NTT DATA

Marzo 2025

Radar 100

números de ciberseguridad

Un viaje a través del tiempo

Editorial por María Pilar Torres Bruna

Desde diciembre de 2016, nuestra revista ha sido y sigue siendo un lugar donde reflejar conocimiento y reflexionar sobre la ciberseguridad. Hoy, al celebrar su edición número 100, nos encontramos ante un hito significativo que invita a la reflexión: ¿qué hemos aprendido durante estos años, y cómo han cambiado las amenazas que tanto nos preocupan?

Cuando comenzamos este viaje, allá por 2016, las ciberamenazas eran, para muchos, algo distante, casi ajeno al día a día de las empresas y los usuarios comunes. Había organizaciones que ni siquiera contaban con políticas de seguridad en materia de ciberseguridad formalizadas, y las brechas de seguridad se percibían como algo aislado o exclusivo de grandes empresas tecnológicas. Sin embargo, en 100 ediciones y 8 años de trabajo continuo, hemos sido testigos de una evolución fascinante.

La evolución de las amenazas: del *malware* a los ciberataques sofisticados

Si echamos la vista atrás, podemos ver cómo las ciberamenazas han dejado de ser simples ataques de *malware* o virus, como aquellos que inundaban los primeros números de nuestra revista, para convertirse en ciberataques de una sofisticación impresionante. Hoy en día, las amenazas incluyen *ransomware*, *phishing* avanzado, ataques dirigidos *zero day* y explotación de vulnerabilidades en la cadena de suministro, entre otras. Sin embargo, lo que más sorprende al observar esta evolución es que, en el fondo, las motivaciones y los objetivos de los atacantes siguen siendo similares a los de hace 8 años: robar datos sensibles, interrumpir operaciones y, sobre todo, explotar las vulnerabilidades humanas.

El verdadero cambio: la forma en que recibimos las amenazas

Lo que ha cambiado radicalmente es la forma en que nos enfrentamos a estas amenazas.

En 2016, los ciberataques llegaban principalmente a través de correo electrónico o *malware* descargado a través de sitios web comprometidos.

Hoy, los vectores de ataque son mucho más complejos y se diversifican a través de redes sociales, dispositivos móviles, internet de las cosas (IoT) y plataformas de colaboración. Los atacantes ahora están en todas partes: desde plataformas de juegos online hasta sistemas de mensajería corporativa. El *phishing*, por ejemplo, ha evolucionado de simples correos electrónicos engañosos a ataques altamente personalizados (*spear phishing*), dirigidos a individuos clave dentro de una organización.

Además, el cibercrimen ha dejado de ser un asunto de "ciberdelicuentes solitarios" para convertirse en una industria altamente organizada y global. Las mafias cibernéticas operan con una estructura empresarial, y los ataques de *ransomware* han pasado de ser incidentes aislados a verdaderos eventos de extorsión a gran escala donde las víctimas no solo sufren la pérdida de datos, sino que se enfrentan a la presión de pagar grandes sumas de dinero para evitar una exposición pública o una interrupción prolongada de sus servicios.

¿Siguen siendo las amenazas las mismas?

Es interesante observar que, aunque las herramientas y técnicas que utilizan los atacantes han avanzado, muchas de las amenazas siguen siendo las mismas. El *phishing*, por ejemplo, sigue siendo uno de los métodos más efectivos de ataque, y las vulnerabilidades humanas continúan siendo el principal problema. Esto nos recuerda que, más allá de las tecnologías avanzadas, la concienciación y formación de los usuarios sigue siendo una de las piedras angulares de nuestra defensa.

Los ciberataques de hoy en día, si bien son más complejos y variados, se alimentan de los mismos errores humanos: hacer clic en un enlace malicioso, usar contraseñas débiles o confiar demasiado en una red Wi-Fi pública. La ingeniería social sigue siendo el arma favorita de los atacantes y, cada vez más, estos agentes comprenden que explotar la confianza humana es el camino más efectivo para infiltrarse en las redes corporativas.

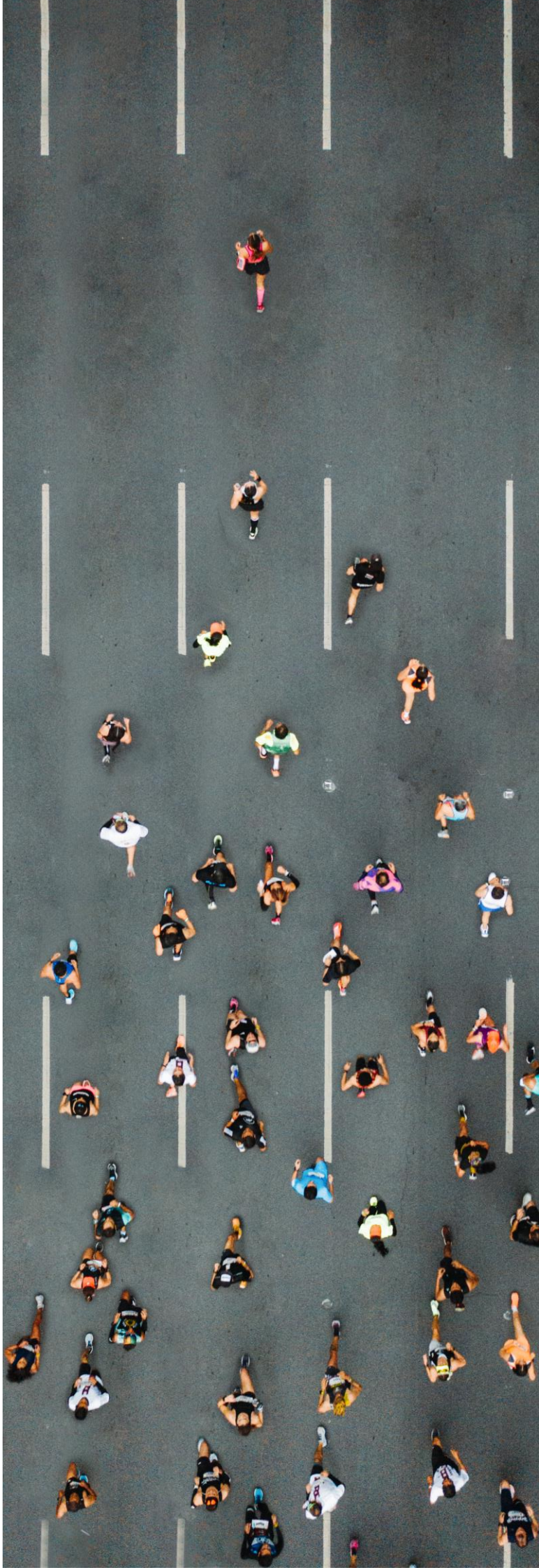
Mirando hacia el futuro

Al mirar hacia el futuro, una de las grandes preguntas es cómo debemos adaptarnos a un panorama que, lejos de estabilizarse, parece volverse más dinámico y desafiante cada día. Los ataques basados en inteligencia artificial, los *deepfakes*, la clonación de voz, las filtraciones de datos masivas y las amenazas relacionadas con la computación cuántica están empezando a surgir como nuevos desafíos en el horizonte.

No obstante, a pesar de la creciente sofisticación de los atacantes, debemos recordar que las amenazas no son imbatibles. La evolución de las estrategias de defensa, desde el *Zero Trust* hasta la integración de IA para la detección de amenazas y la automación de respuestas, prometen ser la clave para enfrentarlas de manera efectiva.

En definitiva, al llegar a nuestra edición número 100 celebramos el camino recorrido, pero sobre todo, nos preparamos para los desafíos que vendrán. Las amenazas cambian, pero lo que no cambia es nuestra misión de proteger lo que más importa: nuestros datos, nuestras infraestructuras y, sobre todo, a las personas.

Gracias por acompañarnos en este viaje. El futuro de la ciberseguridad está lleno de retos, pero juntos, seguiremos evolucionando, aprendiendo y protegiendo.



Cuando el sector salud se convierte en paciente

Cibercrónica por Héctor Palencia Sánchez

Comenzamos nuestra cibercrónica destacando el reciente ciberataque sufrido por Ascension Health, una de las mayores organizaciones de atención médica en Estados Unidos. El 27 de diciembre de 2024, se informó que datos de 5,6 millones de pacientes fueron comprometidos, incluyendo información sensible de salud. El incidente se originó cuando un empleado descargó inadvertidamente malware, lo que permitió a los atacantes acceder a los sistemas internos y robar datos confidenciales.

Como medida de contención, Ascension desvió la atención de emergencia en algunos de sus hospitales, afectando temporalmente los servicios a los pacientes.

Este suceso subraya la importancia de la capacitación continua del personal en protocolos de ciberseguridad para prevenir errores humanos que puedan derivar en brechas de seguridad.

En el ámbito financiero, el fabricante japonés Wacom, conocido por sus tabletas gráficas, fue víctima de un ciberataque a su tienda en línea.

El 8 de enero de 2025, se comprometió la información de pago de clientes que realizaron compras durante ese período.

La empresa está investigando el incidente y ha contactado a los clientes potencialmente afectados, recomendándoles revisar sus extractos bancarios, cambiar contraseñas y estar alerta ante posibles estafas de *phishing*.

En el sector de las telecomunicaciones, Telefónica sufrió un ciberataque el 9 de enero de 2025, en el cual un grupo de hackers extrajo 2,3 GB de datos del sistema interno de gestión de incidencias de la compañía.

Aunque algunos documentos relacionados con clientes se vieron afectados, la empresa confirmó que los datos de clientes residenciales no fueron comprometidos.

Los atacantes publicaron la base de datos en un foro, lo que llevó a Telefónica a tomar medidas para bloquear accesos no autorizados y restablecer contraseñas comprometidas.

En el ámbito gubernamental, se informó en enero de 2025 sobre una brecha de datos que afectó a la Guardia Civil y las Fuerzas Armadas de España.

Se filtraron y pusieron a la venta en un portal de ciberdelincuencia los correos electrónicos y datos de aproximadamente 180.000 miembros de estas instituciones, incluyendo cerca de 20.000 correos electrónicos personales.

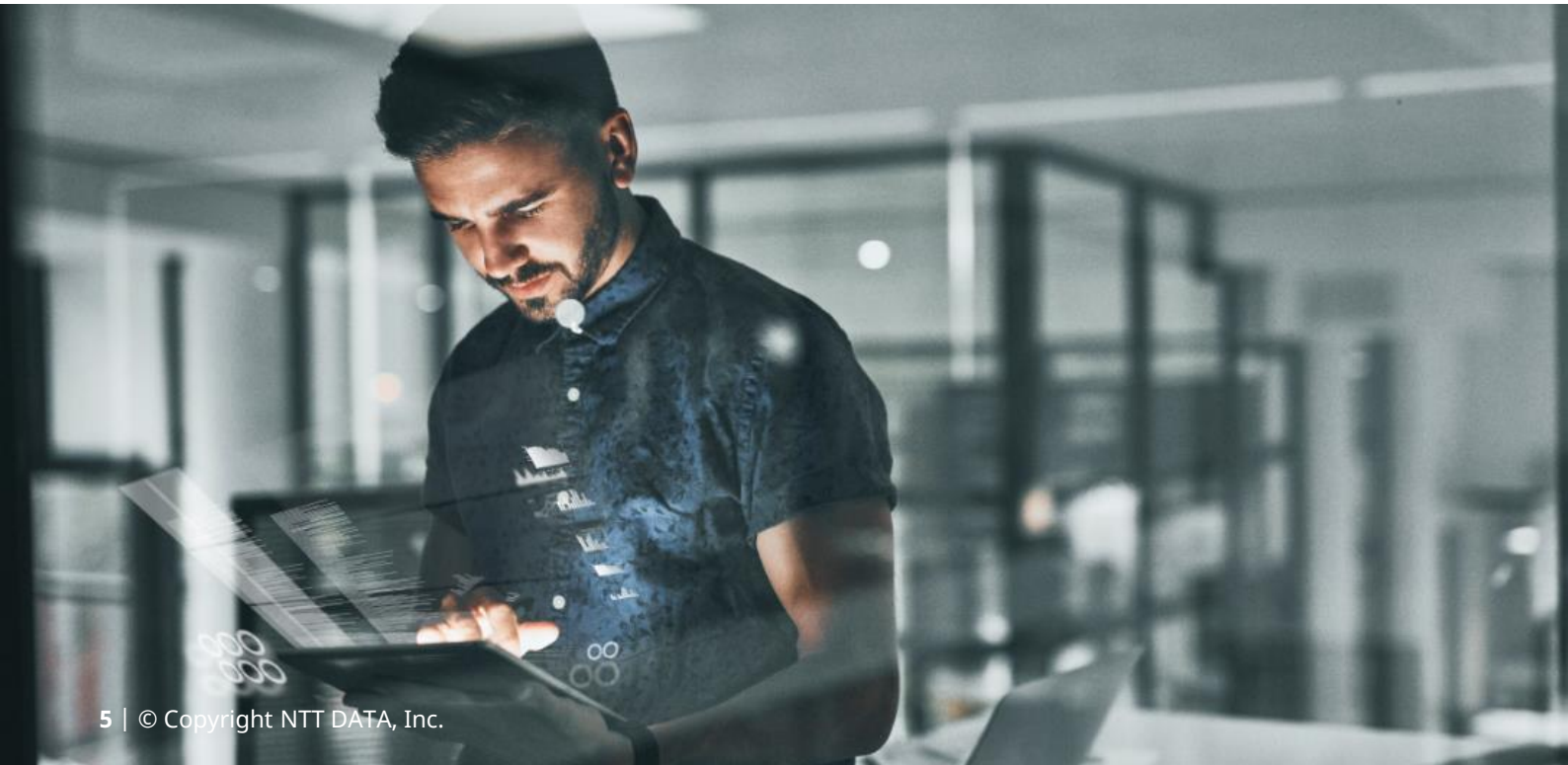
Aunque es probable que el robo de información se produjera un año antes, el incidente salió a la luz recientemente, generando preocupaciones sobre la seguridad de los datos en entidades gubernamentales.

En el sector educativo, el Sistema de la Universidad Tecnológica de Texas (Texas Tech University System) informó el 23 de diciembre de 2024 sobre una filtración de datos que comprometió información personal de estudiantes y empleados. Aunque no se han revelado detalles específicos sobre el alcance del incidente, la universidad está trabajando con expertos en ciberseguridad para investigar y mitigar el impacto.

En resumen, de los incidentes de ciberseguridad analizados se desprenden tres conclusiones clave:

1. **Incremento de ataques de *ransomware* y filtraciones de datos:** organizaciones de diversos sectores, como salud, finanzas y energía, han sido víctimas de ataques que comprometen información sensible y afectan la continuidad de sus operaciones. Este aumento en la frecuencia y sofisticación de los ataques resalta la necesidad de fortalecer las medidas de seguridad.
2. **Importancia de la capacitación y concienciación del personal:** varios incidentes se originaron por errores humanos, como la descarga inadvertida de *malware* o la divulgación de credenciales. La formación continua en protocolos de ciberseguridad y la promoción de una cultura de seguridad son esenciales para mitigar estos riesgos.
3. **Necesidad de una respuesta rápida y efectiva ante incidentes:** la capacidad de detectar, contener y mitigar ciberamenazas de manera eficiente es crucial para minimizar el impacto de los ataques. Implementar planes de respuesta a incidentes y realizar simulacros periódicos pueden mejorar significativamente la resiliencia organizacional.

Estos puntos subrayan la importancia de una estrategia integral de ciberseguridad que abarque tanto la prevención como la respuesta efectiva a incidentes.



2025, año internacional de la Quántica

Espacio cuántico
por María Gutiérrez

La UNESCO ha establecido el 2025 como el Año Internacional de la Ciencia y la Tecnología Cuánticas, con esta iniciativa pretende “aumentar la conciencia pública sobre la importancia de la ciencia cuántica y sus aplicaciones, así como sensibilizar a la sociedad sobre el impacto de estas investigaciones en nuestra vida cotidiana y en el futuro del planeta”, además de celebrar y reconocer los 100 años los primeros desarrollos teóricos de la mecánica cuántica.

Aunque hoy día ya podemos disfrutar de algunas aplicaciones de la cuántica, por ejemplo, láseres, fibra óptica, relojes atómicos, microondas, televisión digital, ordenadores, etc. lo que viene es realmente revolucionario, con impacto en sectores como la medicina, el clima, la energía, la seguridad alimentaria, el agua, etc. nos permitirá tener ordenadores más potentes, comunicaciones más seguras, materiales con mejores propiedades o medidas más precisas, así como posibles explicaciones a muchos fenómenos biológicos y físicos.

Es verdad que el hardware aún no está totalmente disponible, pero sí que ya el mercado está centrando sus esfuerzos en el desarrollo de los más diversos algoritmos: Algoritmos de optimización, algoritmos híbridos y algoritmos de inspiración cuántica.

Las empresas también se están preparando para la transición cuántica identificando la criptografía que no es resistente a la cuántica, por lo que es crucial empezar a crear capacidades, formar al personal y fomentar la concienciación sobre la integración de la informática cuántica en nuestros sistemas.

NTT DATA cuenta con un equipo de Quantum, con la misión de preparar a los clientes para el futuro cuántico, con servicios relacionados con la transición a algoritmos post-cuánticos, avances en genómica, optimización de carteras financieras, logística o ciberseguridad ... alineando la tecnología con la estrategia para una adopción sin fisuras y una ventaja competitiva, y lo hace alrededor de estos elementos:

Computación híbrida

La integración de la informática cuántica y la clásica permite emular posteriormente principios o comportamientos de la física cuántica. De este modo, se abordan las limitaciones actuales al tiempo que se prepara para el pleno potencial de la cuántica.

Metodología basada en casos prácticos

Nuestra forma de trabajar consiste en utilizar los conocimientos sobre tecnología para adaptarla a las necesidades de nuestros clientes y crear casos de uso valiosos.

Creación de conexiones

Creamos una red de contactos para facilitar la cooperación, la investigación y el desarrollo de la tecnología. Nos aliamos con universidades, fabricantes y proveedores que trabajan en el campo de la computación cuántica.

La computación cuántica está en sus inicios, pero evoluciona rápidamente, con avances significativos en hardware, algoritmos y aplicaciones. Las organizaciones que trabajen y exploren para comprender y aprovechar la computación cuántica en esta fase temprana obtendrán una ventaja competitiva en sus respectivos campos.

A lo largo de los siguientes meses os iremos contando las iniciativas y proyectos cuánticos en los que estamos trabajando

12 grandes hitos de nuestros 100 números

1. A. PinTo, la nueva incorporación en plantilla

Artículo Mayo 2017

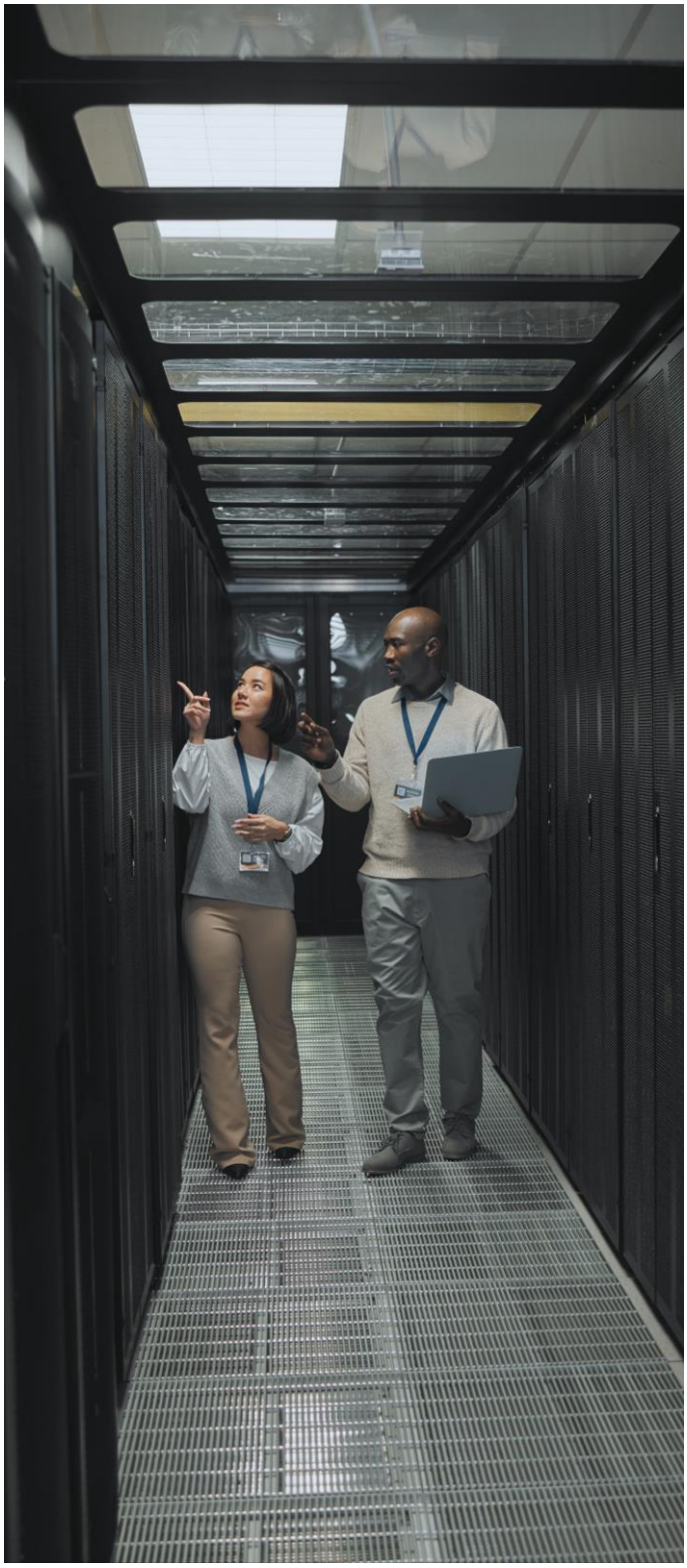
Una de las ciberamenazas que más preocupan a las organizaciones es la que se conoce como APT, las siglas de *Advanced Persistent Threat*. Podemos definirla como el conjunto de acciones y procesos continuos que, de manera sigilosa, sirven para realizar actividades maliciosas. Las APTs son amenazas muy dirigidas que buscan obtener de forma ilícita información sensible, de valor comercial, financiero, etc. Como su nombre indica, hacen uso de las más avanzadas técnicas y tipos de ataques para conseguir penetrar en un sistema y mantener el acceso durante largos periodos de tiempo (pueden ser semanas, meses o incluso años). El objetivo es extraer la mayor cantidad de información posible.

Debido a sus características y a la persistencia de la intrusión, una APT podría incluso considerarse el peor fichaje que puede hacer una empresa.

¿Qué se busca?

Este tipo de ataques suele estar enfocado a obtener un beneficio considerable, normalmente causando un importante perjuicio a la víctima. Los motivos más comunes suelen ser:

- **Motivación económica:** se busca lograr un beneficio económico directo mediante el robo de datos bancarios, la falsificación de facturas, el chantaje, la venta de información, etc.
- **Robo de información:** extracción de información privada de usuarios, comercial, sobre proyectos actuales y futuros, etc.
- **Competencia desleal:** obtener información sobre estrategia comercial, actividades de investigación y nuevos desarrollos, sabotear los sistemas, etc. Básicamente se persigue lograr una ventaja competitiva ya sea adelantándose a la empresa víctima o perjudicándola.
- **Daño a la reputación de la empresa:** en ocasiones el objetivo es dañar la imagen de una empresa, filtrando información interna, comprometiendo sistemas, etc.



¿Cómo lo hacen?

Es difícil determinar un modo de actuación ya que la característica principal de este tipo de ataques es que son dirigidos, y, por tanto, muy personalizados. A pesar de esto, podemos agrupar al conjunto de técnicas en una serie de acciones relativamente habituales:

1. Reconocimiento y escaneo del objetivo

Cuando se decide atacar a un objetivo se comienza por la recopilación de datos. Esta búsqueda se realiza de manera progresiva, empezando por técnicas donde el contacto con la víctima es nulo, usando datos de fuentes OSINT para recopilar noticias relevantes, contactos, datos personales, etc.

Se investiga de forma pasiva al objetivo para obtener toda aquella información estratégica que pueda servir para que el ataque sea efectivo. Esto incluye recolección de nombres de usuario, direcciones de correo o sitios web.

Una vez finalizado este primer reconocimiento pasivo, se realiza una investigación de la infraestructura externa para descubrir potenciales puntos de entrada que puedan ser explotadas para lograr el acceso inicial.

Estas actuaciones suelen ser activas, tienen un efecto directo y es posible detectarlas. Incluye acciones como el escaneo de puertos e IP, identificación de servicios REST/API, detección de vulnerabilidades, etc.

Los atacantes completarán el mapa de la organización utilizando técnicas de escaneo donde ya se toca a la víctima, lo que puede levantar las primeras sospechas.

