THIBER DIGEST

Informe mensual de ciberseguridad

Nº 23/ MAYO 2021

Análisis de la actualidad internacional

CISO Remoto, ¿una profesión con futuro?

CIBERATAQUES ABRIL 2021

COMENTARIO THIBER:

La ciberseguridad de la cadena de suministro en defensa y su reto

Desarrollado por THIBER
The cybersecurity think tank

ÍNDICE / THIBER DIGEST

Informe mensual de ciberseguridad

Nº 23/ **MAYO 2021**

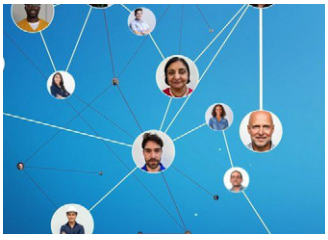
03

Comentario THIBER
La ciberseguridad de la cadena de suministro en defensa y su reto ante la adopción del multidominio

05

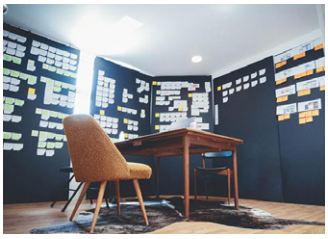
Informes y análisis sobre ciberseguridad publicados en abril de 2021

06



Análisis de actualidad
Ciberataques abril 2021

15



Análisis de la actualidad internacional
CISO Remoto, ¿una profesión con futuro?

22

Libro recomendado
Data nomics

23

Eventos

Comentario THIBER:

La ciberseguridad de la cadena de suministro en defensa y su reto ante la adopción del multidominio

AUTOR: por THIBER

Fuente: Airbus

A la hora de describir el qué y cómo se comunica de forma clásica un activo de las fuerzas armadas, es sencillo imaginarse la utilización de procesos extremadamente robustos en la gestión de la ciberseguridad en el plano táctico-operativo, así como el uso de tecnologías maduras y validadas en su implementación.

Sin embargo, existen multiples ejemplos de incidentes que nos muestran graves fallos en los procesos de la gestión de la ciberseguridad, no tanto a nivel operativo o táctico, sino en un ámbito global donde se incluye a la cadena de suministro de los propios activos. En este sentido, un buen ejemplo sería la captura de un dron RQ-170 norteamericano por parte de Irán en diciembre de 2011, en donde, la teoría más extendida y aceptada se basa en el robo de las claves de autenticación del dron a uno de los proveedores de la cadena de suministro norteamericana.

¿Qué podemos deducir sobre este tipo de incidentes? Más allá del fallo de seguridad específico del proveedor, parece evidente que, hoy en día, la cadena de suministro de los activos del sector de la defensa es un vector de entrada para cualquier potencia enemiga. Además, se podría discutir que precisamente es en este tipo de ataques a proveedores de la cadena de suministro de defensa en donde se convierte la ciberseguridad en ciberdefensa. Dicho de otro modo, un ataque TI clásico a un proveedor (fallo en la ciberseguridad de la industria) se puede convertir en una ventaja táctica muy relevante en el campo de batalla, y ser utilizado por una potencia enemiga (cyberwarfare).

Un ataque TI clásico a un proveedor (fallo en la ciberseguridad de la industria) se puede convertir en una ventaja táctica muy relevante en el campo de batalla, y ser utilizado por una potencia enemiga (cyberwarfare)

Además, estos potenciales vectores de entrada a la cadena de suministro, con implicaciones directas en el campo de batalla, crecen exponencialmente cuando ponemos el foco en las soluciones multidominio y de sistema de sistemas en el ámbito militar.Con arquitecturas funcionales y técnicas que apuestan por la interconexión de multitud de elementos; plataformas aéreas tripuladas, drones, plataformas navales, satélites, fuerzas terrestres, etc... un vector de ataque a uno de los elementos podría, teóricamente, impactar en la fuerza global multidominio si consigue penetrar en la parte core de la red.

En el sector civil esta situación y sus impactos son de sobra conocidos. Existen multitud de ejemplos en donde la penetración de la red en un nodo con un payload de ransomware obliga a desconectar miles de nodos de la red para evitar la propagación del ataque. Ya sea en una empresa multinacional con decenas de miles de empleados o en un hospital, en donde un ataque en un servidor de RRHH del hospital tiene impacto hasta en el uso de máquinas de resonancia magnética.

Sin embargo, en el ámbito militar, con una operación en curso, es muy improbable que el mando decida desconectar de la red todos los sistemas para protegerse de un ataque, se perdería toda la capacidad de Mando y Control.

Esta perspectiva se traduce en que, a futuro, los proveedores de sistemas, subsistemas e incluso componentes de activos para las fuerzas armadas van a cobrar un mayor interés como objetivo de ciberataques por parte de una potencia enemiga, y cualquier ciberataque llevado a cabo con éxito puede impactar de forma directa en el campo de batalla, multidominio, de las fuerzas armadas. La ciberseguridad de la cadena de suministro es, y será, uno de los elemetos claves de la ciberdefensa

En definitiva, será necesario el desarrollo e implementación de nuevas normativas para la cadena de suministro del sector de la defensa en los próximos años.

Informes

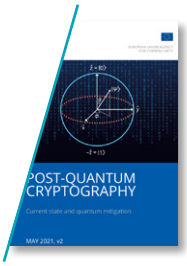
Executive Order on Improving the Nation's Cybersecurity (U.S White House)

National Cybersecurity Organization: Luxembourg (NATO CCD COE)

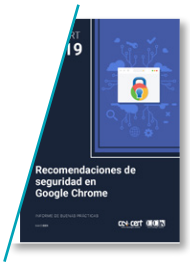
CTF events (ENISA)

Informe Annual 2020 hacktivismo y ciberyihadismo (CCN CERT)

Post-Quantum Cryptography: Current state and quantum mitigation (ENISA)

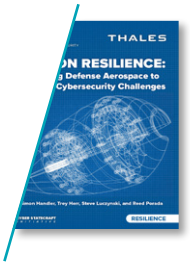


Recomendaciones de Seguridad en Google Chrome (CCN CERT)



