Informe de Predicciones de Seguridad Cibernética 2019 de Forcepoint

Introducción 03

1: ¿El ocaso de la IA? 04

2: Caos a escala en el Internet de las cosas industrial 07

3: Un reflejo falso 09

4: Enfrentamiento en los tribunales 12

5: Trayectoria de colisión hacia la Guerra Fría cibernética 15

6: Dirigidos hacia el borde 17

7: Las culturas de seguridad cibernética que no se adapten, fallarán 19

Conclusión 22

Citas 23

Introducción

La innovación prospera cuando las personas pueden colaborar con confianza, sacando provecho de la información de manera creativa y libre mediante la tecnología.

El traslado de ida y vuelta al trabajo puede parecer algo banal para la mayoría de las personas pero, en verdad, ofrece un vistazo a la relación entre la confianza y la innovación. Una persona puede confiar en una bicicleta, un automóvil o un tren como medio de transporte para ir al trabajo. Las aplicaciones móviles les ayudan a evitar el tránsito, hacer un seguimiento de los reportes climáticos, buscar dónde comprar café y actualizar transacciones de venta. El acceso al CRM corporativo les permite enviar notas rápidas a sus jefes y compañeros de trabajo antes de la primera reunión de ventas del día.

Todo lo que hace una persona durante el breve viaje a la oficina se basa en la confianza: confían en que el tren llegue a la hora programada, que el barista no confunda su pedido con el de otra persona. Confían en que su empleador controle el acceso a su aplicación SaaS, para garantizar que un registro de ventas confidencial no se cargue a un sitio web de phishing no autorizado. Y, dado que la confianza se establece entre las partes, los empleadores confían en que los empleados protejan sus datos críticos en todo momento, y esperan que recuerden la capacitación de seguridad cibernética recibida.

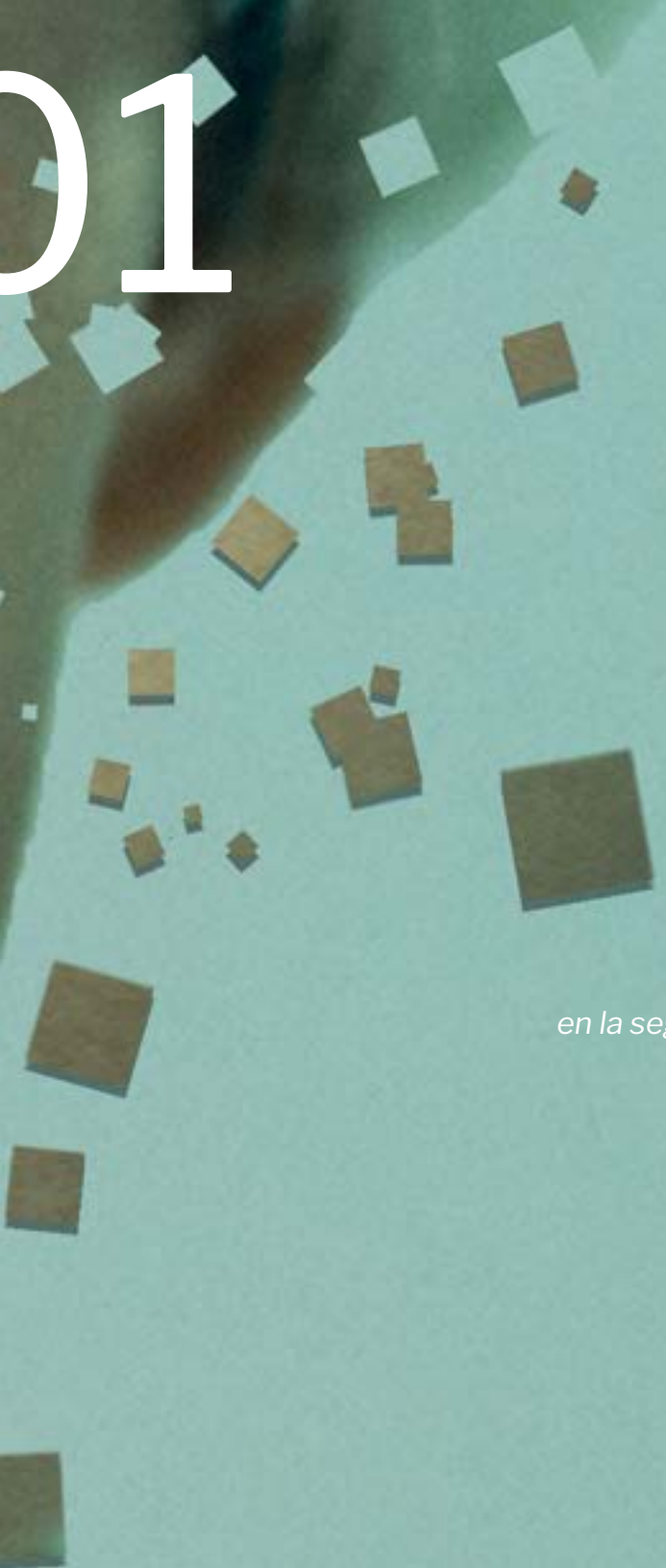
Las interacciones confiables facilitan la creación de valor para una compañía, pero la intersección entre el usuario y los datos es también el punto de mayor vulnerabilidad para una empresa y la principal fuente de intrusiones de seguridad que llevan al riesgo cibernético a niveles nunca antes vistos.

¿Cómo pueden los profesionales de la seguridad saber si el inicio de sesión de un usuario final es el resultado del acceso de un empleado desde una cafetería con WiFi o del uso indebido de un atacante de credenciales autorizadas? ¿Cómo pueden saber si la identidad de un usuario se comporta de manera coherente o errática en la red, en comparación con una rutina establecida? Saber distinguir entre un individuo que genuinamente intenta realizar su trabajo y una identidad comprometida y tomar medidas al respecto es la diferencia entre la innovación y la pérdida de propiedad intelectual (PI), el éxito o el fracaso de una organización.

A medida que los datos y las experiencias digitales pasan a manos de otros, el concepto de la confianza se vuelve incluso más crítico. Una empresa puede triunfar o fracasar como consecuencia de la confianza; las compañías que abusan de la confianza de sus clientes se enfrentan a multas regulatorias de miles de millones de dólares y a la pérdida del valor en el mercado, como en el caso de Facebook y Cambridge Analytica.

En el Informe de Predicciones de Seguridad Cibernética 2019 de Forcepoint exploramos el impacto de que las empresas depositen su confianza en los proveedores en la nube para proteger sus datos, el impacto de la confianza de los usuarios finales en quienes resguardan datos biométricos, el flujo en cascada de la confianza a la cadena de suministro para proteger todo dato crítico en su custodia, y la confianza en los algoritmos y los datos analíticos que pilotean con éxito automóviles y alertan a los profesionales de seguridad sobre posibles incidentes de pérdida de datos.