2. Obtención de acceso / Intrusión inicial

La fase anterior va a proveer a los atacantes de la información necesaria para obtener el primer acceso. Ahora el objetivo es penetrar en la red y establecer un punto de entrada en los sistemas desde el que ir expandiéndose. Para lograrlo se ejecutan ataques contra las vulnerabilidades encontradas mediante exploits, inyecciones de código o incluso acciones de ingeniería social contra correos de empleados.

En este punto resulta más sencillo detectar este tipo de amenazas, ya que habitualmente se está actuando desde el exterior de la infraestructura de red.

3. Establecimiento del punto de entrada

Una vez conseguido el acceso a la red y a los sistemas, el siguiente paso crítico es el establecimiento de un punto de entrada estable, conocido como foothold o beachhead en inglés. De este modo, el atacante podrá continuar su intrusión en la red, buscando cómo avanzar hasta llegar a su objetivo.

Desde dicho punto se establece una conexión con el centro command & control del atacante, normalmente utilizado exclusivamente para cada APT, de manera que se reducen las posibilidades de ser detectado.

4. Movimiento lateral

Es la fase más larga del ataque, que se puede extender durante varios meses o incluso años. El atacante ya ha conseguido entrar en la red/infraestructura de la empresa y busca un mayor acceso para alcanzar su objetivo. En esta etapa se realizan varias acciones:

- **Persistencia:** El primer paso, y punto fundamental para el atacante, es la persistencia: asegurar su presencia dentro de la red. Para ello es común el uso de malware diseñado a medida para pasar desapercibido y mantener el acceso.
- **Reconocimiento interno:** Asegurada la acción anterior, se procede a investigar nuevos accesos, seleccionando los siguientes saltos en la red que se llevarán a cabo para aumentar el rango de acción de los atacantes.
- **Escalado de privilegios:** Tras fortalecer su posición, el intruso continúa el análisis mediante el escalado de privilegios y el robo de credenciales para poder ampliar el acceso a nuevos sistemas dentro de la red.

Estos tres pasos se repiten durante toda la intrusión, permitiendo conseguir y avanzar hacia el objetivo, ya sea extraer información, comprometer los sistemas, o cualquier otro.

5. Extracción de datos y borrado de huellas

Finalmente, una vez que se logra acceder a la información objetivo, se procede a su extracción, completando de esta manera el ataque.

A continuación, el intruso suele borrar las huellas que haya podido dejar, dificultando de esta manera que se pueda determinar cómo logró el acceso a la información una vez descubierta su actuación.

Otra acción muy común, junto con el borrado de huellas, es la instalación de un malware común para distraer a los equipos de IT y complicar la detección del ataque real.

Malware a la carta

Un negocio que ha proliferado considerablemente en los últimos años, y que es provisto en su mayoría a través de desarrolladores que se ofrecen en la Deep Web, es el de la generación de malware a la carta, diseñado a medida contra un objetivo en particular.

En total, se estima que este tipo de actividades, impulsadas especialmente por el ransomware, movió en 2016 más de 1.000 millones de dólares (918,3 millones de euros), según indica el Informe Anual de Seguridad de Trend Micro.

Estos servicios se complementan con otros más tradicionales, como los DDoS, también bajo demanda y durante periodos de tiempo acordados, o el alquiler de equipos zombi de una botnet para su uso en distintos ataques como distribución masiva de malware, minería de bitcoins o craqueo de claves.

Recomendaciones

Como se ha podido observar, las APTs son ciberamenazas sofisticada, de ejecución compleja y suelen tener un gran impacto sobre las organizaciones que las sufren. Si bien estos ataques suelen ser muy elaborados, no son invisibles y pueden ser detectados.

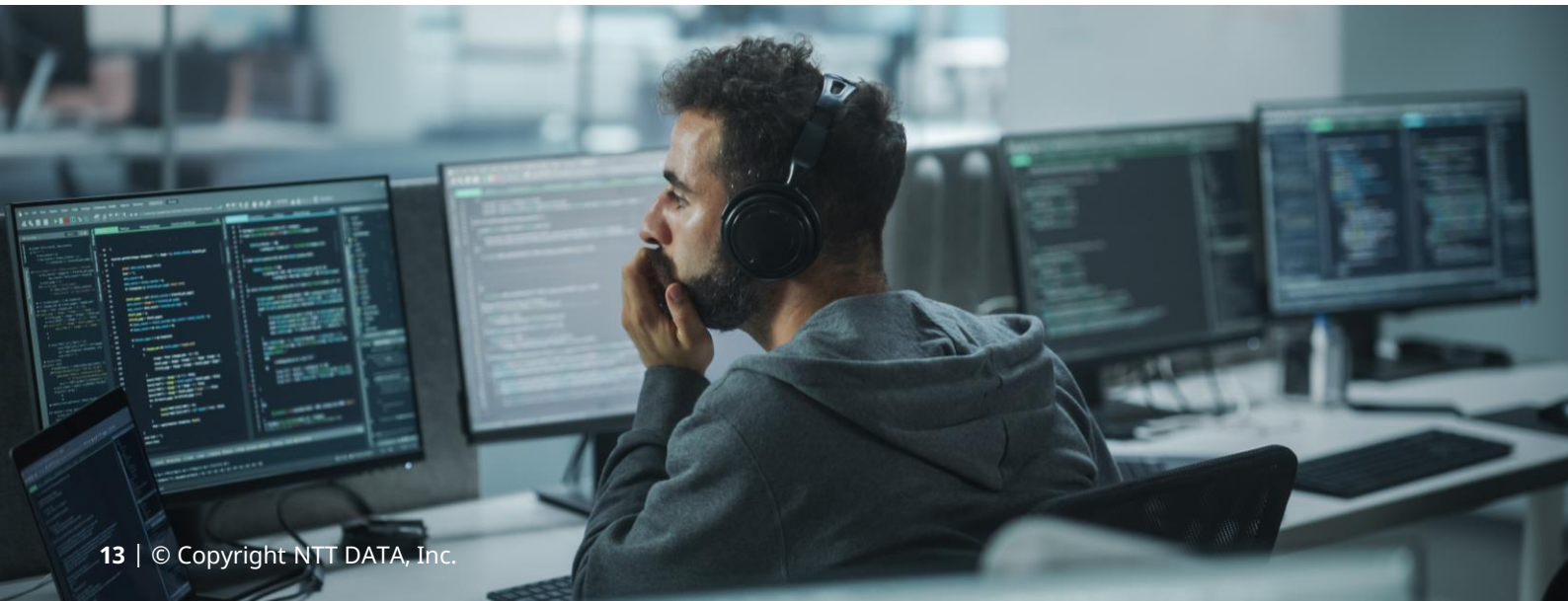
Desde un punto de vista técnico, el control sobre la red de la organización y sobre las conexiones entrantes y salientes adquiere una especial importancia en la prevención de APTs. Son de especial interés en este contexto:

- La monitorización de los elementos de red.
- Las políticas de actualización del software.
- La implementación de soluciones SIEM/IDS para detectar logins no válidos, accesos no controlados, etc.

Por otro lado, muchas veces los eslabones más débiles en la cadena de seguridad, y a través de los que en ocasiones se consigue acceso a las redes de las empresas, son los propios empleados, normalmente poco preparados y concienciados sobre estos temas.

Por ello, toda organización debería impulsar medidas preventivas:

- Desarrollar campañas de concienciación de los trabajadores para evitar robos de credenciales, infecciones, etc.
- Ofrecer formación en buenas prácticas en ciberseguridad.
- Disponer de equipo de respuestas a incidentes y de atención al empleado.



12 grandes hitos de nuestros 100 números

2. Coches inteligentes pero, ¿ciberseguros?

Artículo Agosto 2017

Los nuevos modelos de coches son, cada vez más, un alarde de tecnología y conectividad. Si bien la experiencia de los conductores ha mejorado notablemente en los últimos años gracias a ello, tanto la creciente dependencia de los ordenadores como la entrada de Internet en nuestros vehículos introducen nuevos riesgos a los que la industria debe hacer frente.

Vivimos en un mundo cada vez más interconectado. Prueba de ello es el avance en el uso de la tecnología que el sector de la automoción viene experimentando en los últimos años. Por ejemplo, ya es poco habitual encontrar coches que tengan reproductor de CD y, en su lugar, es más común la presencia de puertos USB a través de los que es posible conectar cualquier dispositivo al ordenador de abordo e interactuar con él, instalar nuevas aplicaciones, etc.

Otras características que presentan los nuevos modelos de automóvil son la sincronización con smartphones, la apertura de puertas mediante Bluetooth, la posibilidad de conducir y aparcar de forma autónoma o de utilizarlos como punto de acceso WiFi.

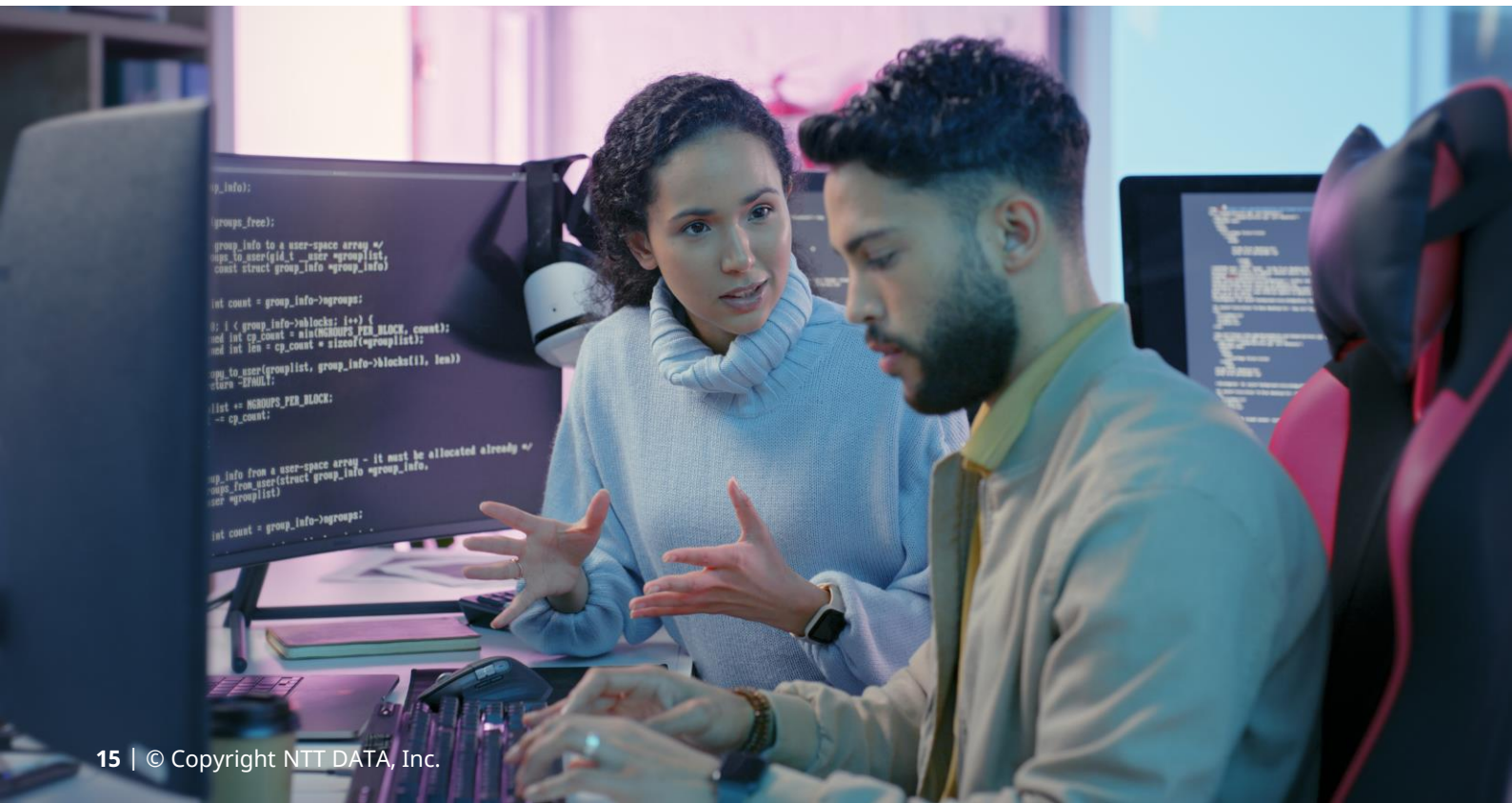
Todo esto supone una mejora significativa para la usabilidad y la comodidad de los usuarios, pero ¿qué riesgos conlleva?

Riesgos y amenazas

Uno de los factores a tener en cuenta es que los protocolos de comunicación utilizados en los vehículos fueron diseñados hace años con unos requisitos de seguridad que, en la actualidad, se encuentran anticuados.

Un ejemplo es el protocolo CAN (Controller Area Networking, por sus siglas en inglés), desarrollado en los años 80 con topología de bus y que se caracteriza por poder transportar tramas de hasta 64kb de datos.

Entre dichas tramas se incluye el identificador de prioridad del mensaje transportado, responsable de establecer el orden de ejecución de las acciones del vehículo.



Riesgos y amenazas

Uno de los factores a tener en cuenta es que los protocolos de comunicación utilizados en los vehículos fueron diseñados hace años con unos requisitos de seguridad que, en la actualidad, se encuentran anticuados.

Un ejemplo es el protocolo CAN (Controller Area Networking, por sus siglas en inglés), desarrollado en los años 80 con topología de bus y que se caracteriza por poder transportar tramas de hasta 64kb de datos.

Entre dichas tramas se incluye el identificador de prioridad del mensaje transportado, responsable de establecer el orden de ejecución de las acciones del vehículo.

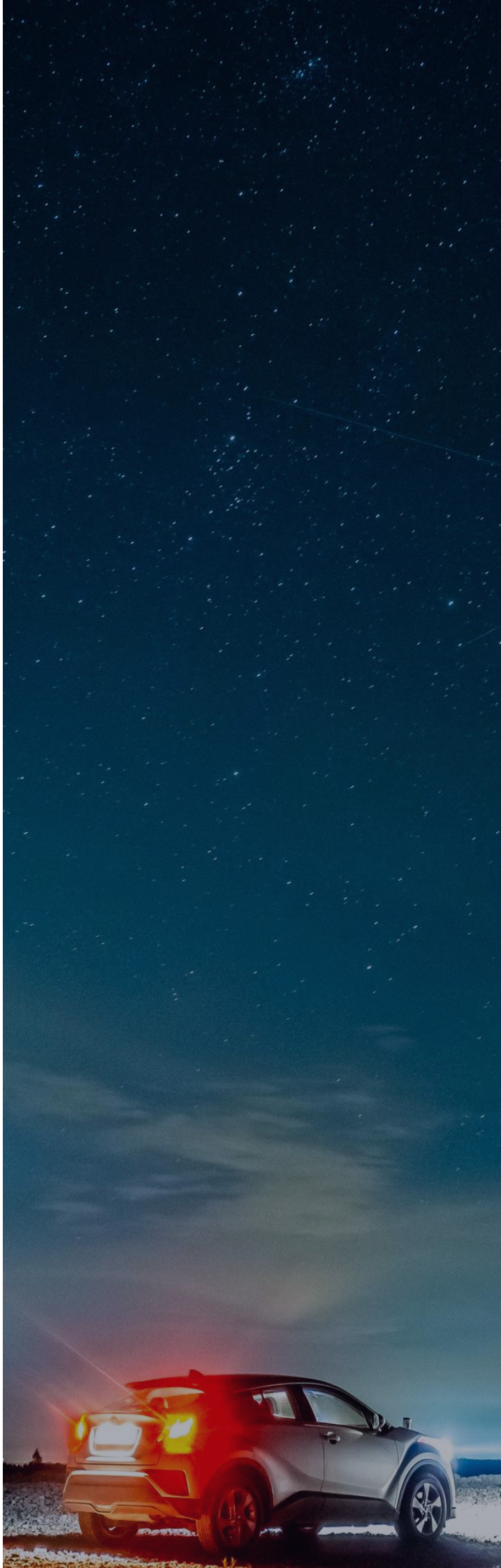
Entre otras cosas, el protocolo CAN permite controlar el motor e interconectar las ECU (Unidades de Control Eléctrico), el cierre centralizado, la apertura de techo solar, las luces, el climatizador o el cuadro de mandos. Debido a su topología, cualquier dispositivo que se conecte al bus podrá enviar mensajes al resto de módulos y que estos le escuchen.

Cabe destacar que este intercambio de mensajes no está cifrado, por lo que es susceptible de ser interceptado y manipulado, pudiendo llegar a provocar una denegación de servicio (DoS) en vehículos comprometidos.

Dado que este protocolo se encuentra implementado en la mayoría de los modelos de coches, un atacante podría utilizar un microcontrolador para inyectar tramas a través del conector OBD-II (*On Board Diagnostic*) y modificar remotamente el comportamiento de las luces, los testigos de aviso o cualquier otro módulo del vehículo, tal y como demostraron Sheila Berta y Claudio Caracciolo en la conferencia Ekoparty de 2016. Además, como la ubicación de este conector no suele ser conocida, es más complicado para un conductor determinar si está siendo víctima de un ataque o si se trata de un fallo real del vehículo.

Por tanto, en función del número de módulos conectados al bus CAN que puedan ser vulnerados por un atacante y las funciones que realicen, la criticidad del ataque será más o menos elevada.

Por ejemplo, si el cuadro de mandos se encuentra comprometido, se podría modificar e indicar que el motor se ha sobrecalentado o que le falta aceite, y así tener que detener el coche.



La conectividad de los dispositivos

Siguiendo con el tema del acceso físico, cabe destacar que acciones como conectar un dispositivo USB, sincronizar nuestro smartphone o tablet para poder interactuar con el vehículo, o personalizarlo con herramientas de hacking como MZD-AIO-TI (MDZ All In One Tweaks Installer, un todo en uno que permite instalar nuevas aplicaciones para alterar el software de fábrica de Mazda), conllevan riesgos: si el dispositivo que conectamos se encuentra infectado con malware o contiene código malicioso, es posible que el coche se vea comprometido.

Jay Turla lo demostró en una PoC (Proof of Concept, por sus siglas en inglés), al conectar a un Mazda3 una memoria USB que contenía una serie de scripts que ejecutaba de forma remota y cuyo resultado se mostraba en la pantalla del dashboard del automóvil.

Al tratarse de una PoC, el código tan sólo devolvía el tipo y versión del sistema operativo instalado, pero podría tratarse de órdenes más críticas que alterasen el funcionamiento del vehículo o pudieran suponer un riesgo para la seguridad ciudadana.

Recientemente se ha conocido que la oleada de ataques provocados por el ransomware Wannacry llegó a afectar también al sector automovilístico.

Algunas plantas de Renault y Nissan en Japón, Reino Unido, Francia, Rumanía e India tuvieron que parar la producción por tener su red comprometida y temer por la posibilidad de que se infectaran los productos. ¿Qué podría pasar si en un coche se ejecutara dicho ransomware?

Sería algo similar a lo que ocurre en el resto de equipos informáticos, se cifraría todo el sistema y pediría un rescate para poder desbloquearlo y retomar la conducción.

A día de hoy aún no se han dado casos reales de ello y toda la información al respecto es teórica. Sin embargo, debido a la evolución constante del IoT y la interconectividad, no es descabellado pensar que podría producirse en cualquier momento.

Por otra parte, a medida que la conexión a Internet se va extendiendo en este sector, aparecen otras vías de ataque diferentes a la conexión física mediante microprocesadores.

Desde el punto de vista de la seguridad de la información, equipar los coches con sistemas cada vez menos dependientes del factor humano y delegar en ellos acciones tan delicadas como el control de la conducción o de la distancia de seguridad obliga a garantizar que estén correctamente segurizados.

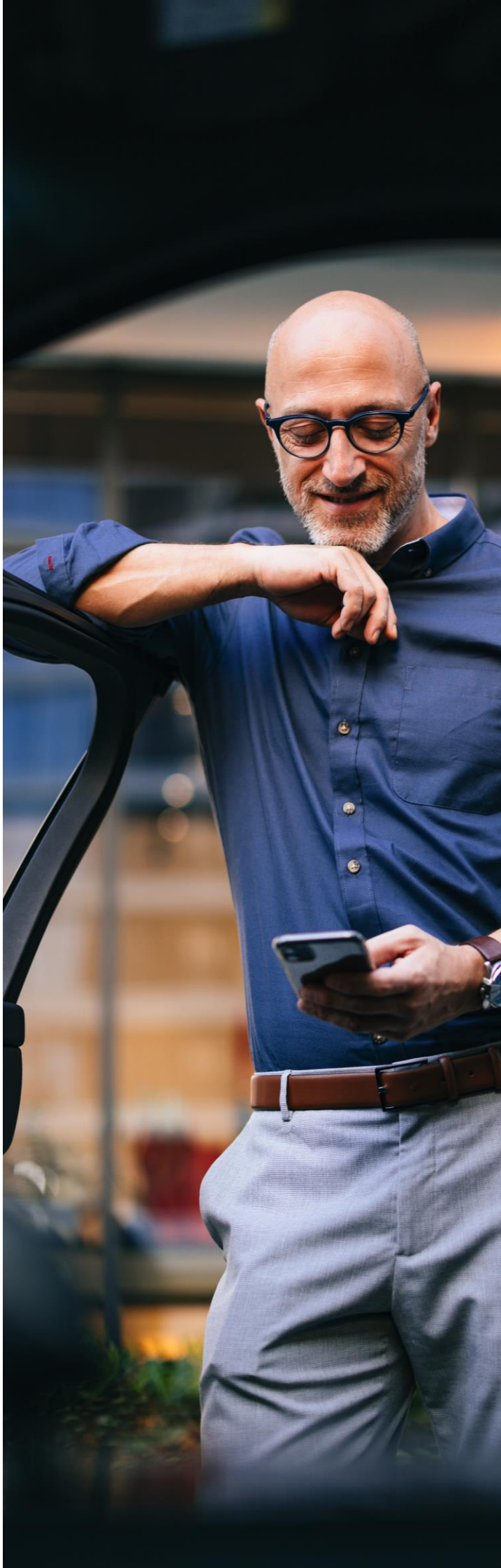
Si no es así, un usuario malicioso pueda aprovecharse de las brechas de seguridad existentes y tomar el control del vehículo de forma remota, llegando incluso a poner en peligro la vida de sus ocupantes.

Precisamente este ha sido uno de los temas protagonistas en varias ediciones de la Black Hat y la DEF CON, las dos conferencias de ciberseguridad más importantes en el mundo del hacking, en las que Chris Valasek y Charlie Miller han presentado sus investigaciones en esta materia. Entre sus contribuciones más sonadas destaca que, en 2015, fueron capaces de controlar de forma remota un Jeep Cherokee aprovechando únicamente que su sistema multimedia se encontraba expuesto en Internet.

Gracias a ello era posible hackearlo desde cualquier ubicación geográfica (en este caso desde el sofá de su casa) para hacerse con el control del sistema de climatización, el audio, los limpiaparabrisas o incluso llegar a bloquear los pedales y apagar el motor.

Esta vulnerabilidad ya ha sido corregida por la firma y según el último estudio de estos investigadores, publicado en 2016, era necesario tener conectado el portátil al sistema informático del coche para realizar el ataque.

Otro tema de interés son los smartphones y las aplicaciones móviles que distribuyen las marcas de automóviles para comunicarse con el vehículo y controlarlo. El año pasado Troy Hunt demostró cómo era posible acceder a un Nissan LEAF a través de la aplicación móvil de la marca, lo que permitía actuar sobre el sistema de climatización o recopilar información almacenada en el ordenador de abordo sobre los viajes recientes, consumo o estado de carga.



Para realizar este ataque bastaba con utilizar un proxy intermedio que capturara las peticiones que la aplicación móvil enviaba al servidor, en las cuales se podía identificar fácilmente dentro de la URL el VIN (Número de Identificación del Vehículo o número de bastidor). Esto, sumado a que es muy sencillo conocer dicho número, implica que era posible hacerse con cualquier Nissan LEAF de forma remota.

Además, Hunt probó que se podía realizar un ataque de fuerza bruta de forma anónima para listar los números de bastidor de diferentes coches de esa marca y obtener datos o controlar remotamente aquellos que respondieran exitosamente a la petición. La aplicación no verificaba la identidad del usuario ni registraba información de la sesión.

Por último, no podemos olvidarnos del eslabón más débil de la cadena: el ser humano. Hace unos meses dos hackers utilizaron técnicas de ingeniería social para engañar a un usuario que esperaba mientras repostaba en una estación de servicio Tesla.

El anzuelo consistía en ofrecer WiFi gratis y una hamburguesa de regalo si se descargaba una aplicación móvil. Lo que el usuario no sabía es que esa aplicación contenía un malware que, una vez instalado, robaba y enviaba a los atacantes sus datos, incluyendo las credenciales que permitirían acceder y arrancar el vehículo.

Por todo esto se hace necesario tomar conciencia de lo importante que es tanto la actualización constante del software del vehículo como la incorporación de la ciberseguridad al inicio del ciclo de vida y desarrollo de cualquier producto que contenga componentes electrónicos o informáticos.

