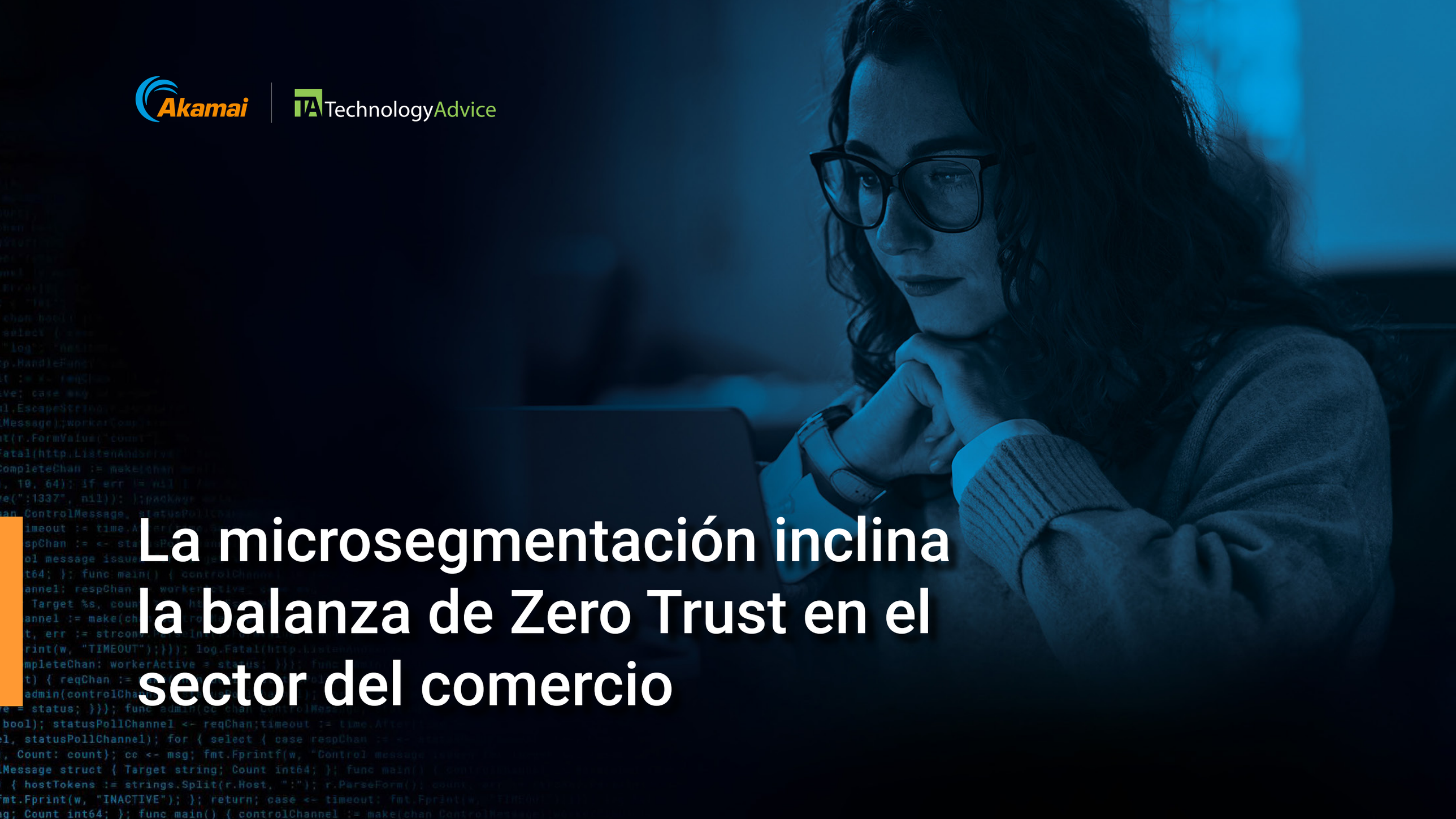


La microsegmentación inclina la balanza de Zero Trust en el sector del comercio

Las organizaciones comerciales de los sectores de retail, turismo y hostelería son objetivos atractivos para los ciberdelincuentes, las bandas de ransomware y los estafadores que pretenden monetizar datos empresariales o financieros confidenciales. Según el informe de estadísticas del sector de RH-ISAC, los tipos más comunes de información destinada al robo incluyen información de tarjetas de crédito y pagos, información de identificación personal (PII) procedente de programas de fidelización o recompensas, y propiedad intelectual.

Estas organizaciones y sus equipos de seguridad, que ya están dentro de la línea de visión de un atacante, deben hacer frente a muchos puntos de intrusión potenciales en la red que los atacantes utilizan para implementar programas de ransomware y otros tipos de malware. Todas las organizaciones se enfrentan a consecuencias derivadas de correos electrónicos de phishing, credenciales de VPN robadas y ataques de día cero, pero muchas empresas comerciales tienen que gestionar el riesgo adicional que presentan los quioscos, los dispositivos del Internet de las cosas (IoT), las tablets de las tiendas, los terminales de punto de venta (POS), la red Wi-Fi de invitados, y mucho más. Para complicar aún más la situación, cada establecimiento de retail, que debe estar abierto al público para desarrollar su actividad, expone a una empresa a una superficie de ataque física y a toda una serie de amenazas adicionales.

El valor que tienen los datos y los numerosos vectores de ataque suben el listón para los expertos en protección, que deben contrarrestar la principal causa de los accidentes: el error humano, que representa el 82 % de los incidentes de seguridad. El mayor escrutinio normativo por parte del sector de las tarjetas de pago (PCI) o las normativas gubernamentales (RGPD, SEC, etc.) añade presión y consume aún más los, ya de por sí, ajustados recursos y presupuestos de seguridad de TI.

