FORO DE LA EMPRESA DEL
Mañana

Patrocinador tecnológico
SAMSUNG

Ciberseguridad

30 buenas prácticas en grandes empresas nacionales e internacionales

Mañana es hoy

La transformación digital de las Grandes Empresas empieza cada día. Hoy también.

orange™

Edición: Orange España S.A.U.
Producción: Evoca Comunicación e Imagen
Fecha de edición: Mayo 2019

Introducción

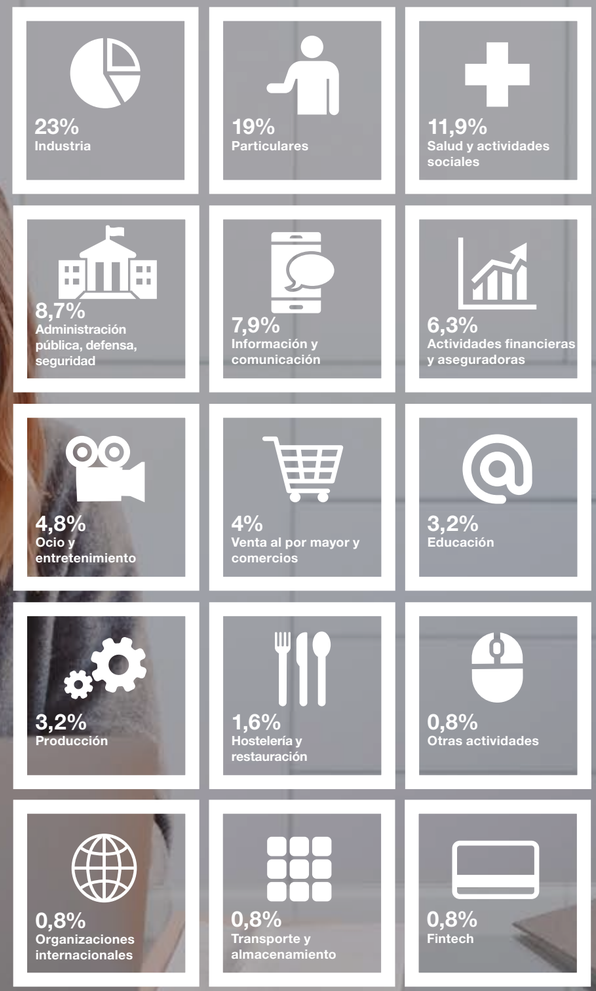
Todas las empresas han sufrido o sufrirán alguna vez las consecuencias de un ciberataque. La pregunta es cuándo vamos a ser atacados por un virus, troyano o robo de identidad y cuántas veces podría haberse evitado con un mínimo conocimiento y medidas básicas de prevención.

El uso de la tecnología implica también cuidar y resolver circunstancias de riesgo que puedan provocar y comprometer la situación económica o reputacional de las empresas. Y es en este entorno donde crece y se desarrolla el sector de la ciberseguridad. El riesgo de ciberataques es uno de los más probables y que mayor impacto puede producir, según las encuestas mundiales. Solo están por encima los desastres naturales.

De hecho, España es uno de los países que recibe mayor número de ciberataques, por detrás de USA y Reino Unido.

Si el sector tecnológico en general crece cada año, la ciberseguridad en particular lo hace a un ritmo aún mayor.

Factores como la digitalización implican un aumento exponencial en el uso e intercambio de datos, creando una dependencia casi absoluta de los sistemas y en consecuencia también de las amenazas. Mientras la información sea almacenada, procesada y transportada, existen riesgos de intervención externa sobre los datos. Y la ciberseguridad es la disciplina que se ocupa de esta especialidad dentro de lo que llamamos Seguridad en la Información, que es un concepto más amplio e incluye otras disciplinas.



Fuente: Gráfica JS por amCharts

La información es dinero, y proteger los datos ya se ha convertido en una de las líneas presupuestarias más importantes en las empresas. Si hablamos de sectores donde los datos son más sensibles, la supervivencia y la credibilidad de estas empresas depende en gran medida de la seguridad en sus datos.

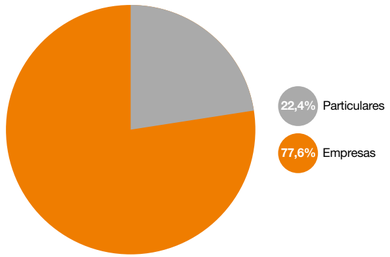
Necesidad de securización

Si tenemos en cuenta el aumento en la conectividad entre distintos dispositivos y aplicaciones, una consecuencia natural de la evolución de la tecnología en todo lo que nos rodea (sensores, ordenadores, móviles, drones, coches, casas conectadas), y la necesidad de que las máquinas ejecuten las instrucciones exactas para las que son diseñadas, nos encontramos ante una necesidad de securización de primer orden. Ya existen más dispositivos Internet of Things (IoT) conectados que población global.

La mayoría de los ataques tienen como objetivo las empresas, siendo un 77,6% de todos los ataques que se producen, mientras que los particulares reciben un 22,4% del total. Dentro de todas las empresas su situación de indefensión, ya sean grandes o medianas compañías, son los principales objetivos de los hackers en los últimos años, ya que muchas de ellas suponen un puente de acceso a grandes corporaciones para las que trabajan o de las que son proveedores de servicios.

Objetivo de los ataques

Fuente: Hackmageddon, 2018



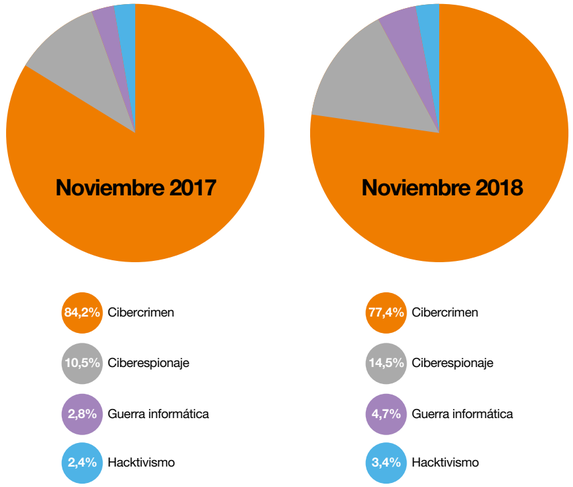
La ciberdelincuencia

Ejemplos recientes como la filtración de datos de Facebook confirman que la preocupación es generalizada y puede afectar tanto a las empresas que los almacenan, como a las personas que están detrás de todo ese Big Data, y que son propietarias de esa información desde un punto de vista de privacidad, identidad e intimidad, aunque cedan sus derechos de uso para otros fines.

La ciberdelincuencia no tiene fronteras y la impunidad que proporciona la distancia, los delitos son perpetrados a miles de kilómetros, impide además actuar de manera contundente y precisa. La ciberseguridad es una ciencia viva, evoluciona a la vez que los riesgos y amenazas, requiere de un rápido aprendizaje y aportar soluciones también ágiles, y precisa de profesionales en constante observación y alerta.

Motivaciones: 2017 VS 2018 (3 meses)

Fuente: Hackmageddon



"El volumen de ciberataques en 2017 por actividad de las empresas tienden hacia determinados sectores como el financiero, energético o utilities.

2

El sector en datos

La ciberseguridad está creciendo a nivel mundial a un ritmo del 13% anual, según la Comisión Europea, que también estima la necesidad de cubrir más de 1 millón de puestos de trabajo, demanda que no va a ser cubierta.

El sector mueve alrededor de 71.000 millones de euros a nivel mundial, unos 1.200 millones de euros en España, según el director general del Instituto Nacional de Ciberseguridad (INCIBE).

Cada 2 segundos una persona es víctima de robo de identidad, según Reuters.

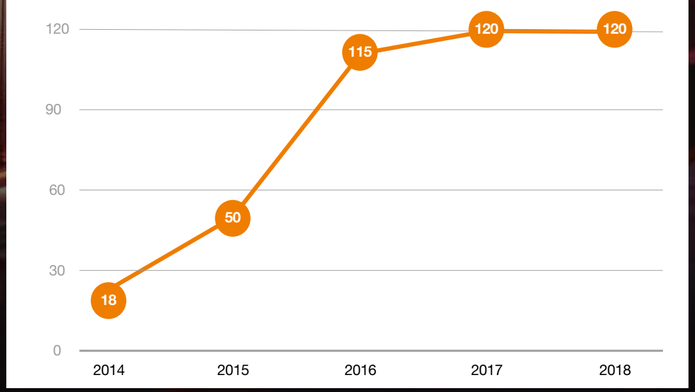
El 30% de los europeos, confiesa haber sido víctima de suplantación de la identidad, siendo el origen de la estafa un correo electrónico. En el caso de España, esta cifra se reduce hasta el 18% e implican la extracción de dinero en el 37% de los casos. La gran mayoría de las amenazas que logran su cometido a diario son las más simples, las que se distribuyen por campañas maliciosas de correo no deseado, phishing y descargas directas, por lo que podrían mitigarse mejorando la concienciación de los usuarios. El problema es que todavía no se destinan los recursos suficientes para hacerlo.

La ciberseguridad mueve unos 1.200 millones de euros en España.

La progresión de los ciberataques

Si hablamos de incidentes declarados en empresas, en 2018 en España se produjeron más de 100.000 incidentes en ciberseguridad, una cifra récord, frente a los 18.000 incidentes registrados en 2014. Esta progresión nos da una idea del alcance y magnitud del problema.

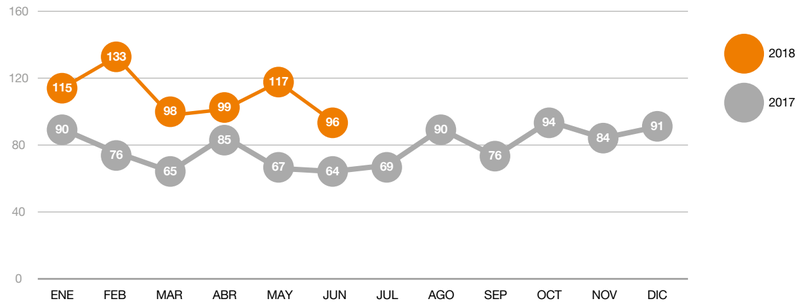
Número de incidencias registradas
(en millares)



> Las amenazas son mayores que la capacidad de monitorizarlas: el 44% de las amenazas diarias no se investigan.

Ataques mensuales (2018 - 6 meses - vs 2017)

Fuente: Hackmageddon, 2018



Amenazas y brechas de seguridad

Se ha alertado de la necesidad de proteger los equipos informáticos, teniendo en cuenta que el virus de mayor impacto que existe ahora en España se desarrolló en el año 2007 aunque al poco tiempo de propagarse se creó un antivirus.

Sin embargo parece existir una diversidad de soluciones similares debido a que el 55% de las organizaciones utiliza más de 6 proveedores de seguridad y el 65% usa más de 50 productos distintos de seguridad.

Las amenazas son mayores que la capacidad de monitorearlas: el 44% de las amenazas diarias no se investigan. Solamente el 56% de las alertas son investigadas y, aunque el 28% de ellas son legítimas, solo al 54% se les da solución.

El 61% de las organizaciones analizadas presentaba brechas de seguridad en el 30% de sus sistemas. De hecho, debido a estos fallos del sistema el 29% de las empresas ha reportado pérdidas de ganancias y el 22% ha perdido a clientes.

Los investigadores de Cisco descubrieron que estaban presentes tres tipos de spyware en el 20% de las 300 compañías de la muestra.

Nadie está a salvo

Según los investigadores de amenazas de Cisco, un tipo de malware como es el spyware también irá en aumento. Mediante su análisis, donde estudiaron tres familias de spyware, descubrieron que estaban presentes en el 20% de las 300 compañías de la muestra.

Finalmente, la tecnología IoT se ha considerado como una de las puertas de entrada más accesibles para los ciberataques, causado por una falta de protección en la red de los dispositivos IoT, que permite a los hackers moverse lateralmente dentro de la red sin levantar sospechas y con relativa facilidad.

Según el último informe de Ontsi, la “ciberconfianza” obtuvo una tasa de 43,1% en el primer semestre de 2018, aunque el 46,4% de los usuarios de Internet lo percibe como más seguro cada día. Este dato posiblemente se halle condicionado por la cantidad de noticias relacionadas con incidencias de seguridad de las que se han hecho eco los medios de comunicación.

Otro de los indicadores se centra en aquellos dispositivos donde se han encontrado archivos maliciosos como ordenadores (69,9%) y Smartphone/tablets Android (77,9%) y que presentan un nivel alto de riesgo en ciberataques malware debido a la naturaleza de los ficheros encontrados en ellos.

La inversión en ciberseguridad

Para 2020 se calcula que Europa necesitará más de un millón de empleados dedicados a la ciberseguridad. Es un sector en clara expansión y crecimiento, aumentando más de un 13% cada año.

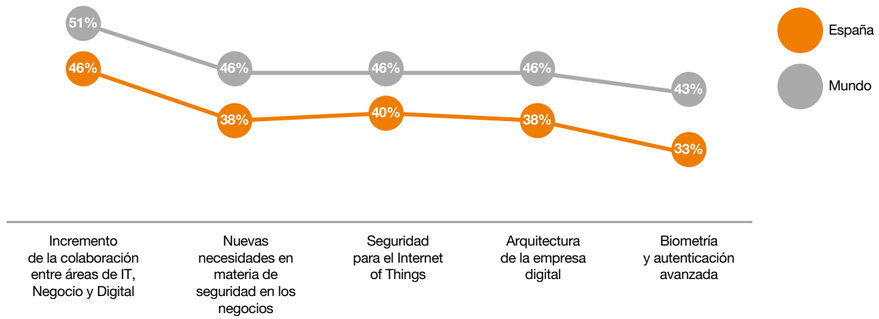
El responsable de seguridad informática de Abanca afirma que su nivel de fraude es bajísimo, pero que en su entidad más del 90% de los incidentes serios corporativos tienen que ver con una mala praxis humana.

Desde 2012 el presupuesto medio en ciberseguridad en las empresas se ha duplicado. Si hay un motor de toda esta inversión es la propia transformación digital de las empresas.

Y ¿dónde van a invertir en ciberseguridad las empresas en los próximos años?

Se estima que entre 2017 y 2021 habrá un gasto total de casi 900 millones de euros a nivel mundial en ciberseguirdad, incluyendo tendencias emergentes, empleo, sector gubernamental o inversión en nuevos modelos de negocio relacionados. Desde 2014 se ha multiplicado por 35 la inversión actual, aunque es muy difícil calcular o determinar estas cifras, ya que el gasto en seguridad no siempre está bien contabilizado y muchas acciones realizadas en las empresas en esta línea se están imputando a otros conceptos.

También se estiman unas pérdidas de 535.000 millones de euros a nivel mundial hasta 2021 provocadas por el cibercrimen. Una estimación que aunque difícil de calcular, aumenta cada año, con nuevos hackers, nuevas comunidades bajo la llamada Dark Web, hackers a sueldo y otras tendencias que también provocan un incremento en el número de ataques.



Fuente: PwC, The Global State of Information Security Survey, 2017

Desde 2014 se ha multiplicado por 35 la inversión actual en ciberseguridad.

Datos más importantes

- La ciberseguridad mueve 71.000 millones de euros en el mundo, 1.200 millones de euros solamente en España.
- Un 18% de españoles ha sufrido algún tipo de robo de identidad. En Europa, cada 2 segundos hay una nueva víctima y hasta un 30% ha sufrido algún incidente.
- El 46,4% de los españoles tiene mucha o bastante confianza en Internet.
- En el 69,9% de los ordenadores y el 77,9% de los teléfonos móviles analizados en España se han encontrado archivos maliciosos.
- Las empresas han pasado de sufrir 18.000 ciberataques a más de 100.000 desde 2014.
- La inversión en ciberseguridad de las empresas en España se ha duplicado desde 2012.
- La ciberseguridad con un ritmo de crecimiento anual del 13%, y creará más de 1 millón de puestos de trabajo en Europa.

10 tendencias clave

Las empresas están dejando de considerar la ciberseguridad como un gasto necesario para empezar a verla como una estrategia. La implantación de mejores herramientas y protocolos de seguridad aumentará la confianza de empleados y clientes.

Los objetivos prácticos de la seguridad de la información deberán enfocarse en salvaguardar la confidencialidad, integridad y disponibilidad de los sistemas informáticos y los datos. Por ello, el aumento de ciberataques como las fugas de datos y los casos en los que se han reportado fallos en el control de la privacidad de clientes y usuarios, desplazan toda la atención una vez más, en garantizar la seguridad de los activos.

10 claves de la ciberseguridad

1 Formación para la prevención

La prevención de ataques en las empresas pasa por la formación a los empleados, proveedores e incluso a clientes. Desde organismos públicos ya se están llevando a cabo políticas de formación frente a los ciberataques.

2 Autenticación más segura

Con herramientas como doble factor, sistemas biométricos o Blockchain, la ciberseguridad debe volcarse en nuevos sistemas de autenticación más seguros y fiables.

3 Herramientas de prevención más sofisticadas

Las herramientas antimalware y Open Source se han convertido en una respuesta ágil y colaborativa, donde los responsables de seguridad cooperan para aportar soluciones y ponerlas a disposición de los demás.

4 Control de datos

Herramientas basadas en Big Data, data analytics y visualización de datos lograrán predecir los ataques. Ya es tendencia el uso de dashboards para monitorizar anomalías en los departamentos de seguridad.

5 Planes de contingencia

Es necesario que los nuevos protocolos de actuación sean más elaborados y estructurados, para poder agilizar los procedimientos de respuesta y dar aviso de los problemas a las personas adecuadas en cada momento.

6 Machine Learning

Ayudará a detectar nuevas amenazas que generalmente escapan de los métodos de detección tradicionales, aprendiendo del comportamiento y actuando sin la intervención humana.

7 Dispositivos más seguros

Los protocolos de comunicación entre los dispositivos, sobre todo en los móviles, se verán reforzados con Blockchain o encriptación de las comunicaciones, y su acceso estará más protegido con métodos de autenticación más robustos como los sistemas biométricos.

8 Redes más controladas

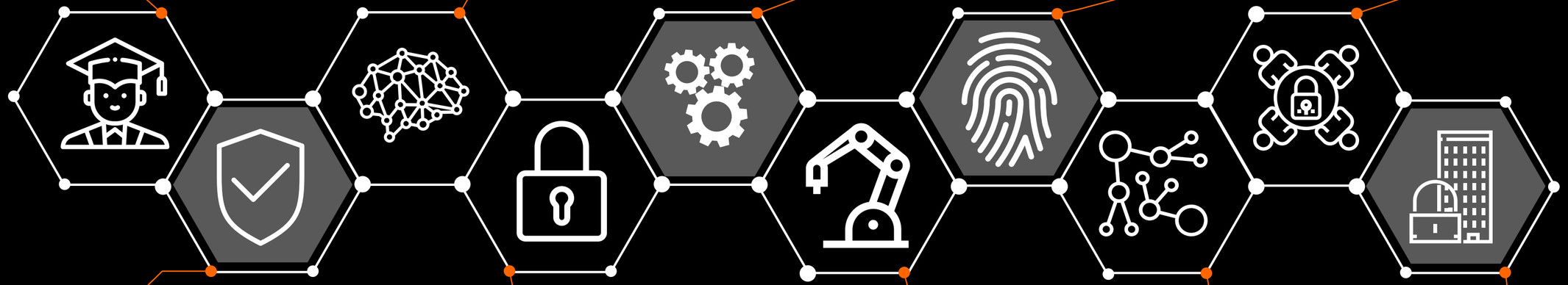
Con medidas como los accesos limitados a usuarios y servicios autorizados, así como un aumento en la seguridad de los protocolos de transmisión de datos, utilizando la encriptación y nuevos certificados como el TSL (Transport Layer Security).

9 Cumplir la normativa

La aplicación de la normativa general de protección de datos (RGPD) necesita un mayor nivel de inversión en ciberseguridad por parte de las empresas.

