accenture

2021

Futuras Amenazas Cibernéticas

Los últimos escenarios de amenazas extremas pero plausibles en los servicios financieros

Contenido

Prólogo

La pandemia ha cambiado la forma de trabajar de todas las organizaciones. Expuso a las organizaciones de servicios financieros a un crecimiento exponencial de las vulnerabilidades potenciales a través de fuerzas de trabajo remotas tanto en sus instituciones como a través de sus terceros. Los actores de las amenazas se aprovecharon de estas exposiciones de nuevas maneras, avanzando aún más sus capacidades y objetivos para el robo y la manipulación de datos, el fraude y la extorsión.

Los bancos son muy conscientes de las amenazas. Pero mientras hacen sus mejores esfuerzos para mantener operativas a las empresas y los gobiernos, existe el peligro siempre presente de que parte del dinero que fluye a través del sistema financiero para mantener las economías de todo el mundo en movimiento, no va a parar a las empresas legítimas. En su lugar, los préstamos están siendo desviados por los ciberdelincuentes: 4.200 millones de dólares sólo en 2020, según el Informe sobre la delincuencia en Internet de 2020 del FBI[1].

Está claro que las instituciones financieras deben mantenerse alerta ante las superficies de ataque y seguir alimentando las transacciones y los mercados que ayudan al crecimiento de las economías. Sin embargo, los equipos de seguridad han sido llevados al extremo durante la pandemia. Los adversarios siguen violando las cadenas de suministro de software y atacando a los proveedores de ciberseguridad en los que las organizaciones confían para mantenerse a salvo. Los defraudadores siguen encontrando nuevas oportunidades de suplantación de identidad.

Los actores de las amenazas están aprovechando la preocupación por la COVID-19 para provocar brechas que involucran a personas internas malintencionadas o involuntarias. Incluso los actores del ransomware parecen haberse vuelto más destructivos y menos propensos a restaurar los sistemas, incluso cuando se les paga.

A medida que las nuevas tecnologías reinventan nuestro lugar de trabajo, abren oportunidades para los ciberdelincuentes. La computación cuántica está avanzando, presentando un riesgo potencial real para los controles que el sistema financiero utiliza para proteger los datos. Las capacidades de deepfake están mejorando, causando preocupación por varios tipos de riesgos relacionados con el fraude para las instituciones financieras y sus clientes. Estos avances plantean futuras amenazas que podrían socavar la confianza en los sistemas actuales.

Para enfrentar estas amenazas, las organizaciones de servicios financieros deben redoblar las estrategias de mitigación probadas en el tiempo y considerar contramedidas de vanguardia. Gran parte del enfoque necesario se reduce a la defensa en profundidad y asumir una mentalidad de violación.[2]

Todo esto y mucho más lo tratamos en este informe, nuestra última visión general de las amenazas para el sector de los servicios financieros. Esperamos que nuestro análisis le ayude a tomar las medidas necesarias para adaptar su estrategia de seguridad y que sirva para informar al sector con estas ideas tan necesarias para el futuro.

Valerie Abend
Director General, Accenture Security

Howard Marshall
Director General, Accenture Security

Amenazas clave

En este tercer informe anual, basado en la investigación del equipo de Accenture Cyber Threat Intelligence (CTI), revisamos las amenazas de los dos últimos informes. Enumeramos una serie de amenazas en curso que hemos identificado en los últimos doce meses y exploramos los resultados probables de estas amenazas.

Para facilitar la lectura, hemos desglosado nuestras conclusiones en lo que está ocurriendo hoy y por qué es importante, y ofrecemos ideas sobre las medidas que pueden tomar las instituciones financieras para mitigar más riesgos.

Los cinco temas clave de las amenazas son:

01 Los ataques a la cadena de suministro se dirigen a programas y servicios esenciales

02 El ciberfraude aumenta a medida que la disrupción abre la puerta a nuevas vías y actores

03 Las amenazas de los infiltrados florecen con el trabajo a distancia

04 Los ataques de extorsión avanzan en su capacidad destructiva

05 Las tecnologías emergentes siguen reinventando el panorama de las amenazas

01
Los ataques a la cadena de suministro se dirigen a programas y servicios esenciales

¿Qué está pasando?

Como hemos visto con varios ataques a gran escala por parte de terceros, las cadenas de suministro son un importante foco de atención para los actores de las amenazas hoy en día, y es probable que lo sean en el futuro. SolarWinds y Microsoft son ejemplos de cómo los actores de las amenazas pueden aprovechar las vulnerabilidades de las infraestructuras críticas intersectoriales para obtener acceso y causar miedo, pérdida de integridad en los sistemas y probablemente dañar la fidelidad de la información procesada en sistemas potencialmente corruptos.

La campaña de espionaje basada en SolarWinds -cuyas víctimas conocidas públicamente son en su mayoría organismos gubernamentales federales y locales de Estados Unidos y proveedores de tecnología de la información (TI) o de ciberseguridad[3]—demostró que los actores de las amenazas pueden acceder a casi cualquier organización conectada vulnerable a través de sus relaciones no seguras.

En particular, los actores de esta y otras campañas se han centrado en un punto clave de la cadena de suministro: los productos y servicios de tecnología de la información y las comunicaciones, incluidos los proveedores de ciberseguridad. En pocos meses de 2020 a 2021, surgieron informes que detallaban violaciones de:

- Software de monitorización en SolarWinds.
- El software de transferencia de archivos del proveedor en la nube Accellion, que afecta a los bufetes de abogados de Estados Unidos, a una empresa de telecomunicaciones de Singapur y a los solicitantes de ayudas al desempleo de Estados Unidos.
- Sistemas en el proveedor de la nube Blackbaud, afectando a numerosas organizaciones sin ánimo de lucro.

Además, un ataque de ransomware contra los servicios de transferencia automática de fondos (AFTS) afectó a numerosas ciudades de Estados Unidos.[4]
En particular, la brecha de SolarWinds abarca varios niveles de la cadena de suministro y llega hasta los entornos de compilación y las bibliotecas de documentos. El malware infectó software no relacionado de desarrolladores cuyas plataformas de construcción albergaban software de SolarWinds. Los actores de la amenaza comprometieron por separado otras herramientas de autenticación, como Duo[5] , y supuestamente abusaron de otros vectores de acceso iniciales.[6]
Los actores de la amenaza se hicieron pasar por proveedores de confianza que entregaban Los actores de la amenaza se hicieron pasar por proveedores de confianza que entregaban una actualización de software firmada digitalmente.[7]
Los adversarios de SolarWinds y otros han abusado de Security Assertion Markup Language (SAML) para obtener acceso a recursos en la nube.

¿Por qué es importante?

El objetivo amplio y profundo de las cadenas de suministro, en particular los proveedores de servicios técnicos y de seguridad, es preocupante porque dichos proveedores sirven de puerta de entrada a las organizaciones de servicios financieros, ya sean procesadores de pagos mayoristas y minoristas, grandes bancos e infraestructuras del mercado financiero, o reguladores.

