VERSLAG

SECURITY CAFÉ – MOBILE APP SECURITY

Gerco Kanbier is directeur van Trust in People – the information protection company.
Hij is te bereiken via gerco.kanbier@trustinpeople.com.

Vier maal per jaar organiseert Trust in People het Security Café. De editie van 26 februari 2013, werd bij Koetjes & Kalfjes te Zoetermeer georganiseerd. Op LinkedIn hadden de inmiddels 700 leden van de groep wederom voor het onderwerp "Mobile App Security" gestemd. Met de feedback van vorig jaar dat er te weinig diepgang was, heb ik Security Officer Derk Tegeler van Service2Media uitgenodigd om te vertellen over technische details bij de ontwikkeling van o.a. banking apps. Onderstaand volgt een impressie van de discussie.

Bedrijven experimenteren flink met mobile applicaties op zoek naar een toegevoegde waarde. Banking applicaties zijn alom geadopteerd door het grote publiek. Social Media applicaties zijn populair om "anytime, anywhere, anyplace" een foto of een gebeurtenis te kunnen delen. De media brengt graag het laatste nieuws op uw mobiel en voor ontspanning zijn vele games beschikbaar.
Maar er zijn ook bedrijven die via een app contactgegevens van alle vestigingen op een rijtje zetten voor de medewerkers en/of klanten. Maar waar laat je zo'n applicatie ontwikkelen en waar moet het aan voldoen?

Bij het bedrijf waar Derk werkt, worden platform-onafhankelijke apps ontwikkeld. Ontwikkelkosten voor professionele apps zijn al snel enkele tonnen. Dat staat in schril contrast met een hobby app met statische content, die je in de cloud kan laten ontwikkelen door '2 kids in garage' voor zo'n 3000 euro. Professionele ontwikkeling hoort echter niet in de hobbysfeer thuis. Professionele apps worden in een ontwikkelomgeving vervaardigd, waar een uniek ontwerp geïmplementeerd wordt in één raamwerk om vervolgens apps te genereren voor de verschillende mobiele platformen. Dit contrasteert met de zogenaamde 'native' ontwikkelingen waar elk OS een eigen implementatie in specifieke programmeertaal is. Dit is duur en moeilijk te onderhouden.

Apps worden door identificeerbare ontwikkelaars gesigneerd en aangeboden aan de online stores. Deze apps worden door deze stores getoetst op een aantal aspecten als merkenrecht en toelaatbaar beeldgebruik. Je bent hier afhankelijk van een extern beoordelingsproces, wat erg onhandig is als je een belangrijke update wil uitsturen en je op goedkeuring moet wachten van de store. Wat in het beoordelingsproces onderbelicht is, is of

de autorisaties in verhouding staan tot de functionaliteit van de app en welke privacy wetgeving van toepassing is. Onder valse voorwendselen kunnen gebruikers wel een app accepteren, maar op de achtergrond wordt andere informatie gelekt. Omdat apps vaak een beveiligde verbinding opzetten, is het nog niet zo eenvoudig om te zien welke data wordt verstuurd. Je kunt een apparaat aan een draadloos netwerk koppelen om vervolgens via man-in-the-middle techniek een netwerkanalyse uit te voeren. Dit is wel erg duur en niet schaalbaar als je dit per apparaat moet controleren. Wees daarom voorzichtig welke voorwaarden je accepteert, daar het daarna eenvoudig is voor een geaccepteerde applicatie om bedrijfs- & privé data, zoals keylogs, foto's, contacten, e-mail en geluid over het internet versleuteld te versturen, zonder dat je erachter komt. Awareness bij (zakelijke) eindgebruikers moet omhoog als het gaat om BYOD in een gecombineerde omgeving van zakelijk en privé.

Terug naar de beveiliging van professionele banking apps. Derk vertelt hoe pen-testen zijn uitgevoerd door een onafhankelijk partij. Allereerst is het belangrijk te weten dat apps vaak een thin-client/fat-server structuur kennen en de standaard tools en aanpak voor pentesten van een website niet bruikbaar zijn. Het testen van mobile apps is nog vrij rudimentair en het begint ook gewoon bij input validatie via de user interface. Het gedrag van de applicatie wordt beoordeeld als het naar de achtergrond gaat. Er wordt namelijk een plaatje van je app gemaakt, net voordat deze in de achtergrond opgaat. Dit is niet altijd wenselijk vanuit de optiek van veiligheid. Copy-paste is ook handig, maar hoe wis ik mijn prikbord als ik een wachtwoord heb gekopieerd? Misschien is het veiliger om dit uit te zetten in een bepaalde context. Een bestaande security-netwerk pentest applicatie wordt ingezet om een grondige netwerkanalyse te doen. Ook is het belangrijk om een goede risicoanalyse te doen en maatregelen te nemen om de schade te beperken als er misbruik plaatsvindt.

Er zijn nog weinig voorbeelden van mobile security incidenten in de zakelijke omgeving. Er zijn daarentegen wel veel rapporten over een explosie in malware in mobile space, vooral op Android. Banken hebben wel een bedrag in gedachten na risicoanalyse. Fraude is een feit, geen mythe. Malware kan namelijk eenvoudig in de keten komen, soms zelfs door de fabrikanten zelf geïnstalleerd. Het Carrier-IQ schandaal begon vast met de beste intenties, met name om statistieken over gebruik te vergaren. Iedereen schrok wel toen zelfs onze toetsaanslagen geregistreerd werden. Niemand weet wat er daarna met deze data is gebeurd... ●

Links

Security Cafe: informatie beveiliging community in Nederland
www.trustinpeople.com/security_cafe.php