10 Protección de activos

La seguridad ha dejado de ser un gasto para pasar a ser una inversión o estrategia clave en cualquier sector, sobre todo cuando el mayor activo de las empresas son sus datos.



Amenazas

Las amenazas en materia de ciberseguridad están relacionadas con el lucro económico o el ciberactivismo, y pueden adoptar distintas formas o estrategias para provocar daños en las infraestructuras, sistemas y datos.

Cada minuto aparecen 16 nuevos tipos de malware. Solamente en 2017 aparecieron un 23% más de programas maliciosos contra Windows que en 2016, según la compañía GDATA, que analiza la evolución año tras año. Además, calcularon que cada usuario recibió una media de 22 ataques en el segundo semestre de 2017 y se apreció un fuerte aumento en los realizados al sistema operativo Android.

Los nuevos tipos de malware aumentan cada año.

Solo en 2015 se produjo un ligero descenso, y frente a los datos de 2007, donde alcanzaron la cifra de 130.000 nuevos virus detectados, en 2017 fueron 8.400.000 los nuevos tipos de ataque detectados.

4. Amenazas

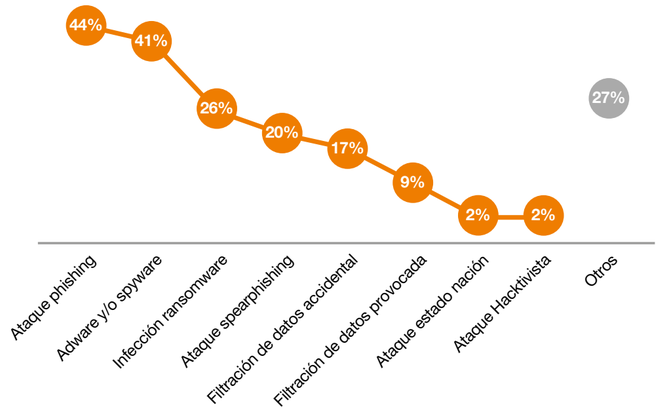
El phishing y el spyware son los tipos de ciberataques más frecuentes, representando más del 40% de los ataques de seguridad ocurridos en el último año.

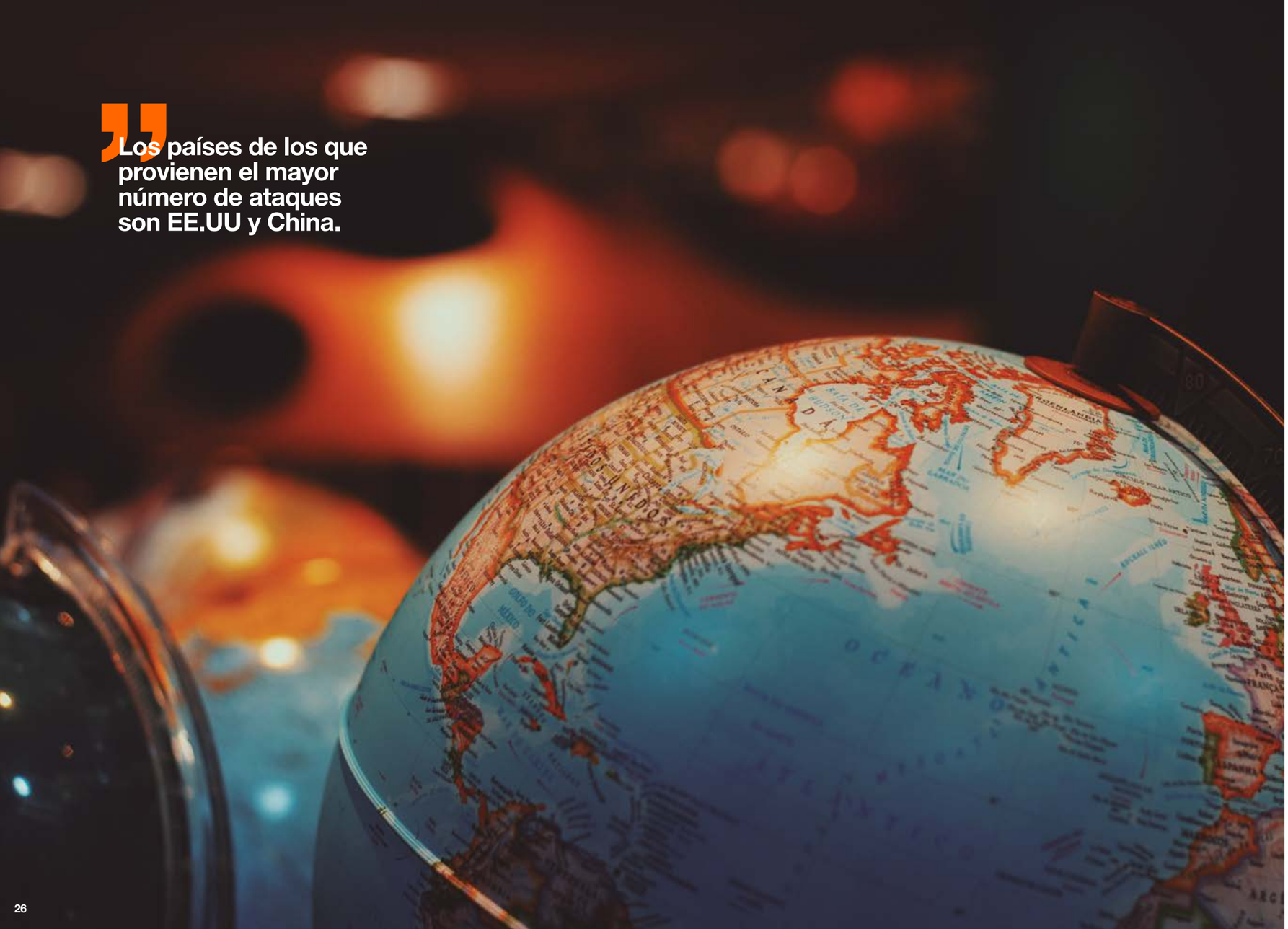
Tipos de ataque

Por tipos de ataque, los que afectan más a las empresas son el ransomware y las modalidades de spearphishing y brechas de acceso a los datos. Sin embargo, si hablamos de volúmenes totales, los tipos de ciberataques más extendidos son el phising y el spyware, aunque afectan principalmente a particulares.

Ataques de seguridad ocurridos en los últimos 12 meses

Fuente: Osterman research Ago 2018





> Los países de los que provienen el mayor número de ataques son EE.UU y China.

Ataques por países

Los países de los que provienen el mayor número de ataque son EE.UU y China, mientras que los países objetivo más importantes han sido de nuevo EE.UU junto a Emiratos Árabes y España.

Origen del ataque

#	País
328	United States
299	China
26	Ukraine
20	Colombia
18	Netherlands
14	South Korea
10	France
10	Switzerland
9	Spain
8	Turkey

Tipo de ataque

#	Tipo de puerto de servicio	
262	25	Unknown
167	8080	Unknown
127	23	Telnet
42	3389	Unknown
34	5900	Unknown
25	3306	Unknown
23	445	Unknown
18	50864	Unknown
10	123	Unknown
9	80	Unknown

Objetivo del ataque

#	País
465	United States
211	United Arab Emirates
52	Spain
26	Singapore
24	Italy
8	Saudi Arabia
6	Philippines
6	Belgium
5	France
5	Australia

Fuente: Capital México oct 2016

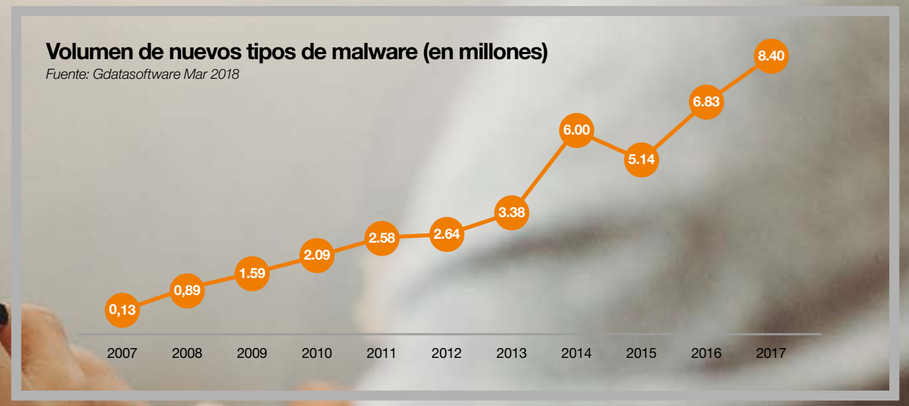
Queremos tener una visión más actual y acorde al impacto de los ataques en los últimos años. Por ello, abrimos así una clasificación de los ciberataques que han tenido o tendrán mayor relevancia en 2019 en los siguientes puntos del informe.

4.1

Malware clásico

El malware es todo software diseñado específicamente para infiltrarse en ordenadores o dispositivos de terceros para dañarlos. Dentro de este tipo de ciberataque encontramos los clásicos virus troyanos y gusanos que siguen activos en la red aprovechándose de la vulnerabilidad de los equipos y de las personas que no cumplen normas básicas en ciberseguridad.

La protección con antivirus de los ordenadores es una buena práctica que no debemos abandonar, pues la mayoría de los ataques que se producen en Internet corresponden a virus y troyanos antiguos que ya llevan activos algunos años y, aunque estén localizados y neutralizados, la inexistencia de antivirus o medidas básicas de prevención en los equipos, pueden desencadenar un ataque de estas características. Además, es habitual que los hackers utilicen otras estrategias como la reutilización de código de malware antiguo y desarrollen mutaciones que sean menos detectables por los antivirus. Esto facilita la aparición de nuevos virus con un esfuerzo de codificación menor. Todos recordamos algunos de los virus más dañinos de la historia: Morris (1988), CIH Chernobyl (1998), Melissa (1999), I love you (2000), Mydoom (2004), o Conficker (2008). Ejemplos mediáticos y que pusieron a la ciberseguridad en primera página de las noticias a nivel mundial.



La mayoría de los ataques que se producen en Internet corresponden a virus y troyanos antiguos.

4.2

Ransonware

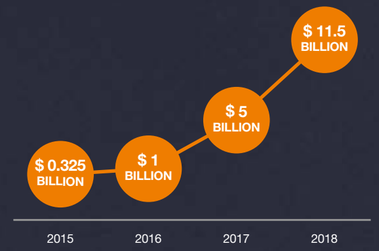
Ransomware es una variedad de malware que encripta los ficheros con una clave privada e impide el acceso a ellos. Los hackers “secuestran” los archivos y tras el pago de un rescate, permiten que el usuario o la empresa pueda recuperarlos.

En los últimos años se han producido importantes acciones de este tipo, como WannaCry, que bloqueó a distintas empresas a nivel mundial. Aunque también es un tipo de malware, abordamos este tipo de ataque de forma independiente dado que últimamente su protagonismo ha aumentado de forma importante. En los próximos años este tipo de ataques continuarán, ya que muchas empresas prefieren pagar por recuperar su información en caso de ser atacadas a incluir en sus presupuestos una partida para ciberseguridad y prevenir esos ataques.

ESET (empresa eslovaca de seguridad informática) advierte que el ransomware ha sido una de las fuentes de negocio de los cibercriminales en 2018, dada la tendencia anunciada anteriormente, y sitúa la elección de las empresa hacia pagar grandes sumas de dinero por recuperar sus sistemas comprometidos en lugar de contar con políticas de ciberseguridad que las mantengan protegidas ante cualquier amenaza.

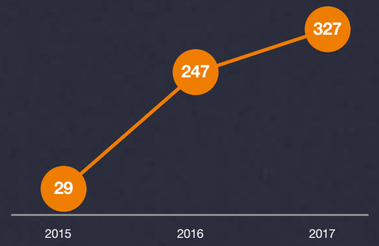
Ransomware: coste total del daño

Fuente: Gdatasoftware Feb2018



Número de familias

Fuente: Statista Feb 2018



Los rescates

Según una investigación realizada por Norton Cyber Security, el 34% de las víctimas paga el rescate exigido por los hackers, sin embargo solo el 47% de los que pagaron el rescate, recuperaron sus archivos o accesos por completo porque el pago no asegura la integridad de los archivos comprometidos. El coste de estos rescates y de resolver los problemas derivados de incidentes con ransomware asciende a más de 440 millones de euros en 2017 y se espera que suponga más del doble en 2019.

A su vez, el número de familias de ramsonware crece cada año. Estamos ante una amenaza que crece cada día y que pone en riesgo los datos y la información de muchas empresas y particulares.

DDoS

Un DDoS (Distributed Denial of Service) satura un servidor con peticiones concurrentes hasta agotar sus recursos. Los ataques destinados a provocar la indisponibilidad de sistemas son habituales y, con el apoyo de bots y programas ejecutables, realizan peticiones a los servidores desde distintas IPs para provocar la caída de los servicios.

Muchos recuerdan los ataques que se produjeron contra el Departamento de Justicia americano y contra Universal, entre otros, tras el cierre de Megaupload, como forma de protesta por parte del colectivo Anonymous. Es el concepto básico del DDoS, aunque se puede modificar para que sea más efectivo. Por ejemplo, se pueden enviar los datos muy lentamente haciendo que el servidor consuma más recursos por cada conexión (por ejemplo Slow Read) o alterar los paquetes para que el servidor se quede esperando indefinidamente una respuesta de una IP falsa (SYN flood).

Otra técnica para llevar a cabo los DDoS es usar botnets: redes de ordenadores infectados por un troyano y que un atacante puede controlar remotamente. De esta forma, los que saturan el servidor son ordenadores de gente que no sabe que están participando en un ataque DDoS, por lo que es más difícil encontrar al verdadero atacante.

Se pueden proteger los servidores de ataques con filtros que rechacen los paquetes mal formados o modificados con IPs falsas, para que solo le lleguen los paquetes legítimos.

Tras el cierre de Megaupload, se produjeron ataques contra el Departamento de Justicia americano y Universal como forma de protesta.

Remote Access Trojan (RAT)

Es una modalidad de ataque que permite el acceso y el control de la máquina comprometida. Los ataques de este tipo son muy peligrosos ya que toman el control del dispositivo atacado y pueden realizar las mismas acciones que sus propietarios, poniendo a disposición de los hackers todas las herramientas y aplicaciones instaladas en el equipo.

Los clásicos RAT son capaces de controlas múltiples funciones cuando acceden al dispositivo, entre ellas están: recopilar información recogida según las pulsaciones del teclado, robar contraseñas almacenadas en caché y datos de formularios, tomar capturas de pantallas, así como hacer vídeos o grabar sonido controlado por la webcam, transferir archivos, recopilar información del usuario y del sistema, y finalmente controlar acciones más sofisticadas como robar claves de exchanges de criptomendas o robar certificados VPN.
Entre otras cosas, es capaz de tomar el control del teléfono, se comunica con un servidor C&C remoto, controla el estado del WiFi, puede supervisar los sensores del teléfono en tiempo real y configurar la propia interfaz de usuario con el acceso al modo nocturno, así como controlar otras funciones como el modo vibración y patrón de acceso. Una vez infectado el dispositivo se puede identificar por que elimina o descarga archivos, también los cambia de nombre y lugar, crea directorios y finalmente envía, intercepta y elimina comunicaciones como los SMS. Troyanos de este tipo son capaces de gestionar en remoto casi todas las funciones clave del móvil.

Los RAT pueden controlar prácticamente todo de un ordenador, desde la webcam hasta la transferencia de archivos o datos.

Phishing

El ataque se basa en la suplantación de identidad de una empresa de confianza mediante un e-mail que te solicita los datos de acceso para así obtener información personal de los usuarios.

El phishing siempre ha sido un quebradero de cabeza para las entidades financieras. Este tipo de ataque provoca cada año un gran volumen de robos de claves y una pérdida económica importante para los clientes afectados. Además, se ha sofisticado mucho. Hace algunos años era fácil detectar que los emails no provenían de la entidad que decían ser, errores ortográficos, traducciones mal realizadas, etc. Pero en los últimos años han sido capaces de camuflar mejor el origen del email, maquetar estas comunicaciones e incluso llevarte a páginas de destino que se parecen mucho al sitio web que suplantan, consiguiendo mayor grado de éxito en estas acciones.

El phishing se ha sofisticado tanto en los últimos años que hoy en día puede resultar difícil diferenciar un correo malicioso de uno real.

El 12,1% de los usuarios a nivel mundial se toparon con phishing en el tercer trimestre de 2018. De hecho, 1 de cada 2.000 correos que se mandan al día contiene un mensaje malicioso y más de la mitad de los ataques pretenden suplantar a bancos y sistemas de pago, aunque también existen y aumentan los correos dirigidos a usuarios de tiendas online, como Amazon, para hacerse con las claves de acceso a este tipo de portales. Es el segundo tipo de amenaza más numerosa en Internet, después de los troyanos.

Ya se está pronosticando un aumento de este tipo de ataques, incluso hacia usuarios de servicios como Netflix, con 110 millones de usuarios, llegando a personalizar las imágenes del mensaje con tus series favoritas. Con este ataque pretenden alertar al usuario para que modifiques tus datos de facturación y así conseguir los datos de tarjetas de crédito, documentos de identidad, etc.

1 de cada 2.000 correos que se mandan al día contiene un mensaje malicioso y más de la mitad de los ataques pretenden suplantar a bancos y sistemas de pago.

Robo de datos

El robo de datos es uno de los ataques más peligrosos, ya que habitualmente se produce dentro de la empresa por parte de empleados infieles o para espionaje industrial.

A veces no requiere software ni conocimientos técnicos para provocar un incidente; con disponer de las claves de un usuario administrador del sistema es suficiente, y se puede realizar desde dentro y en la aparente normalidad. En otros casos, el robo y fuga de datos se produce desde fuera, descargando del sistema de la empresa afectada toda la información crítica y relevante para el objetivo del ataque.

Los datos son un valor en sí mismo y se han convertido en moneda de cambio habitual entre los hackers.

Se pagan importantes sumas de dinero en la Dark Web por la adquisición de lotes de números de tarjetas de crédito, números de la seguridad social, códigos de licencias, etc., para un uso posterior de estos datos en suplantaciones de identidad.

El caso de Equifax -donde se extrajeron los datos crediticios de más de 143 millones de usuarios- es el robo de datos más célebre de la historia de Internet por el volumen e impacto mediático que tuvo.

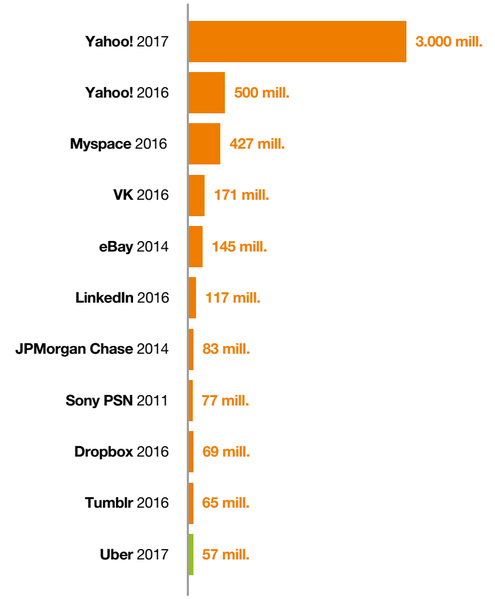
La compañía tuvo que pagar hasta 16,4 millones de euros por demandas de los usuarios mientras que la plataforma que más ha sufrido hackeo y robo de datos históricamente es Yahoo!

Con 3.000 millones de cuentas hackeadas, el portal Yahoo! sufrió en 2017 el mayor hackeo de la historia.

Los mayores hackeos de la historia

Número de cuentas hackeadas en una selección de plataformas tecnológicas

Fuente: Medios de comunicación



Amenazas móviles

La nueva generación de malware específico para teléfonos móviles supone otra amenaza directa contra un dispositivo privado, debido a que tiene acceso a mucha información empresarial y personal.