Los actores de la amenaza que maltratan las herramientas de autenticación para violar los entornos de la nube pueden acceder a documentos internos sensibles, comunicaciones y propiedad intelectual. Pueden utilizar los canales de comunicación de confianza para comprometer el correo electrónico de la empresa (BEC), hacer phishing o introducir enlaces o archivos maliciosos.

El compromiso de correo electrónico del proveedor (VEC) también facilita las operaciones de fraude cibernético.[8] A nivel sistémico, la Junta de Resolución Única (JUR) de la Unión Europea aparece entre las 23 entidades que los investigadores han identificado en la lista final altamente selectiva de los actores de amenazas de SolarWinds.[9] Una infracción de la JUR, que es la autoridad central de resolución para los bancos en problemas, podría dar a los actores de amenazas visibilidad sobre cómo la Unión Europea defiende la estabilidad de todo el sistema financiero europeo. Las recientes brechas en la cadena de suministro amenazan la confianza y la velocidad de las transacciones globales y tienen el potencial de erosionar la fe en los sistemas financieros globales.

¿Qué debe hacer?

Para reducir los riesgos asociados a las cadenas de suministro cibernéticas, Accenture sugiere considerar las siguientes acciones:

- Reforzar los niveles de privilegio y acceso del software desarrollado externamente.

- Elaborar acuerdos de nivel de servicio con los proveedores de software para ayudar a garantizar que localizan y mejoran el software vulnerable antes de su despliegue.[10]

- Despliegue nuevas herramientas para ayudar a detectar anomalías y asegurar el software. La Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA) desarrolló una herramienta llamada Sparrow para detectar actividades maliciosas en los entornos de Microsoft Azure Active Directory, Office 365 y M365. Accenture ha patentado una nueva técnica en la que blockchain podría asegurar las cadenas de suministro de software con listas de materiales de software autorreferenciadas (SBOM).[11]

- Consulte las "Mejores prácticas en la gestión de riesgos de la cadena de suministro cibernética" del Instituto Nacional de Normas y Tecnología (NIST) para trazar las cadenas de suministro, identificar los proveedores críticos y revisar las prácticas de ciberseguridad de los proveedores.

02
El ciberfraude aumenta a medida que la disrupción abre la puerta a nuevas vías y actores

¿Qué ocurre?

El fraude y el compromiso del correo electrónico empresarial (BEC) florecieron en 2020. Mientras los grupos regionales especializados en amenazas combinaban sus esfuerzos, los delincuentes tenían como objetivo los fondos de ayuda para la pandemia de la COVID-19. Las nuevas tácticas, técnicas y procedimientos (TTPs) permitieron a los actores de la amenaza explotar incluso credenciales robadas aparentemente de bajo valor de pequeñas organizaciones.

Los nuevos casos de BEC y de blanqueo de dinero muestran cómo los grupos de delincuencia organizada de África, Oriente Medio, Europa y Asia cooperan en complejas conspiraciones, desempeñando cada uno de ellos un papel especializado, como el diseño de señuelos en los idiomas de destino, el manejo de programas maliciosos, el envío de spam a los objetivos y el control de las mulas.[12]

Los actores de la amenaza también han explotado las interrupciones y los programas de ayuda relacionados con COVID 19.[13] Al principio de la pandemia, los estafadores comenzaron a identificar y utilizar cuentas bancarias corporativas inactivas para solicitar préstamos financiados por el gobierno. También aumentaron el volumen y el precio de la venta de credenciales de cuentas bancarias corporativas legítimas en la Dark Web. Además, los ciberdelincuentes han robado identidades y presentado solicitudes fraudulentas de desempleo reclamaciones de seguros [14, 15] o redirigían las prestaciones a sus propias cuentas bancarias.[16] Las estafas románticas engañaban a personas solitarias para que sirvieran de mulas para el blanqueo de dinero.[17, 18]

Aunque los sistemas antifraude mejorados ayudan a detectar anomalías en la actividad de inicio de sesión de las cuentas y en el comportamiento de los usuarios, los ciberdelincuentes están perfeccionando sus técnicas de evasión. Los mercados como Genesis ofrecen el fraude como servicio,[19] con características como credenciales en la nube, claves de interfaz de programación de aplicaciones (API) robadas, acceso a las credenciales y a la huella digital de un ordenador comprometido (dirección IP, disposición del teclado, información del navegador) y técnicas para eludir la autenticación multifactor (MFA).[20] Los actores de la amenaza, como el usuario "Zanko" en el foro Exploit, venden acceso a empresas proveedoras de servicios financieros y otros sectores, facilitando los ataques VEC.[21]

En medio de un repunte inspirado por la pandemia en el uso de aplicaciones de pago entre pares (P2P) como PayPal y Venmo, los miembros de los foros clandestinos hablan con frecuencia de utilizarlas para comerciar con credenciales robadas, blanquear dinero, retirar fondos o realizar ingeniería social.[22]

¿Por qué es importante?

Las nuevas herramientas de fraude y las redes de cooperación delictiva permiten a los delincuentes monetizar las credenciales de acceso robadas, incluso en el caso de organizaciones aparentemente pequeñas y de poco valor. Los defraudadores pueden hacerse pasar por empleados de una pequeña empresa e interactuar con los contactos anteriores y posteriores de la misma. Aunque a menudo se considera una actividad molesta, los efectos de los fraudes de correo electrónico y de otro tipo en las empresas son muy graves.

Aunque a menudo se considera una actividad molesta, los efectos del compromiso del correo electrónico comercial y otros fraudes en las empresas pueden ser significativos y pueden incluir la interrupción de las operaciones de la empresa, la disminución de los beneficios, la pérdida de ingresos fiscales, la pérdida de puestos de trabajo y el daño a la reputación

Mientras tanto, la Ley de Transparencia Corporativa autorizada por la Ley de Autorización de la Defensa Nacional de los Estados Unidos de 2021 (NDAA) exige a las empresas que revelen sus propietarios efectivos e introduce nuevos requisitos de notificación de actividades sospechosas y contra el blanqueo de capitales, lo que hace que las organizaciones de servicios financieros sean más responsables de la lucha contra el fraude cibernético. Es probable que el Tesoro de los Estados Unidos emita una normativa más específica en 2022.[23]

¿Qué debe hacer?

Para mitigar la amenaza del ciberfraude, Accenture sugiere considerar las siguientes acciones:

- Llevar a cabo una formación de concienciación de los usuarios y aplicar políticas para combatir el phishing y la ingeniería social.

- Centrar los esfuerzos en grupos vulnerables como el personal de atención al cliente y los empleados con acceso a los sistemas de pago y otros datos de alto riesgo.

- Limitar el protocolo de escritorio remoto (RDP).

- Buscar alternativas al servicio de mensajes cortos (SMS) para la autenticación de dos factores.

- Adoptar protocolos de autenticación de correo electrónico fuertes, como el informe de autenticación de mensajes de dominio (DMARC).[24, 25]

03
Las amenazas internas florecen con el trabajo a distancia

¿Qué ocurre?