Nuestros equipos globales de Security Labs, Laboratorios de Innovación, Directores de Tecnología y Directores de Seguridad de la Información han compilado sus principales predicciones para el próximo año. Siga leyendo para descubrir nuestras siete predicciones para el 2019. ¿Cómo guiará a su organización a través de este panorama de confianza cada vez más complejo? ■



01

¿El ocaso de la IA?

Crece la desilusión a medida que se responsabiliza a la inteligencia artificial (IA) y al aprendizaje automático por aquello que afirman

Predicción:
No existe inteligencia artificial (IA) real en la seguridad cibernética, ni probabilidad alguna de que se desarrolle en 2019.

Colaborador:
Raffael Marty,
Vice President of Research and Intelligence

Además del sinfín de amenazas actuales en constante evolución, las organizaciones se ven obstaculizadas por una continua falta de habilidades: los analistas predicen un déficit de 3.5 millones de trabajos en seguridad cibernética para 2021.[1] En un intento por llenar el vacío, las organizaciones recurrieron a la promesa de la inteligencia artificial (IA), el aprendizaje automático y los macrodatos (Big Data).

¿Y por qué no? En otras industrias, estas tecnologías representan un potencial enorme: en el cuidado de la salud, la IA abre la puerta a diagnósticos más precisos y procedimientos menos invasivos. En el campo del marketing, la IA permite un mejor entendimiento de las tendencias de compra de los clientes y una mejor toma de decisiones.[2] En el transporte, los automóviles automatizados representan un gran potencial para la conveniencia y la seguridad de los consumidores. Se espera que los ingresos de IA en el sector automotriz crezcan de $404 millones, en 2016, a $14,000 millones para el 2025.[3]

El revuelo por la IA en la seguridad cibernética es casi tangible. En los dos últimos años, la promesa del aprendizaje automático y la IA ha cautivado y atraído a comercializadores y medios de comunicación, muchos han sido víctimas de ideas erróneas y definiciones de productos poco claras. En algunos casos, las nuevas empresas de IA ocultan cuánta intervención humana

implican los productos que ofrecen.[4] En otros, el incentivo de incluir productos basados en aprendizaje automático es demasiado atrayente como para ignorarlo, aunque no sea mas que para satisfacer a una base de clientes intrigados.

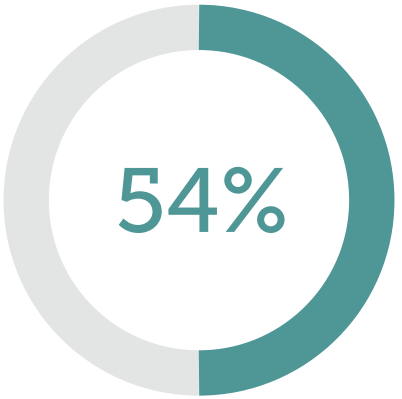
Actualmente, la IA en su sentido más puro no existe en términos de seguridad cibernética y predecimos que no se desarrollará en el 2019. Mientras que la IA se trata de reproducir las facultades cognitivas, las soluciones actuales son en verdad más representativas para el aprendizaje automático, y requieren que personas obtengan nuevos conjuntos de datos de capacitación y conocimiento experto. A pesar de la creciente eficiencia analítica, actualmente, este proceso todavía requiere de entradas, y esas entradas deben ser de alta calidad. Si se ingresan datos de mala calidad a una máquina, los resultados que arroje serán igualmente malos. Las máquinas necesitan de retroalimentación significativa de los usuarios para poder ajustar su monitoreo; sin ella, los analistas no pueden extrapolar nuevas conclusiones.

Por una parte, el aprendizaje automático ofrece claras ventajas en la detección de actividad atípica, lo que beneficia a los análisis de seguridad y las operaciones del centro de operaciones de seguridad (SOC). A diferencia de los humanos, las máquinas pueden manejar miles de millones de eventos de seguridad por día, brindando claridad acerca de la actividad "normal" o "de punto de referencia" de un sistema y marcando todo aquello que sea inusual para la revisión humana. Entonces, los analistas pueden identificar las amenazas más rápido mediante la correlación, la coincidencia de patrones y la detección de anomalías. Mientras que un analista del SOC puede demorarse varias horas en clasificar una sola alerta de seguridad, una máquina puede hacerlo en apenas segundos y seguir, incluso después del horario de oficina.

Sin embargo, las organizaciones confían demasiado en estas tecnologías sin entender los riesgos que implican. Los algoritmos pueden no detectar ciertos ataques si no se depuró debidamente la información de capacitación de puntos de datos anómalos y del sesgo del entorno del que se recolectó. Además, ciertos algoritmos pueden ser demasiado complejos para entender qué es lo que impulsa a un conjunto específico de anomalías.

Además de la tecnología, la inversión es otra área problemática para la IA en la seguridad cibernética. Los capitalistas de riesgo que brindan financiamiento a las firmas de IA esperan un retorno de la inversión oportuno, pero la burbuja de la IA tiene preocupados a muchos expertos. Michael Woodridge, responsable de Ciencias Informáticas en la Universidad de Oxford, ha expresado su preocupación referente a que los "charlatanes y estafadores" actualmente están exagerando el progreso de la IA.[5] Investigadores

Raffael Marty, vicepresidente de Investigación e Inteligencia



Solo 1 de 2 (54%) empleados de empresas con amplia experiencia en el aprendizaje automático verifican si hay imparcialidad y prejuicio.[9]

Solo 1 de 2 (53%) empleados que pertenecen a empresas con amplia experiencia en aprendizaje automático verifican si hay privacidad.[9]

de la Universidad de Stanford lanzaron el índice de IA, un proyecto abierto, sin fines de lucro que busca hacer un seguimiento de la actividad en el campo de la IA. En su informe de 2017, afirman que incluso a los expertos del índice de IA les cuesta entender y realizar el seguimiento del progreso en este ámbito.[6]

La desaceleración del financiamiento para la investigación de IA es algo inminente, lo que recuerda al "ocaso de la IA" de 1969, cuando el Congreso de los Estados Unidos recortó el financiamiento luego de que los resultados fueron mucho menores que las grandes expectativas.[7] Sin embargo, las tácticas de los atacantes no están atadas a las inversiones, lo que permite el avance continuo de la IA como herramienta de los hackers para destacar las brechas de seguridad y el robo de datos valiosos.

Al ser la regla de oro para la eficiencia de la piratería informática, la IA usada como un arma ofrece a los atacantes un conocimiento incomparable sobre qué, cuándo y dónde atacar. Por ejemplo, se descubrió que los tweets de phishing creados por IA tienen un índice de conversión considerablemente mejor que los creados por humanos.[8] Los atacantes artificiales son un contrincante formidable, y seguiremos viendo como progresa la carrera armamentista en torno a la IA y el aprendizaje automático. ■

El **99%** de los clientes encuestados identificaron a los atacantes cibernéticos en evolución como un problema de seguridad importante para su organización.[10]

Las soluciones de IA actuales no están creadas para lidiar con la ambigüedad. Los seres humanos, por otro lado, tienen mayor capacidad de equilibrar múltiples variables y el contexto asociado con el comportamiento para tomar decisiones, especialmente cuando se enfrentan a lo inesperado. La industria de la seguridad cibernética no puede evitar lidiar con esta ambigüedad.