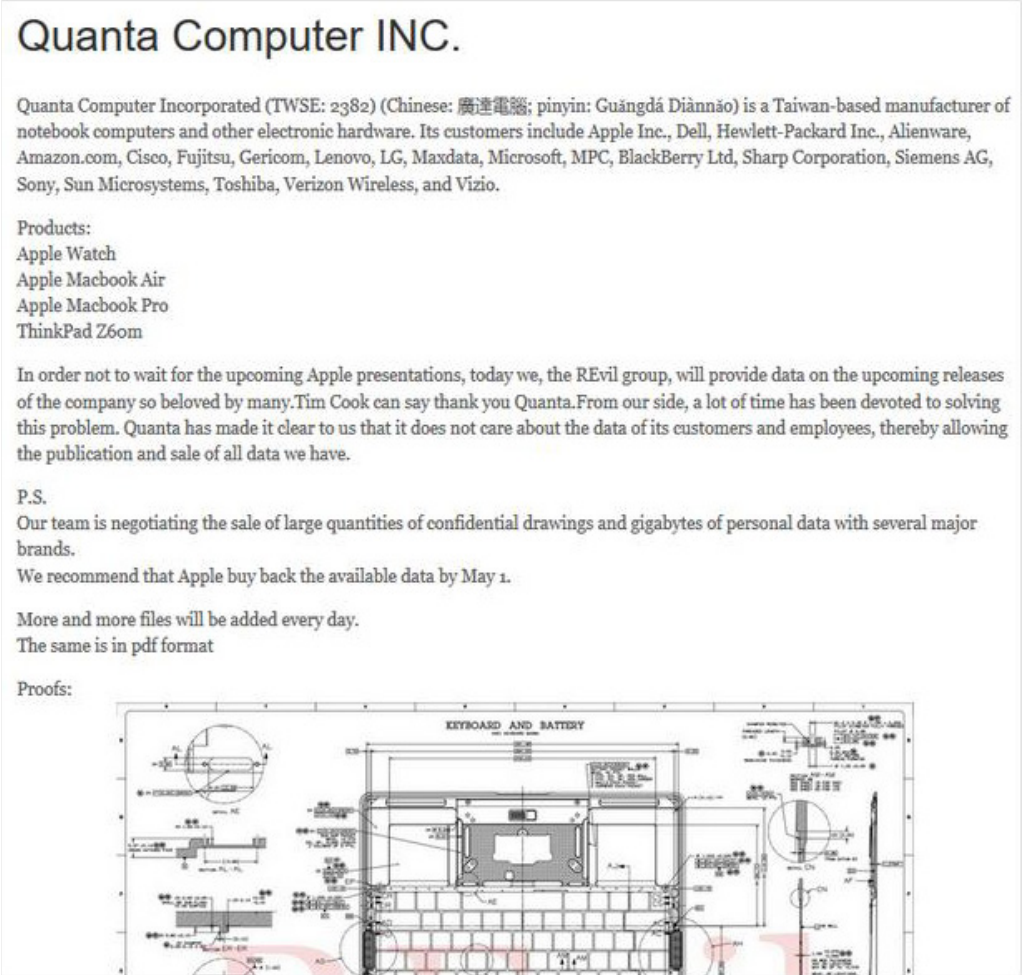
Cyber Considerations for Military Mobility (NATO CCD COE)

Adapting Defence Aerospace to Evolving Cybersecurity Challenges (Atlantic Council)



Análisis de actualidad:

Ciberataques abril 2021



Quanta Computer INC.

Quanta Computer Incorporated (TWSE: 2382) (Chinese: 廣達電腦; pinyin: Guǎngdá Diànnǎo) is a Taiwan-based manufacturer of notebook computers and other electronic hardware. Its customers include Apple Inc., Dell, Hewlett-Packard Inc., Alienware, Amazon.com, Cisco, Fujitsu, Gericom, Lenovo, LG, Maxdata, Microsoft, MPC, BlackBerry Ltd, Sharp Corporation, Siemens AG, Sony, Sun Microsystems, Toshiba, Verizon Wireless, and Vizio.

Products:
Apple Watch
Apple Macbook Air
Apple Macbook Pro
ThinkPad Z6om

In order not to wait for the upcoming Apple presentations, today we, the REvil group, will provide data on the upcoming releases of the company so beloved by many.Tim Cook can say thank you Quanta.From our side, a lot of time has been devoted to solving this problem. Quanta has made it clear to us that it does not care about the data of its customers and employees, thereby allowing the publication and sale of all data we have.

P.S.
Our team is negotiating the sale of large quantities of confidential drawings and gigabytes of personal data with several major brands.
We recommend that Apple buy back the available data by May 1.

More and more files will be added every day.
The same is in pdf format

Proofs:

Ilustración 1. Muestra de algunos blueprints de productos Apple sustraídos en el ataque de double ransom a Quanta Computer.

Cibercrimen

En el ámbito del cibercrimen, el ransomware sigue siendo el vector de ataque hegemónico. Así pues, durante las últimas semanas, se han notificado públicamente diversos casos de *double ransom* vinculados al grupo REvil (Sodinokibi) como Quanta Computer (afirmando en su blog que habían llegado a sustraer los planos de los últimos productos de Apple, pidiendo un rescate de 50M$) y con especial impacto en Francia con víctimas como Pierre Fabre (con un rescate inicial de 25M$) y Asteelflash (con un rescate inicial de 24 M$), o en territorio italiano con víctimas de Doppelpaymer en el ayuntamiento de Brescia, Rho y Caselle Torinese.

También en el plano local se han presenciado diversas víctimas como Phone House España (afectado por Babuk, donde los atacantes solicitaban un rescate inicial de 6M€ y que ha conllevado la publicación de la información de 13 millones de clientes), la Universidad de Castilla La Mancha (Ryuk), el ayuntamiento de Oviedo, el ayuntamiento de Castellón de la Plana y el ayuntamiento de Jijona.

Desde mediados de diciembre del pasado año, un grupo atacantes que algunos analistas han denominado UNC2546, ha estado explotando múltiples 0-days en el File Transfer Appliance (FTA) de Accellion, instalando una webshell llamada DEWMODE. Accellion FTA es un producto que lleva cerca de 20 años en el mercado, llegando ya al final de su vida útil. Si bien durante las primeras semanas no era clara la motivación de los atacantes, ya a finales de enero de 2021, varias compañías afectadas por este grupo comenzaron a recibir correos electrónicos de extorsión de actores que amenazaban con publicar datos sustraídos en la web "CL0P ^ _- LEAKS" en la deepweb.

Así pues, desde febrero de este año, se ha detectado un incremento significativo de víctimas en la web "CL0P ^ _- LEAKS" en países como EEUU, Singapur, Canadá y los Países Bajos. Otros actores, como FIN11, ya habían empleado esa misma web como una táctica de *double ransom* para presionar a sus víctimas para que paguen demandas de extorsión tras el despliegue del ransomware CLOP. Sin embargo, en incidentes recientes vinculados a CLOP, no se desplegó ransomware ni estaban presentes las otras características distintivas de este grupo.

BABUK

Phone House España 13 millions customers data has been stolen, including passports and other privacy information

PHONEHOUSE.ES - MORE THEN 100GB OF SENSITIVE DATA

Phone House

Entre las víctimas de este grupo de ransomware cuyo vector inicial de entrada está basado en la explotación de esta vulnerabilidad de Accellion, se encuentra uno de los bufetes de abogados más grandes del mundo, Jones Day, conocido por ser el despacho al que el expresidente Trump encomendó el pleito por el proceso electoral de noviembre de 2020. De este modo, la firma ha sido afectado por un ataque de *naming & shaming*, empleado para extorsionar a la víctima bajo amenaza de publicación de información confidencial, pudiéndose encontrar parte de la misma publicada en la web.