Los cambios operativos relacionados con la pandemia han abierto la puerta a una mayor exposición de los bancos a las amenazas internas. Ya sea de forma malintencionada o involuntaria, los iniciados han causado interrupciones y pérdidas de datos críticos en casi la mitad de las organizaciones en una encuesta de marzo de 2020 de 457 profesionales de la ciberseguridad encargada por la empresa de análisis del comportamiento Cyberhaven.[26] Los cambios operativos relacionados con la pandemia han abierto la puerta a una mayor exposición de los bancos a las amenazas internas. Ya sea de forma malintencionada o involuntaria, los iniciados han causado interrupciones y pérdidas de datos críticos en casi la mitad de las organizaciones en una encuesta de marzo de 2020 de 457 profesionales de la ciberseguridad encargada por la empresa de análisis del comportamiento Cyberhaven.[26] El "Informe global del costo de las amenazas internas 2020" de Ponemon, basado en una encuesta realizada en 2019 de 964 profesionales de TI y de seguridad de TI en todo el mundo, atribuyó el 62% de los incidentes relacionados con la información privilegiada a la negligencia, el 23% a la información privilegiada criminal y el 14% a las credenciales robadas.[27]Con las oportunidades ampliadas en 2020 por las políticas de trabajo desde casa de la era de la pandemia, la información privilegiada maliciosa puede explotar la supervisión laxa. Los empleados desinformados pueden hacer clic en enlaces de phishing relacionados con la pandemia, mientras que los complacientes pueden utilizar herramientas de colaboración no seguras.[28]

Los esquemas de información privilegiada florecieron en 2020. Muchas instituciones describieron a trabajadores que están solicitando a empleados no bancarios que hagan parte o todo su trabajo por ellos, proporcionando sus credenciales para acceder directamente a los sistemas del banco. Muchas instituciones observan un aumento de la "actividad de inicio de sesión imposible", en la que las credenciales de una persona se registran simultáneamente o en períodos de tiempo cortos, pero desde lugares geográficamente diversos. Un empleado del proveedor de búsquedas ruso Yandex habría vendido el acceso a casi 5.000 buzones de correo de usuarios.[29] Un empleado de Tesla informó de que un conspirador criminal le ofreció un millón de dólares para que le ayudara con un esquema que incluía la distracción mediante la denegación de servicio distribuida (DDoS), la exfiltración de información y el ransomware para la extorsión.

Ese conspirador afirmó que un infiltrado en otra empresa había operado sin ser detectado durante más de tres años.[30] Los foros de delincuentes anuncian habitualmente los servicios de infiltrados en los servicios financieros, las telecomunicaciones y otros sectores.[31, 32] Los infiltrados también han facilitado el intercambio de módulos de identidad de los abonados (SIM),[33, 34, 35] lo que puede permitir la toma de posesión de cuentas.[36]

Las recientes tendencias de desinformación también pueden desempeñar un papel en el fomento del comportamiento irresponsable de los empleados y en la creación de amenazas internas.
Los empleados engañados por la desinformación y las teorías de la conspiración -incluso el personal de alto nivel, con conocimientos de TI y de seguridad- han tomado decisiones poco acertadas que podrían dañar la reputación de un empleador.[37, 38, 39]

¿Por qué es importante?

Las amenazas internas han causado daños a la marca, pérdida de ingresos y un impacto negativo en la ventaja competitiva,[40] además de exponer a las organizaciones a sanciones por filtraciones de datos.

¿Qué debe hacer?

Para minimizar el riesgo de las amenazas internas, Accenture sugiere fomentar el sentido de responsabilidad de los empleados respecto a la seguridad de la organización, así como aplicar los principios de confianza cero en las arquitecturas de seguridad.

Estos pueden incluir:

• Aplicar el privilegio mínimo para las cuentas de usuario y el acceso a los datos, crear contraseñas de un solo uso para el acceso a los datos sensibles y revocar inmediatamente el acceso de los antiguos empleados.

• Implantación de análisis del comportamiento de usuarios y entidades (UEBA) para detectar comportamientos anómalos y habilitar adecuadamente las soluciones de gestión de eventos e información de seguridad (SIEM) para detectar la descarga y el uso no autorizados de software y sitios.

• Limitar el uso de unidades USB por parte de los empleados.

• Supervisión de fuentes abiertas y de la Dark Net para descubrir posibles empleados de alto riesgo e información robada.

• Educar a los empleados con simulaciones de phishing y guías sencillas para situaciones comunes de trabajo desde casa y aclarar las sanciones por incumplimiento.

04
Los ataques de extorsión avanzan en su capacidad destructiva

¿Qué ocurre

Algunos actores del ransomware se presentan como empresas honorables, prometiendo descifrar de forma fiable el ordenador de la víctima y destruir cualquier dato robado tras recibir el rescate.[41] Sin embargo, los actores de la amenaza no siempre cumplen su parte del trato y algunos han desarrollado nuevos medios de extorsión.

• **Pseudo-ransomware y wiper malware:** La empresa de recuperación de ransomware Coveware dijo en febrero de 2021 que había observado un aumento no especificado de la "destrucción de datos al azar", lo que impedía la recuperación de los datos incluso después del pago del rescate.[42] El ransomware MacOs de ThiefQuest (EvilQuest), un ejemplo de pseudo-ransomware, exfiltraba datos pero no daba instrucciones para el pago.[43]

• **Extorsión cruel:** Los sitios de denuncia se multiplicaron, agravando la vergüenza del ransomware y la extorsión por la filtración de datos. El grupo SunCrypt añadió amenazas DDoS a la mezcla,[44, 45] mientras que los actores del ransomware Clop se dirigieron a los altos ejecutivos de las empresas violadas, aparentemente en busca de material de chantaje.[46] El mismo grupo Clop publicó datos robados de la empresa de transferencia de archivos Accellion, pero al parecer sin desplegar el ransomware.[47]

• **Promesas vacías:** Incluso después de que las víctimas paguen un rescate, los actores de la amenaza podrían no eliminar los datos robados como se había prometido.[48, 49] Algunos actores de la amenaza manipulan engañosamente los datos exfiltrados: un grupo filtró selectivamente materiales de la Agencia Europea de Medicamentos (EMA) a principios de 2021 de manera que la EMA dijo que "podría socavar la confianza en las vacunas".[50] Los actores del ransomware también podrían hacer esto.

