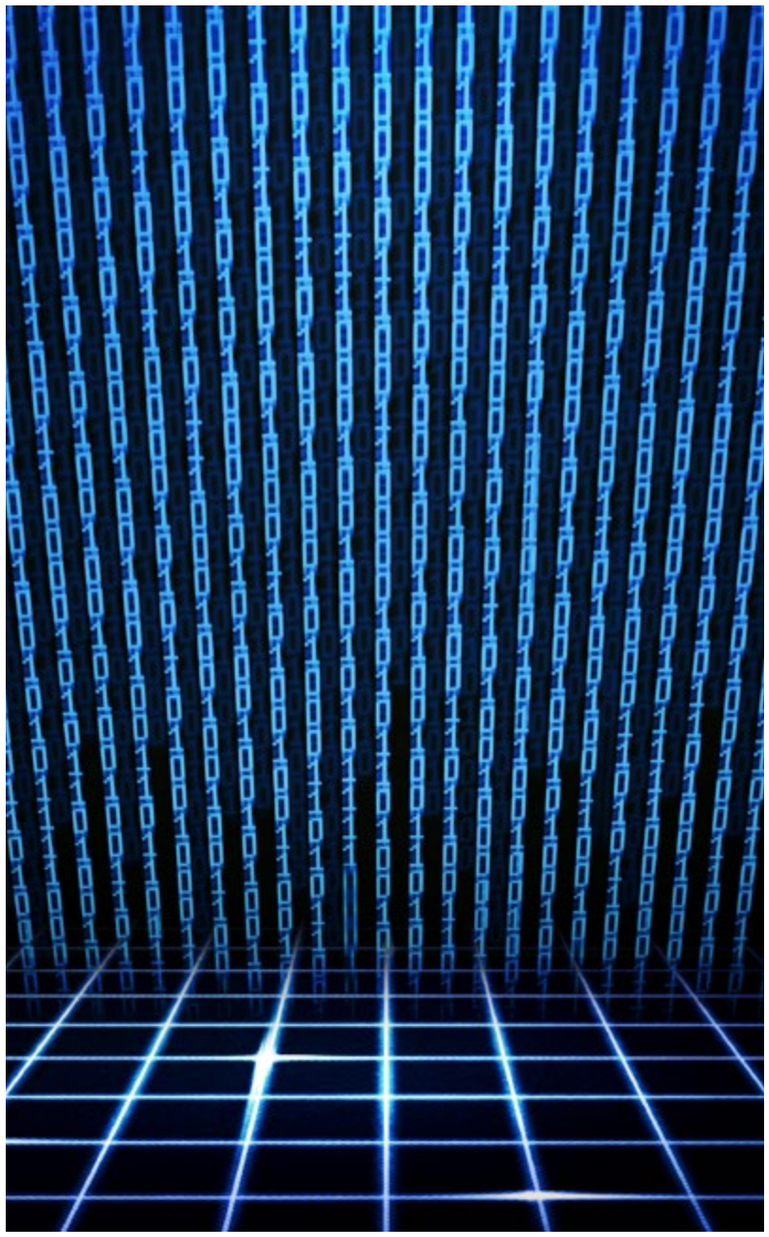
JORGE GIL

Director General de IDC España
Con más de veinte años de experiencia en el sector tecnológico, en los últimos siete Jorge Gil ha desarrollado un papel activo en el área de la transformación empresarial, ayudando y asesorando a compañías de diferentes tamaños, desde grandes corporaciones hasta medianas empresas y startups españolas, formando parte de varios espacios coworking de ayuda a emprendedores.
Jorge es socio fundador de Go2Do, consultora especializada en el asesoramiento y ayuda a la creación de empresas y desarrollo de estrategia de marketing. Anteriormente, ha ocupado los puestos de director general en Panda Security y de consejero y asesor en Afina y Epson respectivamente, además de dirigir el equipo de marketing y desarrollo de negocio a nivel global en Microsoft.