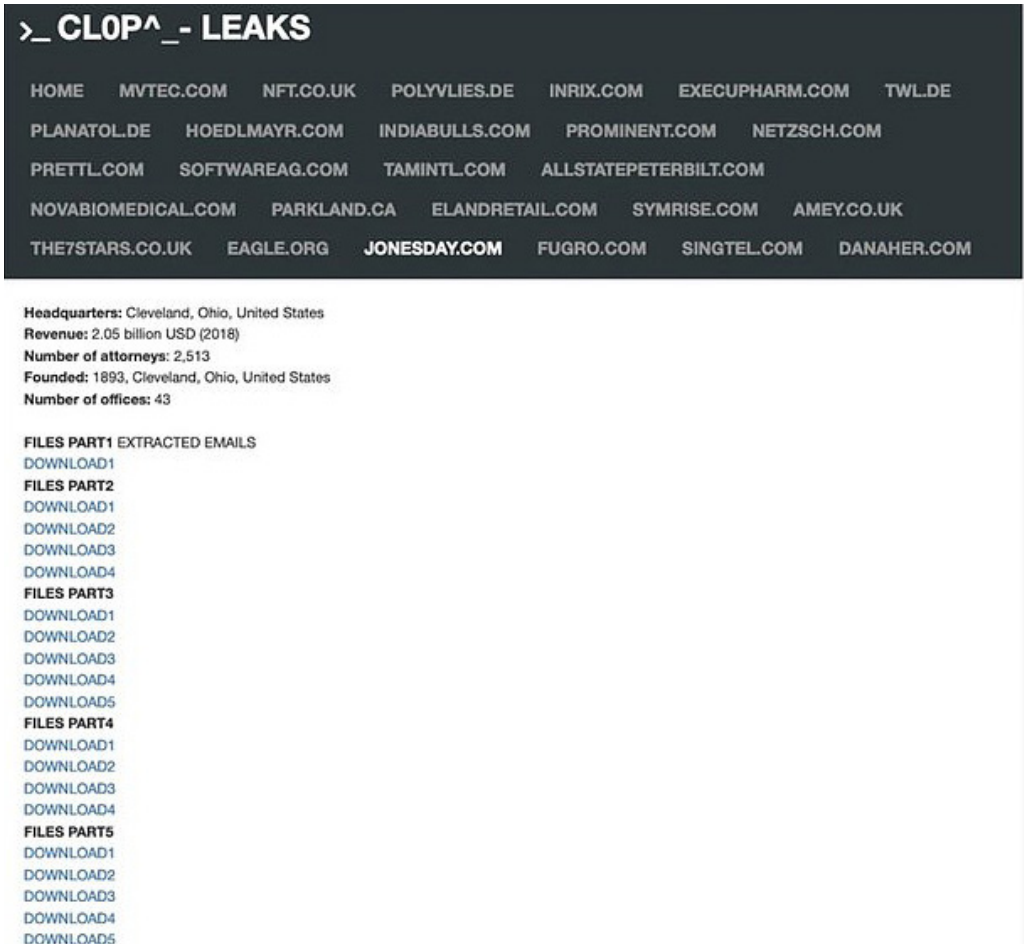


Ilustración 2. Web del grupo Clop en la que se han difundido los datos confidenciales de Jones Day

Durante el Q1 de 2021 hemos presenciado numerosas víctimas de este vector de ataque, desde el fabricante de aviones y compañía de aviación canadiense Bombardier, al proveedor de seguridad Qualys o al gigante de las telecomunicaciones Singtel.

Concretamente, durante los últimos 30 días, la lista de víctimas ha seguido creciendo, encontrando entre las mismas la University of California Berkeley (UC Berkeley), el proveedor sanitario estadounidense Trinity Health (más de 580.000 registros de sus pacientes se han visto expuestos) o el ayuntamiento de Toronto.

Finalmente, la última víctima relevante de un ataque de ransomware ha sido Colonial Pipeline. Este incidente es uno de los ataques de ransomware más disruptivos jamás reportados en territorio norteamericano y ha llamado la atención sobre el nivel de seguridad de la infraestructura energética de EEUU. Un cierre prolongado de la línea haría que los precios de combustible se dispararan antes de la temporada estival (con un alto consumo debido a los movimientos en carretera), lo que supondría un duro golpe para los consumidores y la economía estadounidense.

Colonial Pipeline, que está controlada por compañías como Koch Industries y Royal Dutch Shell (también afectada en el pasado por el ransomware CLOP) es responsable de transportar el 45% del suministro de combustible de la costa este (transporta 2,5 millones diarios de barriles de gas, diesel, combustible para aviones y otros productos refinados). Colonial Pipeline explota un sistema de oleoductos de 5.500 millas que transporta combustible de las refinerías en Houston (Texas) al puerto de Nueva York.

Ilustración 3. La ruta Colonial Pipeline a lo largo de la costa este de EEUU
Fuente: Colonial Pipeline

El ataque informático ha obligado a parar la operación de la infraestructura desde el pasado viernes 7 de mayo. En el momento de redacción del presente documento, no hay certeza de cuándo volverá a recuperarse la operativa habitual. Este ataque se produce poco antes de que el presidente de Estados Unidos, Joe Biden, firme, en los próximos días, una orden ejecutiva para incrementar la ciberseguridad en infraestructuras críticas para la economía del país.

Ilustración 4. Nota de prensa publicada por Colonial Pipelines relativa al incidente de ransomware

Ciberespionaje

El FBI, el Departamento de Seguridad Nacional (DHS) y el CISA estadounidense advirtieron en una nota publicada el 26 de abril sobre los continuos ataques coordinados por el Servicio de Inteligencia Exterior de Rusia (SVR) (también conocido como APT29) contra organizaciones estadounidenses y extranjeras. Esta nota complementa la publicada el15 de abril, compartiendo información sobre vulnerabilidades explotadas por el grupo APT29 con vinculación estatal rusa (también conocido como Dukes, CozyBear e Yttrium).

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Alerts and Tips Resources Industrial Control Systems

National Cyber Awareness System > Current Activity > FBI-DHS-CISA Joint Advisory on Russian Foreign Intelligence Service Cy

FBI-DHS-CISA Joint Advisory on Russian Foreign Intelligence Service Cyber Operations

Original release date: April 26, 2021

Print Tweet Send Share

The Federal Bureau of Investigation (FBI), Department of Homeland Security, and CISA have released a Joint Cybersecurity Advisory (CSA) addressing Russian Foreign Intelligence Service (SVR) cyber actors—also known as Advanced Persistent Threat 29 (APT 29), the Dukes, CozyBear, and Yttrium—continued targeting of U.S and foreign entities. The SVR activity—which includes the recent SolarWinds Orion supply chain compromise—primarily targets government networks, think tank and policy analysis organizations, and information technology companies and seeks to gather intelligence information.

This CSA complements the CISA, FBI, and National Security Agency (NSA) Joint CSA: Russian SVR Targets U.S. and Allied Networks and provides tactics, tools, techniques, and capabilities to help organizations conduct investigations and secure their networks.

CISA encourages users and administrators to review Joint CSA AA21-116A: Russian Foreign Intelligence Service (SVR) Cyber Operations: Trends and Best Practices for Network Defenders and implement the recommended mitigations. For additional information on SVR-related activity, review the following resources:

- CISA-FBI-NSA Joint Cybersecurity Advisory: Russian SVR Targets U.S. and Allied Networks
- CISA Current Activity: NSA-CISA-FBI Joint Advisory on Russian SVR Targeting U.S. and Allied Networks
- White House Statement: Imposing Costs for Harmful Foreign Activities by the Russian Government

Ilustración 5. Comunicado conjunto publicado por la administración de EEUU relativo a los recientes ataques sufridos.