• **Resistencia a pagar:** A finales de 2020, las víctimas de ransomware se negaron cada vez más a pagar un rescate, según Coveware; la cantidad mediana pagada cayó un 55%, pasando de 110.532 dólares en el periodo de julio a septiembre de 2020 a 49.450 dólares en el periodo de octubre a diciembre.[51]

• **Desplazamiento global del ámbito de aplicación:** Funcionarios de Estados Unidos y Canadá evaluaron que algunos ransomware sirven tanto a los servicios de inteligencia de adversarios como a los delincuentes.[52] El grupo de naciones del G7 advirtió que algunos grupos de ransomware "son vulnerables a la influencia de actores estatales" y pueden ayudar a los Estados a evadir sanciones y pagar por armas de destrucción masiva (ADM).[53]

¿Por qué es importante

Las víctimas no pueden asumir que el pago de un rescate restaurará sus datos o evitará las filtraciones. Las copias de seguridad y la recuperación de los datos cifrados ya no son suficientes.[54]

Las organizaciones podrían enfrentarse a multas en virtud del Reglamento General de Protección de Datos (RGPD) de la Unión Europea si la información confidencial se hace pública. El Departamento del Tesoro de los Estados Unidos ha advertido que las entidades de servicios financieros también podrían enfrentarse a sanciones por pagar un rescate a un grupo sancionado por los Estados Unidos o por facilitar pagos a terroristas o desarrolladores de armas de destrucción masiva,[55] con restricciones adicionales para las transferencias de criptodivisas.[56]

Evitar por completo las infecciones de ransomware -la solución ideal- es un reto. Los delincuentes compran fácilmente las credenciales de las cuentas previamente comprometidas.[57, 58] Utilizan programas maliciosos comunes, como Trickbot y Emotet, para distribuir el ransomware. Después de que la acción gubernamental paralizara esas redes de bots, algunos utilizan ahora BazarBackdoor y Buer en su lugar.[59]

No se sabe si el aparente descenso del pago de rescates continuará, haciendo que el ransomware sea menos atractivo para los delincuentes, o si los operadores de ransomware se adaptarán aún más con nuevas variantes de extorsión.

¿Qué debe hacer?

Acciones para prevenir el ransomware:

• Proteger contra los programas maliciosos precursores más comunes, como Trickbot, Emotet y BazarLoader, aplicando rápidamente parches de seguridad a los programas informáticos y formando a los empleados para que reconozcan los mensajes de correo electrónico de phishing.

• Considere la posibilidad de realizar una autoevaluación de ransomware para medir la vulnerabilidad a las operaciones de ransomware.[60]

• Segmentar los sistemas para minimizar el movimiento lateral del malware ransomware.

• Mantener copias de seguridad offline actualizadas regularmente.

• Implantar y poner en funcionamiento buenos sistemas de registro para detectar comportamientos anómalos del sistema.[61]

Acciones después de que se haya producido una violación:

• Asuma que los datos se filtrarán; construya una comprensión completa de la intrusión y del impacto medido.

• Poner en marcha un plan de comunicación de crisis.

• Colaborar con los asesores jurídicos para garantizar el cumplimiento de las obligaciones legales mediante la notificación de un incidente a las autoridades competentes.

• Desarrollar y practicar manuales de respuesta a incidentes y planes de continuidad operativa.

Acciones para predecir comportamientos futuros:

• Evaluar la credibilidad de las demandas y promesas de los actores de la amenaza.

• Piénselo dos veces antes de pagar cualquier rescate;[62, 63] manténgase al día de las sanciones legales y reglamentarias.

• Ejerza la debida diligencia para evitar facilitar el pago de rescates. Presentar un informe de actividad sospechosa si, por ejemplo, un cliente nuevo en el mundo de las criptodivisas adquiere repentinamente una gran cantidad de esta moneda.[64]

• Evaluar las mediciones de riesgo inherente y residual actuales y trabajar con la empresa para identificar cualquier riesgo que supere los niveles aceptables.

05
Las tecnologías emergentes siguen reinventando el panorama de las amenazas

Las amenazas son ágiles y las organizaciones deben seguir el ritmo, también, de las tecnologías emergentes. Estos son algunos de los protagonistas que están reinventando el panorama de las amenazas.

La computación cuántica y la ruptura del cifrado

¿Qué ocurre?

La computación cuántica y las vulnerabilidades asociadas a la criptografía amenazan la seguridad de los actuales sistemas de cifrado. Aunque las aplicaciones prácticas están a años vista, equipos de Estados Unidos, China y Francia han declarado la "supremacía cuántica". Han demostrado que los ordenadores cuánticos pueden resolver problemas de gran complejidad, como romper en un día la encriptación RSA, lo que llevaría miles de años a un ordenador ordinario.[65] El NIST está creando normas de criptografía poscuántica (PQC), cuyos borradores se someterán a comentarios públicos entre 2022 y 2023, y las normas definitivas probablemente en 2024.[66] Mientras tanto, la investigación en computación cuántica está avanzando.[67]

¿Por qué es importante?

Los adversarios son cada vez más inteligentes y capaces, al tiempo que los métodos de seguridad criptográfica más utilizados corren el riesgo de ser socavados por la computación cuántica. Las contraseñas protegidas criptográficamente necesitarán protecciones de seguridad adicionales o normas más estrictas. Muchas organizaciones pueden tener dificultades para cumplir con las nuevas normas PQC del NIST.[68] Las organizaciones pueden encontrarse experimentando con múltiples esquemas de cifrado en un esfuerzo por mantenerse al día tanto con las normas como con las nuevas vulnerabilidades.

¿Qué debe hacer?

Accenture sugiere que las organizaciones trabajen con sus socios para desarrollar la "criptoagilidad", es decir, protocolos de seguridad modulares que puedan admitir nuevos algoritmos y conjuntos criptográficos y alternar entre ellos. La criptoagilidad permite la interoperabilidad entre algoritmos nuevos y obsoletos, de modo que las organizaciones puedan abandonar las antiguas prácticas criptográficas a medida que aparezcan opciones más potentes.

Mientras se desarrollan los módulos criptográficos y el PQC, Accenture también sugiere que las organizaciones:

• Duplicar la longitud de las claves y seleccionar soluciones resistentes a la cuántica, siempre que sea posible.

• Realización de pruebas de desarrollo y evaluación comparativa para valorar la viabilidad y el impacto del PQC.

• Automatizar la rotación de la clave privada para mitigar futuras amenazas mientras se realiza la transición a PQC cuando sea posible.

• Transición a funciones hash derivadas de Keccak (como SHAKE256) que podrían proporcionar la mayor agilidad criptográfica para hashes con salidas de longitud variable.

• Investigue si los métodos de distribución de claves cuánticas (QKD) (como BB84, E91) son adecuados para su organización.

• Automatizar el desarrollo de software y las revisiones de código para encontrar nuevas vulnerabilidades en los métodos criptográficos.

• Considere la posibilidad de adoptar sistemas de autenticación que no dependan de contraseñas.

Biometría y deepfakes

¿Qué ocurre?

