wandera
a Jamf company

# Rapport cloudbeveiliging 2021

**Een nadere blik op de bedreigingen die de data van uw organisatie treffen via uw meest kritieke bedrijfsmiddelen: uw eindpunten, gebruikers en tools voor toegang op afstand. Aangevuld met praktisch advies over hoe u uw zakelijke tools kunt configureren om een snelle en veilige connectiviteit te waarborgen voor alle gebruikers in 2021.**


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

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

# Belangrijke bevindingen

- 52% van de organisaties kreeg in 2020 te maken met een malware-incident op een device op afstand, vergeleken met 37% in 2019; een stijging van 41%.
- Van de mobiele devices die in 2020 door mobiele malware werden getroffen, bleef 37% zakelijke e-mails openen en 11% bleef gebruikmaken van cloudopslag.
- In 2020 gebruikte 28% van de organisaties regelmatig een besturingssysteem met een bekend veiligheidsrisico.
- In vergelijking met pre-coronatijden, zagen we een opmerkelijke toename van maximaal 100% van verbindingen met ongepaste inhoud tijdens kantooruren.
- De kans op installatie van een app met een veiligheidsrisico was 5,3x groter voor Android-devices, in vergelijking met iOS-devices.
- In het weekend kwamen phishing-aanvallen op het hoogste punt 6% vaker voor dan op het hoogste punt tijdens werkdagen.
- In 2020 was 4% van de gebruikers elke week verbonden met een risicovolle hotspot, vergeleken 7% in 2019. Maar:
- 15% van de organisaties had minstens één device met een app die wachtwoordgegevens lekte, vergeleken met 11% in 2019.

**28%**

**van de organisaties gebruikte regelmatig een besturingssysteem met een bekend veiligheidsrisico.**

**5,3x**

**De kans op installatie van een app met een veiligheidsrisico was 5,3x groter voor Android-devices, in vergelijking met iOS-devices.**

# Inleiding

In 2020 zagen veel organisaties zich genoodzaakt om hun bedrijfspraktijken volledig op afstand uit te voeren, waarbij de productiviteit moest worden gehandhaafd. Als gevolg hiervan werd het IT-beleid herzien om te kunnen werken met meer devices, meer netwerken en meer apps, op meer plaatsen dan ooit tevoren.

De onderneming zonder grenzen is realiteit geworden. Uit een enquête onder CFO's van onderzoeks- en adviesbureau Gartner in maart 2020, bleek dat 74% van hen van plan is om een aantal werknemers permanent op afstand te laten werken.

Als gevolg hiervan zien we de oude opvattingen over goede beveiligingspraktijken voor onze ogen veranderen, om te passen bij het nieuwe normaal. De meest succesvolle IT-activiteiten zijn erop gericht gebruikers in staat te stellen om buiten het kantoor te kunnen werken. Dit houdt in dat uw beveiligingsstrategie flexibeler moet zijn om de verschillende behoeften van het verspreide personeelsbestand te kunnen vervullen – en dat kan alleen met een cloud-first model.

De belangrijkste experts in de industrie zijn van mening dat SASE (Secure Access Service Edge) het belangrijkste architectuurmodel zal zijn voor innovatieve bedrijven die afstappen van traditionele technologieën, omdat SASE de functies van netwerken en beveiliging samenbrengt en afstemt in een enkele cloud-native dienst.

SASE is dan misschien de toekomst, maar bedrijven hebben de juiste tools voor nu nodig. Het is cruciaal dat u een goed begrip heeft van cyberrisico's en hoe ze uw organisatie kunnen binnensluipen, en dat is dan ook het doel van dit jaarverslag.

Elk jaar analyseren we de bedreigingen met een impact op mobiele devices die worden gebruikt voor werk. Met de groei van onze productportfolio, die is uitgebreid met andere devices naast smartphones en tablets, is ook ons perspectief op de mobiele werknemers veranderd; het gaat om medewerkers op afstand, en om meer dan alleen mobiele devices.

Het rapport van dit jaar richt zich op de bedreigingen en de trends in beveiliging van echte organisaties met gebruikers die op afstand verbinding maken via een breed scala aan draagbare devices en platforms met een veelvoud aan apps die worden gehost in privé- en openbare datacenters.

Copyright © 2021 Wandera

RISICOFACTOR 1

# Eindpunten

**De introductie van draagbare devices in de afgelopen decennia heeft gezorgd voor een enorme verbetering van ons vermogen om overal te werken en informatie te delen. In 2020 dwong het coronavirus veel bedrijven om regelingen te treffen die het mogelijk maakte voor hun medewerkers om fulltime vanuit huis te werken.**

**De overgang verliep bij de ene organisatie vlotter dan bij de andere; het was met name makkelijker voor werkgevers die al gewend waren aan enkele medewerkers die voltijds thuiswerkten of kantoormedewerkers die af en toe vanuit huis werkten.**

**In veel gevallen moest de IT-afdeling snelle en ingrijpende beslissingen maken over welke devices toegang mochten hebben tot gevoelige bedrijfsgegevens. Dit leidde tot grote inconsistenties waar niet ieder IT- en beveiligingsteam op was voorbereid.**

## Meer devices + meer typen devices

In de afgelopen tien jaar zijn mensen steeds meer gebruik gaan maken van internet via hun smartphone. Met de opkomst van mobiele SaaS-applicaties (zoals Microsoft Office 365 en CRM-tools als Salesforce) is ook het mobiele werkgerelateerde gegevensverkeer gegroeid. In de gemiddelde hedendaagse organisatie is 60% van de devices die bedrijfsgegevens bevatten of daar toegang tot hebben, mobiel.

Als we het voor 2020 hadden over mobiel werken, ging het vaak om een beperkt aantal werknemers die onderweg verbonden bleven met een smartphone, ofwel van henzelf, of van de werkgever. Nu gaat het om mensen die fulltime thuis of vanuit een vakantiehuisje werken, met elk device dat voor handen is – en dat zijn er vaak nogal wat. Cisco voorspelt dat het aantal devices dat in 2023 verbonden is met IP-netwerken, meer dan driemaal zo groot is als de wereldbevolking.

