Anexo 3 - Ejemplo de informe ejecutivo

Teniendo en cuenta la definición y características de un informe ejecutivo, en este anexo usted podrá observar algunos ejemplos reales de este tipo de documentos, asociados al tema de la ciberseguridad; por favor revise cada uno de los materiales. Es importante que considere que la estructura, forma, recursos y presentación propuesta son solo ejemplos, y no implican que usted debe desarrollar sus informes ejecutivos de la misma forma, aunque sí puede usarlos como modelo. Al revisar los informes tenga en cuenta:

- Aspectos de carácter institucional: nombres, logos, códigos, número de formato y qué incluye cada ejemplo.
- Estructura: introducción, encabezados, objetivos y listado de características, si los hay.
- Contenido: características de los activos, descripciones, etc.
- Lenguaje técnico y términos usados.

- Aberdeen Group. (2017). *Ciberseguridad: para los defensores, la clave es el tiempo*. [Resumen ejecutivo] https://www.mcafee.com/enterprise/es-mx/assets/executive-summaries/es-aberdeen-cybersecurity-2017.pdf
- Accenture Security. (2021). *2020 INFORME CYBER THREATSCAPE*. [Resumen ejecutivo] https://www.accenture.com/_acnmedia/PDF-140/Accenture-Informe-Cyber-Threatscape.pdf .

ABERDEEN GROUP

CIBERSEGURIDAD: PARA LOS DEFENSORES, LA CLAVE ES EL TIEMPO

Junio de 2017

Resumen ejecutivo

En muchas áreas de la ciberseguridad, el tiempo corre a favor de los agresores, y esta es una ventaja estratégica que los defensores deben recuperar.

En un informe reciente, Aberdeen Group, a partir de datos del *Informe sobre las investigaciones de fugas de datos (Data Breach Investigations Report)* de Verizon, desvela la distribución de los "tiempos de permanencia" de los ciberdelincuentes, es decir, el tiempo total en días que transcurre desde el ataque hasta la detección.

El tiempo de permanencia medio en el caso de fugas de datos entre 2014 y 2016 fue de aproximadamente 38 días. Esto significa que en la mitad de las fugas de datos que consiguieron su objetivo, los defensores tardaron en detectarlas entre cinco y seis semanas, o menos. En la otra mitad, tardaron ¡*cuatro años!*

¿Cómo afecta este lapso de tiempo al nivel de riesgo? El riesgo, bien entendido, se refiere a la posibilidad de que ocurra un incidente concreto, como una fuga de datos, así como a su impacto potencial en la empresa. Aberdeen ha desarrollado un análisis Montecarlo sencillo con el fin de evaluar el riesgo en función de algunas categorías de seguridad.

El informe de Aberdeen utilizó este análisis para proporcionar cuatro ejemplos que ilustran cómo pueden reducir el riesgo los defensores si consiguen recuperar la ventaja de tiempo.

El tiempo y la protección de datos

El modelo de Aberdeen descubrió que el impacto de una fuga de datos en la empresa es mayor al principio del exploit. Las funciones que permiten agilizar la detección y la respuesta reducen este impacto.

De hecho, al incorporar esta hipótesis al análisis Montecarlo de Aberdeen, se llega a la conclusión de que responder el doble de rápido a las fugas de datos puede reducir el impacto en la empresa en aproximadamente un 30 %.

El tiempo y la detección de amenazas/respuesta a incidentes

La pérdida de datos no es la única consecuencia de un incidente de seguridad. Un ataque sofisticado que afecte a la red de la empresa y a los servicios basados en esta puede tener consecuencias importantes, tanto en la disponibilidad como en el rendimiento de los sistemas de la empresa.

Tras analizar datos empíricos sobre ataques DDoS, Aberdeen descubrió que el impacto en la empresa en el caso de interrupción prolongada aumenta continuamente desde el momento del ataque hasta el momento de la reparación.

Si añadimos esta suposición al análisis Montecarlo llegamos a la conclusión de que, si la detección y la respuesta a la amenaza se realizan dos veces más rápido, el impacto en la empresa se reduce aproximadamente un 70 %.