La autenticación biométrica para sistemas de pago en línea y sistemas conozca a su cliente (KYC) es muy prometedora, pero también presenta riesgos. Los minoristas y los procesadores de pagos han experimentado con sistemas de autorización de pagos, incluido el reconocimiento facial y los pagos sin contacto autorizados por huellas dactilares.[70] Las organizaciones también han explorado tecnologías biométricas como el reconocimiento del iris, el análisis de los latidos del corazón y el mapeo de las venas.[71]

Los bancos se enfrentan a una demanda pandémica de incorporación de nuevos clientes al banco a través del móvil; en Estados Unidos, los usuarios online representan el 64% de las aperturas de cuentas corrientes principales, según el proveedor de biometría Thales. En un procedimiento típico de incorporación al banco a través del móvil, el nuevo cliente sube un carné de conducir y una selfie; el banco comprueba la validez del carné, compara el selfie con la foto del carné y comprueba la selfie para ver si está vivo."[72, 73]

Sin embargo, los "deepfakes" alimentados por la inteligencia artificial podrían permitir a los actores de las amenazas falsificar los datos biométricos. La Fundación Carnegie para la Paz Internacional advirtió en un informe de mediados de 2020 que técnicas como el deepfake voice phishing podrían engañar a las organizaciones financieras.[74]

Mientras que las técnicas de engaño más conocidas actualmente implican métodos como la tinta conductora, las máscaras de látex y el empalme de fotogramas en la alimentación de las cámaras,[75, 76, 77] la inteligencia artificial proporciona nuevas formas de engañar las autenticaciones biométricas. Las filtraciones de los escáneres de huellas dactilares y los sistemas de reconocimiento facial han demostrado la vulnerabilidad de estas herramientas.[78], Los activistas de la privacidad y los investigadores han desarrollado aplicaciones de "camuflaje" para engañar a los sistemas de reconocimiento facial. [80] Los investigadores han entrenado el reconocimiento óptico de caracteres (OCR) para leer erróneamente la información -con aplicaciones potenciales para el fraude bancario en línea81— y han entrenado redes neuronales para ocultar la exfiltración de datos contables sensibles con técnicas esteganográficas.[82]

Accenture, junto con otras organizaciones, está desarrollando pruebas para detectar técnicas de extracción y envenenamiento de modelos, así como productos deepfake. La tecnología de detección de deepfakes sigue teniendo dificultades para evaluar si "vive" en fotos de baja resolución o con poca luz.[83, 84] Los investigadores están explorando técnicas de prevención de deepfakes -como la alteración de píxeles para impedir que un algoritmo produzca imágenes deepfake realistas- pero estas requieren más investigación.[85]

¿Por qué es importante?

Las organizaciones financieras tienen fuertes incentivos para adoptar métodos de inteligencia artificial que ahorren tiempo: Accenture evaluó en 2017 que las tecnologías de IA podrían añadir unos 1,2 millones de dólares al sector financiero para 2035.[86] Sin embargo, muchos usuarios siguen desconfiando de la IA. La Unión Europea, el NIST y otras entidades han elaborado directrices no vinculantes para una "IA de confianza" que sea imparcial, transparente, bajo control humano y segura.[87]

¿Qué debe hacer?

Accenture sugiere que, a medida que las organizaciones desarrollan modelos de aprendizaje automático, deberían considerar medidas para mejorar la seguridad. Éstas pueden incluir:

- Limitación de la cantidad de personas que pueden enviar datos a un sistema de aprendizaje automático.
- Validación y simplificación de las entradas.
- Simplificar las estructuras de los modelos para ofrecer una resistencia natural a los ejemplos adversos.
- Incluir ejemplos adversos durante la fase de entrenamiento para "inocular" el algoritmo contra ellos.[88]

Al incorporar nuevas cuentas, los bancos pueden considerar técnicas para utilizar la geolocalización, la dirección IP del dispositivo y los patrones de tecleo del usuario para conocer el comportamiento legítimo del cliente y descubrir anomalías.[89]

Preparados para la resiliencia

Los servicios financieros son la base de las economías mundiales. Para los gobiernos, la estabilidad del sector financiero es fundamental para la toma de decisiones. Para los clientes, saber que sus finanzas están seguras y su privacidad protegida es esencial para la confianza de los consumidores.

La vulnerabilidad sigue siendo alta, pero hay medidas que las instituciones financieras pueden tomar para mejorar la seguridad a largo plazo.

1. **Conozca sus operacione**s modelando las amenazas contra su cadena de valor de extremo a extremo y teniendo plenamente en cuenta los riesgos de terceros.

2. **Reforzar las defensas** a través de las personas, los procesos y la tecnología. Animar a los líderes de seguridad a ser activos en demostrar por qué la seguridad es fundamental para la estrategia empresarial.

3. **Sea ágil** para seguir el ritmo de las nuevas variantes y las tácticas mejoradas y dejar atrás a los ciberdelincuentes.

4. **Colaborar de forma proactiva** para que todos sepan cómo trabajar juntos antes, durante y después de un evento.

5. **Planificar la resiliencia** Planificar la resiliencia manteniendo altos niveles de higiene de seguridad y centrándose en los riesgos empresariales y operativos.

Contacto

Federico Tandeter

Security Lead, Sudamérica Hispana
federico.tandeter@accenture.com

Referencias

1 FBI releases the Internet Crime Complaint Center 2020 Internet Crime Report, including COVID-19 Scam Statistics, FBI News, March 17, 2021. https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics

2 Microsoft Security Team, Sophisticated cybersecurity threats demand collaborative, global response, 4 February 2021, https://www.microsoft.com/security/blog/2021/02/04/sophisticated-cybersecurity-threats-demand-collaborative-global-response/

3 In addition to publicly reported United States federal agencies, researchers have publicly listed 23 victims of end-stage malware. In addition to domains associated with United States government agencies and information, communications and technology (ICT) or cybersecurity companies, the list includes domains associated with health organizations; the European Union's Single Resolution Board, an apparent local affiliate of Fox news, and Chevron Texaco. "Finding Targeted SUNBURST Victims with pDNS," 7 January 2021, https://www.netresec.com/?page=Blog&month-2021-01&post=Finding-Targeted-SUNBURST-Victims-with-pDNS

4 Lawrence Abrams, US cities disclose data breaches after vendor's ransomware attack, 18 February 2021, https://www.bleepingcomputer.com/news/security/us-cities-disclose-data-breaches-after-vendors-ransomware-attack/

5 Julian E. Barnes and David E. Sanger, White House Announces Senior Official Is Leading Inquiry Into SolarWinds Hacking, 10 February 2021, https://www.nytimes.com/2021/02/10/us/politics/biden-russia-solarwinds-hacking.html

6 US Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, CISA, Alert (AA21-008A) Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments , 8 January 2021, https://us-cert.cisa.gov/ncas/alerts/aa21-008a

7 SITREP: Post-Compromise Authentication Abuse Tactics Expose Cloud Services, 18 December 2020, https://intelgraph.idefense.com/#/node/intelligence_alert/view/e3492fe0-a676-4c7c-a288-74e9c0563895

8 Accenture Cyber Defense, Cyber Defense Looking back to see the future: CIFR DeLorean—2021 edition , 10 February 2021, https://www.accenture.com/us-en/blogs/cyber-defense/cifr-delorean-2021-edition

9 Erik Hjelmvik, Twenty-three SUNBURST Targets Identified, 25 January 2021, https://www.netresec.com/?page=Blog&month=2021-01&post=Twenty-three-SUNBURST-Targets-Identified

10 Accenture Cyber Defense, Cyber Defense Looking back to see the future: CIFR DeLorean—2021 edition, 10 February 2021, https://www.accenture.com/us-en/blogs/cyber-defense/cifr-delorean-2021-edition