Het verschil tussen 'mobiele' werknemers en fulltime 'werknemers op afstand' begint te kristalliseren. En daarmee wordt het steeds duidelijker dat veel van de workflows die werknemers gebruiken niet mogelijk of duurzaam zijn vanaf thuiswerkplekken met traditionele werktools op afstand.

Bij gebrek aan het budget of de toeleveringsketen om goedgekeurde devices aan gebruikers toe te wijzen, hebben veel IT-teams medewerkers toestemming gegeven om hun eigen computerapparatuur voor hun thuiskantoor te kopen of zelfs te kiezen. Dit kan een ultradraagbare en converteerbare computer met enorme rekenkracht zijn, zoals een Surface Pro, of een tablet met groot scherm dat dienstdoet als tweede monitor, of een MacBook Pro met een of twee monitors met hoge resolutie. Werknemers die eerder een vaste telefoon gebruikten, hebben inmiddels misschien een tweede smartphone gekocht om de grens tussen gebruik voor werk en vrije tijd te handhaven. Het is een buffet met allerlei devices en IT-teams hebben er hun buik soms vol van.

Werknemers op afstand vertrouwen ook op nieuwe draagbare internetdevices die een mobiel signaal gebruiken als het te druk is op het Wi-Fi-netwerk thuis. Met mobiele hotspots en Mi-Fi-routers voor meerdere mobiele netwerken zorgen ze voor betrouwbare internetverbindingen binnen en buiten het huis.

**28%**

**In 2020 kreeg 28% van de organisaties te maken met een besturingssysteem met een bekend veiligheidsrisico.**

**Gemiddelde versie besturingssysteem, besturingssystemen en device-modellen**

| < 500 devices | | > 500 devices |
|---|---|---|
| 11,3 | Verschillende versies besturingssystemen | 39,4 |
| 1,4 | Verschillende besturingssystemen | 1,6 |
| 1,8 | Verschillende device-modellen | 2,6 |

**Gemiddeld draaien bedrijven met <500 devices 11,3 verschillende versies van besturingssystemen, op 1,4 verschillende besturingssystemen, op 1,8 verschillende device-modellen. Ter vergelijking: bedrijven met >500 devices draaien 39,4 verschillende versies van besturingssystemen, op 1,6 verschillende besturingssystemen, op 2,6 verschillende device-modellen.**

Copyright © 2021 Wandera

Met een grotere verscheidenheid aan hardware voor werk, komt ook een grotere verscheidenheid aan software. En zoals we goed weten in de IT-beveiliging, is software gevoelig voor kwetsbaarheden. Veel van onze klanten hebben een device-park waarin op de verschillende modellen Android, iOS, Mac en Windows 10 wordt gedraaid. Ze proberen een gestandaardiseerd en consistent beleid op al deze platforms door te voeren, maar dat is niet eenvoudig wanneer elk platform verschillende beheer- en functionaliteitsniveaus heeft en er ook verschillende manieren zijn om beveiligingspatches voor kwetsbare besturingssystemen te verspreiden.

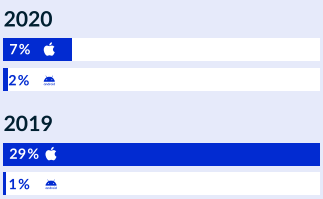
FOCUS OP DE SECTOR

Over het algemeen hebben devices in de publieke sector door de goede beveiligingsmaatregelen minder te maken met bedreigingen dan in andere sectoren. Ze hebben echter vaak verouderde besturingssystemen, met 4,4x zoveel gebruikers met besturingssystemen met minder ernstige beveiligingsrisico's en 3,6x zoveel gebruikers met besturingssystemen met zeer ernstige risico's, in vergelijking met wereldwijde gemiddelden.

**De nieuwe standaard: geen standaardisatie van devices**

Het gebrek aan device-standaardisatie is een nieuwe uitdaging voor IT-teams. Toen organisaties nog maar één type device hadden om zich zorgen over te maken, bijvoorbeeld een Windows-computer, hadden ze slechts één type besturingssysteem om in de gaten te houden. Misschien dat een paar van die devices een versie of twee, drie achterliepen. Dat betekent dat een IT-team slechts vier versies hoefde te kennen en te controleren op risico's. Maar nu zijn meerdere platforms de norm: Mac, Windows, iOS en Android. En als we nu verouderde versies van besturingssystemen meenemen in onze overweging, moeten we geen vier, maar zestien versies van besturingssystemen in het oog houden. De les hier is: als u mensen de keuze geeft, moet u bereid zijn om het beheer op te schalen om deze keuzes te ondersteunen.

**Kwetsbare versie van besturingssysteem**




**In 2020 had 7% van de iOS-devices en 2% van de Android-devices een kwetsbare versie van een besturingssysteem, in vergelijking met respectievelijk 29% en 1%, in 2019. Deze sterke daling van kwetsbare iOS-versies is waarschijnlijk te verklaren door de in 2019 in de pers breed uitgemeten reeks iOS-kwetsbaarheden met betrekking tot iMessage en FaceTime.**

# Het dilemma van eindpuntbeveiliging

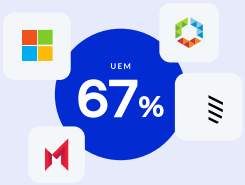
Organisaties willen hun eindpunten goed beveiligen, maar lopen dan tegen bekende dilemma's aan – zoals de tijdelijk beveiliging van devices van onderaannemers die toegang moeten hebben tot gevoelige gegevens, of hoe ze de privacy kunnen respecteren van personeel dat werkt op een eigen device, dat toch in een zekere mate moet worden beveiligd. Gebruikers zijn meestal niet voor beheer- en beveiligingsoplossingen. Ze willen niet worden bespioneerd en weten dat deze oplossingen hun gebruik moeten monitoren om bedreigingen op te vangen.