El tiempo y la seguridad del centro de datos/la nube

El impacto del tiempo en la seguridad del centro de datos y la nube se entiende mejor si consideramos el tiempo, costo y complejidad del método tradicional de aplicación de parches a bases de datos y aplicaciones por parte de los proveedores.

Basándose en el análisis Montecarlo, Aberdeen estima que este método requiere entre 220 y 660 parches de proveedores cada año, con una media aproximada de 410. Además, este método requiere de media unas 910 horas al año de interrupción de servicio de las bases de datos y aplicaciones de la empresa.

Tras analizar el impacto de este período de inactividad en los ingresos y la productividad de los usuarios, teniendo en cuenta el costo del personal administrativo, Aberdeen calcula que con un método tradicional de aplicación de parches de proveedor puede estar entre el 1 y el 8 % de los ingresos anuales, con un 4 % aproximadamente de media.

Hay una alternativa a este enfoque: la aplicación de parches virtuales (también conocida como aplicación de parches externos o blindaje de vulnerabilidades). Con la aplicación de parches virtuales, la ventana de vulnerabilidad, es decir, el período entre la divulgación pública y la mitigación, es significativamente más breve. De esta forma, se reduce la probabilidad de que las bases de datos y aplicaciones de la empresa lleguen siquiera a sufrir ataques.

Además, la aplicación de parches virtuales reduce enormemente el tiempo de interrupción de servicio de las bases de datos y aplicaciones para llevar a cabo los procesos tradicionales de aplicación de parches de proveedores. De esta forma, se minimizan dos de los factores que más contribuyen al impacto anual en la empresa: pérdida de ingresos y pérdida de la productividad de los usuarios.

El tiempo y la seguridad de los endpoints

La importancia del tiempo en el mundo de la seguridad de los endpoints aumenta por el volumen de vulnerabilidades y exploits a los que se somete a los usuarios, por no mencionar el aumento de la sofisticación de los ataques y su carácter cada vez más focalizado.

Un problema fundamental a este respecto es el hecho alarmante de que los parches de proveedores no están disponibles hasta varios días o semanas después de la fecha de divulgación de las vulnerabilidades. Incluso cuando están disponibles, pueden pasar semanas o meses hasta que se actualicen los sistemas de la empresa.

Los profesionales de la seguridad están reduciendo la probabilidad de incidentes de endpoints gracias a una identificación más rápida y a la contención del malware de tipo zero-day. Además, están limitando el impacto que tienen en la empresa estos incidentes mediante la adopción de enfoques de respuesta flexibles que mantienen la productividad de los usuarios y mejoran la de los encargados de responder.

Mirando al futuro

Las empresas necesitan recuperar la ventaja en cuanto a tiempos para superar los riesgos de la ciberseguridad. Para ello, las organizaciones de seguridad deben priorizar las inversiones en funciones apropiadas para la realidad actual de las amenazas y las vulnerabilidades.

Concretamente, deben centrarse en las funciones diseñadas para:

- ➔ **Reducir la posibilidad y el impacto de los ataques en la empresa** reduciendo al mismo tiempo los tiempos de detección y respuesta.
- ➔ **Mantener la productividad de los usuarios** (*minimizar la fricción* en los flujos de trabajo).
- ➔ **Incrementar la productividad de los defensores** (detectar y resolver *más amenazas e incidentes, más rápidamente*).

Autor: Derek E. Brink, CISSP, Vicepresidente e investigador, Seguridad de la información y GRC de TI

Acerca de Aberdeen Group

Desde 1988, Aberdeen Group ha publicado investigaciones que ayudan a las empresas de todo el mundo a mejorar sus resultados. Nuestros analistas obtienen información basada en hechos e independiente de los proveedores de una plataforma de análisis propia, que identifica las mejores organizaciones a partir de investigaciones fundamentales llevadas a cabo por profesionales del sector. El resultado de las investigaciones sirve a cientos de miles de profesionales del sector para mejorar la toma de decisiones y la estrategia empresarial. Aberdeen Group tiene sede en Waltham, Massachusetts, Estados Unidos.


accenture
2020
INFORME CYBER THREATSCAPE
Resumen ejecutivo
Accenture Security

ÍNDICE

OBSERVACIONES DEL 2020

Durante el último año se han puesto a prueba más que nunca las estrategias y las prácticas de seguridad. Las transformaciones digitales aceleradas, las campañas oportunistas de phishing, la discontinuidad de las operaciones de seguridad de la información y las limitaciones financieras están creando la tormenta perfecta en un mundo azotado por el COVID-19. Los CISOs que entiendan estos desafíos y puedan modificar el enfoque de seguridad pueden ayudar a sus organizaciones a emerger más fuertes.