Si bien es imposible eliminar todos los riesgos, las organizaciones comerciales de hoy en día deben adoptar la mentalidad de "asumir siempre que se ha producido una filtración" para detectar y detener rápidamente la propagación de una infección inevitable o la vulneración de las defensas perimetrales. Las soluciones de segmentación Zero Trust de Akamai facilitan y agilizan la protección de las aplicaciones, los servidores y los entornos de red de las empresas comerciales, y evitan tanto el perjudicial cifrado como la exfiltración de datos confidenciales.

La microsegmentación, una función que se respalda mejor con un enfoque definido por software, constituye la piedra angular de los marcos de seguridad Zero Trust, que ofrecen tres capacidades clave para las organizaciones comerciales. En primer lugar, la microsegmentación limita de forma natural las posibles consecuencias de una infección de ransomware bloqueando el movimiento lateral. En segundo lugar, puede ayudar a reducir el coste de lograr y mantener el cumplimiento de la norma PCI. Por último, la microsegmentación ofrece la visibilidad y la cobertura detalladas necesarias para proteger los ecosistemas modernos, más complejos, en entornos híbridos, multinube y de microservicios, así como en la infraestructura heredada.

Limite las posibles consecuencias del ransomware

Un clic en un enlace de phishing por correo electrónico, errores en la configuración de seguridad, puertos RDP abiertos o credenciales robadas proporcionan a los atacantes la oportunidad de comenzar a explorar la red en busca de las "joyas de la corona" de su organización y prepararse para ejecutar un ataque de ransomware. Las empresas que son víctimas de un evento de cifrado masivo, y de la posible doble extorsión mediante la exfiltración de datos, sufren diferentes niveles de pérdidas financieras y daños a la empresa.

