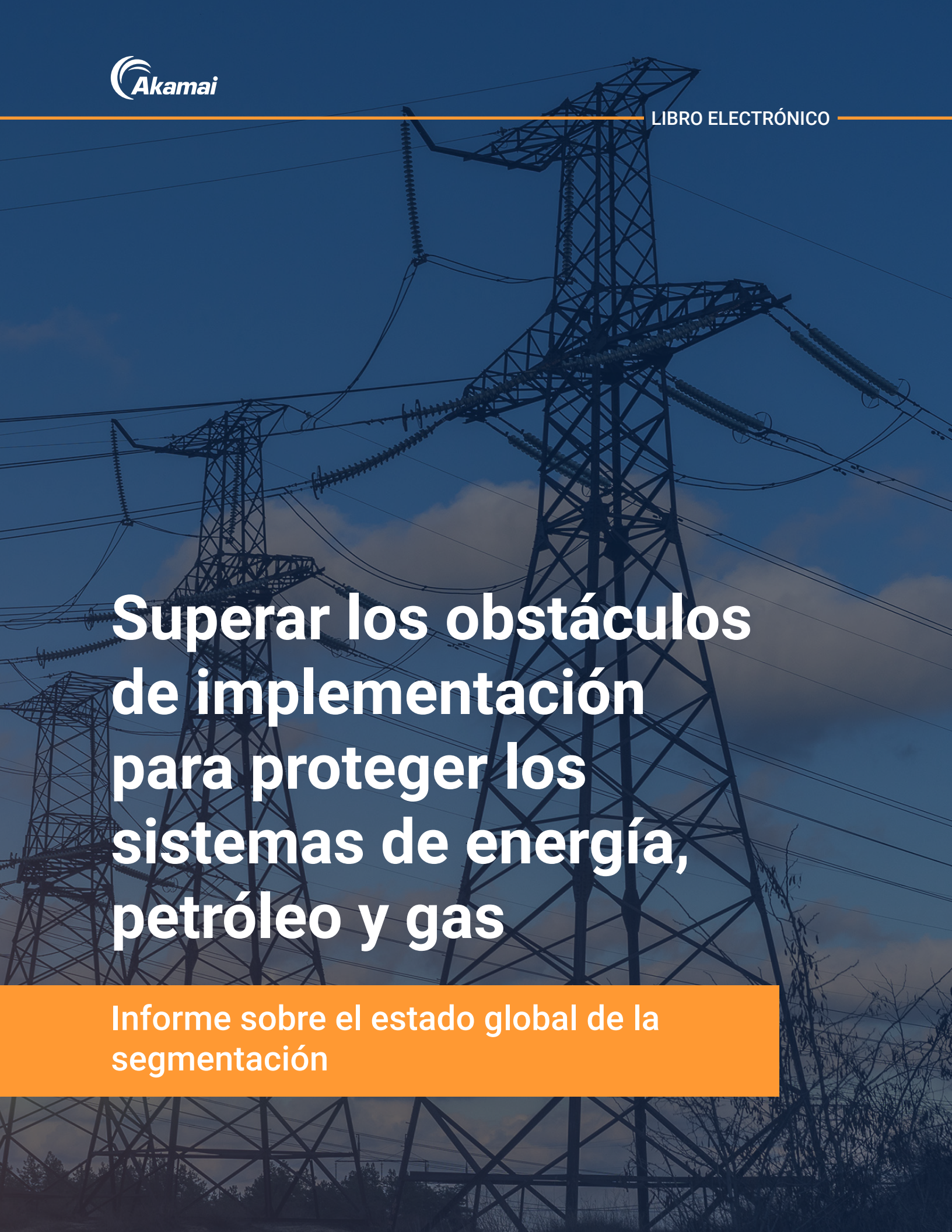

LIBRO ELECTRÓNICO

Superar los obstáculos de implementación para proteger los sistemas de energía, petróleo y gas

