ZIMPERIUM

Cómo implementar Mobile BYO en un entorno de confianza cero

El modelo de seguridad de red basado en el perímetro que definió a los usuarios dentro de un perímetro de red corporativa como "de confianza" ya no proporciona el mismo nivel de seguridad que en el pasado. Hoy en día, la computación en la nube, la movilidad y el trabajo remoto cambian la forma en que las personas se conectan a los recursos digitales. Como parte de estos nuevos modelos, los empleados desean cada vez más usar sus propios dispositivos, lo que hace que las políticas de "Traiga su propio dispositivo" (BYOD por sus siglas en inglés) sean todavía más importantes para la seguridad. La implementación de una arquitectura de confianza cero en un entorno BYOD debe incorporar la defensa contra amenazas móviles (MTD por sus siglas en inglés) para aumentar la pila de tecnología de seguridad.

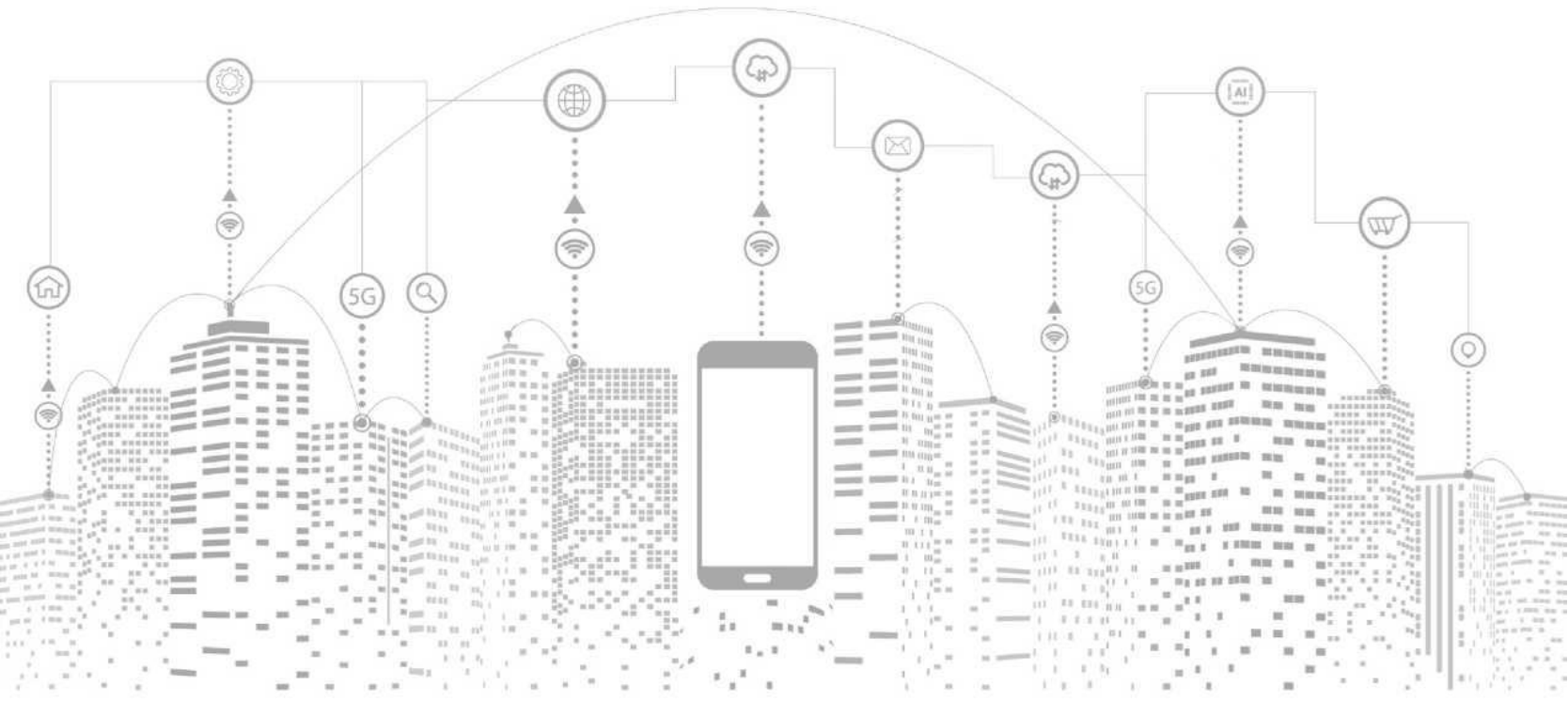
¿Por qué confianza cero?