Las **pérdidas comerciales directas** podrían producirse inmediatamente, ya que los pedidos online y las operaciones de la tienda se ralentizan o se detienen, y los clientes no pueden comprar artículos o hacer reservas de hoteles o aerolíneas. Es posible que las operaciones de comercio electrónico para procesamiento, gestión o envío de pedidos no puedan completarse, ya que los sistemas y servidores esenciales se vuelven inaccesibles o se desconectan en un intento de limitar la propagación de un ataque.

Las **pérdidas comerciales indirectas** comienzan con la humillación pública y el daño a la reputación de la marca si se vulneran los datos confidenciales de la empresa o de los clientes. Como táctica favorita, las bandas de ransomware hacen públicos los ataques y filtran datos como prueba del éxito de sus campañas en sitios diseñados para nombrar y avergonzar a las víctimas con el fin de extorsionarlas y aumentar la presión para que efectúen el pago del rescate. Los recientes requisitos de la SEC también obligan a las organizaciones a que le notifiquen en un plazo de cuatro días el impacto material que ha tenido el ataque en el negocio, lo que alimenta los titulares y los daños a la reputación.

Los **costes de recuperación** por los gastos legales, la respuesta a incidentes, el análisis forense de datos y la corrección de infracciones directamente relacionados con un evento de ransomware serán elevados, ya que implican un esfuerzo notable por parte de los consultores y los equipos de TI para recuperar los datos, restaurar las copias de seguridad y volver a poner los sistemas online. Sin embargo, incluso estos gastos podrían ser aún mayores por los costes de los litigios o las sanciones y multas normativas provocadas por la filtración de información confidencial. Las primas de los seguros cibernéticos pueden aumentar drásticamente, las reclamaciones por los daños provocados por el ransomware pueden denegarse o la cobertura puede interrumpirse por completo.

Hay mucho en juego, y no es de extrañar que los ataques de ransomware se citaran como la principal preocupación en materia de riesgo de los directores de seguridad de la información del sector de retail y hostelería en 2024. Tampoco es de extrañar que los responsables de seguridad estén dispuestos a invertir en controles que puedan ayudar a riesgo una vez que los atacantes hayan logrado poner pie en la empresa. Sin embargo, para que el ransomware se propague, los atacantes deben ser capaces de reaccionar y moverse lateralmente una vez que hayan obtenido acceso inicial para lograr el máximo impacto. El Informe de protección digital de Microsoft de 2022 señala que el 93 % de los incidentes de ransomware se produjeron debido a controles inadecuados del movimiento lateral que permitieron a los atacantes bloquear las aplicaciones y la infraestructura esenciales, y que la media de tiempo para que un atacante comience a moverse lateralmente desde un terminal dentro de la red corporativa es de solo 1 hora y 42 minutos.

Los datos recientes del informe de Akamai sobre el Estado de la segmentación indican que, por sectores, han sido las organizaciones de comercio electrónico las que han registrado el mayor número de ataques de ransomware en los últimos 12 meses. Por eso, los directores de seguridad de la información y los expertos en seguridad recurren a herramientas basadas en el modelo Zero Trust, como la microsegmentación, para reducir el riesgo de una posible infección de ransomware, minimizar las superficies de ataque y acabar con la cadena de exterminio del ransomware.

Al detectar y bloquear la exploración mediante el movimiento lateral, los atacantes tendrán dificultades para acceder a los activos de TI que necesitan para derivar privilegios, localizar información confidencial y propagar ataques de ransomware a gran escala. Mediante la aplicación de principios de acceso con mínimos privilegios a las cargas de trabajo esenciales en toda la infraestructura comercial, la solución de microsegmentación de Akamai, que cuenta con el reconocimiento de los analistas, ofrece una visibilidad detallada del tráfico de datos este-oeste de las aplicaciones y las cargas de trabajo, y facilita una protección exhaustiva mediante políticas definidas por software para restringir el movimiento lateral y detener a los atacantes de raíz.

