wandera
a Jamf company

Informe de seguridad en la nube 2021

Le presentamos un análisis de las amenazas que afectarán los datos de su organización a través de sus activos más críticos: endpoints, usuarios y herramientas de acceso remoto. En este informe también encontrará consejos prácticos sobre cómo configurar herramientas empresariales para proporcionar una conectividad rápida y segura para todos los usuarios en el año 2021.

EMEA 45 Mortimer Street
London W1W 8HJ
+44 (0) 203 301 2660

US 220 Sansome Street, Suite 1400
San Francisco CA 94104
+1 (415) 935 3095

Aspectos clave

- En el 2020, el 52 % de las organizaciones fueron víctimas de un incidente de malware en un dispositivo remoto, un aumento del 41 % respecto al 2019, año en que el porcentaje fue del 37 %.
- De los dispositivos afectados por malware móvil en el 2020, el 37 % siguieron accediendo al correo de la empresa después de la infección y el 11 % siguieron accediendo al almacenamiento en la nube de la empresa.
- En el 2020, el 28 % de las organizaciones utilizaban regularmente un sistema operativo con vulnerabilidades de seguridad conocidas.
- Respecto a la época anterior a la pandemia, el número de conexiones a contenidos inadecuados durante horas laborales ha aumentado, sustancialmente en un 100 %.
- Hemos constatado que los dispositivos Android son 5.3 veces más propensos a tener instalada una app vulnerable que los dispositivos iOS.
- En el punto álgido del fin de semana, los ataques de phishing fueron un 6 % más frecuentes que durante el punto álgido entre semana.
- En el 2020, hubo un 4 % de usuarios conectados a un hotspot de riesgo a la semana, un porcentaje menor que el 7 % del 2019. Sin embargo,
- el 15 % de las organizaciones tuvieron al menos un dispositivo con una app que filtraba datos de contraseñas, un porcentaje superior al 11 % del 2019.

28%

de las organizaciones utilizaron regularmente un sistema operativo con una vulnerabilidad de seguridad conocida.

5.3x

Hemos constatado que los dispositivos Android son 5.3 veces más propensos a tener instalada una app vulnerable que los dispositivos iOS.

Introducción

En el 2020, muchas organizaciones se vieron obligadas a transformar sus prácticas empresariales y a adoptar un modelo totalmente en línea sin afectar los niveles de productividad. Como consecuencia, las políticas de IT tuvieron que revisarse para acomodar más dispositivos, más redes y más aplicaciones en muchos más lugares que antes.

La empresa sin fronteras ha llegado. Una encuesta de Gartner a CFO de marzo del 2020 reveló que el 74 % planean quedarse con parte de los empleados trabajando a distancia de manera permanente.

Ante estas circunstancias, las hipótesis antiguas sobre lo que se consideraban buenas prácticas de seguridad están cambiando a marchas forzadas. Las operaciones de IT más exitosas se centran en facultar a los usuarios para que puedan hacer su trabajo sin pasar por la oficina. Para lograrlo, tendrá que flexibilizar y agilizar su estrategia de seguridad de manera que dé respuesta a las nuevas necesidades de una plantilla de empleados ubicados en distintos lugares. Y eso requiere un modelo basado principalmente en la nube.

Los expertos del sector creen que SASE (Secure Access Service Edge) será la arquitectura clave para las empresas innovadoras que estén listas para dejar atrás las tecnologías tradicionales, ya que SASE converge y permite transferir las funciones de red y seguridad a un servicio nativo y unificado en la nube.

Sí, SASE puede ser el modelo del futuro, pero las empresas también necesitan contar con las herramientas adecuadas para sus operaciones actuales. Es muy importante comprender los riesgos cibernéticos y cómo pueden introducirse en la organización. Y precisamente esto es lo que nos hemos propuesto con este informe anual.

Todos los años, analizamos las amenazas que afectan a los dispositivos que se usan para actividades laborales. Del mismo modo que nuestra cartera de productos ha ido evolucionando con el tiempo (para dar cabida a dispositivos que vayan más allá de los smartphones y las tablets), nuestro concepto de fuerza laboral móvil también ha ido cambiando: los empleados de hoy trabajan remotamente, y con ellos surgen nuevas necesidades que van más allá del uso de dispositivos móviles.

El informe de este año analiza las amenazas y las tendencias de seguridad que afectan a organizaciones reales cuyos usuarios se conectan de forma remota, y a través de una amplia variedad de dispositivos y plataformas portátiles, a una multitud de aplicaciones alojadas en centros de datos privados y públicos.

Copyright © 2021 Wandera

FACTOR DE RIESGO 1

Endpoints

La introducción de dispositivos móviles en los últimos decenios ha mejorado considerablemente nuestra capacidad de colaborar y compartir información dondequiera que estemos. En el 2020, la mayoría de las corporaciones hicieron la transición a un modelo de trabajo remoto a tiempo completo cuando el personal se vio obligado a trabajar desde casa a causa del COVID-19.

Si bien no fue una transición fácil para todos, sí lo fue para algunas organizaciones, especialmente para las que ya tenían a algunos trabajadores haciendo teletrabajo a tiempo completo y al personal de la oficina teletrabajando algún día a la semana.

En muchos casos, IT tuvo que tomar decisiones difíciles y rápidas sobre a qué dispositivos permitir acceso a los datos sensibles de la organización y a cuáles no. Como resultado, hubo una falta de uniformidad para la cual algunos equipos de IT y seguridad no estaban preparados.

Más dispositivos + más tipos de dispositivos

Durante el último decenio, las personas han estado consumiendo cada vez más datos de Internet desde sus smartphones. Y no es de extrañar que lo mismo suceda con los datos relacionados con el trabajo, especialmente con el auge de las aplicaciones móviles SaaS, como suites de productividad (Microsoft Office 365, por ejemplo) y herramientas de CRM (como Salesforce). Actualmente, en la empresa promedio, el 60 % de los dispositivos que contienen o acceden a datos corporativos son dispositivos móviles.