Informe sobre el estado global de la segmentación

Tabla de contenido

Introducción

Los departamentos de seguridad de TI y OT siempre se han enfrentado a importantes desafíos, pero en el caso de las empresas de energía, petróleo y gas, y en el sector de los servicios públicos en general, la presión es todavía mayor debido a lo esenciales que son estos servicios para las poblaciones. También es frecuente que haya conflictos regionales, presiones políticas y disputas ideológicas que agraven las dificultades e intensifiquen los peligros a los que enfrenta este sector. Sin embargo, a medida que los atacantes se vuelven más sofisticados y combinan técnicas para presentar amenazas más grandes y frecuentes, los equipos de seguridad de las empresas energéticas deben hacer frente a una presión sin precedentes. Sin sistemas conectados online, o sistemas conectados a sus redes de OT privadas, es imposible que una empresa energética funcione, y una sola filtración efectuada con éxito puede dañar considerablemente su reputación y sus resultados.

Los hallazgos de este informe señalan que las repercusiones de estos ataques se están intensificando, lo que presiona todavía más a los ejecutivos de seguridad para que elijan soluciones adecuadas que garanticen la seguridad de todo el entorno sin comprometer el rendimiento.

Y, como respuesta al considerable aumento de las amenazas de ciberseguridad a las que se enfrenta este sector y a la naturaleza esencial de los servicios que presta, los organismos reguladores y los gobiernos de todo el mundo están elaborando una serie de directrices y normativas de seguridad. Las empresas energéticas están obligadas a cumplir los estándares normativos y a garantizar el mantenimiento y la seguridad de sus servicios.

Los encuestados de las empresas del sector energético (con representación de todas las regiones, que abarcan EE. UU., LATAM, EMEA y APAC) coinciden de forma abrumadora en la eficacia de la segmentación a la hora de mantener protegidos los activos. No obstante, el progreso general en su implementación en torno a las aplicaciones y los activos empresariales esenciales es menor de lo esperado. El principal obstáculo para las empresas energéticas ha sido el aumento de los cuellos de botella que afectan al rendimiento, lo que sugiere que es posible que los equipos estén teniendo dudas a la hora de embarcarse en proyectos que podrían afectar al rendimiento, sin garantías de que no vayan a hacerlo. Es fundamental tener en cuenta que, dada la naturaleza vital de los servicios que prestan a la sociedad estas empresas, las interrupciones que experimenten sus soluciones pueden causar daños a los clientes o poner en peligro la seguridad del personal de mantenimiento.

A pesar de esta incertidumbre, se espera que el sector energético haga más hincapié en la segmentación que la mayoría de los demás sectores, lo que indica que tienen muy clara su importancia.

El progreso de la segmentación ha sido generalmente lento, pero los que han perseverado han logrado reducir enormemente su riesgo

La segmentación es buena. La microsegmentación es mejor.

La segmentación es un enfoque arquitectónico que divide una red en segmentos más pequeños con el fin de mejorar el rendimiento y la seguridad.

La microsegmentación es una técnica de seguridad que permite dividir lógicamente una red en distintos segmentos de seguridad hasta el nivel de carga de trabajo individual. De este modo, los controles de seguridad y la prestación de servicios se pueden definir para cada segmento único. Este enfoque detallado de la seguridad permite ejercer un control más preciso sobre el acceso a los datos confidenciales y su protección. Al implementar la microsegmentación, las organizaciones pueden limitar las consecuencias de una brecha de seguridad y proteger mejor su red de las ciberamenazas avanzadas. En rasgos generales, combinar la segmentación y la microsegmentación proporciona una estrategia de seguridad integral que resulta esencial para proteger los activos críticos en el complejo y dinámico panorama de amenazas actual.