La mejor forma de prevenir incidentes de seguridad es aplicando las medidas necesarias en el momento de crear y hacer uso de la tecnología.

3. *Machine Learning*: enseñando ciberseguridad a nuestras máquinas

Artículo Abril 2018

La tecnología se mueve rápidamente y, con ella, el deseo por tener el conocimiento y la habilidad de adelantarse a los usuarios. Todos los días usamos y somos usados por esta tecnología que permite predecir qué es lo que el usuario quiere a través del análisis estadístico de enormes cantidades de datos como ubicaciones, búsquedas en Internet o relaciones de amigos. En este artículo vamos a hablar del machine learning y cómo se puede aplicar a la ciberseguridad.

Un ejemplo sencillo de machine learning lo podemos encontrar en la mayoría de los portales de venta. Cuando estamos ojeando productos, la propia página se encarga de recomendarnos otros que nos podrían interesar y, generalmente, aciertan con nuestros gustos. Estos sitios hacen uso del machine learning para sugerir artículos que posiblemente el potencial comprador quiera adquirir y lo hace en función de los datos obtenidos de otros usuarios que están buscando lo mismo. Pero ¿se podría aplicar esta tecnología a la ciberseguridad?

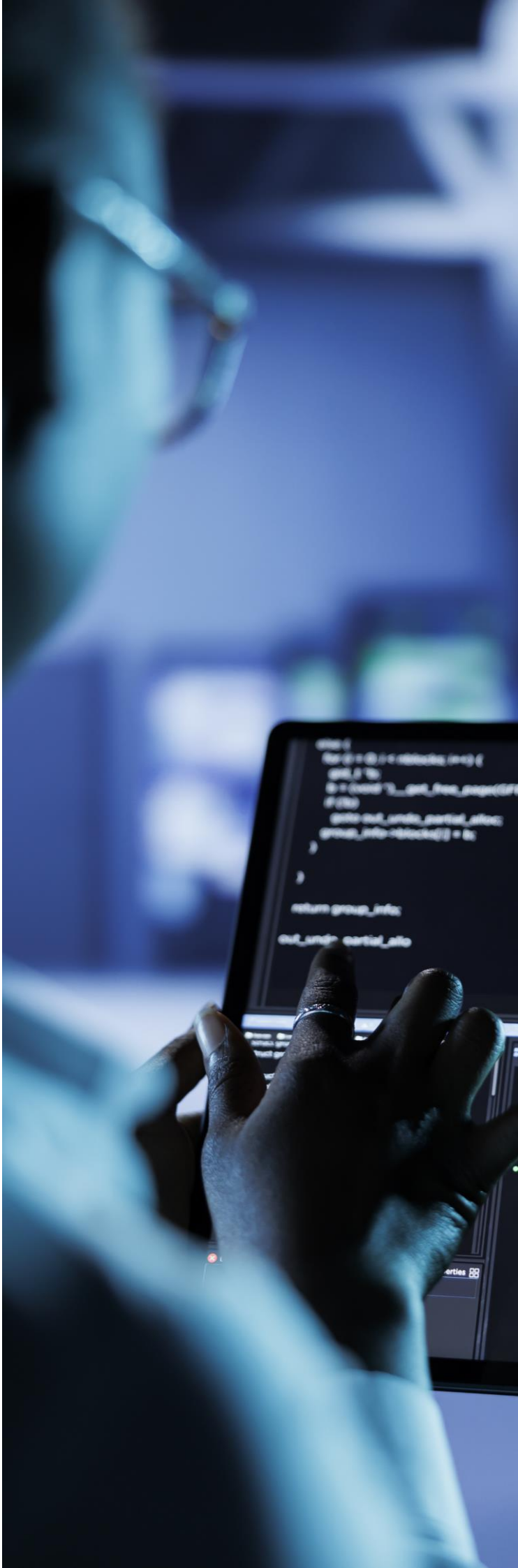
Antes de entrar en materia, hay que definir más detalladamente en qué consiste el machine learning. Como su propio nombre indica, esta tecnología trata de enseñar a una máquina a tomar decisiones por sí misma mediante inteligencia artificial. Esta hace que el desarrollador no tenga que programar manualmente lo que la maquina tiene que hacer, sino que ella se encarga de elegir qué es lo correcto, siendo capaz de resolver problemas para los que un algoritmo estático no podría encontrar solución.

Digamos que, por ejemplo, queremos que nuestra máquina aprenda a distinguir señales de tráfico, más específicamente una señal de stop y de una de prohibido. Para ello, le vamos a entregar 20 imágenes distintas de stops. Si la máquina nos devuelve que 17 de esas imágenes son stops y 3 de ellas prohibidos, podríamos decir que tiene un 85% de acierto. Pero necesitamos que ese porcentaje aumente, por lo que esta vez le vamos a pasar 1.000 imágenes, 10.000 o todas las que hay en Google Maps. De esta forma, a medida que va recibiendo más información, va mejorando su capacidad de detectar cada una de las señales de tráfico que se le aportan.

Podríamos dividir el machine learning en tres grupos según su funcionamiento:

- **Aprendizaje supervisado:** utiliza información de datasets etiquetados para su entrenamiento. Así, analizando datos y aprendiendo a diferenciarlos, es capaz de predecir la etiqueta de un nuevo dato sin etiquetar. Por tanto, este tipo de algoritmos se utilizan para clasificar y categorizar.
- **Aprendizaje no supervisado:** a diferencia del anterior, el algoritmo no tiene etiquetas en los datos para orientarse, sino que es él mismo el que categoriza los datos en función de los patrones que encuentra.
- **Aprendizaje por refuerzo:** esta técnica se basa en recompensar al algoritmo cuando acierte en su predicción y en castigarle cuando falle. De esta manera, va aprendiendo por técnicas de prueba y error a realizar mejor su tarea. Es la técnica más prometedora porque no necesita de grandes cantidades de datos para entrenar al algoritmo. Actualmente se está aplicando en los sistemas de conducción autónoma.

En la actualidad disponemos de enormes cantidades de datos, lo que llamamos big data, por lo que podríamos utilizar técnicas de *machine learning* en cualquier área de conocimiento que se nos ocurra.

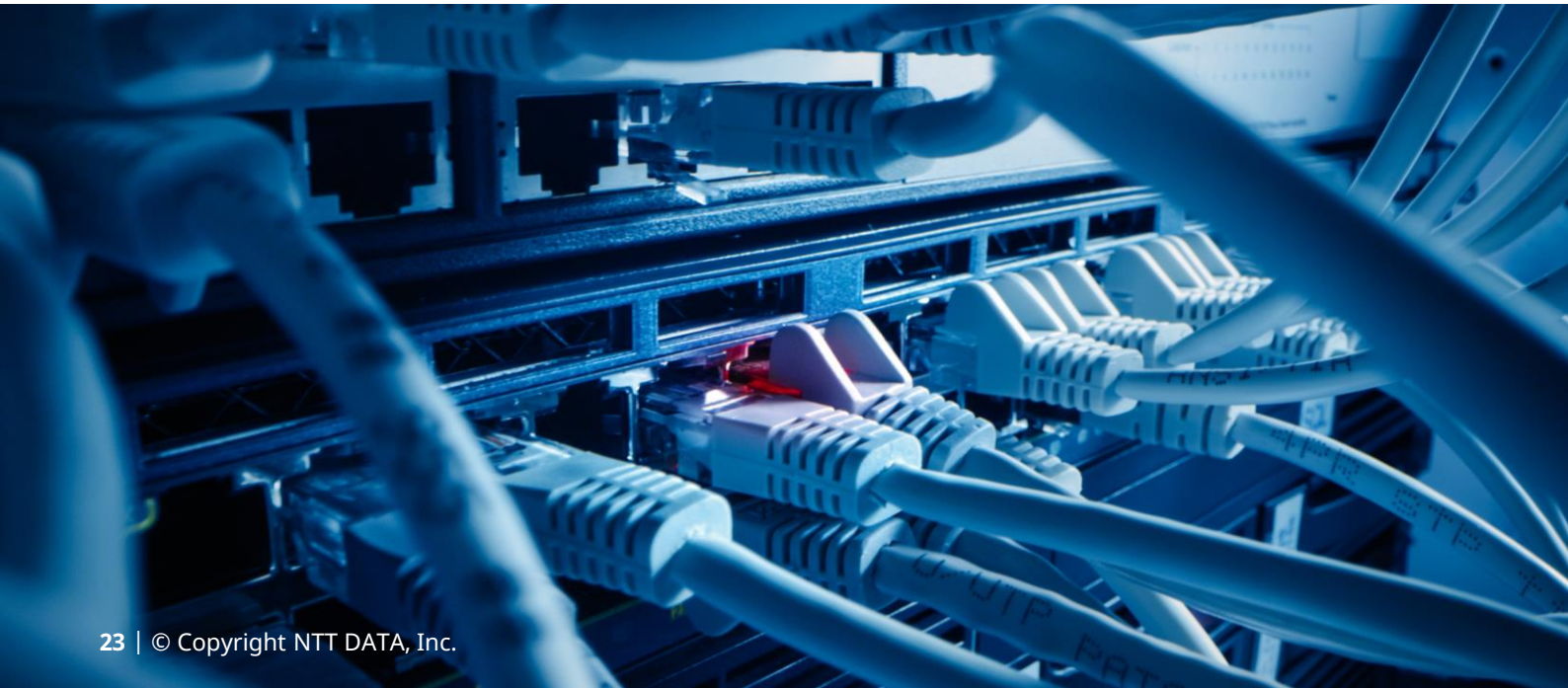


Aplicaciones en la ciberseguridad

El *machine learning* se está aplicando en diversas áreas científicas debido a su adaptabilidad, escalabilidad y capacidad para ajustarse rápidamente a retos desconocidos. Utilizando el *machine learning* como método de apoyo para la ciberseguridad es posible hacer que la máquina pueda predecir cuándo va a ser atacada y decidir cómo puede defenderse, previniendo distintos ataques y analizando los patrones y herramientas que utilizan los delincuentes. Se está utilizando *machine learning* en ciberseguridad especialmente para:

- **Detección de phishing y spam:** analizando los patrones de cuentas de correo emisoras, estructuras de mensaje y su contenido, el algoritmo es capaz de aprender qué puede ser phishing o spam y de aislar los mensajes del buzón del usuario, llegando a ser posible incluso el bloqueo de las direcciones de envío.
- **Sistema de detección de intrusos (IDS):** el IDS monitoriza la red buscando actividad sospechosa. Los sistemas tradicionales se basan en reglas y en una serie de comportamientos esperados en Internet. Los ataques sofisticados pueden saltarse estas medidas defensivas con facilidad porque utilizan patrones nuevos no esperados. Se está aplicando el machine learning para analizar millones de ataques e intentos de intrusión para que el sistema por sí solo evalúe si está siendo atacado o no e intente mitigar o bloquear por completo el problema.
- **Análisis de malware:** se usa como apoyo al analista forense a la hora de recopilar información del sistema atacado, facilitando el etiquetado de logs, organizando las pruebas de ficheros modificados y analizando qué código puede ser nocivo.

Sin embargo, hay que tener en cuenta que, de la misma manera que se está aplicando el aprendizaje automático en la mitigación de ataques, también se está usando por parte de los atacantes para idear malware más sofisticado que sea capaz de esquivar por sí mismo las medidas defensivas del sistema objetivo.



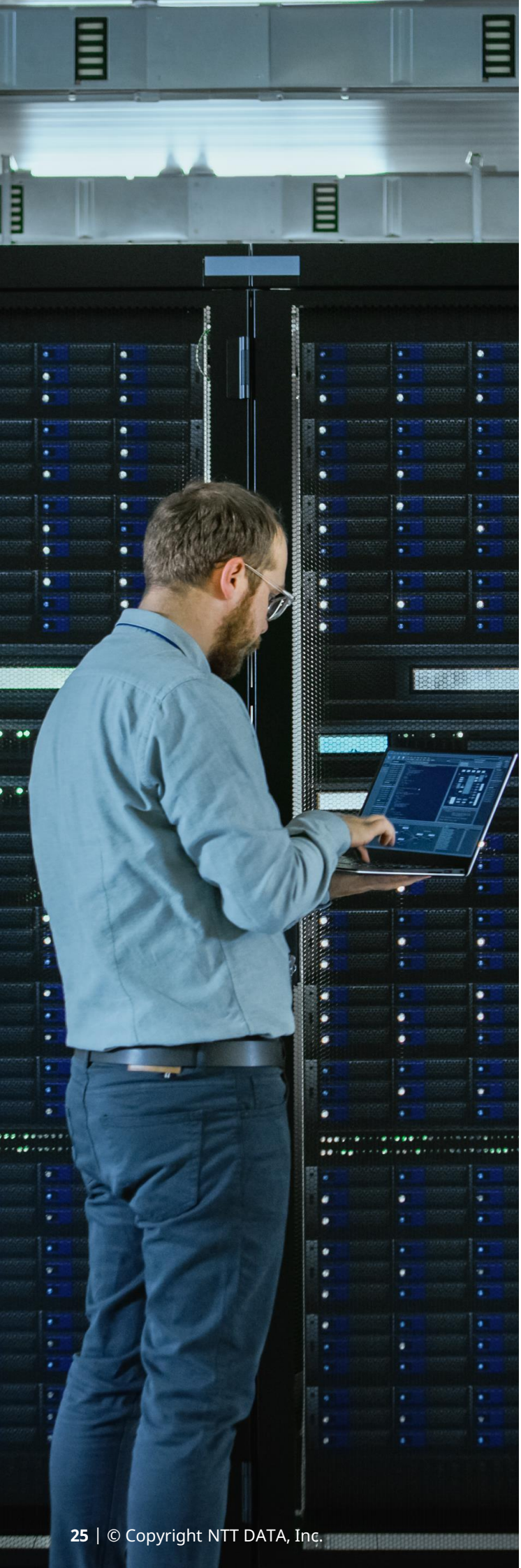
Aplicaciones en otras áreas

En la actualidad, el *machine learning* está siendo usado por muchas compañías que necesitan tratar con enormes cantidades de datos para ofrecer a sus usuarios una experiencia más satisfactoria y personalizada. Los gigantes de la tecnología y la información llevan varios años mejorando y apostando por el *machine learning*, entre estas empresas podemos encontrar a:

- **Amazon:** uno de los portales de venta más grandes del mundo también posee una de las plataformas de inteligencia artificial y *machine learning* más desarrolladas. Mientras compramos y navegamos por su web, nos va sugiriendo artículos que nos interesaría adquirir en función de las compras y patrones de búsqueda de otros usuarios. Amazon también aplica esta tecnología en sus servicios web, AWS, y en su inteligencia artificial, Alexa.
- **Google:** el buscador por excelencia es uno de los pioneros en el uso de la inteligencia artificial y también uno de los que más la emplean. Aplica sus algoritmos de *machine learning* en casi todos sus servicios para ofrecer al usuario los resultados que está buscando (Google. com, Youtube, Google Now), la publicidad que le interesa (AdSense), la traducción que más se asemeja al lenguaje natural (Google Translate) o la autogestión de los correos que recibe (Gmail).
- **Salesforce:** es la compañía estadounidense de *cloud computing* y *big data* con mayor valor del mundo. Son los creadores de Einstein, una inteligencia artificial implementada en sus servicios en la nube, ventas, marketing y aplicaciones, diseñada para mejorar muchos de sus productos con algoritmos de *machine learning.*

Estos son solo un par de ejemplos, pero muchas otras grandes compañías como Facebook, Tesla, Netflix, Microsoft, Apple, Intel, IBM o Alibaba también están usando esta tecnología.

.



Desventajas a tener en cuenta

Como contrapunto a todo lo anterior, tenemos que advertir que no todo en el mundo del *machine learning* es favorable, pues esta tecnología tiene sus desventajas

Se trata de una tecnología cara, que necesita una gran cantidad de recursos computacionales. Generalmente, la computación más utilizada se basa en la nube ya que posee la capacidad de adaptarse a nuestras necesidades en cada momento, pero los alquileres de estas grandes máquinas no son baratos. Para que esta tecnología se desarrolle, necesita de una inmensa cantidad de muestras y datos útiles para que el algoritmo aprenda y pueda reducir su margen de error, ofreciendo menos falsos positivos y aumentando la fiabilidad del sistema.

El *machine learning* es otra herramienta más. Es importante saber cuándo y cómo utilizar un algoritmo en particular. Hay algoritmos más simples y otros más complejos y tendremos que elegir en función de nuestras especificaciones.

Conclusión

El *machine learning* es un área de conocimiento en auge y continua expansión desde hace unos años. Grandes empresas tecnológicas están aplicándola en sus servicios y mejorándola continuamente, ya que dispone de una flexibilidad que otros métodos estáticos no pueden ofrecer.

Presenta un futuro prometedor en el área de la ciberseguridad, puesto que la capacidad de adelantarse al atacante es fundamental para que los sistemas protegidos acaben siendo comprometiendo. Pero no se trata de una solución para todo, sino de una herramienta más para el analista en su tarea por mantener los sistemas seguros.

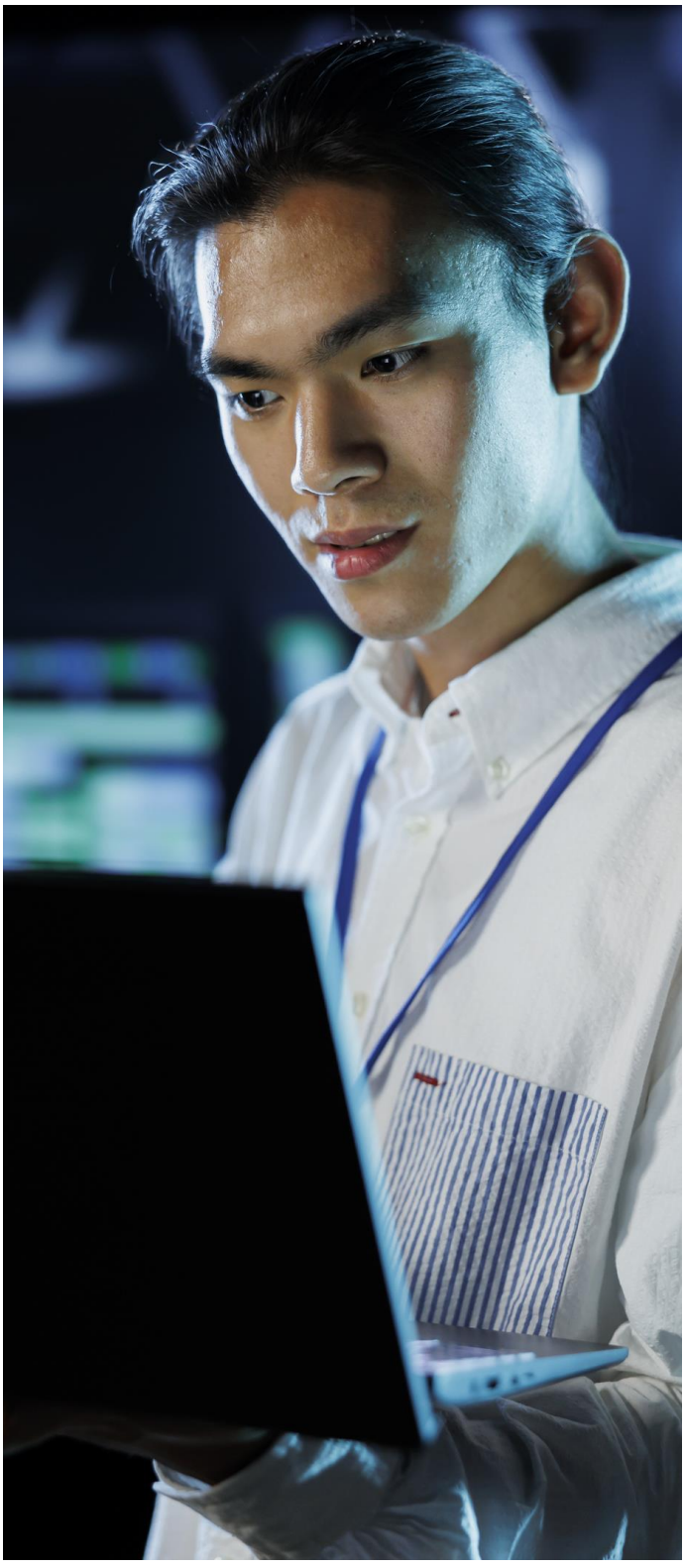
12 grandes hitos de nuestros 100 números

4. Cuando conectas con Internet, Internet se conecta contigo

Artículo Abril 2018

Tal vez el título suene evidente, pero este concepto entraña consecuencias a las que merece la pena prestar atención. Todo el mundo entiende el concepto de Internet y las oportunidades que ofrece la interconexión de sistemas a lo largo del planeta: un mundo a tu alcance. Sin embargo, no se presta tanta atención a que la conexión fluye en ambos sentidos, con lo que eso conlleva. En este artículo vamos a ver los diferentes problemas que puede acarrear estar conectados a la red.

Cuando conectamos algo a esta gran red para aportar ciertas funcionalidades o servicios de forma remota se ha de ser consciente de las implicaciones que eso tiene y qué cosas pueden ser visibles desde el exterior. Cuando un dispositivo accede a Internet a través del router que nos da acceso, se ve expuesto a todo lo que pasa en la red.



Los bots

No todo lo que se mueve por Internet es actividad de personas físicas, gran parte proviene de robots (bots). Si analizáramos todo lo que llega al router que nos da acceso a Internet, veríamos que hay mucha actividad de ellos. Cuando se abre para dar acceso a Internet a un dispositivo, a su vez estos bots también intentarán conectarse al dispositivo.

Entre los bots, hay algunos que son inocuos (por ejemplo los de buscadores como Google, que indexan Internet para que en nuestras búsquedas salgan las webs), y hay otros con propósitos más oscuros. Estos bots malintencionados buscan tener acceso al sistema para poder comprometerlo y tenerlo bajo su control.

Una vez que el sistema es comprometido, los atacantes que estén detrás de ese bot lo podrán usar para un sinfín de posibles acciones. Entre ellas se podrían encontrar, por ejemplo, la minería de criptomonedas, el uso como proxy inverso (para realizar ataques y evitar que pueda ser rastreado) o como parte de un ejército de ordenadores zombi (para ataques masivos de denegación de servicio).

Caso real

Un caso real causado por los bots fue el de la red de ordenadores zombi (o botnet) llamada Mirai. Para aquellos que no la conozcan, realizó uno de los mayores ataques masivos conocidos hasta la fecha, que dejó sin Internet (o afectó considerablemente) a gran parte de las principales páginas web.

En este sentido, se aprovechó de la carencia de seguridad en dispositivos del Internet de las cosas (IoT) para controlarlos.

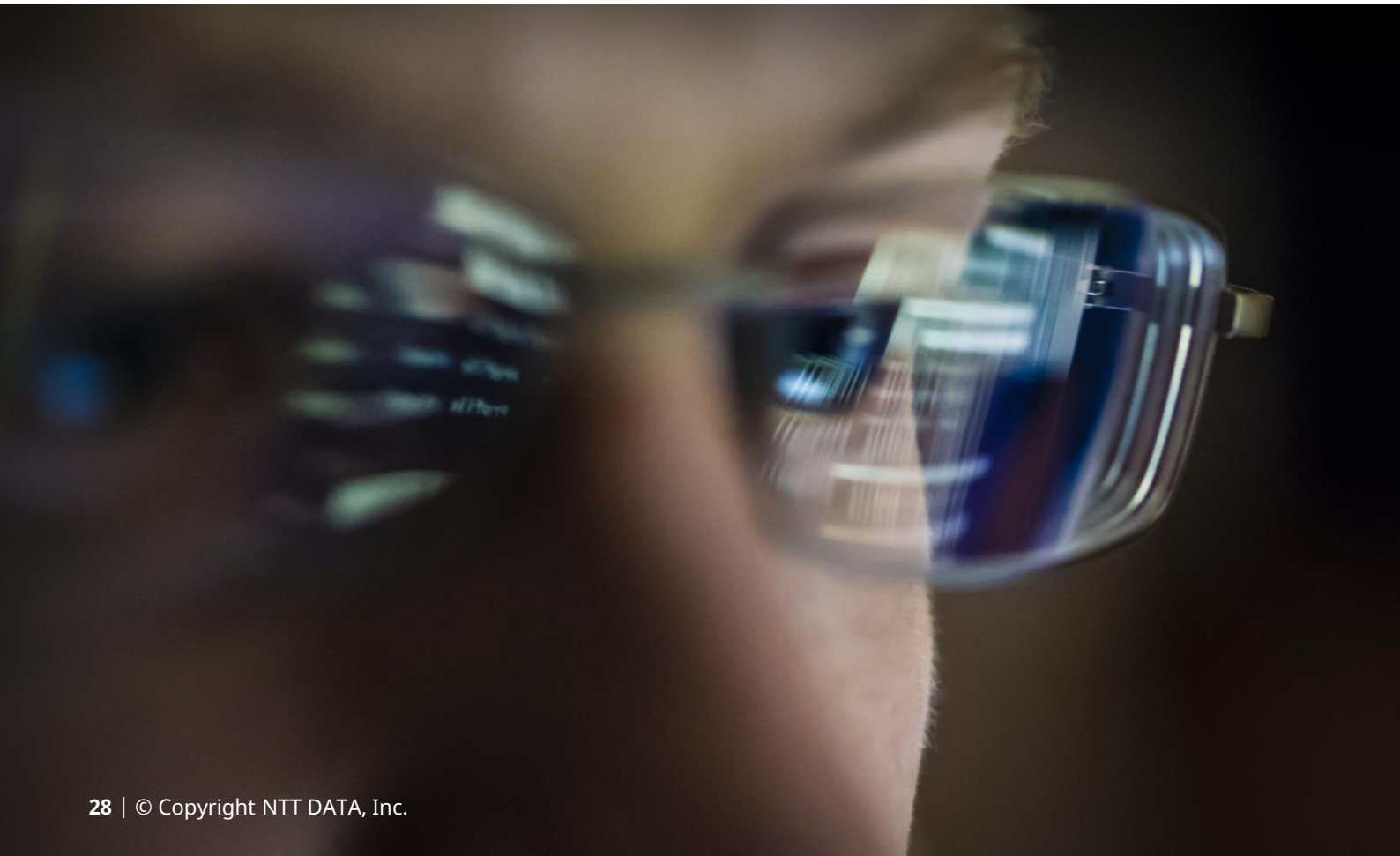
Cualquier cosa que se conecta a Internet, por sencilla que sea, se expone a este tipo de riesgos. Uno de los dispositivos más comprometidos son las cámaras IP. Hay tal volumen de cámaras desprotegidas que existen incluso webs que te permiten conectarte a ellas para ver lo que pasa, como, por ejemplo: www.insecam.org.

