

De Mobiele Overheid

Uitdagingen en oplossingen voor mobiele apparatuur
bij overheidsorganisaties

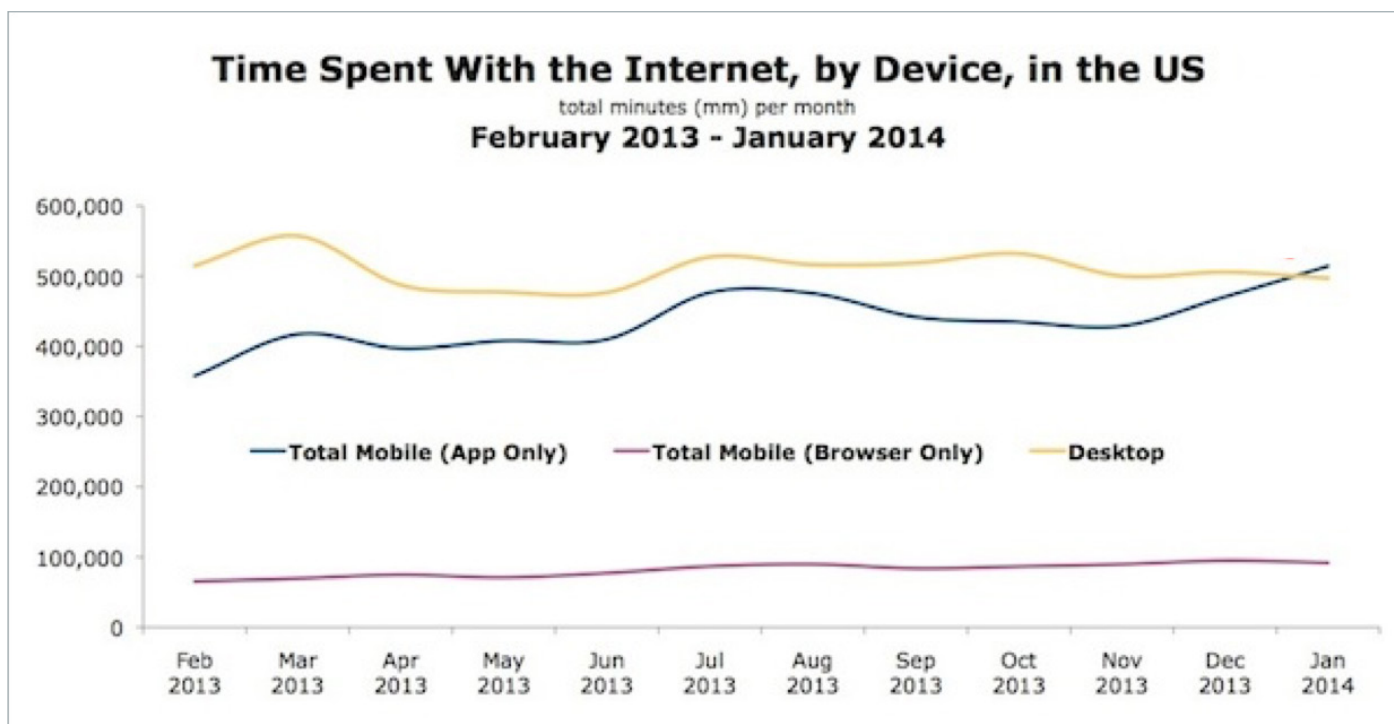


Inhoudsopgave

Inleiding	3
Gebruik mobiele apparatuur	4
Beheer	6
Beveiliging	10
Conclusie	15

Inleiding

Sinds de komst van de smartphone ziet de wereld van de computers er heel anders uit. Vooral de lancering van de iPhone in 2007 betekende voor het eerst dat de computer in je zak bijna net zo krachtig was als een gewone desktop. In 2014 was het omslagpunt: voor het eerst werd de smartphone meer gebruikt voor internet dan de desktop.

