ftm.nl

Groot deel Android-smartphones is zo lek als een mandje

Luuk van der Sterren

Een groot deel van de Nederlandse apparaten met een Android-besturingssysteem zit vol beveiligingslekken. Soms zijn gebruikers zelfs al kwetsbaar voor hackers en cybercriminelen op het moment dat ze de winkel uitlopen. Wat is hier precies aan de hand?

Een gedachte-experiment: wat weet jouw smartphone allemaal van jou? Grote kans dat het antwoord op die vraag luidt: 'aardig wat'. Smartphones leven doorgaans in onze broekzak of handtas en bevatten duizenden foto's, berichtjes, contacten, persoonlijke notities, locatiegegevens, Google-zoekopdrachten, telefoongesprekken, bankgegevens, en nog veel meer persoonlijke informatie. Wat dat betreft is het niet gek om te stellen dat je smartphone waarschijnlijk je meest persoonlijke eigendom is.

Zoals je redelijkerwijs van een vertrouwenspersoon mag verwachten dat diegene jouw geheimen bewaart, zo zou je van een apparaat dat jou door en door kent mogen verwachten dat het redelijk beveiligd is. Misschien is geen enkel systeem honderd procent waterdicht, maar het is volkomen normaal dat niet de eerste de beste trol of cybercrimineel zomaar al jouw data kan stelen. Toch?

> Het is volkomen normaal dat een cybercrimineel niet zomaar jouw data kan stelen. Toch?

De realiteit blijkt echter anders: veel smartphones met het Android-besturingssysteem zijn zo lek als een mandje. Sommige telefoons zijn zelfs al onveilig op het moment van aanschaf.

Verouderde software

De kern van het probleem is dat een groot deel van de Android-apparaten in Nederland draait op verouderde software. Dat wil zeggen: de versie van het Android-besturingssysteem op deze toestellen is dermate oud dat de apparaten kwetsbaar zijn voor kritieke en publiekelijk bekende beveiligingslekken. De toestellen zijn daardoor makkelijk over te nemen door kwaadwillende hackers, die de persoonlijke data op het apparaat bijvoorbeeld misbruiken voor identiteitsfraude.

Wat zijn die beveiligingslekken?

Besturingssystemen zoals Windows, Android en iOS bevatten miljoenen regels programmeercode. Daar zitten altijd wel wat bugs of beveiligingsproblemen in, bijvoorbeeld door een tikfout van een programmeur of een slecht ontworpen functie. Uiteindelijk is het onvermijdelijk dat iemand ontdekt hoe je zo'n foutje kunt misbruiken om bijvoorbeeld het systeem te laten crashen of privégegevens te stelen. Op dat moment spreken we van een beveiligingslek of *exploit*. Recente voorbeelden van zulke lekken zijn het

'Gooligan'-virus en de 'Stagefright'-bug, een kwetsbaarheid die een hacker met één MMS-berichtje het hele toestel laat overnemen.

Op het internet bestaan hele *communities* van hackers en hobbyisten die zich bezighouden met het vinden van dergelijke beveiligingslekken. Op het moment dat zij zo'n lek ontdekken, brengen ze meestal eerst de makers van de software op de hoogte. Die brengen vervolgens een *patch* uit om het lek te dichten; deze wordt vervolgens via een software-update aan gebruikers geleverd. Om veilig te zijn voor beveiligingslekken is het dus belangrijk dat je als gebruiker regelmatig deze updates installeert.

> Er zijn hele *communities* die zich bezig houden met het vinden van lekken

Softwareontwikkelaars brengen echter ook regelmatig nieuwe versies uit van hun programma's. Zo komen er elk jaar nieuwe versies van Android en iOS uit. De makers van de software kunnen niet eindeloos lekken blijven dichten in oude producten, dus geven ze hun software een beperkte 'levensduur' mee. Alleen de meest recente versies blijven patches ontvangen.

Op dit moment maakt Google updates voor de twee meest recente Android-versies: versie 6 (oftewel 'Marshmallow') en versie 7 ('Nougat'). Versie 5, 'Lollipop,' ontvangt alleen nog *security patches* voor de gevaarlijkste beveiligingslekken. Bij Apple ontvangt alleen iOS 10, de nieuwste versie, nog updates. Oudere versies, zoals Android 4 ('KitKat') en iOS 9, ontvangen geen updates meer — ook niet als er een groot beveiligingslek wordt ontdekt. Om toch veilig te blijven is de enige optie in dat geval dus te upgraden naar een nieuwere versie van het besturingssysteem.