Antes del 2020, el trabajo móvil estaba reservado para unos pocos empleados que, por motivos de viaje, se conectaban desde un smartphone de propiedad propia (BYOD) o de propiedad de la organización (COPE). Ahora, muchísimos empleados trabajan a tiempo completo desde su casa o lugar de vacaciones. Usan el dispositivo que tengan a mano en cada momento y suelen tener varias opciones entre las que elegir. Cisco predice que el número de dispositivos conectados a redes IP triplicará la población mundial de aquí al 2023.

La diferencia entre los trabajadores "móviles" del pasado y los "trabajadores en remoto" a tiempo completo de la actualidad se está empezando a materializar. Y, con ella, estamos descubriendo de manera inequívoca que muchos de los flujos de trabajo que se utilizan actualmente en la empresa no son factibles o sostenibles para los trabajadores que ahora trabajan desde casa con las herramientas de trabajo a distancia tradicionales.

Sin el presupuesto o la cadena de suministro adecuados para entregar dispositivos autorizados a los usuarios, muchos equipos de IT dejan que cada empleado compre su propio dispositivo o incluso elija su propio equipo informático para crearse su estación de trabajo en casa. Esto se traduce en factores de forma ultraportátiles y convertibles con una gran potencia de computación, como el Surface Pro, o una tablet de pantalla grande como segundo monitor, o un MacBook Pro con uno o dos monitores de alta resolución. Muchos empleados que antes usaban el teléfono fijo para el trabajo, ahora se han comprado un segundo smartphone para separar el trabajo de la vida personal. Los tipos de dispositivos han proliferado, y los equipos de IT no dan abasto.

Las personas que trabajan desde casa también usan dispositivos de Internet portátiles que se sirven de una señal celular para conectar dispositivos inalámbricos cuando el ancho de banda del Wi-Fi de casa no da para más. Optan por Verizon Jetpacks, hostpots móviles y Mi-Fi como alternativas de red móvil para tener conexiones a Internet confiables dentro y fuera de casa.

28%

En el 2020, el 28 % de las organizaciones se vieron afectadas por sistemas operativos con una vulnerabilidad conocida.

Promedio de versiones de OS, tipos de OS y modelos de dispositivo

< 500 dispositivos		> 500 dispositivos
11.3	Versiones diferentes de OS	39.4
1.4	OS distintos	1.6
1.8	Modelos de dispositivo diferentes	2.6

En promedio, las empresas con menos de 500 dispositivos ejecutan 11.3 versiones de OS diferentes, con 1.4 tipos de OS y en 1.8 modelos distintos de dispositivo. Comparativamente, las empresas con más de 500 dispositivos ejecutan 39.4 versiones de OS diferentes, en 1.6 tipos de OS y en 2.6 modelos distintos de dispositivo.

Copyright © 2021 Wandera

Si se utiliza una gran variedad de hardware para trabajar, también se introduce una gran variedad de software y, como es bien sabido en la industria de seguridad, todo software puede sufrir vulnerabilidades. Muchos de nuestros clientes prestan soporte a una flota de dispositivos que ejecutan una combinación de Android, iOS, Mac y Windows 10. Y se han propuesto estandarizar políticas uniformes para todas estas plataformas, un objetivo que no es nada fácil, porque cada plataforma ofrece distintos niveles de control y funcionalidad, así como distintas formas de expedir parches de seguridad para sistemas operativos vulnerables.

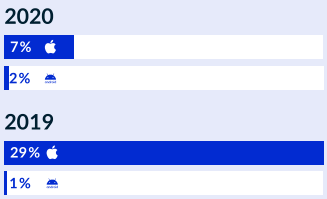
DATO DESTACADO

Por norma general, los dispositivos del sector público sufren menos amenazas que los del privado, gracias a sus buenas prácticas de seguridad. Sin embargo, en comparación con los promedios globales, suelen ejecutar sistemas operativos anticuados: tienen 4.4 veces más usuarios con sistemas operativos con vulnerabilidades leves y 3.6 veces más usuarios con sistemas operativos con vulnerabilidades graves.

La falta de estandarización de dispositivos es el nuevo estándar

La falta de estandarización de dispositivos supone nuevos retos para los equipos de IT. Cuando las organizaciones tenían un único tipo de dispositivo del que preocuparse, por ejemplo, el desktop de Windows, solo tenían que lidiar con un tipo de sistema operativo. Tal vez algunos de estos dispositivos usaban versiones no actualizadas del sistema operativo, por ejemplo, podían llegar a estar tres versiones atrás. Si este era el caso, el equipo de IT solo tenía que conocer y monitorear las vulnerabilidades de cuatro versiones de OS. Ahora, sin embargo, el nuevo estándar es contar con múltiples plataformas (Mac, Windows, iOS y Android), si aplicamos el mismo cálculo de las versiones desactualizadas, lo que antes habrían sido tan solo cuatro versiones de las que preocuparse ahora se han convertido en 16 versiones de OS distintas. La conclusión clave de todo esto es que si se ofrecen opciones a los empleados, la empresa tiene que estar preparada para escalar la gestión y el soporte a todas estas opciones.

Versión de sistema operativo vulnerable



En el 2020, el 7 % de los dispositivos iOS y el 2 % de los dispositivos Android tenían versiones vulnerables del sistema operativo, frente al 29 % y el 1 %, respectivamente, del 2019. Esta reducción drástica del número de versiones de iOS vulnerables seguramente se debe al conjunto de vulnerabilidades de alto perfil de iOS que surgieron en el 2019 y que afectaron a iMessage y FaceTime.

El dilema de la seguridad de endpoints

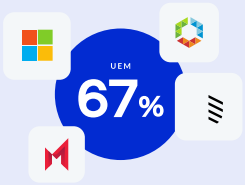
Las organizaciones aspiran a contar con una seguridad de endpoints inquebrantable, pero a menudo se encuentran ante retos comunes: cómo garantizar temporalmente la seguridad de los dispositivos de colaboradores externos cuando acceden a datos confidenciales, o cómo respetar la privacidad de los empleados que utilizan dispositivos BYOD sin dejar de aplicar unos mínimos de seguridad. Los usuarios suelen oponerse a las soluciones de seguridad y gestión. No quieren sentirse espiados y saben que estas soluciones tienen que llevar a cabo algún tipo de control para detectar ataques.

