Informe técnico

Seguridad para comercios minoristas: proteja los datos del cliente y ahorre tiempo y dinero

Lo que aprenderá

Los entornos de TI de comercios minoristas enfrentan un nivel de cambios tecnológicos sin precedentes. Las tiendas tienen más requisitos y los clientes esperan tanto rendimiento como seguridad al usar los servicios en la tienda. Las entidades minoristas también enfrentan piratas cibernéticos organizados y bien financiados que aprovechan cualquier debilidad en las redes y de los sistemas de puntos de venta (POS). El resultado desafortunado de muchos ataques es el robo de datos de tarjetas de crédito y otra información de los clientes.

Este informe técnico resume los desafíos que las redes de los comercios minoristas enfrentan y describe una solución de seguridad de Cisco® que brinda una protección eficaz, actualizada y confiable: Cisco Cloud Web Security (CWS).

Aumento de las amenazas en los entornos de TI de comercios minoristas

El perfeccionamiento de las redes dentro de la tienda para que estén a la altura de las capacidades de seguridad y rendimiento necesarias no es una tarea menor. Desde el simple control sobre el acceso a Internet en la tienda hasta los complejos requisitos de cumplimiento de las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS), las organizaciones minoristas deben pensar proactivamente en cómo controlar el tráfico de red. Una solución de seguridad eficaz debe brindar control de red al mismo tiempo que se adapta a la velocidad cada vez mayor del cambio de las redes en la tienda. Lo que es más importante, debe adaptarse a la creciente complejidad de la variedad de amenazas.

La tasa de ataques y violaciones de gran notoriedad en entornos de TI de comercios minoristas sigue aumentando, a pesar de los esfuerzos de los profesionales de la empresa y de seguridad. Las víctimas van desde los 10 principales comercios minoristas según la revista Fortune hasta franquicias de restaurantes a nivel global (Figura 1). Los atacantes apuntan constantemente a los sistemas de pago. Estas violaciones han resultado en perjuicios para las marcas de las empresas y la confianza de los clientes, además de los esfuerzos de mitigación y restitución que a veces suman cientos de millones de dólares.

Figura 1. Las violaciones más grandes de datos en la historia de los EE. UU. (según el costo de los ataques)

Fuentes: Bloomberg, Privacy Rights Clearinghouse, Breach Level Index

Las experiencias de compras interactivas móviles y el Wi-Fi para usuarios temporales en las tiendas han dado lugar a un aumento de ofertas nuevas, como aplicaciones de compras y acceso a la red en la tienda. Aunque esos servicios en la tienda pueden brindar un valor concreto para el cliente, también aumentan la complejidad de las redes de las tiendas y agregan más presión a los recursos de TI actuales. Los servicios en línea amplían el campo de ataque y dejan a las empresas más expuestas a quienes buscan y aprovechan vulnerabilidades de red. Por eso es importante que los comercios minoristas inviertan en la protección de los datos del cliente, tanto dentro de las tiendas como en la sede central.

Otra tendencia de TI que los comerciantes minoristas deben manejar es Internet de las cosas (IdC). IdC representa una red de objetos físicos conectados a Internet con la tecnología integrada, que interactúa con la red interna y el entorno externo. Por ejemplo, un comerciante minorista podría difundir información relevante en tiempo real acerca de los productos en los dispositivos móviles de los consumidores interesados, en función de la información contextual del cliente recopilada a partir de los productos dentro de la tienda.

Otras aplicaciones empresariales de IdC incluyen control del inventario entrante en tiempo real a través de etiquetas de radiofrecuencia o acceso para proveedores de la cadena de suministro a datos y sistemas internos a fin de agilizar las operaciones. La amplia gama de dispositivos en IdC aumentará la cantidad de tecnologías fundamentales dentro de la propia tienda. En muchos casos, la seguridad no está incorporada en estos dispositivos y quizás se agregue solamente a último momento.

Dado que los márgenes de ganancias plantean un desafío en todo el sector minorista, las organizaciones enfrentan la difícil realidad de abordar un entorno de amenazas en constante evolución y, al mismo tiempo, brindar experiencias de compra innovadoras y personalizadas para los clientes. Cada vez es más necesario actualizar los sistemas de POS o invertir en tecnologías de seguridad para controlar el riesgo de pérdida de datos. En respuesta a un entorno de amenazas cada vez mayor, el sector minorista no se queda de brazos cruzados. Recientemente las organizaciones han aunado esfuerzos para desarrollar la iniciativa Retail Cyber Intelligence Sharing Center (R-CISC).