Lees verder Inklappen

Het is moeilijk om precies te zeggen hoeveel Nederlandse apparaten deel uitmaken van het probleem. Op dit moment hebben zo'n 10,6 miljoen Nederlanders een smartphone; 60 procent van die smartphones maakt gebruik van Android. Uit data van de ontwikkelaars van Android blijkt dat bijna driekwart van alle Android-apparaten een verouderde versie van het besturingssysteem gebruikt.

De ontwikkelaars stellen geen informatie per land beschikbaar, maar we kunnen een redelijke schatting maken. Volgens gegevens van VideoLan, ontwikkelaar van de populaire Android-app VLC, maakt op dit moment zo'n 64 procent van zijn Nederlandse klanten gebruik van verouderde versies van Android. Uit diezelfde data blijkt ook dat slechts een schamele 1,4 procent van de Nederlandse toestellen draait op de laatste versie van Android, Nougat geheten. Ter vergelijking: uit data van Apple blijkt dat op dit moment zo'n 63 procent van alle iOS-apparaten wereldwijd de nieuwste software (iOS 10) heeft. Dit terwijl die versie pas een maand ná Android Nougat uit is gekomen.

Traag updateproces

Een belangrijke oorzaak van het probleem van verouderde software is het proces dat Android gebruikt om updates te leveren. Android is namelijk — in tegenstelling tot iOS, waar Apple zelf de software maakt en rechtstreeks aan gebruikers levert — ontworpen als een 'open' ecosysteem. Dat wil zeggen dat iedereen in principe zijn eigen aangepaste versie van het product kan maken. Fabrikanten van smartphones doen dit

veelvuldig, deels om ervoor te zorgen dat de software goed werkt op hun apparaten, deels om hun eigen 'sausje' mee te leveren.

Dit heeft echter tot gevolg dat fabrikanten iedere software-patch en nieuwe versie van het besturingssysteem zelf moeten aanpassen voor al hun toestellen. Bedrijven als Samsung, LG en Huawei brengen elk jaar veel verschillende modellen smartphones uit; hierdoor is het een hele klus om iedere update ook daadwerkelijk aan te passen voor alle modellen telefoons die op de markt in gebruik zijn. Het resultaat: toestellen ontvangen nieuwe Android-versies over het algemeen pas maanden nadat deze uitkomen, en de tijd dat er beveiligingsupdates worden geleverd is beperkt. Goedkopere toestellen en modellen van vorig jaar krijgen de updates vaak zelfs helemaal niet.

Juridische weg

Voor de Consumentenbond was de situatie reden om afgelopen februari een kort geding aan te spannen tegen Samsung. Dit bedrijf is met afstand de grootste Android-fabrikant in Nederland; door de electronicagigant voor de rechter te slepen hoopt de Consumentenbond uiteindelijk bij alle merken een goed updatebeleid te bewerkstelligen. Woordvoerder Babs van der Staak: 'Fabrikanten moeten zorgen dat ze updates geven, maar ook dat ze daar transparant over zijn. Klanten moeten bij aanschaf kunnen weten hoelang ze nog updates mogen verwachten.'

Volgens de Consumentenbond valt deze verantwoordelijkheid onder de zorgplicht die fabrikanten hebben onder de telecom- en privacywetgeving. Van der Staak: 'Op het moment dat er een lek ontstaat en er komt een update om te zorgen dat dat lek gedicht wordt, maar fabrikanten zetten die niet door naar de toestellen, dan blijven ze in gebreke.'

Babs van der Staak, Consumentenbond

"Klanten moeten bij aanschaf kunnen weten hoelang ze nog updates mogen verwachten"

Het kort geding werd echter door de Consumentenbond verloren. Volgens de rechter was er 'geen spoedeisend belang,' ook zouden de financiële gevolgen voor Samsung te groot zijn. Destijds stelde Samsung dat de uitspraak bewees dat het bedrijf de beveiliging van haar toestellen 'op orde' heeft. Bij navraag verwijst een woordvoerder van Samsung naar het vonnis, waarin staat dat de Consumentenbond 'onvoldoende aannemelijk' had gemaakt dat de Stagefright-bug een acuut veiligheidsrisico vormde voor Samsung-telefoons.