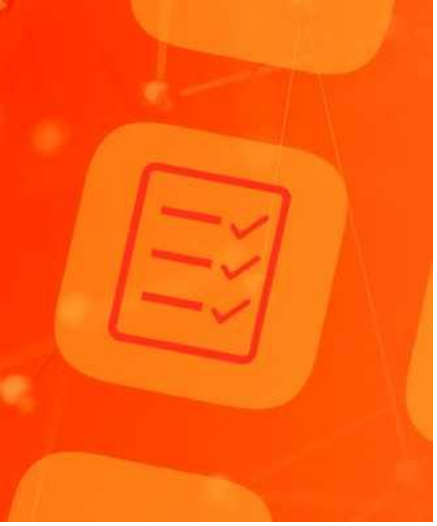
Las nuevas tecnologías y los modelos de fuerza laboral cambian la forma en que las organizaciones deben abordar la seguridad. Por ejemplo, existe una confianza inherente cuando todos los usuarios y dispositivos se conectan a redes protegidas.

Hoy en día, las personas utilizan redes de Internet públicas, incluso dentro de redes protegidas, para acceder a aplicaciones basadas en la web para hacer su trabajo. Además, los socios comerciales externos, al igual que los contratistas, utilizan redes de Internet públicas para cumplir con sus obligaciones.

Un enfoque de seguridad de confianza cero se centra en crear un acceso seguro a los recursos que incorpore:

- Certificado de salud del dispositivo
- Protecciones a nivel de datos
- Gestión de identidad y acceso
- Segmentación estratégica de la red





Por qué el cumplimiento de confianza cero es desafiante

A un alto nivel, confianza cero se centra en seis pilares principales:

Cumplir con confianza cero puede ser todo un desafío p orque, dentro de cada pilar , una organización necesita asegu rar varias cosas. Además, existen muy pocos procesos paso a paso para establecer una arquitectura de confi anza cero.

Por ejemplo, dentro del pilar "Dispositivo", las organizaciones deben garantizar una seguridad continua para las estaciones de trabajo, los dispositivos móviles (incluidas las tabletas y los teléfonos inteligentes), Internet de las cosas, dispositivos IoT como impresoras y servidores.

Bajo este pilar, las organizaciones necesitan gestionar la seguridad de los dispositivos estableciendo protecciones de referencia. Además, necesitan visibilidad sobre la seguridad en el futuro, lo que significa hacer cumplir esas políticas y participar en la certificación continua del riesgo del dispositivo.

Como parte de la función de monitoreo de cumplimiento, debe tener este aspecto:

- **Tradicional:** visibilidad de si un dispositivo cumple con las políticas de seguridad establecidas
- **Avanzado:** capacidad para que la mayoría de los dispositivos cumplan con las políticas
- **Óptimo:** monitorear y validar la postura de seguridad del dispositivo en tiempo real

En entornos BYOD, muchas organizaciones tendrán dificultades para obtener visibilidad sobre si un dispositivo cumple con las políticas de seguridad establecidas. Es posible que no puedan controlar qué dispositivo usa alguien o que tengan dificultades para cumplir con los requisitos de privacidad al aprovechar una tecnología para ayudar a obtener visibilidad.

Cada organización debe proporcionar protección contra estas amenazas de dispositivos móviles

La certificación continua del dispositivo es fundamental para una estrategia BYOD eficaz para cumplir con los requisitos de seguridad de confianza cero. Al elaborar estas estrategias e iniciativas, las organizaciones deben tener en cuenta diversas amenazas que pueden socavar sus objetivos. Los empleados usan constantemente sus dispositivos móviles y, a medida que realizan su labor, se encuentran con amenazas reales.