El punto débil de los comercios minoristas

En 2013 las organizaciones minoristas y los restaurantes fueron el segundo sector que recibió más ataques, según el Informe de investigaciones sobre violaciones de datos de Verizon de ese año (Verizon Data Breach Investigations Report). Aún si los clientes continúan comprando en un comercio minorista que sufrió un ataque, un informe de Retail News Insider sugiere que es probable que comiencen a usar efectivo en lugar de crédito, lo que conduce a una disminución de lo que gastan.

Según un informe de 2014 de Interactions Consumer Experience Marketing, está demostrado que los atacantes no son tan creativos cuando apuntan a las organizaciones minoristas. "En comparación con otros sectores, los atacantes usan relativamente pocos métodos para obtener datos cuando atacan a las organizaciones minoristas", concluyó el grupo. En los ataques minoristas, el 97% involucró la manipulación de sistemas de pago.

Las organizaciones minoristas enfrentan un desafío importante en la detección de violaciones a la seguridad. Generalmente, el malware se encuentra en el entorno de TI de comercios minoristas hasta que terceros (generalmente agentes de seguridad o de detección de fraudes) descubren indicadores de actividad inusual. Según un estudio de tres años realizado por Verizon Enterprise Solutions citado en un artículo de 2014 de Bloomberg Businessweek, solo el 31% de las veces, en promedio, las empresas descubren violaciones mediante supervisiones que realizan ellas mismas. Para los comercios minoristas es el 5%.

La Tabla 1 muestra cuatro ejemplos de las violaciones más importantes informadas en 2014, junto con el período en que el malware se encontraba en el entorno de TI antes de la detección.

Tabla 1. Características de las violaciones de la red más importantes de 2014

Ataque	Período de tiempo	Método de ataque	Punto de falla
Tienda de bebidas alcohólicas de EE. UU.	17 meses	“Malware con tasas de tráfico bajas y lentas”	Tecnología
Cadena de tiendas de artesanías de EE. UU y Canadá	De 8 a 9 meses	Sistemas de POS modificados	Proceso
Cadena de tiendas de artículos para el hogar de EE. UU y Canadá	6 meses	Malware personalizado y diseñado para evadir los registros de detección y ataques	La seguridad no es una prioridad; funciones del producto sin uso
Casa de cambio minoristas en línea	3 meses	Base de datos pirateada	Personas y tecnología

Fuentes: Sophos, Bank Information Security, Krebs on Security, Bloomberg News, Private WiFi.com y Huffington Post

Aumento de las capacidades y los requisitos de TI funcionales

Los entornos de red de TI para comercios minoristas son cada vez más complejos. Además, cada vez es más difícil administrarlos. En el sector de TI, la creciente escasez de habilidades agrava la dificultad para abordar estos entornos conectados a Internet en la tienda. Para combatir la escasez, especialmente, en la seguridad cibernética, los grupos de TI centralizan la administración y el funcionamiento del entorno de TI de los comercios minoristas.

Una de las áreas que plantean el mayor desafío en cuanto a la complejidad se encuentra dentro de las redes en la tienda usadas inicialmente para conectar las terminales de punto de venta (POS) con los servidores de back-end y la red WAN corporativa. Estas redes en la tienda, previstas para manejar tráfico lento, ahora prestan servicios a muchas otras aplicaciones, que incluyen marketing, intranet y acceso a Internet para los empleados, casos de uso de IdC, sistemas de videovigilancia y alarma y Wi-Fi para usuarios temporales.

Surgirán constantemente más tecnologías atractivas en línea para los comercios minoristas, lo que ofrece un valor increíble para los clientes y las convierte en recursos imprescindibles a fin de que los minoristas las implementen en sus tiendas. Al mismo tiempo, estas soluciones consumirán más ancho de banda y requerirán más procesamiento de datos. Lo que complica aún más la cuestión es la dificultad para predecir los requisitos de ancho de banda que varían según las instalaciones. Estos requisitos no solo dependen del tamaño de cada tienda, sino también del uso de diversas tecnologías.