Entre los bots que no tienen malas intenciones se encuentran los que intentan localizar dispositivos vulnerables (como hacen los bots mencionados anteriormente), pero sin ese propósito de hacer actividades ilegítimas.

Por ejemplo, la web de cámaras citada solo identifica y se conecta a esas cámaras. No obstante, el objetivo de este tipo de webs es demostrar el problema que supone el no tomarse la seguridad en serio cuando un dispositivo es accesible desde Internet.

Otra página de este tipo es https://worldofvnc.net , que se basa en VNC, un sistema de acceso a ordenadores remotos parecido en funcionalidad al escritorio remoto de Windows. Esta web intenta entrar en dispositivos desprotegidos usando este sistema y realiza una captura de la pantalla a la que accede. Tiene el mismo objetivo que la página de cámaras anterior, sensibilizar sobre los riesgos de estar expuestos a Internet, pero centrándose en sistemas que usen VNC.

No son las únicas herramientas con ese objetivo. Existe otra llamada Shodan (www.shodan.io), y conocida como “el Google de los hackers”, que analiza las diferentes IPs comprobando qué puertos y servicios están abiertos y son accesibles desde Internet. Este motor de búsqueda nos permite saber qué estamos exponiendo en Internet para poder gestionar su seguridad de forma apropiada.



Al ver algunos de sus resultados es preocupante lo que se puede llegar a encontrar. Hay ordenadores, cámaras, sistemas de control industrial, frigoríficos, etc. La creciente tendencia de incorporar un acceso a Internet a cada vez más dispositivos ha hecho que crezcan los elementos vulnerables en ese motor de búsquedas. Parece que la seguridad en el Internet de las cosas no es una prioridad para los fabricantes, y muchas veces tampoco para sus propietarios.

Además, el famoso motor de búsqueda de Google puede ser usado con el fin de detectar elementos vulnerables, ya que como hemos indicado antes, indexa Internet para poder realizar búsquedas. Esta técnica se conoce como “Google hacking” y se aprovecha de ciertas búsquedas para poner de manifiesto la falta de protección en algún elemento expuesto a Internet.

Estos catálogos de búsquedas pueden modificarse para centrar más el resultado, pudiendo dirigirse contra organizaciones concretas. Si esas herramientas que hemos visto pueden encontrar vulnerabilidades en los dispositivos accesibles desde Internet, los bots malintencionados también. Por ello, si se detectase una situación como las anteriores, se deberían aplicar las medidas correspondientes para evitar que los sistemas sean comprometidos (si no lo han sido ya).

Vulnerabilidades

En el caso de que nuestros dispositivos vulnerables estén en la Unión Europea, o tengan datos de ciudadanos europeos, el resultado puede ser mucho más grave. Ya no sólo implicará el problema de que se comprometa uno de nuestros activos, sino que la multa correspondiente por no cumplir el nuevo reglamento de protección de datos (GDPR) podría suponer un impacto aún mayor.

Al margen del Internet de las cosas, otro tipo de dispositivos que los bots suelen encontrar como vulnerables con frecuencia son componentes y máquinas en la nube, a los que se recurre para poder dar servicios desde Internet sin necesitar infraestructura propia, sobre todo para pequeños componentes. Sin embargo, muchos propietarios o usuarios de estos servicios de computación en la nube no se preocupan por la seguridad de sus máquinas ni de qué datos están expuestos a Internet. En este caso, los proveedores de estos servicios aportan algo de protección para ayudar a que las máquinas no sean controladas por agentes no autorizados. Sin embargo, parte depende del usuario del servicio, por lo que solo las medidas del proveedor no son suficientes.

En este tipo de elementos suele ser más frecuente que haya escapes de información que esté colgada en esos componentes. Ha habido varios casos que han salido en las noticias, como el caso de fuga de información clasificada del Ejército de Estados Unidos, en noviembre de 2017, a través de un servidor en la nube de Amazon que no estaba configurado correctamente. Esto demuestra que los elementos o dispositivos colocados en la nube han de ser protegidos para evitar que esos bots puedan comprometer u obtener información sensible.

Conclusión

Cualquier elemento que sea accesible a través de Internet afronta un conjunto de riesgos que no han de ser subestimados. Lo importante es ser consciente de que, si conectamos algo a Internet, Internet se conecta con ese algo, y con ello, todos los bots que lo patrullan. Da igual si es algo temporal o algún elemento que pensemos que no es importante, el simple hecho de estar conectado a Internet es suficiente para tener la seguridad en mente. Se debe revisar todo aquello que es accesible desde la red para poder estar tranquilos y saber que lo que se conecta con nosotros no traerá sorpresas desagradables.

12 grandes hitos de nuestros 100 números

5. La ciberseguridad en las elecciones: ¿qué puede pasar realmente?

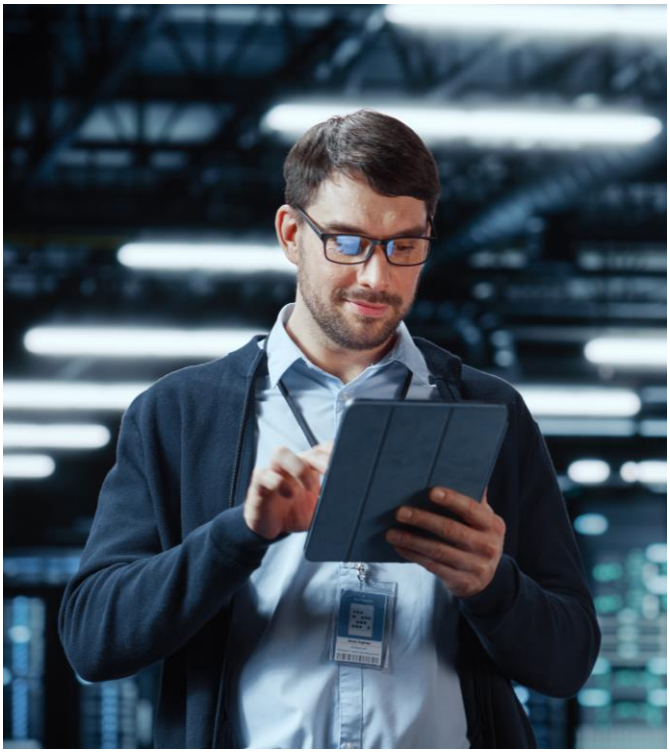
Artículo Mayo 2019

Para contestar a esta pregunta tenemos que plantearnos varias cuestiones: a qué se puede atacar cibernéticamente y con qué objetivos, cómo y quién puede hacerlo. Por último, lo más importante que debemos preguntarnos es cómo nos podemos proteger. En este artículo vamos a ir respondiendo a estas cuestiones.

Hay dos razones que han provocado una gran incertidumbre sobre la ciberseguridad en las próximas elecciones de abril de 2019 en España:

- Existe una creciente preocupación en la sociedad sobre la ciberseguridad en el uso cotidiano de las tecnologías de la información. Por ejemplo, a mi hijo de 12 años le inquieta que haya hackers en el juego del Fortnite que le puedan hacer perder partidas, e incluso mi padre, de 75 años, está preocupado por si le roban dinero al mirar su extracto bancario desde la tablet.
- El debate abierto de una posible injerencia rusa en las elecciones de EE.UU. de 2016, así como las vulnerabilidades descubiertas en el software de votación durante las mismas.

Pero ¿qué podría ocurrir si hubiera un ataque cibernético en las próximas elecciones generales españolas?



¿A qué se puede atacar cibernéticamente y con qué objetivos?

Hay tres elementos principales que son susceptibles de ser atacados:

1. Ante un interés por influir en el proceso electoral, los partidos políticos son objetivos fundamentales. Hay varios casos conocidos que han tenido lugar durante campañas recientes. Por ejemplo, durante las elecciones de EE.UU. ocurrió el hackeo a los correos de Hillary Clinton y ante los comicios franceses se filtraron los correos de Emmanuel Macron. El objetivo principal es claro: desacreditar a los políticos.
2. Los ciudadanos son otro elemento crítico en los procesos electorales. En este caso lo que se pretende es influirles en el momento del voto. Las democracias occidentales no son ajenas a influencias que buscan desequilibrarlas, fundamentalmente a través de las campañas de propaganda y de fake news.
3. Por último, las instituciones gubernamentales son otro objetivo clave en los procesos electorales. En este caso el objetivo es debilitar el sistema democrático para obtener beneficios geopolíticos, económicos e ideológicos. y se suele atacar los sistemas informáticos que soportan los procesos electrónicos, tanto para el voto como para el recuento posterior.

¿Cómo se puede atacar?

Las formas de ataque son múltiples y una de las mayores complejidades a las que nos enfrentamos en estos casos es que son ataques dirigidos y concretos, no se trata de ataques generales.

En primer lugar, me gustaría introducir el concepto de ataque híbrido que, en el ámbito al que nos estamos refiriendo, consiste en combinar medios convencionales como la presión de los medios de comunicación y no convencionales, como las fake news. Estos últimos están asociados generalmente a las redes sociales y nuevas tecnologías.

Las fake news son una de las principales preocupaciones, ya que abordan directamente a los ciudadanos. Conseguir que los medios de comunicación o las redes sociales sean fuentes de desinformación y altavoces de noticias falsas es un ataque claro. En este sentido, colocar fake news en un medio ampliamente conocido y de confianza tiene mucho más impacto que usar una plataforma que nadie conoce, aunque sea solamente de forma temporal.

Otro tipo de ataque consiste en infectar los sistemas de voto electrónico. Aunque en los últimos meses han aparecido numerosas noticias sobre vulnerabilidades en este tipo de software, este tipo de infecciones no aplican todavía en España, pues el voto electrónico no está implantando. No obstante, cabe destacar a modo anecdótico el caso de un niño de 11 años que fue capaz de hackear una réplica del sistema de voto de EE.UU. y que fue presentado durante la última edición DEFCON, o que varios investigadores encontrasen fallos de seguridad en el software electoral suizo antes de su uso en las elecciones de este país.

Por otro lado, sí es posible hackear los sistemas de recuento electoral en España, aunque debido al modelo electoral de este país no se conseguiría mucho más que generar confusión, pues los datos telemáticos siempre se cruzan con los manuales. Se pueden llevar a cabo ataques contra los sistemas informáticos centrales, las comunicaciones o incluso los dispositivos de recuento en los colegios electorales, pero estos no dejarían de ser “males menores”.

Por último, es importante destacar los posibles ataques a los sistemas de información de los partidos electorales y a sus webs. En estos casos, el objetivo principal sería filtrar información confidencial y utilizarla en el formato “ataque híbrido” antes explicado.

Todo esto pone de relieve que no se debe vigilar y probar únicamente el software que se use para el recuento de votos, sino que hay un gran número de factores y participantes vulnerables cuando se trata de afectar al resultado electoral. En ese sentido, aquellas empresas y organizaciones que puedan estar cerca del panorama político o de la comunicación pública deberían hacer ejercicios para intentar minimizar el riesgo de ser partícipes en campañas de injerencia en los procesos electorales.

Los políticos y los partidos deberían prestar especial atención a la ciberseguridad siempre, pero sobre todo antes de unas elecciones, ya que es el momento de más riesgo de que se intente filtrar información. Nada hace más daño a la imagen de un candidato que sacar sus “trapos sucios” en plena campaña electoral.

¿Quién puede atacar?

Principalmente existen tres tipos de atacantes diferentes:

1. Los hacktivistas pueden aprovechar este momento crítico de eleccciones para intentar llevar a cabo acciones que perjudiquen a los que han gobernado y así evitar que sean reelegidos o, simplemente, para darse a conocer.
2. Los partidos políticos y grupos económicos que busquen “arrimar la ascua a su sardina”, como puede haber ocurrido ya en otros procesos electorales en varios países.
3. Los expertos con gran cantidad de recursos para poder llevar a cabo ataques centrados y muy dirigidos a sus víctimas.

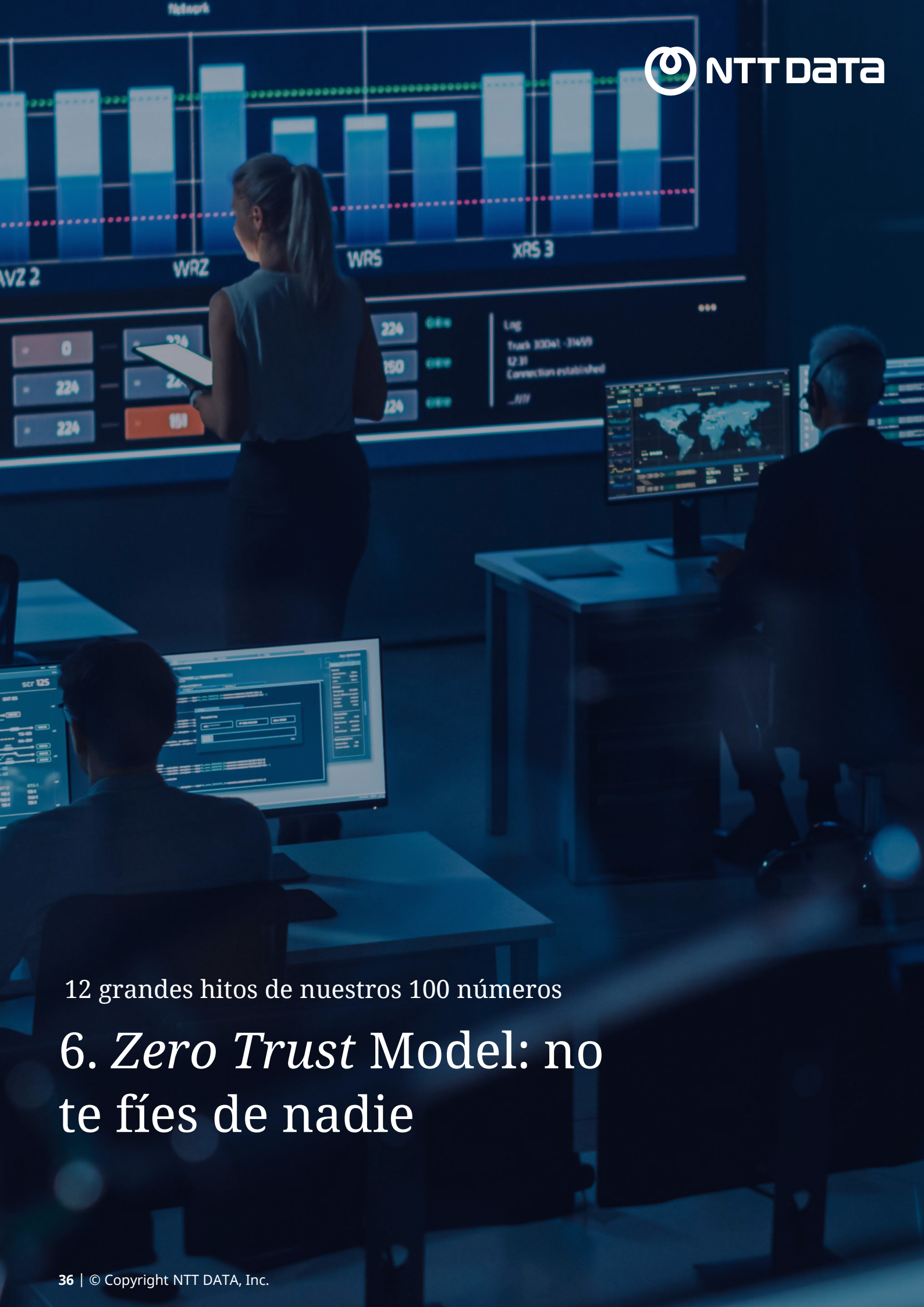
Este último grupo tiene el perfil más probable y más peligroso, pues su conocimiento sobre la tecnología hace que la más mínima deficiencia en los sistemas genere la mayor de las catástrofes.

¿Cómo podemos protegernos?

En primer lugar, es importante señalar que, por mucho que protejas tu casa para que no te roben, siempre es posible que termine ocurriendo. Eso sí, es menos probable que pase si tienes alarmas, rejas y vigilantes privados, que si dejas la puerta abierta.

1. Muchos países están en proceso de mejorar sus barreras de protección y van mejorando poco a poco. Por ejemplo, cabe destacar el caso de ENISA que, en su esfuerzo por proteger las elecciones europeas, organizó junto al Parlamento Europeo, la Comisión Europea y los Estados miembros un ejercicio conjunto para probar su respuesta y plan de contingencia ante potenciales incidentes que puedan afectar a las elecciones europeas. Además, en España se ha creado el Dispositivo Especial de Seguridad (DEC) que cuenta con numerosos organismos gubernamentales involucrados, como el Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC), la Policía Nacional y la Guardia Civil, entre muchos otros, para reforzar la seguridad durante el periodo electoral.
2. Los responsables de las campañas electorales deberían evitar fugas de información, fundamentalmente a través de la implantación de medidas de seguridad básicas y a través de la monitorización de redes sociales e Internet.
3. Los proveedores TIC como Telefónica, Google, Facebook, etc. podrían contribuir eliminando contenidos ilícitos o falsos de forma rápida y evitando, en la medida de lo posible, la creación de perfiles falsos, conocidos como trols.
4. Los medios de comunicación deberían ponderar adecuadamente si es mejor dar una primicia o asegurarse de que la información es veraz. En este sentido es importante destacar que los modelos de financiación a través de publicidad no favorecen este proceso, pues es más lucrativo dar una noticia que atraiga muchas visitas que verificar la fiabilidad de la misma.
5. Los fabricantes de aplicaciones también tendrían que involucrarse y, de hecho, algunos ya lo están haciendo. Por ejemplo, WhatsApp ya no permite difundir noticias a todos tus contactos de forma masiva.
6. Por último, los ciudadanos también deberíamos aportar nuestro granito de arena utilizando el sentido común e implementando medidas de seguridad básicas, por ejemplo, no reenviando lo primero que nos llega o evitando que se instale software malicioso en nuestros dispositivos que luego pueda servir para atacar a otros ciudadanos.

La ciberseguridad es el mejor cimiento para sostener la democracia, especialmente cuando tanto esta como la sociedad se están transformando digitalmente. Si no podemos confiar en la tecnología para los aspectos más críticos, esta dejará de utilizarse, y por tanto no podremos beneficiarnos de sus ventajas.



12 grandes hitos de nuestros 100 números

6. *Zero Trust* Model: no te fíes de nadie

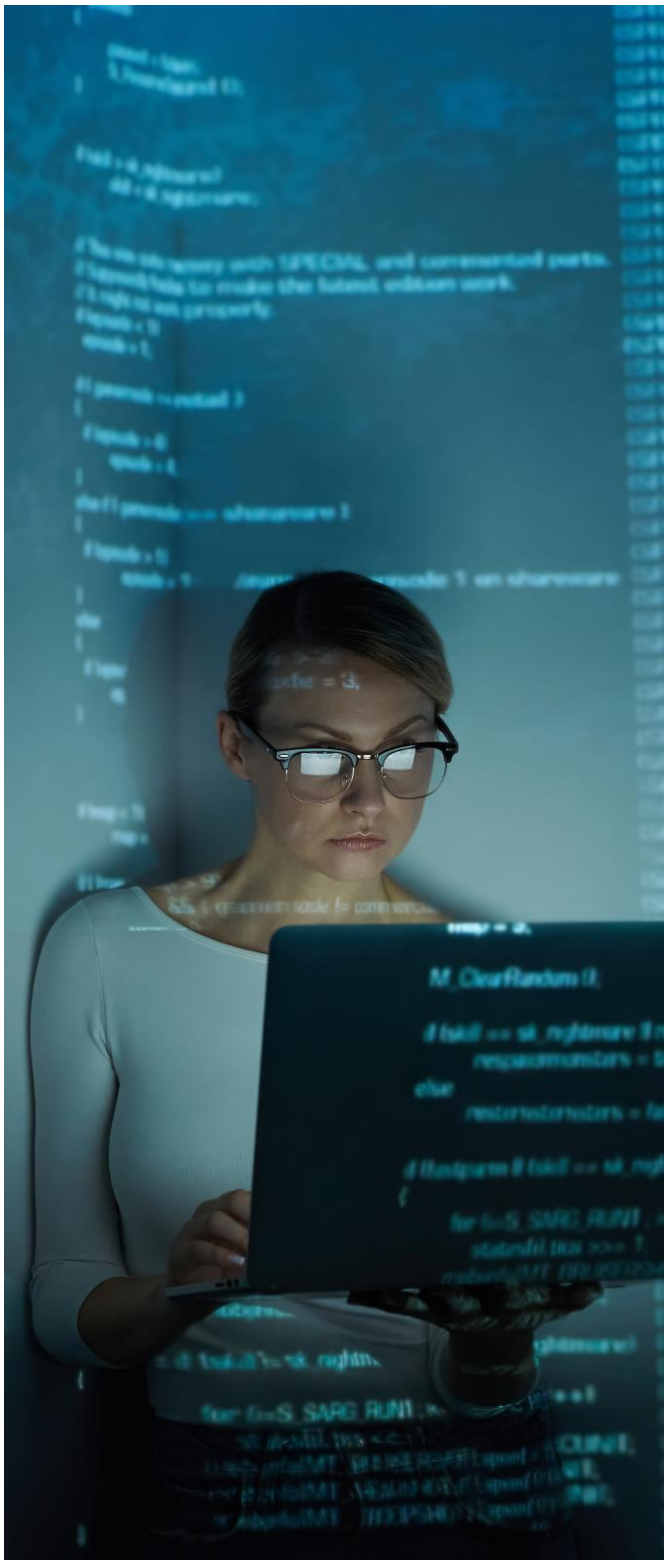
Artículo Octubre 2019

Uno de los eventos de seguridad más destacados en los últimos meses ha sido el caso del banco Capital One, que sufrió una brecha de seguridad exponiendo información de 106 millones de usuarios. El CEO de Akamai comentó en una noticia publicada a finales de Julio que este suceso resaltaba la necesidad del Zero Trust Model, pero, ¿qué es Zero Trust? Este artículo se va a centrar en dar respuesta a esta pregunta.

Este concepto es una nueva forma de entender las redes de las organizaciones que rechaza la idea de “castillo y foso”, en el que todo lo que está fuera de mi red no es de confianza y lo que queda dentro sí lo es. Hoy en día, el perímetro físico de las organizaciones no es el único perímetro digital de la empresa, los usuarios y dispositivos (equipos gestionados) de una organización pueden encontrarse fuera de la red empresarial, y de la misma manera, usuarios o dispositivos ajenos pueden estar dentro de la red. Por ello, no se puede asumir que todo aquello que está dentro de la red es fiable. Las amenazas de seguridad pueden surgir internamente, a través de una infección de malware, por ejemplo, y poner en peligro a toda la organización.

Así pues, este modelo se basa en “nunca confiar y siempre verificar”. Este sistema evita que las amenazas se muevan lateralmente a través de una red, es decir, que los atacantes se abran paso a través de una red para conseguir llegar a los activos y datos. Esto se logra mediante estrategias de mínimo privilegio con un control de accesos exhaustivo, micro segmentación de las redes y monitorización constante del estado de las mismas.

John Kindervag presentó el modelo Zero Trust en el año 2010, exponiendo las micro redes, dedicadas exclusivamente a la monitorización. Se trata de una nueva figura de elemento red (Network Segmentation Gateways) que incluía la seguridad de forma natural al modelo con funciones de criptografía, monitorización, filtrado de contenido, firewall, detección de intrusiones y control de acceso.