La actividad de SVR, que incluye ataques a la cadena de suministro como el sufrido a través de la solución Orion de SolarWinds, está dirigida principalmente a redes gubernamentales, organismos políticos, grupos de expertos y lobbies, así como empresas de tecnología, buscando recopilar información de inteligencia. APT29, SE afirman en el comunicado, continuará con sus labores de ciberespionaje, utilizando una gama de técnicas de explotación inicial que varían en sofisticación, junto con técnicas de intrusión de perfil bajo. La nota conjunta proporciona información adicional sobre APT29 y sus TTPs, destacando el *password spraying*, la explotación de *0 day*, el *malware* WELLMESS, así como ataques a través de la cadena de suministro (como el caso de SolarWinds).

El mismo día de publicación del comunicado, la Casa Blanca atribuyó formalmente el ataque a la cadena de suministro de SolarWinds a APT29. Además, el Joe Biden emitió una orden ejecutiva para incautar bienes con respecto a actividades dañinas del gobierno de la Federación de Rusia.

Administration Priorities COVID-19 Briefi

BRIEFING ROOM

Executive Order on Blocking Property with Respect to Specified Harmful Foreign Activities of the Government of the Russian Federation

APRIL 15, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq.*) (IEEPA), the National Emergencies Act (50 U.S.C. 1601 *et seq.*) (NEA), section 212(f) of the Immigration and Nationality Act of 1952 (8 U.S.C. 1182(f)), and section 301 of title 3, United States Code,

I, JOSEPH R. BIDEN JR., President of the United States of America, find that specified harmful foreign activities of the Government of the Russian Federation — in particular, efforts to undermine the conduct of free and fair democratic elections and democratic institutions in the United States and its allies and partners; to engage in and facilitate malicious cyber-enabled

Ilustración 6. Orden ejecutiva sobre el bloqueo de bienes con respecto a actividades extranjeras agresivas específicas del gobierno de la Federación de Rusia.

El Departamento del Tesoro también emitió sanciones contra varias empresas de tecnología rusas (ERA Technopolis, Pasit, SVA, Neobit, AST y Positive Technologies) por ayudar presuntamente al SVR, al Servicio Federal de Seguridad de Rusia (FSB) y al lanzamiento de la Dirección Principal de Inteligencia de Rusia (GRU). ciberataques contra entidades estadounidenses.

U.S. DEPARTMENT OF THE TREASURY

ABOUT TREASURY POLICY ISSUES DATA SERVICES NEWS

HOME > NEWS > PRESS RELEASES

NEWS

Press Releases

Statements & Remarks

Readouts

Testimonies

Featured Stories

Press Contacts

PRESS RELEASES

Treasury Sanctions Russia with Sweeping New Sanctions Authority

388

April 15, 2021

WASHINGTON — Today, the U.S. Department of the Treasury took multiple sanctions actions under a new Executive Order (E.O.) targeting aggressive and harmful activities by the Government of the Russian Federation. Treasury's actions include the implementation of new prohibitions on certain dealings in Russian sovereign debt, as well as targeted sanctions on technology companies that support the Russian Intelligence Services' efforts to carry out malicious cyber activities against the United States.

Ilustración 5. Orden ejecutiva sobre el bloqueo de bienes con respecto a actividades extranjeras agresivas específicas del gobierno de la Federación de Rusia.

Ilustración 7. El Departamento del Tesoro norteamericano ha emitido un conjunto sanciones contra varias empresas de tecnología rusas por su vinculación con las agencias de inteligencia rusas.

El 20 de abril, la BBC se hacía eco del comunicado emitido por el MI5, en el que se informaba de que al menos 10.000 ciudadanos británicos habían sido contactados por perfiles falsos vinculados actores estatales extranjeros, en la red social profesional LinkedIn durante los últimos cinco años. Ken McCallum, actual responsable del MI5, advirtió de que naciones hostiles están utilizando perfiles maliciosos a escala industrial con el objetivo de engañar a diversos sujetos a compartir información confidencial o secreta.

Entre las víctimas, se encuentran miembros de la práctica totalidad de departamentos gubernamentales, así como industrias clave en UK, a quienes se les ofrecen oportunidades de negocios y viajes que podrían llevar a intentos de reclutamiento para recopilar información. El MI5 ha lanzado una campaña para educar a los trabajadores del gobierno sobre este tipo de amenazas, llamada "Think Before You Link", advirtiendo de que los espías extranjeros están tomando como objetivo a sujetos que potencialmente pueden tener acceso a información confidencial.

Ilustración 8. *"Think Before You Link"*, la campaña de sensibilización lanzada por el ***"Centre for the Protection of National Infrastructure"*** del MI5 incluye guías, carteles y un video

La res social LinkedIn, por su parte, ha aplaudido la iniciativa en su web.

Creating trusted connections

Published on Apr 19, 2021 | Categories: **Company News**

LinkedIn Corporate Communications

We welcome the online safety efforts of the Centre for the Protection of National Infrastructure and its work to expand their **Think Before You Link** campaign in the United Kingdom. Teams at LinkedIn **work to keep LinkedIn a safe place** where real people can connect with professionals they know and trust. We actively seek out signs of state sponsored activity on the platform and quickly take action against bad actors in order to protect our members. Our Threat Intelligence team removes fake accounts using information we uncover and intelligence from a variety of sources, including government agencies. Our teams utilize multiple automated techniques, coupled with human reviews and member reporting to maintain LinkedIn as a safe and trusted platform. And we enforce our policies, which are very clear: fraudulent activity with an intent to mislead or lie to our members is a violation of our terms of service.

For additional information about our work to keep members safe:

https://about.linkedin.com/transparency

https://www.linkedin.com/pulse/look-inside-how-my-team-helps-keep-members-safe-paul-rockwell/

Hacktivismo, guerra electrónica y operaciones de información

A comienzos del mes de abril, un portavoz de la Comisión Europea confirmó en prensa que varias organizaciones de la Unión Europea estaban experimentando un incidente de seguridad en su infraestructura de TI durante la última semana de marzo, y agregó que hasta el momento no se había detectado ninguna violación de información importante.

La Comisión no proporcionó más detalles sobre el ataque, ya que la investigación aún se encuentra en su etapa inicial. Algunas fuentes confirman que los ataques fueron más intensos que el promedio y lo suficientemente graves como para justificar una alerta emitida a todos los altos funcionarios de la CE. Otra fuente anónima explicaba que recientemente se había advertido al personal de la comisión sobre posibles intentos de spearphishing.

Estas acciones se suman al incidente acontecido en la Agencia Europea del Medicamente a finales de diciembre de 2020 así como al DDoS sufrido recientemente por el parlamento belga así como otras instituciones públicas paneuropeas.

También a comienzos de abril, Facebook anunció que había eliminado 14 redes en 11 países por usar cuentas falsas para amplificar campañas de desinformación.