— Audra Simons, jefa de Innovación y Creación de Prototipos, Forcepoint

02

Caos a escala en el Internet de las cosas industrial

Los atacantes buscan vulnerabilidades en el hardware y la infraestructura en la nube

Predicción:

Los atacantes causarán interrupciones en dispositivos del Internet de las cosas industrial (IIoT) a través de vulnerabilidades en la infraestructura de la nube y en el hardware.

Colaborador:
George Kamis,
Chief Technology Officer for Global Governments and Critical Infrastructure

Los sistemas de control industriales (ICS) en red que requieren de conectividad "siempre encendida" presentan mayor superficie de ataque, y esto resulta más evidente en el caso de los dispositivos del Internet de las cosas (IoT). Los sensores conectados por WiFi y en red en los artefactos y vehículos autónomos han introducido un conjunto de requisitos de seguridad que evolucionan con rapidez. Los ataques en el Internet de las cosas (IoT) de consumo son prevalentes, pero la posibilidad de que impacten en la industria de la fabricación y otras similares hace que la amenaza sea mucho más seria.

El Informe de Predicciones de Seguridad Cibernética 2018 de Forcepoint expuso el potencial de los ataques de intermediario (MITM) en las redes del IoT.[11] En 2019, los atacantes irrumpirán en los dispositivos del IoT industrial al atacar la infraestructura de la nube subyacente. Esto resulta más deseable para un atacante, debido a que resulta mucho más redituable una vez que se obtiene el acceso a los sistemas subyacentes de estos entornos de varios clientes.

Existen tres puntos en juego: la mayor conectividad en red con edge computing; la dificultad para proteger esos dispositivos a medida que aumentan los edge computing, como ocurre en instalaciones remotas y en

Carl Leonard, analista principal en Seguridad

El **81%** de los clientes encuestados identificaron a las interrupciones en el IoT como un problema de seguridad importante para su organización.[14]

El **76%** de los clientes encuestados tienen inquietudes sobre la seguridad de la infraestructura o los dispositivos del IoT, ya sea dentro de su empresa o en su cadena de suministro.[15]

dispositivos del IoT; y la cantidad exponencial de dispositivos que se conectan a la nube para buscar actualizaciones y mantenimiento.

A medida que los sistemas de control sigan evolucionando, los proveedores de servicios en la nube crearán parches, mantenimiento y administrarán estos sistemas. Estos proveedores de servicios en la nube confían en la infraestructura, plataformas y aplicaciones compartidas para poder brindar servicios escalables a los sistemas del IoT. Los componentes subyacentes de la infraestructura tal vez no ofrezcan aislación suficiente la una arquitectura para varios clientes o aplicaciones, lo que puede llevar a vulnerabilidades de tecnología compartida. En el caso del IoT industrial, los servidores de back-end se verán comprometidos inevitablemente causando cortes masivos en el servicio y se detendrán de pronto sistemas vitales. La manufactura, la producción de energía y otros sectores clave podrían verse afectados en forma simultánea.

Con Meltdown y Spectre en 2018 vimos vulnerabilidades que eluden las capas de software y firmware que exponen el hardware del procesador. En este escenario, los atacantes utilizan programas con privilegios bajos para acceder a más datos críticos, como archivos privados y contraseñas. Se cree que desde 1995 casi todas las CPUs son vulnerables,[12] y desde entonces se descubrieron nuevas variantes de Spectre. Los atacantes centrarán su atención en el desarrollo de variantes que quebranten la infraestructura de la nube subyacente utilizada por los sistemas del IIoT. Dado que la velocidad de procesamiento es crítica para el desempeño, los fabricantes y los proveedores de servicios en la nube podrían seguir eligiendo la velocidad por sobre la seguridad, para así vencer a la competencia e introducir involuntariamente vulnerabilidades adicionales.

Las organizaciones deberán pasar de la visibilidad al control, justo en el punto donde convergen las redes de TI y TO para protegerse de ataques dirigidos y deliberados al IoT industrial. ■

"El IoT será el área de la seguridad que presente mayores desafíos. No muchos profesionales de seguridad han tenido tiempo de enfocarse en el IoT y esto se está convirtiendo en una tendencia en nuestras vidas. Esto se está volviendo más y más grande, y puede ser muy peligroso cuando los dispositivos del IoT se vean vulnerados".[13]

— Sean Wang, ingeniero de Bank of Hope

03

Un reflejo falso

Se infiltra software de reconocimiento de rostro para robarle la imagen de su rostro

Predicción:
Los hackers manipularán software de reconocimiento facial de usuarios finales y las organizaciones responderán con sistemas basados en el comportamiento.

Colaborador:
Nico Fischbach,
Global Chief Technology Officer

Para un atacante, el robo exitoso de credenciales legítimas debe sentirse como ganarse la lotería. Los usuarios finales quedan imposibilitados para ingresar a sus cuentas, el acceso a servicios en la nube de terceros como Dropbox y Microsoft Office 365 se ve interrumpido, se descargan datos críticos o los elimina por completo. La cantidad cada vez más grande de intrusiones revela una simple verdad: las direcciones de correo electrónico, las contraseñas y la información personal (color favorito, nombre de su mascota) ya no son suficientes para proteger las identidades en línea.

El phishing sigue siendo el método más utilizado para el secuestro de la identidad del usuario final, ocupando el primer lugar en un estudio realizado en el 2017 por Google, la Universidad de California, en Berkeley, y el International Computer Science Institute.[16] Del 2016 al 2017, los investigadores calcularon que hubo más de 12.4 millones de víctimas del phishing, y recomendaron que los mecanismos de autenticación para mitigar el secuestro se hicieran más estrictos.

Si bien el robo de credenciales es el truco más viejo (y el más eficaz) que conocemos, esto no significa que los atacantes no estén probando nuevas alternativas. La doble autenticación (2FA) agrega una capa extra de seguridad, pero incluso este método tiene una vulnerabilidad: generalmente se realiza mediante teléfonos móviles.

En 2018, Michael Terpin, cofundador del primer grupo de inversionistas entusiastas de bitcoin, presentó una demanda por $224 millones contra la compañía de telecomunicaciones AT&T, reclamando la pérdida de $24 millones en criptomonedas como resultado de un "cambio de SIM".[17] Los atacantes usaron tácticas de phishing e ingeniería social para engañar a un representante de servicio al cliente para que portara el número de teléfono de Terpin en un teléfono desechable e imposible de rastrear. Una vez realizado este cambio, solo fue necesario hacer clic en un enlace de "¿Olvidó su contraseña?" para concretar el crimen.

Dejando atrás la 2FA, la autenticación biométrica utiliza datos únicos para cada usuario final. En primer lugar, la posibilidad de verificar la identidad de una persona mediante sensores biométricos fisiológicos parecía una alternativa promisoria a la 2FA. Las huellas digitales, los movimientos y el reconocimiento del iris dificultan la tarea de los atacantes que buscan acceso a recursos para robar la identidad de otra persona.

