**Mobiele apps – beveiligingscriteria – versie 20251028**
**Opsteller: Jeroen Steenbakkers CISSP CRISC CISM CISA**

**Gestelde beveiligingseisen aan mobiele apps voor Drechtsteden.**

## Inleiding

Mobiele apparaten hebben een belangrijkere rol in het (zakelijke en privé) leven. Betekenend dat kwaadwillenden ook deze platformen steeds aantrekkelijker vinden om digitaal aan te vallen. Om die reden is het belangrijk dat; zowel de mobiele apparaten als de apps die daarop draaien veilig zijn. Hierbij rekening houdend met wettelijke kaders en richtlijnen voor gebruik:

- Richtlijnen vanuit de Autoriteit Persoonsgegevens
- Veilig omgaan met APPS

De opbouw voor een veilige architectuur richtlijn adviseert: Gebruik "Zero Trust" principes.
Voor de ontwikkeling zijn er richtlijnen vanuit het NCSC en CIP:

- De NCSC (Nationaal Cyber Security Center) biedt ICT-beveiligingsrichtlijnen voor mobiele apps.
- Het CIP (Centrum informatiebeveiliging en privacybescherming) biedt Normen voor Mobile Apps

Maatregelen om apps en hun gebruikers te beschermen tegen diverse kwaadwillenden/aanvallen. Deze beveiligingsrichtlijn is bedoeld als toetsingsdocument voor apps, technisch van aard, niet alles omvattend. De structuur is vormgeven door eisen op Beleid, Uitvoering en Beheersing(control) domeinen. De beoordeling/wegingsfactoren zijn afhankelijk van de dienst welke wordt ondersteund met de gewenste app.
Testhandreikingen zijn eventueel beschikbaar via OWASP app security.

Deze opzet gaat uit van een volwassen organisatie en procesinrichting.
Waarbij wordt voldaan aan de BIO2.0, CBW en ISO27001/2 en NEN7510/7512.

De volgende eisen dienen te worden gebruikt, om bij aanschaf en inkoop te toetsen of de toepassing voldoet aan gestelde normen.

**Eisen**

| | |
|---|---|
| 1 | Heeft de organisatie operationeel beleid voor mobiele apps, welke bevat richtlijnen en instructies en procedures m.b.t. ontwikkeling, onderhoud en uitfasering van apps. |
| | Voldaan Ja/Nee Toelichting: |
| 2 | Veilige server-side applicatie wordt toegepast. Bij ontwikkeling van de app worden alleen inrichtingskeuzen gemaakt die de veiligheid van de server(applicatie) niet in het geding brengen. Zodoende blijft de veiligheid van de keten van app tot en met server-side applicatie gewaarborgd. End-to-end in de keten. |
| | Voldaan Ja/Nee Toelichting: |
| 3 | Wordt voorkomen dat Third-party-apps ongewenst toegang krijgen tot informatie die door de app moet worden afgeschermd. Third-party-apps kunnen permissies vragen of verborgen functionaliteit hebben waarmee toegang verkregen wordt tot vertrouwelijke informatie, ook als deze is afgeschermd. Ook zouden zij gebruik kunnen maken van onveilige API's en kwetsbaarheden in apps en het besturingssysteem. Het uitgangspunt is dat apps van derden zonder inspectie van het maakproces en de code in principe als onveilig moeten worden beschouwd. |
| | Voldaan Ja/Nee Toelichting: |
| 4 | Veilige broncode bij oplevering wordt gerealiseerd(Hashcontrole bij oplevering) door bij ontwikkeling alleen gebruik wordt gemaakt van vertrouwde broncodebibliotheken. De broncode bevat geen technische informatie over de werking van de app. Oorsprong is bekend en de veiligheid is vastgesteld, up-to-date en bevat geen kwetsbaarheden. |
| | Voldaan Ja/Nee Toelichting: |
| 5 | Integere werking van de app is afgeschermd op het mobiele apparaat tegen ongewenste of onbedoelde manipulatie en de uitkomsten van de bedrijfslogica en worden altijd gecontroleerd op de server. |
| | Voldaan Ja/Nee Toelichting: |
| 6 | Keuze locatie voor de opslag waar de gegevens en informatie van de logica van de app worden opgeslagen is gebaseerd op classificatie, het principe van de vertrouwelijkheid ,risico beoordeling/gebaseerd, waarbij uitgangspunt is lokaal opslaan mobiel apparaat zoveel mogelijk voorkomen. |
| | Voldaan Ja/Nee Toelichting: |
| 7 | Bij het opslaan van vertrouwelijke informatie op het mobiele apparaat zijn de vertrouwelijke gegevens afgeschermd door toepassing van robuuste en met de tijd meegaande crypto grafische technieken. |
| | Voldaan Ja/Nee Toelichting: |