Accenture Cyber Threat Intelligence (Accenture CTI) ha creado inteligencia relevante, oportuna y factible sobre las amenazas durante más de 20 años. A partir de las adquisiciones de Context[1] en marzo de 2020 y de Deja vu Security[2], la empresa dedicada a Security of Things con sede en Seattle, en junio de 2019, Accenture Security ha obtenido 20 años más de informes de inteligencia y una profunda experiencia en técnicas, herramientas y métodos para asegurar los dispositivos conectados y las redes de Internet of Things (IoT). El equipo a cargo de la inteligencia de ciberamenazas, referido en este informe como Accenture CTI, proporciona seguridad y operaciones de negocios con soporte factible y relevante para la toma de decisiones.

Desde nuestro último informe en 2019[3], nuestros equipos de inteligencia de ciberamenazas y respuesta ante incidentes de seguridad han investigado una gran cantidad de casos sospechosos de ciber espionaje y blancos de ataque financieros. Durante estas investigaciones, los analistas y miembros de estos equipos han obtenido visibilidad de primera mano de las tácticas, técnicas y procedimientos (TTPs) que emplean algunos de los ciber-adversarios más sofisticados.

Nuestro historial de experiencia nos ayuda a desentrañar los cambios que han sufrido las ciberamenazas en los últimos 12 meses[4]. A principios de 2020, debido a la pandemia del COVID-19, la mayoría de las organizaciones en todo el mundo se enfrentaron a la necesidad de optar rápidamente por el trabajo remoto—algunas lo hicieron de acuerdo a un plan, otras reaccionaron pero sin cumplir el plan y muchas más ni siquiera tienen un plan. El trabajo remoto ha desafiado el monitoreo de seguridad de las empresas de varias maneras, desde las plataformas utilizadas para comunicarse hasta los dispositivos que las personas utilizan y las redes sobre las cuales transmiten los datos. Hemos visto un aumento en las oportunidades de ingeniería social, a medida que los grupos de ciber espionaje y ciberataques intentan aprovecharse de los empleados vulnerables, que no están familiarizados con la gestión de sus entornos tecnológicos. Las disrupciones económicas y de negocios a nivel mundial han planteado enormes desafíos financieros para las empresas. Esas presiones fluyen inevitablemente hacia las operaciones de seguridad de la información para que mantenga o aumente la cobertura, incluso bajo limitaciones presupuestarias cada vez más estrictas.

1 Accenture Acquires Context Information Security, a UK-Based Cybersecurity Consultancy, March 06, 2020. https://newsroom.accenture.com/news/accenture-acquires-context-information-security-a-uk-based-cybersecurity-consultancy.htm

2 Accenture Acquires Deja vu Security, Seattle-Based 'Security of Things' Company, June 17, 2020. https://newsroom.accenture.com/news/accenture-acquires-deja-vu-security-seattle-based-security-of-things-company.htm

3 2019 Cyber Threatscape Report, Accenture, 2019. https://www.accenture.com/gb-en/insights/security/cyber-threatscape-report

4 Estudio realizado entre junio de 2019 y junio de 2020.

Los atacantes sofisticados están empleando nuevos TTPs para lograr sus objetivos de supervivencia del régimen, aceleración económica, superioridad militar, operaciones de información y ciber espionaje de larga data. Como detallamos más adelante en este informe, nuestros analistas de inteligencia de amenazas han visto cómo los adversarios desarrollan nuevos implantes para utilizarlos contra los entornos de Outlook Web Access (OWA) y Exchange, así como métodos de comando y control más sofisticados que intentan alterar los esfuerzos de detección a través de mecanismos internos de proxy.