11 Alireza Salimi and Benjamin Glen McCarty, Information assurance (ia) using an integrity and identity resilient blockchain, 29 July 2020, https://patents.google.com/patent/EP3687107A1

12 US Department of Justice, Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe, 17 February 2021, https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and; David Dawkins, Nigerian Influencer Ramon 'Hushpuppi' Abbas Laundered Funds For North Korean Hackers, Says U.S. Department Of Justice, 19 Feb 2021, https://www.forbes.com/sites/daviddawkins/2021/02/19/nigerian-influencer-ramon-hushpuppi-abbas-laundered-funds-for-north-korean-hackers-says-us-department-of-justice/?sh=37d0842f1dd5; Gary Warner, Hushpuppi and Mr.Woodbery, BEC scammers: Welcome to Chicago!, 5 July 2020, http://garwarner.blogspot.com/2020/07/hushpuppi-and-mrwoodbery-bec-scammers.html; Catalin Cimpanu, Three suspects arrested in Maltese bank cyber-heist, 31 January 2020, https://www.zdnet.com/article/three-suspects-arrested-in-maltese-bank-cyber-heist/

13 Profile of Successful Cybercriminal Fingerprinting and Credential Store "Genesis," 7 Oct 2020, https://intelgraph.idefense.com/#/node/intelligence_aler/view/8396081f-8482-4c07-adb2-f03220ab8579

14 Brian Krebs, U.S. Secret Service: "Massive Fraud" Against State Unemployment Insurance Programs, 16 May 2020, https://krebsonsecurity.com/2020/05/ u-s-secret-service-massive-fraud-against-state- unemployment-insurance-programs/

15 US Attorney's Office, Southern District of New York, Six Defendants Arrested In Multiple States For Launadering Proceeds From Fraud Schemes Targeting Victims Across The United States Perpetrated By Ghana-Based Criminal Enterprise, 17 February 2021, https://www.justice.gov/usao-sdny/pr/six-defendants-arrested-multiple-states-laundering-proceeds-fraud-schemes-targeting

16 Center for Security Studies, ETH Zuerich, The Evolving Cyber Threat Landscape during the Coronavirus Crisis, December 2020, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/23122020_CyberThreatLandscapeCoronaCrisis.pdf

17 US Attorney's Office, Southern District of New York, Six Defendants Arrested In Multiple States For Laundering Proceeds From Fraud Schemes Targeting Victims Across The United States Perpetrated By Ghana-Based Criminal Enterprise, 17 February 2021, https://www.justice.gov/u-sao-sdny/pr/six-defendants- arrested-multiple-states-laundering-proceeds-fraud- schemes-targeting

18 People aged 70 or older reported median losses of US$9475 from these romance scams, according to a February 2021 US Federal Trade Commission report. Emma Fletcher, Romance scams take record dollars in 2020, 10 Feb 2021, https://www.ftc.gov/news-events/blogs/data-spotlight/2021/02/romance-scams-take-record-dollars-2020

19 Profile of Successful Cybercriminal Fingerprinting and Credential Store "Genesis" https://intelgraph.idefense.com/#/node/intelligence_alert/view/8396081f-8482-4c07-adb2-f03220ab8579

20 iDefense Explains: Cybercriminal Exploitation of Multi-Factor Authentication 19 February 2021, https:// intelgraph.idefense.com/#/node/intelligence_report/view/a03d5d06-1be9-4638-bfac-3cffc458edec

21 Zanko, https://intelgraph.idefense.com/#/node/threat_actor/view/0c09a560-50d9-468d-a494-4feae480d044; Silent Starling: BEC to VEC—The Emergence of Vendor Email Compromise, October 2019, https://www.agari.com/cyber-intelligence-research/whitepapers/silent-starling.pdf

22 Fraudulent P2P Payment App Use - Dark Web Chatter and Pandemic Lockdowns Align, 15 February 2021, https://intelgraph.idefense.com/#/node/intelligence_ alert/view/cdf50597-1c7b-4699-b653-e83889dd62b2

23 Franca Gutierrez Harris et al, 2021 AML Trends and Developments, 19 February 2021, https://wp.nyu.edu/compliance_enforcement/2021/02/19/2021-aml-trends-and-developments-part-iz-of-iii/

24 How to Fight Business Email Compromise (BEC) with Email Authentication? 22 February 2021, https://thehackernews.com/2021/02/how-to-fight- business-email-compromise.html?m=1

25 Alex Weinert, It's Time to Hang Up on Phone Transports for Authentication, 10 November 2020, https://techcommunity.microsoft.com/t5/azure-active- directory-identity/it-s-time-to-hang-up-on-phone- transports-for-authentication/ba-p/1751752

26 Cyberhaven Survey: Lack of Awareness, Cloud App Usage, and Remote Workers Create Perfect Storm for Insider Attacks, 22 April 2020, https://www.prnewswire.com/news-releases/cyberhaven-survey-lack-of- awareness-cloud-app-usage-and-remote-workers-create-perfect-storm-for-insider-attacks-301043845.html

27 Ponemon Institute, 2020 Cost of Insider Threats Global Report, April 2020, https://www.observeit.com/wp-content/uploads/2020/04/2020-Global-Cost-of-Insider-Threats-Ponemon-Report_UTD.pdf

28 SitRep: Cybersecurity Risks Related to COVID-19, 28 April 2020, https://www.accenture.com/_acnmedia/PDF-124/Accenture-SITREP-COVID-19-20200428-V8-Final-Edit.pdf

29 Yandex internal security team uncovers data breach, 12 February 2021, https://yandex.com/company/press_center/press_releases/2021/2021-12-02

30 The Evolving Threat of Initial Access Brokers: Enabling Ransomware Groups, 11 Sept 2020, https://intelgraph.idefense.com/#/node/intelligence_report/view/960c74c3-ee02-4193-8cb7-9df3e776d05e; https://www.zdnet.com/article/russian-arrested-for-trying-to-recruit-an-insider-and-hack-a-nevada-company/

31 Current Underground Trends Further Aid Malicious Insiders, https://www.darkreading.com/endpoint/how-the-dark-web-fuels-insider-threats/a/d-id/1337599, 27 April 2020

32 Actor lalalamag Seeks Insiders at Large Companies , 15 December 2020, https://intelgraph.idefense.com/#/node/malicious_event/view/86eb93f1-bb82-4458-aa8d-d33330aacb9a

33 UK Law Enforcement Arrests Eight for Celebrity SIM Swapping, 12 Feb 2021, https://intelgraph.idefense.com/#/node/intelligence_alert/view/9f67ed26-c9c2-4fc3-8315-ce6e8281f8eb

34 Brits arrested for sim swapping attacks on US celebs, accessed 1 March 2021, https://www. national-crimeagency.gov.uk/news/brits-arrested-for- sim-swapping-attacks-on-us-celebs

35 Prosecutor charges former phone company employee in SIM-swap schemeArs Technica: https://apple.news/A3EAN5wzfRtaKI1OeKmubIA