Sabemos que el 70 % de las filtraciones exitosas se originan en el endpoint. También sabemos que el 83 % de las organizaciones dicen que ofrecer acceso a terceros (por ejemplo, colaboradores externos o socios de la cadena de suministro) es muy difícil, así que se pueden hacer muchas mejoras a la hora de velar por la seguridad de los endpoints no gestionados.

Según Verizon, en el 87 % de las empresas las amenazas en dispositivos móviles han superado en número a cualquier otro tipo de amenazas. Esto se debe, seguramente, al hecho de que los dispositivos móviles son más difíciles de gestionar y proteger, por su naturaleza personal, y a que los agentes maliciosos saben que existe esta brecha de seguridad.

En una encuesta, el 92 % de las empresas FT 500 afirmaron que les preocupaba que su plantilla laboral cada vez fuera más móvil y supusiera mayores riesgos de seguridad. Si bien la mayoría de las organizaciones han adoptado políticas de "trae tu propio dispositivo" (BYOD), la gran mayoría (94 %) señaló que los programas BYOD supusieron un aumento de los riesgos de seguridad móvil.

Es muy probable que el teletrabajo siga siendo parte integral de las prácticas empresariales estándar, incluso una vez hayamos alcanzado un gran porcentaje de vacunación contra el COVID-19 en la población. Por eso, los equipos de IT tienen que establecer prácticas que den respuesta a las necesidades de una gran variedad de dispositivos y redes administrados y no administrados. También tienen que asegurarse de que los dispositivos remotos no estén en la periferia de la seguridad y aplicar una estrategia integral que dé cuenta de los datos de amenazas de todos los endpoints en los informes SOC.



Según nuestros datos, un 67 % de los dispositivos móviles están inscritos en algún software de gestión de dispositivos, como MobileIron o VMware Workspace ONE.

Copyright © 2021 Wandera

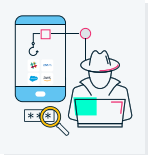
FACTOR DE RIESGO 2

Usuarios

Los sistemas operativos están diseñados para mitigar la gran mayoría de las amenazas de seguridad. Apple y Google han dado un gran paso para reforzar la seguridad de sus sistemas operativos y sus app stores. Sin embargo, a veces los riesgos los introducen las conductas de los usuarios. Para entender los riesgos introducidos por el usuario, debemos tener en cuenta que algunos atacantes explotan las debilidades de los usuarios. Pero también debemos reparar en el hecho de que algunos comportamientos de los usuarios debilitan la seguridad del dispositivo y abren la puerta a potenciales ataques.

Usuarios como víctimas de un ataque dirigido

Los hackers siguen ingeniándoselas para entrar en sistemas operativos protegidos con ataques de ingeniería social como el phishing, que consiste en ponerse en contacto con un usuario específico y engañarlo para que comparta información personal. Los usuarios también pueden ver cómo agentes maliciosos interceptan su tráfico aprovechando la naturaleza insegura de las redes Wi-Fi públicas. Además, los usuarios pueden ser víctimas de aplicaciones no fiables que los expongan a pérdidas de datos, como PII o robo financiero, entre otras estafas.

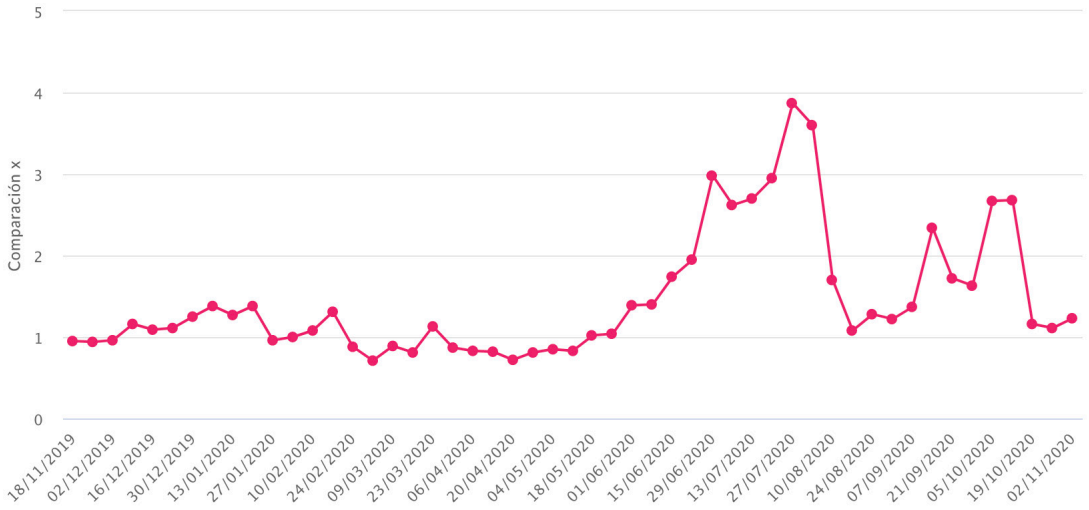


USUARIOS COMO VÍCTIMAS DE UN ATAQUE DIRIGIDO

Phishing

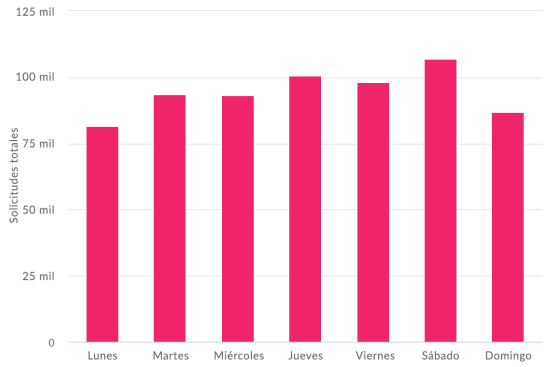
El phishing sigue siendo la amenaza que afecta a más usuarios en dispositivos móviles. Los ataques de phishing suelen basarse en temas o marcas que tengan una alta probabilidad de captar la atención de las víctimas. Por ejemplo, todos los años, cuando se acerca la época de presentar la declaración de impuestos, hay un aumento de ataques de phishing por parte de impostores que se hacen pasar por las autoridades nacionales de recaudación de impuestos, como el IRS (en Estados Unidos), el HMRC (en el Reino Unido) y ATO (en Australia). Del mismo modo, durante la primera mitad de este año identificamos un aumento del tráfico de usuarios a sitios web de phishing relacionados con el COVID-19, e incluso apareció un sitio de e-commerce falso de la marca Clorox (fabricante de toallitas desinfectantes).