Los atacantes seguirán trabajando para monetizar el acceso a los datos o las redes, tal vez ahora con mayor frecuencia que antes dado que la economía sigue siendo vulnerable. Como hemos visto este año, el compromiso de la cadena de abastecimiento y las herramientas listas para usar podrían ser muy importantes, al igual que la evidencia continua de herramientas personalizadas diseñadas para evadir las defensas.

La popularidad del ransomware ha aumentado entre los atacantes, ya que el robo de datos aumenta la presión sobre las víctimas. Con ataques de ransomware que cambian las reglas del juego, como por ejemplo Maze [5], la técnica de la denuncia pública ha ganado impulso y pone en tela de juicio el debate entre el costo y la disrupción.

En un clima así, y con las organizaciones que intentan estabilizar sus operaciones actuales, los CISOs deberían implementar los controles adecuados para crear un entorno seguro. **Accenture ha identificado cuatro elementos de adaptive security** que pueden ayudar: una mentalidad segura, acceso a redes seguras, y ambientes de trabajo y de colaboración seguros. Los CISOs deberían conectarse con los líderes de negocios para planificar, preparar y practicar una mayor resiliencia de ciberseguridad, respaldada por los recursos y las inversiones adecuadas. Accenture cree que una estrategia multidimensional para gestionar la crisis, con muchos flujos de trabajo y equipos que colaboren estrechamente, generalmente de forma diaria, es la mejor manera de lograr resiliencia de ciberseguridad—y puede ayudar a proteger a las empresas de los ataques.

A continuación profundizamos las cinco tendencias de vanguardia identificadas en 2020. Estas perspectivas pueden mejorar el trabajo de los equipos de seguridad y afianzar las inversiones en tecnología de seguridad, los procesos de seguridad y la estrategia de negocios **para ayudar a lograr el nivel deseado de ciber-resiliencia.**

5 Abrams, Lawrence. "Allied Universal Breached by Maze Ransomware, Stolen Data Leaked," Bleeping Computer, November 21, 2019. https://www.bleepingcomputer.com/news/security/allied-universal-breached-by-maze-ransomware-stolen-data-leaked/

CINCO TENDENCIAS DE VANGUARDIA

El informe 2019 Cyber Threatscape advirtió que, de hecho, se realizaron fuertes inversiones en ciberseguridad. Sin embargo, a pesar de ellas, una buena inteligencia de amenazas era la prioridad para abordar la presión implacable de los ciberatacantes y los estados nacionales, y las brechas en la postura de proveedores, socios y adquisiciones respecto de la ciberdefensa.

Ahora, el **informe 2020 Cyber Threatscape revela cinco factores que influyen en el contexto de las ciberamenazas:**

01 EL COVID-19 ACELERA LA NECESIDAD DE CONTAR CON *ADAPTIVE SECURITY*

No existe una solución rápida para los problemas que presenta la pandemia. Incluso a medida que la sociedad y las empresas gestionen los aspectos humanitarios y de salud, las organizaciones necesitan lidiar con las consecuencias económicas y operativas, que están **creando desafíos financieros y presupuestarios para las operaciones de seguridad informática de las empresas** a mediano y largo plazo. La pandemia ha abierto la puerta a amenazas oportunistas, creando oportunidades de ingeniería social, como por ejemplo nuevas campañas de *phishing*. También ha puesto una presión sin precedentes en las organizaciones que lidian con mantener la continuidad del negocio, el trabajo remoto y las restricciones impuestas a los viajes. Dado que los datos continúan siendo un producto atractivo y de alto valor, los líderes de seguridad deberían considerar adoptar *adaptive security*[6]—colocando los controles y el monitoreo adecuado para crear un ambiente de trabajo seguro para sus empresas.