Los ataques de ransomware, y sus efectos, siguen aumentando

El número de ataques de ransomware (tanto logrados como fallidos) a empresas energéticas ha aumentado notablemente en los últimos dos años, de una media de 37 en 2021 a una de 62 en 2023, y no hay motivos para sospechar que esta tendencia no vaya a mantenerse a corto plazo. Las consecuencias de estos ataques pueden tener efectos perjudiciales en la población y en las economías, como cortes del suministro eléctrico o daños a infraestructuras, lo que puede provocar que la empresa pierda credibilidad, se roben datos de individuos y empresas o incluso se ponga en riesgo la vida de las personas. Debido al aumento en la frecuencia y gravedad de los ataques de ransomware, es fundamental que estas empresas protejan sus datos y sus sistemas. Si no consiguen hacerlo, no solo ponen en riesgo a la empresa, sino que también comprometen la seguridad de las personas y las comunidades que dependen de estos servicios. A medida que los ataques de ransomware se vuelven más sofisticados, es imprescindible que las organizaciones permanezcan alerta y adopten estrategias de defensa proactivas para mitigar los posibles daños e interrupciones causados por estas amenazas maliciosas.

Número medio de ataques de ransomware en los últimos 12 meses por sector

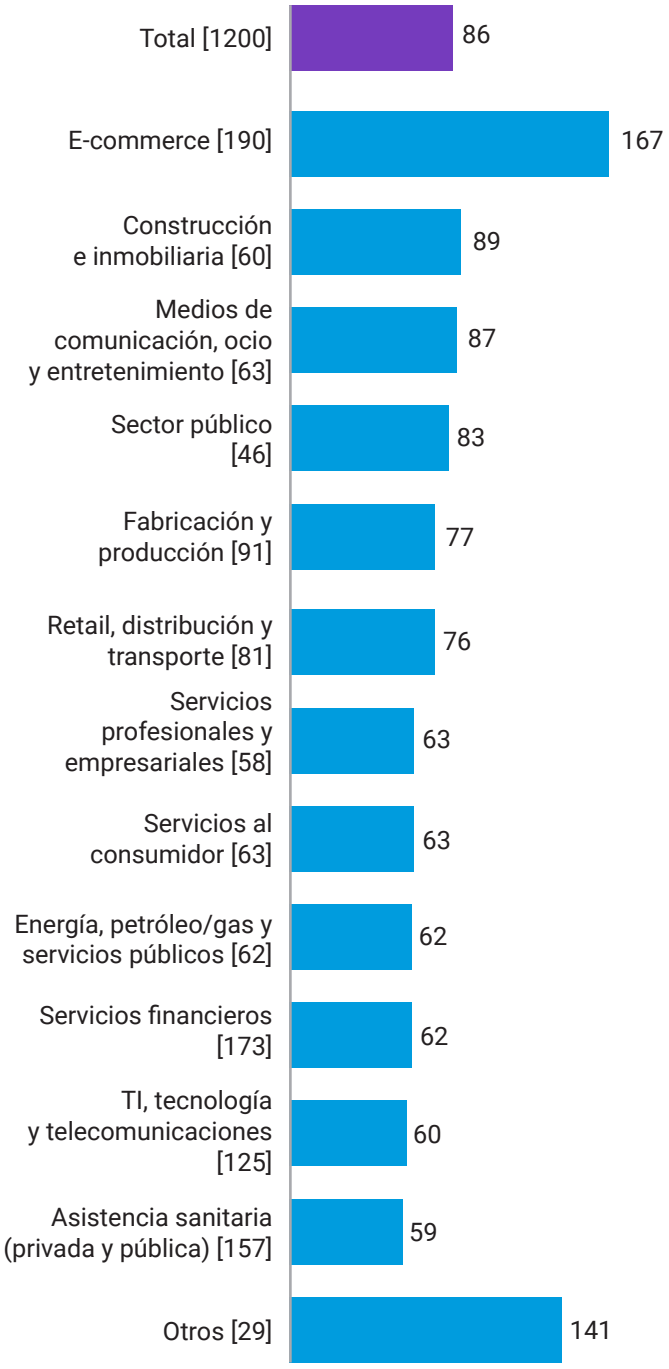

Fig. 1: ¿Cuántos ataques de ransomware se han dirigido a su organización en los últimos 12 meses (independientemente de si han tenido éxito o no)? El gráfico muestra el número medio de ataques durante los últimos 12 meses, con las cifras base divididas por sector.

