Fecha de publicación:
11 de junio de 2020
Autor:
Tanner Johnson

Informe de ciberseguridad del IoT de Palo Alto Networks

La ciberseguridad del IoT ha pasado de ser un problema exclusivo de la industria a una inversión fundamental

Presentado por Informa Tech

Índice

Resumen ejecutivo

Catalizador

Tradicionalmente, solo han sido organizaciones seleccionadas que dependen de dispositivos especializados dentro de sus entornos las que han buscado soluciones de ciberseguridad del IoT. Muchas de estas entidades desplegaron equipos de personal dedicados para abordar los riesgos potenciales asociados con la introducción de componentes del IoT. Actualmente, los dispositivos IoT se han infiltrado en casi todas las industrias y mercados imaginables. Estas organizaciones a menudo dependen del funcionamiento efectivo y la productividad de los dispositivos conectados, a pesar de la escasez de proveedores que integran soluciones de seguridad en la producción de sus dispositivos de IoT. Además, la proliferación y monetización de malware y ransomware han hecho añicos la creencia ingenua de que solo las organizaciones lo suficientemente grandes como para permitirse soluciones de seguridad de terminales son objetivos probables. A medida que la dependencia organizativa de los dispositivos de IoT se vuelve omnipresente, las posibles consecuencias del compromiso derivado de dispositivos de IoT inseguros pueden ser financieramente devastadoras para entidades de todos los tamaños. Esta situación ha hecho que las empresas reconozcan gradualmente que la ciberseguridad del IoT ya no es un lujo, sino una inversión fundamental en la sostenibilidad operativa a largo plazo.

La visión de Omdia

A medida que nuestro ecosistema de IoT sigue creciendo en tamaño, conectividad y complejidad, el requisito de proteger eficazmente los componentes y la información compartida por dispositivos se vuelve fundamental. Este desafío polifacético requiere un esfuerzo integral y coordinado de todos los miembros de una organización para integrar la seguridad del IoT en las prioridades estratégicas operativas actuales. La seguridad debe implementarse en el dispositivo, en toda la red, en la nube y durante todo el proceso de gestión de datos.

Mensajes clave

- Los clientes se enfrentan a desafíos únicos de seguridad del IoT.
- Ante la ausencia de normativas generales, puede sentirse abandonado en el «lejano Oeste».
- Los conceptos erróneos entorno al IoT permiten que estos desafíos persistan.
- La increíble diversidad de dispositivos crea un desafío de seguridad del IoT urgente.
- Cualquier solución debe ser accesible para los equipos de seguridad existentes con la mínima interrupción.

- La implementación de una solución de red integrada puede ayudar a abordar la ausencia frecuente de agentes presentes en los dispositivos de IoT.
- Los equipos actuales de Seguridad de las redes y del Centro de operaciones de seguridad pueden implementar metodologías para crear entornos de IoT seguros:
  - Seguridad en las redes
    - Paso 1: Conozca sus activos de IoT mediante la detección y la visibilidad
    - Paso 2: Establezca una evaluación de riesgos eficaz
    - Paso 3: Defina políticas para el comportamiento aceptable del dispositivo
    - Paso 4: Evite cualquier ataque conocido del IoT
  - Centro de operaciones de seguridad
    - Paso 5: Detecte y responda a amenazas desconocidas del IoT

Desafíos de los clientes del IoT

Más nodos = más problemas

Cada componente IoT conectado proporciona un nodo de comunicación que los ladrones de datos intentarán aprovechar. A medida que el volumen de dispositivos sigue aumentando, el panorama de amenazas se incrementa proporcionalmente. Una de las consecuencias de esta nueva realidad es que las oportunidades para que los ciberdelincuentes obtengan acceso no autorizado a estos dispositivos están aumentando en todo el ecosistema del IoT, ya que no existen límites reales para el tipo de dispositivo al que se puede otorgar conectividad a Internet. Además, a medida que los ciberdelincuentes desarrollen campañas y tácticas más sofisticadas con el tiempo, las amenazas introducidas a consecuencia de la conectividad avanzada requerirán finalmente que el usuario correspondiente implemente medidas de protección adicionales.