El actual contexto europeo de ciberseguridad

En IDC, estimamos que, para 2019, el 70% de las grandes empresas con sede en EE.UU. y Europa serán objeto de ataques de ciberseguridad. Este es un dato representativo de lo que constituye el actual contexto europeo de ciberseguridad, y consideramos que son tres los principales factores que ayudan a explicarlo:

1) El actual contexto de amenazas
El número de actores del crimen cibernético se está expandiendo y la sofisticación de los ataques que son capaces de lanzar está creciendo. Hoy, con frecuencia, asistimos a casos de Ransomware, y nos damos cuenta de la impresionante profesionalización de los hackers, siendo un ejemplo claro la existencia de marketplaces donde el hacking-as-a-service es un concepto ampliamente practicado que pone en evidencia el desarrollo y la madurez de las organizaciones criminales, que cada vez más comparten y evolucionan amenazas de forma colaborativa, como lo hacen las comunidades Open Source. Agravando esta situación, está el hecho de



El hacking-as-a-service es un concepto ampliamente practicado que pone en evidencia el desarrollo y la madurez de las organizaciones criminales

que esto es un fenómeno global, disperso geográficamente, con lo que se vuelve todavía más difícil de combatir.

Esto tiene un efecto claro: el número de amenazas lanzadas sobre empresas e individuos está creciendo exponencialmente. Tomemos conciencia de que hoy son lanzados más de un millón de tipos de malware por día. WannaCry fue solo uno entre un millón de otros tantos virus. Esto significa que los enfoques tradicionales de seguridad ya no son efectivos para lidiar con esta escala de amenazas, siendo necesario cambiarlos. Será, por tanto, fundamental cambiar la mentalidad de las empresas y pasar de la reacción a la proactividad, asumiendo un papel importante el análisis del comportamiento y del contexto, así como adoptar una mentalidad de gestión del riesgo.

Además, la tecnología cobra aquí un papel fundamental, debiendo las organizaciones apostar por soluciones que les proporcionen capacidades de Automatización de procesos de seguridad, tanto los de prevención, como los de detección y de remediación; Integración: ser capaz de gestionar de forma integrada los distintos entornos de tecnológicos; Visibilidad: ser capaz de conocer el estado de seguridad del entorno tecnológico y ser capaz de identificar los impactos en procesos, servicios y activos de negocio.

2) La Transformación Digital de las empresas: Sabemos que la Transformación Digital es hoy una clave de la estratégia del 92% de empresas en España. En IDC la definimos como el proceso continuo a través del cual las empresas se adaptan a o generan cambios disruptivos en sus clientes y mercados mediante el aprovechamiento de competencias digitales para innovar en nuevos modelos de negocio, productos, y servicios que combinan las experiencias física y digital de sus clientes, mientras mejoran la eficiencia operacional y el desempeño organizacional.

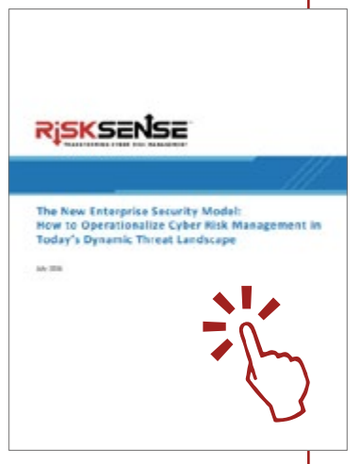
Es importante entender que este momento de transformación digital es motivado por el aparecimiento de empresas nativas digitales, que sabemos sobejamente quien son, y que están provocando una auténtica revolución en los modelos de negocio de las empresas tradicionales a través del uso de tecnología de la Tercera Plataforma. Por ello, para las empresas que se están transformando, entender y explorar la Tercera Plataformas es fundamental. Constituida sobre los pilares de Cloud, Big Data, Movilidad y Social, la Tercera Plataforma es donde hoy el gasto mundial de TI (y el español, por supuesto) está creciendo, lo que evidencia el uso que están haciendo las empresas.