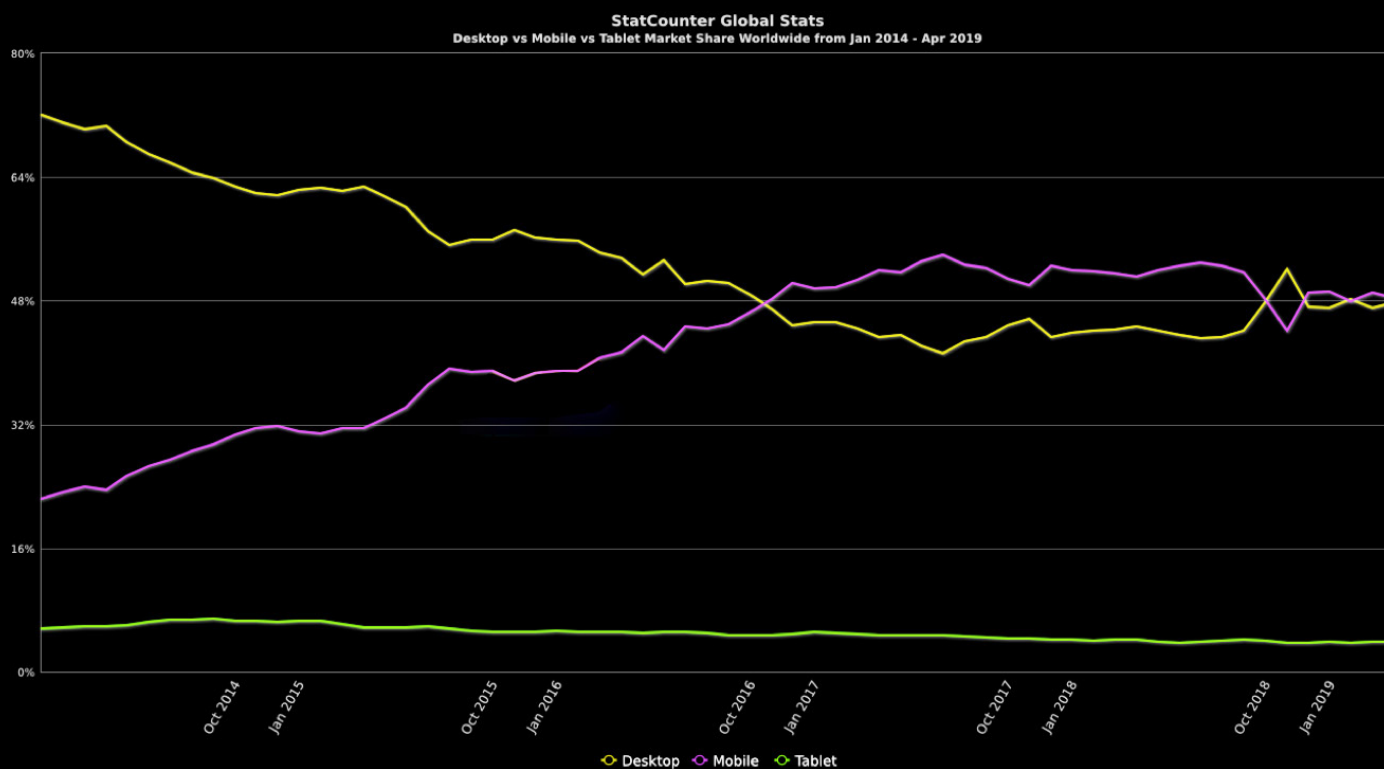


Internetgebruik per apparaat in de VS (februari 2013-januari 2014, in minuten per maand) – Bron: comScore

Dit ging weliswaar over ál het internetgebruik, dus apps en browsen, maar inmiddels ligt het zwaartepunt ook bij alleen websitebezoek bij mobiele apparatuur. Daar lag het omslagpunt in oktober 2016. De laatste cijfers lijken te wijzen op een 50-50 gebruik van desktop en smartphone. De tablet blijft hierbij ver achter.

Er zijn weinig cijfers bekend van het gebruik van mobiele apparaten binnen de overheid, maar er is geen reden om aan te nemen dat dit sterk afwijkt van andere organisaties of in het bedrijfsleven. Wat betekent het voor het Rijk, de provincies, de gemeenten, en uiteraard waterschappen en de grote diversiteit aan bestuursorganen om te moeten gaan met mobiele apparatuur?