Uno de los motivos de este número relativamente bajo de ataques es que el principal activo de una empresa energética tiende a ser físico (petróleo, gas, etc.) en lugar de digital (dinero o datos de clientes). Tampoco tienen fama de ser objetivos "débiles o fáciles", al contrario que otros tipos de empresas a las que no se les imponen tantas normativas, como las de los medios de comunicación o el retail. Esto significa que es más probable que los motivos de los ataques sean políticos en lugar de financieros, lo que puede verse respaldado por el hecho de que, aunque solo el 5 % de los encuestados de entre todos los sectores afirmó que su organización nunca ha detectado un ciberataque, esta cifra asciende a un 24 % si nos ceñimos a los encuestados del sector energético.

Los ataques de ransomware en el sector energético fueron más frecuentes en 2023 que en 2021, pero la gravedad de sus repercusiones es más ambigua (figura 2), ya que nuestros encuestados indicaron un aumento significativo de la pérdida de datos, pero una disminución de todos los demás problemas. Es posible que esta tendencia general se deba a la creciente concienciación sobre el valor de los datos (a los que los hackers están dando cada vez más prioridad), pero también puede ser el resultado de un mejor enfoque entre las empresas del sector energético. El número de empresas energéticas que actualizan sus estrategias o políticas de ciberseguridad al menos una vez a la semana aumentó de un mero 2 % en 2021 a un 23 % en 2023. Dado que una serie de acontecimientos mundiales (relacionados sobre todo con conflictos o con el cambio climático) están haciendo que los países presten más atención a su seguridad energética, no es de extrañar que las empresas energéticas estén reforzando sus estrategias de ciberseguridad.

