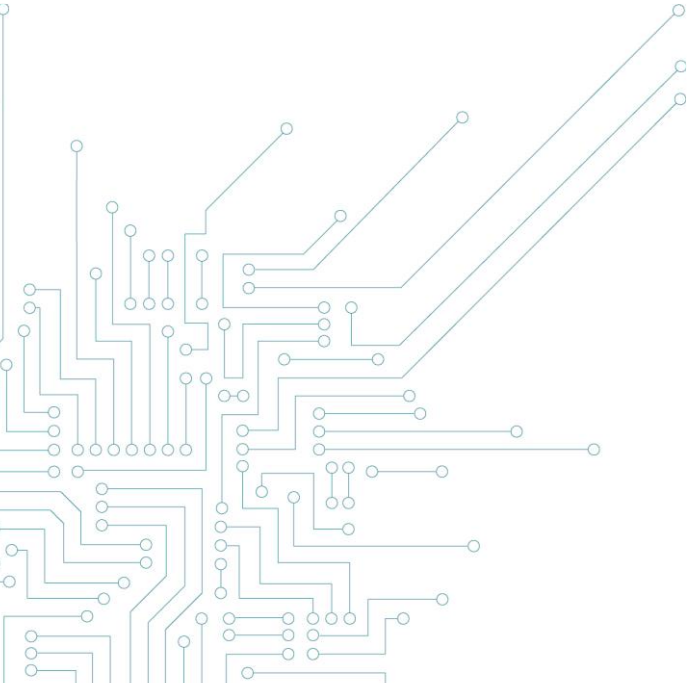
CENTRE FOR CYBER SECURITY BELGIUM

UNDER THE AUTHORITY OF THE PRIME MINISTER

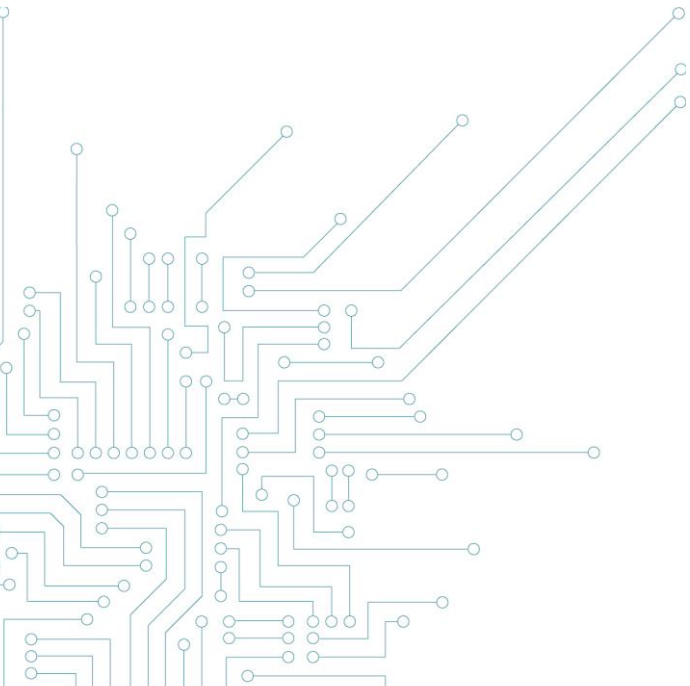
.be

Hoe behoud je de controle over je mobiele apparaten



April 2023

Inhoudsopgave



1 Inleiding

De bedrijfsomgeving en -gegevens kunnen gemakkelijker on-site worden beschermd, maar ook eindgebruikers hebben toegang tot gegevens en bewaren uiteindelijk kopieën op hun mobiele - of soms persoonlijke - apparaten.

Met mobiele apparaten wordt elk apparaat bedoeld dat van buiten het kantoor toegang heeft tot het netwerk en de middelen van de organisatie, dus zowel laptops als smartphones. Laptops worden echter over het algemeen door het bedrijf verstrekt en opgenomen in de beveiligingsstrategie, en door de IT-afdeling geconfigureerd en beveiligd voordat ze aan de werknemer worden gegeven.