Incluso las principales compañías de seguros cibernéticos comprenden el valor de la microsegmentación. Dado que el ransomware está detrás de la contratación del servicio y del aumento de las reclamaciones, muchas compañías de seguros se han visto obligadas a aumentar los requisitos de los controles de seguridad y el escrutinio, a aumentar las primas, a veces hasta un 96 % interanual, y a reducir los límites de cobertura por ransomware para contener las pérdidas. Algunas empresas incluso están siendo excluidas del mercado de los seguros cibernéticos o se les niega la cobertura por completo. Si bien los seguros cibernéticos por sí solos no evitarán una intrusión ni las consiguientes consecuencias financieras, existen controles de seguridad, como la microsegmentación, que permiten a las organizaciones cumplir con más facilidad los requisitos de suscripción más recientes.

"Con un único agente en una máquina, hemos resuelto el problema de los ataques de movimiento lateral en terminales para siempre".

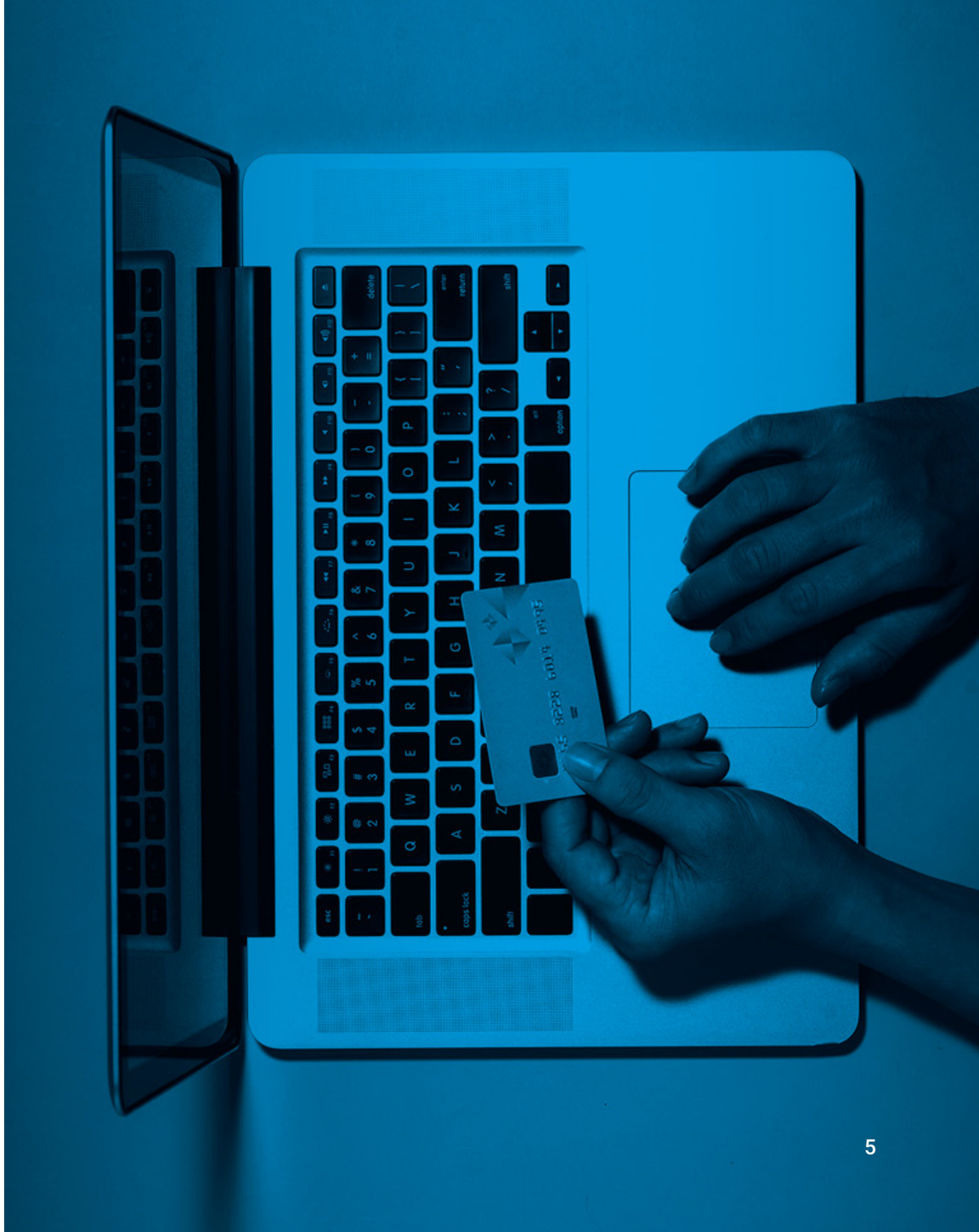
Arquitecto de infraestructura,
Fabricante global de productos para venta retail y bienes de consumo