El dispositivo móvil al igual que otros, es vulnerable y recoge mucha información personal y empresarial que es confidencial y por ello se convierte en uno de los objetivos prioritarios de los ciberataques.

Los ataques a dispositivos móviles han aumentado por el incremento del número de Smartphones en el mundo.

Actualmente, Lokibot, Triada y Hiddad son los 3 malware móvil más comunes a nivel mundial, aunque cambian constantemente.

A medida que los usuarios de banca móvil aumentan año tras año, de la misma forma lo hace el apetito de los criminales por llegar a ellos.

Las tendencias hablan de la aparición de nuevas amenazas que utilizan multitud de variantes de malware móvil, intentando sortear los controles antimalware y técnicas de detección (Overlay y otras tecnologías de bypassing de controles DAC, es decir, del convertidor integrado de audio analógico a digital).

Una de las amenazas móviles más conocidas es la superposición de pantalla. Opfake es un ejemplo de este tipo de programas: puede imitar la interfaz de más de 100 aplicaciones bancarias y modalidades de pago. Así como la familia Acecard, que también es capaz de emular al menos 30 entidades.

"El móvil seguirá siendo uno de los objetivos prioritarios de los ciberataques.

Este es el top 3 de malware móvil a nivel mundial, aunque los números cambian constantemente de un mes a otro.

1

Lokibot: troyano bancario y ladrón de información para Android. Puede convertirse en un ransomware que bloquea el teléfono.

2

Triada: backdoor modular para Android. Confiere privilegios de superusuario para descargar malware.

3

Hiddad: malware para Android que reempaqueta aplicaciones legítimas y las publica en tiendas de terceros.

Malwareless

Este tipo de ataque no requiere de software malicioso y aprovecha las vulnerabilidades de otras aplicaciones, y se apoya en herramientas no maliciosas para llevar a cabo sus ataques.

Si 2017 fue el año del ransomware, 2018 fue el del malwareless. El problema para identificarlo es que ya no se trata de encontrar o bloquear un archivo concreto de malware. Al integrarse con herramientas no maliciosas que forman parte del día a día, se introducen en los sistemas a través de ese software no controlado y más vulnerable, y se ejecutan desde aplicaciones aparentemente seguras y estables en las que confían los responsables. Como consecuencia, son capaces de infectar equipos y personas clave dentro de la organización, que utilizan de forma habitual esas aplicaciones, por ejemplo responsables de IT o de alta dirección, que tienen acceso a información y sistemas internos más atractivos y golosos para los ciberdelincuentes.

La solución al malwareless es el Threat Hunting, basándose en el comportamiento exhibido por los usuarios de la red corporativa. Se trata de monitorizar los equipos y las aplicaciones que se ejecutan en ellos, para observar y controlar el tráfico en la red.Si tenemos estadísticas fiables de todo esto, podremos detectar cualquier desviación o situación sospechosa.

> **La solución al malwareless es el Theart Hunting, que trata de monitorizar los equipos y las aplicaciones que se ejecutan, para poder observar y controlar el tráfico en la red.**

Malvertising

Son banners y publicidad que encubren y ejecutan amenazas para los equipos.

La primera campaña de malvertising fue detectada en octubre del 2015, pero fue a lo largo del 2016 y 2017 cuando el número de casos identificados de esta mala praxis se disparó. A través de la compra legítima de espacios publicitarios, los cibercriminales emplazan anuncios en sitios web o aplicaciones conocidas y percibidas como seguras para dirigir tráfico o descargar archivos que contienen malware u otro tipo de software dañino. Los anuncios aparecen durante un corto periodo de tiempo, con lo que las posibilidades de identificación de estas amenazas son reducidas. Esta técnica viene de la mano de la automatización de la compra de espacios publicitarios o publicidad programática, que permite a los ciberatacantes tener más información sobre el tipo de usuarios que ven los anuncios, y así poder personalizar más sus acciones. El crecimiento previsto en la contratación de publicidad programática favorecerá el incremento en el número de ataques que utilizan esta técnica.

Los usuarios se han vuelto prudentes con este tipo de ataques y en muchos casos instalan adblockers que impiden impresiones publicitarias, limitando las capacidades de las campañas y su efectividad. Si a esto le sumamos la ceguera al banner (banner blindness), nos encontramos con un mercado limitado. Hay que contrarrestar el efecto con campañas originales, seleccionando bien las ubicaciones y ganando la confianza del usuario.

El malvertising es un gran enemigo del marketing digital.

Cryptohacking

Esta modalidad pretende explotar las capacidades de proceso de los sistemas de otros, para el lucro personal de hackers que utilizan las máquinas en minería de criptomonedas.

El auge del mercado de las criptomonedas y el crecimiento explosivo que ha experimentado, pone a estas plataformas en el punto de mira de los cibercriminales. Son comunes las infecciones de equipos con software de minería de criptomonedas o el robo de wallets de usuarios. Los picos históricos en el valor de estas monedas durante 2018 añadieron un aliciente para los ciberdelicuentes que buscaban infectar a este tipo de usuarios y así, sacar un provecho económico muy por encima de una víctima normal.

Con la popularidad de las criptodivisas, los delincuentes tienen en su objetivo a los mineros y usuarios que compran y venden criptodivisas.

También la minería de las criptomonedas sirve como pantalla de humo para la difusión del malware.

Al utilizar servidores con alta capacidad de cómputo, usados en minería, pasan más desapercibidos para los investigadores y se utilizan en muchas ocasiones como plataforma de alojamiento y difusión del malware.

> **La minería de las criptomonedas sirve como pantalla de humo para la difusión del malware, cuyos servidores pasan más desapercibidos.**

Entre los años 2013 y 2017, los virus diseñados para la extorsión en el mercado de las criptomonedas recolectaron cerca de 23.000 Bitcoins por la vía de ataques ransomware, que a día de hoy equivalen aproximadamente a 180 millones de euros.

23.000 Bitcoins = 180 millones de euros

Hacktivismo

Este tipo de ataque pretende influir en las opiniones de los ciudadanos y en la política, desestabilizando regiones o países, y aprovechándose de la viralidad de fake news o de mensajes en redes sociales y plataformas de uso habitual de los usuarios.

Algunas agencias de marketing incluso cuentan con batallones de perfiles fake para campañas políticas o de influencia y en consecuencia, tiene un componente importante de ingeniería social.
Por otra parte, el voto electrónico dista mucho de ser seguro, como se ha demostrado en los países donde se ha probado. Y el aumento de la influencia de la opinión pública en las redes sociales ya se ha demostrado como otra fuente de fraude político desde la que dirigir la demanda de votos y condicionar resultados electorales, como en la última campaña de Trump a la presidencia de EEUU. Si además cuentan con un patrocinador económico, al que le interesa condicionar resultados en una u otra dirección, tenemos el caldo de cultivo perfecto para que este tipo de acciones se sigan produciendo.

> **El aumento de la influencia de la opinión pública en las redes sociales ya se ha demostrado como otra fuente de fraude político.**

Fake news

Se estima que para 2022 se consumirán más noticias falsas que verdaderas. Actualmente no existen soluciones que las bloqueen o eliminen y se estima que crezcan y que puedan llegar a mucha gente en muy poco tiempo con una gran capacidad de manipular la opinión pública. Facebook, la red social más grande del mundo, ya está tomando cartas en el asunto. Si se descubre que una página de Facebook distribuye repetidamente noticias falsas, prohibirá que esta se publicite en la red social.

El caso de Cambridge Analytica y la extracción de datos de usuarios de Facebook es un ejemplo de cómo utilizar el potencial de esta información para influir en la opinión pública ante un proceso electoral. Utilizando aplicaciones de test donde el usuario autoriza el acceso a sus datos, recopilaron información de millones de usuarios y sus contactos (se calcula que casi 87 millones de personas). Utilizando estos datos y preferencias personales, combinadas con el estado de ánimo, etc., eran capaces de establecer patrones de comportamiento y sensibilidad a determinados problemas, dirigiendo de este modo el mensaje de la campaña electoral para contentar a los perfiles que más interesaban al partido republicano de Trump.

La ciberseguridad por sectores

La ciberseguridad actúa y afecta de manera diferente en cada sector clave, pero en todos ellos se ha convertido en una cuestión fundamental.

Aunque todos estamos implicados en la transformación digital, la ciberseguridad es un aspecto crucial en todos los sectores, ya sea por la sensibilidad de los datos gestionados, por su impacto en el mundo real o por salvaguardar la mera privacidad de las personas.

5. La ciberseguridad por sectores

Banca y seguros

La seguridad es la clave de la banca y las entidades aseguradoras. Sin ciberseguridad, no hay garantías para una banca online fiable y, por tanto, su futuro se podría cuestionar.

El 90% de los clientes españoles cambiaría de banco si su entidad fuese víctima de un ciberataque, con el agravante de que el 52% de quienes han sufrido un robo online no han recuperado nada o casi nada de lo sustraído. Algunos casos han sido publicados y difundidos por la prensa, y otros muchos silenciados por las propias entidades financieras para preservar la confianza de sus clientes, y así, evitar la pérdida de negocio o generar situaciones de pánico. El aumento de robos es tal, que los inspectores europeos (BCE y EBA), Banco Central Europeo (BCE) y Autoridad Bancaria Europea (EBA), consideran prioritaria la creación de barreras que hagan frente a este tipo de acciones y que cuenta con métodos que van desde el phishing hasta las fórmulas más sofisticadas de pirateo informático. Las entidades ya están en ello, pero los inspectores van a exigir auditorías internas que evalúen el riesgo derivado de la tecnología con procedimientos y metodologías avanzados y eficientes, para defenderse de una amenaza que no solo atañe a particulares y empresas, sino a la red de todo el sistema financiero.

Ciberamenazas para las entidades financieras

La mayoría de los ataques a entidades financieras están relacionados con:

- **Malware:** dentro de esta categoría están incluidos los virus, gusanos y el spam. Algunos de ellos como STUXNET, FLAME, ANOYMOS o CONFICKER se han cobrado un gran número de víctimas en el ámbito financiero.
- **DDoS:** ataques de denegación de servicio, estos bloquean el acceso de los usuarios y producen una pérdida de la conectividad, que es aprovechada por los ciberdelincuentes para hacerse con el control del dispositivo y sustraer información. Alguno de ellos como el OCTUBRE ROJO, han llegado a generar estragos.
- **Suplantacion de la identidad:** la mayor parte de las estafas por suplantación de la identidad se realizan por medio de falsos correos o falsas llamadas. En este caso, el delincuente se hace pasar por tu banco para conseguir ciertos datos y robarte el dinero. Phishing, Spoofing, Vishing o Smishing son los más habituales. Se pone de moda el Spear Phishing, buscando como blanco a directivos de alto nivel.
- **Ataques a ATMs:** los cajeros siempre han sido un elemento clave para los ciberdelicuentes. Actualmente los ciberataques tienden hacia malwares de nueva creación, utilizados en operaciones remotas y sin archivos, así como ataques dirigidos a los sistemas de autenticación.

Ciberamenazas en entidades aseguradoras

En el caso de seguros, el sector debe cubrir riesgos relacionados con la ciberdelincuencia, y aparecen pólizas relacionadas con la pérdida de reputación, con la seguridad de las infraestructuras, o con la indisponibilidad de sistemas.

Según AIG, una buena póliza de ciberriesgos debe cumplir con una serie de coberturas fundamentales:

- **Gestión de incidentes:** los honorarios de asesoría legal, informática forense y relaciones públicas a la hora de gestionar, administrar y mitigar un incidente de seguridad de red o de privacidad.
- **Protección de datos y responsabilidad cibernética:** que ampare las reclamaciones de terceros derivadas de demandas por un fallo de seguridad en la red del asegurado.
- **Ciberextorsión:** cobertura a las organizaciones ante las pérdidas resultantes de una amenaza de extorsión. Esto incluye rescates para poner fin a una extorsión, así como los honorarios de asesores especializados.
- **Interrupción de la red o pérdida de beneficios:** responder a la pérdida de ingresos y gastos operativos del asegurado cuando su actividad se interrumpe o suspende debido a un fallo en la seguridad en la red.
- **Fraude de transferencia de fondos:** cobertura de la pérdida financiera resultante de transferencias electrónicas realizadas de manera fraudulenta tras un ciberataque.
- **Respuesta ante inspecciones y sanciones regulatorias:** derivadas de un uso indebido, control o proceso de datos personales.

> **El sector de los seguros ha creado pólizas relacionadas con la ciberdelicuencia y que cubren riesgos como la pérdida de reputación, seguridad en infraestructuras o la indisponibilidad de los sistemas.**

Banco Central Europeo (BCE) ayuda a las entidades financieras europeas a detectar riesgos.

El Banco Central Europeo ha publicado una herramienta para que los bancos y otras instituciones financieras puedan realizar pruebas y comprobar su resistencia a posibles ciberataques, incluso a los más sofisticados. El sistema, llamado TIBER-EU (Threat Intelligence-Based Ethical Red Teaming), simula un ataque en las funciones importantes del banco, y le ayuda a valorar su capacidad de detección, protección y respuesta.

Se incluyen además de bancos, sistemas de pago, depositarios de valores, agencias de calificación de riesgo, mercados de valores, plataformas de liquidación de valores, aseguradoras, o gestores de activos, entre otros.

Será una herramienta de uso voluntario, aunque algunas entidades serán invitadas a participar por su relevancia en el mercado.

- **El sistema TIBER-EU simula un ataque en las funciones importantes del banco.**
- **Las entidades financieras podrán valorar su capacidad y la resistencia a los ataques.**

Industria

Los nuevos procesos que trae la Industria 4.0 solo pueden materializarse aprovechando las oportunidades que brindan las nuevas tecnologías como la computación en la nube, Big Data y la virtualización.

Además, se suman a las operaciones tradicionales su soporte en tecnologías de la información que comienzan a traspasar los límites entre el mundo real y el virtual, en lo que se conoce como los nuevos sistemas de producción ciber-físicos (CPSS - Cyber Physical Production Systems). La alta conectividad que requiere la Industria 4.0 ha provocado que se introduzcan sistemas más abiertos y de propósito más general, como los que se utilizan en las TIC desde hace años.

Hoy en día es habitual ver en sistemas de control industrial que la conectividad esté asentada sobre TCP/IP y Ethernet o el uso de sistemas inalámbricos estandarizados. Todos estos protocolos han sido ampliamente desarrollados y analizados, y ofrecen el nivel de madurez y fiabilidad que la nueva Industria 4.0 requiere. También incrementa su visibilidad y exposición a determinados riesgos derivados de ello y que han de ser correctamente gestionados. Por ello, la Industria 4.0 abre un gran abanico de posibilidades, pero también expone a los sistemas a un nuevo escenario en donde las amenazas son mucho más abundantes.

Claves de la ciberseguridad en la industria

Las claves en la industria se centran en:

- **CPS (Cyber Physical Systems o Sistemas Ciberfísicos):** son sistemas que monitorizan los sistemas físicos, crean una copia virtual y realizan decisiones descentralizadas. La sensorización y los elementos de control son capaces de conectar las máquinas y dispositivos con las plantas, flotas, redes y seres humanos.
- **Internet of Things (IoT):** Los CPSs actúan sobre el IoT. Este paradigma establece que los dispositivos y elementos están conectados a protocolos basados en Internet (TCP/IP).
- **Internet de los servicios (IoS):** Este paradigma ofrece tanto servicios internos en la fábrica como horizontalmente a lo largo de la cadena de valor.

Estos conceptos delimitan la Industria 4.0 en términos de tecnología y procesos, y aglutinan, cada uno en su vertiente, una serie de amenazas, vulnerabilidades y retos en torno a la ciberseguridad que deben ocuparse de:

- Asegurar las instalaciones, los procesos de producción de las fábricas y los sistemas CPS.
- Recabar datos entre los dispositivos relacionados protegiendo su integridad y protocolo de comunicación.
- Asegurar el secreto y confidencialidad de los datos que se refieren a la producción de la empresa.

¿Y en el sector de la automoción?

Dentro de la industria hacemos mención especial al sector de la automoción. Cualquiera que sea un asiduo a los eventos de ciberseguridad sabrá que hackear coches es un tema de moda. Por ejemplo en el Car Hacking Village del DEF CON, los expertos de Tencent Keen hackearon un Model X de Tesla por segundo año consecutivo. Demostraron cómo podían desactivar los frenos del coche vía WiFi, posteriormente consiguieron encender y apagar las luces y abrir y cerrar las puertas del vehículo.

Aunque el mayor riesgo para la automoción y la ciberseguridad es el hacking del coche autónomo, aún no existen muchos modelos en el mercado y tardarán mucho tiempo en aparecer en las carreteras, conviviendo durante un tiempo con los coches habituales.

Los vehículos conectados son ecosistemas complejos con diferentes protocolos (CAN, Ethernet), elementos de hardware (microcontroladores ECU, HSM) y de software (como las aplicaciones móviles) necesitan protección para reducir el riesgo de verse comprometidos.

La tecnología será la protagonista dentro del coche inteligente, aportando soluciones en las comunicaciones, informaciones, entretenimiento y control general del vehículo, así como, los dispositivos que lo rodean como cámaras, sensores y radares, que darán paso al coche autónomo. Consultoras como Gartner predicen que en 2020 el número de vehículos de pasajeros conectados en las carreteras rondará los 150 millones, y entre un 60% y un 75% de esos vehículos conectados serán capaces de consumir, crear y compartir datos en la red. McAfee ya ha elaborado un whitepaper con mejores prácticas para los fabricantes de automóviles conectados, considerando precisamente los riesgos en materia de ciberseguridad.

> **En el Car Hacking Village del DEF CON de este año, los expertos de Tencent Keen hackearon un Model X de Tesla por segundo año consecutivo.**

El software de Tesla hackeado varias veces.

El Tesla Model S se vio comprometido por un equipo de investigadores chinos. Permitieron a los piratas informáticos tomar el control remoto de los frenos, las cerraduras de las puertas, la pantalla de información y otras características. A una distancia de 19 km fueron capaces de atacar el sistema de control del automóvil, compuesto de un grupo de procesadores conectados que gestionan todo el control del vehículo, desde las luces hasta las ventanillas eléctricas. Una tecnología que además está presente en casi todos los automóviles hoy en día. Tesla arregló el problema con una actualización de software.

Tesla es uno de los fabricantes más proactivos cuando se trata de alentar a los piratas informáticos a encontrar vulnerabilidades, incluso los recompensa por hacerlo. Posteriormente, la empresa de seguridad noruega Promon demostró lo fácil que es robar un coche como el Tesla Model S a través de su aplicación para iOS y Android que permite verificar el estado de carga del coche, abrir las puertas remotamente, etc. Sin embargo, si el Smartphone de un propietario es hackeado, la aplicación también puede ser utilizada por los ladrones para robarle el coche. Para sustraerlo, estableció un punto WiFi gratuito cerca de una estación de carga Supercharger Tesla y se inventó una promoción que ofrecía hamburguesas gratis a las personas que crearan cuentas en su red. Con el registro, se cargaba un malware en el dispositivo móvil para tener acceso al nombre de usuario y contraseña de la aplicación de Tesla (este tipo de acciones también permitirían a los piratas informáticos acceder a aplicaciones bancarias, cuentas de correo electrónico, etc). Una vez obtenidos los datos, el ciberladrón ya podía controlar el vehículo desde la distancia, sabía dónde estaba en cada momento y podía abrirlo en remoto. Y no solo eso, Tesla permite conducirlo sin llave, por lo que robarlo no resulta difícil. Con esta demostración Promon quería poner de manifiesto la necesidad de proteger las aplicaciones de posibles ciberataques, y de paso, postularse como la solución a esta vulnerabilidad.

- **A una distancia de 19 km fueron capaces de atacar el sistema de control del automóvil.**
- **Se puso de manifiesto la necesidad de proteger las aplicaciones de posibles ciberataques.**

Stuxnet: un virus para retrasar la carrera nuclear iraní.