Tenemos que reconocer que cada uno de los pilares de la Tercera Plataforma representa un factor de exposición al riesgo

Sin embargo, tenemos que reconocer que cada uno de los pilares de la Tercera Plataforma representa un factor de exposición al riesgo. Esto nos lo confirman todos los estudios y encuestas que hacemos en IDC: la seguridad es la principal preocupación de las empresas en su viaje de Transformación Digital. ¿Significa esto, entonces, que las empresas están bloqueadas? No. Hemos identificado dos grandes grupos de empresas: las pragmáticas, que ven que en la nube y en otros pilares de la Tercera Plataforma hay formas de seguridad que están alineadas con algunos de sus objetivos de negocio (o bien financieramente, o bien por el aporte de funcionalidades, agilidad y flexibilidad, o por otro beneficio); y las escépticas, que no confían en la nube. Pero, vemos que el escepticismo está cediendo posición al pragmatismo. Con el tiempo, la seguridad dejará de ser una preocupación tan grande como es hoy. No obstante, cabe a los proveedores de soluciones de seguridad proporcionar esa tranquilidad, garantizando, por un lado, la clareza de sus mensajes y demostrando cabalmente, por otro, las capacidades de sus soluciones.

EL NUEVO MODELO DE SEGURIAD EMPRESARIAL

Uno de los mayores retos de la ciberseguridad es cómo gestionar el volumen, la velocidad y la complejidad de los datos generados por las herramientas de seguridad de TI. Cuantas más herramientas, más difícil es el desafío a la hora de analizar los datos y priorizar los esfuerzos hacia la remediación de un ataque. En lugar de agregar más herramientas, las organizaciones necesitan implementar un nuevo modelo de seguridad empresarial más eficiente. Hablamos de la gestión del riesgo que utiliza el análisis basado en inteligencia para ayudar a las organizaciones a gestionar mejor su seguridad, acabar con los silos y mejorar las tareas de seguridad a través de la automatización.



Enlaces de interés...

- Un entorno Seguro: base para la Transformación Digital
- La tribuna de GDPR: Situación Actual
- 10 mitos alrededor de GDPR
- Guías de Inversión de Seguridad de IDC
- Cómo defender mi empresa híbrida de brechas y amenazas

3) GDPR:

Dentro del contexto regulatorio europeo, aunque cada sector posea su regulación específica, GDPR es el reglamento más importante e impactante para las organizaciones. Desde luego, por su urgencia. En 25 de mayo de 2018, el periodo actual de transición acabará y el reglamento será de carácter obligatorio. Sin embargo, en las conversaciones que mantenemos con las empresas, constatamos que hay un desconocimiento significativo sobre lo que representa e implica esta normativa.

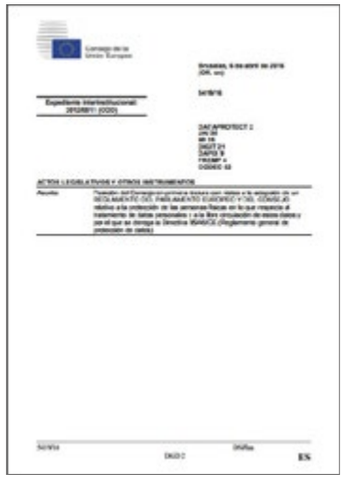
En primer lugar, no es una directiva, sino un reglamento. Una directiva es un acto legislativo global que reserva a cada país miembro la jurisprudencia para definir cómo implementarla. Un reglamento es un acto legislativo vinculante – todos los países tendrán que implementarla de acuerdo con las mismas reglas. En segundo lugar, reemplaza una directiva europea obsoleta, implementada en 1995, anterior a las empresas nativas digitales que han impulsado la creación de la actual economía digital.

Este reglamento destinase a la protección de datos personales (todos los que permitan identificar una persona) de los ciudadanos de la Unión Europea y codifica los derechos que a partir de hoy todas las entidades que procesen datos de ciudadanos de la UE están obligadas a respectar. A título de ejemplo, preconiza para el ciudadano el derecho a acceder a los datos que una entidad posee sobre uno mismo, el derecho al olvido, y el derecho al consentimiento explícito. Representa, por tanto, un aumento de los derechos de los ciudadanos europeos. Además, conlleva para las empresas un conjunto de nuevas obligaciones, como, por ejemplo, la comunicación obligatoria de las brechas de seguridad en 72 horas.