Todo esto, gestionado de forma centralizada para controlar la infraestructura.

El modelo teórico de Kindervag sentó las bases de esta forma de concebir la red, ganando peso con la iniciativa BeyondCorp (https://www.beyondcorp.com) impulsada por Google tras sufrir un ataque llamado Operación Aurora. Tras el ataque, Google realizó una investigación para implementar el modelo Zero Trust en sus redes.

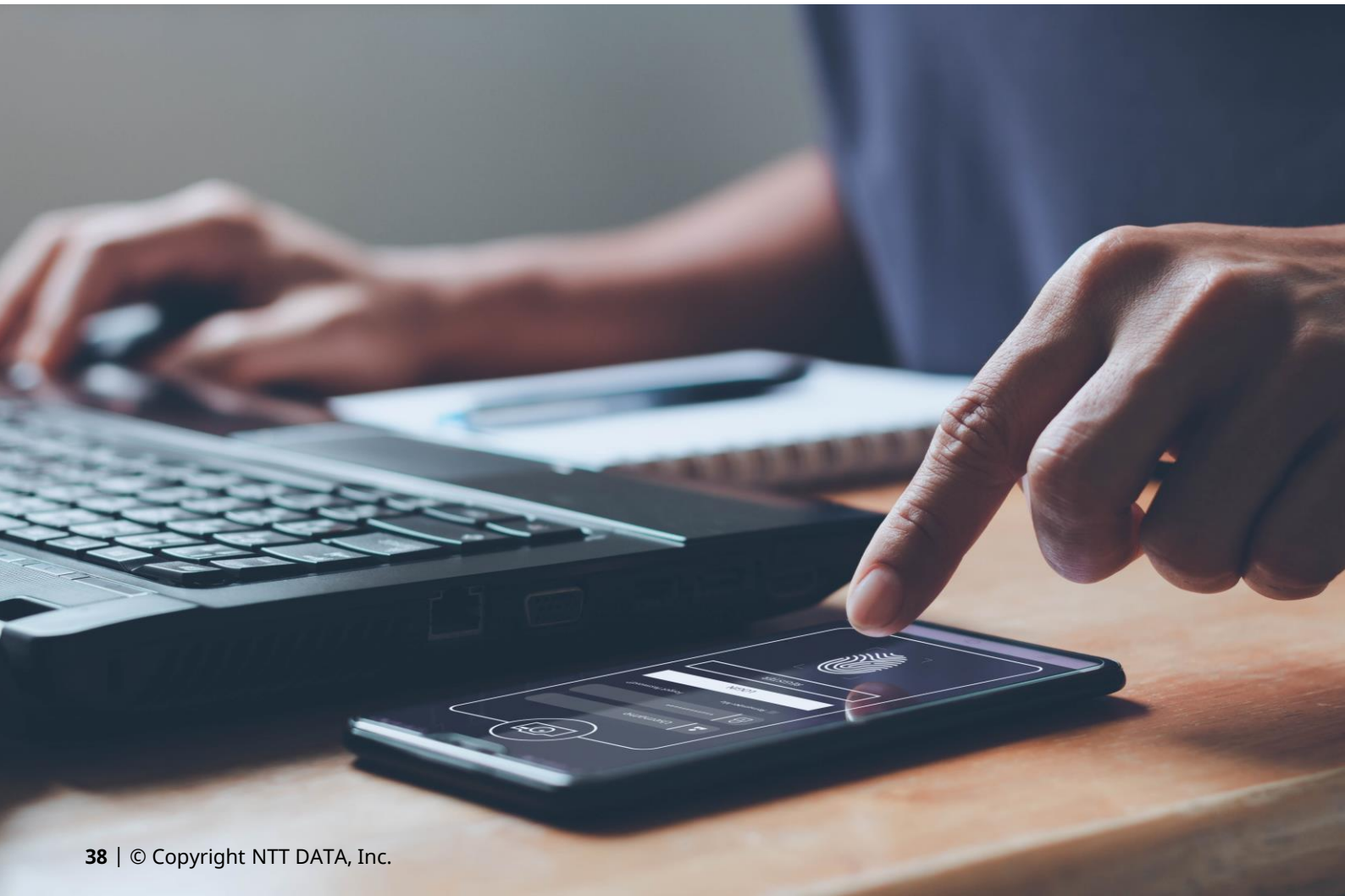
En su página web están publicados los resultados de la iniciativa. Algunas ideas interesantes que mencionan son:

- Llevar un inventario actualizado con todos los dispositivos corporativos donde la identidad se confirme con un certificado generado por cada uno de ellos y que se renueve periódicamente. Mantener además un control de todos los cambios que se han llevado a cabo en los dispositivos corporativos gestionados.

- Todo acceso debe pasar por un motor de control de accesos, independientemente de su posición en la red donde aplica las políticas correspondientes de acceso.

- Usar un motor de inferencia y de confianza que sirva para controlar el grado de confianza de un usuario y dispositivo a lo largo del tiempo en función de su comportamiento. Esta información sirve para asignar o modificar los permisos a lo largo del tiempo.

Llegados a este punto, encontramos un conjunto de ideas interesantes que nos pueden ayudar a incrementar la seguridad en nuestras redes.



Si queremos llevarlas a cabo en nuestras organizaciones, no hay una estrategia única a seguir, ya que depende de las características particulares de cada organización, así como del grado de no confianza al que se quiera llegar.

Queda claro que independientemente de la estrategia elegida, la idea base que se ha de contemplar es la fuerte segmentación de la red, donde siempre habrá un control de accesos en cada segmento, así como la monitorización continua, inventariado y estado de todos los dispositivos de la red. También sería deseable que se requiriera una autenticación del dispositivo y en función de ello, se modificaran los permisos de acceso. Tener claro y controlados los flujos de información que tienen lugar en la red, así como las conectividades necesarias entre los diferentes elementos y conocer su comportamiento temporal (a qué horas debería tener actividad y a qué horas no).

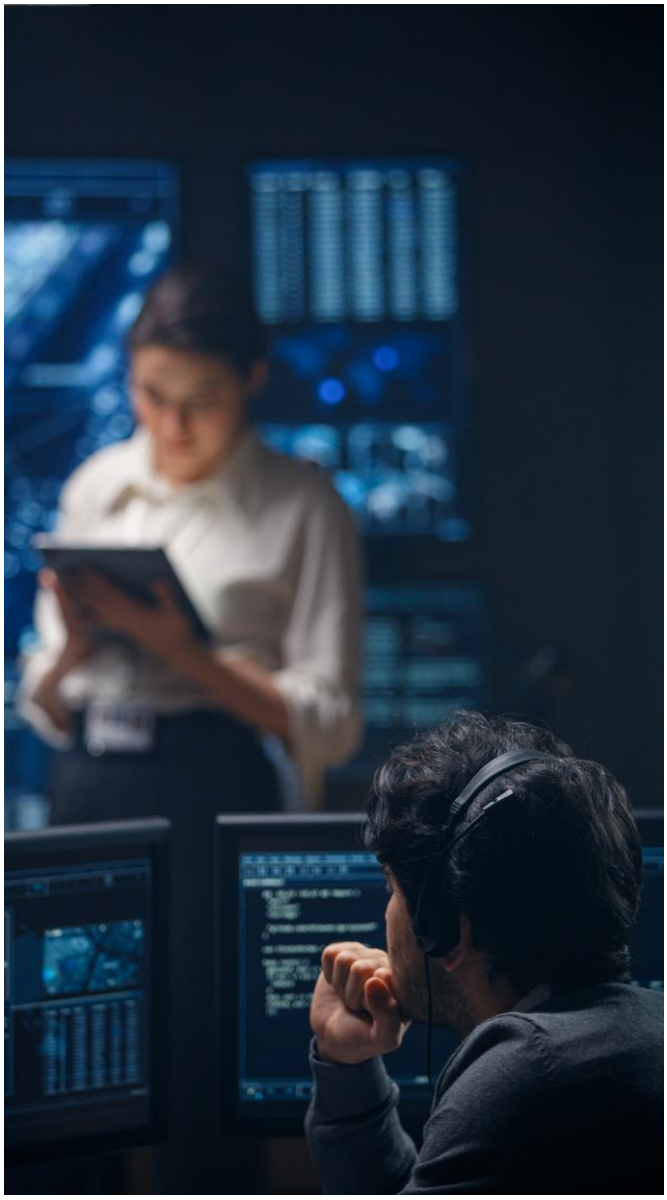
Adicionalmente, se debería implementar una red dedicada a la monitorización que permita vigilar cada segmento de red, y forzar a que las labores de administración de la misma sólo puedan llevarse a cabo en ciertos sitios físicos (autorización basada en localización).

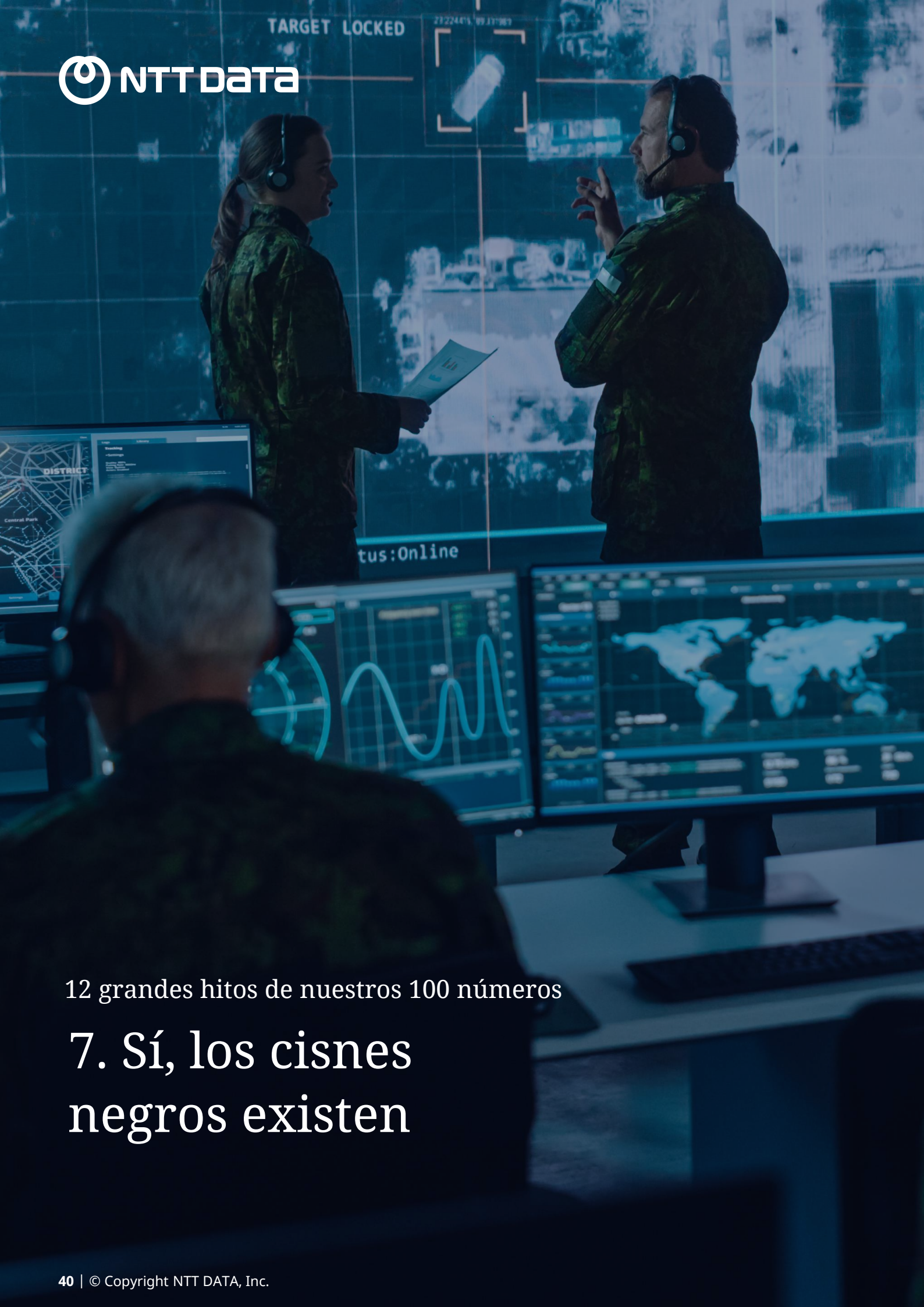
Para limitar los servicios disponibles en función del dispositivo en uso se requerirá el empleo de doble factor a los usuarios, y diferenciar entre dispositivos ya que no debería tener el mismo nivel de confianza un dispositivo que está bajo completo control de la organización, que uno externo, independientemente del usuario que lo utilice.

Una de las medidas más interesantes a añadir sería que los mecanismos de control de accesos pudieran usar información del comportamiento (la evolución temporal de la confianza), como el ejemplo de Google.

Como hemos podido apreciar, este modelo busca asegurarse de que se opera con el mínimo privilegio, evitando así el acceso salvo permiso expreso y comprobando lo que sucede en la red. El control resulta también uno de los pilares clave, como ya hemos comentado, hay que tener actualizado el inventario de dispositivos y su estado, así como el comportamiento esperado de los mismos.

Por último, es importante destacar que este modelo puede implantarse de forma completa o parcial, en una parte de la red o en su totalidad, dependiendo del apetito por el riesgo de la organización. Indistintamente de la decisión que se tome respecto al uso de este modelo, Zero Trust Model debe tenerse en cuenta en el mundo digital, donde el peligro no solo se encuentra fuera de la red.





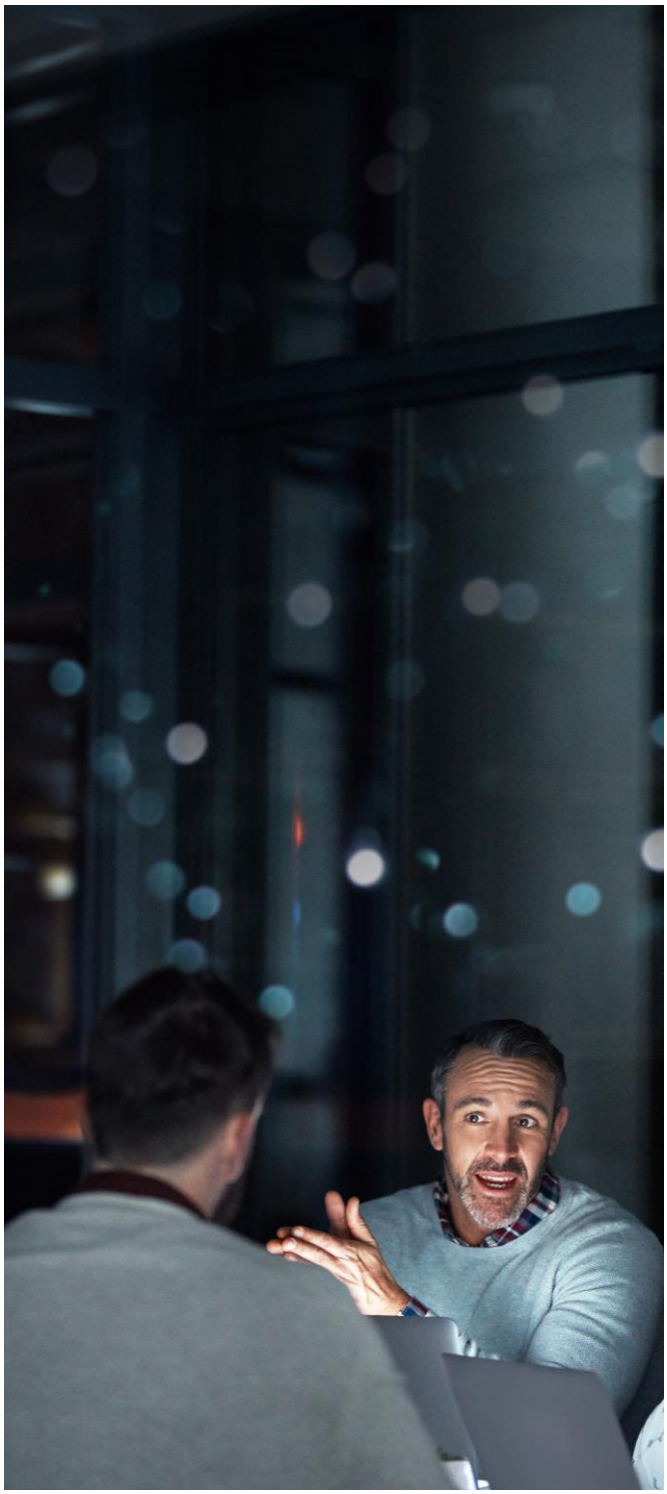
12 grandes hitos de nuestros 100 números

7. Sí, los cisnes negros existen

Artículo Abril 2020

En las últimas décadas hemos vivido hechos insólitos que jamás hubiéramos pensado que pudieran tener un impacto tan grande en la economía y en la sociedad. Estos acontecimientos se contemplan con una probabilidad muy baja de ocurrencia pero, cuando suceden, su impacto es enorme. A estos hechos se les denomina cisnes negros. Por ejemplo, todos recordamos aquel 11 de septiembre. Nadie pensó que dos aviones podrían estrellarse contra las Torres Gemelas. Ahora, una pandemia pone en jaque a la economía mundial y una de las múltiples preguntas que nos surgen estos días es si estamos tecnológicamente preparados para afrontarlo. En este artículo desarrollaremos las medidas que tenemos que tener en cuenta para poder realizar nuestra actividad de manera segura desde casa.

El mundo vive una nueva situación en el que nuestra manera de trabajar, de realizar nuestra vida cotidiana, se ha visto drásticamente modificada. Las empresas se han visto obligadas a impulsar el teletrabajo de forma masiva y a adaptarse a operar en remoto. Ante esta nueva situación, los trabajadores hemos tenido que cambiar nuestras rutinas y hábitos laborales, pero no por ello debemos bajar la guardia. Los ciberdelincuentes se aprovechan de cualquier resquicio para tener una oportunidad de atacar.



Las empresas

Las empresas que no se han visto en la obligación de cerrar y siguen con su actividad han tenido que activar sus planes de continuidad de negocio para poder, en la medida de lo posible, seguir ofreciendo unos servicios, al menos los mínimos. Otras han tenido que implantar en un tiempo reducido soluciones de teletrabajo para ofrecer esta posibilidad a sus empleados.

Estos planes se basan en una primera fase en un Análisis de Impacto para el Negocio, BIA por sus siglas en inglés (Business Impact Analysis). En estos análisis se establecen los servicios críticos de cada organización, así como el personal, material necesario y el impacto que puede causar una interrupción del servicio tanto en activos tangibles (personas), como intangibles (la reputación). En base a los resultados que arroje este análisis se definirán unas estrategias a seguir para los escenarios de disrupción que se planteen.

Tras lo sucedido en las últimas semanas y tras la declaración del Estado de Alarma por el Gobierno, en muchos planes de continuidad se habrán visto que los datos que contienen cada BIA no son del todo correctos y adecuados. Por ello, cuando esta situación termine, tendrán que realizar una revisión completa y una actualización, siendo realistas. Esto supondrá un ejercicio de lecciones aprendidas para poder establecer pautas y acciones para futuras ocasiones.

Uno de los hechos que hará cambiar la mentalidad al enfrentarse a estos análisis será que uno de los escenarios que se contempla para este tipo de casos de pandemia es la indisponibilidad del personal. Por ello, se deberá reforzar para que los impactos directos, como es la falta de personal que se haya infectado, y los indirectos, como no poder salir de casa o tener la posibilidad de ofrecer teletrabajo masivo tanto al personal crítico como al no crítico, sean mitigados.

Los empleados

Ante la pandemia actual se ha establecido el teletrabajo como medida para para evitar contagios y continuar con el funcionamiento de las empresas en la medida de lo posible.

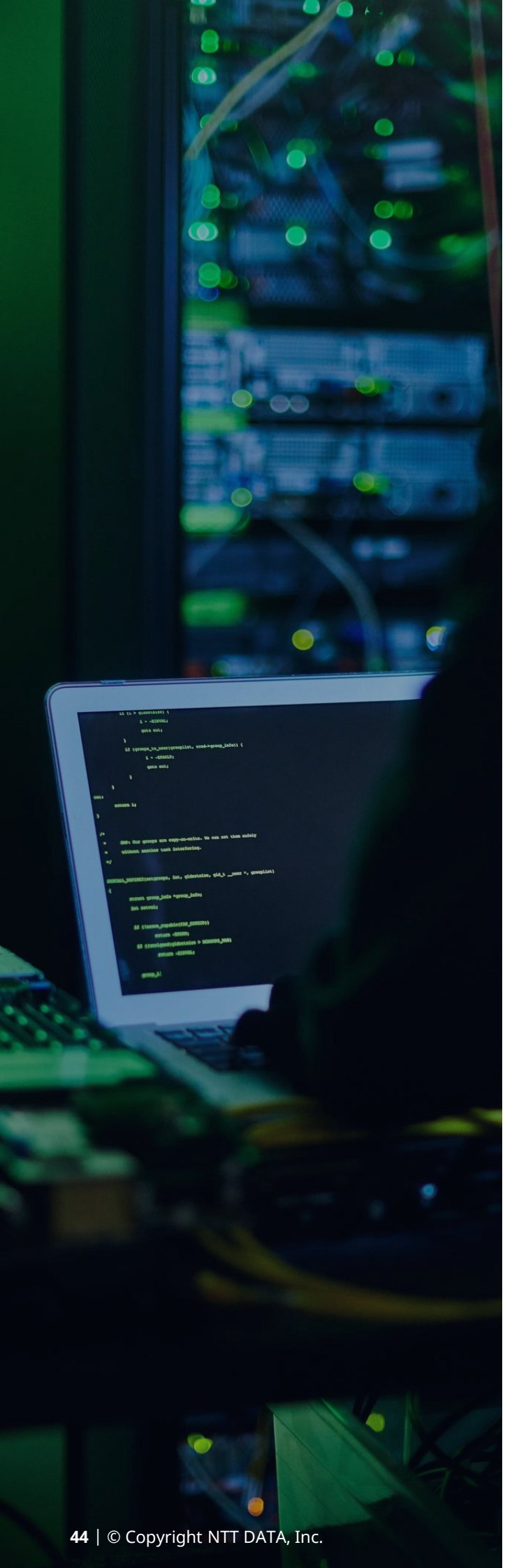
Los trabajadores que no pertenecen a los sectores/ servicios a los que se les permite acudir a su puesto habitual de trabajo, tienen la responsabilidad de quedarse en casa teletrabajando para contribuir a frenar la curva de contagios.

Esta obligación de realizar la actividad laboral desde casa está siendo aprovechada por los ciberdelincuentes. Ahora más que nunca debemos mantenernos alerta ante cualquier indicio de actividad maliciosa. Por ello queremos compartir algunas recomendaciones a seguir durante la jornada laboral de teletrabajo:

Utiliza solamente equipos corporativos. Estos equipos tienen un mantenimiento de seguridad que garantiza la adecuada seguridad de los sistemas.

- Conéctate a la Wi-Fi de tu casa, pero antes cambia la contraseña de tu red por una robusta con una longitud de más de ocho caracteres con mayúsculas, minúsculas, números y caracteres especiales. Las contraseñas por defecto de los routers pueden haberse filtrado.
- Realiza una revisión de actualización de parches y antivirus de tu equipo.
- Presta atención a los emails que recibes y no abras ningún archivo adjunto sobre el Covid-19.
- No accedas a páginas webs desconocidas o que no sean seguras. Recuerda comprobar el protocolo que establece la comunicación y que sea HTTP Secure.
- A la hora de comunicarte con tus compañeros de trabajo utiliza siempre las aplicaciones corporativas que te han proporcionado.
- No instales ningún software que no esté permitido por tu organización ni utilices herramientas de descarga peer-to-peer en el equipo corporativo. Estas acciones pueden poner comprometer la seguridad y la privacidad de tu equipo.
- Una vez acabes la jornada laboral, apaga el equipo y no lo utilices para realizar actividades lúdicas en casa o visualizar contenidos.

Adicionalmente el Centro Criptológico Nacional ha puesto a disposición de los usuarios una guía de recomendaciones para el teletrabajo en el que se tienen en cuenta una serie de pautas que permiten garantizar la seguridad de las herramientas y soluciones utilizadas. Puedes descargarla aquí.



Los ciberdelincuentes

Durante esta crisis sanitaria, la Policía Nacional ha advertido del descubrimiento de ciberataques dirigidos contra los sistemas sanitarios para romper por completo el sistema informático de los hospitales.

El método que se ha descubierto es un ataque de tipo ransomware denominado NetWalker. El modus operandi de este ataque es el envío de correos electrónicos con una temática clara, información sobre el Covid-19, siendo los trabajadores sanitarios y hospitalarios su principal target. Como hemos comentado en anteriores artículos, este tipo de ataques secuestra los sistemas de sus víctimas y pide un rescate para recuperarlos, normalmente en Bitcoins. La Policía Nacional ha alertado a toda la población de estos correos masivos para que mantengan la precaución ante esta amenaza, que aprovecha la enorme cantidad de información que circula estos días en Internet para colarse en nuestros sistemas.