En verano de 2010 se desveló la existencia de Stuxnet, una amenaza muy avanzada que fue diseñada específicamente para retrasar todo lo posible el programa nuclear iraní. El éxito que obtuvo este código malicioso, así como las técnicas usadas para conseguir su objetivo, y la implicación de dos naciones como Estados Unidos e Israel en su desarrollo, sirvió para desvelar que habíamos entrado en una nueva era. Stuxnet ataca equipos con Windows empleando cuatro vulnerabilidades de “Zero-day” de este sistema operativo. Su objetivo son sistemas que emplean determinados programas de monitorización y control industrial de Siemens.

En el caso del programa nuclear iraní más de quince instalaciones fueron atacadas e infiltradas por Stuxnet, presumiblemente a través de una unidad USB de un trabajador al azar. Se estima que destruyó 984 centrifugadoras de enriquecimiento de uranio, lo que supuso una disminución del 30% en la eficiencia de estos procesos.

Fruto de las investigaciones que se realizaron a partir de Stuxnet, se vio que esta no era la única amenaza desarrollada con la finalidad de atacar estos sistemas y que incluso se podían relacionar diversas amenazas entre ellas, tal y como fue el caso de Duqu y Flame con respecto a Stuxnet. Una de las consecuencias provocadas por estas amenazas es que desde entonces cualquier incidente en un sistema industrial, especialmente si se trata de una infraestructura crítica, es mirado con lupa para determinar si hay alguna posibilidad de que exista una ciberamenaza involucrada. Esto ha dado lugar al aumento de una paranoia muchas veces infundada, especialmente cuando está involucrada una central nuclear.

- **Ataca equipos con Windows empleando vulnerabilidades de “Zero-day” y su objetivo son sistemas que emplean programas de monitorización y control industrial.**
- **Se estima que destruyó 984 centrifugadoras de enriquecimiento de uranio, reduciendo un 30% la eficiencia de estos procesos.**

“Stuxnet ataca equipos con Windows empleando cuatro vulnerabilidades “Zero-day” de este sistema operativo.

“A parte del espionaje, Dragonfly ataca los sistemas de control industriales para organizar operaciones de sabotaje.

Dragonfly y los ataques a estaciones de energía.

Dragonfly es un grupo de hackers que desde 2013 ha ampliado rápidamente sus actividades, especializándose en el sector de la energía, principalmente en Norteamérica y Europa. Este grupo parece estar siguiendo los pasos de la amenaza Stuxnet, nuevamente apuntando a organizaciones que usan sistemas de control industriales (ICS). Su objetivo principal parece ser el espionaje; sin embargo, sus ataques contra ICS le brindan la capacidad de organizar operaciones de sabotaje que podrían haber interrumpido el suministro de energía en varios países europeos. Se les atribuyen los cortes de energía que hubo en Ucrania en los años 2015 y 2016 que afectaron a cientos de miles de personas.

Dragonfly aprovecha dos componentes fundamentales de un programa malicioso: herramientas de acceso remoto y obtener acceso a equipos infectados y controlarlos. Dragonfly también ha refinado el uso de los tres métodos principales de implementación de su malware: correos electrónicos infectados, sitios web en peligro, y programas maliciosos introducidos en paquetes de software legítimos de otros fabricantes.

- **Tenían la capacidad de organizar operaciones de sabotaje para interrumpir el suministro de energía en varios países.**
- **Aprovechan 2 componentes: herramientas de acceso remoto y el control a equipos infectados.**

> **Una de las peculiaridades de Industroyer es que utiliza cuatro componentes maliciosos para obtener el control directo de los interruptores y disyuntores de una subestación eléctrica.**

Industroyer, el siguiente paso en malware.

En el informe que ESET acaba de publicar sobre la amenaza Industroyer se reveló que fue el malware escogido por el grupo de hackers Dragonfly, y no el malware BlackEnergy, como responsable de los apagones en Ucrania en diciembre de 2016.También vemos con detalle lo avanzado de este malware modular y que, en lugar de infectar los sistemas de control industrial usados en centrales eléctricas, utiliza los protocolos de comunicación industrial para realizar acciones maliciosas. Estos protocolos se crearon hace décadas y en ese momento no se pensó en la seguridad lógica, puesto que la idea era que los sistemas industriales estuvieran aislados del mundo exterior. Por ese motivo, los atacantes que utilizaron Industroyer no necesitan buscar vulnerabilidades en los protocolos, tan solo deben enseñar al malware a hablar el mismo lenguaje que esos protocolos.

Una de las peculiaridades de Industroyer, que lo distingue de otras familias de malware que también tienen como objetivo infraestructuras críticas, es que utiliza cuatro componentes maliciosos para obtener el control directo de los interruptores y disyuntores de una subestación eléctrica. Cada uno de estos componentes está pensado para afectar a un protocolo de comunicación industrial, protocolos que vienen especificados en unos estándares accesibles de forma pública. Lo que hace realmente peligroso a Industroyer (a diferencia de Stuxnet, que estaba pensado para atacar un objetivo en concreto) es que puede ser utilizado para atacar prácticamente cualquier sistema de control industrial que utilice los protocolos de comunicación implementados a nivel mundial en infraestructuras de todo tipo, entre las que se incluyen las de suministro de energía eléctrica, sistemas de control de transporte y otros sistemas encargados de gestionar el abastecimiento de agua o gas, por poner solo unos ejemplos.

- **Utiliza los protocolos de comunicación industrial para realizar ciberataques sin necesidad de buscar las vulnerabilidades.**
- **Usa cuatro componentes maliciosos para controlar los interruptores y disyuntores de una subestación eléctrica.**
- **Puede ser utilizado para atacar prácticamente cualquier sistema de control industrial que utilice los protocolos de comunicación implementados a nivel mundial.**

Retail

Los ataques en los últimos años a comercios minoristas se han duplicado con respecto a los del año anterior debido a que los hackers los consideran un buen blanco para sus ataques, sobre todo para obtener las bases de datos de los usuarios de los comercios.

Redoblar esfuerzos en esta materia es una necesidad y además, la ciberseguridad se convierte en un factor de decisión importante para los consumidores vía online. Así se refleja en el informe anual de Capgemini sobre este sector, donde un 77% de los comercios consideran un factor clave la privacidad de los datos. De hecho, en algunos países, como en la India, es incluso el factor nº1 que consideran a la hora de comprar: el 40% de los consumidores incrementaría su gasto online en un 20% si estuvieran tranquilos con la seguridad de sus datos. Esto convierte la ciberseguridad en una oportunidad para los comercios que implementen y demuestren un entorno de compra más seguro. Por ejemplo, la encriptación en los datos incrementa hasta un 140% la percepción de calidad del usuario, mientras que solo un 48% de los comercios han implementado soluciones de este tipo.

Un 77% de los comercios consideran un factor clave la privacidad de los datos de sus consumidores.

Debilidades del retail online

Las amenazas van ligadas a las vulnerabilidades propias del sector:

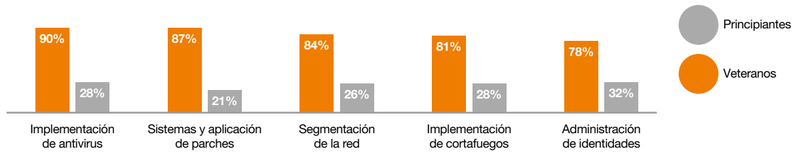
- **La inclusión de nuevas tecnologías como Internet of Things (IoT).**
- **Retraso en el cumplimiento de las normas de seguridad.**
- **Arquitectura de sistemas obsoleta.**
- **Ausencia de productos antimalware suficientemente avanzados.**
- **Ausencia de defensas adecuadas para medios de pago y puntos de venta.**

Las empresas más veteranas cuidan más la seguridad de sus negocios, casi un 90% de esas compañías cuentan con antivirus en sus equipos.

Sin embargo, los principiantes olvidan muy a menudo implementar soluciones y solo un 28% de estos nuevos negocios están equipados con algún antivirus. La diferencia es importante en casi todas las soluciones de seguridad informática.

Tipo de protección en las empresas

Fuente: Capgemini may 2018



Solo un 28% de los nuevos negocios están equipados con algún antivirus.

El comercio minorista

Las claves para el comercio minorista están en cuidar algunos detalles, como afirma John Lewis, experto en seguridad europeo que considera que “la principal amenaza es la apatía”.

Las claves son:

- Utilizar la nube (combinada con lo físico y almacenamiento propio) para dispersar el riesgo.
- Subcontratar ciberseguridad, ya que es importante que la gestione un experto.
- Tener una adecuada política de seguridad de la información.
- Cumplir estándares de seguridad de datos, como PCI DSS.
- Tender hacia el software libre, menos vulnerable y actualizado.
- Añadir sistemas de autenticación avanzados, más allá del usuario y password.
- Encriptación de datos que sean enviados entre un sistema y otro.
- Formar a los empleados.
- Exigir a los partners el cumplimiento de medidas de seguridad.
- Manejar adecuadamente la omnicanalidad de clientes, para evitar la fuga o pérdida de datos privados.

Este sector está expuesto como todos a la ciberdelincuencia y no deben dejarse de lado todas las acciones encaminadas a proteger los datos de los clientes, que en este caso son el principal objetivo de los ataques.

Por ello, un 54% de las empresas ya han aumentado su inversión para 2018 en ciberprotección. Entrando en detalles, el 64% invirtió concretamente en nuevas tecnologías, el 33% apostó por la formación de sus empleados y contrató a expertos, y finalmente el 21% contrató un seguro de ciberseguridad.

Home Depot y el robo de decenas de millones de datos de clientes.

Uno de los casos más conocidos del sector retail es el de Home Depot, que expuso los datos de sus clientes a los ciberatacantes. En concreto, afectó a todos los clientes que compraron entre abril y septiembre de 2014 en más de 4.000 tiendas que tienen desplegadas entre USA y Canadá. La intrusión duró 5 meses sin ser detectada, y facilitó a los hackers los datos de tarjetas de crédito y datos personales de 70 millones de clientes. Aunque más grave fue el silencio que mantuvo la empresa hasta que sus propios empleados informaron a investigadores externos del problema. Habían encontrado una variante de BlackPOS en sus sistemas, la misma que había robado datos a Target, otro de los casos más conocidos de hackeo en el sector, que sucedió en 2013. Se detectó el ataque a partir de una serie de bugs (errores de software) que provocaron un mal funcionamiento en el sistema operativo Windows que usaba la empresa.

- **Home Depot expuso los datos de sus clientes a los ciberatacantes.**
- **La intrusión duró 5 meses sin ser detectada.**

Contact Center y recobros

Los Contact Centers son otro de los blancos interesantes para los hackers, ya que almacenan gran cantidad de información sensible de los usuarios, especialmente si realizan pagos con tarjeta.

El gran número de empleados que tiene acceso a estos datos abre mucho más el abanico de posibilidades de fuga de datos interna. Aunque los empleados sean leales y el sistema sea seguro, a todos nos asalta cierta inseguridad cuando tenemos que indicar por teléfono el número de tarjeta, la fecha de caducidad y el CVV. Por eso existen protocolos que permiten certificar el buen uso de esta información dentro de los Call Centers. Pero la norma deben cumplirla todos los eslabones de la cadena de tratamiento de los datos, lo que hace que sea un proceso complejo, costoso y de difícil implementación.

Debido a la inseguridad que sienten los usuarios al dar sus datos, se han desarrollado protocolos que permiten certificar el buen uso de esta información en los Call Centers.

Una de las soluciones en materia de ciberseguridad son las relacionadas con el tratamiento de los datos a través de plataformas de Respuesta de Voz Interactiva (IVR). Se trata de una plataforma que en el momento del pago deriva la llamada a una pasarela donde el cliente puede escuchar el contexto de su transacción y teclear los datos sensibles de su tarjeta en el teclado de su terminal, evitando el cruce de esta información por voz. Finalmente los datos son encriptados y los agentes del Call Center no tienen ningún contacto con ellos en todo el proceso, aunque sí pueden seguir la ejecución del pago para facilitar el servicio contratado. Esta solución ayuda al cumplimiento de la normativa PCI DSS y además ha aumentado las tasas de recobro en un 10-15%.

La seguridad en los datos

La normativa PCI DSS establece un estándar de seguridad en los datos para la industria de tarjetas de pago que obliga a:

- Desarrollar y mantener una red segura.
- Proteger los datos de los propietarios de tarjetas.
- Mantener un programa de gestión de vulnerabilidades.
- Implementar medidas sólidas de control de acceso.
- Monitorizar y probar regularmente las redes.
- Mantener una política de seguridad de la información.

Esta validación es realizada por auditores autorizados, aunque si hacen menos de 80.000 operaciones al año, tienen la opción de realizar una autoevaluación con un cuestionario.

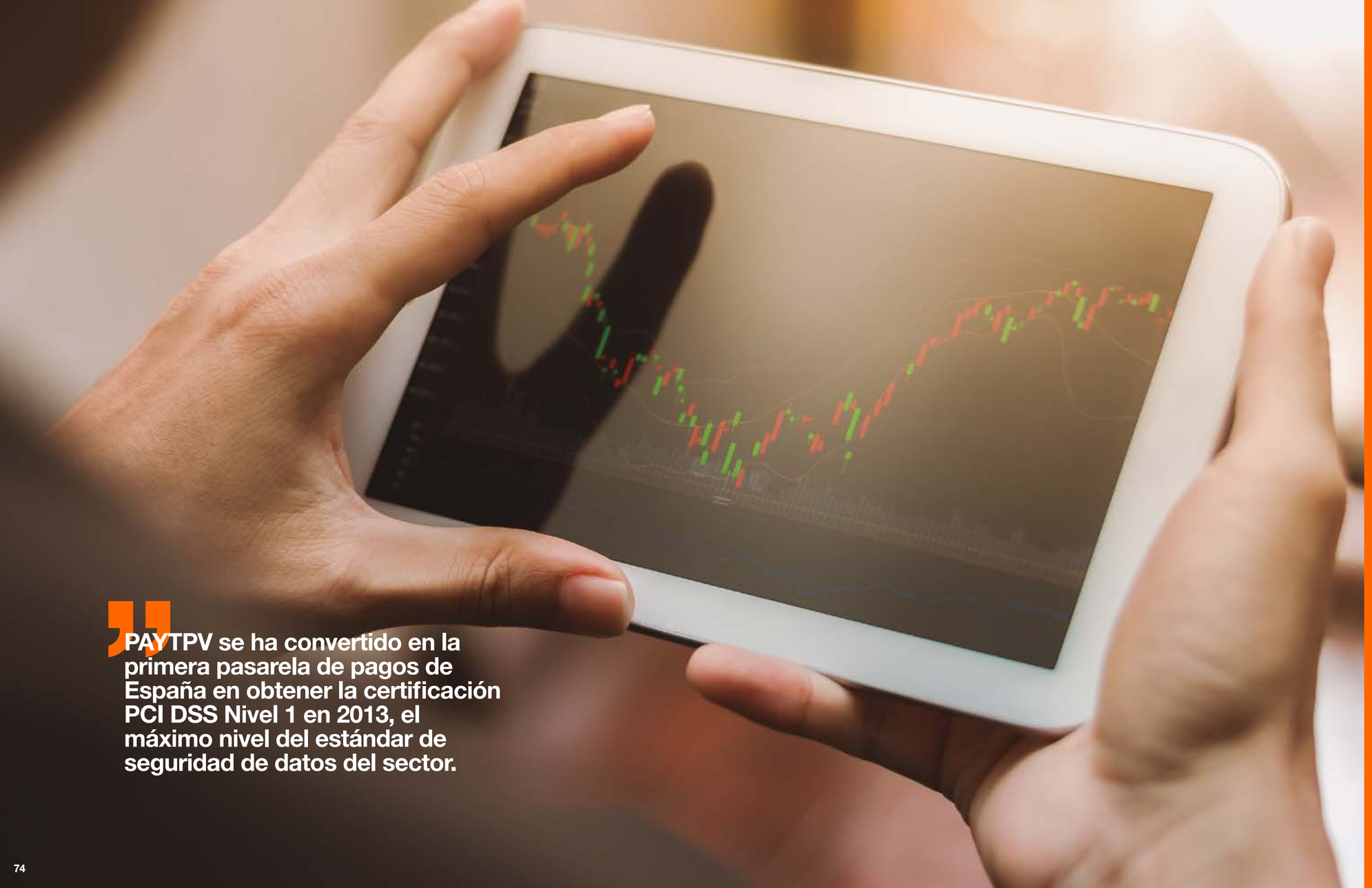
“La industria de tarjetas está obligada a mantener una red segura para proteger los datos.

> La fuga de datos costó a AT&T una multa de 22 millones de euros.

AT&T y el robo de datos a su proveedor Contact Center.

El Contact Center proveedor de AT&T fue atacado y los hackers se apropiaron de más de 280.000 registros de clientes con números de la Seguridad Social y datos personales. Actuaron sobre varios países, concretamente Filipinas, México y Colombia. La ausencia de sistemas de monitorización fue la causa de este ataque, además de la falta de control del personal contratado, pues el causante tenía antecedentes. La fuga de datos costó a la empresa una multa de 22 millones de euros y la información se utilizó para desbloquear dispositivos robados que eran enviados a México. Desde allí se utilizaban los datos para cambiar el número de serie del dispositivo y poder revenderlo. Aunque solo fueron detenidos empleados del proveedor del Call Center, el caso provocó el despido final de 800.

- **Los hackers se apropiaron de más de 280.000 registros de clientes con números de la seguridad social y datos personales.**
- **La ausencia de sistemas de monitorización y la falta de control del personal fue la causa de este ataque.**



> **PAYTPV se ha convertido en la primera pasarela de pagos de España en obtener la certificación PCI DSS Nivel 1 en 2013, el máximo nivel del estándar de seguridad de datos del sector.**

PAYTPV, una solución PCI DSS a la española.

La plataforma de pagos PAYTPV se creó en 2010 y opera como un proveedor de soluciones de pago pionero en innovación, apostando por la seguridad de las transacciones como eje de su estrategia. Prueba de ello es que fue, en 2013, la primera pasarela de pagos de España en obtener la certificación PCI DSS Nivel 1, el máximo nivel del estándar de seguridad de datos del sector. A finales de 2018 InnoCells, el hub de negocios digitales y corporate venture de Banco Sabadell, adquirió la plataforma que posteriormente ha pasado a llamarse PAYCOMET.

Entre sus soluciones destacan el TPV virtual para pagos en comercio electrónico; el servicio IVR para cobros automáticos en Call Centers, o la tokenización de tarjetas para sistemas de reservas hoteleras. Todas las soluciones que permiten procesar pagos 3D Secure están adaptadas a la normativa PSD2.

Coincidiendo con el cambio de marca, PAYCOMET integra en su oferta una nueva solución dirigida a marketplaces y plataformas online. Se trata de un servicio diseñado para poder retener y distribuir los depósitos de las transacciones realizadas entre vendedores y compradores. Para ofrecer este servicio es imprescindible contar con una licencia de Entidad de Pagos del Banco de España, según la ley europea conocida como PSD2, que PAYCOMET tiene desde 2017. En 2018 la plataforma procesó cerca de 500 millones de euros en operaciones.

- **Opera como proveedor de soluciones de pago, apostando por la seguridad de las transacciones como eje de su estrategia.**
- **Cuenta con la certificación PCI DSS Nivel 1 y con una licencia de Entidad de Pagos del Banco de España, además de tener sus soluciones adaptadas a la normativa PSD2.**

Salud

El sector salud recibe un 340% más de ciberataques que otras industrias y en uno de cada 600 ataques está involucrado algún malware avanzado.

El sector sanitario tiene un 64% más probabilidades de sufrir un ataque, en concreto phishing. La Asociación Médica Mundial ya está alertando sobre los ciberataques a las instituciones de salud, sobre todo en la proliferación de los registros médicos electrónicos y los sistemas de facturación. Las instituciones y los asociados comerciales, desde la más pequeña consulta privada hasta los más grandes hospitales, son vulnerables no solo al robo, alteración y la manipulación de registros electrónicos médicos y financieros de los pacientes, sino también a intrusiones en sofisticados sistemas que pueden poner en peligro la capacidad para atender a pacientes y responder a urgencias médicas.