We weten dat 70% van de succesvolle inbreuken op de beveiliging beginnen bij het eindpunt. We weten ook dat 83% van de organisaties het moeilijk tot extreem moeilijk vindt om externe partijen (bijvoorbeeld onderaannemers of toeleveringsbedrijven) toegang te bieden. Er is dus nog veel te doen met betrekking tot de beveiliging van onbeheerde eindpunten.

Volgens Verizon meldt 87% van de bedrijven dat de mobiele bedreigingen de andere typen bedreigingen hebben ingehaald. Dit komt waarschijnlijk omdat mobiele devices moeilijk te beheren en beveiligen zijn, vanwege hun persoonlijke karakter – en kwaadwillige geesten zijn zich bewust van deze tekortkoming in de beveiliging.

92% van de FT 500-bedrijven zei in een onderzoek zich zorgen te maken dat hun mobiele werknemers een toenemend risico op beveiligingsproblemen vormen. De meeste organisaties hebben een beleid voor eigen devices ingesteld, maar de overgrote meerderheid (94%) zei dat eigen devices zorgen voor meer mobiele beveiligingsrisico's.

Thuiswerken blijft waarschijnlijk deel uitmaken van de standaard bedrijfsvoering, zelfs nadat voldoende mensen zijn gevaccineerd tegen COVID-19. IT-teams moeten dus maatregelen instellen die aansluiten bij de behoeften van een breed scala aan beheerde en niet-beheerde devices en netwerken. Ze moeten er verder voor zorgen dat externe devices niet langer een randgebeuren zijn van het beveiligingswerk, maar de risicogegevens van alle eindpunten samenbrengen in het Security Operations Center.




**Volgens onze gegevens zijn 67% van de mobiele devices geregistreerd bij software voor devicebeheer, zoals MobileIron of VMware Workspace ONE.**

Copyright © 2021 Wandera

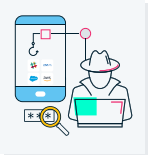
RISICOFACTOR 2

# Gebruikers

**Besturingssystemen zijn gebouwd om de meeste beveiligingsbedreigingen te beperken. Apple en Google hebben grote stappen ondernomen om de beveiliging van hun besturingssystemen en app-stores te versterken. Maar risico's kunnen zich voordoen door gebruikersgedrag. Om inzicht te krijgen in gebruikersrisico's moeten we onderzoeken hoe bepaalde aanvallen gebruikmaken van de zwakke punten van gebruikers. Maar we moeten ook kijken naar het gedrag van gebruikers dat de beveiliging van devices verzwakt en de deur opent voor aanvallen.**

## De gebruiker als mikpunt

Hackers slagen er nog altijd in om beveiligde besturingssystemen te omzeilen met social engineering-aanvallen zoals phishing, waarbij wordt geprobeerd een gebruiker te bedriegen om deze gevoelige informatie te laten overhandigen. Kwaadwilligen kunnen ook onveilige openbare Wi-Fi-netwerken misbruiken om het verkeer van gebruikers te onderscheppen. Daarnaast zijn er ook malafide apps die gebruikers kwetsbaar maken voor dataverlies, zoals identiteitsdiefstal, financiële diefstal of andere oplichting.

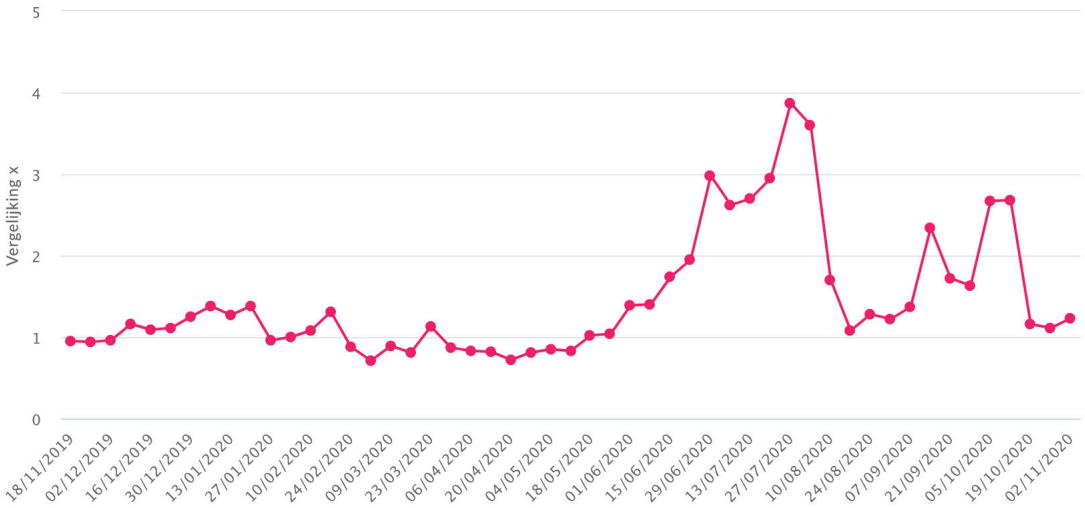


DE GEBRUIKER ALS MIKPUNT

### Phishing

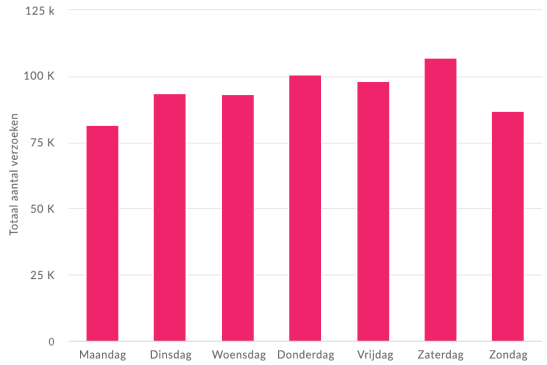
Phishing blijft de grootste bedreiging voor gebruikers van draagbare devices. Phishing-aanvallen zijn meestal gericht op onderwerpen, merken of thema's waarmee makkelijk slachtoffers kunnen worden gelokt. Zo zijn er elk jaar wanneer de belastingaangifte moet worden ingediend meer phishing-aanvallen met berichten waarin de afzender zich voordoet als de Amerikaanse, Britse of Australische belastingdienst. En in de eerste helft van 2020 zagen we een stijging van het verkeer naar corona-gerelateerde phishing-sites, en zelf een imitatie van de webshop van een bekende producent van desinfectiemiddelen.