Impacto del ransomware y los ciberataques en el sector energético

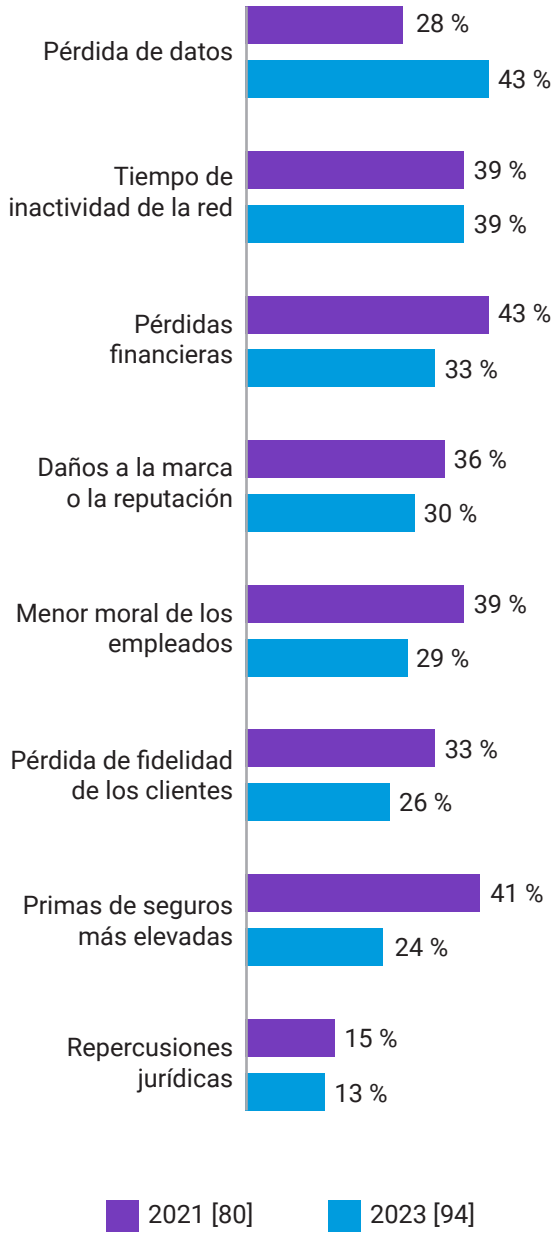

Fig. 2: En el pasado, tras detectarse ataques de ransomware u otros tipos de ciberataques, ¿cuáles de las siguientes repercusiones ha tenido en su organización? El gráfico muestra el tamaño de la base por año, sin mostrar todas las opciones de respuesta, dividido por datos históricos. Solo se incluyen datos del sector energético.

La segmentación se reconoce ampliamente como una parte importante de la arquitectura Zero Trust

Nuestros encuestados del sector energético están de acuerdo en que la segmentación es importante para garantizar la seguridad de su organización, especialmente a la hora de abordar el malware. El 66 % (una de las cifras más elevadas de entre todos los sectores) afirma que es extremadamente importante, y el 95 % cree que es fundamental para poner fin a los peores ataques.

La segmentación también desempeña un papel importante en un marco Zero Trust, y la buena noticia para las empresas energéticas es que ya se han hecho avances en este ámbito. Todas (el 100 %) están implementando o han implementado ya un marco de seguridad Zero Trust, aunque menos de la mitad (46 %) afirman que su marco Zero Trust está totalmente completo y definido y, por tanto, maduro. Se trata, por tanto, de un área en la que la segmentación puede ayudar a las empresas energéticas en su transición hacia Zero Trust. Este es el resultado de la encuesta en lo que respecta a los entornos de TI de las organizaciones, y las conclusiones relativas a los entornos de OT pueden ser diferentes debido a las tecnologías empleadas.

La mayoría de los encuestados de las empresas energéticas aspiran a ir más allá e implementar la microsegmentación, que protege las cargas de trabajo de las aplicaciones a un nivel detallado: el 88 % afirma que la microsegmentación es, al menos, una prioridad alta, y el 47 % la nombra como su prioridad principal. De entre todos los sectores, solo el 34 % afirma que la microsegmentación es su máxima prioridad, lo que demuestra que las empresas del sector energético tienden más, de media, a abogar porque se implementen soluciones de este tipo lo antes posible. Además, casi todos (98 %) los responsables de la toma de decisiones de TI y seguridad en este sector afirman que la microsegmentación ha sido adoptada por al menos una minoría, lo que indica que se trata de una solución ampliamente conocida.

Las implementaciones son lentas, pero la perseverancia produce resultados transformadores

La dura realidad: incluso con un consenso tan amplio de que la segmentación es la clave para detener los ataques, la implementación de la segmentación ha sido más lenta de lo esperado. En 2023, solo el 38 % de las empresas del sector energético ha segmentado más de dos áreas de negocio críticas (en comparación con el 30 % de 2021), mientras que el 33 % afirma haber iniciado un proyecto de segmentación de red hace dos años o más, lo que sugiere que las iniciativas se han estancado.

La lentitud de las implementaciones se explica con mayor claridad si atendemos a los principales obstáculos a los que se enfrentan los encuestados: aumento de los cuellos de botella que afectan al rendimiento (49 %), requisitos de cumplimiento (43 %) y equipo propiedad de la empresa (41 %, figura 3).