Sin embargo, en años recientes incluso la autenticación biométrica ha comenzado a tambalear. En el 2016, investigadores de la Universidad Estatal de Michigan descubrieron formas simples y económicas de imprimir la imagen de una huella digital usando tan solo una impresora de inyección de tinta común.[18]

Y en el 2017, investigadores de la Facultad de Ingeniería Tandon de la Universidad de Nueva York (NYU) pudieron igualar las huellas digitales de cualquier persona usando "huellas maestras" alteradas digitalmente.[19]

El reconocimiento facial se ha vuelto masivo gracias al lanzamiento del iPhone X de Apple, el cual utiliza un emisor de luz, una cámara infrarroja y un proyector de puntos para medir rostros en 3D, un método que ellos afirman no puede ser burlado por fotografías, videos o cualquier otro tipo de medio en 2D.[20] Pero la realidad es que el reconocimiento facial tiene serias vulnerabilidades y es por eso que los hackers robarán los rostros del público en 2019. De hecho, esto ya ha sucedido, aunque solo a solicitud de los investigadores. En el 2016, especialistas de visión por computadora y seguridad de la Universidad de Carolina del Norte burlaron sistemas de reconocimiento facial usando fotografías digitales públicas, disponibles en redes sociales y motores de búsqueda junto con tecnología de realidad virtual (VR) móvil.[21]

Mientras las contraseñas pueden cambiarse, los datos biométricos físicos son genéticos y específicos de cada persona. Del mismo modo, los datos biométricos del comportamiento brindan una capa de autenticación continua al incorporar las acciones físicas de una persona, como pulsación de teclas, movimiento del

Nico Fischbach, director global de Tecnología

mouse, velocidad de desplazamiento, cómo se mueven de un campo a otro, y cómo manipulan su teléfono según lo que indican el acelerómetro y el giroscopio.[22] Es simplemente imposible que los impostores imiten estas acciones.

La combinación de datos biométricos del comportamiento con una autenticación sólida, ya sea basada en una tecnología avanzada como FaceID o 2FA, es un enfoque más sensato. Las organizaciones pueden identificar intrusos que secuestran trabajo abierto mediante el inicio de sesión y en uso con autenticación continua, preparando el camino para que métodos basados en el riesgo disparen puntos de verificación y de autenticación cuando los niveles de riesgo aumenten.[23] ■

"La principal inquietud es la ingeniería social, ya que muchos usuarios todavía tienden a no estar conscientes de esos tipos de ataques y son fácilmente engañados".[24]

—David Timmins, Server Administrator, Daystar Television Network

04

Enfrentamiento en los tribunales

Las amenazas internas terminan en un juego de litigios y culpas

Predicción:

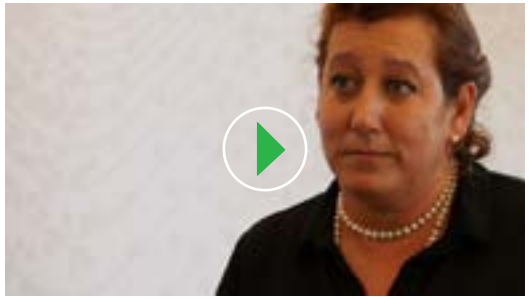
Durante el 2019 veremos una causa judicial en la que, tras una fuga de datos, un empleado se declare inocente y un empleador alegue que hubo una acción deliberada.

Colaborador:
Marlene Connolly,
Group Counsel and Senior Director

Las regulaciones de protección de datos han reforzado la habilidad de un empleado para alegar una falta cuando ocurre una fuga de datos en el lugar de trabajo, en especial cuando resulta en la exposición de su información de identificación personal (PII).[25] Sin embargo ¿qué sucede cuando un empleador demanda a un empleado alegando que causó la fuga o robó los datos intencionalmente?

Esto no debe confundirse con mera negligencia. Existe la necesidad de abordar la protección de datos críticos en un mundo donde el 24% de los empleados en el Reino Unido admiten compartir información comercial confidencial.[26] Incluso funcionarios electos han discutido abiertamente el compartir contraseñas de la computadora laboral con sus empleados.[27] A pesar de que muchos incidentes se clasifican como accidentales, los que resultan de intenciones maliciosas causan más fugas. El robo, el uso del malware o el acceso no autorizado, son tres veces más propensos a ser categorizados como una fuga de datos que los incidentes involuntarios o no intencionales.[28]

En el 2019 veremos una causa judicial en donde, tras una fuga de datos, un empleado se declare inocente y un empleador alegue que hubo una acción deliberada.



Audra Simons, jefa de Innovación y Creación de Prototipos

El **83%** de los clientes encuestados identificaron a la GDPR y otras regulaciones como una inquietud de seguridad importante para su organización.[33]

En el caso Int'l Airport Centers, L.L.C. v. Citrin (Int'l Airport Centers, L.L.C. c/Citrin), un empleado fue demandado después de haber borrado todos sus datos de la computadora portátil de la compañía tras decidir iniciar su propio negocio.[29] Y en octubre de 2017, Todd Reyling fue declarado culpable de copiar y luego eliminar varios de los archivos de las computadoras de su empleador antes de renunciar a su trabajo.[30] Los tribunales han sostenido que incluso si un empleado tiene acceso a los archivos, ese acceso "ya no es autorizado" si utilizan la información de una manera que sea desleal a su empleador.[31]

El 20 de junio de 2018, se presentó una demanda contra Martin Tripp, un exempleado de Tesla que, según los documentos presentados ante el tribunal, recopilaba y filtraba datos en un intento de advertir a los inversionistas y al público sobre supuestos informes de producción engañosos y baterías defectuosas instaladas en automóviles Tesla.[32] Tesla refuta los alegatos de Tripp y afirma que lo que llevó a Tripp a que cometiera sabotaje industrial fue su mal desempeño laboral y su eventual reasignación, y acusa a Tripp de instalar un software que siguió recopilando datos incluso después de que dejara la compañía. Tripp además expuso fotografías confidenciales y un video del sistema de fabricación de Tesla.

Todavía está por determinarse si Martin Tripp es un saboteador o un informante. Normalmente, cuando un empleado destruye datos, envía propiedad intelectual (PI) a un competidor o a un nuevo empleador intencionalmente, suele resultar en una situación de "mi palabra contra la de ellos". En este caso, las acciones de Tripp de filtrar información confidencial no están en disputa, sino su motivo para hacerlo, lo que influirá significativamente en la parte que obtiene la protección del tribunal y la simpatía del público.

Todo se centra en el impacto financiero potencial sobre una compañía. Cuando la fuga de datos y la pérdida de PI no solo causan daños a la reputación sino también multas que ocupan los titulares bajo la Regulación General de Protección de Datos (GDPR) y otras regulaciones asociadas, el contexto y la motivación detrás de una fuga se vuelven mucho más relevantes.

En el caso de una fuga, que un empleador gane una demanda en un tribunal probando que hubo negligencia o malas intenciones de parte del empleado es meramente una victoria pírrica. En cambio, sirve para resaltar públicamente las medidas de seguridad cibernética deficientes de una organización.