**De onderstaande grafiek toont de toename van phishing-aanvallen op werknemers op afstand gedurende 2020.**




Copyright © 2021 Wandera

Op zoek naar andere phishingtrends van 2020 viel ons op dat phishing-aanvallen het vaakst worden uitgevoerd op zaterdag. Op het hoogste punt in het weekend komen ze 6% meer voor dan op het hoogste punt tijdens werkdagen. Dit onderstreept het idee dat wanneer werknemers niet 'in de werkstand staan', hun ontspannen toestand hen kwetsbaarder maakt voor phishing-aanvallen op zakelijke devices.





DE GEBRUIKER ALS MIKPUNT

## Man-in-the-Middle-aanvallen via Wi-Fi

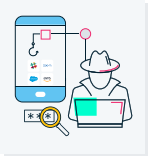
Wi-Fi-netwerken vormen een groot privacyrisico wanneer zich een Man-in-the-Middle-aanval (MITM) voordoet. Er zijn twee belangrijke vormen van MITM-aanvallen die van invloed zijn op mobiele gebruikers. In het eerste geval heeft de aanvaller de fysieke controle over de netwerkinfrastructuur, zoals een nep Wi-Fi-toegangspunt, zodat al het gegevensverkeer daarop kan worden gevolgd. Bij de tweede strategie manipuleert de aanvaller het netwerkprotocol dat gegevens zou moeten versleutelen, waarmee gegevens die beschermd zouden moeten zijn, kwetsbaar worden. Het is schrikbarend dat meer dan 80% van de werknemers een openbaar Wi-Fi-netwerk gebruiken voor werkactiviteiten, zelfs wanneer dat officieel verboden is.

> In 2020 was 4% van de gebruikers elke week verbonden met een risicovolle hotspot, vergeleken met 7% in 2019.

**Hier ziet u hoe de impact van dreigingen via de Wi-Fi, met inbegrip van MITM-aanvallen, is veranderd gedurende 2020.**


Bij onze analyse hielden we rekening met een daling om een voor de hand liggende reden – mensen reizen niet zoveel voor hun werk als voor het coronavirus (dat echt toesloeg rond februari en maart 2020). De grafiek laat een kleine stijging zien in januari, toen werknemers terugkeerden na de kerstvakantie. In februari zet een scherpe daling in, parallel met de stijging van het aantal Covid-19-gevallen. Werkgevers annuleerden zakenreizen en adviseerden werknemers om thuis te werken voor hun veiligheid.

Copyright © 2021 Wandera



DE GEBRUIKER ALS MIKPUNT

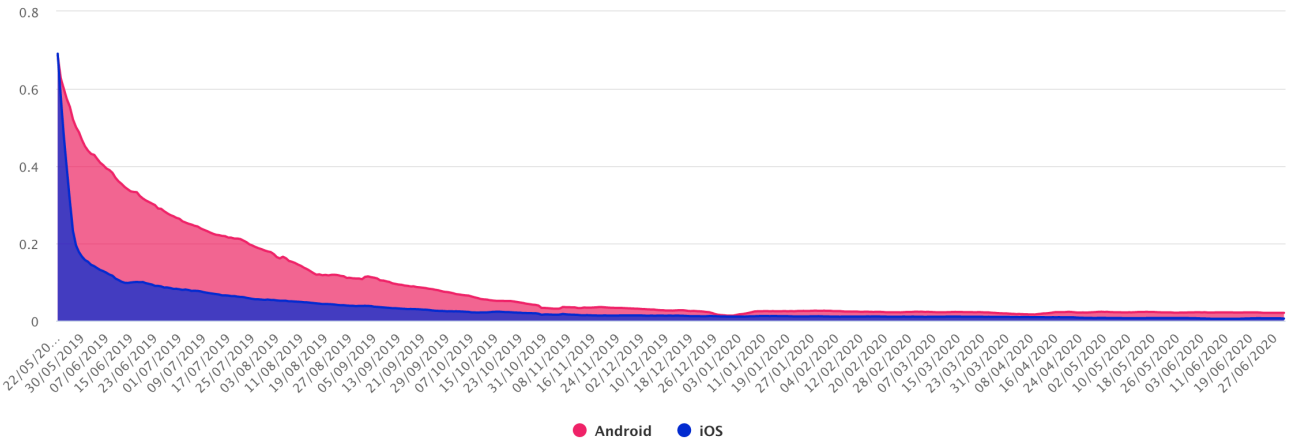
# App-risico's

Schadelijke apps zoals malware gebruiken steeds vaker slimme technieken om detectie te ontlopen. Zo kan geavanceerde malware een aantal stappen wachten voordat schadelijk gedrag begint. Misschien vindt dit alleen plaats op een bepaald netwerk, of bevat de malware een slapende command-and-control-code die op elk moment kan worden geactiveerd door een hacker. Eenvoudige controles zoals uitgevoerd door app-stores zijn onvoldoende om verfijnde en verrassend vaak voorkomende schadelijke apps op te sporen.

> In 2020 kreeg 52% van de organisaties te maken met een malware-incident op een device op afstand, vergeleken met 37% in 2019.

Naast verborgen malware in applicaties, kunnen apps ook gewoon slecht worden gebouwd, beveiligd, of onderhouden door de ontwikkelaars, waardoor ze gevaarlijk kwetsbaar kunnen zijn, zoals het geval was bij WhatsApp in 2019 en 2020.

> In de onderstaande grafiek ziet u dat Android-gebruikers er langer over deden om hun apps bij te werken nadat in mei 2019 een grote kwetsbaarheid was gevonden in een oudere versie van WhatsApp. Tussen half mei en half juli 2019 was ongeveer 85% van de resterende devices met risicovolle versies van WhatsApp bijgewerkt. Maar slechts ongeveer 50% van de kwetsbare Android-devices werd in die periode bijgewerkt.