Obstáculos detectados al segmentar la red en el sector energético

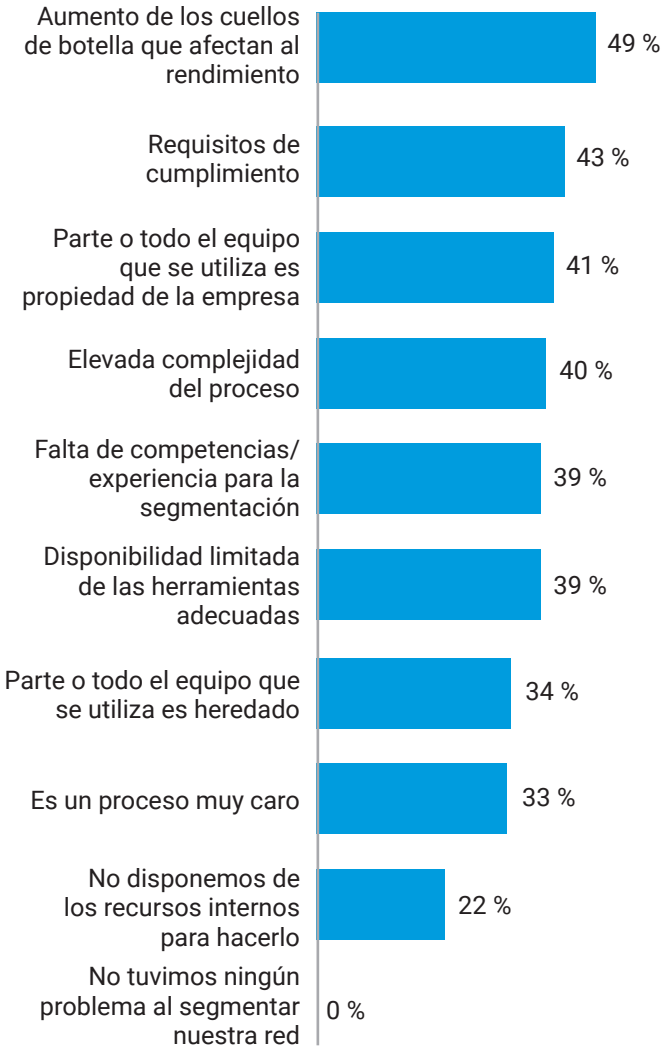

Fig. 3: Si su organización ha tenido o prevé tener problemas al segmentar la red, ¿cuáles han sido o cree que serán? El gráfico refleja un tamaño de base de 94. La pregunta solo se hizo a los encuestados que habían segmentado su red en algún momento, no se muestran todas las opciones de respuesta y solo se incluyen datos del sector energético.

Un dato alentador para el sector energético es que el 42 % afirma que su proyecto de segmentación de red comenzó como resultado de la recomendación de un directivo o una junta directiva. Se trata de la cifra más alta de entre todos los sectores (la media general es de un 28 %) y demuestra que este sector reconoce claramente la importancia de la segmentación.

Cómo una solución de microsegmentación basada en software ayuda a resolver los desafíos

La microsegmentación no solo permite una segmentación más avanzada y detallada, sino que también facilita su implementación.

Las soluciones basadas en software, como Guardicore Segmentation de Akamai, se pueden implementar rápidamente sin tener que realizar cambios físicos en la red. No es necesario volver a asignar la dirección IP a los nuevos segmentos ni preocuparse por dónde se encuentran físicamente los servidores y los dispositivos. Esto hace que la solución sea mucho más rápida y fácil de implementar que los enfoques basados en la infraestructura, como los firewalls y las VLAN. Además, dado que la solución utiliza su propio controlador en propiedad para la aplicación de políticas, funciona a la perfección en diferentes máquinas y sistemas operativos: desde servidores bare metal hasta implementaciones multinube, desde tecnología heredada como Windows Server 2003 hasta los últimos dispositivos IoT/OT y tecnología contenedorizada. Esto significa que solo necesita administrar una solución con una única interfaz para visualizar y gestionar las conexiones realizadas por diferentes sistemas operativos y dispositivos en todo el entorno, independientemente de su ubicación física.