Disparidad de dispositivos de IoT

Una complicación adicional que surge cuando se intenta abordar la seguridad del IoT son las formas casi ilimitadas que puede adoptar el IoT. Por ejemplo, en el mercado empresarial tradicional, estos dispositivos pueden incluir cámaras, termostatos, automatización de edificios, sistemas de climatización, televisiones, sistemas de punto de venta, impresoras, routers Wi-Fi, vehículos conectados y mucho más. Pese a la adopción masiva de la conectividad IoT, la comodidad que surge de la diversidad de aplicaciones viables también constituye el mayor obstáculo para una seguridad efectiva. La variedad adicional de dispositivos de IoT en cuanto a tipo, naturaleza y funcionalidad conlleva su propio desafío de seguridad. Además, estos distintos dispositivos pueden utilizar una amplia gama de sistemas operativos (si tienen alguno incorporado), lo cual añade una complejidad aún mayor a la iniciativa de seguridad. Asimismo, la decisión de adoptar estas tecnologías se puede llevar a cabo con poca o ninguna participación del personal de seguridad de TI habitual.

Ausencia de normativas sobre el IoT

En los mercados tradicionales, uno de los métodos principales para implementar controles efectivos es adoptar alguna forma de unificación. Multitud de mercados cuentan con pautas bien establecidas, generalmente derivadas de años de aprendizaje de las dificultades encontradas durante el desarrollo, que contribuyen a la creación de políticas que todo el mercado cumple. Sin embargo, el IoT es una tecnología tan reciente que no ha tenido tiempo suficiente para evolucionar hacia un mercado comparativamente maduro. Conforme seguimos aprendiendo de forma colectiva a utilizar esta tecnología, puede resultar difícil para los equipos de seguridad determinar

cuál es el comportamiento «aceptable» de los dispositivos de IoT. Además, la diversidad de los dispositivos dificulta la aplicación universal de las políticas de seguridad acordadas, como la gestión eficaz de parches y las actualizaciones de firmware. Si bien la legislación de seguridad del IoT ha empezado a tomar forma, como en el Reino Unido y California, los requisitos de seguridad que se imponen son de una naturaleza bastante elemental y carecen de una aplicación integral de las medidas de seguridad de chip a nube.

Desafíos de servicio existentes

Conceptos erróneos anteriores

«Conéctese primero; la seguridad… si es rentable». Lamentablemente, muchos fabricantes de equipos originales (OEM) de IoT y de tecnología operacional (OT) continúan participando en esta práctica insegura al diseñar sus respectivos dispositivos. Existen múltiples razones para esta práctica. En primer lugar, la seguridad puede ser costosa, y muchas veces la forma más rápida de lanzar un producto en el mercado es escatimar en medidas de seguridad. En segundo lugar, muchos fabricantes de dispositivos de IoT carecen del conocimiento de seguridad integral necesario para implementar soluciones de protección de datos en el proceso de desarrollo. Además, la forma más sencilla de garantizar que los clientes puedan conectar sus dispositivos a Internet lo más rápido posible es utilizar las mismas credenciales predeterminadas para cada dispositivo fabricado. Desafortunadamente, el cliente no puede cambiar esta información predeterminada en algunos dispositivos. Si bien esto puede ser cómodo para el fabricante de equipos originales y el usuario final, puede convertirse en una pesadilla para los equipos de seguridad de TI de la empresa.

Traducción industrial

La comodidad que ha introducido la comunicación de dispositivos de IoT en el ecosistema tecnológico global ha logrado infiltrarse en todos los mercados imaginables. Los consumidores ahora tienen acceso a cafeteras, tostadoras, cepillos de dientes, frigoríficos e incluso lavadoras conectados. Los dispositivos conectados a Internet se han infiltrado profundamente en el mercado del transporte, y se han puesto en alto riesgo varios vehículos a consecuencia de componentes de IoT inseguros. El ámbito médico ha adoptado la tecnología del IoT para posibilitar un diagnóstico más preciso y planes de tratamiento del paciente. Los equipos de fabricación industrial y las infraestructuras críticas también han implementado tecnologías del IoT como un medio para aumentar la eficacia operativa y el control, al mismo tiempo que reducen el tiempo de inactividad.