Websitebezoek per apparaat wereldwijd (januari 2014 – april 2019)



Bron: StatCounter

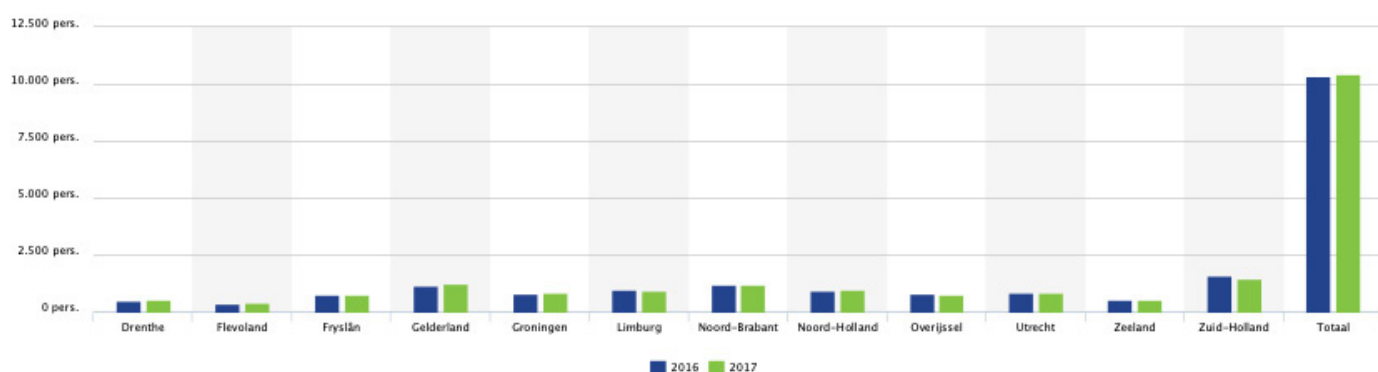
De overheid als moderne werkgever

Dat wordt benadrukt in het stuk Strategisch Personeelsbeleid Rijk 2025, waarin minister Ollongren inzicht geeft in hoe de Rijksoverheid als werkgever de arbeidsmarkt gaat benaderen. Een belangrijke notitie daarin is: *Wendbare medewerker en organisatie: flexibel inspelen op de veranderende omgeving en de veranderende rol en taken voor de overheid door het Rijk en haar medewerkers flexibeler in te zetten. Inzetten op andere manieren van werken en organiseren.*

De populariteit van de smartphone en tablet stelt overheidsorganisaties voor verschillende uitdagingen. Deze apparaten zijn niet alleen bedoeld voor gebruik op kantoor, maar worden ook overal mee naartoe genomen. Hoe zorg je ervoor dat de beveiliging daarbij op orde blijft? Hoe beheer je deze apparaten? En wat doe je met het steeds populairder wordende verschijnsel Bring Your Own Device?

2. Gebruik mobiele apparatuur

Er zijn geen exacte cijfers bekend over het gebruik van mobiele apparatuur zoals smartphones en tablets binnen de overheid. Dat deze devices wel worden ingezet, blijkt uit allerlei documentatie die te vinden is. Sommige overheden hebben al enkele jaren een richtlijn voor het gebruik van smartphone of tablet binnen de organisatie. Zo heeft de provincie Limburg de Gedragscode gebruik smartphone¹, waarin is vastgelegd dat aan elke medewerker in dienst van de provincie een smartphone voor zakelijk gebruik ter beschikking wordt gesteld. In Limburg gaat het daarbij om ongeveer 950 personen. Alle provincies hebben vergelijkbare regelingen en bepalingen. In totaal werken er bij alle provincies gezamenlijk ruim 10 duizend personen.



Aantal werkzame personen bij de provincies, 2016 en 2017 – Bron: A&O-fonds Provincies²

Gemeenten

Bij de gemeenten zijn vergelijkbare regelingen te vinden, maar daar zijn ze wat creatiever met de titels en inhoud. De gemeente Vlaardingen kent een 'Regeling bruikleen communicatiemiddelen', waar Krimpenerwaard een 'Regeling ICT-middelen' heeft³. Het is aannemelijk dat elke gemeente in Nederland een of andere voorziening heeft voor het uitlenen of in bruikleen geven van ICT-middelen, waaronder smartphones. In totaal werken er bij de gemeenten bijna 161 duizend personen (2017)⁴.