Phishing

El mayor énfasis en los ataques de phishing por parte de los actores de amenazas no es nada nuevo. Según un artículo de SC Media, los ataques de phishing desde Rusia se multiplicaron por ocho entre el 27 de febrero de 2022 y el 1 de marzo de 2022.

Según nuestro Informe de amenazas móviles globales de 2022, el 55 % de los encuestados dijo que la "explotación a través del phishing" era su mayor riesgo, y el 61 % afirmó que había visto un aumento en los ataques de phishing durante la pandemia de COVID-19.

Si bien la mayoría de las veces los usuarios finales nunca tienen la intención de causar daño, la mayor sofisticación y el aluvión de actividades dificultan la separación del grano de la paja en Internet. Las soluciones tradicionales de phishing o antivirus basadas en firmas ofrecen un punto de partida. Sin embargo, muchas de ellas son de naturaleza reactiva y no abordan adecuadamente el desafío del volumen de nuevos sitios de phishing que aparecen cada segundo.

Más preocupante aún, los investigadores de Zimperium han detectado un aumento en los sitios web de phishing específicos para móviles. Después de analizar nuestra información y datos públicos basados en dos años, el número de sitios web de phishing específicos para móviles creció en un 50 %. Además, a lo largo de 2021, el 75 % de los sitios de phishing analizaron dispositivos móviles específicos y entregaron contenido apropiado para el formato móvil.

Por ejemplo, los atacantes apuntaron a dispositivos móviles con las dos técnicas siguientes:

- **Sitios web adaptativos:** dependiendo del dispositivo utilizado, los sitios web adaptativos pueden cargar diferentes contenidos y redirigir a sitios alternativos. Al adaptar el contenido en función del agente de usuario de un terminal móvil, los atacantes pueden dirigirse exclusivamente a dispositivos móviles.
- **Sitios web receptivos:** dado que estos adaptan el tamaño y la ubicación de los objetos en función del tamaño de la pantalla del terminal final, los atacantes pueden utilizar estas características legítimas para dirigirse a los dispositivos móviles.

Los dispositivos móviles ofrecen una capa adicional de complejidad que hace que los enfoques tradicionales de antivirus y phishing no sean adecuados para dispositivos móviles. En primer lugar, la conectividad de un dispositivo a una nube, además de las consideraciones de privacidad y las preocupaciones de latencia, hace que cualquier enfoque de nube prioritaria no sea factible tanto desde una perspectiva de seguridad técnica como operativa. Además, los dispositivos móviles no pueden descargar o admitir archivos de firmas grandes, por lo que cualquier dependencia de bases de datos conocidas, o fuentes de amenazas, es inadecuada e inviable.

Esto significa que las únicas opciones viables para proteger los dispositivos móviles deben ser capaces de hacerlo en el dispositivo sin depender de la nube y deben ser capaces de detectar amenazas conocidas y desconocidas sin tener que haberlas visto antes. El motor de detección z9 de Zimperium utilizando sus clasificadores de aprendizaje automático (ML por sus siglas en inglés) se ajusta a esta factura no solo a través de phishing, sino también dispositivos, redes y amenazas de aplicaciones.

Aplicaciones descargadas

Muchas organizaciones ya conocen los riesgos que puede causar la TI en la sombra en los dispositivos tradicionales. Sin embargo, la imposibilidad de añadir estas aplicaciones a los inventarios de activos lleva a una falta de visibilidad.

Las aplicaciones descargadas en dispositivos móviles se vuelven aún más arriesgadas. Los miembros de la fuerza laboral utilizan dispositivos móviles personal y profesionalmente, lo que provoca que las organizaciones no puedan controlar la seguridad de las aplicaciones que utilizan para administrar su uso personal.