Cambio de los ciclos de vida de los dispositivos

A menudo, se presentan desafíos de seguridad del IoT adicionales cuando estos dispositivos conectados duran más que el soporte del fabricante. Continuar ofreciendo soporte a equipos antiguos puede resultar bastante costoso para el fabricante, y, como la investigación y el desarrollo se dirigen hacia ofertas de productos más innovadores, el soporte para componentes más antiguos se acabará suspendiendo. Sin embargo, a medida que estos dispositivos se siguen utilizando, se descubren vulnerabilidades con

mayor regularidad. Si el desarrollador ha suspendido el servicio del dispositivo, este permanece vulnerable hasta que se sustituya. Lamentablemente, muchos de los componentes del IoT esenciales a menudo siguen operando en sus entornos mucho más allá de su ciclo de vida de seguridad.

Soluciones orientadas al IoT

Soluciones existentes

Los desafíos que existen en el panorama actual de las soluciones de seguridad del IoT son bastante numerosos. La implementación de cualquier estrategia de seguridad del IoT probablemente será lenta y compleja, especialmente si la organización nunca ha intentado auditar su ecosistema de IoT. Como la visibilidad del entorno es el primer paso en cualquier oferta de seguridad, esto a menudo puede requerir la adopción de nuevos sensores de red y configuraciones de equipos adicionales para integrarse de manera efectiva con la infraestructura de seguridad existente de una organización. Además, muchas soluciones de clasificación de dispositivos utilizan un enfoque basado en firmas que requiere una interacción constante para mantener la precisión. Asimismo, ante la ausencia de recomendaciones de políticas de seguridad generadas automáticamente, los entornos en red del IoT pueden seguir siendo vulnerables.

Requisitos para la evolución

Al igual que con cualquier tecnología, los requisitos para una seguridad del IoT efectiva se encuentran en un estado de cambio constante. Dado que muchos de los dispositivos de IoT que se utilizan hoy en día carecen de un agente integrado con el que interactuar, existe una creciente demanda de un enfoque sin agentes para la seguridad del IoT. Como resultado, estas soluciones probablemente dependerán del aprendizaje automático y enfoques sin firmas para la clasificación de dispositivos. Además, como las organizaciones deberán establecer un comportamiento normal de referencia, necesitarán sugerencias de políticas automatizadas y estrategias de aplicación integrales. Las soluciones modernas deberán aplicar respuestas sensibles al contexto a los incidentes de seguridad, como la segmentación de la red. Por último, las soluciones deben integrarse a la perfección con las inversiones de seguridad actuales de la organización.

Mejora de las operaciones

Finalmente, los principales beneficios de la implementación de cualquier solución orientada al IoT deberían otorgar capacidades operativas mejoradas a los equipos de Seguridad de las redes y del Centro de operaciones de seguridad de la organización. Los equipos de Seguridad de las redes y del Centro de operaciones de seguridad deben poder implementar sin problemas cualquier solución de seguridad del IoT adoptada, sin la necesidad de establecer un equipo exclusivo específicamente dedicado a abordar la seguridad del sistema de IoT. Cuando se implementan correctamente, las soluciones de seguridad orientadas al IoT deben permitir a los equipos de seguridad de red descubrir y controlar fácilmente los activos del IoT no gestionados en la red, establecer una evaluación integral de riesgos y generar políticas de seguridad recomendadas basadas en

el comportamiento aceptable del dispositivo para ayudar a mitigar cualquier ataque del IoT conocido. Para ser realmente integral, una misma solución de seguridad orientada al IoT también debería permitir a los equipos del Centro de operaciones correspondientes detectar y prevenir amenazas del IoT desconocidas.

Solución de seguridad del IoT de Palo Alto Networks

Una de las soluciones capaces de abordar estas exigencias de seguridad del IoT en desarrollo es la solución de seguridad del IoT de Palo Alto Networks. La solución basada en suscripción, unida a un firewall y entregada en la nube va más allá de proporcionar visibilidad del tráfico de red de referencia al ofrecer una identificación y seguridad completas de dispositivos terminales de IoT para cualquier entorno empresarial. Esta solución permite al equipo de seguridad de la red empresarial tomar medidas proactivas para proteger su ecosistema de IoT. La solución ofrece una integración perfecta con la posición de seguridad actual de una organización y los procesos del Centro de operaciones de seguridad (SOC), al mismo tiempo que ofrece recomendaciones de políticas automatizadas basadas en comportamientos de dispositivos contextualizados y evaluaciones de riesgos.