Además de la distribución del ransomware, estos días también es habitual la publicación masiva de fake news. Se han registrado más de 200 bulos y falsas noticias que únicamente pretenden infundir miedo y pánico. Por ello os recomendamos que siempre contrastéis toda información con los medios oficiales y no difundáis bulos. Además, ante esta situación la Guardia Civil ha abierto un canal de comunicación ciudadana para recibir información sobre fraudes y estafas online para poder colaborar y denunciar.

Conclusiones

Vivimos una situación difícil al tener que estar recluidos en nuestras casas, pero no por ello debemos bajar la guardia en materia de ciberseguridad. Los trabajadores debemos acostumbrarnos a esta situación y realizar las mismas acciones que haríamos estando en oficinas o en clientes. A su vez, las empresas deben proteger a sus empleados y tener también contemplados ciertos escenarios que a veces, tal vez por parecer inverosímiles, ocupan un papel secundario en los análisis de riesgos. Porque los cisnes negros existen, aunque entre todos podemos superarlos.

12 grandes hitos de nuestros 100 números

8. La digitalización del sector utilities y la ciberseguridad

Artículo Noviembre 2020

Nos encontramos en plena era de la digitalización, una carrera frenética para no quedarse atrás. No obstante, como hemos podido comprobar, cuanto más rápido se avanza, también dejamos errores que nos pasan factura en el largo plazo. En este artículo vamos a visualizar cómo el sector utilities ha conseguido avanzar en la carrera digital pero también ha sido víctima de los problemas que puede conllevar no tener en cuenta la ciberseguridad en sus procesos.

Partamos de la base que la digitalización está aportando a las empresas y al conjunto del sector de utilities una gran mejora de sus servicios, ya que se modernizan las infraestructuras, mejorando eficiencia y fiabilidad, algo que de un modo u otro repercute de manera satisfactoria y positiva en el consumidor. Sin embargo, no dejamos de observar un aumento de ciberataques en un sector que, no olvidemos, forma parte de nuestra red de infraestructuras críticas (energía, agua, gas, etc.) y como se puede observar en los numerosos estudios que se realizan por organizaciones como el CCI (Centro Nacional de Ciberseguridad Industrial) aquí en España, o la propia ENISA (European Union Agency for Cybersecurity), la ciberseguridad es un aspecto que no se está teniendo en cuenta, cuando en realidad debería ser priorizada y actualizada de una manera continua.

La necesidad de obtener, analizar, tratar y almacenar el dato es un peaje a pagar que las empresas actualmente ven como ineludible para no perder el tren del futuro de la tecnología a corto y medio plazo. No perdamos de vista que la gran mayoría de empresas del sector utilities poseen un negocio cuyo alcance no se limita sólo a infraestructuras IT, sino que lo hace en gran medida al sector industrial (OT).

Esta combinación de infraestructuras IT y OT, y la convergencia entre ambas hace que este tipo de compañías deban afrontar estrategias de ciberseguridad integrales que cubran las necesidades de dos mundos tan diferentes y que sirvan de escudo contra posibles ataques que afecten a su servicio.

No tenemos más que imaginar si durante un largo periodo de tiempo no hubiera luz, agua, o gas. No sólo se vería afectado el propio consumidor, sino las interdependencias o efectos cascada que ello acarrearía a otros sectores como, por ejemplo, el transporte o el sector nuclear o incluso a otros países que consuman esos recursos.

Si conocemos los peligros y de los daños que puede causar un ciberataque, ¿por qué no tenemos en cuenta la ciberseguridad?

¿Estamos preparados para la siguiente década?

La irrupción de nuevas tecnologías (Cloud, Big Data, etc.), la hiperconectividad y la psicosis por la captación de datos para su procesamiento y mejora de la eficiencia en los procesos, ha convertido a todas las infraestructuras de sistemas en un objetivo vulnerable ante posibles ataques. Como se apuntaba anteriormente, las empresas del sector utilities están expuestas a los riesgos tanto del mundo IT como del mundo OT.

Se ha hablado largo y tendido de cómo afrontar la ciberseguridad en el ámbito IT, pero especialmente significativo, tanto por su importancia como por sus consecuencias, es el caso de los Sistemas de Control Industrial (SCI), núcleo de cualquier proceso automatizado del ámbito OT (plantas de generación, subestaciones, infraestructura de abastecimiento y saneamiento de aguas, etc.).

Si bien los sistemas actuales son diseñados, implantados y operados teniendo en cuenta la ciberseguridad como requisito inicial (o al menos deberían), el mayor desafío que se nos plantea en el mundo industrial es el que suscitan los sistemas heredados, cuyas medidas de seguridad no se pensaron para afrontar las ciberamenazas actuales. Uno, sino el que más, de los principales problemas que proponen estos sistemas de operación (OT), radica en los ciclos de vida del mismo.

A diferencia de los sistemas IT, los sistemas OT poseen un ciclo de vida que no es extraño supere los 25 años. Esto es debido a que son sistemas pensados para perdurar en el tiempo, debido a su complejidad y a la necesidad de ofrecer la máxima disponibilidad del proceso a controlar. Por lo tanto, se plantea la necesidad de “securizar” sistemas ya operativos y “añadir” seguridad a sistemas que fueron diseñados e instalados sin tener en cuenta las medidas de control para amenazas actuales y para los que una sustitución no sería una opción viable, por su complejidad y por la inversión necesaria.

Habida cuenta de que una gran puerta de entrada de amenazas para los SCI viene dada por su apertura y convergencia con el mundo IT, no hay que olvidar que el corazón del sistema automatizado es el controlador y la instrumentación que le provee de señales. Tomar medidas de protección dirigidas al núcleo del sistema debe ser obligatorio (bastionado de equipos, control de accesos, control de la configuración y del cambio, autentificación, etc.). Combinar este tipo de herramientas y medidas con soluciones de gestión del cambio y configuración en componentes críticos dentro de los entornos industriales, confiere a la estrategia de una gran visibilidad sobre los activos del sistema, para que ante el caso de detección de anomalías, estar en disposición de tomar las acciones oportunas para no perder el control del proceso.

Como hemos podido ver en los diversos ataques producidos, los ciberdelincuentes lanzan sus ataques con diferentes objetivos, que van desde el cobro de una suma de dinero, generalmente en bitcoins por el secuestro de los datos o de los servicios; el robo de información sensible de clientes, el daño de la imagen pública de la empresa y hacer caer sus acciones; las interrupciones del servicio hasta provocar el malfuncionamiento de infraestructuras críticas y causar pérdidas humanas. Por ello, las empresas deben hacer frente a estos ciberdelicuentes y estar bien preparadas para los retos que vienen en los próximos años y afrontar las particularidades que este sector ofrece, por lo que deberían tener en cuenta los siguientes puntos:

- Aumentar la cultura empresarial en ciberseguridad en toda la compañía involucrando a todo el personal para sentirse parte de esa cultura de ciberseguridad y estar preparados ante posibles incidentes.
- Formar y concienciar a los empleados como centro de la ciberseguridad y así reducir los riesgos que puedan conllevar a provocar una amenaza interna.
- Disponer de políticas y procedimientos que definan claramente y guíen a los profesionales, siempre siguiendo los estándares y regulaciones que afecten al sector. Consiguiendo definir una buena estrategia de ciberseguridad industrial que minimice las amenazas existentes.
- Dichos procedimientos deben también actualizarse y adaptarse a novedosas soluciones como IIoT (Industrial Internet of Things), en las que se abandonan las capas claramente definidas del modelo Purdue, que llevan 20 años ayudando a bastionar entornos operacionales, en favor de soluciones basadas en la nube que están cambiando la forma de implementar redes de control industrial, el corazón del sector.
- Definir y llevar a cabo un plan y una estrategia de ciberseguridad específica tanto en el ámbito IT como en el OT que afronte las necesidades de dos mundos claramente diferenciados que en la actualidad convergen como consecuencia de la hiperconectividad de sistemas.
- Establecer e identificar los activos y componentes del sistema OT para realizar una monitorización usando tecnología Deep Packet Inspection (DPI).
- Realizar planes de seguridad con las medidas necesarias para poder prevenir, detectar y responder ante cualquier tipo de incidente, realizando una correcta y rápida gestión y comunicación de incidentes a las autoridades oportunas.
- Estar actualizado en cuanto a las nuevas regulaciones, amenazas, estudios, medidas de contingencia que las instituciones y organismos puedan presentar.
- Colaborar con dichos organismos e instituciones, participando en los diferentes foros de conocimiento existentes donde se comparte información y buenas prácticas.
- Garantizar que las oportunidades que ofrecen las nuevas tecnologías tendrán una protección e integridad de los datos.
- Mantener un proceso de auditorias anuales para mantener un sistema actualizado, robusto, junto con un análisis exhaustivo de riesgos y las medidas necesarias para poder mitigarlos.

Estos aspectos deberían ser consensuados por la organización dado el gran impacto que causan y por eso hay que conseguir encontrar una igualdad entre las nuevas medidas implantadas de ciberseguridad y la respuesta que se consiga realizar ante los incidentes.

Además, no sólo las organizaciones de estos sectores deben estar preparadas, sino que hay que pensar en los diferentes agentes que están dentro de la cadena de valor del sector, ya que todos debemos estar enfocados y tener en mente la ciberseguridad. Por ejemplo, los fabricantes deben tener en cuenta la privacidad y seguridad por defecto desde el diseño.

Por ello, todos los integrantes deben tener claro que para afrontar los siguientes años donde la tecnología ofrecerá grandes ventajas, pero también se producirán ataques más sofisticados, cada parte implicada debería:

- **Operadores**: mejorar su capacidad de recuperación ante cualquier tipo de incidentes.
- **Fabricantes**: proporcionar equipamiento seguro y que se distribuyan los parches de seguridad cuando se detecten las vulnerabilidades.
- **Proveedores de soluciones de ciberseguridad**: proporcionar tecnología y soluciones para una alerta temprana de ciberataques además de una monitorización de la red.
- **Empresas de servicios de ciberseguridad**: ayudar y colaborar en la aplicación e implantación de políticas y estándares.
- **Proveedores cloud**: adquirir la responsabilidad de alojar aplicaciones que interaccionen con componentes de los sistemas de control, con todas las garantías de confidencialidad, disponibilidad e integridad.

Conclusiones

El sector utilities resulta de vital importancia dentro de la economía y la sociedad, asegurando su resiliencia y capacidad de adaptación y continuidad del servicio ante cualquier tipo de amenaza o incidente de ciberseguridad.

Para la profunda transformación con la digitalización y la conectividad que conllevará el mundo IoT junto con el 5G, será necesario asegurar un buen funcionamiento de las infraestructuras existentes, y como hemos comentado, será necesario tener en cuenta la ciberseguridad, junto con la privacidad y seguridad por defecto desde el diseño y a lo largo de toda la cadena de suministro, así como de su ciclo de vida.

Por eso, es fundamental la definición y seguimiento de estándares claros, junto con un marco de gobierno dentro de las organizaciones que aporte seguridad a usuarios, fabricantes y operadores. Con todo ellos conseguiremos fomentar una cultura de ciberseguridad que permitirá hacer frente a las amenazas que provienen del exterior, ya sea definiendo políticas y formando a nuestros empleados con un mayor conocimiento para poder reaccionar y pensar respuestas ante posibles incidentes.

12 grandes hitos de nuestros 100 números

9. Industrializando las labores de seguridad en el ciclo de vida del desarrollo del software

Artículo Febrero 2021

Durante años, en lo referente al desarrollo de software, las compañías han prestado más atención a la cantidad y la operación que a la calidad y a la seguridad. Actualmente, con el incremento de los ciberataques, esta tendencia está cambiando y cada vez son más los controles de seguridad que se integran en el ciclo de vida del desarrollo software.

La carrera hacia la digitalización está provocando en las organizaciones la necesidad de generar un gran volumen de software. Esto ha desembocado en una tendencia a industrializar los procesos de construcción, testing, despliegue y operaciones, que se traduce en ahorro de costes, tiempos, y en la mejora de la calidad del software, gracias a la integración herramientas automáticas a lo largo de todo su ciclo de vida. La expansión de este modelo repercute también en el ámbito de la seguridad del software, la cual debe integrarse paralelamente y formar parte de estos procesos automáticos.

Pero ¿Cómo podemos incluir adecuadamente la seguridad en su ciclo de vida?,¿Cómo podemos saber si los controles de seguridad adoptados son suficientes?, ¿Cómo automatizamos las tareas de control? Existen metodologías para comprobar el nivel de madurez en seguridad sobre el SDLC de una organización, OpenSAMM es un ejemplo.

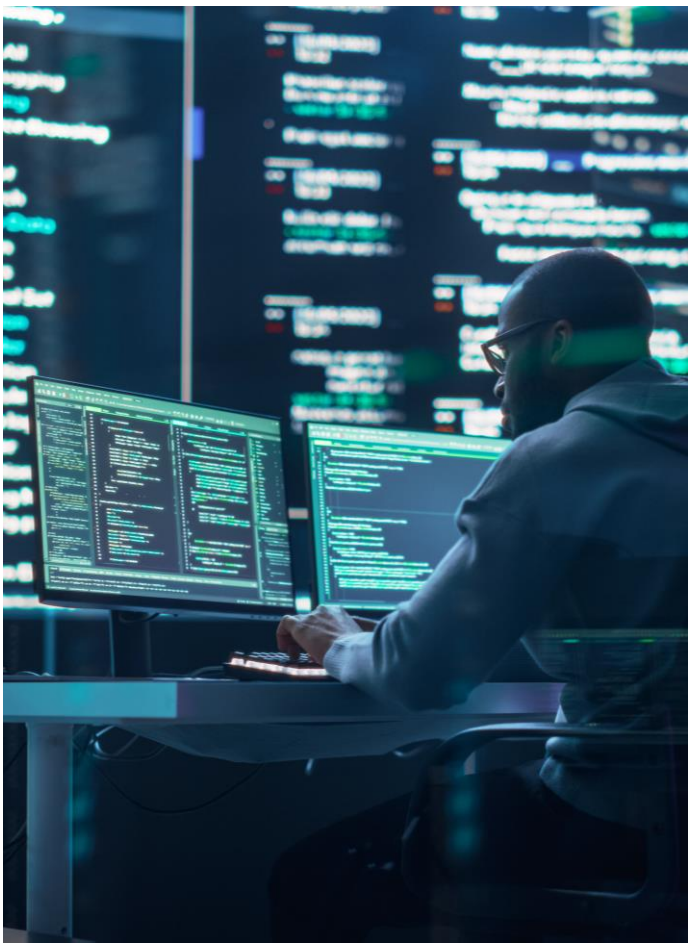
Antes de profundizar, debemos comprender en qué consiste el concepto de ciclo de vida de desarrollo del software (al que en adelante llamaremos SDLC) y cómo su industrialización y automatización de procesos desemboca en lo que conocemos como DevOps.

El SDLC (Security Development Life Cycle) es la metodología adoptada por una compañía que define, organiza y orquesta todos los procesos y tareas implicadas desde que nace la necesidad de crear un software hasta que éste se despliega en producción. Cuando se integra la seguridad en todos estos procesos y tareas se consigue lo que se conoce como Secure SDLC (o SSDLC).

Dentro del SSDLC, las tareas y procesos son agrupados en fases claramente diferenciadas por su tipología, haciendo más fácil definir los límites de responsabilidad y de cumplimiento de la seguridad para permitir el paso del software a la siguiente fase.

Para todo aquel que de alguna manera haya participado en proyectos de desarrollo, las siguientes fases de un SSDLC le resultarán familiares:

1. Requisitos.
2. Diseño.
3. Implementación - desarrollo.
4. Testing y verificación.
5. Despliegue.
6. Operación.

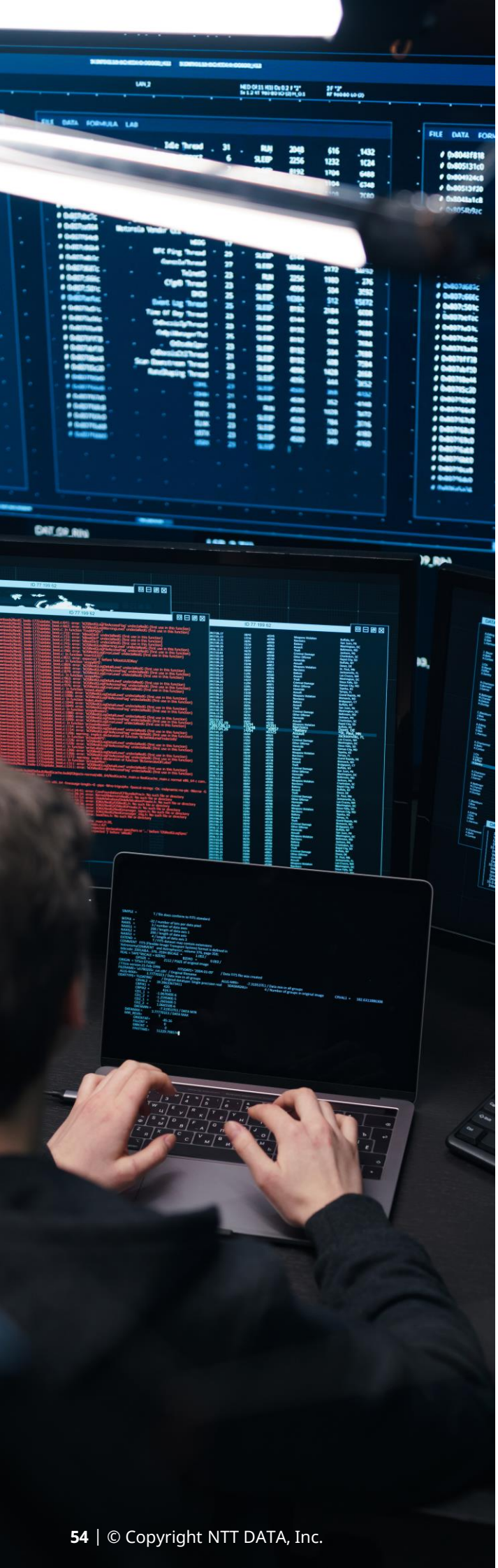


A continuación, enumeramos una serie de tareas que se recomienda realizar cuando se busca incrementar el nivel de madurez en seguridad de un SDLC para convertirlo en un Secure SDLC:

1. Durante la toma de requisitos siempre debería existir un rol de arquitecto de seguridad que sepa establecer las necesidades de seguridad según los requisitos de negocio del software, así como la línea base de requisitos que debe cumplir. Siempre es una buena práctica apoyarse en estándares como OWASP ASVS, OWASP WSTG, PCI DSS (si aplica), etc., con el objetivo de cubrir todos los dominios de la seguridad.

2. Diseñar y modelar el software en función de los requisitos es una tarea importante que va ganando cada vez mayor peso desde el punto de vista de la seguridad. Es en esta fase donde se lleva a cabo el análisis de las superficies de ataque y el modelado de amenazas. La importancia de estas tareas radica en el descubrimiento de vulnerabilidades potenciales en etapas tempranas del ciclo de vida del software, incluso antes de que comience el propio desarrollo. Detectar las posibles carencias de seguridad en los inicios, permite mejorar su seguridad, reducir las vulnerabilidades a futuro y, por consiguiente, reducir los costes de desarrollo para mitigarlas.

3. La ejecución de escaneos de seguridad sobre el código fuente durante la etapa de implementación/desarrollo permite descubrir vulnerabilidades mientras se desarrolla. Disponer de herramientas SAST y SCA en sistemas CI/ CD, posibilita que los desarrolladores puedan detectar las vulnerabilidades mientras están desarrollando, tanto en el código como en las dependencias. En esta fase se hace muy interesante disponer del rol de Security Champion, una figura que pertenecerá al equipo de desarrollo, pero que dispondrá de conocimientos básicos de seguridad, lo que le hará capaz de traducir al equipo de desarrollo los términos del equipo de seguridad.



4. Cuando el software ya es funcional y comienza a desplegarse en entornos de integración o testing, comienza la fase de testing y verificación. Aquí las pruebas suelen ser ejecutadas tanto por herramientas automáticas como manuales (estas últimas ejecutadas por hackers éticos), intentando reproducir el comportamiento de usuarios mal intencionados. Estas pruebas son complementarias a las pruebas sobre el código fuente, ya que son capaces de descubrir debilidades en el software que difícilmente se encontrarían analizando el código, como por ejemplo el escalado de privilegios o la gestión de sesiones.

5. Finalmente, y tras haber superado con éxito las pruebas de seguridad en las fases previas, se procede al despliegue del software en entornos productivos. Estos entornos son los reales, donde la versión liberada se pone a disposición de los usuarios finales y, por tanto, está accesible a posibles usuarios mal intencionados. Por tanto, en esta fase del SSDLC se continuarán realizando pruebas de testing (automáticas y manuales, principalmente éstas últimas) como en el punto anterior, pero en este caso con ciertas limitaciones, ya que no queremos causar la indisponibilidad del software: se definirán ventanas de pruebas, se evitarán pruebas de denegación de servicio, etc.

6. En la última fase, el software ya se encuentra desplegado y ha de mantenerse operativo y protegido durante el tiempo que la versión en cuestión se encuentre en producción. Con este objetivo, existen herramientas y sondas de detección de ataques y protección del software en tiempo real. Un ejemplo de este tipo de herramientas son las IAST, encargadas de monitorizar, detectar e incluso en algunos casos, detener el ataque. En esta fase se recomienda registrar y monitorizar los eventos de los elementos de seguridad perimetral (firewalls, IPS, IDS, agentes, etc.) para detectar funcionamientos anómalos provocados por un atacante.

El hecho de que la ejecución de las tareas anteriores repercuta exitosamente sobre la seguridad del software, dependerá en gran medida de la orquestación entre cada una de las fases. Como si de un director de orquesta se tratase, el equipo de seguridad debe ser quien se encargue de establecer un sistema de gestión y administración de las vulnerabilidades detectadas en cada fase, así como realizar un seguimiento de éstas según su criticidad y el momento en que fue descubierta (cuanto mayor sea este, mayor serán las penalizaciones).

Un punto de interés en la orquestación de tareas es el establecimiento de puntos de control de seguridad. Hemos hablado de cómo analizar la seguridad en cada fase, sin embargo, no hemos comentado nada sobre el establecimiento de penalizaciones si los resultados de las pruebas no son exitosos, evitando que se pase a la siguiente fase si el software tiene un alto número de vulnerabilidades críticas o éstas llevan largo tiempo sin solventarse. Estos puntos de control son llamados Security Gates y funcionan como umbrales o limitaciones que evitan que un software vulnerable pase a la siguiente fase en su ciclo de vida y pueda incluso llegar a ser desplegado en un entorno productivo.

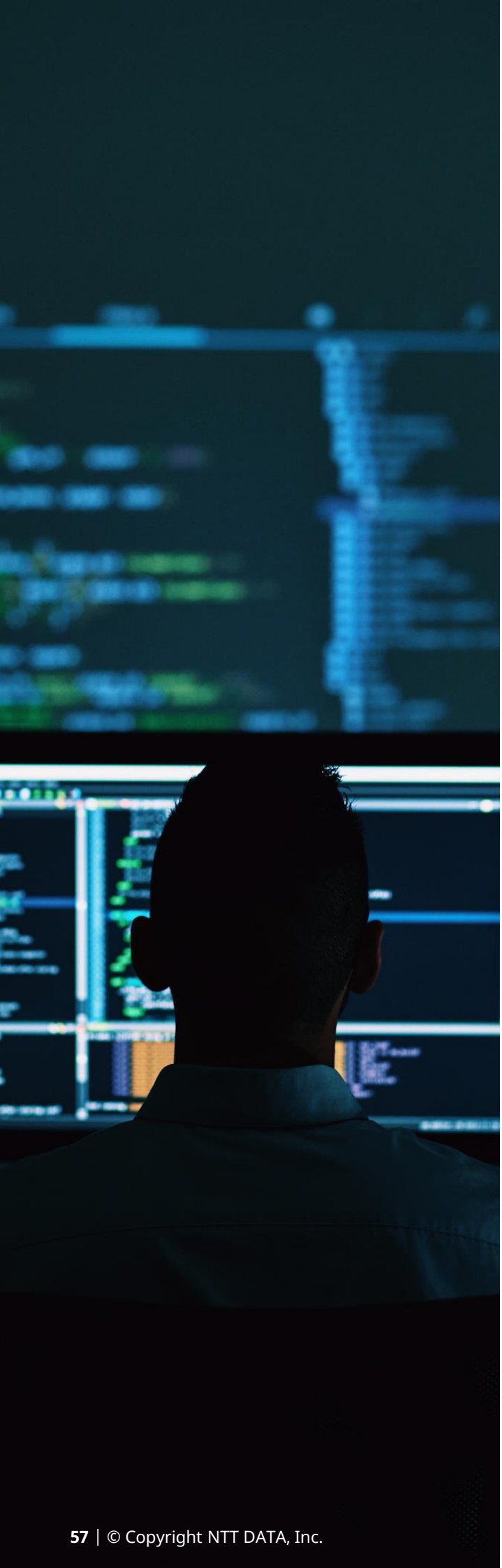
Con el objetivo de establecer estos umbrales, se definen modelos teóricos mediante fórmulas, como, por ejemplo:

$$health = 100\ x \frac{\log_{10}((4\ x\ CVN + 3\ x\ HVN + 2\ x\ MVN + LVN) + 1)}{\log_{10}(nº\ of\ lines)}$$

La fórmula anterior representa la salud obtenida al ponderar los resultados de un análisis SAST, donde:

- **CVN (Critical Vulnerability Number):** es el número de vulnerabilidades críticas encontradas.
- **HVN (High Vulnerability Number):** es el número de vulnerabilidades altas encontradas.
- **MVN (Medium Vulnerability Number):** es el número de vulnerabilidades medias encontradas.
- **LVN (Low Vulnerability Number):** es el número de vulnerabilidades bajas encontradas.
- En número de líneas se corresponde con el total del número de líneas de Código que se han analizado.
- Los factores 4, 3, 2 representan la ponderación asignada a cada tipo de vulnerabilidad según su criticidad, asignando mayor peso a las vulnerabilidades críticas.