Rijksoverheid

Volgens de Kennisbank Openbaar Bestuur van het Ministerie van BZK stonden er eind 2018 ruim 121 duizend personen in de salarisadministratie van de Rijksoverheid⁵. Over centrale regelingen met betrekking tot ICT-voorzieningen of de verstrekking van een smartphone is geen informatie beschikbaar. Het is duidelijk dat in alle lagen van de overheid smartphones, tablets en notebooks gebruikt worden. Wat zijn daarvan de gevolgen voor beheer en beveiliging?

1 http://decentrale.regelgeving.overheid.nl/cvdr/xhtmloutput/Historie/Limburg/CVDR615456/CVDR615456_1.html

2 <https://personeelsmonitorprovincies.onderzoek.nl/index.cfm?action=main.report>

3 http://decentrale.regelgeving.overheid.nl/cvdr/xhtmloutput/Historie/Vlaardingen/CVDR297591/CVDR297591_1.html.en
http://decentrale.regelgeving.overheid.nl/cvdr/xhtmloutput/Historie/Krimpenerwaard/CVDR622769/CVDR622769_1.html

4 <http://personeelsmonitor2017.aeno.nl>

5 <https://kennisopenbaarbestuur.nl>

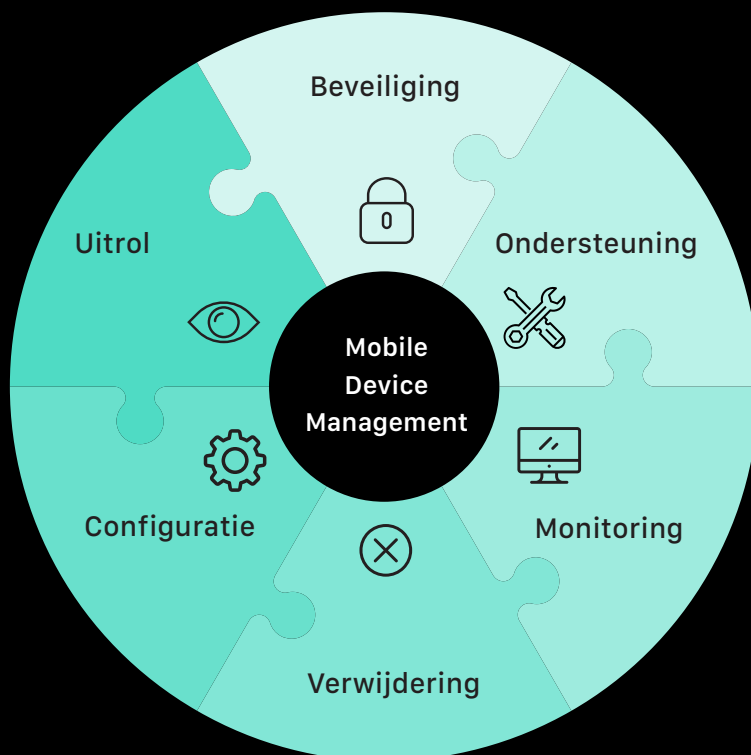
3. Beheer

Het beheer van ICT-apparatuur in middelgrote en grote organisaties – waaronder de meeste overheidsorganisaties vallen – is een flinke uitdaging. Personeelwisselingen zorgen dat er voortdurend nieuwe, standaard geconfigureerde apparaten moeten worden opgeleverd. Dat is met desktops al een hele klus, maar met mobiele apparaten zoals smartphones en tablets is dat nog een stuk lastiger. Grootste probleem is de verscheidenheid aan besturingssystemen, niet zozeer de twee belangrijkste (Android en iOS), maar vooral de verschillende subversies. Android kan door de leveranciers van de smartphones zelf aangepast worden, wat een veelvoud aan versies oplevert. iOS is daarentegen gestandaardiseerd, en zelfs tussen verschillende hoofdversies is weinig verschil als het gaat om beheer.