Las consecuencias para las empresas que no estén en conformidad con el reglamento GDPR son severas: podrán ser objeto de multas hasta el 4% de sus ingresos o € 20M, lo que sea más elevado. Podrán también ser prohibidas de procesas datos personales, lo que puede ser sinónimo de prohibición de facturar. Esto significa que la gestión del riesgo en las empresas va a cambiar definitivamente. Podemos, efectivamente, decir que habrá un antes y un después de la GDPR.

Ante este escenario polifacético y complejo, importa referir que el modelo de seguridad empresarial del futuro debe acomodar estos tres factores, esperándose que las empresas apuesten por racionalizar la tecnología y simplificar el propio entorno de seguridad, para que puedan ser más ágiles y efectivas las empresas a la hora de afrontar las amenazas, y por implementar el liderazgo y los modelos organizativos necesarios. En este sentido, la figura del director de seguridad de la información (CISO) se asume como fundamental, pues debe aunar tanto el conocimiento de la seguridad y de la regulación como del negocio, de tal forma que pueda entender los riesgos asociados a las nuevas oportunidades, influyendo en las decisiones que desde la alta dirección se lleven a cabo.

GDPR es el reglamento más importante e impactante para las organizaciones



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 quieres la GDPR original, sin comentarios, aquí la tienes.

Gestión del riesgo y la seguridad a la velocidad del negocio digital

La Transformación Digital está cambiando el paisaje tradicional de gobierno y control de TI. Por un lado, la autoridad del responsable de las Tic se ve a menudo superada a favor de una mayor autonomía en el despliegue de nuevas tecnologías digitales. Por otro, el incremento de nuevos elementos (sistemas, dispositivos e incluso datos) genera problemas de escalabilidad para los que algunas soluciones de seguridad no están preparadas. ¿Cómo hacer frente a esta nueva realidad manteniendo bajo control la gestión del riesgo y la seguridad?

Cómo defender mi empresa híbrida de brechas y amenazas

Para acceder a recursos no autorizados, los hackers apuntan a cuentas de usuario privilegiadas, porque cuantos más privilegios más poder. Sin un control adecuado, un hacker con una sola cuenta privilegiada comprometida puede causar un daño generalizado e irreparable a la infraestructura de una organización, la propiedad intelectual y el valor de marca. En este documento se ofrecen las claves para proporcionar una protección amplia y coherente entre las credenciales y los niveles de acceso.

El nuevo modelo de Seguridad Empresarial

Uno de los mayores retos de la ciberseguridad es cómo gestionar el volumen, la velocidad y la complejidad de los datos generados por las herramientas de seguridad de TI. Cuantas más herramientas, más difícil es el desafío a la hora de analizar los datos y priorizar los esfuerzos hacia la remediación de un ataque. Este documento explora la emergente disciplina de la gestión de riesgos impulsada por la inteligencia como una respuesta a los ciberataques, las amenazas persistentes avanzadas y las fugas de información privilegiada.

La Seguridad TIC a un solo clic

it Digital MEDIA GROUP

it whitepapers

DANIEL LARGACHA

Director del Centro de Ciberseguridad de ISMS Forum
Head of CCG-CERT MAPFRE

Daniel Largacha Lamela es Global Control Center Assistant Director en MAPFRE, puesto en el que confluyen en el plano operativo los ámbitos tradicionales de seguridad física y seguridad de la información. Asímismo Daniel colabora en los subgrupos de Cyber-riesgos del CROF (Chief Risk Officer Forum de entidades aseguradoras europeas) y de transformación digital del EFR (European Financial Services Round Table).

La carrera de Largacha ha estado siempre vinculada a las Tecnologías de Información principalmente en el ámbito de la Seguridad, actividades que ha desarrollado en grandes empresas como Telefónica, Deloitte, y Azertia. Largacha es Ingeniero Superior en Informática por la Universidad Politécnica de Madrid y Máster en Dirección Aseguradora por el ICEA (Investigación Cooperativa de Entidades Aseguradoras y Fondos de Pensiones).