La convergencia de aplicaciones móviles/aplicaciones de escritorio en el sistema operativo moderno es una tendencia que facilita a los actores de amenazas el uso de dispositivos móviles como puerta trasera en sistemas y redes. Según los datos del Informe de amenazas de Zimperium, el 42 % de las empresas informaron de aplicaciones y recursos no autorizados que accedían a datos empresariales.

La solución MTD de Zimperium está dedicada explícitamente a la prevención de amenazas, detección y respuesta para dispositivos con sistemas operativos iOS, Android y Chrome. Si bien una solución de gestión de dispositivos móviles (MDM por sus siglas en inglés) puede ayudar con la administración y aplicación de políticas, la MTD de Zimperium protege a la organización al compartimentar la información y los procesos confidenciales, reduciendo la superficie de ataque.

Malware dentro de aplicaciones descargadas

Dado que la superficie de ataque móvil difiere de la superficie de ataque tradicional, el malware móvil también es único. A veces, la aplicación es el malware, mientras que, en otras ocasiones, los atacantes usan aplicaciones para enviar el malware a través de una vulnerabilidad.

Aplicaciones maliciosas

En 2021, el análisis de seguridad móvil de Zimperium descubrió 2 034 217 nuevas muestras de malware detectadas en la naturaleza. De media, eso son casi 36 000 nuevas variantes de malware a la semana (más de 5000 al día). Por ejemplo, los atacantes se dirigieron a los usuarios de dispositivos móviles durante la temporada navideña de 2021 con mensajes de texto y enlaces de correo electrónico que promovían descuentos, con la esperanza de que las personas los usaran para descargar una aplicación maliciosa.

Mientras que algunas variantes de malware para móviles actúan como ataques a terminales tradicionales, otras lucen y actúan de manera diferente. Por ejemplo, algunas pueden:

- Robar credenciales de autenticación de dos factores (2FA) a través de SMS o notificaciones de aplicaciones.
- Realizar ataques de superposición cuando un usuario introduce credenciales en una aplicación secundaria que cree que es legítima.
- Monitorizar otras aplicaciones instaladas a través de los permisos del servicio de accesibilidad.
- Utilizar el seguimiento de la ubicación a través de los servicios de GPS.
- Activar cámaras o micrófonos para grabar audio y vídeo.
- Acceder a contenido confidencial como fotos, contactos o datos personales.
- Capturar y rastrear los datos del sensor.

Aplicaciones arriesgadas

Como tecnología más reciente, las aplicaciones móviles pueden no tener el mismo nivel de seguridad incorporado en su ciclo de desarrollo de software, especialmente cuando las empresas intentan sacar nuevas experiencias rápidamente.

En la segunda mitad de 2021, Zimperium descubrió que aproximadamente el 81 % de las más de 160 aplicaciones móviles financieras globales investigaron y analizaron datos potencialmente filtrados. Más allá de las aplicaciones financieras, Zimperium descubrió que el 77 % de las aplicaciones de salud, venta minorista y estilo de vida de Android y el 46 % de las aplicaciones de iOS usaban o podrían usar al menos un algoritmo de cifrado vulnerable.

En otras palabras, incluso cuando los usuarios finales descargan aplicaciones legítimas, pueden crear riesgos que afectan a la organización. Con la seguridad del desarrollo de aplicaciones móviles todavía en su estado incipiente, las empresas deben considerar cómo protegerse de estos riesgos.

Ataques de red

Trabajar desde cualquier lugar significa que los empleados se conectan a redes wifi no seguras. Si bien esto no es nuevo, los ataques de intermediarios (MitM por sus siglas en inglés) siguen siendo efectivos, y la investigación de Zimperium encontró que el 13 % de los dispositivos se encontraron con ataques MitM.

Igualmente problemático, las redes wifi anteriormente "protegidas" pueden verse socavadas a través de ataques gemelos maliciosos donde los actores maliciosos falsifican una wifi gratuita que utiliza un portal para la entrada, como en un hotel o aeropuerto. Según la investigación de Zimperium, alrededor del 16 % de los dispositivos móviles se encontraron con una red maliciosa conocida, manipulación del tráfico o un punto de acceso fraudulento. Dicho esto, es más probable que los usuarios finales que se conectaron previamente a la red wifi real confíen en que es segura. Sin embargo, cuando el usuario inicia sesión en el portal de la empresa a través de esta red wifi falsa, los actores maliciosos pueden robar sus credenciales.