Una de estas campañas fue analizada en profundidad por Facebook, proporcionando un análisis en profundidad sobre una granja de trolls operada en Albania vinculada al grupo de oposición iraní exiliado Mojahedin-e Khalq. La compañía dijo que eliminó 128 cuentas, 41 páginas, 21 grupos y 146 cuentas de Instagram vinculadas a la operación, que estaba dirigida principalmente a una audiencia iraní. Facebook confirmó que la operación comenzó en 2016 y alcanzó su punto máximo en 2017, reduciéndose drásticamente en 2018 y 2019, identificando un repunte en la segunda mitad de 2020 que dio lugar a la investigación. Facebook identificó las señales de una una granja tradicional de trolls: un grupo de varios cientos de cuentas que se ejecutan desde una sola ubicación con una infraestructura técnica compartida. Las cuentas incluso operaban en un horario, publicando siete días a la semana, generalmente entre las 6:00 y las 19:00 (hora local), con un descanso alrededor del mediodía.

Ilustración 9. Organización de los Muyahidines del Pueblo de Irán (también conocidos como PMOI, MEK o MKO) o Moyahedin-e Jalq en persa.

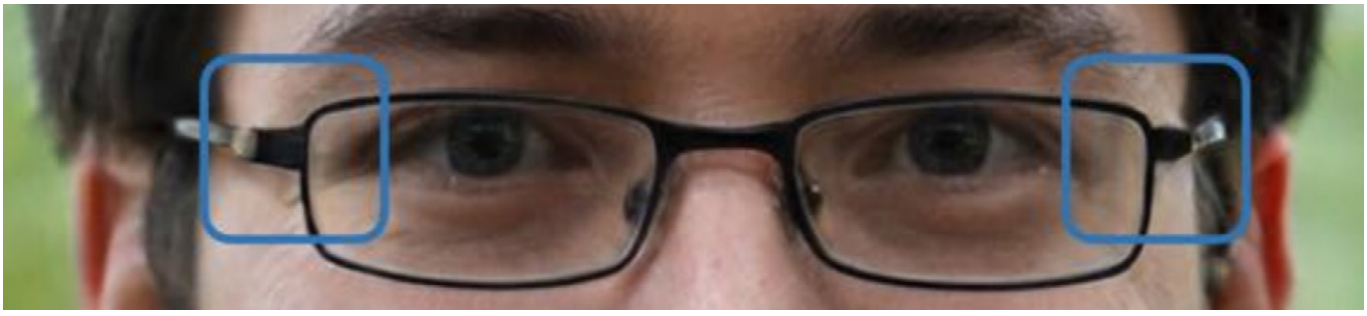


Ilustración 10. Detalle de una foto de perfil generada por inteligencia artificial, mostrando la asimetría de la montura de las gafas.

Así pues, la red social eliminó 1.167 cuentas de Facebook, 290 cuentas de Instagram, 255 páginas y 34 grupos en el mes de marzo por sus conexiones con estas campañas de "comportamiento coordinado falso", que se dirigieron a una variedad de países, incluidos Israel, México, Benin, y Georgia.

Facebook también destacó en su informe que tres grupos contra los que tomó medidas estaban usando fotos de perfil probablemente generadas por tecnologías de aprendizaje automático. Había eliminado a otros cuatro grupos utilizando técnicas similares desde septiembre de 2019. La compañía afirmó que a menudo puede reconocer fácilmente estas fotos a través de errores reveladores, como fondos o rasgos faciales distorsionados de manera artificial; una imagen que la compañía incluyó mostraba gafas que tenían marcos asimétricos con diferentes patas, bisagras y conexiones en cada lado. Aunque estas imágenes pueden detectarse automáticamente, ejemplifican cómo los actores están adoptando nuevos TTPs para tratar de mejorar sus campañas.

Finalmente, el 28 de abril, FireEye publicaba un nuevo informe sobre la actividad de Ghostwriter. Desde el informe

inicial de FireEye sobre Ghostwriter, la actividad se ha expandido con nuevas narrativas, y los atacantes han comenzado a aprovechar las cuentas de funcionarios polacos comprometidas de Twitter, Facebook e Instagram para difundir contenido destinado a crear inestabilidad política en el país. Esta actividad, inicialmente identificada y detallada en julio de 2020, ha estado operativa durante años y parece alineada con algunos ejes de política exterior e intereses rusos, estando actualmente dirigida a audiencias en Lituania, Letonia y Polonia con temática relativa a la OTAN.

Entre octubre de 2020 y enero de 2021, FireEye identificó cinco nuevas operaciones de Ghostwriter realizadas tanto en polaco como en inglés, pero que no parecían estar relacionadas con la actividad anterior de este actor, basada en webs comprometidas, correos electrónicos spoofeados, perfiles falsos y contenido con narrativa de la OTAN.

Sin embargo, en octubre de 2020 se identificó una campaña con los TTPs habituales de Ghostwriter, con un mensaje que sugería que la OTAN estaba preparando sus fuerzas armadas para una guerra con Rusia, y que la batalla tendría lugar en Polonia, Letonia y Lituania. La narrativa se promovió a través de un artículo falso publicado en varias webs, pero también se utilizaron cuentas comprometidas de las redes sociales de funcionarios polacos para difundir la historia.

Adicionalmente, FireEye identifica actividad de un actor relacionado a campañas de ciberespionaje con vinculación estatal denominado UNC1151 tras algunas de las actividades de influencia de Ghostwriter. UNC1151 habría ejecutado operaciones destinadas a la recolección de credenciales y la entrega de malware a través de ataques de *spearphishing*. Los ataques de robo de credenciales tenían como objetivo organizaciones gubernamentales, militares y de medios de comunicación en Polonia, Ucrania y los países bálticos, pero también se observó que el grupo intentaba comprometer las cuentas de otras entidades de interés, incluidos periodistas y activistas.

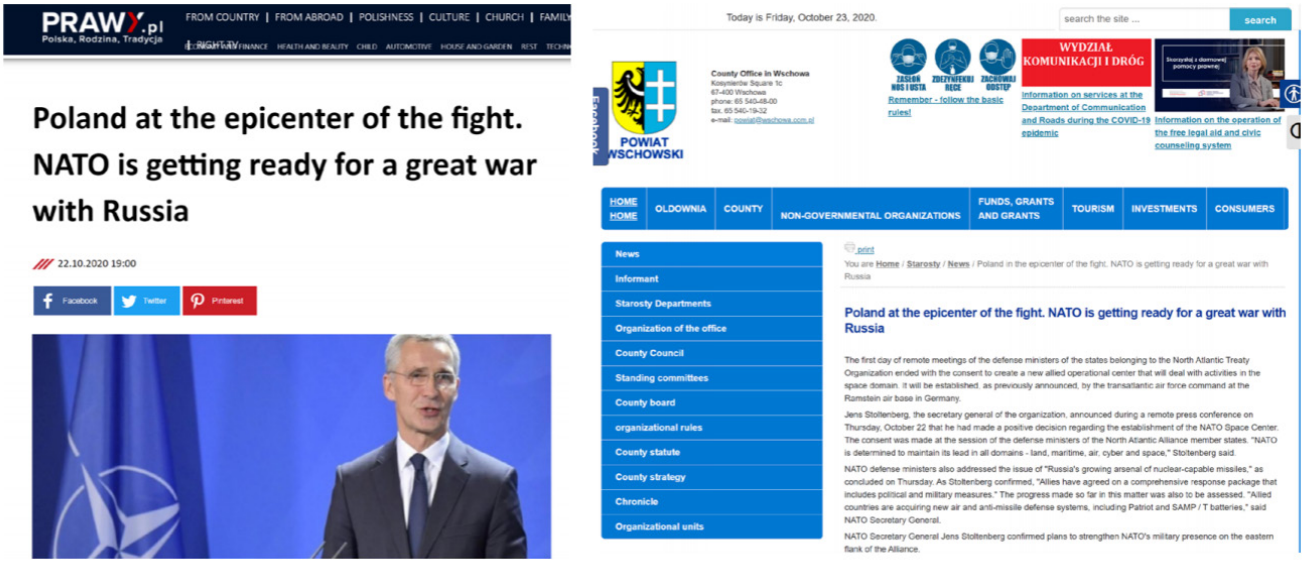


Ilustración 11. Artículo falso (fakenew) publicado en la web de noticias Prawy.pl (izquierda) y en la web de la administración del condado de Wschowie en Polonia (derecha). Desde entonces, ambos sitios han eliminado el artículo. Fuente: FireEye