Limite el alcance de las auditorías de cumplimiento de la norma PCI

Como bien saben las organizaciones de comercio electrónico, garantizar la conformidad con la norma PCI representa una parte considerable de los presupuestos anuales de gobierno, riesgo y cumplimiento, y puede suponer una carga significativa para los empleados a tiempo completo y los recursos de seguridad. Las normas de seguridad de datos del sector de las tarjetas de pago (PCI DSS) requieren auditorías continuas de las políticas y los controles de seguridad para proteger el entorno de datos de los titulares de tarjetas (CDE). El alcance de la norma PCI, que se refiere a la identificación de personas, procesos y tecnologías que interactúan con la seguridad de los datos de los titulares de tarjetas (CHD) o que podrían afectar a dicha seguridad, también puede aumentar drásticamente los costes asociados a la realización de una auditoría al respecto.

Aunque la segmentación de la red no es un requisito oficial de la norma PCI DSS, las organizaciones comerciales llevan años utilizando métodos tradicionales de segmentación de la red, como VLAN, ACL y firewalls internos, para reducir el alcance, el coste, el riesgo y la dificultad de mantener el cumplimiento. Sin embargo, a medida que los entornos de TI de las empresas de retail modernas se han vuelto más dinámicos en arquitecturas híbridas, multinube y de microservicios, las tecnologías y técnicas de segmentación heredadas no pueden mantener el ritmo, lo que genera sobrecarga operativa, complejidad y tiempo de inactividad de las aplicaciones, así como brechas de seguridad.

Esto se debe a que los métodos de segmentación heredados son difíciles de gestionar y mantener, y consumen recursos para garantizar que los sistemas, las redes y las aplicaciones que se encuentran dentro de los límites del CDE están protegidos y controlados correctamente. Dado que las organizaciones gestionan desde el centro de datos y la nube hasta los activos basados en contenedores, muchas carecen de una visibilidad completa de los flujos de comunicación de las aplicaciones y los sistemas, y tienen dificultades para mantener el cumplimiento con las normas de configuración de firewall que requiere la norma PCI.



Esto desemboca en prácticas de segmentación deficientes que pueden crear brechas de seguridad y dar lugar a que no se supere una auditoría de la norma PCI. Por eso, las organizaciones comerciales están recurriendo a la segmentación definida por software para aplicar más fácilmente la separación entre el CDE y los sistemas no incluidos en el ámbito de las infraestructuras, reducir el alcance de una auditoría de la norma PCI y acelerar el cumplimiento al habilitar la segmentación y la aplicación hasta el proceso de la capa 7, lo cual va mucho más allá de lo que las herramientas heredadas pueden admitir. El agente ligero de Akamai no requiere firewall, cambios de red ni reinicios en los servidores, y funciona independientemente de la infraestructura subyacente, lo que se traduce en la desaparición del tiempo de inactividad de las aplicaciones y la posibilidad de evitar los periodos de mantenimiento y control de cambios.