6 Emerge stronger with adaptive security, Accenture, June 2020. https://www.accenture.com/gb-en/insights/security/coronavirus-adaptive-security

02 TTPS NUEVOS Y SOFISTICADOS AMENAZAN LA CONTINUIDAD DE LOS NEGOCIOS

Se observa que las plataformas establecidas están bajo asedio, dado que los ciberatacantes sofisticados han apuntado agresivamente a sistemas de soporte de Microsoft Exchange[7] y OWA, como por ejemplo el Client Access Servers (CAS). Estos compromisos son un caldo de cultivo para actividades maliciosas. Los sistemas y servicios web, con gran cantidad de datos que suelen comunicarse **externamente, pueden facilitar que los adversarios oculten su tráfico en el ruido de fondo,** mientras los servicios de autenticación podrían abrir una oportunidad de recolección de credenciales para los ciberdelincuentes. Los ataques contra estas plataformas no siempre son iguales—pueden variar de despiadados a simples o sofisticados, especialmente a medida que los atacantes perfeccionan sus técnicas para explotar esas vulnerabilidades todo el tiempo. Campañas recientes contra entidades gubernamentales **han involucrado familias de malware recientemente diseñado, configurado con infraestructura de comandos y controles ruteables internamente,** probablemente diseñados también para la evasión. Estos tipos de innovación pueden desafiar a los expertos en defensa de las redes. Los atacantes podrían continuar—en la mayoría de los casos—necesitando enfatizar el sigilo y la persistencia para satisfacer sus objetivos de recopilación de inteligencia. Estas capacidades y enfoques para detectar la evasión subrayan la importancia de identificar y registrar a los principales adversarios **para luego perseguir los comportamientos específicos que éstos emplean.**

7 Accenture CTI internal research

03 LOS CIBERATAQUES ENMASCARADOS O "RUIDOSOS" COMPLICAN LA DETECCIÓN

Los ciberatacantes suelen combinar herramientas listas para usar con técnicas *living-off-the-land*—una frase que describe el abuso creativo de las herramientas fácilmente disponibles—que complican la detección y atribución. **Dado que las herramientas listas para usar ofrecen los beneficios de denegación, efectividad continua** y facilidad de uso, es probable que el uso acelerado de las mismas continúe en el futuro. El *spear phishing* también se ha intensificado. Grupos reconocidos de ciberamenazas han apuntado a organizaciones gubernamentales y empresas, generando el robo de información Estas actividades han ocurrido en Europa, Norteamérica y América Latina, con considerable **actividad dirigida hacia las economías emergentes.** Y los atacantes—grupos de ciber delincuentes cada vez más organizados—continúan tratando de comprometer las cadenas de abastecimiento de sus víctimas. Apuntan a los proveedores de servicios gestionados y de software, pero también explotan la conectividad directa entre las organizaciones que trabajan en proyecto conjuntos. La inteligencia de amenazas, continua y adaptada al perfil específico de una organización es una prioridad—desde lo estratégico, lo táctico y lo técnico—al igual que un enfoque de seguridad basado en inteligencia que se concentre en las mitigaciones más importantes para los **adversarios identificados. Las organizaciones deberían asegurarse de entender** las herramientas y técnicas comúnmente utilizadas, especialmente aquellas que involucran el uso malicioso de sistemas nativos y herramientas de pruebas de penetración, y validar que puedan ser detectadas en sus entornos.

04 EL RANSOMWARE ALIMENTA NUEVOS MODELOS DE NEGOCIOS RENTABLES Y ESCALABLES

Junto con encontrar nuevas maneras de infectar a las empresas con *ransomware* (secuestro de datos), los atacantes están encontrando nuevas maneras de influenciar a las víctimas para que paguen. En noviembre de 2019, una nueva cepa revolucionaria de ransomware conocida **como Maze afectó a una importante empresa de personal de seguridad, robó datos de la compañía y notificó a los medios—hasta finalmente liberar públicamente 700MB** de datos ante la falta de pago del rescate[8]. Este enfoque del tipo "denuncia pública" agrega presión sobre las víctimas para que paguen, incluso aunque la policía y la industria de ciberseguridad siempre han aconsejado no pagar los rescates. Solo los ciberatacantes obtienen beneficios. **Coveware, una empresa que se dedica a responder y recuperar *ransomware* para sus clientes, advirtió que en el primer trimestre de 2020** el pago promedio de un rescate aumentó hasta US$ 178.254, un 60% más que el mismo período el año anterior.[9] La situación podría convertirse en algo mucho peor. **A medida que aumentan las ganancias de los ciberatacantes, pueden innovar e invertir en ransomware más avanzado** y aprovechar las mayores vulnerabilidades que ofrece el trabajo remoto. Accenture anticipa que los ciberatacantes que emplean estas tácticas van a continuar evolucionando y proliferar para el resto de 2020 y más allá.