Es perceptible a la vista que los modelos teóricos son muy complejos y difícilmente medibles a la hora de automatizar tareas, por eso normalmente se toman como referencia el volumen de vulnerabilidades y sus criticidades. Por ejemplo, si tras un análisis SAST, el código fuente presenta una vulnerabilidad crítica, el software no podrá pasar a la fase de testing y validación. Esto es mucho más sencillo que desarrollar un script que realice la operación logarítmica del modelo y tome una decisión.



Llegados a este punto, hemos conseguido establecer en nuestra organización un SSDLC con un nivel de madurez que dependerá de cuántos de los procesos de seguridad expuestos anteriormente se hayan cubierto.

Estos procesos se deberán mantener y mejorar con el tiempo para evitar la obsolescencia y mantener/mejorar el nivel de madurez de seguridad adquirido.

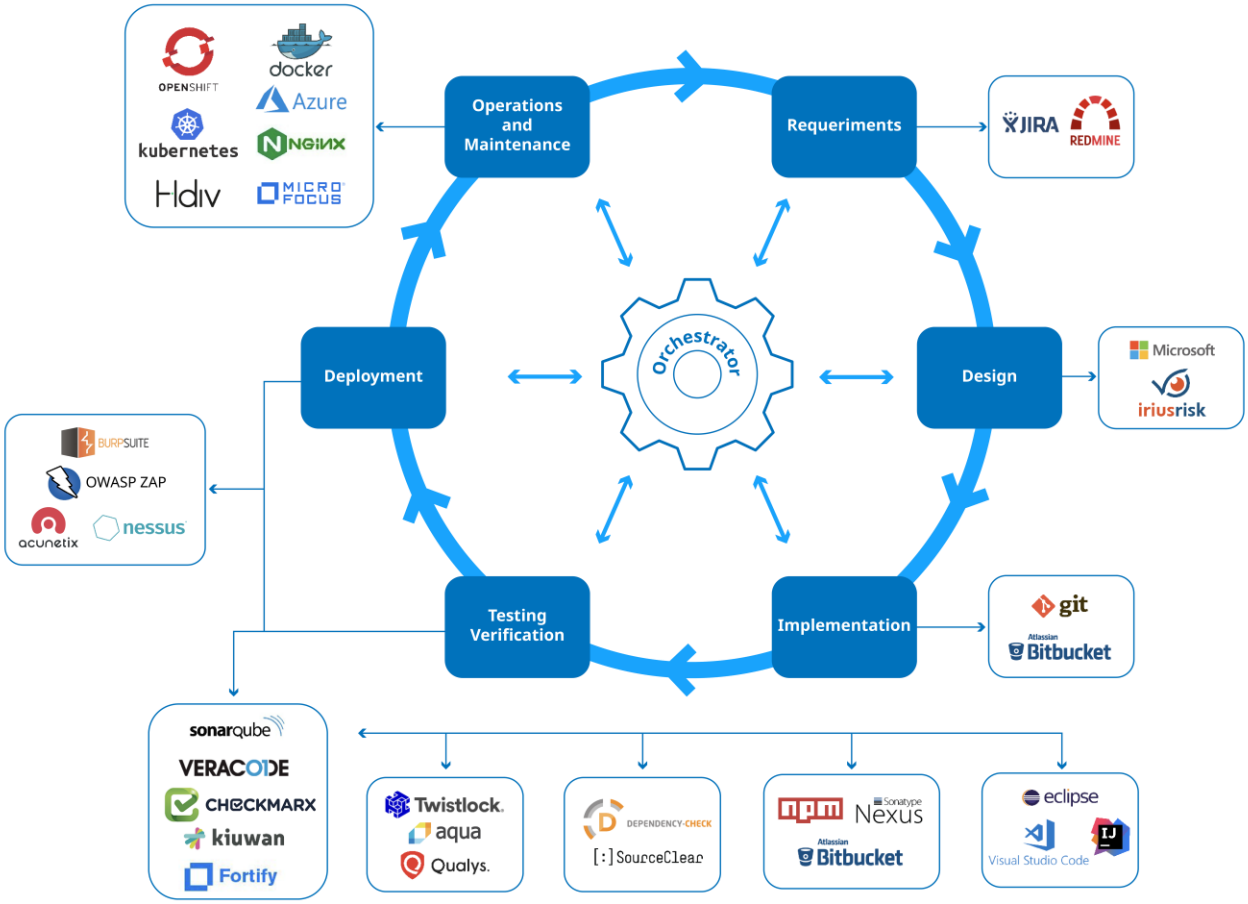
Como introducíamos al inicio, las compañías están tendiendo a la industrialización de los procesos. Cuando se automatizan los procesos del SSLDC obtenemos un SecDevOps (o DevSecOps). Existen numerosos foros de discusión sobre dónde colocar la sílaba 'Sec' en la palabra 'DevOps', en este caso, hemos optado por ponerla al principio, ya que pensamos que la seguridad debe estar desde el inicio del desarrollo, desde la toma de requisitos y el diseño hasta las fases de mantenimiento y operaciones en entornos finales o productivos.

La automatización se consigue insertando herramientas que realicen las tareas y procesos definidos en la metodología de nuestro SSDLC. La pieza básica de este engranaje de herramientas será el orquestador, el cual lanzará las herramientas.

Cumpliendo con la metodología, el orquestador marcará el flujo de fases, de tal forma que, si los resultados obtenidos por alguna de las herramientas no son exitosos, se detendrá la ejecución de herramientas. En estos casos fallidos, donde no se ha superado el Security Gate definido, se debería generar una alerta, tanto para los responsables del equipo de seguridad, como para los Security Champions de los equipos de desarrollo. De esta forma se garantizará que se revisen las ocurrencias detectadas y en caso de ser necesario se registren como vulnerabilidad en el sistema de gestión de vulnerabilidades.

Un ejemplo de orquestador muy usado es la herramienta Jenkins, de la cual existen numerosos plugins para la integración con herramientas de seguridad que automatizan pruebas en el SSDLC. En este caso, Jenkins permite definir procesos llamados 'Pipelines', donde se configura el flujo, el orden y las instrucciones de ejecución de las herramientas en caso de éxito o fallo.

A continuación, podemos ver ejemplos de herramientas que suelen usarse en entornos SecDevOps para la automatización de tareas en el SSDLC:



Hemos apreciado la tendencia al alza de las compañías hacia la integración de la seguridad en su SDLC. Igualmente, hemos detectado en nuestros clientes una alta conciencia de adoptar las buenas prácticas de seguridad desde las primeras fases del desarrollo software. Sin embargo, la inversión en seguridad aún es pequeña comparada con la empleada en los desarrollos y, en muchos casos, insuficiente.

Más allá de la necesidad de seguir mejorando la seguridad en el SDLC, el verdadero reto se anuncia con la migración de las organizaciones hacia entornos Cloud, donde se abandona el modelo OnPremise y las herramientas de seguridad se integrarán como un servicio más dentro del Cloud del que dispongamos.

En este nuevo modelo, los equipos de seguridad y desarrollo deberán estar más cerca que nunca ya que la línea entre entornos, configuraciones, desarrollo, implementaciones, será cada vez menos apreciable y el modelo SecDevOps se cobra como un nuevo paradigma.

12 grandes hitos de nuestros 100 números

10. La privacidad, desinterés generalizado

Artículo Agosto 2022

Con la evolución de la tecnología, surge nuevos servicios a disposición de las personas, que permiten desde realizar comprar a través de la voz desde nuestras casas a llevar una completa monitorización de parámetros de nuestra salud en el smartphone.

Para el desarrollo y la mejora de estos servicios y métodos de interacción con la tecnología, es necesaria la recolección de datos del uso que las personas hacen de los mismos, lo que ha permitido optimizar los procesos y adaptarlos a las necesidades de los consumidores.

Además del fin puramente técnico de la recolección de datos, surgen a su vez nuevas oportunidades, basadas en la recogida de los datos para su uso en fines comerciales, es decir, su venta a terceros para identificar los gustos y preferencias de los usuarios con el fin de construir un perfil que las compañías de anuncios utilizarán para enfocar su contenido hacia un público más específico, consiguiendo así un mayor impacto en sus anuncios.

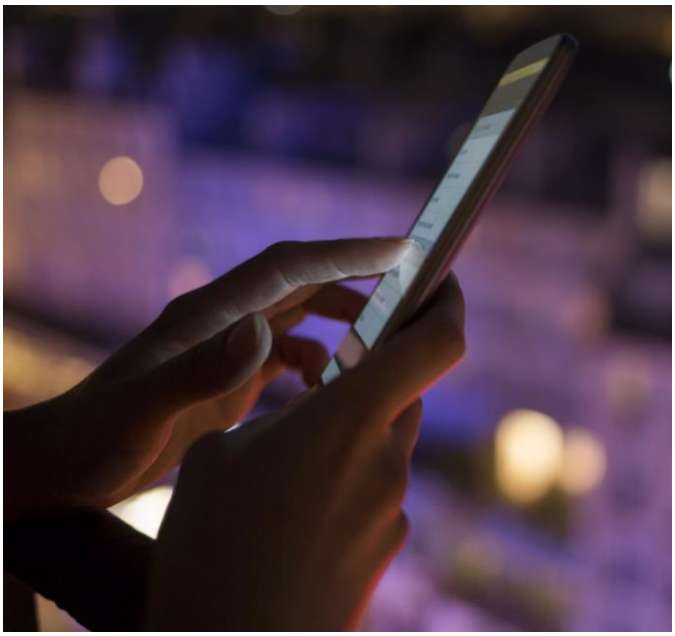
A la par, se crean nuevos mecanismos de recolección de información, que permiten extraer datos de ámbitos anteriormente no accesibles, al no contar con un soporte digital.

Generalmente, la forma de comunicación a los usuarios sobre qué datos se están recogiendo y cómo se procesan se realiza a través de una política de privacidad, que debe ser leída y aceptada por dichos usuarios antes de poder utilizar cualquier servicio que procese y recoja datos.

El uso que se hace de esta información ha derivado en diversos problemas de privacidad, tanto desde un punto de vista más comercial, como desde un ámbito gubernamental, en el que idealmente, los datos sobre los ciudadanos se utilizan para aumentar su seguridad. Como se expone a continuación, el tratamiento de la información de las personas dista de encontrarse en un escenario ideal, ya que han salido a la luz diversas prácticas que hacen que nos cuestionemos hasta qué punto se está respetando la privacidad de los usuarios, actuando en supuesto beneficio de la optimización de las aplicaciones y servicios o el mantenimiento de la seguridad de los ciudadanos.

Orígenes y evolución

Hace algunos años, la privacidad era algo casi desconocido para muchas personas, las mismas que hacían uso de las nuevas tecnologías para facilitarles el día a día, realizando una llamada telefónica, enviando un email, navegando por internet o haciendo uso de alguna aplicación de mensajería instantánea.



Los problemas en torno a la privacidad empezaron a aparecer en 2013, cuando un antiguo empleado de la Agencia Central de Inteligencia (CIA) y la Agencia de Seguridad Nacional (NSA) llamado Edward Snowden, reveló información que indicaba el uso de programas de espionaje masivo por parte de la NSA, como PRISM y XKEYSCORE.

Este escándalo a nivel mundial reveló cómo se había estado espiando en secreto a ciudadanos de todo el mundo. Snowden quiso hacer pública esta información para que las personas fueran conscientes de que su privacidad había sido comprometida sin su consentimiento. Adicionalmente, reveló su identidad y decidió no esconderse anónimamente de las filtraciones, ya que según él no había hecho nada malo.

Han pasado unos cuantos años desde que Snowden mostrara al mundo lo vulnerable que es la privacidad, debido a que los usuarios no disponen de tanta como ellos creen. En este nuevo caso más sonado, el protagonista es una empresa israelí llamada NSO Group, la cual ha desarrollado un software de espionaje conocido como Pegasus.

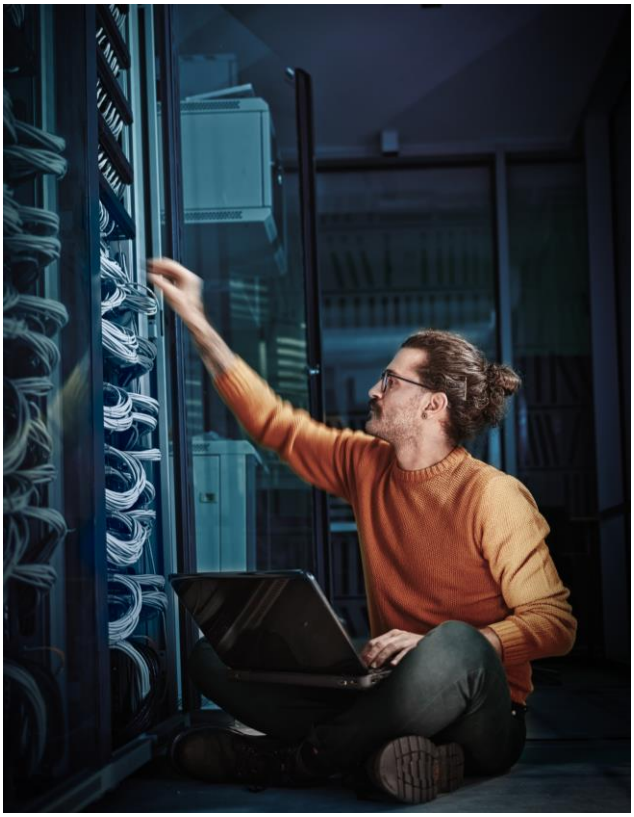
Este software permite infectar y controlar un dispositivo casi sin necesidad de interacción por parte del usuario, otorgándole un control total al software para extraer información a demanda, como escuchar las llamadas, ver los mensajes intercambiados o geolocalizar el dispositivo.

En ambos casos, la “justificación” de la creación de este tipo de software de espionaje intrusivo no es otro que el de evitar el terrorismo o delincuencia grave. Esto no hace más que generar inquietud en aquellos que se pregunten: ¿Hasta qué punto está permitido este comportamiento intrusivo y cuánto pone en peligro la intimidad de los usuarios?

A raíz de esta cuestión, y desde un punto de vista comercial, se han producido varios casos destacados en los que algunas empresas vulneraron la privacidad de los usuarios, realizando un procesamiento de los datos de los usuarios que ha sido considerado abusivo, o no constaba en sus políticas de privacidad.

Uno de los casos recientes en cuestión de privacidad de los usuarios afectó a tres de las empresas tecnológicas más grandes: Con el auge del mercado de los asistentes personales inteligentes, el tratamiento de los datos de voz de sus usuarios se hizo cada vez más habitual. Si bien en la mayor parte de los casos el procesamiento de datos es realizado por medios automatizados, según el NY Times se descubrió que las tres compañías contaban con empleados que escuchaban algunos de los mensajes de voz de los usuarios, sin haberles informado previamente sobre la posibilidad de que sus grabaciones de voz pudieran ser escuchadas y procesadas por personas.

Todas las compañías declararon que este procesamiento se realizaba de forma que las grabaciones permanecían anónimas, pero algunos informes señalaron la posibilidad de que las grabaciones pudieran incluir el nombre del usuario, identificadores del usuario o del dispositivo que se utilizó. Después de estos hechos, , todas las compañías, informan debidamente sobre la revisión humana de grabaciones de voz, dando la posibilidad a los usuarios de sus asistentes inteligentes de decidir si sus muestras de voz pueden ser analizadas por personas o no.



Uso de los datos y tendencias actuales

En el día a día realizamos numerosas interacciones con distintos dispositivos tecnológicos, como un ordenador, móvil o asistente de voz, y seguramente no nos paramos a pensar en la cantidad de información que facilitamos por el simple uso de estos.

Es habitual que durante una navegación por internet se solicite la configuración de las cookies para continuar mostrando el contenido. Esta solicitud suele venir de manera intrusiva con un mensaje que impide la visualización del contenido y el cual requiere que se le preste atención seleccionando alguna de las opciones disponibles. En un primer vistazo la opción más resaltada será la de “Aceptar todas las cookies” y continuar viendo el contenido deseado, quizás sea la opción más rápida, pero ¿Y si en lugar de aceptarlo todo se revisa la configuración? ¡Sorpresa!, en numerosas ocasiones se está proporcionando más información de la que a priori sería necesaria.

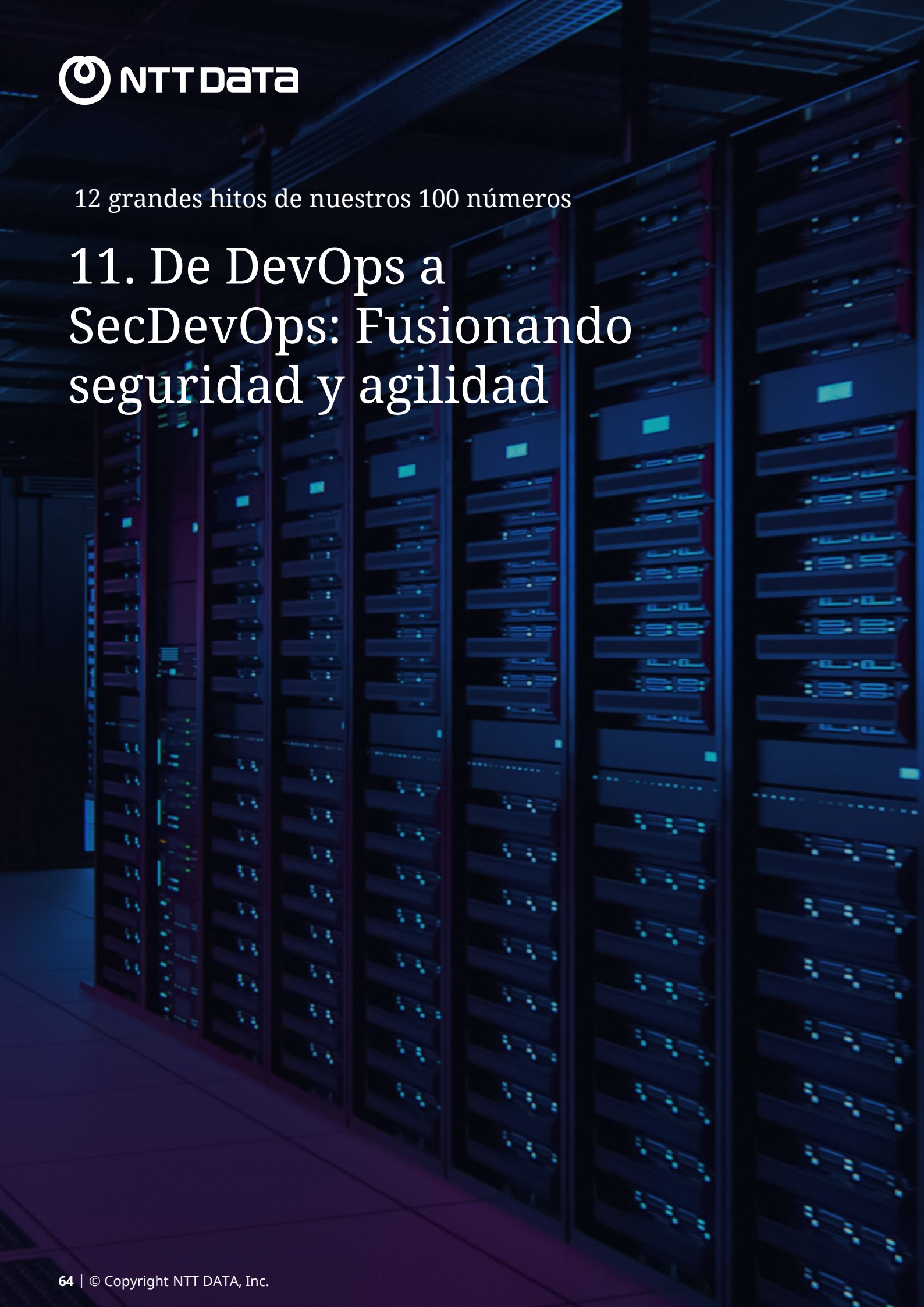
Por otro lado, muchos usuarios disponen de un wearable, como un reloj inteligente, el cual está monitorizando el ritmo cardíaco, calidad del sueño, contando los pasos, compartiendo la ubicación o incluso los mensajes que llegan desde el dispositivo móvil. Toda esta información es manejada por el fabricante de este producto, el cual tiene el poder de decisión de qué hacer con ella, si venderla, compartirla o apostar por la privacidad y que no sea conocida por terceros, este tipo de información dependerá de la política de privacidad que tenga cada uno.

En los últimos años, gracias en parte a la exposición de algunas prácticas, como las mencionadas anteriormente, han surgido iniciativas para proporcionar a los usuarios una mayor protección frente a una recolección abusiva de sus datos. Por ejemplo, los Marketplace de aplicaciones (primero en la App Store de iOS y más tarde en la Play Store de Android), incorporan una nota sobre los datos que se recogerán del usuario cuando utilice alguna aplicación que descargue del Marketplace, dando una vista más adecuada que resume parte de la política de privacidad de la aplicación, que de otra forma el usuario normalmente no leería para comprobar cómo se utilizarán sus datos.

Así mismo, el sistema que gestiona los permisos de los sistemas operativos móviles más populares ha ido mejorando para dar un control más preciso sobre qué opciones del dispositivo puede o no puede utilizar una aplicación. Se da la posibilidad a los usuarios de seleccionar opciones más respetuosas con la privacidad, por ejemplo, a la hora de compartir los datos de ubicación de su dispositivo con ciertas aplicaciones, se permite dar una ubicación aproximada, en vez de proporcionar una ubicación exacta.

Junto con las mejoras nativas de los sistemas operativos, han surgido aplicaciones con la idea de proteger la privacidad de los usuarios, frente a las aplicaciones tradicionales de distintos ámbitos. Por ejemplo, en el caso de las aplicaciones de mensajería, mientras que Facebook Messenger recoge y asocia a los usuarios datos como información financiera, localización, contactos, historiales de búsqueda, contenido del usuario (fotos, vídeos, etc.) o información de contacto (nombre, correo electrónico, dirección física, etc.), otras aplicaciones como Signal no recogen este tipo de información para vincularla a cada usuario y utilizarla con fines comerciales.

La percepción de la privacidad de los consumidores ha ido evolucionando, dándole cada vez más peso a la hora de elegir un servicio u otro, aunque queda mucho trabajo por hacer para pasar de un argumento más de venta a un control real que permita a los usuarios decidir con quien se pueden compartir sus datos y con qué fin.



12 grandes hitos de nuestros 100 números

11. De DevOps a SecDevOps: Fusionando seguridad y agilidad

Artículo Diciembre 2023

DevOps: Development + Operations. Fusionar los procesos propios de desarrollo del software con aquellos pertenecientes a la integración y despliegue de dichos desarrollos. Suena difícil, y, de hecho, lo es. Si sumamos a la ecuación la ciberseguridad, se complica. A partir de ese momento pasamos a hablar de DevSecOps, o incluso de SecDevOps, dependiendo de lo presente que esté la seguridad en todo el proceso.

Las sinergias entre ciberseguridad y DevOps

Inicialmente DevOps surge de la necesidad de construir y entregar software de forma continua y automática lo más rápido posible. Un equipo de desarrolladores termina de implementar una nueva funcionalidad en una aplicación web, e interesa que esa funcionalidad sea probada, integrada y desplegada lo antes posible en los entornos productivos con el objetivo de disponibilizarla cuanto antes al usuario final.

Los conceptos clave aquí son “colaboración” y “acelerar”. Necesitamos colaborar para conseguir la agilidad en la entrega de software a la que aspiramos. Esto presenta una serie de desafíos, mayormente el cambio de mentalidad y que la necesidad de comunicación entre departamentos a veces se demuestra que no es fácil. Un rol de operaciones no se puede meter en la mente de un desarrollador y viceversa. Sin embargo, el cambio tampoco tiene por qué ser inmediato y se pueden ir incorporando procesos/tecnologías poco a poco.