La segmentación definida por software desvincula la seguridad de la infraestructura subyacente y los sistemas operativos, de modo que la segmentación se puede realizar de forma independiente, sin intervención de la red ni la aplicación. Al adoptar este enfoque, las organizaciones comerciales pueden lograr una visibilidad detallada de la red y los activos en todos los entornos, con una solución que actúa como un firewall de inspección con estado distribuido para lograr una cobertura completa. Además, dado que la implementación y la gestión necesitarán menos esfuerzo y recursos, y con una mejora del 95 % aproximadamente en la productividad de SecOPS, las organizaciones pueden lograr una estrategia de seguridad más sólida y, al mismo tiempo, evitar los numerosos quebraderos de cabeza que implica el cumplimiento de la norma PCI. Como ventaja adicional, nuestra solución permite a las organizaciones comerciales aprovechar las vistas históricas y en tiempo real de su red para validar el cumplimiento durante las auditorías.

> "Con la segmentación definida por software pudimos crear y aplicar políticas de segmentación en los procesos, con lo que mejoramos significativamente nuestra estrategia de seguridad y pudimos cumplir los requisitos técnicos de PCI-DSS".
>
> Ingeniero de infraestructura sénior, The Honey Baked Ham Company

Obtenga visibilidad y cobertura en todo el Internet de las cosas (IoT) y en la infraestructura heredada

Además de detener la propagación del ransomware y gestionar los controles de seguridad para garantizar el cumplimiento de la norma PCI, las organizaciones comerciales también se enfrentan a la complejidad añadida de tener que proteger ubicaciones físicas como puntos de venta, instalaciones de producción y almacenes de distribución. En el caso de las aerolíneas, los sensores y dispositivos de IoT pueden permitir la supervisión en tiempo real y el mantenimiento predictivo de los sistemas de la aeronave para mejorar el rendimiento y la seguridad. Y las empresas de hostelería usan dispositivos del IoT para crear habitaciones de hotel inteligentes a fin de mejorar la experiencia del cliente y la eficiencia operativa.

Está claro que muchos de estos lugares y entornos contienen innumerables activos del Internet de las cosas (IoT) o de tecnología operativa (OT) que no pueden ejecutar agentes de seguridad basados en host, lo que los hace aún más propensos a las vulnerabilidades de hardware y software. El estudio de Forrester "The State of IoT Security, 2023" (El estado de la seguridad del IoT, 2023) reveló que el 33 % de los principales responsables de la seguridad a nivel global mencionaron los dispositivos de IoT como el principal objetivo de los ciberataques externos. Por lo tanto, las organizaciones deben implementar una solución de segmentación con funcionalidad sin agentes que pueda proteger los entornos de IoT y OT, y minimizar el riesgo de que un atacante aproveche una vulnerabilidad de un dispositivo en un intento de obtener acceso a la infraestructura de TI más amplia.

Este tipo de solución debe ser capaz de supervisar continuamente los nuevos dispositivos conectados y bloquear automáticamente la comunicación con la red de los dispositivos no autorizados. Con la funcionalidad integrada para reconocimiento de la huella digital, la solución de Akamai detecta y clasifica automáticamente los dispositivos conectados en grupos lógicos que sirven de base para establecer políticas de seguridad abstractas y escalables. Es posible crear políticas de segmentación para los dispositivos de IoT y OT a través de una interfaz unificada y, al igual que otras políticas, harán un seguimiento del dispositivo con huella digital, independientemente de dónde se encuentren (incluso cuando los dispositivos se desplacen a nuevas ubicaciones de red) o cuántos haya en el entorno.

Las políticas basadas en Zero Trust se aplican a través de ACL de conmutadores de red sin necesidad de un agente, lo que elimina posibles brechas que pueden originar riesgos en las implementaciones de IoT y OT. El establecimiento de estos límites seguros sigue permitiendo las conexiones necesarias a los sistemas de gestión de TI, servidores de actualización dedicados y servidores de registro para reducir las fricciones de seguridad. Nuestra solución le permite detectar, visualizar y asignar todos los sistemas de IoT y OT, así como su infraestructura de TI, para obtener una visión única de los activos de su empresa.