Daarom zal dit document zich voornamelijk toespitsen op de bedrijfs- en persoonlijke smartphones die door werknemers worden gebruikt. Deze toestellen en de daarmee verbonden apparaten (smartwatches, enz.) staan open voor de wereld, onder meer via de sociale netwerken. Ze vormen een hub van belangrijke persoonlijke, professionele of vertrouwelijke gegevens.

Of je nu een privépersoon bent, een werknemer in een kritieke sector, een minister, een militair of wie dan ook, de verzamelde gegevens moeten zorgvuldig worden beschermd. Het gaat om je locatie, biometrische gezondheid en gewoonten. Ze zijn waardevol en dreigen onbedoeld uit te lekken of te worden bespioneerd, niet alleen door privébedrijven, maar ook door concurrenten, andere landen of criminelen.

Het probleem van de gegevensbeveiliging is niet alleen technisch of direct afhankelijk van de gebruiker. Het kan ook voortkomen uit de wetgeving van het land waar de gegevens worden gehost. Want sommige landen geven de overheid bij wet toestemming om de uitgewisselde en opgeslagen gegevens van gebruikersaccounts te raadplegen. Dit kan zowel gelden voor een cloudoplossing die automatisch gegevens synchroniseert als voor wat gebruikers via sociale netwerken delen.

Als je een openbare gezagsdrager bent of als je persoonlijk een risico kunt vormen vanwege je positie of je kennis, moet je ook in een privé-context rekening houden met je bescherming en op zijn minst je persoonlijke en professionele digitale leven volledig gescheiden houden. Meer nog, je zou er goed aan doen de persoonlijke gegevens die je op sociale netwerken deelt in het algemeen te beperken. Die zouden namelijk tegen jou of je omgeving kunnen worden gebruikt.

In dit artikel bespreken we de beste praktijken en technologieën voor Mobile Device Management (MDM) op mobiele apparaten. Ze zijn bedoeld om gegevens die buiten de beveiliging van het bedrijfsnetwerk vallen en persoonlijke gegevens te beschermen.
Tegenwoordig omvatten de meeste MDM-oplossingen DLP. Daarom gaan we het hebben over de integratie van mobiele apparaten met MDM-oplossingen.

2 Device management policy

Eerst en vooral moet de organisatie de risico's identificeren en bepalen. Zoals in de inleiding uiteengezet, verschilt de situatie afhankelijk van jezelf, de omvang van het bedrijf, het kritieke karakter van de sector, de capaciteiten van de concurrenten, kortom: je waarde, en de waarde van de gegevens die je beschermt.

Het organisatiebeleid voor de levering van apparaten zal in de meeste gevallen een van de volgende zijn:

- Bedrijfsapparaat: het apparaat wordt gekocht en geconfigureerd door de organisatie.

- Bring Your Own Device (BYOD): de tools van de organisatie en de toegang worden ingesteld op het apparaat van de werknemer.

De beste aanpak is een evenwicht te vinden tussen veiligheid en werkcomfort voor de werknemers. Een volledig beperkte toegang is veiliger, maar maakt het leven van de werknemers ingewikkeld en misschien onproductief. Als werknemers toestemming hebben om hun persoonlijke apparaten te gebruiken (voor de organisatie misschien om financiële redenen), is het normaal dat zij eigenaar blijven van hun hardware en er voldoende rechten op behouden.

In een BYOD-situatie is de gebruiker eigenaar van het apparaat, niet de organisatie. Dit maakt het voor IT wat lastiger om de beveiliging in te stellen en te handhaven.

Een situatie waarbij het bedrijf eigenaar is, is duidelijker. De IT-afdeling kan alle gewenste beperkingen opleggen, zoals het verwijderen van administratieve toegang tot het apparaat, het kiezen van de toepassingen die worden geïnstalleerd, het beperken van de toegang tot bronnen afhankelijk van de locatie, het blokkeren van synchronisaties met externe providers, en al het nodige beleid om ongewenste acties te voorkomen.
Maar is het mogelijk een dergelijke "bedrijfs"-beveiliging toe te passen op persoonlijke apparaten? Hieronder vind je een aantal elementen van antwoord.