El modelo de seguridad de la mayoría de las redes en la tienda se diseñó inicialmente para proteger el tráfico de red interno. Las tiendas ahora son compatibles con comunicaciones fuera de la red doméstica, incluidas las conexiones con los partners comerciales, los proveedores e Internet.

Brindar seguridad adecuada requerirá que las organizaciones implementen nuevos controles de detección y prevención en redes en la tienda que puedan ofrecer una separación más sofisticada de dispositivos y usuarios a nivel de red, controles avanzados de uso de red y cumplimiento de políticas de uso aceptable. Dados los tipos de malware y ataques que se observan en el sector minorista, se entiende que todos los dispositivos conectados a las redes minoristas se ejecutan en un entorno hostil.

¿Cómo puede definirse el entorno de amenazas? Principalmente, los atacantes apuntan al camino que ofrece menos resistencia para introducirse en un entorno. Esto generalmente incluye poner el foco en los terminales de POS. Desafortunadamente, muchos de los principales sistemas de POS se desarrollan con componentes de software, sistemas operativos y hardware básicos que se ven fácilmente comprometidos cuando sufren ataques poco sofisticados. Incluso si los proveedores de POS implementan revisiones en los sistemas correctamente, el costo operativo de aplicarlas en cientos de miles de dispositivos es significativo y, generalmente, requiere actualizaciones manuales.

Las conexiones tradicionales de sistemas de POS a Internet pública incitan al riesgo. Dicha configuración posibilita las operaciones remotas, en los casos en que los sistemas de back-end de POS se encuentran en otras instalaciones y cuando no se puede dar soporte remoto. Sin embargo, los grupos operativos deben elegir entre la optimización de la administración de los dispositivos y la reducción del riesgo de ataques de red. Esto no es un intercambio justo ni necesario.

Las gateways de seguridad en la web tradicionales requieren la instalación de una gateway centralizada en la oficina principal. Cada tienda o sucursal envía todo el tráfico al punto de agregación central para su inspección antes de salir a Internet. Dado el mayor tráfico (entrante y saliente) en las tiendas, este enfoque consume grandes cantidades de ancho de banda limitado. El cumplimiento es también un factor significativo que se debe considerar, ya que la TI de los comercios minoristas se mantiene dentro del alcance de PCI DSS. Para cumplir con la normativa y aprobar las evaluaciones anuales, las organizaciones deben implementar controles de red proactivos para proteger las conexiones y ayudar a garantizar la seguridad continua de los sistemas que procesan los datos de los titulares de tarjetas de crédito.

En resumen, es habitual que las redes en la tienda se hayan desarrollado con el solo propósito de conectar sistemas de POS con WAN corporativas. Estas soluciones suelen implementarse dentro del perímetro de seguridad de la organización. Las infracciones de seguridad recientes en organizaciones minoristas que involucran sistemas de POS sugieren que esta arquitectura de red ya no es viable para desarrollar ni operar redes en la tienda.

Brechas comunes en entornos de TI

Debido a las presiones sobre los comercios minoristas para que aborden los problemas de seguridad lo antes posible, las organizaciones minoristas suelen suponer que una solución específica protegerá los recursos importantes. Sin embargo, un modelo de seguridad unificado debe proporcionar más que una solución específica y debe implementar los controles de seguridad de red suficientes para enfrentar los problemas actuales y cumplir con los requisitos futuros.

La diferencia entre una solución específica y una solución de seguridad integral se ejemplifica mediante la implementación de conectividad a Internet directa para las tiendas. Cuando se implementa una conexión a Internet directa, un firewall nuevo se agrega para proteger la red de la tienda. El firewall se implementa en uno de dos modelos.