8 Abrams, Lawrence. "Allied Universal Breached by Maze Ransomware, Stolen Data Leaked," Bleeping Computer, November 21, 2019. https://www.bleepingcomputer.com/news/security/allied-universal-breached-by-maze-ransomware-stolen-data-leaked/

9 Ransomware Attacks Fracture Between Enterprise and Ransomware-as-a-Service in Q2 as Demands Increase, Coveware, August 3, 2020. https://www.coveware.com/blog/q2-2020-ransomware-marketplace-report

05 LA CONECTIVIDAD TIENE SUS CONSECUENCIAS

Con la exposición de los sistemas más críticos y las tecnologías poderosas e Internet que facilitan una mayor conectividad, los atacantes **encuentran nuevas maneras de explotarlas. Las organizaciones utilizan cada vez más dispositivos no probados y sin parches**—que plantean un objetivo mucho más realista y accesible. Los dispositivos conectados a Internet y cloud son mucho más populares. **Los líderes de seguridad están repeliendo los ataques usando programas públicos** de bug bounty y frameworks de detección, pero las amenazas para la Tecnología Operativa (OT) aún plantean la necesidad de contar con controles de seguridad más efectivos. Las pruebas de seguridad pueden ser costosas—y es difícil evaluar el riesgo que plantea cada dispositivo, dadas las diferencias dinámicas en las pruebas de seguridad de los mismos entre los fabricantes pequeños y los grandes. De forma lenta **pero segura se están identificando y remediando las amenazas.** Según describimos en detalle en este documento, los investigadores informaron que este año aumentaron las vulnerabilidades de OT que los proveedores abordaban a través de parches. Muchas de las clases comunes de vulnerabilidad que afectan a los dispositivos de IoT han sido solucionadas, al menos parcialmente, y el desafío es aplicar ahora este conocimiento donde sea posible. En el futuro, los líderes de seguridad deberían compartir este conocimiento y desarrollar sistemas estándar que sean simples, fáciles de integrar y soporten un escrutinio minucioso.

En este informe, Accenture CTI ofrece prácticas líderes para ayudar a enfrentar estas tendencias de vanguardia e introducir medidas de adaptive security que puedan asegurar la mentalidad, el acceso a las redes, los ambientes de trabajo y la colaboración.

Accenture CTI pretende ayudar a sus clientes, socios y miembros de la comunidad en general proporcionando esta información para que puedan mantenerse a la vanguardia de las amenazas relevantes para sus negocios, industrias y geografías.

UN FUTURO FLEXIBLE

Hace un año, nadie hubiera predicho el impacto de la crisis humanitaria y sanitaria que se apoderó del mundo en el 2020. Tampoco hubiéramos podido predecir cómo estas circunstancias sin precedentes abrirían la puerta a los ciberataques innovadores. Y a medida que los atacantes se aprovechan de la susceptibilidad de los nuevos trabajadores remotos, ofreciéndoles señuelos y trampas que imitan fuentes creíbles, los Security Operations Centers descubren que necesitan aprovechar la inteligencia de las amenazas tácticas, operativas y estratégicas para identificar las tendencias y tecnologías que amenazan la continuidad de los negocios.

Las organizaciones pueden adaptarse y **actuar para lograr un futuro más flexible y seguro si:**

Piensan "en cualquier momento, en cualquier lugar"

Asegurar a todos los usuarios, dispositivos y tráfico de red de manera consistente con el mismo nivel de efectividad, independientemente de dónde estén basados. Recordar que el acceso seguro a redes y aplicaciones es igual de rápido con seguridad como sin ella.

Son transparentes

Dar acceso a los usuarios a lo que necesitan, cuando lo necesitan. Hacer que estos cambios sean transparentes para ellos—sin pedirles que "sorteen obstáculos" para hacer su trabajo con efectividad.