3 Minimale beveiligingsconfiguratie

Als je met gegevens te maken hebt, wil je er altijd zeker van zijn dat de persoon die er toegang toe heeft, geïdentificeerd is en voldoende rechten heeft. Je zult ook willen dat het kanaal waarlangs de gegevens worden doorgestuurd niet door iemand anders kan worden gelezen. Verder zal je er zeker van willen zijn dat de gegevens niet door iemand anders kunnen worden gelezen wanneer ze worden opgeslagen. Dit zijn de drie principes die integriteit, vertrouwelijkheid en authenticiteit garanderen.

Op grond daarvan moet elk mobiel apparaat dat toegang heeft tot bedrijfsinformatie of deze opslaat ten minste:
- geconfigureerd zijn voor gebruikersidentificatie en sterke authenticatie (sterk wachtwoord, MFA),
- versleuteld zijn,
- actuele anti-malwaresoftware draaien (of beter een EDR die ook abnormaal gedrag detecteert in plaats van alleen bekende handtekeningen),
- en gebruikmaken van VPN-verbindingen (Virtual Private Network) om toegang te krijgen tot het bedrijfsnetwerk.

Voor een zakelijke Microsoft-omgeving, wat het vaakst voorkomt, geeft Intune al veel mogelijkheden. Deze oplossing kan ook IOS-apparaten beheren als werknemers zowel Android- als IOS-apparaten hebben.

4 Beveiliging van mobiele apparaten

De volgende maatregelen zijn aangewezen voor een betere beveiliging van de apparaten en de gegevens:
- Het apparaat wordt geregistreerd via een MDM-oplossing,
- Er worden regelmatig back-ups gemaakt,
- Gebruikersvoorlichting over Data Loss Prevention en beste praktijken op dat gebied,
- De gegevens worden geclassificeerd (labelen is iets anders dan classificeren),
- Het beleid inzake gegevensbeheer, classificatie en gebruik wordt uitgestippeld en toegelicht op het niveau van de organisatie (de norm voor gegevensclassificatie moet worden opgenomen in het algemene beveiligingsbeleid van je organisatie),
- Een mobiele DLP-software houdt de mobiele gebruikers in de gaten, maar deze wordt tegenwoordig vaker opgenomen in MDM.

5 Anti-malwareoplossingen

Tegenwoordig biedt het belangrijkste mobiele Android-OS sandboxing voor toepassingen. Dat betekent dat toepassingen standaard niet met elkaar kunnen communiceren en beperkte toegang hebben tot het OS.
Bedrijfsapplicaties kunnen samengaan met persoonlijke applicaties, maar moeten wel strikt gescheiden blijven. Je kunt bijvoorbeeld twee versies van je favoriete berichtenapplicatie hebben, een professionele en een persoonlijke met aparte contactlijsten, berichtengeschiedenis, enz.

De isolatie met IOS is nog sterker en zal de interacties tussen applicaties zonder toestemming van de gebruiker sterk beperken. Daarom kan antivirussoftware in een IOS-omgeving niet efficiënt werken, omdat ze de acties van andere toepassingen niet kan analyseren.

Meer nog, veel bedreigingen waartegen anti-malware van derden beschermde, worden nu standaard aangepakt wanneer de juiste configuratie op OS-niveau is ingesteld. Dit geldt zowel voor laptops als voor smartphones. Maar ook al is de ingebouwde anti-malwarebeveiliging goed, vergeet niet dat deze up-to-date moet worden gehouden. Updates van apps en OS-niveau kunnen automatisch gebeuren, maar het kan ook zijn dat apps van een fabrikant een handmatige tussenkomst vereisen.