El estado de la ciberseguridad en España

La base del estado del bienestar en la sociedad actual está arraigada en pilares como la sanidad, la educación y la satisfacción de las necesidades básicas, pero además está también ligado necesariamente a algunos aspectos más básicos como el agua corriente, el suministro eléctrico que por lo esencial de su naturaleza (en la sociedad actual) pasan inadvertidas. Con la ciberseguridad, nos ocurre algo parecido, es una cuestión que está intrínsecamente relacionada con la tecnología, aunque a diferencia de lo comentado anteriormente, es completamente intangible y su ausencia puede pasar desapercibida o no apreciada hasta que realmente se hace evidente y necesaria.

Lo cierto es que, gracias a la adopción de la tecnología por parte de los individuos en los años 90

El concepto de seguro no existe y no es algo propio de la tecnología

con la aparición de Internet en los hogares, los ordenadores personales tomaron un nuevo hueco, motivando la primera burbuja tecnológica. En el ámbito de la ciberseguridad, la rápida expansión de la tecnología tuvo efectos negativos, debido a que el objetivo de la entrega primó sobre otros requisitos frente a la ciberseguridad. Algunos fabricantes atendiendo al riesgo potencial en el que nos encontrábamos inmersos, decidieron entonces cambiar sus estrategias de desarrollo de productos limitando su expansión y elevando el peso de los requisitos de ciberseguridad.

En la situación actual, el número de ordenadores ha aumentado geométricamente con la introducción de los smartphones, tablets, dispositivos IoT (que entran dentro de lo que se entiende por un ordenador), hasta el punto de que en los países desarrollados se ha pasado de uno por hogar a más de uno por persona. Esta tendencia ha despertado el interés de todos los sectores, cuestión que podemos ver en la “smartización” de bienes de consumo no vinculados históricamente con la informática, como por ejemplo los electrodomésticos (neveras, lavadoras…), automóviles, etc.

Sin embargo, en el ámbito de la ciberseguridad, aunque también se ha despertado cierto interés, mejorando en términos relativos, el crecimiento no ha seguido la misma proporción, y su evolución no ha ido necesariamente en la misma medida que la tecnología. Para ayudarnos a entender bien el escenario vamos a exponer cuales son los principales factores que influyen sobre este:

- **El concepto de seguro no existe y no es algo propio de la tecnología.** En muchos ámbitos no hablamos de ignífugo o impermeable sino realmente de resistente al fuego o resistente al agua. En la tecnología hay que partir de la base que el software es imperfecto per se, por lo que nunca podemos asegurar con certeza que un sistema es seguro.
- **Mayor exposición:** la aparición y conexión a una red global de miles de millones de nuevos dispositivos cuyo funcionamiento está basado en software (imperfecto) aumenta la posibilidad de éxito que tendría un potencial atacante.
- **La falta de equilibrio que existe en escenarios de proteger versus atacar.** La globalización y la conexión desde cualquier punto del mundo muestra un escenario desigual a la hora definir estrategias o medidas de protección frente a posibles ataques.
- **Aumento de tamaño de la amenaza, debido principalmente a dos factores.** El aumento de los “actores” que destinan sus esfuerzos a atacar y la mayor sofisticación de estos ataques.

A todos estos factores además hay que añadirle el más importante, y es la dependencia actual que tenemos tanto la sociedad en su conjunto, como

DOLPHINATTACK, O LOS FALLOS DE SEGURIDAD DE SIRI, ALEXA O GOOGLE NOW

Se trata de susurrar, de hablar tan bajito que el oído humano no lo detecte, pero sí los micrófonos de los dispositivos móviles. Se trata de hablar por debajo de los 20kHz. Después de esto basta con decir "activar modo avión" para que el usuario quede desconectado de la red; o susurrar la dirección de una página web para acceder a una que pudiera ser maliciosa. Por ahora es un estudio, una prueba de concepto, pero quién sabe.

> La aparición y conexión a una red global de miles de millones de nuevos dispositivos cuyo funcionamiento está basado en software aumenta la posibilidad de éxito que tendría un potencial atacante

las personas de manera individual sobre las tecnologías de información. La tecnología juega hoy un rol crítico en todo lo que hacemos en nuestro día a día, y nadie es ajeno a ello. Desde que nos levantamos y encendemos la luz del dormitorio, hasta que bebemos el último vaso de agua. Tanto gobiernos como empresas son conscientes de la sensibilidad del escenario actual, y desde ambos frentes se trata de mejorar lo máximo posible este escenario, que pasa inexorablemente por sensibilizar a los principales grupos de interés (ciudadanos, accionistas, consumidor, empleados… etc.).