Inspiran calma y confianza

Convertir a los líderes de seguridad en catalizadores del cambio usando empatía y compasión para proporcionar una respuesta más ágil. El uso de adaptive security crea confianza; por ejemplo, las organizaciones pueden usar cloud o expandir el acceso a más usuarios remotos.

Simplifican en la medida de lo posible

Considerar los servicios gestionados y automatizar cuando tenga sentido. Por ejemplo, la respuesta ante eventos de seguridad, la implementación de herramientas y la gestión de reglas pueden beneficiarse a partir de una intervención humana limitada.

Construyen para lograr resiliencia

A medida que las organizaciones tratan de emerger más fuertes, la continuidad del negocio y los planes de gestión de crisis deben adecuarse a su propósito. Los líderes del negocio deben esperar que las crisis sean más frecuentes. Precisan transformar la manera de pensar sobre la seguridad. ¿Es realmente económico hacer todo dentro de nuestras propias instalaciones? ¿Deberían aprovechar a una empresa global para asegurar sus ecosistemas? Es fundamental conectarse con los líderes del negocio para planificar, preparar y practicar mayor resiliencia de ciberseguridad, respaldada por los recursos y las inversiones adecuadas.

Al implementar estas medidas, las organizaciones pueden superar la incertidumbre, emerger más fuertes de las crisis y lograr una mayor ciber resiliencia.

ACERCA DEL INFORME

El informe 2020 Cyber Threatscape representa los resultados clave del estudio realizado por el equipo de inteligencia de ciberamenazas de Accenture, con importantes contribuciones de algunas de nuestras recientes adquisiciones, como por ejemplo Context y Deja vu Security. Abarca las tendencias relacionadas con las ciberamenazas que el equipo de Accenture CTI ha observado y analizado de junio de 2019 a junio de 2020. Proporciona un resumen de las tendencias y la manera en que Accenture CTI cree que podrían evolucionar y desarrollarse durante el año.

Este informe puede servir como referencia y complemento estratégico de los informes diarios de inteligencia, para proporcionar a los equipos de seguridad de TI y de operaciones de negocios un soporte relevante y factible para la toma de decisiones en base a inteligencia de ciberamenazas realizada por Accenture. Apunta a informar a los equipos de seguridad de TI, de operaciones de negocios y a los líderes de las organizaciones cuáles son las ciber tendencias y amenazas emergentes, con el objetivo de ayudarles a anticipar los desarrollos clave de ciberseguridad para el resto del año calendario 2020 (y en algunos casos más allá), y a proporcionar, cuando resulte apropiado, soluciones para ayudar a reducir la investigación de los riesgos de las organizaciones usando material *open-source* primario y secundario.

CONTACTOS

Joshua Ray

Managing Director, Accenture Security
joshua.a.ray@accenture.com

Josh Ray es Managing Director for Cyber Defense en Accenture Security a nivel mundial. Cuenta con más de 20 años de experiencia combinada en el área comercial, de gobierno y militar, en el campo de la ciber inteligencia, la seguridad de la información y las operaciones. Se graduó como Bachelor of Science en Tecnología de la Información en George Mason University, tiene un Executive Certificate en estrategia e innovación otorgado por el MIT Sloan School of Management y prestó servicios honorablemente como miembro de la Marina de los Estados Unidos de Norteamérica.

Howard Marshall

Managing Director, Accenture Security
howard.marshall@accenture.com

Howard Marshall es Managing Director for Cyber Threat Intelligence y lidera la práctica a nivel mundial. Antes de incorporarse a Accenture, fue FBI Deputy Assistant Director of the Cyber Readiness, Outreach, and Intelligence Branch. Se graduó como Bachelor of Arts en Ciencias Políticas y como Juris Doctorate de University of Arkansas.

Scott Bachand

Global Intelligence Director & Strategy Lead
scott.bachand@accenture.com

Scott dirige la estrategia de productos, supervisa y gestiona las operaciones de Accenture CTI a nivel global. Antes de incorporarse, Scott presto servicios como el Chief Technical Officer of Mission Cyber en Accenture Federal Services. Prestó servicios en la Fuerza Aérea de los Estados Unidos, donde desempeñó una carrera distinguida, retirándose como Technical Director of Operations of US Cyber Command (USCYBERCOM).