El siguiente gráfico ilustra el aumento de los ataques de phishing dirigidos a personas que trabajaron desde casa durante el año 2020.



Copyright © 2021 Wandera

Cuando nos planteamos identificar otras tendencias de phishing que surgieron en el 2020, observamos que el día de la semana en que suelen acumularse más ataques de phishing es el sábado. En el punto álgido del fin de semana, los ataques de phishing fueron un 6 % más frecuentes que durante el punto álgido entre semana. Esto refuerza la idea de que aunque los empleados no estén trabajando, son más susceptibles a los ataques de phishing desde sus dispositivos corporativos porque están más relajados.



USUARIOS COMO VÍCTIMAS DE UN ATAQUE DIRIGIDO

Ataques de intermediario por Wi-Fi

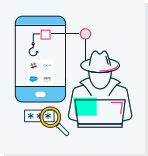
Las redes Wi-Fi presentan un gran riesgo de privacidad cuando se produce un ataque de intermediario (MitM). Hay dos tipos principales de ataques MitM que suelen afectar a los usuarios móviles. El primero se da cuando el atacante tiene el control físico de algún elemento de la infraestructura de red, como un punto de acceso Wi-Fi falso, y es capaz de fisgonear el tráfico que fluye a través de este; el segundo se da cuando el atacante manipula el protocolo de red, que se supone que cifra los datos, exponiendo así información que debería estar protegida. Según un dato alarmante, más del 80 % de los empleados usan redes de Wi-Fi públicas para tareas de trabajo, aun cuando lo tienen oficialmente prohibido.

> En el 2020, hubo un 4 % de usuarios conectados a hotspots de riesgo a la semana, un porcentaje, eso sí, inferior al 7 % del 2019.

Echemos un vistazo a cómo el impacto de las amenazas de Wi-Fi, incluidos los ataques MitM, ha ido cambiando a lo largo del año 2020.

Cuando llevamos a cabo este análisis, esperábamos observar una disminución por una razón obvia: las personas no viajan por trabajo tanto como antes de la irrupción del COVID-19 (alrededor de febrero o marzo del 2020). En este gráfico vemos un pequeño repunte en enero, cuando las personas regresaron al trabajo, seguido por un descenso pronunciado en febrero, cuando los números de casos de COVID-19 se dispararon y las empresas empezaron a cancelar los viajes de trabajo y a recomendar a sus empleados que trabajaran desde casa para protegerlos.

Copyright © 2021 Wandera



USUARIOS COMO VÍCTIMAS DE UN ATAQUE DIRIGIDO

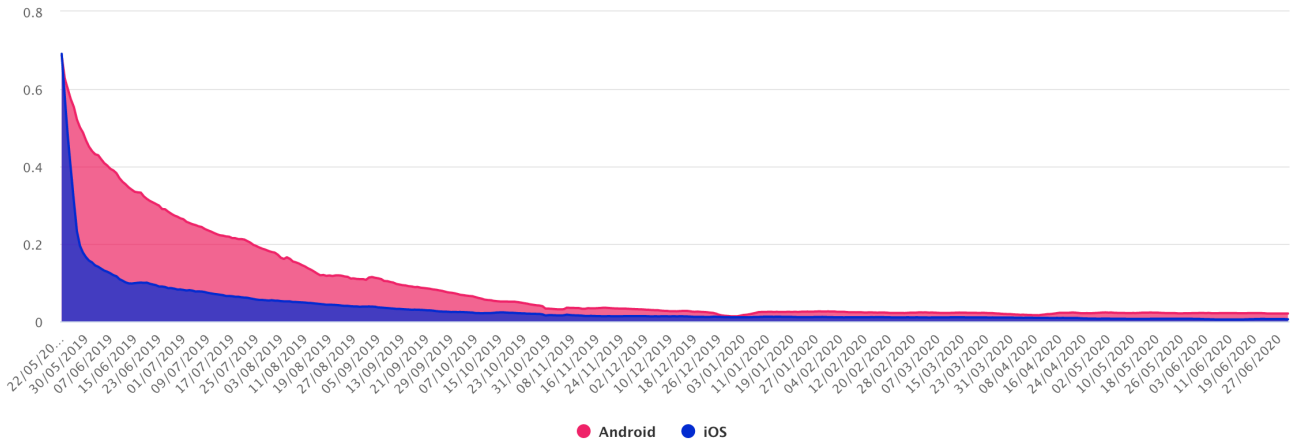
Riesgo de apps

Las apps maliciosas, como las que contienen malware, usan técnicas cada vez más inteligentes para evitar ser detectadas. Por ejemplo, hay programas de malware sofisticados que esperarán algunos pasos antes de iniciar un comportamiento malicioso; por ejemplo, tan solo se comportarán mal en una red en concreto, o contendrán código de comando y control latente, que cualquier hacker puede activar cuando desee. Las comprobaciones básicas, como las que llevan a cabo las tiendas de apps, no son capaces de identificar apps maliciosas sofisticadas pero sorprendentemente comunes.

> En el 2020, el 52 % de las organizaciones experimentaron por lo menos un incidente de malware en un dispositivo remoto, un aumento considerable respecto al 37 % del 2019.

Más allá de la posibilidad de que las aplicaciones contengan malware oculto, las apps pueden estar mal construidas, o sus desarrolladores pueden no velar por su seguridad o mantenimiento y, por ende, ser susceptibles a vulnerabilidades peligrosas, como las que se descubrieron en WhatsApp en el 2019 y el 2020.