Ook geeft Samsung aan dat het 'alle toestellen tot twee jaar na introductie' voorziet van 'regelmatige veiligheidsupdates'. Het bedrijf verwijst daarbij naar deze support-pagina, waar te lezen is dat een aantal '*flagship*'-modellen — de Galaxy S7 en S7 Edge bijvoorbeeld — op maandelijkse basis beveiligingsupdates ontvangt. Voor andere (goedkopere) modellen worden op dit moment 'de mogelijkheden bekeken' om updates op kwartaalbasis uit te voeren.

De Consumentenbond laat het er niet bij zitten: in november is de organisatie een bodemprocedure tegen Samsung gestart. Dergelijke zaken nemen over het algemeen echter gemakkelijk een jaar of langer in

beslag. Het gaat dus nog wel even duren voor er via deze weg een oplossing komt.

Nog een tussenstation

Fabrikanten zijn niet de enige factor in het probleem. Een aantal telecomproviders — zoals T-Mobile en Vodafone in Nederland — past de Android-software namelijk ook nog eens aan. Dit doen ze bijvoorbeeld om hun eigen applicaties en logo's mee te leveren, of om de telefoon van een simlock te voorzien. Hierdoor ontstaat er nóg een 'tussenstation' alvorens een nieuwe versie van Android de eindgebruiker bereikt, met extra vertraging als gevolg.

De telecombedrijven verkopen ondertussen ook doodleuk telefoons met sterk verouderde software aan hun klanten. Zo kun je bij KPN bijvoorbeeld een smartphone van het type HTC Desire 620 bestellen: gratis bij een tweejarig abonnement van 19 euro per maand. Een koopje.

> KPN is lang niet de enige provider die telefoons met verouderde software verkoopt

De website van KPN verzuimt echter te vermelden dat deze telefoon draait op Android versie 4, dat er geen update naar een nieuwere versie beschikbaar is, en dat die er hoogstwaarschijnlijk ook nooit gaat komen — hartstikke onveilig dus. Ook de Samsung Galaxy S6 is bij KPN te koop. Als je deze smartphone vandaag aanschaft, ontvang je hooguit nog een paar maanden updates. En daar zit je dan contractueel twee jaar aan vast.

KPN is bij lange na niet de enige provider die telefoons met verouderde software verkoopt. Zo kun je bij Vodafone en T-Mobile de Samsung Galaxy J3 krijgen. Voor dit toestel — tevens de bestverkochte Android-telefoon op Bol.com — bestaat in Zuid-Korea al sinds mei 2016 een update naar Marshmallow, maar in Nederland is die vooralsnog niet beschikbaar.

Ook bij het Phone House-filiaal om de hoek van de FTM-redactie liggen de onveilige Acers, Alcatels en HTC's gewoon in het schap. Het is weinig verrassend: van de 86 door de Consumentenbond geteste Android-telefoons die in Nederland 'goed verkrijgbaar' zijn, worden er 38 geleverd met verouderde versies van Android.

Wat nu?

Wat kun je nu als Android-gebruiker zelf doen? Eén veelgehoord advies aan consumenten is om voor een duurder model te gaan; met deze zogeheten *flagship*-modellen heb je over het algemeen namelijk een grotere kans op toekomstige software-updates dan met de goedkopere modellen. Een ander advies is om toch maar over te stappen op een iPhone.

Niet iedereen heeft echter het budget voor een telefoon van 800 euro. Het goede nieuws: dat hoeft ook helemaal niet. Het 'open' ontwerp van de Android-markt heeft namelijk ook een groot voordeel — er is ontzettend veel keuze. Je kunt dus zelf zoeken naar telefoons waarbij het waarschijnlijk is dat ze gedurende

langere tijd software-updates ontvangen. Voor sommige telefoons zijn ook *custom ROMs* beschikbaar, die je zelf op je toestel kunt installeren. Ook kun je bijvoorbeeld in de winkel navragen hoe het zit met de veiligheid van een telefoon voor je hem koopt.

Heb je al een Android-telefoon? Op deze website kun je controleren welke versie van Android op jouw telefoon staat. Als dit versie 5 of lager is, controleer of er (binnenkort) een update naar Marshmallow beschikbaar is. Zo niet, dan is het misschien beter om een nieuw toestel te kopen.