Apps kunnen 'scams' (pogingen tot oplichterij) of andere frauduleuze activiteiten bevatten. Vaak worden hiervoor advertenties van derden gebruikt. We hebben apps gezien die de officiële controles van de app-store hebben doorlopen, maar desondanks bomvol pop-upadvertenties zitten die het hele scherm overnemen, waarmee het device onbruikbaar wordt. We noemen dit mogelijk ongewenste apps en treffen er een aan op 1 van de 200 devices.

Er zijn zelfs ontwikkelaars die zo slordig zijn dat ze geen versleuteling toepassen en daarmee de gebruiker (en ook de werkgever) blootstellen aan het risico van gegevensverlies.

- 15% van de organisaties had in 2020 minstens één device met een app die wachtwoordgegevens lekte, vergeleken met 11% in 2019
- iOS-devices liepen in 2020 een 3,2 maal zo groot risico om getroffen te worden door lekkende applicaties dan Android-devices

Uit onze recente analyse blijkt dat zodra het risico is geïntroduceerd door een niet-goedgekeurde app, het risico toeneemt.

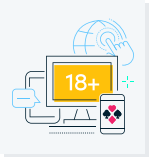
- Bedrijven met minstens één door malware getroffen device, lopen een 4,4x zo groot risico om te maken te krijgen met een wachtwoordlek dan andere bedrijven.
- Gebruikers met een kwetsbare applicatie op hun device lopen 59x zoveel risico om in aanraking te komen met pogingen tot cryptojacking dan andere gebruikers.

Het onafhankelijk controleren van de veiligheid van een app is arbeidsintensief werk, maar noodzakelijk. Met meer devices dan ooit tevoren, hebben gebruikers toegang tot allerlei applicaties. Het gebruik is niet altijd slecht bedoeld; misschien wil een gebruiker een tool voor het samenvoegen van pdf's of een andere app gebruiken die niet is goedgekeurd door IT, maar deze app kan risico's met zich meebrengen. Er zijn twee belangrijke redenen waarom de IT-afdeling op de hoogte moet zijn van de apps die medewerkers willen gebruiken voor hun werk. Ze moeten worden beoordeeld op veiligheid en uit het oogpunt van productiviteit. Als het veilige apps zijn die de productiviteit ten goede komen, moeten ze worden omarmd en beschermd.

Copyright © 2021 Wandera

# De gebruiker als slechte beslisser

In het vorige gedeelte bespraken we risico's die beginnen bij de gebruiker, met de gebruiker in een hoofdzakelijk passieve rol. We gaan nu kijken naar risico's die eveneens beginnen bij de gebruiker, maar waarbij deze een actievere rol speelt, bijvoorbeeld door bewust het bedrijfsbeleid en de beveiligingsmaatregelen te omzeilen. Gebruikers kunnen zich problemen op de hals halen door slechte beslissingen te maken, zoals het bekijken van niet-conforme content, of door te knoeien met de beveiliging van hun devices zoals het jailbreaken van devices, sideloaden van apps en het uitschakelen van vergrendelingsschermen.

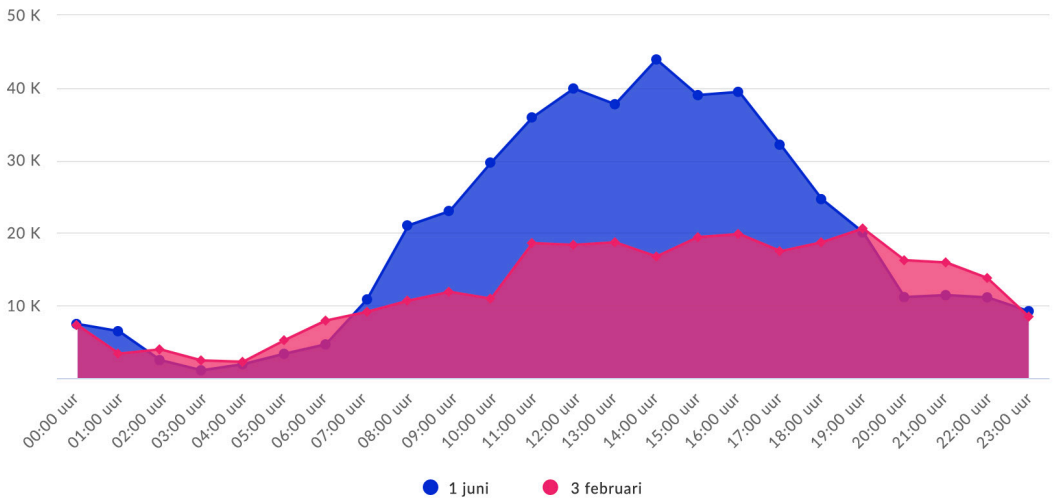



DE GEBRUIKER ALS SLECHTE BESLISSER

## Ongepaste content

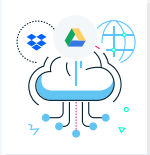
Met devices in uw IT-infrastructuur die toegang bieden tot de donkerste krochten van het internet, dient zich een risico voor uw bedrijfsvoering aan. Met ongepaste content bedoelen we de categorieën content die gericht zijn op volwassenen, gokken, extreme onderwerpen en illegale zaken. Voor dergelijke inhoud geldt dat het risico op datalekken, gebruik van technologieën zonder versleuteling en andere zaken die een organisatie kwetsbaar maken, veel groter is. Verrassend genoeg zijn er veel mensen die de schaduwzijde van het internet bezoeken met hun werkdevice.

In vergelijking met pre-coronatijden, zagen we een opmerkelijke toename van maximaal 100% van verbindingen met ongepaste inhoud tijdens kantooruren. Bij het thuiswerken is het uiteraard noodzakelijk dat medewerkers het beleid voor acceptabel gebruik op afstand naleven op hun devices.