La amenaza puede ir desde el robo del historial médico hasta una modificación de los ajustes en los equipos, poniendo en peligro a los pacientes.

Cada equipo médico conectado a Internet puede ser blanco de ciberataques, según alertó este mismo año el Ministerio de Emergencias de Rusia. La amenaza puede variar desde el robo del historial médico hasta una modificación de los ajustes en los equipos que pondría en peligro la vida de los pacientes. El Kremlin señaló que la lucha contra las amenazas en Internet no debe violar libertades e indicó que el mayor peligro surge cuando los piratas informáticos se alían con los terroristas para llevar a cabo ciberataques masivos contra infraestructuras energéticas, redes de comunicación y todos aquellos sistemas vitales que podrían producir emergencias y catástrofes tecnológicas con numerosas víctimas. En 2017 se multiplicaron por cuatro los ciberataques a los sistemas informáticos de Rusia, la mayoría mediante virus extorsionadores (36%), seguido de las brechas que dejan vulnerabilidades (26%) y los ataques DDoS de denegación de servicio (8%).

El Blockchain resuelve el principal riesgo de la información médica: la seguridad e inviolabilidad de los datos del paciente.

Qué atacan en un centro de salud

Dentro del sector sanitario encontramos una multiplicidad de infraestructuras de tecnología de la información que pueden ser intervenidas, como los programas de imágenes en radiología, sistemas de videoconferencias, cámaras de vigilancia, dispositivos móviles, impresoras y sistemas de vídeo digitales utilizados para el control en tiempo real y procedimientos remotos. Pero no solo estos dispositivos son sensibles a los ataques, objetos como marcapasos, wearables que monitorizan el estado físico de pacientes, prótesis artificiales conectadas, implantes inteligentes o realidad aumentada utilizada para mejorar capacidades, también son susceptibles de sufrir algún ciberataque.

Tecnología como Blockchain resuelve con su operativa el principal riesgo y problema dentro del ámbito de información médica: la seguridad e inviolabilidad de los datos recogidos en sistemas integrales que recopilan toda la información médica de los pacientes. Además, permite compartir de forma segura la información entre todo el personal sanitario. Un ejemplo de uso es la alianza entre la Administración de Alimentos y Medicamentos de Estados Unidos (FDA) e IBM Watson Health para explorar el uso de Blockchain en el uso compartido de información médica. El convenio incluye el intercambio de datos de pacientes procedentes de varias fuentes, incluyendo registros médicos electrónicos, ensayos clínicos, datos genómicos y datos de salud procedentes de dispositivos móviles, wearables e Internet of Things.

Otro ejemplo es el acuerdo firmado entre Alibaba Health Information Technology y el Gobierno chino, que pretende almacenar los datos del sistema de salud a través de Blockchain. La empresa tecnológica pretende conectar la infraestructura médica con el sistema de tratamiento médico. Los médicos autorizados serán instantáneamente informados del historial médico del paciente y de cualquier información sobre los exámenes de salud. Esto ayudará a los médicos a evitar cualquier repetición de exámenes básicos de salud para brindar atención al paciente de una manera más rápida, eficiente y más barata.

> **Los marcapasos de Abbott Laboratories sufrieron un fallo en el firmware que permitió hackear los dispositivos.**

Abbott Laboratories y las actualizaciones de sus marcapasos.

Un fallo en el firmware de los marcapasos, que comercializaba Abbott Laboratories en USA, produjo un agujero de seguridad que permitió hackear los dispositivos. Para solucionarlo, la empresa lanzó una actualización que permitía instalar un parche con un software interno de cifrado de datos para evitar intromisiones y posibles ciberataques a más de 465.000 pacientes.

El laboratorio, nada más conocer el error, advirtió en un comunicado abierto a los médicos: en caso de ataque, un individuo no autorizado podría obtener acceso y emitir órdenes al implante a través de la transmisión de radiofrecuencia. Finalmente, recomendaron a los usuarios visitar su clínica habitual para que el médico ponga los dispositivos en modo copia, cerrando la brecha de seguridad en apenas 3 minutos.

- **En caso de ataque, un individuo no autorizado podría obtener acceso y emitir órdenes al implante.**
- **El agujero de seguridad se solucionó con un software interno de cifrado de datos que evita las intromisiones.**

Gobierno

La ciberseguridad es para los gobiernos una cuestión de defensa nacional. Un informe realizado por la empresa McAfee sobre seguridad informática a 23 países, destacó que Israel, Finlandia y Suecia son los países más avanzados, mientras que México, China y Brasil fueron los más débiles ante un posible ciberataque.

Por otro lado, la ciberdefensa se enfrenta a numerosas ambigüedades ya que puede ser considerada como una estrategia militar que permite debilitar al adversario o como la defensa de las infraestructuras vitales del Estado y de sus informaciones. Como primer paso, los gobiernos tienen que aprender a prever y a detectar una amenaza; todavía les falta ir un paso por delante de los cibercriminales. Desde los gobiernos el reto consiste en intensificar la cooperación, impulsar políticas de mejora y lograr una mayor resistencia cibernética.

Las acciones a considerar:

- Comenzar a adoptar estándares de seguridad para este sector.
- Definir políticas de seguridad.
- Implementar metodologías.
- Comenzar a concienciar sobre los riesgos de seguridad, al tiempo que se capacita al personal.
- Monitorizar desde el punto de vista de la seguridad y crear inteligencia que permita compartir conocimiento y experiencias.

> **El reto de los gobiernos consiste en intensificar la cooperación, impulsar políticas de mejora y lograr una mayor resistencia cibernética.**

Israel: un país cibersecurizado.

Israel, desde su fundación en 1948, ha estado enfrentado a los países de su entorno. El sector de defensa es muy avanzado, pero especialmente en ciberdefensa, tanto que ha desarrollado una potente industria que exporta a los 5 continentes. Hasta la OTAN ha decidido priorizar este segmento en su estrategia de defensa. En Israel colaboran el sector público, privado y las fuerzas de defensa con epicentro en la Universidad Ben-Gurión, en la ciudad de Beerseba, donde se forman a las mentes más privilegiadas en seguridad informática, cerebros que luego lideran las empresas especializadas y startups dentro del país.

En Israel se facturaron más de 5.100 millones de euros anualmente en ciberseguridad y el 20% de las empresas mundiales de seguridad se encuentran ubicadas en este país. Las claves de su avance en esta materia son tener uno de los mejores escudos de seguridad del mundo, la colaboración sin restricciones entre universidad, empresas y gobierno, y contar con un organismo nacional (similar al Centro Criptológico Nacional -CERT- español) cuya misión es proporcionar seguridad informática a todo el país.

- **Colaboran el sector público, privado y las fuerzas de defensa.**
- **El 20% de las empresas mundiales de seguridad se encuentran ubicadas en Israel.**

Israel posee uno de los mejores escudos de seguridad del mundo debido a la colaboración sin restricciones entre universidad, empresas y gobierno.

A Hidden Cobra se le atribuye el ataque a Sony en 2014, el robo de 89 millones de euros al banco de Bangladesh en 2016, y la difusión del ransomware WannaCry.

Operación “Hidden Cobra” desde Corea del Norte.

Tras las investigaciones realizadas por el FBI y el departamento de seguridad nacional estadounidense, se desveló que el grupo de hackers denominado Hidden Cobra, también conocido como Lazarus Group y Guardians of Peace, ha sido el responsable de los ataques de seguridad realizados a grandes empresas en Estados Unidos desde el año 2009. Se les atribuye el ataque a Sony en 2014 (mediante el gusano Wiper, con capacidad para sobrescribir las unidades de disco de los PCs dejándolos inoperativos), el robo de 89 millones de dólares al banco de Bangladesh en 2016 (posiblemente a través del troyano de acceso remoto Win32/Agent.XZH), y la difusión del ransomware WannaCry entre otros ciberdelitos. La operación BlockBuster realizada por empresas de ciberseguridad como Novetta, Kapersky Lab y Alienvault consiguió desmontar sus herramientas y descubrir el origen de todos estos incidentes, siguiendo sus denominadores comunes para finalmente detectar la autoría.

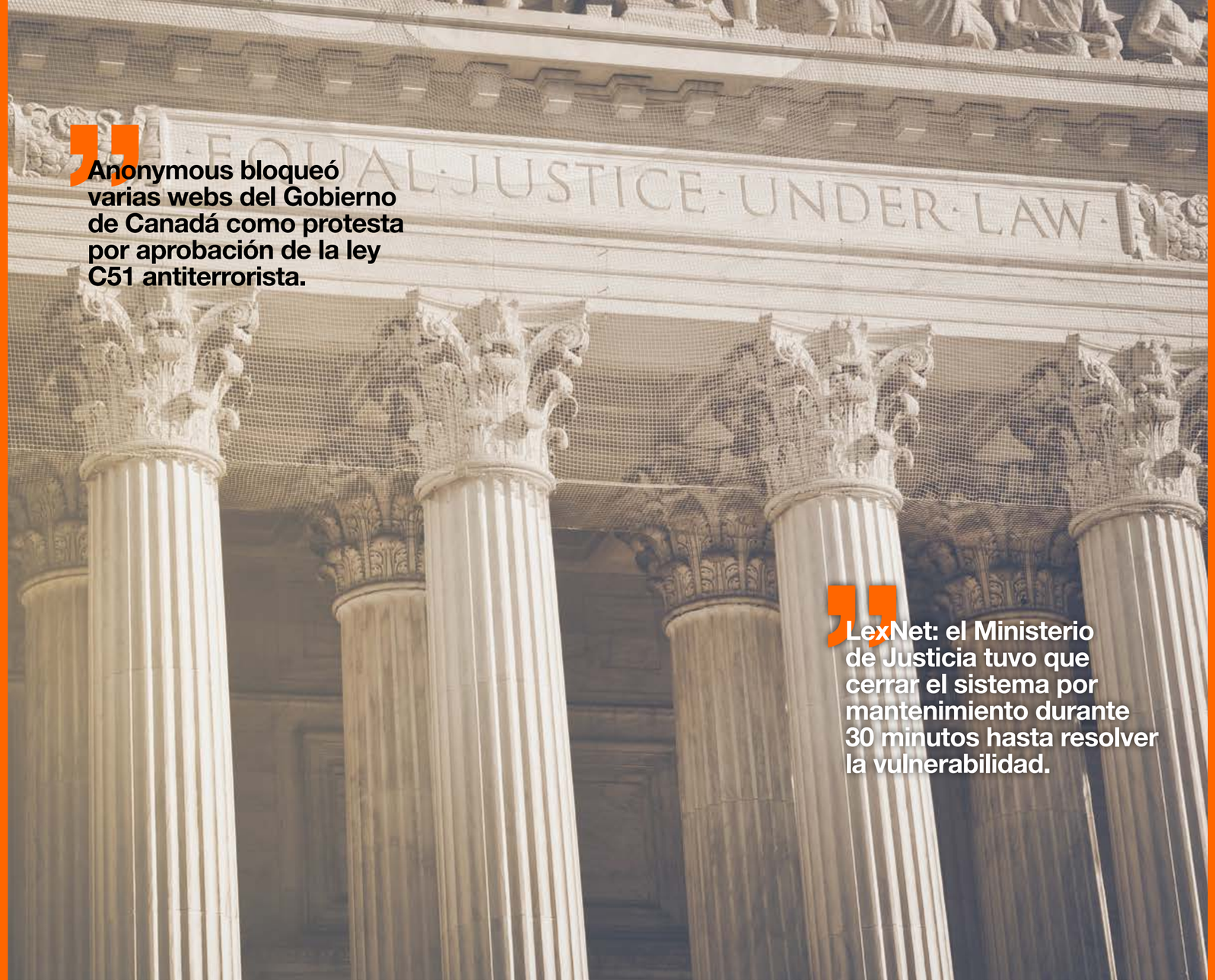
- **Son responsables de los ataques de seguridad realizados a empresas en USA desde 2009.**
- **Novetta, Kapersky Lab y Alienvault consiguieron descubrir el origen de todos los ataques.**

Anonymous: contra la ley C51 del gobierno canadiense.

Tras el anuncio del gobierno de Canadá de poner en marcha la llamada ley C51 antiterrorista (ley que extiende el poder de sus servicios de inteligencia, con el objetivo de luchar contra el terrorismo y que, entre otras cosas, permite a las autoridades realizar un amplio control de las actividades en Internet), los ciberactivistas de Anonymous iniciaron acciones contra ese gobierno, alegando el recorte de libertades básicas que supone para las personas. Se bloquearon distintas webs gubernamentales, incluidas la del Senado, el departamento de Justicia, y las agencias de espionaje canadienses CSEC y CSIS.

Las webs funcionaban de forma intermitente y sus responsables comentaron que los datos no estaban en riesgo, pero durante un tiempo reconocieron tener problemas para acceder a su correo. Además, se bloquearon las consultas telefónicas y como consecuencia, el gobierno decidió incrementar los recursos destinados a ciberseguridad.

- **Las webs funcionaban de manera intermitente pero los datos no estaban en riesgo.**
- **En consecuencia, el Gobierno decidió incrementar los recursos destinados a ciberseguridad.**



Anonymous bloqueó varias webs del Gobierno de Canadá como protesta por aprobación de la ley C51 antiterrorista.

LexNet: el Ministerio de Justicia tuvo que cerrar el sistema por mantenimiento durante 30 minutos hasta resolver la vulnerabilidad.

LexNet y el acceso a todos los casos judiciales.

En enero de 2016, el Ministerio de Justicia en España implantó LexNet, un software de administración para notificaciones entre todos los juzgados y profesionales. Por un error en la definición inicial del sistema se pudo acceder a todos los casos abiertos, desde la Gürtel a cualquier pleito local. El Ministerio tuvo que cerrar el sistema por mantenimiento durante 30 minutos hasta resolver la vulnerabilidad, pero el caso tuvo una especial repercusión entre el gremio, donde exigían la dimisión del Ministro, teniendo en cuenta los fallos del sistema desde que se implantó. Se convierte en un error de filtración de información comprometida y muy relevante que pone de manifiesto la importancia de la ciberseguridad para las Administraciones Públicas. El origen se ha situado en una actualización que causó el fallo y que incluía un defecto en el control de accesos por un error en la programación del código.

- **Un error en la definición inicial del sistema permitió el acceso a todos los casos abiertos.**
- **El caso tuvo una especial repercusión entre el gremio, donde exigían la dimisión del ministro.**

Ámbitos de alcance de la ciberseguridad

Ante la realidad de los incidentes en ciberseguridad, los protocolos de actuación se han modernizado y transformado para ser capaces de responder, clasificar y mitigar cualquier tipo de ciberataque.

ANTES

Medidas de seguridad
- Política de seguridad
- Normas de seguridad
- Medidas organizativas
- Medidas ISO 27001

Cifrado de datos y seudonimización
- Datos ininteligibles
- Clave bien custodiada
- Datos disociados
- Intencionalidad

Plan de actuación ante un incidente
- Protocolo de actuación
- Responsables
- Tiempo de respuesta

DESPUÉS

Análisis del incidente
- Alcance
- Número de afectados
- Origen
- Intencionalidad

Evaluación del riesgo
- Tipo de violación de la seguridad
- Sensibilidad de los datos
- Gravedad del impacto para los afectados
- Facilidad de identificación

Decisión final
- Riesgo bajo: no notificar
- Riesgo alto: notificar a la AEPD
- Riesgo muy alto: comunicar a los afectados

Prevención

¿Es la prevención la cuenta pendiente para las empresas en materia de ciberseguridad?

La prevención cuesta dinero, y mantener los sistemas a salvo de cualquier futuro problema es una quimera, ya que no existe un antivirus perfecto, ni el jefe de seguridad perfecto. Todas las empresas están expuestas a posibles ataques. Son las grandes empresas las que invierten más en prevención, y siguen expuestas a nuevos ataques. Las soluciones de prevención se basan en soluciones antifraude, antimalware, fuga de información, protección de las comunicaciones y protección de dispositivos móviles. Además, aparecen en el mercado más feeds y espacios donde es posible compartir información y prevenir los ataques.

Las soluciones de prevención se basan en soluciones antifraude, antimalware, fuga de información, protección de comunicaciones y de los dispositivos móviles.

La ciberseguridad lidera la inversión en formación en las grandes empresas con un (69%), seguida de la atención al cliente (65%) y por último el Cloud & Virtualización (63%).

Servicios de protección

Algunos ejemplos de infraestructura y de servicios con los que cuentan los sistemas, y que están enfocados a evitar el problema antes de que se produzca, son:

- Cortafuegos
- Antivirus, Antispam, Antiphishing, Antiadware, Antispyware
- Filtrado de navegación
- UTM (Unified Threat Management)
- ILM (Information Lifecycle Management)
- Cifrado
- VPN
- Seguridad en la web
- Seguridad en el correo

Uno de los aspectos clave en la prevención de ataques para las empresas es la formación a los empleados, y en algunos sectores como en la banca, a los propios clientes. La ciberseguridad lidera la inversión en formación en las grandes empresas con un (69%), seguida de la atención al cliente (65%) y por último el Cloud & Virtualización (63%). Sin embargo hay que destacar que no hay un responsable con formación específica en estas disciplinas clave para la transformación digital, una situación que afirman con un 40% y 60% las empresas españolas, así como un 70% de los directivos consideran que no reciben la formación necesaria para competir con garantías de éxito en un entorno cada vez más digital y global.

El Estado Mayor de la Defensa en España puso en marcha una campaña para la concienciación en materia de ciberseguridad, con consejos y advertencias básicas para evitar los ciberataques.

Campañas de concienciación

El Estado mayor de la Defensa en España incluso encargó una campaña a una agencia de marketing para la concienciación en materia de ciberseguridad con una serie de acciones de comunicación centradas en consejos y advertencias básicas para poner coto a los ciberataques. Los ámbitos de esta campaña iban desde la concienciación general, hasta información sobre la identificación y credenciales de acceso, navegación por Internet, correo electrónico, servicios en la nube, actividad en redes sociales, USB y otros soportes de información, protección del entorno doméstico, prevención y reacción ante los incidentes, y movilidad fuera de la oficina.

La gran mayoría de las incidencias en ciberseguridad tienen su origen en una mala actuación por parte de algún empleado o partner.

Las claves en la prevención en 2018 estuvieron marcadas en la prestación de servicios más accesibles y ágiles, en concienciar y formar a las personas. La gran mayoría de las incidencias en ciberseguridad tienen su origen en una mala actuación por parte de algún empleado o partner, que son evitables con medidas preventivas.

Imagine with Orange: convocatoria de ideas sobre ciberseguridad.

Iniciativas como la de Imagine with Orange, donde se lanzan concursos de ideas, y en particular sobre ciberseguridad, permiten que aflore el talento y se presenten ideas de emprendedores para la mejora en todos los frentes del sector y desde personas ubicadas en todo el mundo. Los expertos saben que el talento y la innovación dependen en gran medida de las iniciativas de startups y emprendedores, y es un acierto atraer estos perfiles a la empresa para colaborar en el desarrollo de mejores soluciones.

Otras iniciativas de la empresa en este sector son la compra de Lexsi en 2016, empresa especializada en ciberseguridad que cuenta con más de 1.000 empleados, y de SecureData, proveedor británico de servicios de ciberseguridad.

Además, desde la compañía también se fomenta el uso seguro de Internet a través de iniciativas dirigidas a poner a disposición de padres y educadores, mecanismos de control de acceso, clasificar los contenidos, luchar contra los contenidos ilegales, y proporcionar información y consejos de uso responsable de los servicios de telecomunicaciones.

- **Ideas de emprendedores para la mejora en todos los frentes del sector.**
- **Desde la compañía también se fomenta el uso seguro de Internet con iniciativas que se ponen a disposición de padres y educadores.**

El talento y la innovación dependen en gran medida de las iniciativas de startups y emprendedores.