Valentino De Sousa

Europe & Latin America CTI Lead
valentino.de.sousa@accenture.com

Valentino De Sousa lidera Accenture CTI en Europa y América Latina. Desempeñó funciones anteriores liderando diferentes equipos de inteligencia de amenazas, responsables del análisis, investigación y desarrollo de malware, análisis de adversarios, campañas activas e indicadores líderes de ataques inminentes. Se graduó como Bachelor of Science en administración de empresas en American University of Rome y tiene un Master of Science en estudios de terrorismo otorgado por University of East London.

Jayson Jean

CTI Business Development Lead
jayson.jean@accenture.com

Jayson Jean es Director of Business Operations for Accenture CTI en la región de Norteamérica y Asia pacífico, con responsabilidad por el desarrollo de negocios del portfolio de Inteligencia de Ciberamenazas. Antes de desempeñar su función actual, sumó 14 años de experiencia desarrollando la dirección estratégica y liderando el desarrollo de productos para la gestión de vulnerabilidades en Accenture CTI.

Simon Warren

Business Development, Accenture Security
simon.warren@accenture.com

Simon lidera la práctica de Business Development for Accenture CTI en Europa y América Latina. Anteriormente lideró la práctica de Accenture CTI en Australia y antes de incorporarse a Accenture, trabajó más de 10 años en el ejército.

Colaboradores

Patton Adams, Omar Al-Shahery, Joseph Chmiel, Amy Cunliffe, Molly Day, Oliver Fay, Charlie Gardner, Gian Luca Giuliani, Samuel Goddard, Larry Karl, Paul Mansfield, Hannaire Mekaouar, Mei Nelson, Nellie Ohr, y Kathryn Orme.

Acerca de Accenture

Accenture es una empresa global de servicios profesionales con capacidades líderes en desarrollos digitales, cloud y de seguridad. Combinando experiencia inigualable y habilidades especializadas en más de 40 industrias, ofrecemos servicios de Estrategia y Consultoría, Interactive, Tecnología y Operaciones—impulsados por la red de centros de Advanced Technology e Intelligent Operations más grande del mundo. Nuestros 506,000 empleados cumplen la promesa de combinar la tecnología con el ingenio humano cada día, prestando servicios a clientes en más de 120 países. Adoptamos el poder del cambio para crear valor y compartir éxito con nuestros clientes, empleados, accionistas, socios y comunidades.

Visitanos en **www.accenture.com**

Acerca de Accenture Security

Accenture Security es proveedor líder de servicios integrales de ciberseguridad, que incluyen ciberdefensa avanzada, soluciones de ciberseguridad aplicada y operaciones de seguridad gestionada. Aportamos innovación en materia de seguridad, sumada a la escala global y a una capacidad de provisión de soluciones a nivel mundial a través de nuestra red de centros de Advanced Technology e Intelligent Operations. Con el respaldo de nuestro equipo de profesionales idóneos, ayudamos a los clientes a innovar de manera segura, desarrollar ciber resiliencia y crecer con confianza.

Seguí a @AccentureSecure en Twitter o visitanos en **www.accenture.com/security**

Dada la naturaleza inherente a la inteligencia de amenazas, el contenido incluido en el presente informe se basa en información obtenida y conocida al momento de su creación. La información vertida en el presente informe es de naturaleza general y no toma en cuenta las necesidades específicas de su ecosistema y red de TI, que puede variar y requerir la aplicación de medidas singulares. Como tal, Accenture proporciona la información y el contenido en el estado actual en que se encuentran, sin efectuar ninguna declaración ni otorgar ninguna garantía al respecto, ni aceptando la responsabilidad por ninguna acción o falta de acción en respuesta a la información contenida o referenciada en el presente. El lector es responsable de determinar si debe seguir o no cualquiera de las sugerencias, recomendaciones o posibles mitigaciones establecidas en este informe, a su total y exclusivo criterio.