Het filteren van content is een effectieve manier om het bedrijfsbeleid voor acceptabel gebruik te handhaven op een breed scala aan eindpunten om de juridische risico's en die op het gebied van veiligheid en naleving te beperken, voor zowel werknemers als hun werkgevers.

Copyright © 2021 Wandera



DE GEBRUIKER ALS SLECHTE BESLISSER

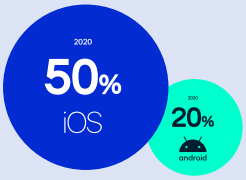
# Het omzeilen van beveiligingsmaatregelen

Gebruikers worden niet altijd zomaar geconfronteerd met risico's; soms maken ze hun devices kwetsbaar, al dan niet opzettelijk.

## Jailbreaken

Door een device te jailbreaken (iOS) of te rooten (Android), maakt een gebruiker het besturingssysteem vrij. Deze risicovolle configuratie maakt het mogelijk om niet-goedgekeurde softwarefuncties en -toepassingen te installeren. Dergelijke methodes worden ook vaak gebruikt om devices simlockvrij te maken.

- In 2020 steeg het aantal vrijgemaakte iOS-devices met 50%, terwijl het aantal vrijgemaakte Android-devices toenam met 20%.
- De kans dat vrijgemaakte devices in aanraking komen met schadelijk netwerkverkeer is 28% groter dan voor devices die niet zijn vrijgemaakt.
- Bedrijven met minstens één vrijgemaakt device onder hun beheer lopen 31,6x zoveel risico dat devices te maken krijgen met schadelijk netwerkverkeer dan andere bedrijven.
- Bij vrijgemaakte devices is de kans dat een app met een bekende kwetsbaarheid is geïnstalleerd, 33x groter dan bij devices die niet zijn vrijgemaakt.




**In 2019 steeg het aantal vrijgemaakte iOS-devices met 50%, terwijl het aantal vrijgemaakte Android-devices toenam met 20%**

## Apps sideloaden

Er zijn iOS-gebruikers die bewust hun mobiele device vrijmaken om beveiligingsverbeteringen te installeren, maar de meeste gebruikers doen het om applicaties te installeren die niet beschikbaar zijn in de officiële app-stores. Het is ook mogelijk om apps van derden te installeren zonder het device vrij te maken. Dit wordt gedaan door apps te sideloaden. De gebruiker hoeft het device alleen zo te configureren dat het een bepaalde ontwikkelaar vertrouwt, waarna elke app van die ontwikkelaar kan worden geïnstalleerd zonder de app-store te bezoeken. Op deze wijze installeren veel bedrijven apps voor hun werknemers, zonder dat ze in de App Store hoeven te worden gepubliceerd.

Google vergrendelt het besturingssysteem van Android niet zo strikt als Apple doet met iOS. Met de standaardconfiguratie van Android is het niet mogelijk om apps te sideloaden, maar de instellingen kunnen worden gewijzigd om apps van derden toe te staan. Volgens onze informatie hebben een op de vijf Android-gebruikers hun devices zo geconfigureerd dat apps van derden kunnen worden geïnstalleerd.

Gebruikers die apps sideloaden lopen een verhoogd veiligheidsrisico omdat het controleproces van de officiële app-stores van Apple en Google wordt omzeild. Het device is dus minder beschermd tegen onopzettelijk geïnstalleerde malware.


**In 2020 had 1 op de 10 Android-devices die worden gebruikt voor werk een app-store van derden geïnstalleerd (een andere app-store dan Google Play).**

FOCUS OP DE SECTOR - JURIDISCHE SECTOR

De kans dat gebruikers in de juridische sector apps sideloaden en installeren op hun device, is 2,5x groter dan in andere sectoren.

FOCUS OP DE SECTOR - PRODUCTIE

De kans dat devices in de productiesector te maken krijgen met malware is tweemaal zo groot als in vergelijking met andere sectoren. Dit houdt wellicht verband met het feit dat 50% meer gebruikers een app-store van derden hebben geïnstalleerd, en dat de kans dat Android-gebruikers onbekende bronnen hebben ingeschakeld, tweemaal zo groot is.

Copyright © 2021 Wandera

## Het vergrendelingsscherm uitschakelen

Het wekt verbazing dat een van de eenvoudigste beveiligingsmaatregelen voor een mobiel device nog vaak wordt genegeerd: het vergrendelingsscherm. Op de meeste devices is het vergrendelingsscherm standaard actief, maar sommige gebruikers nemen de moeite om het uit te schakelen, waardoor hun devices kwetsbaarder zijn wanneer ze gestolen worden. Het wijst ook op slechte beveiligingsgewoonten, en uit onze gegevens blijkt dat zich meer andere dreigingen voordoen op devices waarbij deze fundamentele veiligheidsmaatregel is uitgeschakeld.

- In 2020 had 3% van de devices die worden gebruikt voor werk het vergrendelingsscherm uitgeschakeld, vergeleken met 6% in 2019.
- Gebruikers die hun vergrendelingsscherm uitschakelen, lopen een 16x groter risico dan andere gebruikers op een besturingssysteem met een bekende kwetsbaarheid.
- Gebruikers die hun vergrendelingsscherm uitschakelen, lopen 2,4x meer risico dat hun e-mailadres wordt gelekt dan andere gebruikers.

FOCUS OP DE SECTOR - IT-DIENSTEN

Gebruikers werkzaam in IT-dienstverlening hebben 2,2x zo vaak hun vergrendelingsscherm uitgeschakeld op hun devices, in vergelijking met wereldwijde gemiddelden.