Secur@ Index efectúa una auditoría con el objetivo de incrementar el nivel de protección de datos en las empresas.

Test de ciberseguridad de Bankia para las empresas.

La entidad financiera Bankia, consciente del problema que supone la ciberseguridad para las empresas, que no cuentan con presupuestos tan abultados como las grandes corporaciones para protegerse del cibercrimen, ha lanzado una herramienta de autoevaluación de ciberseguridad. Con este test, podrán conocer el nivel de seguridad que protege su información digital, así como las mejoras que podrían realizar y llevar a cabo para una gestión correcta de los riesgos digitales.

La herramienta, denominada Secur@ Index, consiste en un cuestionario que permite efectuar una auditoría sobre la seguridad informática de la empresa, con el objetivo de incrementar el nivel de protección de sus datos y detectar los ámbitos donde se podrían reforzar los sistemas. Esta iniciativa de Bankia prevé que las empresas pongan en marcha procesos para prevenir riesgos de ataques cibernéticos, y un plan de acción para gestionarlos, al añadir información sobre las principales medidas de protección existentes.

- **Herramienta de autoevaluación de ciberseguridad.**
- **Bankia prevé que las empresas pongan en marcha procesos para prevenir riesgos de ataques cibernéticos.**

Control

La monitorización en tiempo real de la actividad en la red y la gestión de alertas de seguridad son una pieza clave para el control de sistemas debido a que los ataques pueden producirse de forma indiscriminada y de manera continua.

Sin embargo, las compañías investigan solamente el 56% de las alertas que reciben, dejando el resto sin revisar. Además, de las incidencias investigadas, el 34% son legítimas, y de ellas, casi la mitad (el 49%) se quedan sin remediar. Las herramientas de control en ciberseguridad tratan un gran volumen de datos, logs de actividad, y deben detectar entre ellos un posible ataque o patrón de comportamiento inadecuado. Para dar soluciones a esta gestión de información aparecen en el mercado herramientas de visualización de datos que facilitan esta labor como son Tableau Software, Word2vec, Vizipedia o DataViz. Frente a estas herramientas más operativas y complejas aparecen en el mercado otras soluciones que nos permiten integrar varias fuentes distintas, como Kilpfolio o Zeus, con las que elaborar un dashboard de control de manera ágil e intuitiva.

El perfil profesional del experto en visualización de datos ya es una realidad y hay una gran demanda en las empresas. Eso sí, debe aunar una serie de conocimientos y aptitudes, como son user experience, diseño de aplicaciones, manejo de redes neuronales y de programación y desarrollo, algo difícil de encontrar actualmente.

> **Las compañías investigan solamente el 56% de las alertas que reciben, dejando el resto sin revisar.**

6.3

Mitigación

Lo que no se haya podido prevenir y erradicar antes, requiere una mitigación y recuperación tras las consecuencias que haya provocado el ciberataque.

Entre las posibles acciones de mitigación y recuperación ante un ciberataque encontramos:

- Planes de contingencia y continuidad.
- Herramientas de recuperación de sistemas.
- Backups y copias de seguridad.
- Infraestructuras de respaldo.
- Ciberseguros.
- SIEM (Security Information and Event Management).
- Soluciones Big Data.

La mitigación de los ataques también requieren de soluciones ágiles y versátiles para poder llegar a restaurar y recomponer la información. De esta manera se facilita la disponibilidad del sistema cuanto antes e incluso con el mismo nivel de rendimiento previo a los ataques.

"La mitigación de los ataques requieren de soluciones ágiles y versátiles para poder llegar a restaurar y recomponer la información.

Reactivación del negocio.

Los planes de contingencia y continuidad permiten reactivar el negocio lo antes posible, con la tranquilidad de haber realizado los pasos en el orden adecuado. Aun así, más de un 40% de las empresas no tienen definido un plan de actuación ante una crisis de ciberseguridad y el 60% que sí lo tiene, no siempre cumplen con todas las mejores prácticas que un plan de crisis requiere.

¿Tiene algún plan de respuesta en caso de una emergencia de ciberseguridad? En caso afirmativo, ¿su plan incluye alguna de las siguientes prácticas?

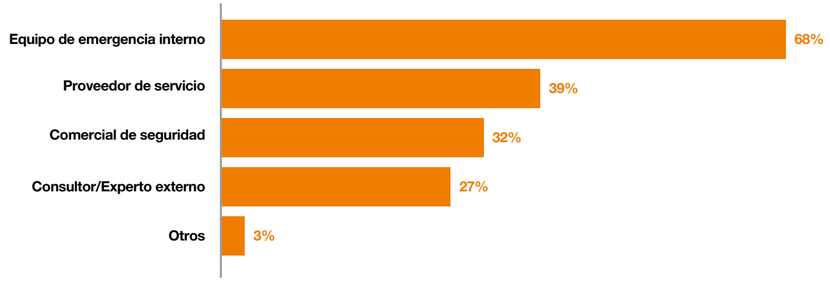
Enterprise Resource Plan	Total
No	**40%**
Sí	**60%**
Recolección y análisis de datos	53%
Copia de seguridad de los procedimientos de emergencia	52%
Notificaciones de e-mail para clientes y socios	51%
Simulacros de escenarios de emergencia	43%
Usar un sistema SIEM para alertas	42%
Crear un comité de emergencia con expertos en seguridad	40%
Autosincronización con DRC para proteger los datos	32%
Comunicación externa vía RRSS y/o web de la compañía	29%
Desvío del tráfico no deseado (RTBH)	23%
Bitcoin en mano en ataques ransom	7%
Otros	4%

Fuente: Radware, Global Application & Network Security Report 2016-2017.

Proveedores externos

La mitigación en muchos casos depende de empresas externas y aunque un 68% tiene un equipo interno preparado para contingencias, casi siempre está compuesto por personal de IT y no personal específico. La realidad es que existen porcentajes muy grandes de empresas que se apoyan en proveedores externos, y en los que delegan esta responsabilidad.

¿A quién recurren las empresas en caso de ciberataque?



Fuente: Radware, Global Application & Network Security Report 2016-2017.

Las entidades financieras han lanzado nuevos productos orientados a dar una cobertura que cubra las consecuencias de sufrir un ciberataque.

Pólizas para ataques

En ciberseguros, las entidades financieras lanzan nuevos productos orientados a dar cobertura a este tipo de incidencias. Además de los clásicos productos de responsabilidad civil, aparecen coberturas para crisis de reputación o para compensar indisponibilidad de sistemas.

Empresas como BitSight o SecurityScorecard están creciendo y son cada vez más relevantes en el panorama de la gestión de ciber-riesgos.

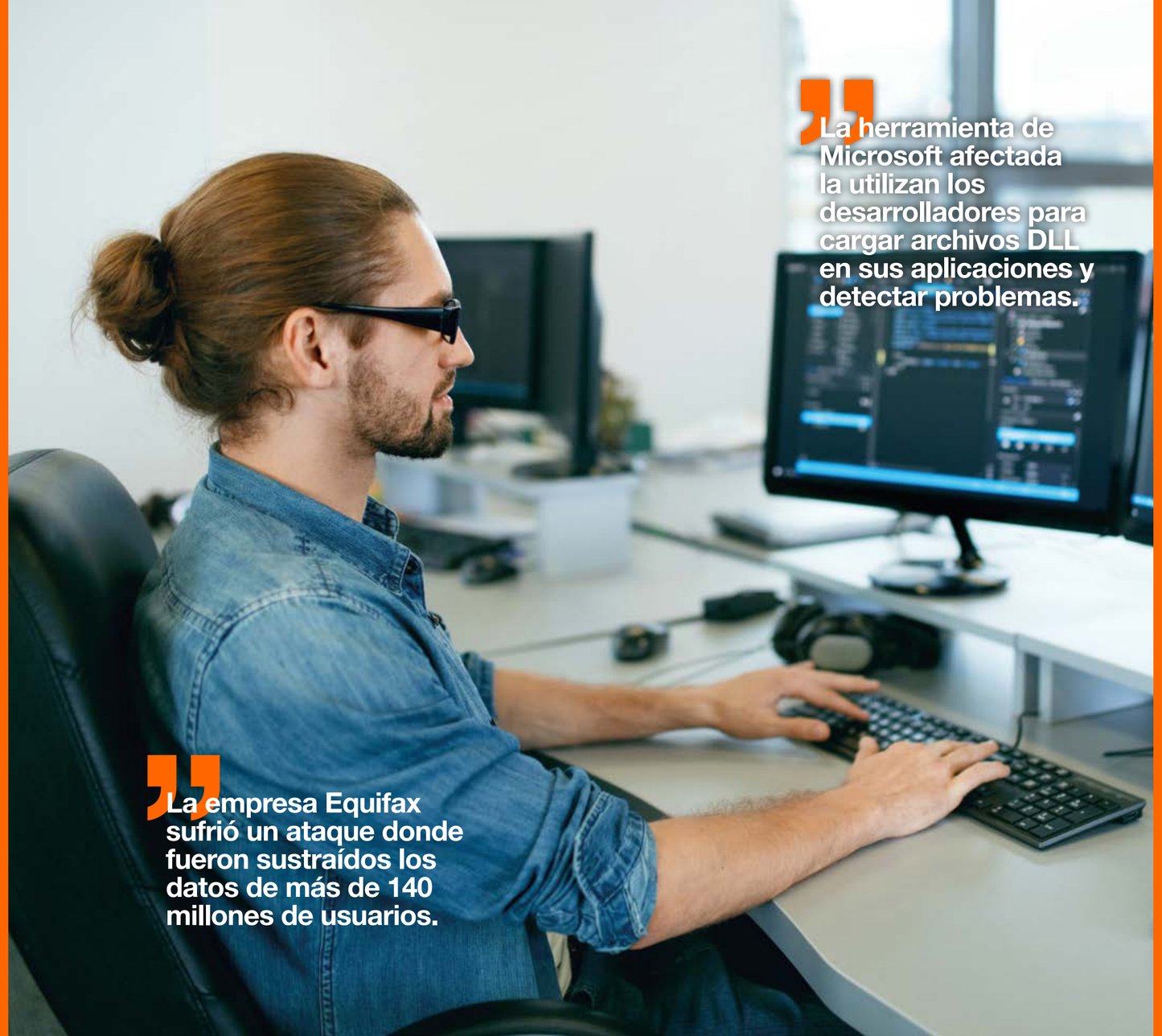
Sin embargo, el resultado de su actividad en la actualidad todavía no es clave ni aceptado colectivamente por todos los stakeholders. Son pocas las compañías que se atreven a firmar pólizas de este tipo, ya que las amenazas son difícilmente cuantificables.

Equifax, y la importancia de los datos de usuarios.

Equifax, dedicada a la comercialización de insights e informes, sufrió un ataque donde fueron sustraídos los datos de más de 140 millones de usuarios, números de la seguridad social especialmente, y datos sobre permisos de conducir. Los datos fueron extraídos entre mayo y julio de 2017 por medio de una vulnerabilidad antigua dentro la aplicación web de un portal de la empresa en Estados Unidos, que no tenía los parches actualizados aunque estaban disponibles desde marzo de ese mismo año.

Como respuesta Equifax tuvo que desplegar todo un dispositivo abierto de consulta de la información que se vio afectada y facilitar a los perjudicados el uso de servicios relacionados con la consulta de crédito disponible, etc., así como hacer frente a posibles suplantaciones de identidad de sus clientes para la obtención de préstamos.

- **El robo de datos se llevó a cabo por medio de una vulnerabilidad antigua dentro la aplicación web, que no tenía los parches actualizados.**
- **La empresa tuvo que desplegar un dispositivo abierto de consulta.**



"La empresa Equifax sufrió un ataque donde fueron sustraídos los datos de más de 140 millones de usuarios.

"La herramienta de Microsoft afectada la utilizan los desarrolladores para cargar archivos DLL en sus aplicaciones y detectar problemas.

Microsoft atacado por DoubleAgent.

Investigadores de la firma de seguridad Cybellum descubrieron una vulnerabilidad en su herramienta "Application Verifier" que afectaba a todos los sistemas operativos de Windows (desde su versión XP hasta Windows10). La herramienta permite a los desarrolladores detectar y solucionar fallos en otras aplicaciones mediante la carga de un archivo DLL.

En este caso los hackers utilizaron esa función a la inversa para inyectar archivos DLL maliciosos y así poder tomar el control de los sistemas operativos, secuestrar el antivirus y transformarlo en software malicioso, como ransomware.

Entre los antivirus vulnerables se encuentran Avast, AVG, Avira, Bitdefender, Trend Micro, Comodo, ESET, F-Secure, Kaspersky, Malwarebytes, McAfee, Panda, Quick Heal y Norton. Las compañías responsables de las soluciones antivirus fueron notificadas al respecto, pero solo Malwarebytes y AVG lanzaron sus respectivos parches de forma rápida. Obviamente también es responsabilidad de Microsoft responder ante la vulnerabilidad en Application Verifier, aunque la gravedad del problema es que los antivirus deben evitar a toda costa ser manipulados por una aplicación o comportamiento maliciosos.

- **Los hackers podrían tomar el control de los sistemas operativos y transformar el antivirus en software malicioso.**
- **Los antivirus deben evitar a toda costa ser manipulados por una aplicación o comportamientos maliciosos.**

Autenticación

Actualmente, la autenticación online se basa en un usuario y una contraseña, añadiendo en algunas ocasiones el uso de autenticación de doble factor. El problema con estos métodos es que las contraseñas son notoriamente inseguras y la autenticación de doble factor generalmente se basa en el envío de un código a través de SMS o un servicio de un tercero, un proceso cuyo nivel de seguridad no es el más óptimo.

Una solución podría ser la utilización de una cadena Blockchain, ya que los mismos principios criptográficos con lo que se diseñan podrían aplicarse a la autenticación. Cada vez que se agregue una “transacción” o bloque de datos a la cadena, la mayoría de la red debe verificar su validez, lo que garantizaría su integridad.

Incluso la biometría nos aporta, desde los entornos físicos y reales, una nueva forma de demostrar la identidad, una solución más segura y más sofisticada que las claves de acceso tradicionales. Pero a día de hoy también puede ser hackeada, ya que la huella biométrica que establecemos, por ejemplo, en los teléfonos móviles, tiene detrás un “hash” que puede ser robado y utilizado para crear una copia física falsificada.

En este escenario aparece la nueva normativa de protección de datos GDPR que obliga a implantar cifrado y sistemas de autenticación de doble factor, incluso sobre los datos considerados de nivel básico. La ciberseguridad por tanto debe volcarse en nuevos sistemas de autenticación fiables y que aborden nuevas maneras de comprobación de identidad más imaginativas.

> **La solución de Keynetic se sitúa en la boca de la red para identificar cada nuevo elemento que se conecta.**

Keynetic Technologies: autenticación con seguridad para la Industria 4.0.

La solución tecnológica de Keynetic se focaliza en identidad digital y control de acceso basado en SDN (Redes Definidas por Software). Su solución de seguridad de red permite controlar el acceso a los servicios en base a la identidad del usuario y dispositivo para poder visibilizar los usuarios y servicios conectados a la red protegida definida por software. “Las redes se convierten en autopista de comunicación que, a día de hoy, posibilitan la innovación en todos los negocios”, dice Jon Matías, CTO de la compañía. Su solución se sitúa en la boca de la red para identificar cada nuevo elemento que se conecta. “Primero pregunta quién es y qué quiere y después controla que esa máquina solo acceda a los servicios autorizados”. Pero también es la red la que se convierte en una pieza esencial de la Industria 4.0 con sus consecuentes riesgos. En otro tipo de organizaciones, podrían apagarse los ordenadores para evitar el daño ante una amenaza, pero cuando se trata de industrias, es inviable porque significa parar la producción y conlleva un elevado coste para la empresa. Lo que propone Keynetic para estos entornos es una solución de seguridad de red que permite controlar el acceso a los servicios en base a la identidad del usuario/dispositivo. Entre otras cosas, implica proteger cada uno de los elementos que se quieren conectar a esa red de manera que, cualquier tráfico no habilitado, no podrá entrar. Propician, además, una visibilidad total de la red frente a la opacidad actual pudiendo controlar en todo momento quién está conectado. Todo ello en un entorno amigable y fácilmente gestionable poniendo a disposición de la empresa el control de esa seguridad.

- **Su solución de seguridad de red permite controlar el acceso a los servicios en base a la identidad del usuarios y dispositivos conectados.**
- **Protegen cada uno de los elementos que se quieren conectar a esa red de manera que, cualquier tráfico no habilitado, no podrá entrar.**

GDPR y protección de datos

Desde mayo de 2018 cada persona ha tenido y tendrá que dar su consentimiento inequívoco para que las empresas puedan usar sus datos si es ciudadano europeo.

Las empresas tendrán que decir qué datos están utilizando, cómo los están tratando, para qué y quién es la persona responsable de los mismos. GDPR es el reglamento general de protección de datos (General Data Protection Regulation) que afecta a todos los países que dispongan de datos de ciudadanos europeos.

> **Las empresas deben comunicar qué datos están utilizando, cómo los están tratando y para qué y quién es el responsable.**

Biometría, ¿la solución más eficaz?

La biometría nos aporta, desde los entornos físicos y reales, una nueva forma de demostrar la identidad, una solución más segura y más sofisticada que las claves de acceso tradicionales. Pero a día de hoy también puede ser hackeada, ya que la huella biométrica que establecemos, por ejemplo, en los teléfonos móviles, tiene detrás un “hash” que puede ser robado y utilizado para crear una copia física falsificada. En este escenario aparece la nueva normativa de protección de datos GDPR que obliga a implantar cifrado y sistemas de autenticación de doble factor, incluso sobre los datos considerados de nivel básico. La ciberseguridad por tanto debe volcarse en nuevos sistemas de autenticación fiables y que aborden nuevas maneras de comprobación de identidad más imaginativas.

Cumplimiento de la ley de protección de datos

Las multas para quienes incumplan la normativa puede suponer el 4% de los ingresos de la empresa, y puede llegar hasta 20 millones de euros. La ley de protección de datos no es solamente un problema de Compliance o cumplimiento regulatorio para las empresas, requiere una transformación en la forma en que almacenamos y disponemos de los datos, y es una de las tendencias que tenemos que considerar para este sector, ya que durante 2018 se disparó la demanda de servicios relacionados con el correcto tratamiento de estos datos.

Por otra parte, está aumentando el número de empresas que hacen negocio con la venta de datos de usuarios, ofreciendo software gratuito, incluidos antivirus, que pretende la explotación fraudulenta de esos datos, comprometiendo la privacidad de sus usuarios. Mientras tanto el cibercrimen también se adapta y busca otras puertas de entrada a los sistemas. Las organizaciones más pequeñas siguen siendo un objetivo fácil para los criminales y, en muchas ocasiones, son utilizadas como puerta de entrada a firmas más grandes, conocida como “Acceso desde la cadena de confianza”.

La medida es ser conscientes de los ataques.

Por primera vez el público comienza a ser consciente de los ataques que se producen, y que en muchos casos se esconden, gracias a la aplicación del reglamento GDPR, puesto que las empresas estarán obligadas a informarles en caso de fuga de información.

> **El cumplimiento de la ley de protección de datos requiere de una transformación en la forma en que almacenamos y disponemos de los datos.**

7

Tecnologías y ciberseguridad

Las nuevas tecnologías se han puesto al servicio de la ciberseguridad, proporcionando nuevos ámbitos de aplicación.

La tendencia indica que, cada vez más, las empresas incorporan estas tecnologías en sus procesos para sus propios objetivos, estableciendo nuevos niveles de seguridad y escenarios de control.

7. Tecnologías y ciberseguridad

Blockchain

Blockchain es por definición una tecnología segura, y por su sistema de anotación distribuida, imposible de hackear. Pero la mayor parte del mercado y exchanges que giran en torno a las criptomonedas y el software que permite la minería, sí son blanco de los ataques.