36 SIM Swap Fraud: An old but resilient enemy, 3 December 2020, https://blogs.lexisnexis.com/fraud-and-identity-in-focus/sim-swap-fraud/

37 Joe Ondrak and Nick Backovic, QAnon Key Figure Revealed as Financial Information Security Analyst from New Jersey. 10 September 2020. https://www.logically. ai/articles/qanon-key-figure-man-from-new-jersey; Kyle Rempfer, Army PSYOP officer resigned commission prior to leading group to DC protests. 11 January 2021. Army Times. https://www.armytimes.com/news/your-army/2021/01/11/army-psyop-officer-resigned-commission-prior-to-leading-group-to-dc-protests/; From Navy SEAL to Part of the Angry Mob Outside the Capitol, 26 January 2021 https://www.nytimes.com/2021/01/26/us/navy-seal-adam-newbold-capitol.html; Dave Troy, 14 February 2021, https://twitter.com/davetroy/status/1360992025848524800?s=12

38 People at the US Capitol riot are being identified and losing their jobs, updated 9 January 2021, https://www.cnn.com/2021/01/07/us/capitol-riots- people-fired-jobs-trnd/index.html

39 Behind the Nashville Bombing, a Conspiracy Theorist Stewing About the Government, 24 February 2021, https://www.nytimes.com/2021/02/24/us/anthony-warner-nashville-bombing.html

40 Communication, Cloud & Finance Apps Most Vulnerable to Insider Threat, https://www.darkreading.com/ cloud/communication-cloud-and-finance-apps-most- vulnerable-to-insider-threat/d/d-id/1337636 and conducted by Cybersecurity Insiders

41 Paul Mansfield, Tracking and combatting an evolving danger: Ransomware extortion. 15 December 2020, https://www.accenture.com/us-en/blogs/cyber- defense/evolving-danger-ransomware-extortion; Azim Khodzhibaev et al, Interview with a Lockbit Ransomware Operator, 4 January 2021, https://talos-intelligence- site.s3.amazonaws.com/production/document_files/files/000/095/481/original/010421_LockBit_Interview.pdf

42 Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands, 1 February 2021, https://www.coveware.com/blog/ransomware- marketplace-report-q4-2020

43 2021 State of Malware Report, February 2021, https://resources.malwarebytes.com/files/2021/02/ MWB_StateOfMalwareReport2021.pdf

44 Ransomware Gang Extortion Techniques Evolve in 2020 to Devastating Effect, 6 Nov 2020, https://intelgraph.idefense.com/#/node/intelligence_alert/view/f469943c-a0c5-46c8-ad91-2b0f7e84febd

45 Paul Mansfield, Tracking and combatting an evolving danger: Ransomware extortion. 15 December 2020, https://www.accenture.com/us-en/blogs/cyber-defense/evolving-danger-ransomware-extortion.

46 Catalin Cimpanu, Some ransomware gangs are going after top execs to pressure companies into paying, January 9, 2021, https://www.zdnet.com/article/some-ransomware-gangs-are-going-after-top-execs-to-pressure-companies-into-paying/

47 Andrew Moore et al, Cyber Criminals Exploit Accellion FTA for Data Theft and Extortion, 22 February 2021, https://www.fireeye.com/blog/threat-research/2021/02/accellion-fta-exploited-for-data-theft-and-extortion.html (data appeared on its CL0P^_- LEAKS site)

48 Paul Mansfield, Tracking and combatting an evolving danger: Ransomware extortion. 15 December 2020, https://www.accenture.com/us-en/blogs/cyber-defense/evolving-danger-ransomware-extortion.

49 Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands, 1 February 2021, https://www.coveware.com/blog/ransomware- marketplace-report-q4-2020

50 EMA Vaccine Data Potentially Leaked for Disinformation, 19 Jan 2021, https://intelgraph.idefense.com/#/node/intelligence_alert/view/e7fd82c5-058a-4cfb-83f0-3858af5fbae2

51 Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands, 1 February 2021, https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020. The average paid ransom declined 34%, from US$233,817 in Q3 to US$154,108 in Q4.

52 US Cybersecurity and Infrastructure Security Agency, Alert (AA20-205A) NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems, 23 July 2020, https://us-cert.cisa.gov/ncas/alerts/aa20-205a; Canadian Centre for Cyber Security, Cyber Threat Bulletin: Modern Ransomware and Its Evolution, https://cyber.gc.ca/en/ guidance/cyber-threat-bulletin-modern-ransomware- and-its-evolution, 30 November 2020.

53 Ransomware Annex to G7 Statement, 13 October 2020, https://home.treasury.gov/system/files/136/G7- Ransomware-Annex-10132020_Final.pdf

54 Melissa Michael, Episode 49| Ransomware 2.0, with Mikko Hypponen, 19 January 2021, https://blog.f-secure. com/podcast-ransomware-mikko/

55 US Treasury Department, Ransomware Advisory, 1 October 2020, https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20201001

56 Frost Brown Todd LLC, Ransomware and Bitcoin - Tax Troubles?, 10 Feb 2021, https://www.lexology.com/library/detail.aspx?g=d06237b0-9685-48c4-819a- ab0b3-fb5f551

57 Paul Mansfield and Thomas Willkan, Shady deals: The destructive relationship between network access sellers and ransomware groups, 12 October 2020, https://www.accenture.com/us-en/blogs/cyber-defense/destructive-relationship-between-network-access-sellers-and-ransomware-groups

58 Melissa Michael, Episode 49| Ransomware 2.0, with Mikko Hypponen, 19 January 2021, https://blog.f-secure.com/podcast-ransomware-mikko/

59 Accenture CTI. Threat Actor Memeos Offers Buer Loader as Malware-as-a-Service on Exploit and XSS Forums. 11 November 2020, https://intelgraph.idefense.com/#/node/intelligence_alert/view/82a84bd9-062a-44f6-a350-e8f997ee6e96

60 Ransomware Self-Assessment Tool, October 2020, Developed by the Bankers Electronic Crimes Task Force, State Bank Regulators, and the United States Secret Service, https://www.csbs.org/sites/default/files/2020-10/R-SAT_0.pdf

61 Melissa Michael, Episode 49| Ransomware 2.0, with Mikko Hypponen, 19 January 2021, https://blog.f-secure.com/podcast-ransomware-mikko/

62 Accenture Security. 2020 Cyber Threatscape Report. https://www.accenture.com/_acnmedia/PDF-137/ Accenture-2020-Cyber-Threatscape-Report. pdf#zoom=50

63 Ryan LaSalle, Securing your business and the world from ransomware , 30 November 2020, https://www.accenture.-com/us-en/blogs/security/ securing-business-and-world-from-ransomware

64 FinCen Advisory FIN-2020-A006, Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments , 1 October 2020, https:// www.fincen.gov/sites/-default/files/advisory/2020-10-01/ Advisory%20Ransomware%20FINAL%20508.pdf