> Como puede observarse en el siguiente gráfico, los usuarios de Android tardaron más tiempo en actualizar sus apps después de que en mayo del 2019 se descubriera una vulnerabilidad importante en una versión anterior de WhatsApp. Desde mediados de mayo hasta mediados de julio del 2019, se actualizaron alrededor del 85 % de los dispositivos afectados por versiones de WhatsApp vulnerables. Comparativamente, durante ese tiempo se actualizaron aproximadamente apenas el 50 % de los dispositivos Android vulnerables.



A veces, las apps contienen una estafa o alguna otra actividad fraudulenta, y a menudo los desarrolladores introducen estas estafas a través de alguna infraestructura publicitaria de terceros. Hemos visto apps que lograban superar todos los controles de las tiendas de apps oficiales a pesar de estar cargadas de anuncios pop up que ocupan la pantalla entera y las hacen inutilizables. 1 de cada 200 dispositivos tiene instaladas una de estas apps, que denominamos apps potencialmente no deseadas.

Algunos desarrolladores pueden incluso ser lo bastante descuidados como para ni siquiera usar el cifrado y, por consiguiente, exponer al usuario (y también a la empresa que le paga) a escenarios de pérdida de datos.

- En el 2020, el 15 % de las organizaciones tenían al menos un dispositivo que usaba una app que filtraba datos de contraseñas, lo que supuso un aumento respecto al 11 % del 2019.
- En el 2020, los dispositivos iOS tenían una probabilidad 3.2 veces superior de verse impactados por aplicaciones que filtraban datos que los dispositivos Android.

Nuestro análisis más reciente muestra que una vez que una aplicación no aprobada introduce el riesgo en un dispositivo, dicho riesgo se multiplica.

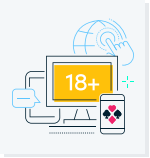
- Con al menos un dispositivo comprometido con malware: tienen una probabilidad 4.4 veces mayor de verse afectados por un robo de contraseñas que las demás empresas.
- Con una aplicación vulnerable instalada en su dispositivo: tienen una probabilidad 59 veces mayor de haberse cruzado con tráfico de cryptojacking que los demás usuarios.

Los exámenes de seguridad independientes para aplicaciones son una tarea laboriosa pero necesaria. Los usuarios tienen más dispositivos que nunca y, con ello, acceso a todo un mundo de aplicaciones. Es posible que la intención no siempre sea mala. Un usuario puede querer usar un programa que combine PDFs o alguna otra herramienta de gestión de archivos no aprobada por IT, y dicha app puede conllevar riesgos. IT tiene que saber qué apps eligen los usuarios para trabajar, principalmente por dos motivos: (1) deben auditarse para determinar su riesgo y (2) deben evaluarse desde el punto de vista de la productividad. En caso de que se demuestre que son seguras y que fomentan la productividad, entonces hay que adaptarlas y protegerlas.

Copyright © 2021 Wandera

El usuario como responsable de malas decisiones

En la sección anterior hemos visto los riesgos incurridos por usuarios con una actitud más bien pasiva. Esta sección examina el riesgo incurrido por usuarios con una actitud más activa, como la evasión de políticas corporativas y las medidas de seguridad en vigor. Los usuarios pueden meterse en problemas por culpa de decisiones negligentes, por ejemplo, si acceden a contenidos que infringen ciertas normas, o si manipulan las características de seguridad de sus dispositivos, ya sea mediante un jailbreak o un sideloading, o deshabilitando la función de bloquear pantalla.

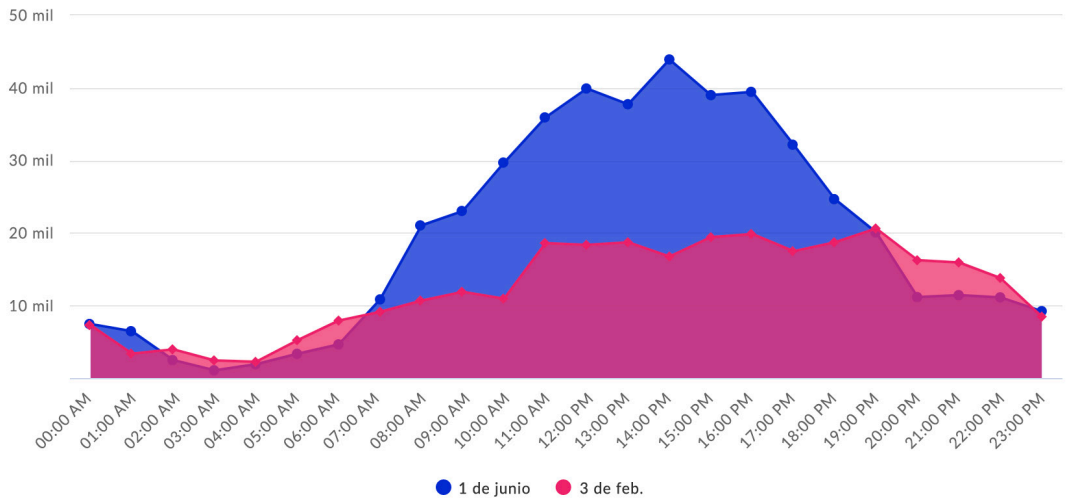


EL USUARIO COMO RESPONSABLE DE MALAS DECISIONES

Contenido inapropiado

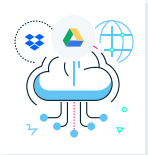
Tener dispositivos en la infraestructura de IT que puedan acceder a los rincones más oscuros de Internet supone riesgos para su empresa. Cuando hablamos de contenidos inapropiados, nos referimos a categorías de contenidos adultos, de juegos de azar, extremos e ilegales, que tienen una probabilidad mucho más elevada de filtrar datos, emplear tecnologías no cifradas o exponer a las organizaciones al riesgo de alguna otra forma. Sorprendentemente, hay muchas personas que acceden a los rincones más oscuros de Internet mediante sus dispositivos de trabajo.