Las empresas encuentran en esta tecnología una oportunidad para ofrecer servicios más ágiles y seguros. Desde transacciones financieras, incluyendo criptomonedas, hasta operaciones logísticas, documentales, de producción o la propia gestión de identidad (en dura competencia con las soluciones biométricas o de doble factor), el Blockchain comenzará a implantar un nuevo modelo en la seguridad de los datos.

Blockchain garantiza la integridad de los datos ya que cada vez que se agrega una transacción o bloque de datos a la cadena, la mayoría de la red debe verificar su validez.

Una nueva opción de autenticación

El Blockchain puede utilizarse como nueva opción de autenticación y acceso garantizando la integridad de la información y evitando la manipulación de datos. Además la descentralización en una cadena de bloques propia de esta tecnología, favorece la disponibilidad inmediata de la información, altamente robusta y a prueba de fallos, que puede protegerse incorporando algoritmos criptográficos de cifrado. Supone una gran oportunidad en seguridad informática, si tenemos en cuenta precisamente los conceptos que definen el Blockchain.

Una solución a la autenticación podría ser la cadena blockchain, ya que los mismos principios de esta tecnología son aplicables a la autenticación. Al distribuir un ledger entre todos los miembros de la red, la autenticación blockchain erradica el poder modificarlo maliciosamente. Cada vez que se agrega una transacción o bloque de datos a la cadena, la mayoría de la red debe verificar su validez, lo que garantiza su integridad.

La solución ideal sería una forma de autenticación que solo otorgue acceso a cierta información, eliminando así, la necesidad de que cada proveedor de servicios almacene credenciales para cada cliente.

La tecnología Blockchain puede ofrecer este enfoque mediante la descentralización de la propiedad de las credenciales y disponibilidad en una cadena inmutable de datos. Estos datos, en lugar de ser almacenados por una aplicación, se almacenan en el ledger. Este ledger compartido es descargado por cada usuario individual, reflejando un registro de cada transacción realizada.

Servidores de Tesla para minar criptomonedas.

Los servidores Cloud de Tesla, que están alojados en Amazon Web Services, fueron hackeados para instalar un 'malware' que extrae criptomonedas, según informó Panda Security. En 2017, el ataque contra servidores de empresas creció un 8%, como apunta la compañía en un comunicado. El caso del ataque a los dos gigantes tecnológicos, Tesla y Amazon, se enmarca en las técnicas conocidas como 'cryptohacking', ciberataques basados en el minado de criptomonedas.

Los atacantes accedieron a los servidores Cloud de Tesla por medio de Kubernets, una consola de administración que no requiere una clave de acceso. Una vez vulnerada la seguridad de estos servidores, procedieron a la instalación del software Stratum, diseñado para minar criptomonedas. Según detallan desde Panda Security, los servidores vulnerados contenían información relativa a la telemetría de sus coches eléctricos, que podría tener "un gran valor" en el mercado del espionaje industrial, pero, para la compañía, "los hackers prefirieron servirse de la escalabilidad de los servidores para minar criptomonedas". Según predicen desde Panda Security, este tipo de ataques se multiplicará en los próximos años.

- **Los servidores Cloud de Tesla fueron hackeados para instalar un 'malware' que extrae criptomonedas.**
- **Este tipo de ataques se multiplicará este año.**

> **"El caso del ataque a los dos gigantes tecnológicos, Tesla y Amazon, se enmarca en las técnicas conocidas como 'cryptohacking'.**

> **"La potencia de computación requerida para resolver los problemas de minado ha crecido exponencialmente y ahora se necesitan grandes bancos de servidores para descifrar códigos.**

Minando criptomonedas desde un banco italiano.

Durante un evento organizado por The Wall Street Journal, la CEO de Darktrace confirmó a los asistentes que tienen localizados más de 1.000 casos de minado de criptomonedas en los últimos seis meses solo en EE.UU, con empleados que usan la infraestructura de la empresa para ello. El criptominado es el proceso mediante el cual se crean nuevos bitcoins e implica la resolución de problemas criptográficos complejos. La potencia de computación requerida para resolver estos problemas ha crecido exponencialmente desde la creación del bitcoin en 2009 y ahora se necesitan grandes bancos de servidores para descifrar códigos. Como resultado de este protagonismo, han surgido pools de minería online que permiten a la gente compartir su capacidad informática y ganar una parte de las recompensas colectivas.

La ejecutiva afirmó que su compañía había encontrado un caso en el que un banquero junior de un banco italiano robó servidores que él había firmado en nombre de su compañía. "Había cogido 12 y los había escondido bajo el centro de datos del banco. Luego había establecido su propio campo de minado. Esto no se detectó durante un tiempo. Afortunadamente, lo detectamos porque había conexiones extrañas fuera del banco con sitios de minado".

- **Han surgido pools de minería online que permiten a la gente compartir su capacidad informática y ganar una parte de las recompensas.**
- **Un banquero junior de un banco italiano robó servidores que él había firmado en nombre de su compañía.**

La nube

La tendencia de migración de los datos desde servidores propios hacia modelos cloud, fruto de la transformación digital de las empresas, ha provocado un aumento de ciberataques a este tipo de infraestructuras.

El año pasado más del 50% de los incidentes de seguridad se produjeron en la nube. Esta cifra provoca también un aumento en la implantación de soluciones y servicios de ciberseguridad enfocadas hacia ese entorno. Los servicios Cloud ya cuentan con sus propios sistemas de seguridad y backup, pero no se trata solamente de salvaguardar los datos almacenados sino de derivar a este espacio también los servicios y soluciones de software de seguridad, para que estén disponibles desde ahí, y no alojados en los ordenadores de cada empleado.

Los servicios Cloud en cifras

La firma de análisis Gartner habla de un aumento del 21% interanual en este formato de entrega, generando un mercado de en torno a 5.200 millones en 2017 y de 8.000 millones de euros a finales de esta década.

Por segmentos de facturación de servicios Cloud en ciberseguridad nos encontramos con estos datos:

- **Gestión de identidades y accesos:** con 3.035 millones previstos en 2020.
- **Seguridad Web:** con 861,3 millones de gasto.
- **Protección del gateway de correo:** 627,8 millones de euros en facturación.
- **Testing de aplicaciones:** 506,6 millones previstos.
- **Security Information and Event Management:** con 318 millones gastados en servicios de seguridad.
- **Gestión remota de vulnerabilidades:** 220 millones facturados en 2017.

Ciberseguridad en España:
¿Qué áreas de la empresa están actualmente en la nube?

Fuente: PwC, The Global State of Information Security Survey, 2017

> Los hackers consiguieron acceso a los datos gracias a un despiste de los ingenieros de la compañía, que dejaron las credenciales de acceso a sus bases de datos en el código fuente de la app.

Uber y el robo de datos de 57 millones de conductores y clientes.

Aunque sucedió en octubre de 2016, la noticia saltó en 2017 porque la compañía había ocultado el ciberataque. De alguna manera el responsable de seguridad ocultó la filtración de datos. Sin embargo, fue despedido por la junta directiva de la empresa cuando tuvieron conocimiento del incidente. Un hacker robó los datos personales de 57 millones de clientes y conductores entre los que se incluian nombres, direcciones de correo electrónico, números de teléfono y, en el caso de chóferes estadounidenses, números de licencia de conducir.

El problema de seguridad podría haber sido uno más de los más conocidos en los últimos tiempos, pero que la multinacional lo ocultase pagando además 88.000 euros al atacante indignó a gran parte de la comunidad. Iba en contra de la confianza de usuarios y conductores, y de la obligación legal que tenían de comunicar el suceso a las agencias gubernamentales y personas afectadas. Los hackers consiguieron acceso a los datos gracias a un despiste de los ingenieros de la compañía, que dejaron las credenciales de acceso a sus bases de datos (alojadas en la infraestructura de Amazon Web Services) en el código fuente de la aplicación. Los atacantes solo tuvieron que ingeniárselas para entrar en el repositorio de este código, alojado en el popular servicio GitHub y usar esas credenciales para acceder a los datos. Uber asegura que los números de tarjetas de crédito o los datos de los viajes realizados por los clientes no se han visto afectados.

- **Un hacker robó los datos personales de 57 millones de clientes y conductores.**
- **El problema de seguridad podría haber sido uno más de los más conocidos en los últimos tiempos, pero que la multinacional lo ocultase pagando además 88.000 euros al atacante indignó a gran parte de la comunidad.**

Bots y Machine Learning

Los bots ya son una tendencia en muchos otros sectores. En Ciberseguridad los podemos encontrar en uno y otro lado, tanto para los hackers como para los responsables de seguridad informática, que ya empiezan a utilizar esta tecnología para sus propios objetivos.

Además, asistiremos al uso de chatbots para suplantar identidades y obtener datos de los usuarios, así como la Inteligencia Artificial permitirá también averiguar antes las password de los usuarios basándose en datos geográficos o demográficos, reduciendo el esfuerzo de los hackers para descifrar las claves. Aparecerán ataques criptográficos, basados en el reconocimiento de patrones, que reducen la complejidad para crear un ciberataque.

La aplicación del Machine Learning como solución no es algo nuevo, lleva más de 10 años desarrollándose, y no es una “bala de plata”, ni la solución definitiva, pero claramente ayuda a detectar nuevas amenazas que generalmente escapan a los productos o servicios de detección tradicionales y a los ojos del ser humano, mostrando las tendencias y comportamientos que de otra manera pasarían desapercibidos.

El uso de IA para eludir las herramientas de control de patrones empezará a ganar cada vez más protagonismo.

> **Microsoft, Europol, Interpol, FBI y ESET desmantelaron una red que había llegado a infectar más de 1,1 millones de sistemas en todo el mundo.**

Gamarue, una botnet desmantelada y que operaba desde 2011.

A finales de 2017, la colaboración entre Microsoft, la Europol, Interpol, FBI y ESET consiguió desmantelar una red que operaba desde 2011 y que había llegado a infectar más de 1,1 millones de sistemas en todo el mundo. Gamarue (Win32/Gamarue.AR) se vendía en la Deep Web como un kit para robar credenciales y para descargar e instalar malware adicional a los usuarios afectados.

Esta familia de malware contiene una botnet personalizable que permite a los propietarios del kit crear y usar plugins específicos, que hacen posible el robo de contenidos en formularios web o la infección y encriptación de ficheros, por los que se pide un rescate para recuperar los datos, y que permiten a los cibercriminales conectarse a los sistemas comprometidos y tomar su control. La forma de detectar la actividad se realizó utilizando otra botnet que rastreaba los servidores y lo que instalaban a los usuarios afectados por el malware, para acabar detectando el origen y los dominios de los cibercriminales.

- **Gamarue se vendía como un kit para robar credenciales y descargar malware adicional a los usuarios afectados.**
- **La forma de detectar la actividad se realizó utilizando otra botnet que rastreaba los servidores.**

Big Data y data analytics

Tecnologías como el Big Data necesitan de materia prima como son los datos para poder ser útiles, pero toda esa información hay que almacenarla, procesarla, gestionarla y sobre todo, protegerla.

Las empresas son las que tienen la responsabilidad y obligación de gestionar y guardar aproximadamente el 85% de la información, incluso aquellos datos considerados desestructurados, y que se encuentran dispersos y sin clasificar, como son las imágenes y vídeos. Aun así, la analítica de datos para prevenir y detectar amenazas es un clásico de la ciberseguridad. Las entidades financieras, por ejemplo, llevan años haciendo sus deberes en este sentido "y analizando patrones para detectar operaciones anormales de sus clientes", asegura el director académico del Master in Cibersecurity de IE School of Human Sciences and Technology.

> **Ya existen en el mercado herramientas basadas en el análisis de los historiales de actividad para detectar patrones de conducta inadecuados que puedan suponer una amenaza, generando alertas.**

El Big Data frente a los ataques

El Big Data se convierte en el arma secreta para poder prever los futuros ataques. De hecho, ya existen en el mercado herramientas basadas en el análisis de los historiales de actividad para detectar patrones de conducta inadecuados, no habituales, o aumentos en los accesos que puedan suponer una amenaza, generando alertas para los responsables y usuarios.

Como valor añadido, la analítica de datos permite detectar ataques de malwareless, modalidad que no requiere de software de ataque. La clave para combatir un ataque carente de malware radica en la capacidad de detectarlo basándose en el comportamiento exhibido por los usuarios de la red corporativa. Para "cazar" estas amenazas es necesario disponer de herramientas de Threat Hunting que monitoricen el comportamiento de los equipos, de las aplicaciones que se ejecutan en ellos y, fundamentalmente, de los usuarios que se mueven en la red. Disponer de una cantidad tan ingente de datos y de perfiles de comportamiento, permite cotejar los modelos contra los datos reales para alertar de cualquier desviación sobre el comportamiento que resulte sospechosa.

A continuación, los sistemas de Machine Learning priorizarán los incidentes potenciales, que serán estudiados en profundidad con herramientas de análisis forense remotas integradas en plataformas de Threat Hunting.

Banco Santander despliega todos sus datos para ciberseguridad.

Banco Santander ha creado recientemente Santander Analytics, un nuevo departamento integrado por matemáticos e ingenieros que se centra en el control de riesgos y en la prevención del fraude. La nueva unidad permitirá incrementar y adaptar la prevención y respuesta ante cualquier tipo de amenaza; acortar los tiempos de reacción y defensa, además de visibilizar tanto el histórico como la actividad en tiempo real de los endpoints; mejorar la capacidad analítica y los procesos, clasificándolos automáticamente; y realizar análisis forenses de amenazas y ataques.

La creación de Santander Analytics se enmarca en la política del banco de realizar una gestión prudente del riesgo y contar con un modelo de operaciones sólido, que se viene reforzando con el uso de tecnologías digitales y de herramientas avanzadas. Según datos de finales de 2018, el departamento había incorporado alrededor de 200 especialistas en campos clave del Big Data (matemáticas, estadística, ingeniería o data science), que colaboran con expertos mundiales en análisis de datos. Con ellos, la organización está implantando nuevas técnicas basadas en analíticas de datos, inteligencia artificial y Machine Learning para conseguir una gestión más predecible del riesgo.

- **Santander Analytics es un nuevo departamento del banco que se centra en el control de riesgos y en la prevención del fraude.**
- **Cuenta con especialistas en campos clave del Big Data, para realizar una gestión más predecible del riesgo mediante analíticas de datos, inteligencia artificial y Machine Learning.**

> **Santander Analytics es un nuevo departamento que se dedica al control de riesgos y a la prevención del fraude.**

> **Secure Endpoint de Orange proporciona un control de todos los procesos en ejecución y reduce la superficie posible de ataque.**

Orange lanza su protección para endpoints “Secure Endpoint”.

Ante este escenario, Orange ha lanzado para las grandes empresas el servicio Secure Endpoint, su solución contra ataques APT (Advanced Persistent Threat) para entornos de escritorio y servidores Windows. Este servicio proporciona una visibilidad detallada de toda la actividad en los endpoints, es decir, proporciona un control de todos los procesos en ejecución y, reduce la superficie posible de ataque. Su funcionamiento basado en técnicas analíticas de Machine Learning y Big Data clasifica como goodware o malware cada una de las acciones ejecutadas dentro de la red y servidores corporativos.

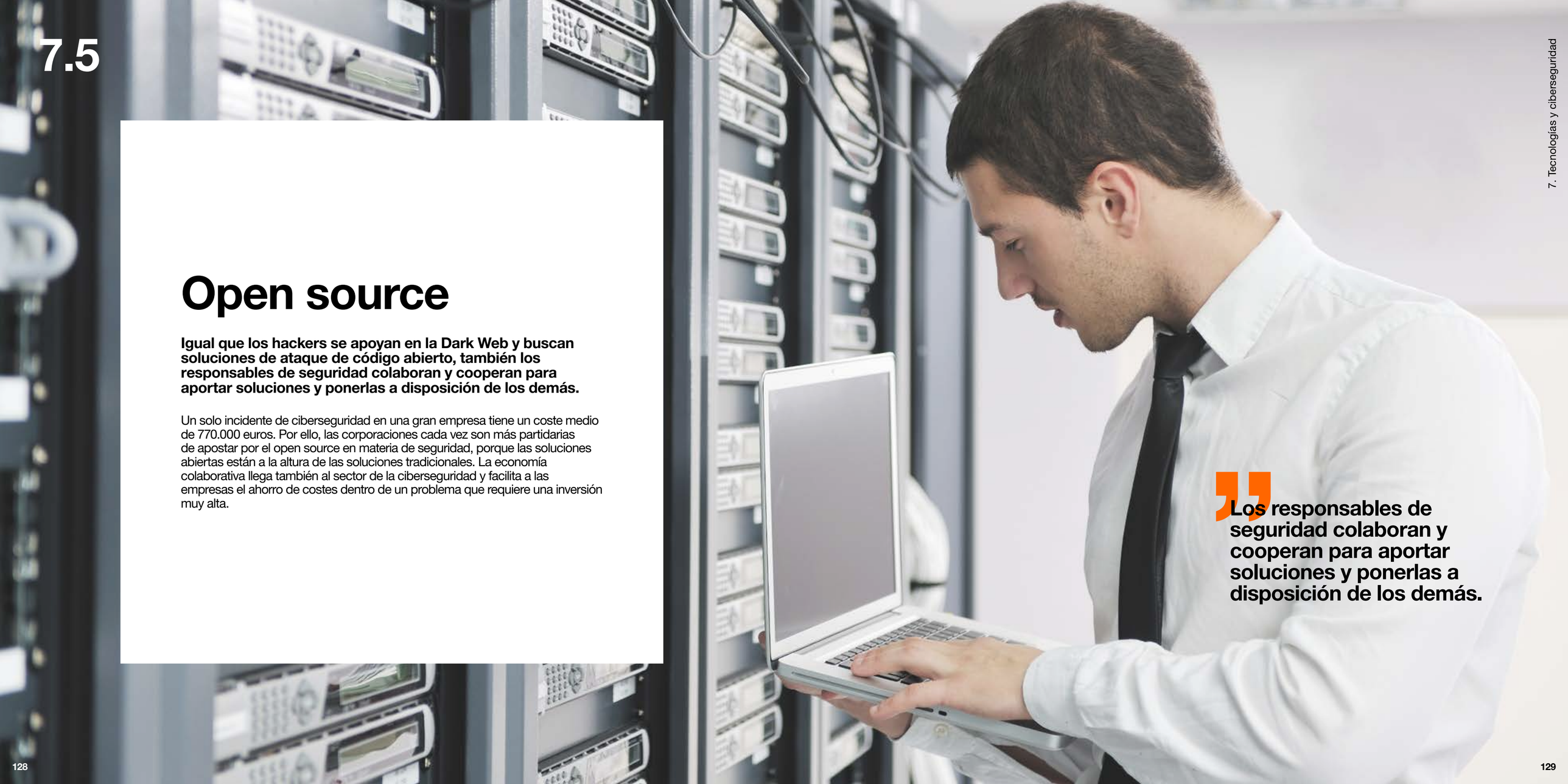
La solución Secure Endpoint, incluye un servicio de detección y respuesta (EDR) que clasifica cada proceso ejecutado en los equipos de las organizaciones de forma precisa, ejecutando únicamente lo que es confiable (clasificado como goodware). La capacidad de monitorización en tiempo real de todos los procesos, aporta la visibilidad necesaria para poder adelantarse a los ciberataques, bajo la filosofía Threat Hunting. Así, se pueden descubrir nuevos patrones de ataque, mediante la identificación automática de anomalías en el comportamiento de cada usuario, proceso y máquina.

- **Solución contra ataques APT para entornos de escritorio y servidores Windows.**
- **Se basa en técnicas analíticas de Machine Learning que el Big Data clasifica como goodware o malware.**

Open source

Igual que los hackers se apoyan en la Dark Web y buscan soluciones de ataque de código abierto, también los responsables de seguridad colaboran y cooperan para aportar soluciones y ponerlas a disposición de los demás.