Con Zimperium, las organizaciones pueden hacer cumplir los requisitos de acceso condicional cuando las personas cambian su ubicación porque la "condición" del dispositivo se supervisa continuamente. Con la solución MTD de Zimperium, la compañía tiene visibilidad de la seguridad del dispositivo y puede negar el acceso de forma más apropiada desde una conexión wifi fraudulenta.

Estaciones de carga

Cuando las organizaciones consideran los riesgos móviles, a menudo se preocupan más por el phishing. Sin embargo, centrarse únicamente en el phishing no tiene en cuenta otros métodos de distribución de malware.

Recientemente, la FCC advirtió a los consumidores que las estaciones públicas de carga USB, como las de los centros comerciales y aeropuertos, estaban siendo explotadas por los ciberdelincuentes. Este tipo de ataque, conocido como "juice jacking" (ataque de carga), se puede ejecutar a través del puerto USB o un cable dejado por los ciberdelincuentes. Cuando los usuarios conectan sus teléfonos, el malware puede bloquear un dispositivo o exportar credenciales.

zIPS de Zimperium proporciona una implementación de seguridad en el dispositivo para comprender el riesgo del dispositivo de un usuario. La postura de amenaza proporciona la certificación necesaria para determinar si una empresa debe confiar en ese dispositivo. Incluso a medida que los ciberdelincuentes evolucionan sus metodologías, zIPS ofrece la certificación de dispositivos necesaria para implementar estrategias de confianza cero para BYOD.

Evitar el compromiso de los dispositivos móviles es fundamental para las arquitecturas de confianza cero

Si los dispositivos móviles no cumplen con los requisitos de seguridad de una organización, socavan sus políticas de confianza cero.

Según la investigación de Zimperium, 7 de cada 10 organizaciones consideran que los dispositivos móviles son fundamentales para sus operaciones. Sin embargo, los empleados usan dispositivos móviles personales para acceder a todo, desde listas de clientes y estrategias de cuenta hasta modelos financieros. Como estos acceden y almacenan información confidencial, un dispositivo móvil comprometido puede provocar una filtración de datos.

Además, estos dispositivos son a menudo el medio principal de la organización para implementar la autenticación de múltiples factores a través de SMS o una aplicación de 2FA. Como resultado, un dispositivo móvil comprometido puede usarse como parte de un ataque más grande contra la organización, aprovechando las credenciales del usuario, interceptando la 2FA y obteniendo acceso que permite el movimiento lateral.

En resumen, un dispositivo móvil comprometido puede socavar el dispositivo y los pilares de identidad de confianza cero.

Mejorar la seguridad de dispositivos móviles BYOD para implementar la arquitectura de confianza cero

La incorporación de BYOD en una arquitectura de confianza cero plantea muchos desafíos. Si bien BYOD proporciona a los empleados una mayor flexibilidad, también crea nuevos riesgos de seguridad. Las organizaciones deben incluir MTD como parte de sus estrategias de confianza cero para mejorar la seguridad de BYOD.

zIPS de Zimperium es una solución avanzada de defensa contra amenazas móviles para empresas, que proporciona protección persistente en el dispositivo tanto para dispositivos corporativos como para dispositivos BYOD. La seguridad en el dispositivo zIPS de Zimperium proporciona a las organizaciones la certificación de integridad del dispositivo móvil necesaria para un enfoque completo de confianza cero. Además, por diseño, zIPS protege la privacidad del usuario final, asegurando que las organizaciones cumplan con la arquitectura de confianza cero (ZTA por sus siglas en inglés) y los requisitos de privacidad.

Para ver una demostración y obtener más información sobre cómo proteger su organización de las amenazas móviles, visite www.zimperium.com/contact-us/.