El número de conexiones a contenidos inadecuados durante horas laborales ha aumentado sustancialmente en un 100 % respecto a la época anterior a la pandemia. Aunque los empleados trabajen de forma remota, es evidente que hay que asegurarse de que estos sigan respetando las políticas de uso aceptables en sus dispositivos remotos.



El filtrado de contenidos es una forma eficaz de aplicar políticas de uso aceptable en una serie de endpoints para así mitigar los riesgos legales, de seguridad y cumplimiento tanto para los empleados como para las empresas.

Copyright © 2021 Wandera



EL USUARIO COMO RESPONSABLE DE MALAS DECISIONES

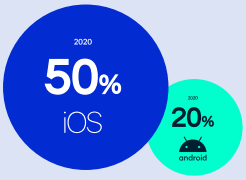
Sortear las medidas de seguridad

Las vulnerabilidades no siempre "afectan" a los usuarios: a veces son estos quienes, intencionadamente o no, dejan sus dispositivos en situación de vulnerabilidad.

Jailbreak

Practicar un jailbreak o rootear un dispositivo significa introducir una configuración de riesgo que permite a los usuarios acceder al sistema operativo de un dispositivo e instalar funciones y aplicaciones no autorizadas. Estos métodos también son populares entre aquellos usuarios que desean liberar dispositivos bloqueados por las operadoras.

- En el 2020, el número de dispositivos iOS con jailbreak aumentó un 50 %, mientras que el número de dispositivos Android rooteados aumentó un 20 %.
- Los dispositivos con jailbreak tienen una probabilidad 28 veces mayor de toparse con tráfico de redes maliciosas que los que no han sido objeto de jailbreak.
- Las empresas que cuentan con al menos un dispositivo con jailbreak en su flota tienen una probabilidad 31.6 veces superior de que sus dispositivos se topen con tráfico de redes maliciosas que las otras empresas.
- Los dispositivos con jailbreak tienen una probabilidad 33 veces mayor de tener vulnerabilidades conocidas instaladas que los dispositivos sin jailbreak.



En el 2019, el número de dispositivos iOS con jailbreak aumentó un 50 %, mientras que el número de dispositivos Android rooteados aumentó un 20 %.

Sideloading de apps

Si bien algunos usuarios de iOS pueden llevar a cabo el jailbreak de sus dispositivos móviles a propósito para instalar mejoras de seguridad, la mayoría de los usuarios lo hacen para instalar aplicaciones que no estén disponibles en las tiendas de apps oficiales. También es posible instalar apps de terceros sin llevar a cabo un jailbreak; este proceso se conoce como sideloading. Para ello, un usuario solo tiene que configurar el dispositivo para que este confíe en un desarrollador específico, y a continuación puede instalar cualquier app de ese desarrollador sin pasar por la tienda de aplicaciones. Así es como muchas empresas instalan aplicaciones para sus empleados sin tener que publicar esas apps en las tiendas de aplicaciones.

Google no bloquea tanto los dispositivos Android como lo hace Apple con los dispositivos iOS. Si bien la configuración por defecto de Android no permite las aplicaciones instaladas mediante el sistema de sideloading, es posible cambiar dichas configuraciones para permitir las apps de terceros. Según nuestros datos, uno de cada cinco usuarios de Android tiene sus dispositivos configurados para permitir la instalación de apps de terceros.

Los usuarios que instalan apps mediante el método de sideload enfrentan mayores riesgos de seguridad, porque el sistema se salta el proceso de revisión de las aplicaciones implementado por Apple y Google en sus tiendas oficiales y, por consiguiente, el dispositivo tiene menos protección contra el malware instalado de forma involuntaria.

En el 2020, 1 de cada 10 dispositivos Android utilizados para el trabajo contenía una tienda de apps de terceros instalada (es decir, una tienda que no era Google Play).

DATO DESTACADO - SECTOR JURÍDICO

En el sector jurídico, los usuarios tienen una probabilidad 2.5 veces mayor de tener aplicaciones instaladas mediante el método de sideload que en cualquier otro sector.

DATO DESTACADO - SECTOR DE LA FABRICACIÓN

En el sector de la fabricación, los dispositivos tienen el doble de probabilidades de toparse con malware que en el resto de los sectores. Eso puede tener relación con el hecho de que un 50 % más de los usuarios tienen app stores de terceros instaladas, y que los usuarios de Android tienen el doble de probabilidades de tener fuentes desconocidas habilitadas.

Copyright © 2021 Wandera

Deshabilitar el bloqueo de pantalla

Sorprendentemente, una de las medidas de seguridad más simples de los dispositivos móviles sigue pasándose por alto en algunas ocasiones: el bloqueo de la pantalla. A pesar de que la función del bloqueo de la pantalla está activada de manera predeterminada en la mayoría de los dispositivos, algunos usuarios optan por deshabilitarla manualmente, una decisión que hace que los dispositivos sean muy vulnerables en caso de robo físico. También es un indicador de unos hábitos de seguridad deficientes, y nuestros datos revelan que otras amenazas proliferan en dispositivos que tienen esta medida de seguridad tan básica deshabilitada.

- En el 2020, el 3 % de los dispositivos utilizados en el trabajo tenían la función de bloquear la pantalla deshabilitada, un porcentaje menor frente al 6 % del 2019.
- Los usuarios que deshabilitan el bloqueo de la pantalla tienen una probabilidad 16 veces mayor de contar con un sistema operativo con una vulnerabilidad conocida.
- Los usuarios que deshabilitan el bloqueo de pantalla tienen una probabilidad 2.4 veces mayor de que les hackeen el correo electrónico.

DATO DESTACADO - PROVEEDORES DE IT

Los usuarios que son proveedores de servicios de IT tienen una probabilidad 2.2 veces mayor de tener la función de bloqueo de pantalla deshabilitada en sus dispositivos, en comparación con el promedio mundial.

En el 2020, el 3 % de los dispositivos utilizados en el trabajo tenían la función de bloquear la pantalla deshabilitada, un porcentaje menor frente al 6 % del 2019.