| | |
|---|---|
| 8 | Vertrouwelijke informatie is in het cachegeheugen op basis van een risicoafweging(lang/kort/wipe/truncate) per gegeven tot een minimum beperkt; dit geldt zowel binnen als buiten de eigen app, afgeschermd voor toegankelijkheid van gevoelige informatie door onbevoegden. |
| | Voldaan Ja/Nee Toelichting: |
| 9 | Sessietime-out voor de app beëindigt een gebruikerssessie na een vooringestelde periode van inactiviteit/onbedoeld onbeheerd achtergelaten sessie van de gebruiker via automatische sessiebeëindiging overeenkomstig uitloggen(Hoog risico 2-5 minuten, overige 15-30 minuten). |
| | Voldaan Ja/Nee Toelichting: |
| 10 | Logging bevat geen onnodig gedetailleerde informatie over de werking van de app(ook geen third-party programmabibliotheken) of over de gebruiker (persoonsgegevens) welke beschikbaar komt voor een aanvaller(geen debugging/opslag crashlog/dumps/testdata in productie). |
| | Voldaan Ja/Nee Toelichting: |
| 11 | Transport/sessie versleuteling in de applicatie past encryptie toe op alle communicatie via netwerken(ook app en server)volgens NCSC's vingerende ICT beveiligingsrichtlijnen voor TLS. |
| | Voldaan Ja/Nee Toelichting: |
| 12 | Certificaatverificatie wordt door de app gecontroleerd d.m.v. certificaat pinning |
| | Voldaan Ja/Nee Toelichting: |
| 13 | Hardening van de apps wordt gewaarborgd zodat toegang tot de app alleen mogelijk is via interacties/poorten/code/autorisaties, die noodzakelijk zijn voor het correct functioneren van de applicatie(lees en schrijfrechten o.b.v. need-to-know/least privilege). |
| | Voldaan Ja/Nee Toelichting: |
| 14 | Least privilege/toegangsrechten van de app tot functies en data worden/zijn alleen expliciet uitgegeven waar zij het onderbouwde doel en belang van de gebruiker dienen, ook voor andere apps. |
| | Voldaan Ja/Nee Toelichting: |
| 15 | Invoernormalisatie wordt toegepast in de app op ontvangen invoer voor verwerking, welke voorkomt manipulatie, inzage, wijziging, verlies en misbruik van gegevens via daartoe geëigende karakters of commando's in de invoer van de app. |
| | Voldaan Ja/Nee Toelichting: |
| 16 | Invoervalidatie wordt toepast in de app op alle ingangen(ook webview-aanroepen), voordat deze invoer wordt verwerkt middels white -en blacklist van resp. werkbare en malafide invoer. |
| | Voldaan Ja/Nee Toelichting: |

| | |
|---|---|
| 17 | De app gebruikt alleen de http(s)-methoden die nodig zijn voor het communiceren met andere apps en services, al dan niet over het netwerk. |
| | Voldaan Ja/Nee Toelichting: |
| 18 | De app beperkt de mogelijkheid tot manipulatie door alle externe XML-invoer te beschermen(lekken van informatie en DoS aanvallen) tegen entiteitinjectie. |
| | Voldaan Ja/Nee Toelichting: |
| 19 | Up-to-date apps worden gerealiseerd door De leverancier past (LCM) lifecyclemanagement toe op apps die worden geleverd, waardoor gebruikers altijd over de veiligste versie kunnen beschikken(contractuele garantie/conformiteit beveiligingseisen). Dwing meldingen en updates af. Voorkom gebruik onveilige versies. |
| | Voldaan Ja/Nee Toelichting: |