Nog niet toe aan een nieuw toestel? Veel beveiligingslekken zitten in de webbrowser. Gebruik dus niet de standaard Android-browser, maar een alternatief, zoals Google Chrome of Firefox for Android (gratis te downloaden in de Google Play Store). Spyware, de programma's waarmee hackers je telefoon afluisteren, zit ook vaak verpakt in onschuldig ogende Android-apps. Installeer dus alleen apps die je vertrouwt. Tot slot: op deze website kun je lezen hoe je jezelf beschermt tegen de Stagefright-bug.

Reacties betrokken partijen

FTM heeft Google, Samsung, T-Mobile, KPN, Vodafone en The Phone House benaderd voor commentaar. T-Mobile en The Phone House hebben niet op dit verzoek gereageerd.

Reactie Google

Google (with help from open source contributors) develops platform updates and monthly security updates. It's then up to hardware vendors to make the necessary adjustments to implement these updates on their devices. For Pixel and Nexus devices, Google pushes the updates directly, with devices getting platform updates for at least two years from release and security updates for at least three years from release.

It's not accurate to say that almost three quarters of Android devices worldwide are currently running on old and unsupported software. According to our dashboard, 60.7% of active devices are running 5.x, 6.x or 7.x, versions of Android for which we currently provide security patches.

We are also working to make it easier for companies to implement these security updates, and to make the update experience better for users. For example, in Android 7.0 Nougat, we implemented a new update model in which software updates download and install in the background, so users won't have to wait while their devices sync with the latest security tools. Pixel currently uses these seamless updates and we expect many more devices to use them over time.

Reactie Vodafone

Wij ontwikkelen zelf geen software voor toestellen, dit gebeurt door de fabrikanten van de toestellen. In sommige gevallen voegen we enkele Vodafone-elementen aan de software toe (zoals logo en Vodafone applicaties), maar dit verandert niets aan de kern van de software zoals de fabrikant deze heeft

ontwikkeld. Vodafone test de werking van de software voordat wij toestellen introduceren, maar wij testen ook bij software updates voor Vodafone-branded toestellen. Zo brengt Samsung maandelijks een SMR (Security Maintanance Release uit). Deze wordt vervolgens door Vodafone getest alvorens deze wordt geaccepteerd of afgewezen.

Ons huidige assortiment heeft Android 6 of hoger. Mogelijk dat er nog enkele oude (prepaid) toestellen een eerdere versie van Android bevatten, echter deze zijn vrijwel altijd te upgraden naar Android 6. Mocht er een toestel zijn dat niet upgradable blijkt, dan plaatsen we daarbij een waarschuwing in onze kanalen.

Reactie Samsung

Veiligheid en gebruikerservaring hebben hoogste prioriteit bij Samsung en wij zien het zeker als onze verantwoordelijkheid om onze gebruikers daarin te ondersteunen. Ik wil wel benadrukken dat een software-update los staat van de kwetsbaarheid van een toestel. Wij voorzien alle toestellen tot twee jaar na introductie van regelmatige veiligheidsupdates zodat je toestel altijd veilig is. Voor meer informatie kun je terecht op: http://www.samsung.com/nl/support/skp/faq/1097862/.

In reactie op een verklaring voor de stelling van Samsung in het NOS-bericht over het kort geding dat 'het vonnis bevestigt dat [Samsung] de beveiliging van [haar] toestellen op orde [heeft]', verwees de woordvoerder naar rechtsoverweging 4.2 uit het vonnis. Deze overweging leest als volgt:

"(...) Voorshands is onvoldoende aannemelijk dat van stagefright en stagefright 2.0 een zo acuut beveiligingsrisico uitgaat als de Consumentenbond stelt. Samsung heeft, mede aan de hand van de verklaringen van twee van haar medewerkers, [naam 4] en [naam 5] (producties 2 en 3) verduidelijkt dat het niet om een beveiligingslek in Android gaat, maar om een zwakke plek in het besturingssysteem, en dat het misbruik maken van deze kwetsbaarheid een bijzonder ingewikkeld, duur en tijdrovend proces is. Hiervoor is vereist dat een exploit wordt ontwikkeld. Dit is een computerprogramma om op een kwetsbare plek in het besturingssysteem een lek te maken waarmee toegang tot gevoelige informatie op een smartphone wordt verkregen (hacken). Eén exploit kan bovendien niet voor meerdere modellen smartphones worden gebruikt. De kans op "succesvol" gebruik van een exploit is volgens Samsung uitermate gering. Naar het oordeel van de voorzieningenrechter is dit standpunt van Samsung onvoldoende weerlegd door de Consumentenbond. Integendeel, de Consumentenbond heeft als productie 24 een rapport in het geding gebracht van DPA B-Able waaruit voorshands eveneens kan worden afgeleid dat het gevaar van stagefright thans gering of niet (meer) aanwezig is. In dit rapport, dat dateert van 30 januari 2016, is immers onder meer opgenomen:

There is no evidence that the Stagefright vulnerability can be actively exploited on Samsung devices... Voorts is van belang dat de Consumentenbond niet aannemelijk heeft gemaakt dat ook maar één smartphone van Samsung buiten een testomgeving ("in the wild") is gehackt, laat staan dat hierdoor een gebruiker van een Samsungsmartphone is benadeeld.

Tot slot is van belang dat uit de verklaring van Lee (productie 2) alsmede uit de e-mail van G.J. ter Haar

(medewerker van Samsung) van 10 februari 2016 (productie 13 van Samsung) voorshands volgt dat alle toestellen van Samsung die na juli 2013 in Nederland zijn geïntroduceerd (inmiddels) tegen stagefright (2.0) zijn beveiligd. Weliswaar zijn er enkele oudere modellen smartphones na juli 2013 verkocht waar nog geen patch voor is uitgebracht, te weten de Ace 2, de S3 en de S3 mini, maar dat het hier om substantiële aantallen smartphones gaat is niet duidelijk geworden.

Al met al is niet duidelijk dat stagefright en stagefright 2.0 een zodanig acuut risico voor gebruikers van Samsung smartphones vormen dat voldoende spoedeisend belang bestaat om daartegen in kort geding op te komen."

Reactie KPN

In reactie op de vraag of KPN het als haar verantwoordelijkheid ziet om veilige producten te leveren, en of digitale veiligheid daar ook onder valt:

KPN vindt het belangrijk om veilige producten en diensten te leveren voor iedereen en heeft de privacy van zijn klanten hoog in het vaandel staan. Gespecialiseerde teams waken 24 uur per dag, 7 dagen per week over onze netwerken en systemen en de data van onze klanten.

In reactie op de vraag waarom KPN de eerder genoemde HTC Desire 620 in haar webwinkel had staan:

Bij iOS worden software updates centraal geregisseerd door Apple. Android van Google wordt aan verschillende smartphonefabrikanten geleverd. Smartphonefabrikanten verspreiden de software (en de updates) vervolgens naar eindgebruikers zonder enige tussenkomst van KPN. Daarmee ligt de verantwoordelijkheid voor veilige software dus ook bij de smartphonefabrikant.

Zodra wij vanuit de smartphonefabrikant het signaal krijgen dat een smartphone of softwareversie niet (meer) veilig is, halen we deze uit het assortiment. Dat is bij dit bewuste toestel niet het geval. Wel is het zaak dat smartphonefabrikanten updates blijven doorgeven aan eindgebruikers van dit specifieke toestel, als KPN hebben we daar geen rol in.

We verzoeken smartphonefabrikanten waarvan wij de producten verkopen, deze producten actief te blijven ondersteunen. Daarom hebben we ook de vraag uitstaan bij HTC of dit bewuste toestel nog steeds wordt voorzien van de laatste beveiligingsupdates. In afwachting van een reactie vanuit HTC bieden wij het toestel voorlopig niet commercieel aan.

In reactie op de vraag of KPN haar klanten adviseert over de risico's van verouderde software:

Wij adviseren klanten altijd de laatste softwareversie te installeren. Met enige regelmaat worden er nieuwe updates aangeboden, vaak bevatten deze ook beveiligingsupdates. Zo houden klanten de meeste internetgevaren al buiten de deur. Zie onder meer www.kpn.com/veilig (https://www.kpn.com/service/internet/veilig-internetten/veilig-online-op-je-smartphone.htm. Ook bieden we KPN ToestelVeilig aan

(https://www.kpn.com/mobiel/bundels/toestel-veilig.htm), daarmee kunnen gebruikers hun smartphone beschermen en beveiligen. KPN ToestelVeilig is beschikbaar voor Android telefoons en heeft een anti-virusfunctionaliteit. Bij een Alles-in-1 en Internet abonnement van KPN is ToestelVeilig bovendien gratis voor twee toestellen (bijvoorbeeld smartphone en tablet).

Lees verder Inklappen