Copyright © 2021 Wandera

FACTOR DE RIESGO 3

Acceso remoto

Hemos analizado los riesgos de dispositivos y sistema operativo, así como los introducidos por el usuario, pero ¿y los riesgos que todas estas cosas suponen para las aplicaciones empresariales sensibles cuando el acceso remoto no está bien configurado ni protegido? ¿Con qué tipo de protección deberíamos contar entre el dispositivo o el usuario de riesgo y los datos confidenciales de las aplicaciones empresariales?

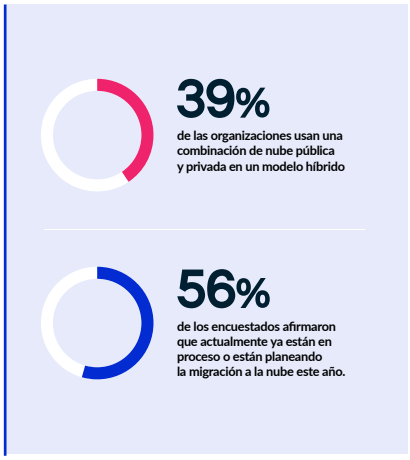
Cuando hablamos de proteger las aplicaciones empresariales, no nos referimos a la protección de las aplicaciones ni al Mobile Application Management (MAM), sino que hablamos de velar por el acceso seguro a la propiedad intelectual crítica que se esconde en estas aplicaciones y cargas de trabajo ejecutadas en la nube.

Según el informe "Remote Workforce Security Report 2020" de Cybersecurity Insiders, el 65 % de las organizaciones permiten que los empleados accedan a las aplicaciones gestionadas desde sus dispositivos personales y no gestionados.

Además, según el informe "Remote Access and Security Challenges & Opportunities" de IDC, el 40 % de los ciberataques surgen precisamente porque usuarios autorizados acceden a sistemas no autorizados.

Muchas apps empresariales en muchos lugares

Si hay algo que sabemos con toda certeza en el sector de la seguridad es que los profesionales de IT a los que hemos encuestado tienen la mirada puesta en la nube. Según los datos de la encuesta de O'Reilly "Cloud Adoption in 2020 Report", el 39 % de las organizaciones usan una combinación de nube pública y privada en un modelo híbrido. Es más, en este estudio, más del 56 % de los encuestados afirmaron estar desarrollando o planeando proyectos de migración a la nube para este año.



Estos datos revelan que muchas organizaciones han adoptado (o están en proceso de adoptar) un entorno híbrido descentralizado en el que los datos se albergan en una infraestructura diversa. Algunas conservan el control de ciertas aplicaciones indefinidamente, pero las soluciones de nube y SaaS permiten que muchas aplicaciones se ubiquen fuera del perímetro corporativo, de tal modo que el acceso a dichas aplicaciones se ha convertido en un ámbito clave para los servicios de seguridad.

Muchos lugares de trabajo modernos priorizan las aplicaciones en la nube porque su implementación, gestión y mantenimiento resultan sencillos y rentables para el negocio; tanto los servicios públicos como privados en la nube cuentan con un historial aceptable, lo que los hace viables para empresas de todos los tamaños. Asimismo, para algunas aplicaciones se prefieren las soluciones SaaS porque permiten a la organización desentenderse de los pesados procesos de desarrollo y mantenimiento. Es indudable que, en el caso de las aplicaciones SaaS, los beneficios superan los riesgos. ¿Para qué cavar un pozo cuando se puede usar agua corriente? Gartner ha predicho que las soluciones SaaS generarán ingresos próximos a los 105 000 millones de dólares tan solo en el 2020.

Muchas organizaciones están migrando algunas apps a la nube y ampliando el número de apps SaaS que utilizan, gestionando más apps que nunca en más lugares que nunca. Además, según Okta, cuanto más grande es la organización, más apps utiliza.

El número de apps de software implementadas por grandes empresas de todos los sectores a nivel mundial ha aumentado un 68 % a lo largo de los últimos cuatro años, hasta alcanzar un promedio de 129 apps por empresa a finales del 2018, según un estudio de Okta. Casi el 10 % de las empresas disponían de más de 200 apps en el momento del estudio.

Copyright © 2021 Wandera

La necesidad de acceso remoto moderno

En el pasado, las empresas querían proteger una sola cosa, el centro de datos, y lo controlaban físicamente. Las herramientas de acceso remoto heredadas como VPN o RDI se construyeron en torno a la base de un perímetro corporativo y funcionaron adecuadamente mientras las aplicaciones se ejecutaban desde el centro de datos. Con un modelo de seguridad "castle-and-moat", la confianza entre quienes se encuentran dentro de la red es inherente. Eso significa que los atacantes potenciales pueden acceder a segmentos de red enteros porque las VPN y los RDI "confían" implícitamente en las conexiones, sin un método sólido para verificar la identidad del usuario o verificar la situación de seguridad del dispositivo.

42%

de las empresas que tienen dispositivos comprometidos por malware, al menos uno de estos dispositivos tienen acceso a herramientas

Según IDC, en el 68 % de los principales incidentes con herramientas de acceso remoto se usaba una VPN. No solo eso, sino que en realidad un 40 % de las vulneraciones cibernéticas tienen su origen en usuarios autorizados que acceden a sistemas no autorizados.

¿Por qué es importante que las evaluaciones de riesgo continuas se conviertan en una parte esencial de la estrategia de acceso remoto? Dejemos que hablen los números.