Además de proteger los activos de IoT/OT y otros terminales aislados, muchas organizaciones de retail confían en sistemas, servidores y aplicaciones que se ejecutan en sistemas operativos e infraestructura heredados u obsoletos a los que no se pueden aplicar parches, lo que genera un riesgo significativo. Muchos de estos servidores heredados no se pueden eliminar porque siguen generando ingresos para la organización o son la columna vertebral de la empresa, especialmente en el caso de las empresas de comercio electrónico que no se han originado en la nube. Con la cobertura y la compatibilidad más amplias, líderes del sector, los agentes de Akamai se ejecutan tanto en sistemas operativos modernos como heredados y proporcionan plena visibilidad de los flujos de red al nivel de procesos y servicios individuales para los sistemas operativos Windows y Linux, así como para terminales MacOS.

Otras soluciones solo proporcionan visibilidad parcial para sistemas operativos heredados, sin visibilidad en sistemas Microsoft Windows anteriores a Windows Server 2008 R2. Esto se debe a que el agente de las soluciones de microsegmentación tradicionales se basa en el firewall de Windows para aplicar las políticas, que solo estaba disponible en sistemas posteriores a 2002. Los agentes para sistemas Linux solo admiten visibilidad de capa 4, sin reglas en el nivel de procesos de capa 7 para entornos Linux, y dependen de iptables para aplicar las políticas. La funcionalidad Akamai Guardicore Segmentation es compatible con casi todos los sistemas operativos Windows y Linux, tanto nuevos como antiguos, ya que nuestra solución no depende de la infraestructura subyacente.

Sencillo, rápido, intuitivo y más seguro

Desde la sede central hasta la tienda de retail, y desde el centro de datos hasta la nube, y más allá, la microsegmentación es fundamental para adoptar el enfoque Zero Trust con el fin de proteger los activos de TI esenciales.

La sencillez de Akamai Guardicore Segmentation reduce drásticamente el tiempo y el nivel de esfuerzo para la implementación y la aplicación de políticas, la supervisión y la respuesta a incidentes en comparación con los métodos tradicionales de segmentación de la red, más lentos. Cualquier cambio en la política se puede implementar rápidamente y no requerirá complejos cambios en la red, lo que puede ser fundamental durante las temporadas pico de ventas, promociones, lanzamientos de productos u otros eventos importantes.

Conclusión: Al igual que no les pediría a sus clientes, invitados o pasajeros que eligieran entre calidad y seguridad, una buena solución de microsegmentación no le pedirá que elija entre seguridad y agilidad. Ha llegado el momento de dejar de segmentar de manera compleja.

¿Desea obtener más información?

Descubra cómo reducir la superficie de ataque, proteger las aplicaciones esenciales y optimizar el cumplimiento con Guardicore Segmentation de Akamai, parte de la cartera de soluciones Zero Trust de Akamai.

Más información

TechnologyAdvice | Akamai

Akamai protege la experiencia de sus clientes, su personal, sus sistemas y sus datos, ayudándole a integrar la seguridad en todo lo que crea, dondequiera que lo cree o distribuya. La visibilidad de las amenazas globales que ofrece nuestra plataforma nos permite adaptar y desarrollar su estrategia de seguridad para integrar el enfoque Zero Trust, detener el ransomware, proteger las aplicaciones y las API o combatir los ataques DDoS, y le proporciona la confianza necesaria para innovar, crecer y transformar todo su entorno. Para obtener más información acerca de las soluciones de cloud computing, seguridad y distribución de contenido de Akamai, visite akamai.com y akamai.com/blog, o siga a Akamai Technologies en X, antes conocido como Twitter, y LinkedIn.