6 Mobile Device Management

Een goed en duidelijk omschreven beleid voor het beheer van toestellen is de eerste stap naar succes.
Daarna zullen tools je helpen om je doelen te bereiken en controle te houden over je mobiele apparaten.
Houd er ook rekening mee dat het beheer van een extra laag tijd en mensen vergt (bv. toepassen van beveiligingspaches, updates, testen van nieuwe merken, enz.)

Mobile Device Management (MDM)-oplossingen zijn beschikbaar bij vele leveranciers op de markt.
Ieder apparaat wordt in de MDM-toepassing geregistreerd voordat het aan de werknemer wordt geleverd.
Het apparaat kan nu op afstand worden beheerd door de IT-afdeling en dat verbetert het onboardingproces en de onderhoudstijd aanzienlijk.
Met deze oplossingen kun je over een actuele inventaris van je apparaten beschikken, applicaties beheren, bewaken, wissen, lokaliseren, en beleid afdwingen zoals wachtwoordsterkte, MFA, encryptie, een verplichting om via VPN verbinding te maken met de bedrijfsomgeving, data-exfiltratie detecteren, enz. Dit zijn de belangrijkste functies en een must-have voor een goed beheerde vloot van mobiele apparaten.

Er zijn voornamelijk twee manieren om mobiele apparaten te beheren met een MDM-oplossing. De eerste is om het apparaat volledig te isoleren. De tweede is het creëren van twee afzonderlijke en geïsoleerde omgevingen op hetzelfde apparaat. Deze laatste is de moeilijke oplossing en is soms zwaar voor de hardware.

Beveiligingsfouten zullen voornamelijk ontstaan door de installatie van kwaadaardige toepassingen waaraan de gebruiker toegangsrechten voor de opslag geeft, of door legitieme toepassingen waarvan het gegevensbeheer op de achtergrond niet wordt gecontroleerd.
In beide gevallen zal de MDM-oplossing de IT-afdeling het recht geven de goedgekeurde toepassingen met meer mogelijkheden op het gebied van apparaatbeveiliging en gegevensbeheer te selecteren. De selectiecriteria zullen gebaseerd zijn op zowel de bedrijfsbehoeften als de veiligheidstests van de toepassing.

Hier volgen enkele van de meest voorkomende MDM-oplossingen:

- Ivanti MobileIron
- VMWare Workspace ONE
- BlackBerry Unified Endpoint Management

- Microsoft Intune
- Citrix Endpoint Management
- IBM MaaS360
- Cisco Meraki
- Kandji (voor IOS)
- etc.

7 Wat heb je nodig om mobiele apparaten doeltreffend te beheren (checklist)

7.1 Om controle te krijgen op mobiele apparaten moet het volgende gebeuren:

- Er bestaat een lijst van toegestane mobiele apparaten en platforms die verbinding mogen maken met het (de) bedrijfsnetwerk(en).
- Een norm voor mobiele beveiliging definieert eisen en configuratiebasislijnen voor mobiele apparaten en platforms.
- Verloren of gestolen apparaten worden gemeld, gevolgd en beheerd via een standaardproces en via een geïmplementeerde MDM-oplossing.
- Een gecentraliseerd platform voor het beheer van mobiele apparatuur wordt ontwikkeld en gebruikt om het gebruik en de configuratie van apparatuur etc. te controleren en te volgen, en voert integriteitscontroles uit (bv. detectie van *jailbreaks*) alvorens toegang te verlenen tot interne bronnen.
- Voor BYOD-apparaten wordt een basisset toegangsrechten en configuratieregels gedefinieerd en geïntegreerd in de MDM-oplossing.
- Vertrouwelijke gegevens en toepassingen op mobiele apparaten zijn alleen toegankelijk via een veilige, geïsoleerde *sandbox* of een beveiligde container.
- Mobiele apparaten implementeren basis DLP (Data Loss Prevention) use cases zoals monitoring en alarmering en zijn geïntegreerd met de SIEM-infrastructuur van het bedrijf voor monitoringdoeleinden.
- Voor BYOD-apparaten gelden dezelfde of betere beperkingen en veiligheidscontroles dan voor mobiele apparaten die eigendom zijn van het bedrijf.