**In 2020 had 3% van de devices die worden gebruikt voor werk het vergrendelingsscherm uitgeschakeld, vergeleken met 6% in 2019**

Copyright © 2021 Wandera

RISICOFACTOR 3

# Toegang op afstand

**We hebben nu gekeken naar risico's die verband houden met het device en het besturingssysteem, en naar risico's die door de gebruiker worden veroorzaakt. Maar hoe zit het met het hieraan gekoppelde risico voor gevoelige zakelijke applicaties wanneer de toegang op afstand slecht is geconfigureerd of helemaal niet is beveiligd? Voor welke bescherming moeten we zorgen tussen het risicovolle device of de risicovolle gebruiker en de gevoelige gegevens in zakelijke apps?**

**Bij de bescherming van zakelijke applicaties gaat het niet om de bescherming van apps of Mobile Application Management (MAM), maar om veilige toegang tot gevoelige intellectuele eigendom in die applicaties en taken in de cloud.**

**Volgens het Remote Workforce Security Report 2020 van Cybersecurity Insiders laat 65% van de organisaties hun medewerkers beheerde applicaties openen vanaf onbeheerde devices in privébezit.**

**En het IDC-rapport Remote Access and Security Challenges & Opportunities stelt dat 40% van de internetlekken beginnen bij geautoriseerde gebruikers die ongeautoriseerde systemen gebruiken.**

## Een veelvoud aan zakelijke apps op allerlei plekken

Eén ding weten we zeker in de beveiligingssector: de ondervraagde IT-professionals zijn dol op de cloud. Volgens de resultaten in het rapport Cloud Adoption in 2020 van O'Reilly's kiezen 39% van de organisaties voor een hybride model met privé- en openbare cloudoplossingen. En in dit onderzoek antwoord meer dan 56% dat ze momenteel werken aan cloudmigratieprojecten voor dit jaar, of deze aan het plannen zijn.

**39%**

van de organisaties gebruiken een hybride model met privé- en openbare cloudoplossingen

**56%**

van de respondenten zei dat ze momenteel werken aan cloudmigratieprojecten voor dit jaar, of deze aan het plannen zijn.

Uit deze gegevens blijkt dat veel organisaties een gedecentraliseerde hybride omgeving gebruiken – of hiernaar op weg zijn – waarin data in een diverse infrastructuur is opgeslagen. Er zijn organisaties die voor altijd het beheer zullen behouden over bepaalde applicaties, maar met cloud- en SaaS-oplossingen komen applicaties buiten de bedrijfsgrens, wat de toegang ertoe een kritiek thema maakt voor beveiligingsdiensten.

Cloudapplicaties zijn geliefd binnen het hedendaagse bedrijfsleven. Ze zijn eenvoudig en goedkoop om te implementeren, beheren en onderhouden voor een bedrijf. Daarnaast hebben zowel privé- als openbare clouddiensten een aanvaardbare reputatie opgebouwd, waardoor ze een goede optie zijn voor bedrijven van alle grootte. Op vergelijkbare wijze genieten SaaS-oplossingen de voorkeur voor bepaalde toepassingen, omdat de organisatie zich helemaal niet druk hoeft te maken over ontwikkeling en onderhoud. Het lijdt geen twijfel dat bij SaaS de beloning opweegt tegen het risico: waarom zou je een waterput graven als je gewoon een kraan kunt opendraaien? Gartner voorspelde dat SaaS-oplossingen in 2020 alleen al bijna $ 105 miljard zullen genereren.

Nu veel organisaties apps naar de cloud verplaatsen en meer SaaS-apps gebruiken, beheren ze meer apps dan ooit, op meer plekken dan ooit. Daarbij stelt Okta dat hoe groter de organisatie is, hoe meer apps er worden gebruikt.

Okta ziet dat het aantal softwareapplicaties dat in alle sectoren wereldwijd door grote bedrijven wordt ingezet, in vier jaar met 68% is gestegen, waarmee eind 2018 een gemiddelde van 129 apps per bedrijf werd bereikt. Bijna 10% van de bedrijven had ten tijde van het onderzoek meer dan 200 apps.

Copyright © 2021 Wandera

# Tijd voor moderne toegang op afstand

Er was een tijd dat ondernemingen één ding moesten beschermen: het datacenter. En ze hadden ook fysieke controle over dat ding. Oudere tools voor toegang op afstand zoals VPN en RDI waren ontwikkeld rond het principe van de bedrijfsgrens en werkten naar behoren toen applicaties vanuit het datacenter werden uitgevoerd. Bij het zogenoemde kasteel-en-gracht-beveiligingsmodel wordt iedereen binnen het netwerk per definitie vertrouwd. Hierdoor konden potentiële aanvallers toegang krijgen tot hele netwerksegmenten, omdat VPN's en RDI's impliciet verbindingen vertrouwen, zonder een grondige controle van de identiteit van de gebruiker of de veiligheid van het device.

Volgens IDC werd in 68% van de grote incidenten met tools op afstand gebruikgemaakt van VPN. En 40% van de internetlekken beginnen bij geautoriseerde gebruikers die ongeautoriseerde systemen gebruiken.

Waarom zijn voortdurende risicobeoordelingen een belangrijk onderdeel van de strategie voor toegang op afstand? De getallen spreken voor zich:

- 1 op de 83 devices met een kwetsbaar besturingssysteem werd in 2020 ten tijde van de kwetsbaarheid gebruikt om e-mail te openen, terwijl 1 op de 6 actief gebruikmaakte van cloudopslag.
- Van de mobiele devices die in 2020 door mobiele malware werden getroffen, bleef 37% zakelijke e-mails openen en 11% bleef gebruikmaken van cloudopslag.
- Bij 42% van de bedrijven met door malware getroffen devices bleek dat minstens één van de getroffen devices productiviteitstools gebruikte.
- 1 op de 200 devices die toegang hebben tot cloudopslag, heeft het vergrendelingsscherm uitgeschakeld.
- Bij meer dan 40% van de bedrijven met gebruikers met kwetsbare besturingssystemen maakt minstens een van die kwetsbare devices actief gebruik van cloudopslag.
- 1,3% van de klanten heeft een device dat is getroffen door malware en waarmee productiviteitstools worden gebruikt, inclusief Office 365 en Google Workspace.
- Het is dus duidelijk dat gebruikersverificatie alleen onvoldoende is om gevoelige zakelijke gegevens te beschermen tegen getroffen devices. Wat is de oplossing? Zero Trust Network Access is fundamenteel anders dan de traditionele aanpak. Geen dozen meer, geen applicaties, geen fysieke devices. En – heel belangrijk! – via de cloud geleverde netwerkbeveiliging is schaalbaar. Zonder is het simpelweg onmogelijk om voldoende applicaties aan te schaffen om al die data te beschermen die over de bedrijfsgrens wordt verplaatst naar de cloud.