Cuando un juez falla a favor de un empleado, los ejecutivos se darán cuenta que la carga probatoria para demostrar medidas de seguridad adecuadas y apropiadas, a nivel organizacional y técnico, recaen en sus sistemas y procesos

internos. Las organizaciones deben identificar la actividad maliciosa a medida que ocurre y detenerla antes de que dañe sistemas críticos y PI, y deben tomar medidas para implementar tecnologías de seguridad cibernética y de monitoreo en el lugar de trabajo, en su entorno de TI con el fin de comprender el panorama completo en torno a un incidente y probar las intenciones del usuario final.

Esto no significa que el 2019 será el año de "nosotros contra ellos" o de enfrentar a los empleados contra sus empleadores. Los empleados tienen un interés personal en el éxito de la compañía, y el monitoreo en el lugar de trabajo se trata de proteger a las personas y los datos. Manejar las amenazas dentro de una organización mediante el monitoreo en el lugar de trabajo es un elemento vital en la caja de herramientas de un profesional de seguridad, una forma confiable de proteger a los clientes, la propiedad intelectual y la marca, así como la buena reputación de sus empleados.

Sin embargo, los programas de monitoreo en el lugar de trabajo deben introducirse enfocados en tres principios clave: propósito legítimo, proporcionalidad y transparencia total durante la implementación. La protección de los datos personales y la privacidad ya no son las mejores prácticas, sino que son cuestiones esenciales y básicas para cualquier organización exitosa. ■

Estamos esperando contar con legislación similar a la GDPR aquí en los Estados Unidos. Como profesional de TI en el campo del cuidado de la salud, la seguridad de los datos y la protección de nuestros pacientes, y de nuestros empleados, es una cuestión crítica.[34]

—Cody Taggart, administrador de sistemas de Medical Arts Hospital

05

Trayectoria de colisión hacia la Guerra Fría cibernética

Los embargos comerciales provocan una ola de espionaje industrial

Predicción:

Las políticas comerciales aislacionistas incentivarán a los estados nacionales y a las entidades corporativas a robar secretos comerciales y usar tácticas cibernéticas para crear caos en industrias claves, infraestructura crítica y gobiernos.

Colaborador:
Luke Somerville,
Head of Special Investigations

Los canales de noticias han descrito el 2018 como el comienzo de una guerra comercial de 20 años.[35] Históricamente, la apertura de las fronteras comerciales ha llevado a una polinización cruzada de tecnología a través de mercados existentes y emergentes. Sin embargo, durante el 2018 hemos visto un cambio hacia posturas más proteccionistas en forma de embargos comerciales, esto como resultado del quiebre de la confianza entre las potencias mundiales.

En ambos lados, las tarifas ahora acompañan a todo, desde dispositivos electrónicos personales hasta productos de seguridad y salud. Desde el punto de vista de los actores en estados nacionales desfavorecidos, las disputas comerciales limitan las oportunidades legítimas de adquirir software y hardware que podrían reforzar sus capacidades cibernéticas. Desde el punto de vista de las empresas, los embargos comerciales afectan el acceso a nueva tecnología, el intercambio de conocimiento, e incluso la disponibilidad de talento humano.

Se ha escrito mucho sobre la "guerra cibernética" y su lugar junto a técnicas militares más convencionales. Esto tiende a crear temor de una guerra sin cuartel en Internet y trae visiones de ataques cibernéticos que escalen a nivel de un ataque cinético. El informe de Predicciones de Seguridad Cibernética 2017 de Forcepoint habló de las implicaciones del Artículo 5 de la OTAN,

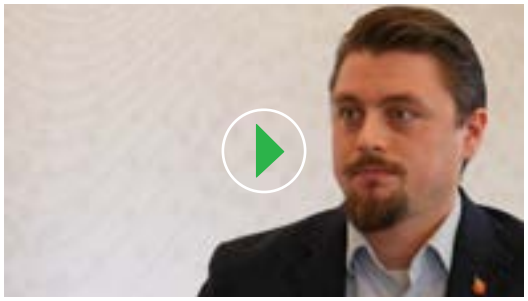
la nueva “Política mejorada de ciberdefensa de la OTAN”, que permite un ataque cinético como respuesta a un incidente en el ciberespacio.[36]

Una mejor analogía para describir las posibles implicaciones de los embargos comerciales sería la guerra fría, con “operaciones” cibernéticas ligadas a la función de los servicios de inteligencia exterior de los países. Los cambios al flujo y la disponibilidad de la información entre fronteras nacionales podrían llevar a un futuro que se asemeje cada vez más a los años entre finales de la década de 1940 y comienzos de la de 1990, donde el acceso a estas tecnologías se adquiría a través del espionaje. Tanto las naciones como las compañías siempre han sido naturalmente protectoras de su propiedad intelectual, pero a medida que disminuyen las oportunidades de comprar acceso legítimo a esta, las personas del otro lado de los embargos tienen un incentivo real para adquirirla por medios maliciosos.

En lugar de crear muros más altos para evitar que los hackers patrocinados por estados nacionales ataquen a plantas de fabricación y generadores eléctricos, la industria de la seguridad cibernética debe comprender mejor cómo, cuándo y por qué las personas interactúan con datos sensibles, sin importar donde se encuentren. Tanto los estados nacionales como las empresas necesitan entender quién está tocando los contenidos críticos y por qué.

Para evitar el robo de PI, las organizaciones deben enfocarse en comprender el comportamiento normal de los usuarios legítimos con acceso a secretos comerciales y saber cuándo ese comportamiento cambia, lo que indica la intención de robarlos. ■

El **88%** de los clientes encuestados están preocupados por posibles ataques a la infraestructura crítica de la que dependen sus organizaciones.[37]



Luke Somerville, jefe de Investigaciones Especiales

06

Dirigidos hacia el borde

Las organizaciones buscan reforzar la privacidad pero logran avanzar poco debido al quiebre en la confianza

Predicción:

La preocupación de los consumidores respecto a las fugas hará que las compañías adopten más edge computing para optimizar la privacidad. Los diseñadores enfrentarán desafíos significativos en cuanto a la adopción dada la baja confianza de los usuarios.

Colaborador:
Dr. Richard Ford,
Chief Scientist

Para el usuario promedio, pareciera que las noticias están repletas de historias sobre fugas o abuso de datos personales. Para muchas personas, este torrente constante de malas noticias les hace pensar que sin importar lo que hagan, su información será filtrada eventualmente, para luego surgir en la Dark Web en algún momento a futuro. Por ello, la confianza en muchos servicios en línea es baja y el optimismo, escaso.

En respuesta a estas inquietudes, los proveedores intentan encontrar un equilibrio entre las necesidades legítimas de privacidad de los usuarios y la suya propia, para así poder monetizar los servicios que brindan. Lo que es aún mejor, algunos desarrolladores se han dado cuenta de que, con esfuerzo suficiente, es posible aplicar los principios de la "privacidad por diseño" para crear una solución que sea mutuamente beneficiosa para los clientes y los usuarios finales.