- De entre los dispositivos que usaban un sistema operativo vulnerable en el 2020, 1 de cada 83 tenía acceso a sus correos electrónicos y 1 de cada 6 tenía acceso a sistemas de almacenamiento en la nube en el momento de la vulnerabilidad.
- De los dispositivos afectados por malware móvil en el 2020, el 37 % siguieron accediendo a correos de empresa después de la infección y el 11 % siguieron accediendo al almacenamiento en la nube.
- El 42 % de las empresas que tienen dispositivos comprometidos por malware, por lo menos uno de esos dispositivos comprometidos accede a herramientas de productividad.
- 1 de cada 200 dispositivos que acceden a sistemas de almacenamiento en la nube tienen los bloqueos de pantalla desactivados.
- En más del 40 % de las empresas con usuarios que usan sistemas operativos vulnerables, por lo menos uno de esos dispositivos vulnerables accede a sistemas de almacenamiento en la nube.
- El 1.3 % de los clientes tienen un dispositivo comprometido por malware con herramientas de productividad, como Office 365 o Google Workspace.
- Así pues, sabemos que la autenticación de usuario por sí sola no permite proteger los datos sensibles de los negocios frente a dispositivos comprometidos. ¿Cuál es la solución? Zero Trust Network Access supone un cambio fundamental con respecto al enfoque tradicioinal. Se terminaron las cajas, los aparatos y los dispositivos físicos. Y, lo más importante, la seguridad de red en la nube es escalable. Sin dicha seguridad, no se pueden comprar suficientes dispositivos para proteger todos estos datos que abandonan el perímetro corporativo y migran a la nube.

De entre los dispositivos que usaban un sistema operativo vulnerable en el 2020, 1 de cada 83 tenía acceso a sus correos electrónicos y 1 de cada 6 tenía acceso a sistemas de almacenamiento en la nube en el momento de la vulnerabilidad.

Además, Zero Trust Network Access puede llevar a cabo evaluaciones de riesgo continuas de todos los dispositivos que soliciten acceso a sus aplicaciones sensibles para garantizar que el dispositivo cumpla con todas las normas: que el dispositivo se encuentre en una red confiable y en la ubicación esperada, que esté libre de infecciones y vulnerabilidades, y que el usuario tenga permiso para realizar determinadas solicitudes.

Copyright © 2021 Wandera

Recomendaciones

A pesar de que hace décadas que se intentan definir los estándares de IT corporativo, muchos negocios han llegado a un punto en el que el estándar es la falta de estandarización. ¿Qué OS utiliza su negocio? Todos. ¿A qué tipo de usuarios permite acceder a sus aplicaciones? A todos. ¿Desde qué ubicaciones se les permite trabajar a los usuarios? Desde todas.

Las soluciones de acceso remoto seguro deben ser lo bastante flexibles y ágiles para permitir (no bloquear ni estorbar) la productividad. Recomendamos usar esta lista para desarrollar una estrategia de seguridad SASE moderna que encaje con las necesidades de los entornos de IT actuales.

Describa los requisitos a partir de los nuevos casos de uso que están surgiendo con el trabajo remoto.

- ¿Qué quiere permitirles hacer a sus empleados en sus dispositivos? ¿Acceder al correo electrónico o a bases de datos sensibles? Segmente los datos para que el acceso pueda ser granular.
- Evalúe sus casos de uso y defina los requisitos para su personal remoto.
- Los requisitos anteriores determinarán su modelo de propiedad de dispositivos: ¿a qué tipos de dispositivo dará compatibilidad? ¿De quién son propiedad y cómo se gestionan?

Conectividad

- En lo relativo a la conectividad y a las aplicaciones en la nube, determine qué necesita saber sobre usuarios, dispositivos, redes y aplicaciones antes de concederles acceso a los recursos corporativos.
- Limite a los usuarios a las herramientas de la empresa que necesitan, ya que así evitará que alguien explote una cuenta con un exceso de privilegios para atacar un gran número de sistemas.

Defina el uso aceptable.

- Revise sus políticas de uso aceptable existentes y asegúrese de que incorporen todos los tipos de endpoints.
- Implemente una política de uso aceptable para cada subconjunto de dispositivos, de tal modo que pueda controlar el shadow IT y los usos no deseados, además de garantizar el cumplimiento de las regulaciones.

Amplíe las políticas de gestión de acceso para que incorporen la situación de riesgo de los dispositivos.

- Implemente una solución de IAM (Identity and Access Management) para la autenticación en las apps corporativas en todos los dispositivos, incluidos los celulares.
- Incorpore las evaluaciones de riesgo de los dispositivos en sus políticas de IAM para asegurarse de que se tenga en cuenta la situación de riesgo de los dispositivos.
- Asegúrese de que la situación de riesgo se evalúe de forma continua durante cada sesión.

Copyright © 2021 Wandera

Implemente un sistema de protección de endpoints en todos los dispositivos; disponer de una solución de seguridad en la nube es particularmente relevante para protegerse contra una amplia gama de ciberataques y riesgos de los usuarios.

- Asegúrese de que su solución de seguridad disponga de una capacidad de detección de endpoints y de una arquitectura de red lo bastante potentes para evitar los ataques antes de que estos lleguen a un dispositivo.
- Asegúrese de que su solución de seguridad pueda abordar tanto las ciberamenazas externas (como el phishing, los ataques MitM o el malware) como los riesgos derivados del uso (apps cargadas con sideloading, etc.).
- En el caso de las herramientas de seguridad, asegúrese de establecer las configuraciones adecuadas para abordar los vectores de amenaza propios intrínsecos a su empresa al tiempo que respeta la privacidad de sus usuarios finales.
- Evalúe la capacidad de aprendizaje automático de su solución de seguridad para comprender de qué forma el motor de amenazas identifica nuevas amenazas y protege contra ellas.

Implemente una solución de UEM para garantizar el control a nivel de los dispositivos.

- Si es necesario, implemente una solución de UEM que le permita proporcionar recursos corporativos a los dispositivos y llevar a cabo controles de cumplimiento constante en los dispositivos.

Revise esta lista y considere qué cambios deben introducirse en función de lo siguiente:

- Cambios en el tamaño y la composición de la empresa, como fusiones, o adquisiciones
- Nuevas regulaciones que afecten a la forma de manejar los datos
- Estrategia de IT evolutiva
- Amenazas que ha visto que afectan a los empleados
- Nuevas aplicaciones que los empleados necesitan para hacer su trabajo

Jamf ayuda a las organizaciones a alcanzar el éxito con Apple. Porque permitimos que IT confiera mayor poder a los usuarios, trasladamos la legendaria experiencia de Apple a las empresas, el sector educativo y las organizaciones gubernamentales.

wandera
a Jamf company