7.2 Apparaat encryptie toepassen

- Alle apparaten maken gebruik van sterke encryptie tijdens opslag en transmissie.
- Er worden technologieën voor volledige disk-encryptie toegepast (bv. BitLocker in Windows, Filevault in MacOS) met authenticatie vóór het opstarten.
- Door FIPS (U.S. Federal Information Processing Standards) goedgekeurde algoritmen zoals AES, of gelijkwaardige bedrijfsstandaarden, worden toegepast.
- Encryptiestandaarden worden gepersonaliseerd en aangepast op basis van het kritieke karakter van het apparaat en de gegevens die op het apparaat zijn opgeslagen.

7.3 Mobiele apparaten correct configureren en beveiligen

- Controles om ongeoorloofde wijzigingen in configuraties en baseline builds te voorkomen.
- Voor alle technologieplatforms, inclusief iOS, Android enz., zijn normen voor veilige configuratie of *hardening* vastgesteld en gepubliceerd, en deze zijn voor elk apparaat vereist voordat het met het netwerk kan worden verbonden.V
- Eindgebruikers hebben geen beheerdersrechten op hun *endpoint*.
- Er worden regelmatig patches van besturingssystemen of toepassingen uitgevoerd.
- Apparaten zonder de laatste beveiligingspatches worden in quarantaine geplaatst en gepatcht vóór ze met het netwerk worden verbonden.
- Baseline / build images en normen worden periodiek herzien en bijgewerkt.

- Er worden geautomatiseerde instrumenten gebruikt om afwijkingen van de normen voor beveiligingsconfiguratie op te sporen, en er worden tijdig corrigerende maatregelen genomen om afwijkingen te corrigeren.

7.4 Host-based detectie implementeren, zoals anti-malware

Je vindt alle nuttige informatie in ons gerelateerd document: https://cert.be/en/paper/recommendations-anti-virus-edr-and-xdr-security-solutions

7.5 Mobiele apparaten en software traceren

- Er bestaat een centrale inventaris van alle geautoriseerde en niet-geautoriseerde software en apparaten, waarin de nodige details over de desbetreffende apparatuur zijn vastgelegd (bv. eigenaar, kriticiteit, enz.).
- Deze inventaris wordt ten minste jaarlijks herzien en bijgewerkt.

7.6 Mobile devices ownership & lifecycle monitoring implementeren

- Kritieke apparaten worden in de hele organisatie bewaakt en hebben een gekende eigenaar.
- Apparaten, inclusief hardware en software, worden gevolgd gedurende hun gehele levenscyclus, van aankoop tot buitengebruikstelling, en alle veranderingen van eigenaar worden bijgehouden.
- Er bestaat een wijzigingsbeheerproces voor het aanvragen en goedkeuren van wijzigingen aan apparaten gedurende hun gehele levenscyclus.
- Automatisch monitoren van de apparaten door middel van inventarisatie.

7.7 Mobiele apparaten labelen en controleren

- De apparaten zijn voorzien van de juiste beveiligingsrubricering
- De apparaten worden periodiek gecontroleerd en opnieuw gelabeld bij veranderingen.

Bronnen:

- Lindros, E. T. K. (4 februari 2023). *5 Ways to Prevent Data Loss in Mobile Environments*. CIO. https://www.cio.com/article/288235/mobile-security-5-ways-to-prevent-data-loss-in-mobile-environments.html
- Geekflare. (25 september 2021). *8 Best Data Loss Prevention Solutions that could Save You Millions*. https://geekflare.com/data-loss-prevention-solutions/
- Desai, P. (7 maart 2023). *Step-by-Step New Windows Autopilot Setup Guide [2023]*. Prajwal Desai. https://www.prajwaldesai.com/new-windows-autopilot-setup-guide/
- *Antivirus and other security software. (n.d.).* https://www.ncsc.gov.uk/collection/device-security-guidance/policies-and-settings/antivirus-and-other-security-software