Una forma atractiva de mejorar la privacidad es que los clientes conserven el control de sus datos y se muevan los algoritmos que ayudan a procesarlos al dispositivo final. Este enfoque de sacar provecho del dispositivo final en armonía con la nube se conoce como "computación en el borde" o Edge Computing. Si bien algunas personas tienden a ver al Edge Computing como algo en conflicto con el movimiento hacia

la nube, esto representa más precisamente la concreción completa de la visión de Cloud Computing, donde la nube y el dispositivo final trabajan en conjunto para brindar un servicio.

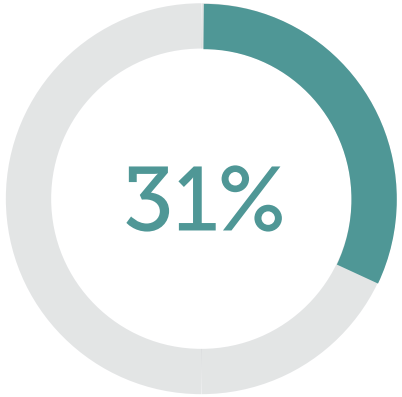
Un ejemplo reciente de una solución que preserva la privacidad que aprovecha el Edge Computing es la calificación de confianza del usuario de Apple, que está diseñada para detectar el uso fraudulento de un dispositivo al examinar el comportamiento del usuario.[38] Tal como está implementada, los cálculos de los datos se realizan en el dispositivo, y solo se envían los metadatos a la nube, protegiendo así la privacidad del usuario. Sin embargo, estos beneficios de privacidad solo son significativos en los casos en que los usuarios finales están preparados para tomar en serio a la empresa y creer que sus datos, de hecho, nunca salen de sus dispositivos.

El problema es la confianza. Dados los principales cambios en la confianza observados durante los últimos 10 años, la confianza en las instituciones se ha visto reemplazada por un modelo de confianza entre pares (P2P). Esto es en parte lo que ha impulsado el éxito de compañías como Uber y AirBnB, que esencialmente funcionan como mediadores de confianza entre dos partes. Aún no existe un proceso similar para las empresas, algo que resulta perjudicial para estas soluciones mejoradas. La aparición de los índices de confianza respecto de la seguridad puede cambiar el juego. En muchos aspectos, la percepción es la realidad.

Nuestra predicción entonces se divide en dos partes. En primer lugar, predecimos que muchos proveedores comenzarán a aplicar los principios del edge computing para brindar servicios con un mayor grado de privacidad. De cualquier modo, precedimos también que muchos usuarios finales no entenderán estas mejoras o no tendrán la confianza suficiente en la empresa para permitir que la privacidad real se convierta en un diferenciador competitivo fuerte.

No es suficiente para las organizaciones comprender y proteger los datos en el dispositivo y en la nube. Para generar confianza deben lograr que los consumidores crean no solo en la promesa, sino en la realidad de cómo se protegen y utilizan sus datos. ■

Carl Leonard, analista Principal en Seguridad



Casi un tercio (31%) de los clientes de Forcepoint encuestados ya están limitando los datos que incluyen en la nube debido a inquietudes de seguridad.[39]

07

Las culturas de seguridad cibernética que no se adapten, fallarán

Los “índices de confianza respecto a la seguridad” recompensan a algunas organizaciones y castigan a otras

Predicción:

Los "índices de confianza respecto a la seguridad" de toda la industria surgirán a medida que las organizaciones busquen garantías de que sus socios y sus cadenas de suministro son confiables.

Colaborador:
Meerah Rajavel,
Chief Information Officer

Cuando una organización adquiere servicios o firma un acuerdo de sociedad, realiza una diligencia debida considerable basada en la seguridad financiera y el cumplimiento de las leyes y las normas de la industria. Hoy, nuestro mundo con prioridad en la nube e impulsado por la tecnología móvil ve cómo los usuarios y los datos deambulan libremente por las redes, dejando a los datos críticos y la propiedad intelectual más expuestos que nunca. En el futuro, la debida diligencia se extenderá a qué tanta confianza puede depositar una organización en la seguridad de un socio.

Por eso, en el 2019 veremos la creación de “calificaciones de confianza respecto a la seguridad” en toda la industria. Tal como existen rankings y calificaciones para la confianza de distintas instituciones financieras, opciones de inversiones o incluso restaurantes, el futuro traerá una calificación de confianza respecto de la seguridad similar a los negocios que manejan, almacenan o interactúan con datos. Estas calificaciones indicarán qué tan seguro es permitirles a los proveedores gestionar información de identificación personal (PII) u otros datos críticos. ¿Qué tal es la higiene cibernética de sus empleados? ¿Tiene el proveedor un historial de riesgo de fugas?

Las compañías previsoras deben planear con antelación, ya que su propia higiene de seguridad estará ahora visible como acreditaciones

o certificaciones de la industria.[40] No habrá forma de esconderse de los malos hábitos y la mala cultura de seguridad. Según lo demuestra el malware encontrado en los sistemas existentes en Micros, una división de Oracle y uno de los principales proveedores de punto de venta (PoS) a nivel global, los pirateos de las cadenas de suministro que ocupan los titulares no solo tienen un impacto financiero inmediato en la forma de multas regulatorias, sino que también dañan la reputación de la compañía y alejan futuros negocios.[41,42]

La forma de desarrollar una calificación de confianza mejorada es mediante un cambio en la cultura de la seguridad cibernética. La seguridad no puede ser solamente responsabilidad de los equipos de TI y las tecnologías que ellos implementan, sino que debe convertirse en un valor comercial y cultural que sea reconocido y recompensado. Para crear una fuerza laboral unida como una defensa contra la ciberdelincuencia, las organizaciones deben integrar la seguridad a su cultura desde los niveles más altos y en forma descendente.

La cultura incluye mucho más que el clima de una ubicación de oficinas específica o que los valores, las normas y reglas de una organización. También incluye la cadena jerárquica, la delegación de autoridad, la responsabilidad por los comportamientos y las estrategias de comunicación amplias. Las políticas mal definidas o en conflicto entre sí crean confusión y malas interpretaciones. Toda confusión acerca de las reglas, las expectativas o la responsabilidad pueden aumentar el riesgo, incluso el riesgo de fuga de datos.

Las culturas corporativas actuales tienen fronteras expansivas que se extienden a través de las cadenas de suministro y otras asociaciones debido a la conectividad y el uso de la nube. A medida que las organizaciones grandes modifiquen su actitud hacia la seguridad cibernética, esto se verá reflejado a través de la cadena de suministro. La introducción de las calificaciones de confianza respecto de la seguridad recompensará a las empresas que vayan más allá de las intervenciones superficiales como la capacitación "justo a tiempo", que son ineficaces y pueden causar molestia, cansancio y apatía en los empleados.