Un solo incidente de ciberseguridad en una gran empresa tiene un coste medio de 770.000 euros. Por ello, las corporaciones cada vez son más partidarias de apostar por el open source en materia de seguridad, porque las soluciones abiertas están a la altura de las soluciones tradicionales. La economía colaborativa llega también al sector de la ciberseguridad y facilita a las empresas el ahorro de costes dentro de un problema que requiere una inversión muy alta.



> **Los responsables de seguridad colaboran y cooperan para aportar soluciones y ponerlas a disposición de los demás.**

> Uptane ha creado una asociación empresarial para proteger las actualizaciones y módulos de conexión de los vehículos de nueva creación.

Uptane: ciberseguridad open source para automoción.

Uptane es un consorcio de investigadores de ciberseguridad que ha lanzado un framework open source para proteger las actualizaciones y módulos de conexión (WiFi) de los vehículos de nueva creación. Se trata de una joint venture creado por la Universidad de Michigan, NYU Tandon, Instituto de Transporte de Michigan y el Instituto de Investigación del Sur para combatir ataques mediante un software que se actualiza sin tener que recurrir al concesionario. Uptane permitirá a los fabricantes de coches controlar totalmente el software crítico, mientras se comparte el control con agencias de seguridad, y se permite desplegar medidas correctivas para taponar vulnerabilidades de forma rápida y barata.

- **El marco de trabajo open source protege las actualizaciones y módulos de conexión de los vehículos de nueva creación.**
- **Permite desplegar medidas correctivas para taponar vulnerabilidades.**

Netflix puso en marcha una iniciativa para compartir herramientas de código libre para software de alta velocidad y distribuido (Cloud).

Netflix y su contribución a la ciberseguridad open source.

Hace casi 4 años Netflix puso en marcha una iniciativa para compartir herramientas de código libre para software de alta velocidad y distribuido (Cloud), lanzando distintas herramientas, entre ellas Security Monkey. Esta herramienta de código libre se encarga de monitorizar la seguridad en entornos cloud, incluyendo el análisis y respuesta a configuraciones erróneas, así como vulnerabilidades y otros temas de seguridad. Incluso Google ha confiado su Cloud Platform a esta herramienta. Otra herramienta fue FIDO, creada para ofrecer respuestas automáticas a incidentes Lemur, agilizar la gestión de certificados SSL/TLS o BLESS y poder firmar claves públicas SSH.

Todos estos y muchos otros proyectos se pueden seguir de manera pública en GitHub y aprovechar el conocimiento desarrollado por los equipos internos de Netflix y todo lo que han aportado otros desarrolladores en abierto.

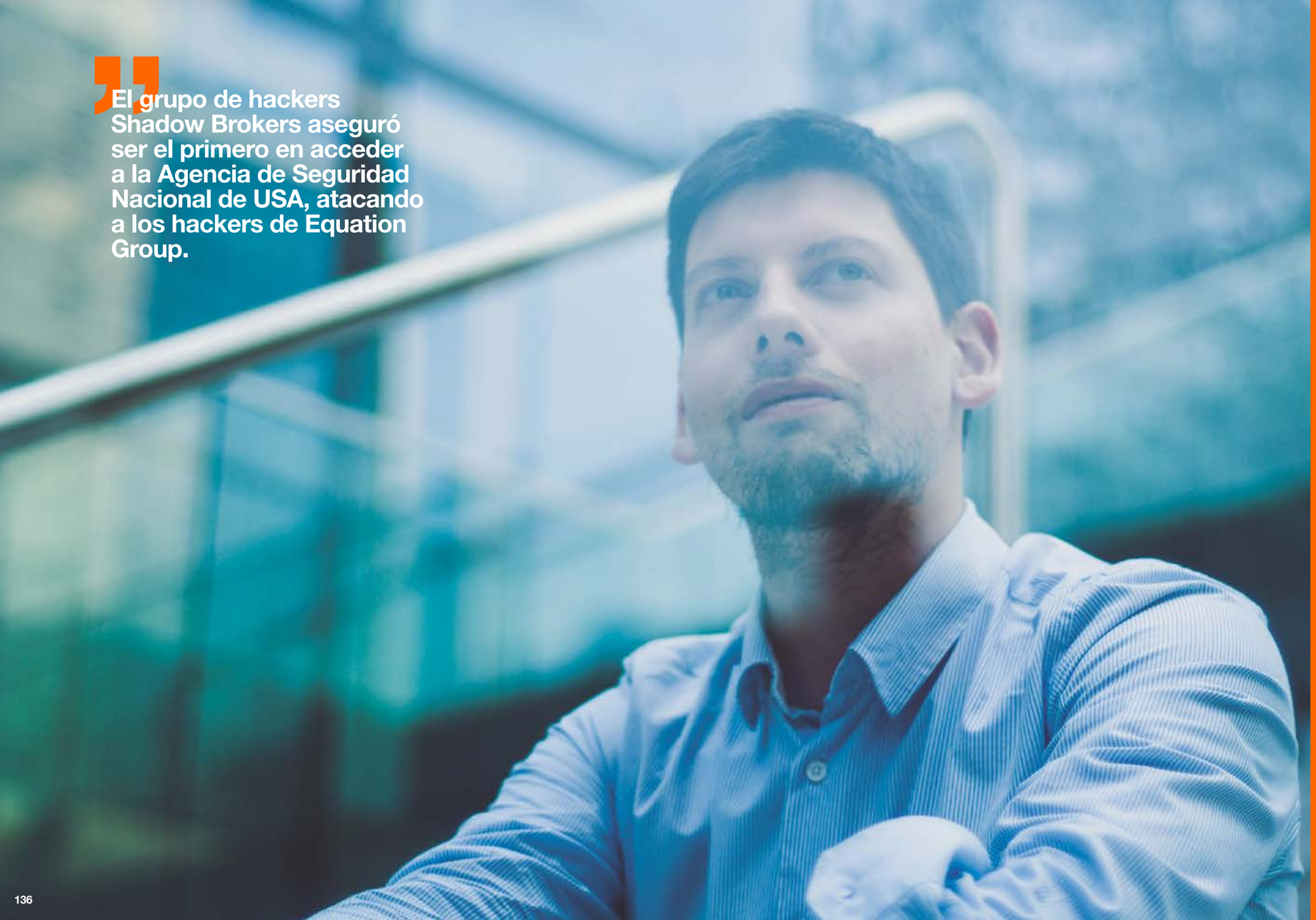
- **Iniciativa para compartir herramientas de código libre para software de alta velocidad.**
- **Otra herramienta fue FIDO, creada para respuestas automáticas a incidentes.**

Crime as-a-Service

Hemos pasado del software como servicio (SaaS) al crimen como servicio (CaaS), en un entorno donde los cibercriminales podrán adquirir herramientas y servicios que les permitan realizar ataques sin grandes conocimientos técnicos.

La misma estrategia que jugó un papel relevante para dar soluciones empresariales estandarizadas y baratas en la nube a las empresas, se revela como un agente negativo para los próximos años en materia de ciberseguridad. Además, han aparecido los conocidos “exploit kits”, o packs de herramientas que permiten perpetrar ataques sin los conocimientos básicos para ello.

Recientemente han aparecido los “exploit kits”, packs de herramientas que permiten perpetrar ataques sin los conocimientos básicos para ello.



> El grupo de hackers Shadow Brokers aseguró ser el primero en acceder a la Agencia de Seguridad Nacional de USA, atacando a los hackers de Equation Group.

Shadow Brokers y la subasta de malware.

Shadow Brokers es una organización de hackers que asegura ser la primera en haber accedido a la NSA (Agencia de Seguridad Nacional de Estados Unidos), hackeando al Equation Group, que había logrado instalar un spyware en los discos duros de la Agencia. Shadow Brokers se dio a conocer en agosto de 2016, publicando en Tumblr (red social de blogs) los archivos extraídos y sus peticiones, iniciando además una subasta para que se los llevase el mejor postor. Anunciaron que no devolverían los importes de la subasta, pero que premiarían de alguna forma a los participantes. Se filtró y anticipó que el contenido de esos archivos incluía programas de espionaje contra Cisco, Juniper, Fortigate y Topsec, así como el gusano Stuxnet, utilizado para hackear instalaciones nucleares. Posteriormente pusieron a la venta exploits en ZeroWeb, por importes entre 1 y 100 bitcoins y un lote especial por 1.000 bitcoins.

Una vez más volvieron a intentar hacer negocio con un paquete de software que en teoría servía para aprovechar exploits de Windows y saltarse los antivirus, que pertenecía a la NSA.

En 2017 liberaron un set de herramientas para comprometer la seguridad de Windows y en el mismo año, publicaron documentación en Github sobre cómo atacar sistemas bancarios.

Tras más de un año de la investigación, la NSA aún no ha podido establecer quién estuvo detrás de la fuga: si los hackers piratearon el sistema de la NSA o si los datos fueron robados o filtrados accidentalmente por algún empleado de la agencia.

Por otro lado, un informe publicado este año por la empresa de ciberseguridad Symantec señala que un grupo presuntamente vinculado al Estado chino, al que se denomina Buckeye, estaba usando las mismas herramientas de hacking vinculadas a la NSA un año antes de que Shadow Brokers las filtrara. Buckeye se considera una de las principales responsables de una gran cantidad de ataques de espionaje, principalmente contra organizaciones críticas y de defensa en Estados Unidos.

- **En abril de 2017 liberaron un set de herramientas para comprometer la seguridad de Windows.**
- **Además, publicaron documentación en GitHub sobre cómo atacar sistemas bancarios.**

Internet of Things

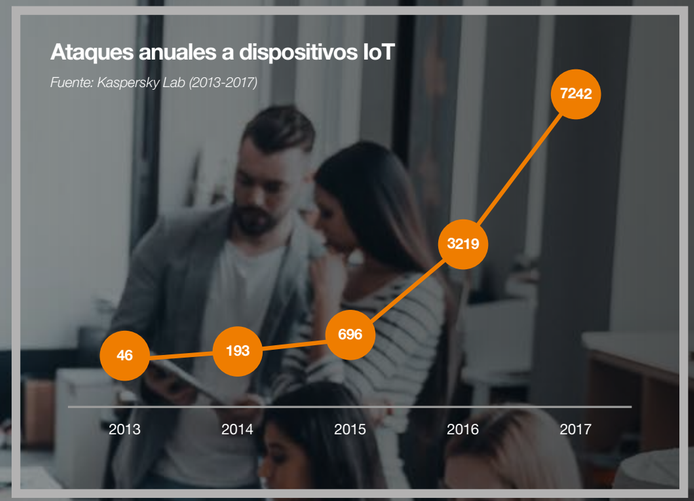
Otro de los ámbitos de aplicación de la ciberseguridad es Internet de las Cosas, ya que, desde la aparición de esta tecnología, surge la necesidad de securizar también el control de todo tipo de dispositivos conectados a la red y que pueden ser susceptibles de un ciberataque.

La posibilidad de que estos dispositivos sean hackeados tiene consecuencias devastadoras, ya que afectan directamente en el mundo real y offline.

Algunos sectores son especialmente vulnerables bajo este paraguas de IoT, como son el sector de la automoción o la industria, que cuentan con sistemas formados por infinidad de elementos conectados a la red. La proliferación de dispositivos conectados en red aumenta la capacidad de ataque, y podremos asistir a contextos de ataque inesperados, como routers, televisores, juguetes, hasta centrales eléctricas, estaciones de servicio o incluso marcapasos.

El ámbito de acción aumenta a medida que se van conectando nuevos aparatos a la red. Lo que sucede es que estos dispositivos aumentan la superficie de ataque, por lo que utilizarlos como vía de entrada a la red de la empresa va a ser cada vez más frecuente. Las limitadas capacidades de muchos de los dispositivos IoT serán aprovechadas por los cibercriminales mediante código dirigido, incluyendo la creación de marcos de desarrollo para hacer crypto-mining y spam masivo distribuido como servicio, uno de los nuevos casos de uso del cibercrimen.

Los ataques a dispositivos IoT aumentan de manera exponencial cada año.



La proliferación de dispositivos conectados aumentará la capacidad de ataque hacia contextos como televisores, juguetes, y hasta centrales eléctricas.

“Firewall dinámico” para Internet de las Cosas.

CryptoniteNXT y el firewall de nueva generación de Palo Alto Networks (NGFW) lanzan una solución para dificultar el acceso de hackers a los endpoints de la red evitando comprometer dispositivos de Internet de las Cosas. Los atacantes utilizan técnicas cada vez más sofisticadas para penetrar en las arquitecturas de red mejor defendidas. La defensa cibernética (MTD) en movimiento, de CryptoniteNXT, cambia la vista de la red a una estructura dinámica y abstracta, transformando la red en un objetivo dinámico en movimiento. Esto restringe de forma importante la capacidad de un atacante de recopilar información procesable sobre la red o disfrazarse como otro endpoint legítimo. La reciente explosión de dispositivos IoT ha añadido un nuevo grupo de dispositivos en riesgo, como cámaras de seguridad corporativas, que se convierten en puntos clave para ciberataques avanzados y hackers, que acceden a dispositivos de construcción “inteligentes” como iluminación automatizada, controles de energía y termostatos. Sin embargo, con la integración de CryptoniteNXT y Palo Alto Networks, los clientes pueden beneficiarse de una red que es dinámica y difícil de mapear.

- **La defensa cibernética en movimiento cambia la vista de la red a una estructura dinámica y abstracta.**
- **Los dispositivos IoT se convierten en puntos clave para ciberataques avanzados y hackers.**

“La reciente explosión de dispositivos IoT ha añadido un nuevo grupo de dispositivos en riesgo, como cámaras de seguridad corporativas.

“El CEO de Roomba decidió vender a grandes compañías como Amazon o Google los datos de los planos de las casas que han limpiado.

La polémica de Roomba y los planos de las casas que limpia.

Recientemente ha saltado la polémica por la decisión del CEO de Roomba (robots aspiradora del hogar que todos conocemos) de vender a los grandes (Amazon, Google, etc.) los datos de los planos de las casas que han limpiado. Estos robots, como dispositivo IoT recogen información sobre el hogar para ir optimizando las rutas de limpieza y detectar posibles reformas y cambios. Estos datos, en los modelos que están conectados al WiFi, viajan por la red y son recopilados por la empresa. Ahora surge la polémica por parte de los usuarios, ya que nadie quiere que sus datos privados, como el mapa de su casa, pueda ser objeto de cambio entre la empresa y otras empresas que pretenden explotarlo para mejorar también cuestiones de domótica y otros proyectos. El debate está servido, aunque no habría dudas ni problemas si tuviésemos la seguridad de que estos datos viajan de manera segura por la red. En caso contrario, cualquier hacker podría obtener un plano de tu casa.

- **Estos robots recogen información sobre el hogar para optimizar las rutas de limpieza y detectar posibles reformas y cambios.**
- **Estos datos, en los modelos que están conectados al WiFi, viajan por la red y son recopilados por la empresa.**

7.8

Redes

El último nivel de control en ciberseguridad es el de la seguridad en las redes, que engloba la confianza del transporte en la información a través de los diferentes mecanismos transmisores.

En este último nivel de alcance se incluyen los cortafuegos, las redes privadas virtuales, sistemas de prevención y detección de intrusiones, herramientas para la protección de redes inalámbricas y dispositivos móviles, así como herramientas para el control de tráfico de red y comunicaciones.

Se trata de garantizar la seguridad en los accesos remotos de equipos entre redes, y la transferencia de información, permitiendo solo a usuarios autorizados la supervisión, análisis y control de los tráficos entrantes y salientes y garantizando la continuidad de conectividad de los equipos transmisores.

> **El 74% de las empresas a nivel mundial ya utilizan la IA/Machine Learning.**

Medidas y herramientas capaces de monitorizar el comportamiento de la red

Se hace necesaria la implantación de herramientas de análisis de comportamiento de red:

- El 93% de los consultados por Cisco en España afirmaron que las herramientas de análisis de comportamiento de red funcionan adecuadamente (91% en EMEAR-Europa, Oriente Próximo, África y Rusia, y un 92% a escala global).
- El 83% se apoyan en la automatización para reducir su nivel de esfuerzo y reforzar la ciberseguridad (dato global).
- El 74% de las empresas a nivel mundial ya utilizan la IA/Machine Learning.

> **Investigadores de la Universidad de Leuven han descubierto que el protocolo WPA2, el más avanzado y seguro que se usa en todo el mundo para la conexiones vía WiFi, era vulnerable.**

Problemas de seguridad con el protocolo WPA2.

Investigadores de la Universidad de Leuven han descubierto que el protocolo WPA2, el más avanzado y seguro que se usa en todo el mundo para la conexiones vía WiFi, era vulnerable. Lo pusieron a prueba y descubrieron que cualquiera puede ser espiado a través de su red doméstica. Pero, aunque todos los expertos han dicho que es un fallo gravísimo, no se ve una solución sencilla a corto plazo. El mayor problema de este ataque a la WPA2 es que no daña a un tipo de router, una marca o un tipo de conexión sino al protocolo (el único que se usa en todo el mundo en este tipo de tecnología). Por eso, los expertos avisan: no se puede hacer mucho para mejorar nuestra ciberseguridad, pues el lenguaje es igual para todos, pero sí podemos hacer algo para ponerles más difícil a los hackers entender lo que mandamos. La clave está en la encriptación de los datos.

¿Cómo saber qué aplicación es segura? Pues en tecnología móvil la mayoría de servicios de mensajería como WhatsApp, por ejemplo, ya ofrecen este tipo de seguridad en todas las conversaciones. Mientras que en el PC todas las web que ya sean HTTPS (la mayoría ya lo son) también dan al usuario un encriptado extra. En cuanto al correo electrónico la mayoría de proveedores, empezando por Google, utilizan un protocolo de seguridad TLS (Transport Layer Security, seguridad de la capa de transporte) que protege la privacidad de los mensajes.

- **Se puso a prueba que cualquiera puede ser espiado a través de su red doméstica.**
- **El mayor problema de un ataque a la WPA2 es que no daña a un tipo de router o conexión, sino a todo el protocolo.**

Retos para la ciberseguridad

La falta de presupuesto, la compatibilidad de los sistemas o la arquitectura obsoleta son algunos de los retos a los que se enfrenta la ciberseguridad.

El 28% habla de la compatibilidad de los sistemas y arquitectura obsoleta, y el 25% comenta la falta de talento capacitado y certificaciones entre los empleados. Además, un 25% señala un liderazgo poco involucrado en las decisiones de seguridad y solo el 14% de los Consejos Directivos tiene experiencia en seguridad.

El 25% de lo ejecutivos comenta la falta de talento capacitado y certificaciones en materia de ciberseguridad entre los empleados.

¿Qué áreas habría que reforzar?

Desde McAfee se destacan tres áreas que son el talón de Aquiles para la mayoría de los CEOs y altos directivos que abordan los nuevos retos de ciberseguridad en sus organizaciones. Mientras los entornos son ágiles y fluidos en la ciberdelincuencia, dentro de los procesos internos de las empresas se produce una ralentización en la implementación de las políticas de seguridad, y una falta de profesionales cualificados en ciberseguridad. Todo esto representa una oportunidad para los cibercriminales y para poder hacerles frente, las empresas deberían ganar en agilidad.

De acuerdo con el informe McAfee, el 90% de las empresas afirma tener una estrategia de ciberseguridad, pero solo el 49% ha implementado esta estrategia completamente.

En resumen, las barreras más importantes para el despliegue de buenos sistemas de ciberseguridad en las empresas son:

- Mayor necesidad de presupuesto.
- Mayor implicación de los trabajadores.
- Actualización de la arquitectura de los sistemas.
- Capacitación de las personas y conocimiento.
- Mayor velocidad de implantación.
- Necesidad de políticas internas de seguridad.
- Estrategia coherente y ligada a su implementación.

El 90% de las empresas afirma tener una estrategia de ciberseguridad, pero solo el 49% ha implementado esta estrategia completamente.

FORO DE LA EMPRESA DEL

Mañana

Mañana es hoy

La transformación digital de las Grandes Empresas empieza cada día. Hoy también.

Patrocinador tecnológico
SAMSUNG

orange™