Además, la solución de seguridad del IoT de Palo Alto Networks se puede fusionar con la infraestructura de seguridad de red actual del cliente, independientemente del proveedor que proporcionó el equipo antiguo. Este enfoque independiente elimina el costoso requisito de los componentes de control adicionales. La solución de control de redes asociada con el firewall de última generación (NGFW) permite una identificación rápida y precisa de los dispositivos de IoT para distinguir de forma eficaz entre los dispositivos de IoT legítimos nuevos y existentes conectados a la red, y aquellos que no entran en la clasificación de IoT por contar con un mayor número de integraciones para inventario de activos, registro y aplicación de políticas. Además, esta solución se puede implementar en entornos que carezcan de firewalls tradicionales, lo cual ofrece una protección integral del IoT al mismo tiempo que elimina la necesidad de subsanar continuamente las lagunas de seguridad con soluciones univalentes.

Apéndice

Autor

Tanner Johnson
Analista senior de ciberseguridad, conectividad e IoT
tanner.johnson@omdia.com

Póngase en contacto con nosotros

www.omdia.com
askananalyst@omdia.com

Consultoría Omdia

Omdia es una empresa de datos, investigación y consultoría líder en el mercado orientada a ayudar a los proveedores de servicios digitales, las empresas de tecnología y los responsables de la toma de decisiones empresariales a prosperar en la economía digital conectada. A través de nuestra base global de analistas, ofrecemos análisis de expertos y conocimientos estratégicos en las industrias de TI, telecomunicaciones y medios.

Creamos ventajas comerciales para nuestros clientes al ofrecer información útil que respalde la planificación comercial, el desarrollo de productos y las iniciativas de comercialización.

Nuestra combinación única de datos autorizados, análisis de mercado y experiencia en la industria vertical está diseñada para potenciar la toma de decisiones, lo que permite a nuestros clientes beneficiarse de las nuevas tecnologías y capitalizar los modelos de negocio en evolución.

Omdia forma parte de Informa Tech, una empresa de servicios de información entre empresas que presta servicios al sector de tecnología, medios y telecomunicaciones. El grupo Informa cotiza en la Bolsa de Londres.

Esperamos que este análisis le ayude a tomar decisiones empresariales fundadas e imaginativas. Si tiene más requisitos, el equipo de consultoría de Omdia ayudará a su empresa a identificar tendencias y oportunidades futuras.

Aviso sobre los derechos de autor y descargo de responsabilidad

La investigación, los datos y la información de Omdia a los que se hace referencia en este documento (los «Materiales de Omdia») son propiedad intelectual de Informa Tech y sus subsidiarias o filiales (en conjunto, «Informa Tech») y representan datos, investigaciones, opiniones o puntos de vista publicados por Informa Tech, y no son representaciones de hechos.

Los Materiales de Omdia presentan información y opiniones de la fecha de publicación original y no de la fecha de este documento. La información y las opiniones expresadas en los Materiales de Omdia están sujetas a cambios sin previo aviso y, como resultado, Informa Tech no tiene ningún deber ni responsabilidad de actualizar los Materiales de Omdia ni esta publicación.

Los Materiales de Omdia se entregan en su estado actual y según la disponibilidad. No se hace ninguna representación ni garantía, expresa o implícita, en cuanto a la imparcialidad, precisión, integridad o corrección de la información, opiniones y conclusiones presentes en los Materiales de Omdia.

En la medida máxima permitida por la ley, Informa Tech y sus filiales, funcionarios, directores, empleados y agentes renuncian a cualquier responsabilidad (incluida, entre otras, cualquier responsabilidad derivada de culpa o negligencia) en cuanto a la precisión, integridad o uso de los Materiales de Omdia. Informa Tech no se hará, bajo ninguna circunstancia, responsable de ninguna decisión de negocios, de inversión, comercial o de otro tipo que se base en los Materiales de Omdia o se apoye en ellos.