Vier risico’s bij te weinig zicht op uw apps

Heeft u voldoende zicht op de “apps” op uw smartphone of slimme apparaten?

Factsheet FS-2023-01 | versie 0.9 | Maart 2023

Het gebruik van applicaties (apps) op smartphones en andere slimme apparaten is onvermijdelijk. We gebruiken ze voor allerlei zakelijke en persoonlijke doeleinden. Medewerkers hebben vaak een vrije keuze in welke applicaties geïnstalleerd worden, inclusief applicaties die niet direct nodig zijn voor de dagelijkse werkzaamheden. Ook op de door uw organisatie beheerde apparaten bevinden zich applicaties. Terwijl hedendaagse (sociale media) applicaties steeds meer data verzamelen en uitgebreide permissies vragen kan het overzicht houden op deze applicaties lastig zijn.

Dergelijke ontwikkelingen kunnen een negatief effect hebben op uw bedrijfsvoering. Wie heeft er onterecht toegang tot uw bedrijfsgeheimen en personeelsbestand door apps? Waar vloeit deze data heen? En wat gebeurt er buiten het zichtveld van uw organisatie?

In deze factsheet belicht het NCSC vier risico's van onvolledig zicht op applicatiegebruik binnen uw organisatie en hoe hiermee om te gaan.

Doelgroep

Deze factsheet richt zich op mensen op het tactisch niveau binnen de organisatie die grip willen krijgen op de risico's die horen bij het werken met applicaties op slimme apparaten.

Risico 1: Applicaties volgen het gedrag gebruikers

Om inzicht te krijgen hoe gebruikers zich gedragen in applicaties, maken bedrijven gebruik van meerdere manieren om gedrag te meten en te volgen.

Met zogenaamde trackers[1] wordt data verkregen die bijvoorbeeld ingezet kan worden om bedrijven gerichter te laten adverteren. Maar deze gedragsdata kan ook voor andere doeleinden worden ingezet, zoals bijvoorbeeld netwerkanalyses of het verbeteren van bedrijfsalgoritmes. Kwaadwillenden kunnen deze informatie gebruiken voor verschillende doeleindes, zoals het maken van verfijnde phishing mails en andere social engineering technieken.

Veel applicaties bevatten een of meerdere trackers. In sommige gevallen loopt dit aantal flink op. Verder zijn de bedrijven die deze trackers beheren ook regelmatig buiten de Europese Unie gevestigd waar andere privacystandaarden gelden.

Daarnaast is het in kaart brengen van de werking van trackers niet eenvoudig en zijn bedrijven vaak niet transparant over de precieze data die verzameld wordt. Dit maakt het controleren waar data heen vloeit complex, zeker wanneer gebruikers een groot aantal verschillende applicaties gebruiken.

[1] Trackers zijn software of code die gedrag van de gebruiker monitoren en registreren binnen applicaties en websites. Deze data wordt doorgestuurd naar bedrijven die het kunnen verwerken voor advertenties, monitoring, verbeteren van producten, en andere analyse doeleinden.

Risico 2: Dataverwerking gebeurt niet legitiem

Partijen die data uit applicaties verwerken moeten dit conform Europese privacywetgeving te doen.

De praktijk wijst echter uit dat het lastig is om de wetgeving te handhaven en dat er regelmatig ook overtredingen plaatsvinden.

Sommige bedrijven zijn onduidelijk over hoe de data verwerkt wordt. Dit maakt het lastig om de gebruikte algoritmes te doorgronden of audits uit te voeren op de dataverwerking van bedrijven die de applicaties beheren. Dit creëert een situatie waarin uw organisatie niet in de positie is om te doorgronden of, hoe en welke van uw data verwerkt wordt.

Risico 3: Applicaties delen data met derde partijen zoals buitenlandse overheden

Naast verwerking door bedrijven zelf, wordt data ook regelmatig gedeeld met derde partijen.

Hoewel deze partijen ook onder privacywetgeving vallen en zich aan dezelfde regels moeten houden als de hoofdverwerker, is het soms onduidelijk aan wie de data is doorgegeven. Het komt voor dat mobiele applicaties data delen met derde partijen waar de gebruiker geen weet van heeft.

Voorbeeld:

Sommige buitenlandse overheden hebben wetgeving die bedrijven verplicht stelt om data met hen te delen wanneer hier om gevraagd wordt. Soms is de invloed van overheden nog groter wanneer deze overheden deels eigenaar blijken te zijn en daarmee directe invloed op het personeelsbestand van het bedrijf hebben.

Het delen van data met derde partijen en overheden maakt het voor organisaties complex om eigenaarschap over de data uit te oefenen. Datadeling kan plaatsvinden buiten het zichtveld van de organisatie en toegankelijk worden voor buitenlandse overheden.

Risico 4: Permissies van applicaties

Voordat applicaties data mogen verzamelen moet de gebruiker of organisatie eerst de permissies van de applicatie goedkeuren.

Applicaties vragen regelmatig om een grote hoeveelheid permissies voor het gebruik van onder andere camera, microfoon, toegang tot contacten, locatiegegevens, en interne opslag. Deze lijst aan vereiste permissies is vaak meer dan wat er strikt noodzakelijk is voor het functioneren van de applicatie.