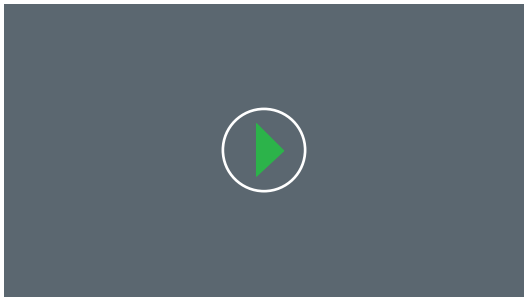
Las empresas que adapten su cultura de seguridad a las amenazas sofisticadas resultarán vencedoras. Sin embargo, la uniformidad de seguridad cibernética sistémica se requiere para todas las operaciones y los usuarios, lo que incluye sus socios de la cadena de suministro. ■

"Los errores humanos son el mayor desafío y serán un problema considerable".[43]

— Profesional de negocios de una empresa de servicios informáticos grande

"Nos preocupan las amenazas por correo electrónico y el malware en plena evolución, así como los ataques de ingeniería social. Porque nuestros empleados pueden ser nuestro eslabón más débil y necesitamos una seguridad fuerte para que actúe como red de contención".[44]

—Profesional de TI de una empresa minorista mediana



Meerah Rajavel, Chief Information Officer

"La falta de constancia es la amenaza más grande para una organización. Siempre existen grupos dentro de una empresa que creen que lo que ellos hacen es demasiado importante, o demasiado diferente, y que insistirán con una excepción. En el 2019, los líderes necesitan ayudar a sus equipos a entender que las excepciones crean riesgo significativo para toda la organización."

Jeff Brown,
Vicepresidente y CISO de Raytheon

Conclusión

Para evaluar qué sucederá en el 2019, necesitamos analizar el *porqué*, para poder así predecir el *qué*. La motivación detrás de las acciones cibernéticas, el desarrollo de malware avanzado o las tendencias macroindustriales, es esencial para darnos el contexto necesario para formular predicciones precisas. Las empresas pueden aplicar ese enfoque al evaluar cómo proteger de mejor manera sus negocios, incluido su personal y datos críticos.

¿Por qué la comunicación de un usuario final no está cifrada? ¿Por qué un atacante centra sus esfuerzos en una industria específica? ¿Por qué ese comportamiento malicioso evidente pasó inadvertido?

Los profesionales de seguridad cibernética saben que los ataques específicos cambiarán y evolucionarán pero que los temas siguen siendo los mismos: los datos confidenciales son un objetivo atrayente para los atacantes. Los "malos", quienes realizan amenazas, crean malware, etc., siguen inventando métodos para eludir sistemas de protección diseñados por la industria de seguridad cibernética. Los atacantes cibernéticos y los analistas de seguridad destinan su energía en un ciclo constante de fuga, reacción y elusión, un verdadero juego de gato y ratón. Tenemos que lograr escapar de ese juego. Al detenernos a examinar tendencias y motivaciones cada año, podemos ver el bosque completo de entre los millones de árboles.

El concepto de confianza está integrado en nuestras siete predicciones para el 2019. La confianza es vital para las relaciones personales y de negocios. Puede hacer que un negocio triunfe o fracase, sin embargo, las personas suelen tener una relación complicada con la confianza porque es intangible. Considere que la confianza existe en un continuo entre la fe total y la desconfianza absoluta; en medio de ese continuo, se encuentra la zona gris de la incertidumbre.

La opción de "confiar pero verificar" puede ser aplicable a ciertas situaciones pero solo si está respaldada por la visibilidad del comportamiento cibernético de un usuario final. Tomar una decisión sobre la seguridad si el barómetro del riesgo no se inclina claramente hacia un lado u otro es todo un desafío. El riesgo puede transferirse porque el control se delegó a través de la cadena de suministro, quizá a un proveedor en la nube que ahora administra la ubicación de los datos e incluso la autenticación de los usuarios para limitar el acceso a los datos.

La manera de recuperar el control y librarse del juego del gato y el ratón es mediante la creación de modelos de comportamiento de los usuarios o, más específicamente, sus identidades digitales. Entender cómo actúa un usuario en la red y dentro de las aplicaciones puede identificar las anomalías, permitir comprender las intenciones y ganar confianza. El comportamiento puede considerarse como algo de bajo riesgo, de alto riesgo o no determinado. Un entendimiento más profundo del comportamiento significa que podemos ser más fuertes al determinar la confianza y el riesgo. En lugar de tomar una decisión de blanco o negro, como los enfoques de seguridad tradicionales, nuestra respuesta en el presente y en el futuro se puede adaptar a medida que el riesgo cambia, evitando la fricción comercial y permitiéndonos detener a los malos y liberar a los buenos.

Como siempre, repasaremos la precisión de nuestras predicciones de seguridad cibernética para 2019 a lo largo del año. Después de todo, usted confía en que sean correctas. ■

Citas

1. Kuranda, Sarah. *'Study: Cybersecurity Skills Gap Will Grow To 3.5M Positons By 2021." CRN*, 6 de junio de 2017, www.crn.com/news/security/300086546/study-cybersecurity-skills-gap-will-grow-to-3-5m-positons-by-2021.htm.
2. McCormick, J. *Predictions 2017: Artificial Intelligence Will Drive The Insights Revolution*. Forrester, 2 de noviembre de 2016.
3. *Automotive Artificial Intelligence Revenue to Reach $14 Billion by 2025, According to Tractica | Business Wire.* 24 de mayo de 2017, https://www.businesswire.com/news/home/20170524005456/en/Automotive-Artificial-Intelligence-Revenue-Reach-14-Billion.
4. Solon, O. *The Rise of 'pseudo-AI': How Tech Firms Quietly Use Humans to Do bots' Work | Technology | The Guardian*. 6 de julio de 2018, https://www.theguardian.com/technology/2018/jul/06/artificial-intelligence-ai-humans-bots-tech-companies.
5. Hornigold, T. *How Fast Is AI Progressing? Stanford's New Report Card for Artificial Intelligence.* 12 de enero de 2018, https://singularityhub.com/2018/01/18/how-fast-is-ai-progressing-stanfords-new-report-card-for-artificial-intelligence/#sm.00001vlq30ylzcs1sf722zbsynfyj.
6. Shoham, Y., R. Perrault, E. Brynjolfsson, and J. Clark. *Artificial Intelligence Index 2017 Annual Report.* Noviembre de 2017, https://aiindex.org/2017-report.pdf.
7. *AI: 15 Key Moments in the Story of Artificial Intelligence*. https://www.bbc.com/timelines/zq376fr.
8. Dvorsky, George. *Hackers Have Already Started to Weaponize Artificial Intelligence.* Gizmodo, 12 de septiembre de 2017, gizmodo.com/hackers-have-already-started-to-weaponize-artificial-in-1797688425.
9. Lorica, B., and P. Nathan. 5 *Findings from O'Reilly's Machine Learning Adoption Survey Companies Should Know* - O'Reilly Media. 7 de agosto de 2018, https://www.oreilly.com/ideas/5-findings-from-oreilly-machine-learning-adoption-survey-companies-should-know.
10. Fuente: TechValidate. TVID: 108-7E9-1A6
11. "Predicciones de seguridad para 2018 de los Laboratorios de seguridad de Forcepoint". Forcepoint, 21 de junio de 2018, www.forcepoint.com/resources/reports/2018-security-predictions-forcepoint-security-labs.
12. Melendez, Steven. *'Spectre" And 'Meltdown" Chip Flaws Touch 'Almost Every System," Say Researchers.* Fast Company, 4 de enero de 2018, www.fastcompany.com/40513416/spectre-and-meltdown-chip-flaws-touch-almost-every-system-say-researchers.
13. Fuente: TechValidate. TVID: CBE-B96-18C
14. Fuente: TechValidate. TVID: 680-5DE-BF9
15. Fuente: TechValidate. TVID: 6B7-B75-241

16. Thomas, Kurt, et al. *Data Breaches, Phishing, or Malware? Understanding the Risks of Stolen Credentials – Google AI.* Google AI, 1 de enero de 1970, ai.google/research/pubs/pub46437.