65 Martin Koppe, A CNRS collaboration achieves quantum supremacy, 23 February 2021, https://news.cnrs. fr/articles/a-cnrs-collaboration-achieves-quantum- supremacy; Tom Simonite, China Stakes Its Claim to Quantum Supremacy, 12 March 2020, https://www.wired. com/story/china-stakes-claim-quantum-supremacy/

66 Dustin Moody, NIST PQC Standardization Update-Round 2 and Beyond. 23 September 2020. https://csrc.nist.gov/CSRC/media/Presentations/pqc-update-round-2-and-beyond/images-media/pqcrypto-sept2020-moody.pdf

67 Accenture, The race to crypto-agility, 2021, https://www.accenture.com/_acnmedia/PDF-145/ Accenture-Crypto-Agility-POV-v7-0

68 Dustin Moody, NIST PQC Standardization Update-Round 2 and Beyond. 23 September 2020. https://csrc.nist.gov/CSRC/media/Presentations/pqc-update-round-2-and-beyond/images-media/pqcrypto-sept2020-moody.pdf

69 Accenture, The race to crypto-agility, 2021, https://www.accenture.com/_acnmedia/PDF-145/ Accenture-Crypto-Agility-POV-v7-0

70 The Thales Group, Facial recognition: top 7 trends (tech, vendors, markets, use cases & latest news), 20 February 2021, https://www.thalesgroup.com/en/ markets/digital-identity-and-security/government/ biometrics/facial-recognition

71 Davey Winder, New Hand Gesture Technology Could Wave Goodbye To Passwords, 9 September 2019, https://www.forbes.com/sites/daveywinder/2019/09/09/ exclusive-new-hand-gesture-technology-could-wave- goodbye-to-passwords/#31aee09d5286

72 The Thales Group, Liveness in biometrics: spoofing attacks and detection, 4 December 2020, https://www. thalesgroup.com/en/markets/digital-identity-and- security/government/inspired/liveness-detection

73 FaceTec Raises Biometric Spoof Bounty to US$100,000 Total, 5 August 2020, https://findbiometrics.com/facetec-raises-biometric-spoof-bounty-to-100000-total-908051/

74 Jon Bateman, Deepfakes and Synthetic Media in the Financial System: Assessing Threat Scenarios. 1 July 2020. https://carnegieendowment.org/2020/07/08/deepfakes-and-synthetic-media-in-financial-system-assessing-threat-scenarios-pub-82237

75 The Thales Group, Liveness in biometrics: spoofing attacks and detection, 4 December 2020, https://www. thalesgroup.com/en/markets/digital-identity-and- security/government/inspired/liveness-detection

76 Critical Vulnerabilities Present in GeoVision Fingerprint Scanner and Surveillance Security Devices, iDefense Global Research Intelligence Digest for July 1, 2020, https://intelgraph.idefense.com/#/node/intelligence_ alert/view/e7b76-cea-a163-40ef-8fc3-c961b6d2f17b

77 FaceTec Raises Biometric Spoof Bounty to US$100,000 Total, 5 August 2020, https://findbiometrics.com/facetec-raises-biometric-spoof-bounty-to-100000-total-908051/

78 Acronis Security, Backdoor wide open: critical vulnerabilities uncovered in GeoVision , 26 June 2020, https://www.acronis.com/en-us/blog/posts/backdoor-wide-open-critical-vulnerabilities-uncovered-geovision

79 Zack Whittaker, Security Lapse Exposed Clearview AI Source Code, 16 April 2020, https://techcrunch.com/2020/04/16/clearview-source-code-lapse/

80 Thales, Facial recognition: top 7 trends (tech, vendors, markets, use cases & latest news), 20 February 2021, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition

81 Accenture Labs, Know Your Threat: AI Is the New Attack Surface, 2019, https://www.accenture.com/_acnmedia/Accenture/Redesign-Assets/DotCom/Documents/Global/1/Accenture-Trustworthy-AI-POV-Updated.pdf

82 Marco Schreyer, Leaking Sensitive Financial Accounting Data in Plain Sight using Deep Autoencoder Neural Networks. 13 Dec 2020. https://arxiv.org/abs/2012.07110.

83 Ruben Tolosana et al, DeepFakes Evolution: Analysis of Facial Regions and Fake Detection Performance, 2 July 2020, https://arxiv.org/pdf/2004.07532.pdf

84 Deepfake Detection Challenge, https://ai.facebook.com/datasets/dfdc/

85 Ruben Tolosana et al, DeepFakes Evolution: Analysis of Facial Regions and Fake Detection Performance, 2 July 2020, https://arxiv.org/pdf/2004.07532.pdf

86 Mark Purdy and Paul Daugherty, How AI Boosts Industry Profits and Innovation, 2017, https://www.accenture.com/-fr-fr/_acnmedia/ 36dc7f76eab444cab6a7f44017cc3997.pdf

87 Dave Nyczepir, NIST methodically releasing guidance on trustworthy AI, 12 November 2020, https://www. fedscoop.-com/nist-guidance-trustworthy-ai/; European Union, ALTAI - The Assessment List on Trustworthy Artificial Intelligence, accessed 1 March 2021, https:// futurium.ec.europa.eu-/en/european-ai-alliance/pages/ altai-assessment-list-trustworthy-artificial-intelligence

88 Malek Ben Salem, The New Cyberattack Surface: Artificial Intelligence - Know your threat, 3 August 2020, https://thecyberwire.com/stories/e690945213514cd78a5cb9dcf91e4d06/the-new-cyberattack-surface-artificial-intelligence-know-your-threat

89 The Thales Group, Risk management cloud services for an optimised digital banking experience, accessed 1 March 2021, https://www.thalesgroup.com/en/markets/digital-identity-and-security/banking-payment/digital-banking/fraud-prevention

Acerca de Accenture

Accenture es una compañía global de servicios profesionales con capacidades líderes en el ámbito digital, la nube y la seguridad. Combinando una experiencia inigualable y habilidades especializadas en más de 40 sectores, ofrecemos servicios de Estrategia y Consultoría, Interactivos, de Tecnología y de Operaciones, todo ello impulsado por la mayor red mundial de centros de Tecnología Avanzada y Operaciones Inteligentes. Nuestras 537.000 personas cumplen la promesa de la tecnología y el ingenio humano cada día, atendiendo a clientes en más de 120 países.
Adoptamos el poder del cambio para crear valor y éxito compartido para nuestros clientes, personas, accionistas, socios y comunidades. Visítenos en **www.accenture.com**

Acerca de Accenture Security

Accenture Security es un proveedor líder de servicios de ciberseguridad de extremo a extremo, incluyendo ciberdefensa avanzada, soluciones de ciberseguridad aplicada y operaciones de seguridad gestionadas. Aportamos innovación en seguridad, junto con una escala global y una capacidad de entrega mundial a través de nuestra red de centros de Tecnología Avanzada y Operaciones Inteligentes. Con la ayuda de nuestro equipo de profesionales altamente cualificados, permitimos a los clientes innovar de forma segura, crear ciberresistencia y crecer con confianza. Síganos en @AccentureSecure en Twitter o visítenos en **www.accenture.com/security**