Een andere problematische ontwikkeling is de toename van in-app browsers. Hierdoor worden links geopend in een browser binnen de applicatie. Daardoor kan de applicatie met meer permissies acties uitvoeren die wellicht niet eerder zijn goedgekeurd of buiten het beveiligingsbeleid van de organisatie vallen. In het extreemste geval betekent dit zelfs dat de applicatie alle toetsaanslagen en handelingen kan monitoren die binnen de in-app browser worden uitgevoerd.

De combinatie van een groot aantal permissies en daarmee de mogelijkheid om ongewenste acties uit te voeren, maakt het belangrijk dat organisaties vooraf goed controleren welke permissies bij gebruikte applicaties worden gevraagd. Zo kan worden voorkomen dat applicaties op uw beheerde mobiele apparaten ongewenste toegang krijgen tot (gevoelige) data.

Ook de gegevens van mensen en bedrijven die de applicatie niet gebruiken zijn voor bedrijven interessant.

Er zijn buiten applicaties ook technieken die kunnen worden ingezet om profielen van niet-gebruikers te creëren.

Wanneer u zelf geen gebruiker bent van een bepaalde applicatie, kunnen bedrijven toch shadow profiles opbouwen met uw gegevens door gebruik te maken van informatie waar de applicatie toegang toe heeft. Denk bijvoorbeeld aan contactgegevens in het adressenboek of informatie in berichtenverkeer. Zo kunnen gegevens van mensen en organisaties die de applicatie niet gebruiken toch in kaart worden gebracht met behulp van de applicatie.

Datalekken bij de betreffende bedrijven die deze mobiele applicaties beheren kunnen zo verregaande gevolgen hebben voor zowel gebruikers als niet-gebruikers.

Wat kan ik doen?

Hieronder geven we u een aantal mogelijke opties om de hierboven beschreven risico's te beperken.

Zorg voor overzicht van applicaties die in gebruik zijn.

Om risico's ten aanzien van applicaties te beperken is in eerste instantie overzicht van de applicaties die in gebruik zijn noodzakelijk.

Alleen mensen en organisaties die voldoende overzicht hebben kunnen een goede risicoafweging maken. "W*at levert het gebruik van de applicatie mij of de organisatie op? Staat dit in verhouding met de risico's die hieraan kleven?*".

De managementsoftware op door de organisatie beheerde apparaten biedt veelal geautomatiseerde mogelijkheden om dit overzicht te creëren. Bij zogenaamde Bring Your Own Device (BYOD) apparaten is dit veelal niet het geval.

Voorkom de installatie van ongewenste applicaties.

Applicaties kunnen geen schade aanrichten indien deze niet zijn geïnstalleerd. Er zijn twee invalshoeken om dit principe toe te passen: allowlisting en denylisting.

Allowlisting

Bij **allowlisting** staat de organisatie slechts goedgekeurde apps toe. Bij door de organisatie beheerde apparaten kan dit beleid veelal technisch worden afgedwongen. Hierdoor wordt voorkomen dat ongewenste applicaties worden geïnstalleerd. Het nadeel van deze maatregel is dat de flexibiliteit van het apparaat wordt beperkt. Dit kan negatieve impact hebben op de effectiviteit van medewerkers en vergroot de kans op shadow IT.

> Shadow IT is het gebruik van bepaalde IT-producten die niet door de IT-afdeling van uw organisatie zijn goedgekeurd of die buiten uw veiligheidsbeleid vallen.
>
> Shadow IT kan betrekking hebben op zowel hardware (bijv. slimme apparaten) als software (bijv. mobiele applicaties). Shadow IT vindt vaak plaats buiten het zichtveld van de organisatie en kan een gevolg zijn van IT-regels die als te streng of hinderlijk worden ervaren.

Denylisting

Een andere methode is **denylisting**. Hierbij kunnen medewerkers alle applicaties installeren, met uitzondering van applicaties die als ongewenst zijn bestempeld. Deze applicaties komen op de denylist te staan. Ook dit beleid is veelal op door de organisatie beheerde apparaten technisch af te dwingen.

Het nadeel van denylisting als maatregel is dat het bijhouden van de denylist een uitdaging is doordat er constant nieuwe applicaties verschijnen. Hierdoor is er een reële kans dat er ongewenste applicaties zijn die niet op de denylist staan.

Beheersen

Het is mogelijk om de risico's van geïnstalleerde ongewenste applicaties te beperken. Dit kan op verschillende manieren. Hieronder een tweetal opties.

Beperken van rechten

Door het beperken van de rechten die een applicatie krijgt op een apparaat, zal deze in mindere mate in staat zijn gegevens te verzamelen. Er kleven nadelen aan deze maatregel. Zo wordt de functionaliteit van de applicatie mogelijk beperkt of functioneert deze geheel niet meer. Ook kan deze

maatregel een vals gevoel van veiligheid geven indien de applicatie nog altijd in staat is vertrouwelijke gegevens te verwerken.

Afschermen zakelijke applicaties

Een andere maatregel is het verplaatsten van de zakelijke applicaties naar een afgeschermd deel van het apparaat. Op deze manier kunnen zakelijke applicaties en gegevens worden beschermd tegen de applicaties die buiten het afgeschermde deel zijn geïnstalleerd. Dit is een veelgebruikte techniek bij BYOD en zakelijke apparaten die deels ook privé gebruikt mogen worden.

Mobile Device Management (MDM) en Mobile Application Management (MAM) tools bieden de mogelijkheid om de hierboven genoemde maatregelen of delen hiervan te implementeren.

Uitgave
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

Maart 2023
**