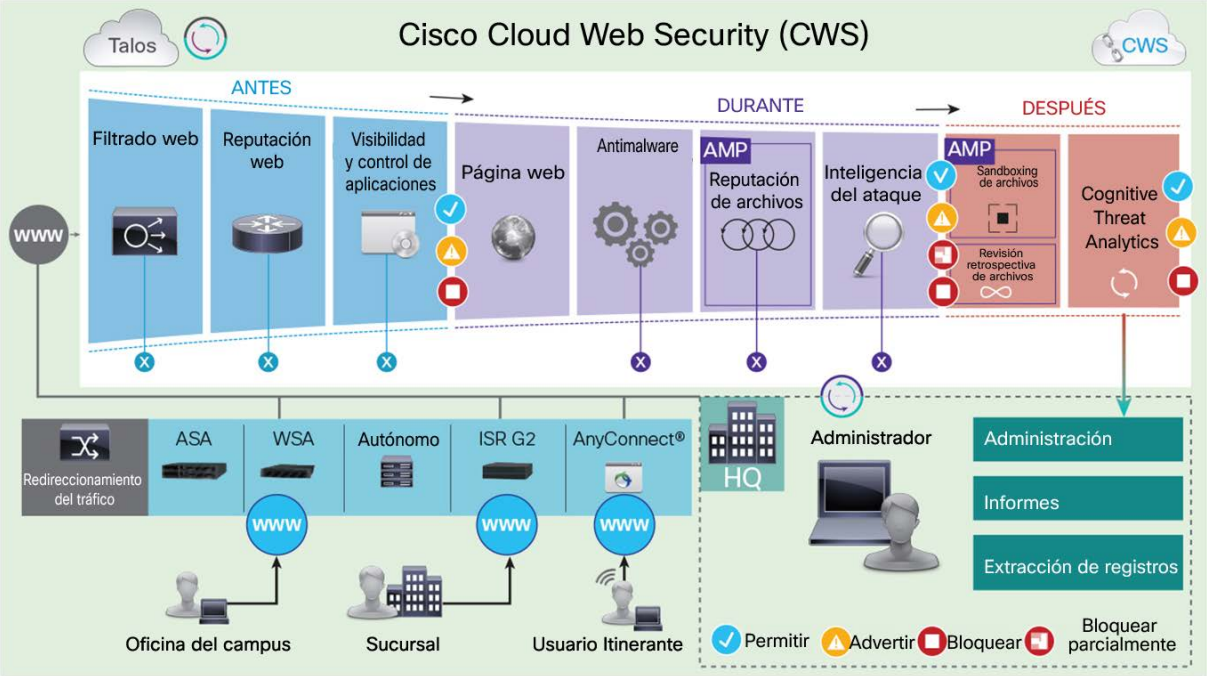
1. Las reglas se pueden configurar en el router WAN para transferir el tráfico procedente de Internet al firewall nuevo.
2. Los dispositivos conectados a la red en la tienda pueden usar el firewall como gateway predeterminada y, de ese modo, se eliminan el control o la supervisión de la red. Cuando se implementa conectividad de Wi-Fi en la tienda, si el tráfico no se desvía correctamente a un punto de inspección, no es posible garantizar que los datos corporativos no se filtren a Internet. Además, no hay garantía de que se sigan las políticas de uso aceptable continuamente.

En general, un conjunto de productos específicos crea una situación donde el riesgo real para la organización no se controla, observa ni administra fácilmente.

Las amenazas a comercios minoristas han ocupado los titulares durante años, como la importante violación de información de un comercio minorista en 2006 que puso en riesgo los datos de hasta un millón de tarjetas de crédito. Los piratas cibernéticos aprovecharon los controles débiles dentro de las tiendas para obtener acceso a información sobre tarjetas de crédito y otros datos de los clientes. Una vez que encuentran una vulnerabilidad, los atacantes se mueven lateralmente a través de las redes corporativas y, de esa manera, perjudican otros datos privados.

Dada la capacidad de los piratas cibernéticos para intercambiar tácticas de ataque y automatizar sus ofensivas, apuntan a corporaciones grandes a través del eslabón más débil de la cadena, que, generalmente, consiste en un comercio minorista con controles deficientes.

Figura 2. Cómo funciona Cisco Cloud Web Security



Control y protección flexibles

Cisco ha desarrollado un conjunto de productos y capacidades que satisfacen las necesidades de seguridad y redes de los entornos de TI de comercios minoristas. Estas soluciones abarcan desde puntos de acceso inalámbrico, routing y switching hasta servicios de seguridad avanzados en la nube.

La Figura 3 brinda una descripción general de las opciones para comprar Cisco CWS.