La situación actual requiere el compromiso por todas las partes, gobiernos, empresas y la sociedad. La comprensión y aceptación de la situación es uno de los factores críticos de éxito. El otro es el consenso de los compromisos en seguridad que sean necesarios acometer. Un elemento catalizador que puede favorecer la aparición y persistencia de estos factores críticos de éxito es el papel que juegan las asociaciones como el ISMS, ya que pueden acercar las posturas de éstos, así como facilitar recursos, actividades, o capacidades desde una posición más neutra que facilite el entorno de colaboración.

¿Te avisamos del próximo IT Digital Security?

La rápida expansión de la tecnología tuvo efectos negativos, debido a que el objetivo de la entrega primó sobre otros requisitos frente a la ciberseguridad

Existen tres pilares sobre los que los que se puede cimentar una mejora sostenible del escenario actual:

- **La mejora de la capacidad de las organizaciones: aumentando la capacidad de detección y prevención ante un ataque para una entidad, es un aspecto crítico que puede permitir el bloqueo o minimización del ataque.** Para este punto la colaboración entre entidades en la compartición de información de eventos que puedan ser dañinos posibilita que el resto de entidades puedan estar preparadas ante eventos similares.
Otro factor que afecta directamente a la capacidad de reacción de las organizaciones tiene que ver con los planes de respuesta y gestión de crisis ante incidentes de seguridad. Estas situaciones requieren de la toma de decisión de alto calado, en periodos de tiempo críticas, una buena preparación de estos escenarios minimiza los impactos que pueden tener los incidentes de seguridad en las organizaciones.
- **El fomento de la seguridad: tanto en la sociedad en su conjunto, tanto a individuos como organizaciones empresariales.** La creación de escenarios de colaboración a través de los cuales las organizaciones puedan compartir sus experiencias y necesidades con otras organizaciones, de forma que se optimicen esfuerzos tanto internos como externos, potenciando su capacidad de influencia en la sociedad.
- **La capacitación y especialización de profesionales: enfocados en la seguridad de la tecnología.** Tanto universidades, como entidades privadas deben de facilitar a la sociedad la creación de perfiles con capacidad suficiente, que abarquen todos los ámbitos, desde los perfiles más técnicos, pasando por perfiles de especialistas en procesos y gestión, hasta perfiles directivos.

Enlaces de interés...

- ISMS Fórum
- Incibe

#ITWEBINARS

it Digital Security

Jueves, 26 de octubre - 11:00 (CET)

Regístrate en este IT Webinar y conoce las principales claves de la Regulación Global de Protección de Datos, la nueva normativa europea que exige una nueva forma de gestionar y proteger la información que manejan las empresas, y que será de obligado cumplimiento a partir del 25 de mayo de 2018. ¿Están preparados tus sistemas?

Registro

Martes, 28 de noviembre – 11:00 (CET)

Las organizaciones exigen e implementan nuevas soluciones que les permitan agilizar las operaciones, aprovechar nuevas oportunidades de negocio y ofrecer un mejor servicio a sus clientes.
Pero estas nuevas soluciones y tecnologías también requieren que los responsables de TI mantengan la protección de los activos de su organización y de sus clientes, incluso cuando decidan mover el control de la red, las plataformas, las aplicaciones y los datos más allá de las tecnologías y límites tradicionales de su organización.

Registro

PABLO FERNÁNDEZ BURGUEÑO

@Pablofb

Abogado y socio en NevTrace y Abanlex

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

Seguridad Informática y previsiones de futuro

para el sector financiero

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

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

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

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

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

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

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

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

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

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

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

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

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

Así son los ataques informáticos que sufre el sector financiero

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

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

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

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

PASADO, PRESENTE Y FUTURO DEL RANSOMWARE

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

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

Previsiones de futuro para el sector financiero

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

Enlaces de interés...

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

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

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

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

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

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