La preocupación de las empresas en torno a la ciberseguridad ha ido aumentando en estos últimos años, a medida que fueron creciendo tanto el número de ataques como la gravedad de las consecuencias.

Se hizo patente que era necesario desarrollar software poniendo especial atención a la seguridad de este.

Tenemos un escenario en el que necesitamos construir y entregar software de forma ágil (DevOps), pero a la vez garantizando su robustez ante ciberataques (Sec). Así nace el DevSecOps. De nuevo, esto presenta sus desafíos, ya que ahora no es sólo una colaboración entre Devs y Ops, sino que también se integran el equipo de ciberseguridad.

Además, la inclusión de herramientas y procesos de seguridad al final puede repercutir en la rapidez con la que un desarrollo sale a un entorno productivo. Esto se debe a que el hecho de incluir los análisis necesarios para verificar la seguridad de dicho desarrollo puede ralentizar el proceso global, sobre todo si es necesario incluir un filtrado de falsos positivos. Sin embargo, debemos decidir qué es lo importante: que los desarrollos salgan lo más rápido posible a entornos productivos independientemente de las vulnerabilidades que puedan contener, o que, a pesar de una menor rapidez en este despliegue, nuestros desarrollos cuenten con un grado suficiente de seguridad.

De la teoría a la práctica: herramientas para hacer seguro el desarrollo

Hoy en día existe un amplio abanico de herramientas que nos ayudan a aportar seguridad a los desarrollos incluidos en un entorno DevSecOps. Dependiendo del tipo de tarea que lleven a cabo y del momento en que se ejecuten, podemos diferenciar los siguientes tipos:

- **SAST: Static Application Security Testing**. En esta clasificación encontramos aquellas herramientas que analizan el código fuente de los desarrollos en busca de posibles defectos que puedan provocar vulnerabilidades de seguridad. Ejemplos de tecnologías SAST son: Veracode, Fortify o Coverity.
- **SCA: Software Composition Analysis**. Este tipo de software se encarga de detectar si existen vulnerabilidades de seguridad conocidas en las dependencias externas utilizadas en los desarrollos. Ejemplos de herramientas SCA son: Snyk, Black Duck o XRay.
- **DAST: Dynamic Application Security Testing.** Similar al SAST, pero con la diferencia de que en vez de analizar el código fuente de los desarrollos, analiza el comportamiento de estos una vez desplegados. Realiza pruebas automáticas en busca de comportamientos que podrían fallos de seguridad, como fugas de información o indisponibilidad de los servicios. Ejemplos de herramientas DAST son: Burp Suite, Nessus, Acunetix.
- **RASP: Runtime application self-protection**. Similar a la tecnología de los WAF (Web Application Firewall). Se encarga de detectar y bloquear posibles intentos de ataque sobre aplicaciones desplegadas. A diferencias de los WAF, que funcionan a nivel de red, los RASP se ejecutan a nivel de aplicación. Cuentan con cierta información sobre la funcionalidad e infraestructura interna de las aplicaciones que protegen y, por lo tanto, son más precisos a la hora de detectar posibles ataques. Ejemplos de RASP son: Imperva, Hdiv y OpenRASP.

DevSecOps vs SecDevOps

Hoy en día, ambos términos se utilizan indistintamente como sinónimos y la diferencia es bastante difusa. Sin embargo, hay algunos matices que los diferencian.

• DevSecOps es un entorno de DevOps al que se le han incluido añadidos de seguridad: Herramientas SAST/SCA para analizar el código y las dependencias, tal vez un RASP para monitorizar y proteger los desarrollos ya desplegados... En definitiva, la seguridad existe en el entorno DevOps como un añadido necesario, pero sin que afecte a todas y cada uno de los procesos que se ejecutan.

• SecDevOps es un entorno de DevOps en el que se prioriza la seguridad y se pone un foco consciente en que cada uno de los procesos existentes se lleven a cabo teniéndola en cuenta. Los desarrolladores tienen disponibles herramientas de análisis SAST en sus IDEs; existe una batería de pruebas de seguridad actualizada periódicamente que se ejecuta cada vez que se sube código a los repositorios; se ejecutan análisis completos SAST, SCA, DAST y/o IAST con security gates que evitan que se desplieguen desarrollos vulnerables, y se monitorizan y protegen los desarrollos desplegados mediante herramientas RASP y/o SIEM.

Mientras que en DevSecOps la seguridad es contemplada y se tiene en cuenta, en SecDevOps se prioriza y se considera el elemento que tiene que abarcar al resto.

Como nota final, nuestro objetivo es construir software, no sólo de forma ágil, sino también con las mayores garantías de seguridad posible. Por lo tanto, deberíamos apuntar siempre a contar con un entorno SecDevOps. Sin embargo, lo más probable es que intentar pasar directamente de un entorno DevOps a uno SecDevOps sea contraproducente, ya que todos los usuarios implicados se verán sobrepasados con tal volumen de nuevas herramientas y procesos. La mejor estrategia consistirá en ir implementando poco a poco dichas herramientas y, al mismo tiempo, ir formando a los usuarios en el uso de las mismas.

12 grandes hitos de nuestros 100 números

12. *Awareness*: Los catastrofistas de la ciberseguridad

Artículo Junio 2024

El factor humano sigue siendo uno de los aspectos más críticos y, a veces, vulnerables en la seguridad cibernética. Las acciones y decisiones de las personas pueden afectar significativamente la postura de seguridad de una organización, ya sea fortaleciéndola o comprometiéndola. Es por ello que la concienciación y la formación son piedras angulares en la defensa contra las cada vez más sofisticadas amenazas cibernéticas.

Los profesionales de la formación en ciberseguridad tenemos la tarea de educar a los clientes sobre los riesgos cibernéticos y capacitarlos para proteger sus datos y sistemas. Esta labor conlleva un delicado equilibrio: por un lado, es vital destacar la gravedad de las amenazas y las potenciales consecuencias de sufrir un ciber- ataque; por otro lado, exagerar o enfatizar en exceso estos peligros puede generar miedo y desconfianza entre los usuarios.

Debido a esta fina línea, quienes nos dedicamos a esta tarea a menudo enfrentamos una etiqueta curiosa: los "catastrofistas" de la ciberseguridad. Destacar los riesgos inherentes en el mundo digital y las consecuencias catastróficas de un ataque exitoso, nos coloca en una posición incómoda, vista por algunos como portadores de malas noticias o alarmistas.

Esta percepción, aunque común, es una simplificación de un trabajo crucial y multifacético. En todas nuestras acciones formativas, los participantes se enfrentan directamente a la realidad de las ciber-amenazas, explorando de primera mano lo fácil que puede ser caer en una trampa.

A través de ejercicios prácticos y demostraciones interactivas, se ilustra la sofisticación y la variedad de técnicas utilizadas por los ciberdelincuentes para engañar a las víctimas y comprometer la seguridad de la información. Los formadores en ciberseguridad, a fin de cuentas, somos educadores, no profetas del desastre.

Sin embargo, en reiteradas ocasiones, los usuarios nos han expresado su inquietud por la sensación de ansiedad y temor que experimentan al participar en algunas acciones formativas. Cuando creen haber aprendido a defenderse de una amenaza específica, surge una nueva vulnerabilidad o técnica de ataque para la que no están preparados. Esta preocupación ha sido tan frecuente que, en tono jocoso, hemos llegado a bromear sobre la idea de distribuir valerianas al término de dichas sesiones.

Y es que es comprensible que los empleados puedan experimentar cierta ansiedad al enfrentarse al ciber-crimen. Apenas hace un año seguíamos recomendando buscar errores ortográficos en los emails para identificar ataques de ingeniería social. Hoy, los estafadores redactan sus mensajes fraudulentos con una gramática envidiable gracias a la inteligencia artificial.

Esta percepción refleja la naturaleza siempre cambiante y evolutiva del panorama de la ciberseguridad, donde los ciberdelincuentes constantemente desarrollan nuevas estrategias y la sensación de estar constantemente un paso atrás puede generar frustración entre los usuarios.

Para evitar este desaliento es importante poner el foco en la adopción de hábitos y comportamientos seguros en línea, aprender sobre medidas preventivas y conocer los beneficios de una buena higiene digital. Además, la educación en ciberseguridad no debe ser un evento único, sino un proceso continuo. Como eslabón (que no débil, sino esencial) de la cadena de la ciberseguridad, es nuestra obligación mantenernos informados sobre las últimas amenazas y mejores prácticas de seguridad.

Estamos familiarizados con las medidas preventivas para proteger nuestra casa mientras estamos de viaje durante las vacaciones, pero ¿somos conscientes de los riesgos asociados con conectarnos a redes Wi-Fi públicas de hoteles sin ninguna precaución?

Ambos tipos de riesgos son reales y persistentes, por lo tanto, deberemos asumir el papel de defensores de nuestra propia seguridad y la de nuestras organizaciones. La seguridad cibernética es un esfuerzo colectivo y cada contribución es esencial. Nuestro objetivo es educar de manera proactiva y entendemos que la ciberseguridad puede resultar intimidante, pero siempre os guiaremos de manera segura a través del vasto ciber-espacio.

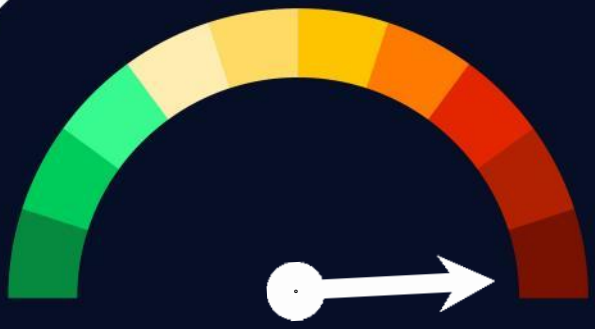
Estamos comprometidos a brindar el apoyo y conocimiento necesario para que las personas se sientan seguras y confiadas en su capacidad para enfrentar cualquier desafío.

Más que catastrofistas, piensa en nosotros como esos amigos que siempre te recuerdan llevar paraguas incluso en un día soleado. Confía en nosotros, algún día lloverá y nos lo agradecerás.

Vulnerabilidades

Vulnerabilidad crítica en productos Apple

Fecha: 27 de enero de 2025
CVE: CVE-2025-24154



CVSS: 9.8

CRÍTICA

Descripción

La vulnerabilidad CVE-2025-24154 se debe a un problema de escritura fuera de límites que afecta a varias de las versiones de los sistemas operativos de Apple macOS, iOS, iPadOS y visionOS.

Este tipo de vulnerabilidad ocurre cuando un programa escribe datos fuera de los límites de la memoria asignada, lo que permite a un atacante causar la terminación inesperada del sistema o la corrupción de la memoria del *kernel*.

Esto representa un riesgo significativo, ya que la corrupción de la memoria del *kernel* puede ser utilizada para ejecutar código malicioso con privilegios elevados.

Solución

Apple ha abordado esta vulnerabilidad mediante la mejora de la validación de entradas fuera de límites.

Se recomienda a los usuarios actualizar sus dispositivos a las versiones corregidas para mitigar este problema.

- macOS Ventura 13.7.4
- macOS Sonoma 14.7.4
- macOS Sequoia 15.3.1
- visionOS 2.3.1
- iOS 18.3.1
- iPadOS 18.3.1

Productos afectados

Esta vulnerabilidad afecta a las siguientes versiones de Apple:

- macOS Ventura 13.7.3
- macOS Sonoma 14.7.3
- macOS Sequoia 15.3
- visionOS 2.3
- iOS 18.3
- iPadOS 18.3

Referencias

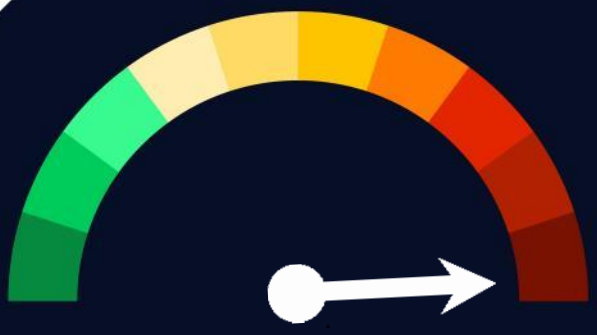
- nvd.nist.gov
- apple.com (iOS y iPadOS)
- apple.com (macOS Ventura)
- apple.com (macOS Sonoma)
- apple.com (macOS Sequoia)
- apple.com (visionOS)

TLP:WHITE

Vulnerabilidades

Vulnerabilidades críticas en productos Microsoft

Fecha: 4 de febrero de 2025
CVE: CVE-2025-21396 y 1 más



CVSS: 9.9

ALTA

Descripción

Microsoft ha publicado dos nuevos avisos sobre vulnerabilidades críticas en sus productos:

- Vulnerabilidad crítica de omisión de autenticación (CVE-2025-21396) con un CVSS Score de 9.8 que podría permitir a los atacantes falsificar credenciales y obtener acceso no autorizado a cuentas de Microsoft. Afecta a los mecanismos de autenticación que dependen de métodos de validación insuficientes o defectuosos.

- Vulnerabilidad crítica de elevación de privilegios (CVE-2025-21415) con un CVSS Score de 9.9, que afecta al servicio Azure AI Face y permite a los atacantes eludir los mecanismos de autenticación a través de una suplantación de identidad.

Solución

Según Microsoft, la vulnerabilidad no se ha revelado públicamente y no se conocen formas de explotarla.

Las vulnerabilidades fueron descubiertas como parte de una iniciativa de Microsoft para agregar transparencia al proceso de actualización de seguridad al revelar vulnerabilidades, incluso si ya se han corregido en el servidor y no se requiere ninguna acción del usuario en estos casos.

Microsoft ofrece más detalles de ambas vulnerabilidades en sus boletines de seguridad:

- CVE-2025-21396
- CVE-2025-21415

Productos afectados

Estas vulnerabilidades afectan a los siguientes servicios:

- Microsoft Account
- Azure AI Face

Referencias

- cybersecuritynews.com
- thehackernews.com

TLP:WHITE

Boletín de seguridad de febrero de Android

Fecha: 3 de febrero de 2025
CVE: CVE-2024-53104 y 47 más

Crítica

Descripción

El boletín de seguridad de Android de febrero de 2025 aborda un total de 48 vulnerabilidades, incluidas dos críticas. Una de ellas es una *zero-day* en el *kernel* de Android (CVE-2024-53104), mientras que la otra se trata de un fallo de corrupción de memoria en el componente WLAN de Qualcomm (CVE-2024-45569). Se conoce que la primera ha sido explotada, representando un riesgo para los usuarios.

Este boletín soluciona las vulnerabilidades de severidades críticas y altas que involucran al sistema operativo y distintos componentes, y que podrían provocar desde la escalada de privilegios, la ejecución remota de código y la corrupción de la memoria, hasta la caída del sistema y el acceso no autorizado a información sensible.
.

Productos afectados

Los componentes afectados por estas vulnerabilidades son:

- Framework
- Plataforma
- Sistema
- Kernel
- Componentes de Terceros:
  - Arm
  - Imagination Technologies
  - MediaTek
  - Unisoc
  - Qualcomm

Además, los dispositivos con Android 10 y versiones posteriores también han sido afectados.

Solución

El fabricante ha publicado los parches de seguridad correspondientes y se recomienda actualizar los productos afectados a la última versión publicada para protegerse contra estas vulnerabilidades.

Referencias

- android.com
- incibe.es
- csirtcv.gva.es

TLP:WHITE

Boletín de seguridad de Cisco Identity Services Engine (ISE)

Fecha: 6 de febrero de 2025
CVE: CVE-2024-20124 y 1 más

Crítica

Descripción

El boletín de seguridad de Cisco, publicado el 6 de febrero de 2025, aborda múltiples vulnerabilidades críticas en Cisco Identity Services Engine (ISE) y Cisco ISE Passive Identity Connector (ISE-PIC).

Estas vulnerabilidades podrían permitir a un atacante remoto autenticado que ejecute comandos de forma arbitraria con permisos de *root* en el dispositivo afectado.

Además, podría permitir que un atacante no autorizado pudiera acceder a información sensible, modificar la configuración de los nodos y reiniciarlos.

Productos afectados

Las versiones de los productos afectados que son vulnerables son los siguientes:

- Cisco ISE: todas las versiones de software de Cisco ISE.
- Cisco ISE-PIC: todas las versiones de software de ISE-PIC.

Como se puede observar, la vulnerabilidad afecta a todas las versiones de dichos productos.

Solución

Cisco ha publicado actualizaciones que solucionan estas vulnerabilidades. Por lo tanto, se recomienda encarecidamente a los usuarios actualizar sus sistemas a las versiones de *software* más recientes.

Referencias

- incibe.es
- cisco.com

Eventos

Mobile World Congress (MWC) 2025
3 – 6 de marzo

Del 3 al 6 de marzo, Barcelona acogerá el Mobile World Congress, el evento más influyente del mundo en el ámbito de la conectividad móvil. Organizado por la GSMA, el MWC25 reunirá a líderes empresariales, innovadores y expertos para debatir y mostrar las últimas tendencias y avances en tecnología móvil, incluyendo temas destacados como la inteligencia artificial y el 5G.

Durante tres días, el evento se centrará en explorar las principales tendencias en estrategias, herramientas y estándares de ciberseguridad. La agenda estará compuesta por sesiones educativas e interactivas diseñadas para promover la generación de conocimientos, la planificación estratégica y el intercambio de experiencias entre expertos del sector.

Enlace

RootedCON 2025
6 - 8 de marzo

Del 6 al 8 de marzo tendrá lugar en Madrid una nueva edición del congreso de seguridad RootedCON, un punto de encuentro fundamental para profesionales del sector, empresas y organizaciones en el que compartir y debatir sobre los últimos avances en ciberseguridad y tecnología. El congreso contará con diferentes charlas conducidas por expertos del sector, así como bootcamps adicionales sobre temáticas especializadas, como Hardware Hacking u OSINT.

Enlace

Liga Nacional de Retos en el Ciberespacio (Ciberliga) - Fase Final
10 -14 de marzo

La Guardia Civil organiza la VI edición de la Liga Nacional de Retos en el Ciberespacio, una competición que busca concienciar a estudiantes sobre el uso seguro y responsable de las nuevas tecnologías. La fase final se llevará a cabo del 10 al 14 de marzo de 2025 en el Centro Universitario de la Guardia Civil en Aranjuez, Madrid, donde los participantes se enfrentarán a "ciber-retos" que simulan incidentes reales.

Enlace

Microsoft AI Tour
27 de marzo

El 27 de marzo Madrid será una de las paradas del Microsoft AI Tour, un evento gratuito dirigido a ejecutivos que explora cómo la inteligencia artificial puede impulsar el crecimiento empresarial y crear valor duradero. El *tour* ofrece contenido valioso sobre seguridad y está adaptado a las necesidades específicas de los asistentes, brindando una visión profunda de las aplicaciones de la IA en el mundo empresarial

Enlace

Recursos

El INCIBE publica el Boletín de Seguridad de Android

El Boletín de Seguridad de Android de febrero de 2025 aborda múltiples vulnerabilidades críticas y altas que afectan a las versiones 12, 12L, 13, 14 y 15 del sistema operativo Android. Estas vulnerabilidades pueden provocar problemas graves como escalada de privilegios, ejecución remota de código, corrupción de memoria y acceso no autorizado a información sensible. Se recomienda a los usuarios de dispositivos Android verificar y aplicar los parches de seguridad proporcionados por los fabricantes para mitigar estos riesgos

Enlace

El Riesgo de Terceros: principal Preocupación de Ciberseguridad para Empresas en 2025

La revista Ciberseguridad destaca que el riesgo de terceros se ha convertido en la principal preocupación de ciberseguridad para las empresas en 2025.
Este riesgo surge de las vulnerabilidades y amenazas asociadas con la integración de servicios y proveedores externos. La gestión de riesgos de terceros (TPRM) es crucial para prevenir brechas de seguridad que puedan comprometer datos sensibles y operaciones comerciales. La ciberinteligencia se utiliza para complementar la TPRM, proporcionando información y contexto para la toma de decisiones informadas.

Enlace

Actualización de Seguridad de Microsoft

Microsoft ha publicado las actualizaciones de seguridad correspondientes a febrero de 2025, corrigiendo 64 vulnerabilidades. Entre ellas, 4 son críticas, 57 importantes, 1 moderada y 2 bajas. Las vulnerabilidades críticas incluyen problemas de ejecución remota de código y elevación de privilegios. Se recomienda a los usuarios aplicar las actualizaciones de seguridad para proteger sus sistemas contra posibles explotaciones.

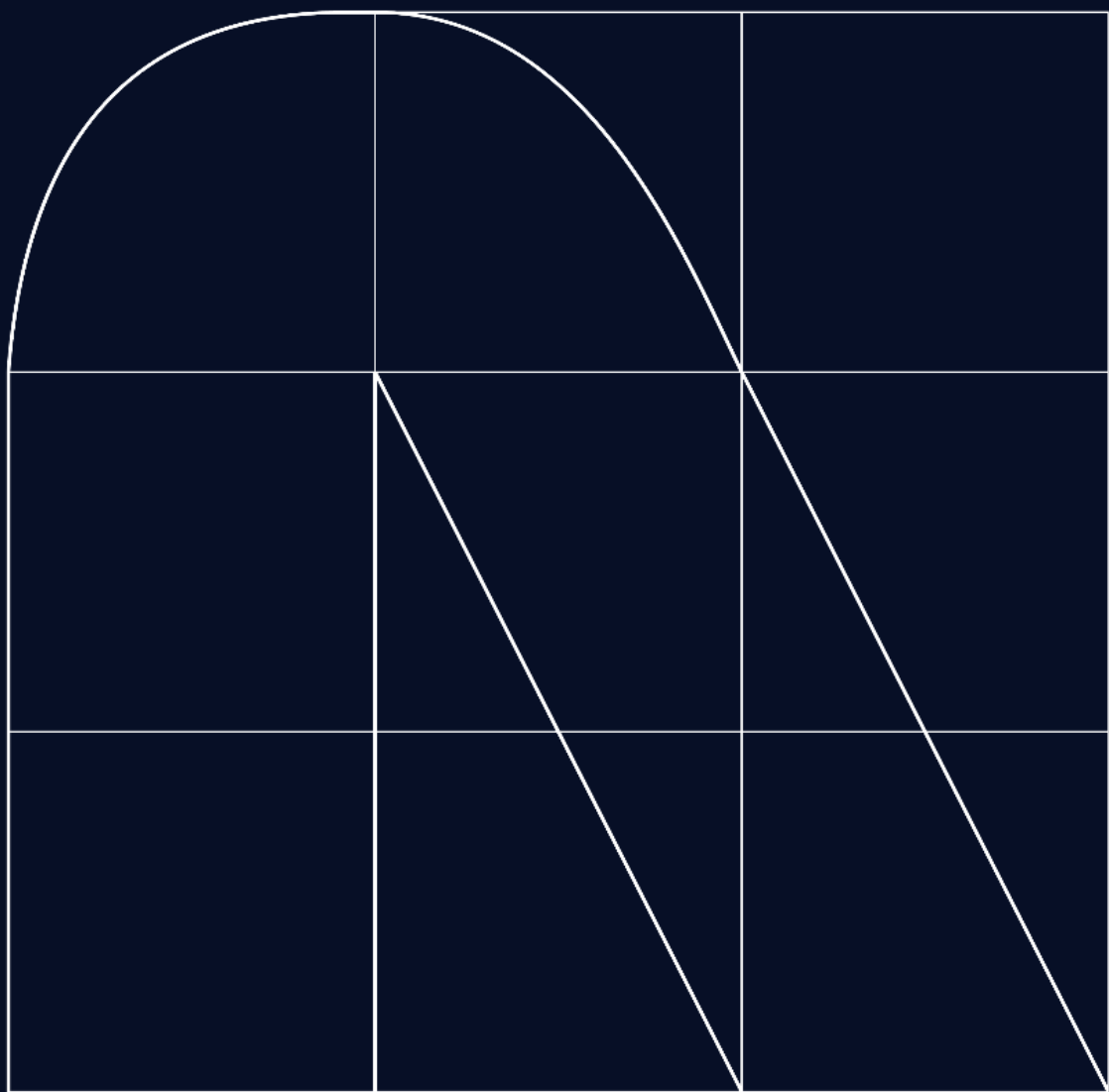
Enlace

La IA y la Ciberseguridad: claves para las PYMES en 2025

Este artículo destaca cómo la inteligencia artificial (IA) se ha convertido en una herramienta esencial para mejorar la ciberseguridad en las pequeñas y medianas empresas (*pymes*) en 2025. La IA ayuda a detectar y responder a amenazas de manera más eficiente, automatizando procesos y mejorando la precisión en la identificación de vulnerabilidades. Además, se discuten casos de uso específicos y tendencias emergentes que las *pymes* deben considerar para protegerse contra ciberataques cada vez más sofisticados.

Enlace

Suscríbete a RADAR



Powered by the cybersecurity NTT DATA team

es.nttdata.com