Figura 3. Opciones de compra de Cisco CWS

Web Security Essentials	Web Security Premium	Conjunto de detección avanzada de amenazas	A la carta
	Protección avanzada contra malware a través de Cognitive Threat Analytics	Protección avanzada contra malware a través de Cognitive Threat Analytics	AMP
			Extracción de registros
Movilidad AnyConnect para el análisis de malware con filtrado web (URL)	Movilidad AnyConnect para el análisis de malware con filtrado web (URL)		

Los productos líderes en el mercado Cisco Web Security Appliance (WSA) y Cisco Cloud Web Security (CWS) ofrecen modelos de implementación flexibles, que brindan seguridad de contenidos a través de la nube y en las instalaciones. Cuando selecciona Cisco WSA para dar protección a nivel de red en la sede central a la vez que elige Cisco CWS para las sucursales, se satisfacen los requisitos de seguridad de TI mientras que, en gran medida, evita la necesidad de comprar hardware nuevo para que todas las sucursales aumenten la protección. Mediante la integración directa con tecnologías en la tienda, que incluyen los firewalls de Cisco Adaptive Security Appliance (ASA),

los routers de servicios integrados (ISR) de Cisco y el cliente Cisco AnyConnect®, Cisco CWS le permite usar las inversiones existentes y los procesos de soporte operativo para obtener una mayor protección y una asistencia de ejecución más eficaz.

Cisco reduce la protección de las conexiones de Internet al nivel de la tienda sin requerir hardware adicional y retorna el tráfico solo cuando así se establece. El tráfico de bajo riesgo va directamente a Internet, mientras que el otro tráfico se envía a la ubicación central para una mayor inspección.

Para proteger contra amenazas conocidas y emergentes, Cisco CWS busca ataques con una diversidad de técnicas, que incluyen las firmas de malware tradicionales, así como filtros de reputación de sitios, archivos y estallidos. Además, Cisco CWS se integra con Cisco Collective Security Intelligence (CSI), la capacidad de inteligencia contra amenazas líder del sector de Cisco, que incluye un grupo de investigación e inteligencia de seguridad Talos. La asistencia de Cisco CSI y de Talos garantiza que los clientes se beneficien de las decenas de miles de clientes que usan la tecnología de Cisco.

Cisco CWS ofrece informes detallados que incluyen datos tradicionales de seguridad de la información, así como un análisis exhaustivo del uso y del consumo de ancho de banda. En entornos con ancho de banda restringido, esta visibilidad es una herramienta fundamental para la eficacia en distintos sectores. Otra función avanzada de informes detalla los hábitos de exploración en Wi-Fi para usuarios temporales, lo que brinda visibilidad y protección contra las comparaciones y verificaciones de precios con comercios minoristas en línea, así como la visualización de contenidos ofensivos. Por lo tanto, las capacidades de informes de Cisco CWS tienen valor no solo para el equipo de seguridad de TI, sino también para la organización minorista en general.

Quizás lo más importante sea, como solución en la nube, que Cisco CWS (Figura 2) es brinda fácil ampliación y mejoramiento de las capacidades de ancho de banda para cualquier organización. Esto redunda en el ahorro de costos cuantificables y directos, e importantes mejoras en la eficacia de la organización para manejar las amenazas dentro de la tienda. Los ahorros provienen de la transferencia del procesamiento para el control y la administración del tráfico en el hardware local a los sistemas basados en la nube. Además, mediante el modelo de software como servicio (SaaS) para ejecutar las decisiones basadas en políticas sobre el tráfico, Cisco CWS reduce significativamente la carga en el hardware de red en la tienda.

¿Cómo Cisco CWS puede ayudar a una organización minorista?

Este ejemplo real muestra cómo Cisco CWS puede proteger una organización minorista del entorno actual de amenazas: se ha asignado a un gerente de seguridad de TI la protección de una cadena de 1500 tiendas que está implementando una tecnología en los locales para brindar acceso a Internet a los clientes, además de diversos servicios adicionales. El gerente de seguridad está al tanto de que recientemente ha habido un crecimiento de ataques avanzados de malware que se usan para poner en riesgo los sistemas en la tienda (incluidos los dispositivos de POS) y desea que estos ataques se detecten rápidamente y solucionen con eficacia. Para agravar estas dificultades, muchas de las tiendas tienen ancho de banda limitado y la solución debe optimizar las conexiones de red en cada tienda.