Es importante tener en cuenta que la solución Akamai Guardicore Segmentation también se puede utilizar en entornos de OT, lo que permite aplicar la microsegmentación a redes de control privadas, sistemas operativos heredados y dispositivos IoT sin agentes.

Cómo facilita la implementación

La microsegmentación genera primero una imagen interactiva de todas las conexiones que se realizan en su entorno, lo cual es un componente fundamental para superar los principales obstáculos de la implementación. Además, Akamai ha incorporado en nuestra solución formas activas de abordar los cuellos de botella que afectan al rendimiento y los requisitos de conformidad.

Los cuellos de botella que afectan al rendimiento no surgen necesariamente de ningún motivo técnico en un sistema causado por una solución de segmentación, sino de los cuellos de botella derivados de la plantilla y que surgen por la necesidad de segmentar manualmente las áreas de negocio y, a continuación, solucionar manualmente los problemas de esas áreas cuando las cosas no funcionan. Akamai trabaja para resolver este problema (y para resolver el principal obstáculo para la implementación: la falta de experiencia) reduciendo la necesidad de realizar la segmentación manualmente y ofreciendo asistencia técnica y servicios profesionales de primer nivel. Nuestros expertos en segmentación colaboran con usted durante todo el proceso de implementación para garantizar el cumplimiento de sus objetivos de segmentación en su exclusivo entorno de TI u OT.

La asistencia para la implementación también proviene de la propia solución: sus recomendaciones de políticas basadas en IA y sus plantillas de políticas listas para usar para casos de uso comunes ahorran tiempo y clics, simplifican el flujo de trabajo, reducen el tiempo total de implementación de políticas y evitan configuraciones erróneas debido a errores humanos. Uno de nuestros clientes tenía un proyecto de segmentación detallada con una duración estimada de dos años y un presupuesto de más de 1 millón de dólares estadounidenses en costes totales; nosotros pudimos completarlo en tan solo seis semanas con un solo ingeniero, lo que redujo el coste total del proyecto en un 85 %. Esto demuestra que la segmentación detallada se puede implementar rápida y fácilmente, sin sufrir cuellos de botella.

Cómo facilita el cumplimiento

Muchos de nuestros clientes implementan nuestra solución para garantizar y certificar el cumplimiento de una serie de requisitos nacionales e internacionales, como PCI DSS, SWIFT, Sarbanes-Oxley, HIPAA, RGPD, LGPD y muchos más. Estos requisitos de conformidad suelen exigir que los datos dentro del ámbito de aplicación se separen de otros sistemas de su entorno. Aunque hacer esto puede resultar extremadamente difícil si se utilizan firewalls y VLAN, nuestra solución basada en software le permite crear segmentos específicamente para los datos dentro del ámbito de aplicación y aplicar reglas de comunicación sobre lo que puede y no puede acceder a esos datos. Con nuestro mapa visual con vistas casi en tiempo real y con perspectiva histórica, puede certificar su conformidad con estos requisitos mostrando físicamente que los usuarios y equipos no autorizados no están accediendo a los datos dentro del ámbito de aplicación.

Persevere con la solución y la asistencia adecuadas para transformar su estrategia de seguridad

La segmentación puede ser extremadamente difícil de implementar. Pero, como muestra este informe, quienes logran implementarla de forma eficaz ven reducciones masivas en su riesgo cibernético. Disponer de una segmentación adecuada limita el movimiento lateral de las amenazas y le permite reaccionar más rápido durante una filtración. En caso de que se produzca una filtración, las tareas de recuperación son seguras y tardan menos tiempo en completarse, ya que el impacto queda restringido solamente al segmento afectado.