Bovendien kan Zero Trust Network Access continue risicobeoordelingen uitvoeren van de devices die toegang vragen tot uw gevoelige applicaties, om te controleren of het device conform is. En dat kan verschillende dingen betekenen: of het op een goed netwerk is, op de verwachte locatie, vrij van infecties en kwetsbaarheden, en of de gebruiker geautoriseerd is om een bepaald verzoek te doen.

**42%**

van de bedrijven met door malware getroffen devices gebruiken productiviteitstools met minstens een van die getroffen devices.

**1 op de 83 devices met een kwetsbaar besturingssysteem werd in 2020 ten tijde van de kwetsbaarheid gebruikt om e-mail te openen, terwijl 1 op de 6 actief gebruikmaakte van cloudopslag.**

Copyright © 2021 Wandera

RAPPORT CLOUDBEVEILIGING

# Aanbevelingen

**Ondanks jarenlange pogingen om zakelijke IT-standaarden vast te stellen, hebben veel bedrijven een punt bereikt waar het gebrek aan standaardisatie de norm is. Welk besturingssysteem gebruikt uw bedrijf? Allemaal. Welk type gebruiker geeft u toegang tot uw apps? Iedereen. Vanaf welke locaties mogen gebruikers werken? Vanaf overal.**

**Oplossingen voor veilige toegang op afstand moeten flexibel genoeg zijn om mogelijkheden te creëren. Ze opties blokkeren en productiviteit hinderen. Wij adviseren het gebruik van deze checklist voor het ontwikkelen van een moderne SASE-beveiligingsstrategie die aansluit bij de behoeften van de IT-omgevingen van vandaag.**

## Maak een overzicht van de vereisten op basis van de nieuwe gebruikssituaties van werken op afstand.

- Wat moeten uw medewerkers kunnen doen op hun devices: hun e-mail gebruiken of toegang hebben tot gevoelige databases? Categoriseer de gegevens, zodat u gedetailleerd toegang kan toewijzen.
- Evalueer uw gebruikssituaties en definieer vereisten voor uw personeel op afstand.
- De bovenstaande vereisten zullen bepalend zijn voor het eigendomsmodel voor uw devices: welke typen device zult u ondersteunen, wie zal ze bezitten en hoe worden ze beheerd?

## Connectiviteit

- Bepaal wat u moet weten over gebruikers, devices, netwerken en apps in verband met connectiviteit en cloudapplicaties, voordat u hen toegang geeft tot bedrijfsmiddelen.
- Beperk gebruikers tot de zakelijke tools die ze nodig hebben. Hiermee voorkomt u dat accounts met onnodig veel privileges worden misbruikt om grote aantallen systemen aan te vallen.

## Definieer acceptabel gebruik

- Herzie uw bestaande beleid voor acceptabel gebruik en zorg ervoor dat alle soorten eindpunten worden meegenomen.
- Voer een beleid in voor acceptabel gebruik voor elke toepasselijke subset van devices voor het beheersen van ongewenst gebruik en gebruik van IT, IT-devices, IT-toepassingen, etc. zonder expliciete toestemming, en om te zorgen voor naleving van de regelgeving.

## Neem risico's van individuele eindpunten op in het beleid voor toegangsbeheer

- Implementeer een gebruiksvriendelijke IAM-oplossing (Identity and Access Management) voor verificatie van zakelijke apps op alle devices, inclusief mobiel.
- Neem risicobeoordelingen van devices op in uw IAM-beleid om risico's van individuele eindpunten te kennen.
- Zorg dat risico's van individuele eindpunten tijdens een sessie continu worden geëvalueerd.

Copyright © 2021 Wandera

## Gebruik eindpuntbescherming op alle devices. Een cloudgebaseerde beveiligingsoplossing is vooral belangrijk voor het beschermen tegen het brede spectrum van cyberbedreigingen en gebruiksrisico's.

- Zorg dat uw beveiligingsoplossing goed is uitgerust om eindpunten op te sporen en voorzien is van een in-network-architectuur, zodat aanvallen worden voorkomen voordat ze een device bereiken.
- Zorg dat uw beveiligingsoplossing zowel externe cyberbedreigingen aankan (zoals phishing, Man-in-the-Middle-aanvallen, malware) als risico's voortkomend uit gebruikersgedrag (apps sideloaden, etc.).
- Alle beveiligingstools moeten de toepasselijke configuraties hebben voor de bedreigingen die van toepassing zijn op uw bedrijfsvoering en tegelijk de privacy van uw eindgebruikers respecteren.
- Evalueer het vermogen voor machine-learning van de beveiligingsoplossing om te begrijpen hoe de 'threat engine' nieuwe bedreigingen identificeert en ertegen beschermt.

## Gebruik een UEM voor de controle op device-niveau

- Gebruik – indien van toepassing – een UEM-oplossing (Unified Endpoint Management) waarmee u devices kunt uitrusten met bedrijfsmiddelen en voortdurende controles op naleving door devices kunt uitvoeren.

## Bekijk deze lijst regelmatig en overweeg of u veranderingen moet doorvoeren, op basis van het volgende:

- Wijzigingen in de aard en omvang van het bedrijf, bijvoorbeeld als gevolg van fusies of overnames.
- Nieuwe regelgeving die van invloed is op uw omgang met gegevens.
- Veranderende IT-strategie.
- Bedreigingen die medewerkers hebben geraakt.
- Nieuwe applicaties die medewerkers nodig hebben voor hun werk.

Jamf helpt organisaties succesvol te zijn met Apple. Door eindgebruikers met behulp van IT de controle te geven, brengen we de legendarische Apple ervaring naar het bedrijfsleven, het onderwijs en de overheid.

wandera
a Jamf company