Mobile device management

De oplossing voor zulke grootschalige omgevingen met mobiele apparaten is mobile device management (MDM). Dit is een all-in beheeromgeving waarin de systeembeheerder controle heeft over welk mobiele apparaat toegang heeft tot welke voorzieningen in de organisatie (op apparaatniveau of op accountniveau). In het geval van iOS betekent dit ook de mogelijkheid om op afstand apps te installeren op iPhones en iPads – of apps (van derden) te verbieden. Vooral in het onderwijs wordt deze functie veel gebruikt voor iPads in de klas.

De functies van Mobile Device Management



Functionaliteit van MDM

De functionaliteit van MDM bestaat uit zes basisonderdelen.



Gestroomlijnde uitrol van configuraties

Deze functie zorgt ervoor dat alle mobiele apparaten een standaardconfiguratie krijgen, met de juiste apps en instellingen. Ook worden hiermee de juiste certificaten op het apparaat gezet, waardoor deze toegang krijgt tot de voorzieningen binnen de organisatie.



Management

Zorgt voor upgrades ('over the air' dus via het draadloze netwerk), het lokaliseren van apparaten, locken en unlocken, en synchronisatie.



Beveiliging

Zorgt ervoor dat de apparaten op de juiste manier zijn beveiligd, onder meer doordat altijd verbinding wordt gemaakt via een VPN, checkt welke apps zijn geïnstalleerd.



Monitoren

Met deze functie worden de verbruiksgegevens van de apparaten in de gaten gehouden, waaronder de opslag op het apparaat, dataverbruik, netwerkgegevens.



Verwijdering

Mobiele apparatuur kan op afstand worden gewist.



Ondersteuning

Via MDM kan ondersteuning worden geboden aan de gebruiker.

MDM en Apple's Device Enrollment Program

Apple heeft een eigen voorziening voor Mobile Device Management, waarbij een organisatie zelf een MDM-server kan opzetten voor alle Apple-apparatuur (iPhones, iPads en Macs). Deze biedt alle functionaliteit hierboven beschreven. Maar in combinatie met het Device Enrollment Program (DEP) van Apple komt hier extra functionaliteit bij.

Nieuw aangeschafte apparatuur – iOS of macOS – kan worden aangemeld bij MDM vóórdat ze in gebruik worden genomen. Daarbij kan de systeembeheerder al configuratie-instellingen opgeven, die meteen bij het opstarten van het apparaat actief worden. Alle apparaten van Apple kennen een configuratie-assistent met stappen die normaliter doorlopen moeten worden door de eerste gebruiker. Via MDM/DEP kan de beheerder aangeven dat bepaalde stappen moeten (of kunnen) worden overgeslagen, bijvoorbeeld omdat ze niet relevant zijn, of omdat die via MDM vooraf al bepaald zijn.

4. Beveiliging

Beveiliging van mobiele apparatuur is al een uitdaging sinds de eerste laptops op de markt verschenen. Deze zijn bij uitstek bedoeld om overal mee naar toe te nemen, zodat ze buiten het bereik en de controle van de systeembeheerder komen. Dit is met de komst van de smartphone en de tablet nog meer een uitdaging. Deze apparaten zijn behalve via een draadloos netwerk ook via het mobiele netwerk van een provider online, waardoor ze op zulke momenten vrijwel helemaal van de radar van een organisatie verdwijnen. Dankzij mobile device management kan dat gelukkig grotendeels ondervangen worden, maar smartphones en tablets vormen een groot beveiligingsrisico voor overheidsorganisaties.

Bring Your Own Device

Het concept Bring Your Own Device (BYOD) vergroot de problemen daarbij ook flink. Veel medewerkers van organisaties hebben al een smartphone en willen deze vaak graag voor zakelijke doeleinden gebruiken. Waarom met twee telefoons rondlopen? Datzelfde geldt overigens ook voor laptops.



50%

van de werknemers zal in **2020** wereldwijd mobiel werken

Bron: MarketWatch



6 van de **10**

organisaties heeft een policy voor BYOD

Bron: Syntonic



In **36%**

van de organisaties maakt minstens **de helft** gebruik van de smartphone voor hun werk

Bron: Cisco

Welke risico's kleven er aan het gebruik van mobiele apparatuur buiten de kantoor-omgeving? En wat kun je doen om deze risico's te vermijden of te minimaliseren?