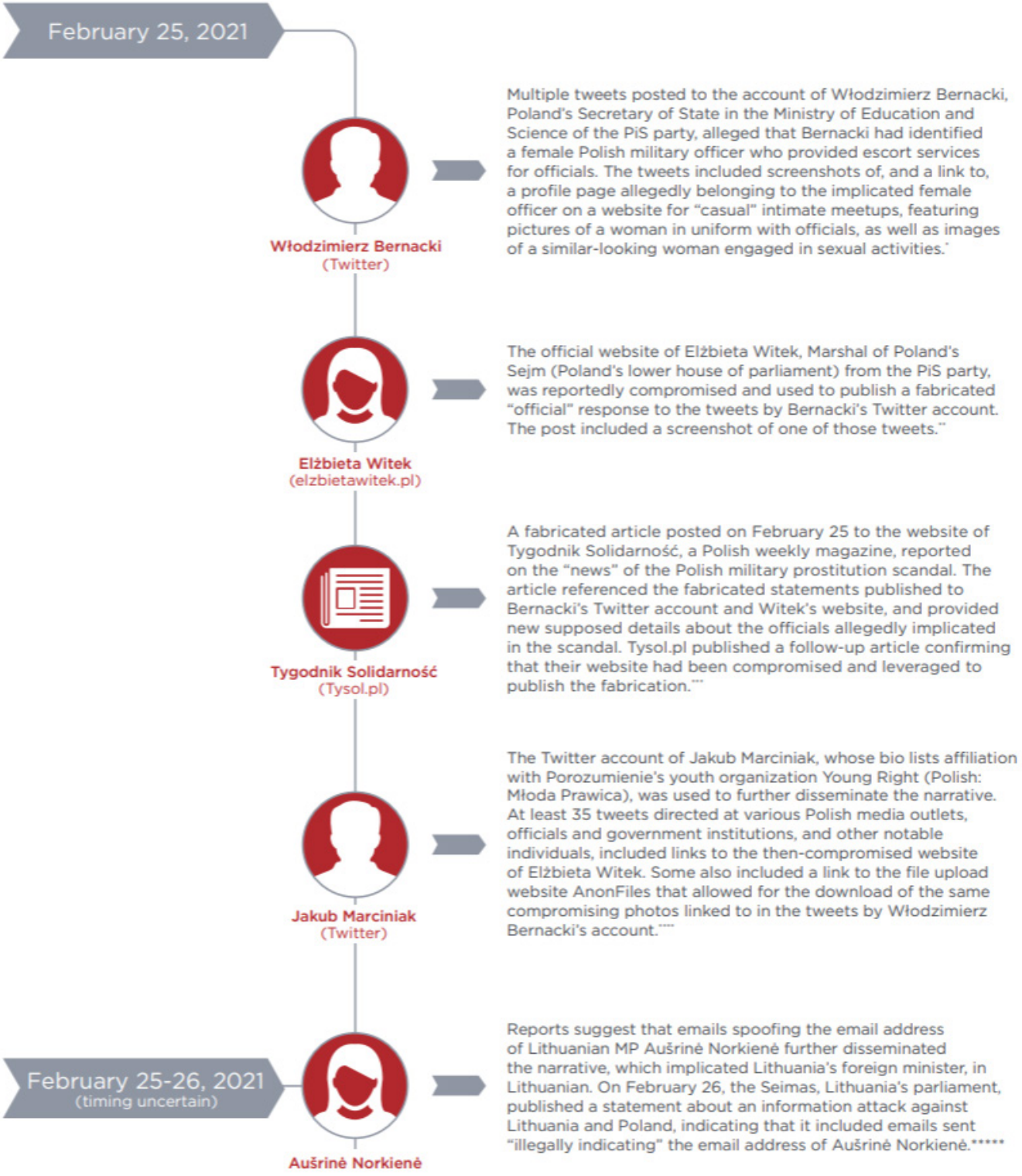


Ilustración 12. La fase de difusión de la operación utilizó correos electrónicos potencialmente falsos, así como varias cuentas de redes sociales y sitios web que sospechamos que estaban comprometidos para promover declaraciones oficiales falsas y un artículo inventado. Fuente: FireEye

CISO Remoto, ¿una profesión con futuro?

AUTOR: Fernando de la Mata, Chief Information Security Officer BBVA USA

Cada vez más y, sobre todo, desde la proliferación del teletrabajo derivada de la situación mundial de pandemia, se está empezando (quizá no a imponer, pero sí a extenderse de manera amplia) la figura del Virtual CISO o del remote CISO.

Este artículo pretende, desde la experiencia personal, aclarar algunos conceptos centrados en la creencia extendida de que determinadas funciones de ciberseguridad se deben ejecutar de manera presencial y la manera de cómo abordar las funciones estándar de un CISO desde la "tranquilidad" del uso de cualquiera de las herramientas de videoconferencia actuales y solventando la distancia interpersonal con otras técnicas complementarias, con un resultado parecido

Que es un CISO remoto

Puede parecer un tanto simplista el tratar de definir un *job profile* como éste basado sólo en un concepto básico, la deslocalización, pero básicamente es en lo que consiste la diferencia de este rol con los CISOs "convencionales". Lo relevante de la proliferación de esta figura es que no sólo viene derivado por las consecuencias del trabajo remoto fomentado por la pandemia, sino que hay una fuerte corriente de compañías deslocalizadas, cuyo *footprint* se extiende por diferentes geografías, y que tienden a tener pequeños equipos en cada uno de los países en los que tiene presencia. Además, estos modelos de negocio cada vez apalancan más su capacidad de IT en la nube, por lo que el concepto tradicional de "donde tengas tu *datacenter* tendrás a tu equipo de IT y seguridad" ya no aplica para estas empresas.

Adicionalmente, cabe reseñar que existe otro modelo, al que podríamos denominar *Ciso-as-a-Service*, en el que generalmente una compañía de servicios de seguridad, se encarga de realizar las funciones de CISO, sin formar parte de la plantilla de la compañía, y son otro servicio externalizado

Este artículo pretende, desde la experiencia personal, aclarar algunos conceptos centrados en la creencia extendida de que determinadas funciones de ciberseguridad se deben ejecutar de manera presencial y la manera de cómo abordar las funciones estándar de un CISO

el concepto tradicional de “donde tengas tu *datacenter* tendrás a tu equipo de IT y seguridad” ya no aplica.

más. Esta propuesta es algo diferente, ya que generalmente, las adoptan compañías de tamaño y presupuesto destinado a ciberseguridad reducido, bien porque su modelo de negocio y gestión de riesgos no requiere tener equipo interno y con la dotación necesaria, o bien por que las circunstancias les ha hecho optar por subcontratar a un tercero.