17. Krebs, Brian. *Hanging Up on Mobile in the Name of Security.* Krebs on Security, 16 de agosto de 2018, https://krebsonsecurity.com/2018/08/hanging-up-on-mobile-in-the-name-of-security/

18. Waddell, Kaveh. *Fake Fingerprints from an Inkjet Printer Can Fool Your Smartphone.* Atlantic Media Company, 8 de marzo de 2016, www.theatlantic.com/technology/archive/2016/03/fake-fingerprints-from-an-inkjet-printer-can-fool-your-smartphone/472638/.

19. Schlesinger, Jennifer. *Why the Emerging Ransomware Threat's next Target Could Be Your Smartphone or Tablet.* CNBC, 20 de mayo de 2017, www.cnbc.com/2017/05/19/new-hacking-threats-fingerprint-vulnerabilities-and-sophisticated-ransomware.html.

20. Peterson, Becky. *Apple Worked with Hollywood Mask Makers to Make Sure the IPhone X's Facial-Recognition System Can't Be Fooled Easily.* Business Insider, 12 de septiembre de 2017, www.businessinsider.com/apple-says-the-iphone-xs-face-id-system-cant-be-fooled-by-masks-2017-9.

21. Newman, Lily Hay. *Hackers Trick Facial-Recognition Logins With Photos From Facebook (What Else?).* Conde Nast, 19 de agosto de 2016, www.wired.com/2016/08/hackers-trick-facial-recognition-logins-photos-facebook-thanks-zuck/.

22. Koong, et al. *A User Authentication Scheme Using Physiological and Behavioral Biometrics for Multitouch Devices.* The Scientific World Journal, 24 de julio de 2014, www.hindawi.com/journals/tswj/2014/781234/.

23. *'IBM Security Risk Based Authentication Solution."* IBM Security Risk Based Authentication Solution - Descripción general - Estados Unidos, IBM, 23 de octubre de 2018, www.ibm.com/us-en/marketplace/risk-based-authentication-solution?ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US.

24. Fuente: TechValidate. TVID: 113-FE0-D0C

25. Bantz, Phillip. *'One CLO Tested His Employees' GDPR Knowledge and Was 'Shocked' at What He Found."* Legaltech News, 2 de agosto de 2018, www.law.com/legaltechnews/2018/08/02/one-clo-tested-his-employees-gdpr-knowledge-he-was-shocked-at-what-he-found-397-10326/?slreturn=20180923031020.

26. *24% Of UK Employees Maliciously Misuse Company Emails: Research.* CISO MAG, 7 de noviembre de 2017, www.cisomag.com/24-uk-employees-maliciously-misuse-company-emails-research/.

27. *'Privacy Regulator Warns MPs over Shared Passwords."* BBC News, BBC, 4 de diciembre de 2017, www.bbc.com/news/technology-42225214.

28. Sher-Jan, Mahmood. *Data Indicates Human Error Prevailing Cause of Breaches, Incidents. The Privacy Advisor | Data Indicates Human Error Prevailing Cause of Breaches, Incidents Related Reading: IAF, Hong Kong DPA Release Ethical Accountability Report, Framework,* 26 de junio de 2018, iapp.org/news/a/data-indicates-human-error-prevailing-cause-of-breaches-incidents/.

29. *FindLaw's United States Seventh Circuit Case and Opinions.* Findlaw, www.caselaw.findlaw.com/us-7th-circuit/1392048.html.
30. Tribunal de Distrito de los Estados Unidos, S.D. Illinois. KASKASKIA ENGINEERING GROUP, Plaintiff, v. TODD REYLING, Et Al., Defendants (KASKASKIA ENGINEERING GROUP, Demandante, c/TODD REYLING, Et Al., Demandados). 2 de octubre de 2017.
31. Artículo 1030 del Título 18 del Código de los EE. UU. - Fraud and Related Activity in Connection with Computers (Fraude y Actividad Relacionada en Conexión con las Computadoras). Cornell Law School, www.law.cornell.edu/uscode/text/18/1030.
32. Isidore, Chris. *Tesla Sues Ex-Employee for Hacking and Theft. But He Says He's a Whistleblower.* CNN, 20 de junio de 2018, money.cnn.com/2018/06/20/technology/tesla-sues-employee/index.html.
33. Fuente: TechValidate. TVID: A0A-01D-862
34. Fuente: TechValidate. TVID: 541-863-071
35. Hankla, Charles. *The next Cold War? US-China Trade War Risks Something Worse.* The Conversation, 24 de septiembre de 2018, theconversation.com/the-next-cold-war-us-china-trade-war-risks-something-worse-103733.
36. "Informe Predicciones de Seguridad 2017 de Forcepoint". Forcepoint, 13 de agosto de 2018, https://www.forcepoint.com/resources/reports/2017-forcepoint-security-predictions-report.
37. Fuente: TechValidate. TVID: 900-9BB-779
38. Cuthbertson, Anthony. *Apple Is Quietly Giving People Black Mirror-Style 'Trust Scores' Using Their iPhone Data.* Independent Digital News and Media, 21 de septiembre de 2018, www.independent.co.uk/life-style/gadgets-and-tech/news/apple-trust-score-iphone-data-black-mirror-email-phone-fraud-a8546051.html.
39. Fuente: TechValidate. TVID: 214-C6D-148
40. *All Clouds Are Not Equal - Forcepoint Cloud Compliance.* Forcepoint, 7 de marzo 2018, https://www.forcepoint.com/all-clouds-are-not-equal-forcepoint-cloud-compliance.
41. Ashford, W. *Oracle Micros Breach Highlights PoS and Supply Chain Security Risks.* 21 de junio de 2016, https://www.computerweekly.com/news/450302206/Oracle-Micros-breach-highlights-PoS-and-supply-chain-security-risks.
42. Drinkwater, Doug. *'Does a Data Breach Really Affect Your Firm's Reputation?"* CSO Online, CSO, 7 de enero de 2016, www.csoonline.com/article/3019283/data-breach/does-a-data-breach-really-affect-your-firm-s-reputation.html.
43. Fuente: TechValidate. TVID: 214-C6D-148
44. Fuente: TechValidate. TVID: B30-66D-75E
45. Fuente: TechValidate. TVID: C4A-4A6-FA4

Disfrute del webcast y conozca más:

forcepoint.com/**2019Predictions**