El gerente de seguridad implementa routers perimetrales Cisco ISR en todas las tiendas. Estos dispositivos son compatibles con las capacidades Cisco Intelligent WAN (IWAN) para proteger y optimizar el ancho de banda en todas las tiendas. IWAN puede ayudar a administrar el ancho de banda mediante conexiones de Internet de costo más bajo en comparación con los enlaces de red privada más costosos. Además, el producto ofrece un programa de migración estable para que la organización pueda abandonar los enlaces de red privada a su propio ritmo. Para asegurarse de que los dispositivos móviles se conecten a la red correcta en cada tienda, Cisco Identity Services Engine (ISE) protege los sistemas en la tienda, determinando qué usuarios y dispositivos pueden acceder a determinadas partes de las redes de las tiendas.

Para proteger el tráfico web, la organización usará Cisco CWS Premium for Direct Internet Access, que puede implementarse a través de los routers perimetrales Cisco ISR, sin requerir hardware adicional. Cisco CWS Premium contiene Cisco Advanced Malware Protection (AMP) y Cognitive Threat Analytics (CTA) para proteger a todos los usuarios mediante capacidades avanzadas de defensa contra amenazas. CTA es un sistema de análisis del comportamiento de la red casi en tiempo real que usa el aprendizaje automático y estadísticas avanzadas para identificar actividades inusuales en la red a fin de detectar posibles ataques. AMP usa una combinación de reputación, sandbox y análisis retrospectivo de archivos para identificar y detener las amenazas que ya están presentes en la red.

Con estos productos de seguridad de Cisco, la cadena de 1500 tiendas puede administrar su uso de ancho de banda, niveles de acceso de usuario, defensas contra amenazas y seguridad de contenido. Esta es solo una combinación posible de los productos de seguridad de Cisco. En este caso, el gerente de seguridad de TI alcanza los objetivos conexión y de seguridad de la empresa para su red distribuida de comercios minoristas.

Beneficios de Cisco CWS

La organización que use la solución integrada de Cisco para proteger sus redes puede aplicar una política común, detectar ataques avanzados y optimizar el uso del ancho de banda en la WAN. Cisco CWS Premium, integrada con los routers perimetrales Cisco ISR, también posibilita el seguimiento de botnets. Esto ayuda a garantizar que los dispositivos de POS no estén en riesgo y puedan transferir datos de forma segura hasta la sede central. Además, la organización podrá aumentar sus ahorros mediante paquetes de soluciones.

La organización no debe preocuparse por integrar los elementos individuales de la solución porque todas las capacidades están diseñadas para funcionar en conjunto. El resultado es un ahorro para el personal de TI que, según las estimaciones de Cisco, pueden ser de hasta el 40% del tiempo dedicado, debido a que hay menos configuración y soporte de implementación. La organización también se beneficia con un nivel de seguridad alto y uniforme en su red a nivel global, de modo que puede continuar creciendo y enfocándose en su empresa en lugar de preocuparse por los atacantes que intentan penetrar en las redes en la tienda.

Conclusión

Los minoristas pueden disminuir significativamente la carga operativa de la supervisión, la administración y el mantenimiento de sus redes con herramientas habilitadas para la nube como Cisco CWS. Al trabajar fácilmente con los productos Cisco ASA y Cisco ISR, CWS reduce de manera inteligente la necesidad de que se cumpla la política de seguridad localmente, lo que se traduce en menos requisitos de ancho de banda para cada tienda individual. Reconocida por Gartner como líder en el mercado, Cisco CWS ofrece una manera inteligente de agregar las capacidades de seguridad más eficaces a las redes en la tienda sin incrementar la complejidad operativa.

Para más información

Para obtener más información, visite http://cisco.com/go/cws.

Sede central en América
Cisco Systems, Inc.
San José CA

Sede Central en Asia-Pacífico
Cisco Systems (EE. UU.) Pte. Ltd.
Singapur

Sede Central en Europa
Cisco Systems International BV Amsterdam.
Holanda

Cisco tiene más de 200 oficinas en todo el mundo. Las direcciones, los números de teléfono y los números de fax están disponibles en el sitio web de Cisco en **www.cisco.com/go/offices**.

Impreso en EE. UU. C11-733817-00 02/15