Como hacer el onboarding

Este artículo se centrará en las técnicas y capacidades que un CISO remoto debe desarrollar dejando para un análisis posterior el segundo modelo referido.

Uno de los momentos más delicados cuando se toma el liderazgo de un equipo, sin duda es el momento de conocerlo, tomando el control de lo que estás haciendo y, a la vez, identificar qué actividades no están priorizadas o no forman parte del *core*. En este punto, se vuelve crucial el equilibrio entre las entrevistas 1:1 con los reportes directos, con los diferentes subequipos y con sesiones plenarias tipo *Town Hall*. Al hacer todo el proceso por videoconferencia se debe en cuenta dos puntos principales: la falta de interacción física y la disminución del lenguaje no verbal en las comunicaciones. Ante esta falta de interacción directa, el esfuerzo a dedicar a la inteligencia emocional debe ser muy superior para poder obtener la misma información que obtendrías en reuniones presenciales. Se debe leer y escuchar aún más, para tratar de extraer toda aquella información que sea básica para la toma de control de la situación.

El esfuerzo a dedicar a la inteligencia emocional debe ser muy superior

Otro punto que cambia sensiblemente es el proceso de toma de decisiones, que debe enfocarse hacia el modelo colaborativo. El equipo tiene mucho que decir y seguro que dispone de mucha más información que no es sencillo que pueda transmitir sin esas pequeñas reuniones de café, por lo tanto, es más sensato confiar en estos primeros momentos en su criterio y luego ir haciendo pequeños ajustes o redefiniciones de estrategia y/o de proyectos más que hacer una aproximación de cambios traumáticos o de rotación severa del equipo en los primeros momentos.

El proceso de toma de decisiones, que debe enfocarse hacia el modelo colaborativo

Governance y reporting

Este es otro de los puntos en los que se debe alterar con respecto al modelo presencial. En primer lugar, la relación con los *stakeholders* cambia y hay que suplir esa generación de "confianza" personal, por un aumento de la capacidad de medición y con datos que soporten que hemos tomado el control de la situación. Incluso es recomendable sobre-medir la actividad del equipo, reportando esta telemetría de manera adicional a los KPIs y KRIs que la organización ya tenga establecidos. No hay que dedicar un tiempo excesivo a la implantación KRIs o del framework seleccionado de seguridad. Las necesidades de transformación deben dejarse para una fase posterior, lo primero que hay que demostrar es que se tiene todo bajo control (o al menos lo más crítico y lo que proporciona cierta solidez al modelo).

Gestión de incidentes

Y precisamente uno de los temas centrales que hay que priorizar bajo este modelo es el de gestión de incidentes. Al no tener la capacidad de concentrar al equipo en la misma sala y poder coordinar el incidente de forma convencional, es necesario complementarlo con dos técnicas muy útiles.

Primero, es deseable realizar varias simulaciones, de manera que rápidamente se identifiquen los roles que cada uno debe tener (detectando quién tiene los conocimientos técnicos de la infraestructura y quién gobierna cada una de las funciones claves de la organización, como comunicación externa, legal, relación con reguladores, seguridad física, etc,). Adicionalmente, se podrá aprovechar para que vean cómo se actúa y cómo es el proceso de toma de decisiones. Por

lo tanto, estos ejercicios tienen una función doble, porque es un foro adicional a los comités y reuniones 1:1 y permite pulsar las capacidades y también las necesidades que puede tener el equipo de cara a gestionar estos eventos. Y sin duda, es lo que más rodado debe estar, y cuanto antes se engrase esa maquinaria, mejor.

En segundo lugar, suele ser interesante que al principio se aumente el nivel de intensidad en la gestión de los eventos de menor importancia. La actividad recurrente del equipo puede tener carencia de playbooks formales, tener ciertos automatismos desfasados, en definitiva, permite pulsar el estado real del equipo de gestión de incidentes. Cierto es que hay que gestionar la molestia que eso generará en tu equipo, porque lo interpretan con una cierta desconfianza hacia su labor, ya que se está examinando tareas rutinarias, pero eso es gestionable relajando esta intensidad al cabo de 2- 3 semanas de escrutinio. Pero permite extraer información muy valiosa de cara al plan estratégico y operativo que sin duda se tendrá que presentar en un plazo establecido (normalmente entre 30 y 90 días).

Es deseable realizar varias simulaciones, de manera que rápidamente se identifiquen los roles que cada uno debe tener

Qué cosas no pueden sustituir al momento presencial

Por último, aunque ya se han señalado un gran número de actividades que un CISO que trabaje de manera remota puede realizar de manera exitosa, no hay que ocultar que esta modalidad entraña algunos riesgos, que evidentemente, no generan el mismo resultado que con la modalidad presencial.

En primer lugar, todos los intangibles en las relaciones personales, tan importantes además cuando se realiza un trabajo como el de CISO que puede pasar por situaciones de mucha tensión o se ve forzado a tomar decisiones en minutos, se vuelven más complicados, por la falta de *input* y *feedback* directos.

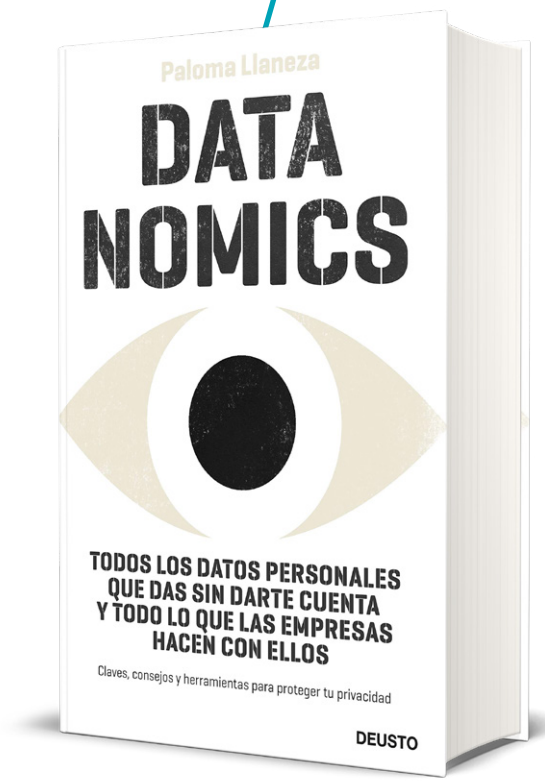
En segundo lugar, las reuniones de equipo, en aquellas donde la comunicación es clave, cuando se transmite la estrategia y los objetivos, y cuando más se puede hacer uso de las técnicas de liderazgo, se ven más limitadas con esta modalidad. Por eso se deben compensar con modelos de relación que refuercen el contacto diario y la interacción más frecuente, no solo con los reportes directos, sino permeando sobre la mayor parte del equipo que sea posible.