Onbeveiligde netwerken

Gebruikers die op locatie zijn hebben de neiging om draadloze wifi-netwerken te gebruiken waar mogelijk. Meestal onbewust van de risico's die kleven aan zulke onbeveiligde netwerken. Hotspots in cafés of op straat zijn berucht en kunnen eenvoudig worden afgeluisterd. Het is dan ook zaak om het gebruik van een VPN te forceren, wat bijvoorbeeld heel goed mogelijk is via MDM.



Malware

Lange tijd waren smartphones nauwelijks gevoelig voor malware in de vorm van spyware, adware en ransomware, maar die tijd is helaas voorbij. Er zijn inmiddels zoveel apps beschikbaar, dat het vrijwel onmogelijk is om het kaf van het koren te scheiden. Een uitzondering is het iOS-platform van Apple. Er kunnen alleen apps uit de App Store worden geïnstalleerd, en deze worden vooraf allemaal gecheckt of ze bona fide zijn. Uiteraard kunnen andere apps wél geïnstalleerd worden op iPhones (of iPads) die zijn 'gejailbreakt', waarbij ze zijn voorzien van een niet officiële versie van iOS. Dit speelt uiteraard vooral bij BYOD, zodat het belangrijk is om de staat van deze smartphones en tablets in de gaten te houden binnen MDM.



Verlies en diefstal

Misschien wel het grootste beveiligingsrisico, zeker bij smartphones, is verlies en diefstal. Daarnaast worden laptops en tablets regelmatig gestolen, vaak uit auto's. Wanneer de apparaten slecht zijn beveiligd tegen indringers – bijvoorbeeld door gemakkelijk te raden wachtwoorden, of zelfs helemaal geen pincode bij smartphones – liggen de gegevens van de organisatie op straat. Er zijn verschillende dingen die kunnen worden gedaan om de gevolgen zoveel mogelijk te beperken.

Gegevens kunnen in de cloud worden opgeslagen in plaats van op het apparaat zelf. Dat maakt het aanzienlijk lastiger voor de crimineel om zomaar over de data te beschikken. Gebruikers moeten ook zoveel mogelijk uitloggen uit apps na gebruik. Via MDM kunnen apparaten op afstand worden gelockt en zelfs helemaal gewist. Apple-gebruikers hebben nog een extra optie tot hun beschikking: 'Find your own device'. Hierbij kan op afstand worden gekeken op een kaart waar het apparaat zich (ongeveer) bevindt. Dat werkt zowel voor iPhone als voor iPad én de Mac. Voorwaarde is wel dat het apparaat op enig moment aan staat. Maar zelfs dan is het nog mogelijk om een waarschuwing te krijgen wanneer dit weer online komt.



Er zijn **2,7** miljard smartphonegebruikers **wereldwijd**

Bron: Statista



In 2018 waren er **194** miljard app-downloads

Bron: App Annie



Elk jaar raken er **70** miljoen smartphones kwijt, slechts **7 procent** worden teruggevonden

Bron: Kensington

Andere maatregelen

Natuurlijk zijn er allerlei maatregelen en standaardzaken die voor iedere gebruiker gelden. Zo is het zaak ervoor te zorgen dat het besturingssysteem en de apps altijd up-to-date zijn. Dit kan trouwens eenvoudig worden afgedwongen via MDM. Datzelfde geldt voor de wachtwoordpolicy: sterke wachtwoorden, op tijd een nieuw wachtwoord. Om problemen te voorkomen kun je ook het downloaden van apps (behalve die door de organisatie zijn toegestaan) helemaal verbieden. Vanzelfsprekend geen erg populaire maatregel, maar het kan noodzakelijk zijn voor overheidsinstanties die met vertrouwelijke gegevens moeten werken. Tenslotte kan het noodzakelijk zijn om antivirussoftware te installeren, al is dat (nog steeds) in principe niet nodig op Apple-apparatuur.

Conclusie

Mobiele apparaten zijn niet meer weg te denken in organisaties. Ze bieden zoveel voordelen en flexibiliteit dat eigenlijk niemand nog zonder wil. Dat geldt ook voor overheidsorganisaties. Het beheer en de beveiliging vergt wat meer nadenken en moeite dan bij traditionele desktop-computers, maar is in principe dankzij MDM en Apple's DEP geen probleem meer.