La elección de una solución diseñada para superar los desafíos comunes de la implementación de la segmentación, y la colaboración con expertos que están a su disposición a medida que avanza en el proceso, le sitúa en la mejor posición posible para transformar su estrategia de seguridad. Además, cuantas más áreas de negocio segmente, más avanzará en su arquitectura Zero Trust, lo que le permite reducir el riesgo al que se enfrenta actualmente y garantizar una defensa de primera línea contra futuros vectores de amenazas.

Conclusiones

La segmentación y la microsegmentación son más importantes en el sector energético que en muchos otros sectores: Los responsables de la toma de decisiones de TI, seguridad de TI y OT de las empresas del sector energético (66 %) tienden más a afirmar que la segmentación de la red es extremadamente importante para garantizar la seguridad de su organización que los de las empresas de servicios al consumidor (36 %), pero menos que los del sector de TI y tecnología (73 %).

Los encuestados del sector energético tienden mucho más a declarar que la microsegmentación es la máxima prioridad (47 %) que sus homólogos de las organizaciones de servicios al consumidor (12 %), y ligeramente menos que los de las del sector público (48 %).

Las empresas del sector energético son de las que menos tienden a no haber aplicado ninguna medida de segmentación: los encuestados de empresas energéticas no tienden a afirmar que no se ha segmentado ningún activo esencial (4 %) y, aunque no llegan a alcanzar la cifra de los sectores de la construcción, los servicios al consumidor y los medios de comunicación (un 0 % en todos ellos), van por delante de las organizaciones del sector público (15 %).

Las empresas del sector energético son de las que más tienden a haber hecho el mayor avance con la segmentación: los encuestados de empresas energéticas tienden ligeramente menos a haber segmentado más de dos activos esenciales (38 %) que los del sector del retail (43 %) y mucho más que los del sector de los servicios al consumidor (3 %).

Nuestro grupo de estudio

En el estudio de investigación completo, entrevistamos a 1200 responsables de la toma de decisiones de TI y seguridad de 10 países para medir el progreso que las organizaciones han realizado en la protección de sus entornos, haciendo hincapié en el papel que desempeña la segmentación.

Se les hicieron preguntas sobre sus enfoques de seguridad de TI y sus estrategias de segmentación, así como sobre las amenazas a las que sus organizaciones se habían enfrentado en 2023. Estos datos y resultados nos ofrecen detalles sobre cómo han cambiado las estrategias de seguridad desde 2021 y en dónde se tienen que realizar mejoras todavía.

Se encuestó a personas de países de todo el mundo, como EE. UU., India, México, Brasil, Reino Unido, Francia, Alemania, China, Japón y Australia. Procedían de organizaciones con más de 1000 empleados, así como de una amplia gama de industrias y sectores.

Nota: Esta muestra difería ligeramente de la de 2021. Tamaño de las muestras: 2023: 1200 encuestados; 2021: 1000 encuestados. En 2023, también se entrevistó a personas procedentes de Australia, Japón y China. Los sectores diferían ligeramente de los de 2021.

Para elaborar este informe, analizamos las respuestas de 94 (2023) y 80 (2021) participantes que trabajan en el sector energético.

Obtenga más información sobre Akamai Guardicore Segmentation

Akamai potencia y protege la vida online. Las empresas líderes de todo el mundo eligen Akamai para crear, proteger y ofrecer sus experiencias digitales, ayudando así a millones de personas a vivir, trabajar y jugar cada día. 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. Puede obtener más información sobre las soluciones de Akamai en akamai.com y akamai.com/blog. También puede seguir a Akamai Technologies en X, anteriormente conocido como Twitter, y en LinkedIn. Publicado el 24 de mayo.

Vanson Bourne es una empresa independiente especializada en investigaciones de mercado para el sector tecnológico. La reputación de solidez y credibilidad de sus análisis se basa en principios de investigación rigurosos y en su capacidad para recabar las opiniones de los responsables de la toma de decisiones sénior en los diferentes cargos técnicos y comerciales, en todos los sectores de actividad y en los principales mercados. Para obtener más información, visite www.vansonbourne.com.