En conclusión, lo que se pretende ilustrar con este artículo es que el modelo de CISO remoto es perfectamente aplicable, y que, salvo por determinados ajustes o priorizaciones que son necesarios hacer para compensar la no presencialidad con otros recursos, es muy probable que cada vez más compañías adopten el modelo junto con el incremento de la propia descentralización de las empresas.

En conclusión, lo que se pretende ilustrar con este artículo es que el modelo de CISO remoto es perfectamente aplicable

Libro recomendado:

Data nomics



Autor: : Paloma Llaneza

Editorial: Ediciones Deusto

Año: 2019

Páginas: 303

Precio: ---

COMPRAR

Sinopsis

Casandra, sacerdotisa de Apolo, llegó a un pacto con el dios de la verdad para que le fuera concedido el don de la profecía. Más adelante, al verse rechazado por Casandra, Apolo la maldijo y la condenó a que nadie creyera sus pronósticos.

La autora utiliza el mito griego en uno de sus capítulos para advertir de que los avisos que se dan al público acerca de la cesión de datos no son meras llamadas alarmistas. Antes al contrario, se trata de advertencias sobre los riesgos ciertos que conlleva para la privacidad el uso de determinadas aplicaciones y la cesión de datos que, por la fuerza de la costumbre, se perciben como irrelevantes, por mucho que el usuario facilite más información sobre su vida de la probablemente es consciente que cede.

Cualquier actividad de la vida cotidiana que acometamos tiende a quedar plasmada en redes sociales. Parece pensarse que la utilización de las redes sociales y demás aplicaciones comunes solo conlleva que el usuario comparta parte de su vida con el resto del público que accede a la misma, la parte de su vida que de manera soberana y consciente decide mostrar. Sin embargo, la utilización de dichas redes o aplicaciones supone la revelación, entre otras cosas, de nuestras conductas diarias explícitas y también de muchos datos que no son aparentemente objeto de conocimiento por terceros.

Y ahí es, precisamente, donde la autora pone el foco: las grandes corporaciones digitales (Google o Facebook, por ejemplo) almacenan y obtienen continuamente una canti-

dad de detalles y datos que posibilitan un cierto ejercicio de poder real del que no se tiene conciencia. Estas entidades acaban conociendo casi en su totalidad qué hacen sus usuarios, qué quieren sus usuarios, adónde van y dónde están en cada momento.

¿Suena exagerado? ¿Se ceden, en realidad, datos suficientes como para posibilitar tanto conocimiento y, por tanto, control? DATA NOMICS es precisamente un aviso a navegantes sobre los peligros que conlleva el facilitar (vía cesión) nuestros datos en las aplicaciones que usamos durante el día a día. La autora Paloma Llaneza dedica parte de sus esfuerzos como abogada y consultora de seguridad a los aspectos legales y regulatorios de internet, y centra especialmente esta obra en evidenciar algunas de las prácticas que consienten los usuarios cuando hacen click en el botón de "acepto" de las aplicaciones más comunes.

Uno de los supuestos más llamativos que comparte la autora, que por sí solo debiera provocar cierto nivel de preocupación, es el rastreo continuo que hace Google en las ventas físicas a través de las tarjetas bancarias que utilizan los usuarios. Tras realizar una búsqueda de un producto en internet o cliquear un anuncio de un producto, el usuario puede decidir comprarlo días después en una tienda física. Google remite esa información (tanto el click en el anuncio como la compra hecha en la tienda física con la tarjeta, con todos los datos y metadatos asociados, huellas temporales y demás) a los anunciantes, de manera que éstos conozcan el porcentaje de compradores que vieron su anuncio, lo cliquearon e hicieron una compra.

Otra cuestión, menos directamente aprehensible, es la manera en que las aplicaciones son desarrolladas, buscando (y obteniendo, a la vista está) generar una cierta adicción en los usuarios, que acaban estando permanentemente conectados y haciendo uso de tales herramientas.

Es cierto, y así lo contempla el libro, que la Unión Europea ya ha intentado poner algo de coto al uso y tratamiento de datos personales mediante la publicación del Reglamento Europeo 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos. Y también es cierto que tras el escándalo de "Cambridge Analytica" (uno de ellos) varias entidades gubernamentales intentaron mostrar cierta voluntad de contención frente a Facebook y su CEO, Mark Zuckerberg, por la filtración de datos de millones de usuarios depara su utilización en una campaña electoral.

Sin embargo, ni los intentos gubernamentales ni los del propio mercado servirán por sí solos si los usuarios no paran un momento a pensar qué datos ceden y qué uso van a tener tales datos por parte de sus receptores. Este libro es precisamente una herramienta útil para conocer qué se hace con nuestros datos y qué cosas está en manos del público hacer para proteger la privacidad en los términos que se deseen.

Probablemente la mayor virtud de esta obra sea, además de advertir de los riesgos con datos y conocimiento de las prácticas de las grandes corporaciones digitales, la de huir de generalidades, tecnicismos o conceptos abstractos, apostando por las evidencias y su aplicación a casos muy concretos. Paloma Llaneza ha sido capaz de elaborar un libro muy práctico, sin que por ello haya renunciado a una exposición detallada de las cuestiones de mayor calado.

AUTORA: Julia Rubiales,
abogada asociada, MAIO LEGAL

Eventos

FECHA	LUGAR	ORGANIZADOR	TÍTULO
11-12 Mayo	Online	NCSC	CYBERUK 2021
11-12 Mayo	Online	Proidea	Oh My Hack
13 Mayo	Online	8.8	8.8 Gobierno
12-13 Mayo	Online	Tactical Edge	Tactical Edge 2021
17 de mayo	online	RSA	RSA Conference USA 2021
19-21 Mayo	Online	EuroForum	European Data Protection Days (EDPD) 2021
22- 23 Mayo	Online	Zurich	7th International Conference on Artificial Intelligence (ARIN 2021)
25-26 Mayo	Online	Seguritecnia	IV Jornada de Seguridad en el Comercio, la Distribución y la Logística
25- 28 Mayo	Online	CCDCOE	CyCon
27 Mayo	Online	ISMS Forum	X Foro de la Ciberseguridad
2-3 Junio	Semipresencial	ASLAN	Congreso & EXPO ASLAN 2021

THIBER
The cybersecurity think tank

Copyright y derechos:

THIBER, the Cyber Security Think Tank

Todos los derechos de esta Obra están reservados a THIBER, the Cyber Security Think Tank.

El titular reconoce el derecho a utilizar la Obra en el ámbito de la propia actividad profesional con las siguientes condiciones:

a. Que se reconozca la propiedad de la Obra indicando expresamente el titular del Copyright.

b. No se creen obras derivadas por alteración, trasformación y/o desarrollo de esta Obra.

El titular del Copyright no garantiza que la Obra esté ausente de errores. En los límites de lo posible se procederá a corregir en las ediciones sucesivas los errores señalados. Eventuales denominaciones de productos y/o empresas y/o marcas y/o signos distintivos citados en la Obra son de propiedad exclusiva de los titulares correspondientes.

Informe editado en Madrid.

Más información:

THIBER, The Cyber Security Think Tank.

Con la colaboracion de:

SysAdmin OK