Hoe operators hun netwerk kunnen beveiligen

Old-school hacking treft smartphones

Smartphones en tablets zijn vatbaar voor allerhande virussen en malware-infecties. Meestal is het de taak van de gebruiker om zich daartegen te beschermen. Hij moet pincodes instellen, firewalls opzetten en virusscanners installeren. Cybercriminaliteit is echter niet een probleem van de eindgebruiker alleen. Ook operators hebben er belang bij om het te bevechten en bezitten daar tevens de middelen toe.

DOOR FRANK FRANSEN, TIM HARTOG, FRANK MULLER EN THIJS VEUGEN

SMS-o'-death doet smartphones crashen

Sinds 2002 wordt, voornamelijk door leveranciers van virusscanners, al gewaarschuwd voor het gevaar van virussen en andere kwaadwillende applicaties op smartphones. Deze applicaties noemt men ook wel mobiele malware (de naam is een afgeleide van malicious software). Hoewel de hoeveelheid gedetecteerde mobiele malware sinds 2002 alleen maar is toegenomen, heeft dit tot nu toe nooit tot grootschalige besmettingen of problemen geleid.
Toch is het de verwachting dat deze situatie zal veranderen door de groeiende populariteit van iPhones en Androids en door het succes van virtuele applicatiemarkten, zoals Android Market en de App Store. De veelgebruikte webbrowser en e-mailclient maken deze telefoons kwetsbaar. Door de toename van de persoonlijke en financiële informatie op de apparaten worden smartphones een steeds interessanter doelwit voor cybercriminelen. Recente studies naar de belangrijkste securityrisico's van smartphones richten zich vooral op de gevolgen voor bedrijven en consumenten. Een paar voorbeelden:

1. Wanneer je toestel wordt gestolen of wanneer je het verliest of verkoopt, dan is je persoonlijke informatie eenvoudig te achterhalen door een kwaadwillende die het toestel in handen krijgt.
2. Apps hebben vaak, zonder dat de gebruiker zich daarvan bewust is, toegang tot locatie-informatie, persoonlijke data op het toestel of zelfs de microfoon en camera. Dit kan een legitiem onderdeel van de app zijn, maar het kan ook gaan om illegale spyware die persoonlijke data verzamelt om er geld mee te verdienen.
3. Via internet, e-mail, maar ook sms kunnen aanvallen worden gedaan die in vergelijkbare vorm al eerder in de pc-wereld zijn gebruikt, zoals phishing met fake berichten om user credentials te verzamelen. Denk ook aan ongewenste berichten via sms en e-mail oftewel spam en malware-infecties om gevoelige financiële gegevens te achterhalen.

Om dergelijke securityrisico's te reduceren bestaan er diverse maatregelen, die ook al worden toegepast. Een voorbeeld is het gebruik van digitale handtekeningen waarmee de integriteit van een app kan worden verbeterd, doordat je zeker weet van wie deze afkomstig is. Een ander voorbeeld is de sandbox. Deze creëert een gecontroleerde omgeving in het operating systeem waarin apps kunnen draaien. Ook capability-based security biedt de mogelijkheid van extra controle binnen het operating system door de toegang tot systeembronnen te reguleren. Door af te dwingen dat apps alleen via de virtuele markt kunnen worden geïnstalleerd, krijgen Apple en Google de mogelijkheid om software van derden aan een controle te onderwerpen voordat de app kan worden aangeboden.
De voornoemde risico's en maatregelen zijn redelijk bekend, maar richten zich vooral op de gebruiker van de smartphone. De risico's voor operators blijven echter vaak onderbelicht, terwijl ze juist vragen om andersoortige oplossingen. Een operator is gebaat bij een correcte afhandeling en betaling van de mobiele telecomdiensten. De twee belangrijkste dreigingen die dat in de weg staan bij het gebruik van smartphones zijn dialers en denial-of-serviceaanvallen (DoS).

Dialers

Het probleem van dialers bestaat al lang in de telecomwereld. Pc's hadden een inbelmodem om verbinding te maken met het internet. Zodra de gebruiker kon worden verleid om dialersoftware te installeren, vaak onder het mom van toegang tot speciale content, ontstond de mogelijkheid om de pc dure betaalnummers te laten bellen. De aanvaller, die deze nummers beheerde, zag het geld illegaal binnenstromen. Ondanks de onvoorzichtigheid van de gedupeerden stelden de operators hen vaak deels schadeloos en zo kregen ook zij een deel van de rekening gepresenteerd. De eigenaar van het betaalnummer had immers wel recht op zijn geld. Dialers werden hierdoor een serieus probleem voor operators.
Met de opkomst van ADSL en kabelinternet, en daarmee het verdwijnen van de inbelmodems, raakte deze dreiging op de achtergrond. De groeiende adoptie van de smartphone, die naast een internetverbinding ook belfunctionaliteit heeft, zorgt mogelijk weer voor een opleving van de kwaadaardige dialersoftware. De afgelopen jaren zijn er apps voor Symbian en Android ontdekt die heimelijk sms'jes sturen naar dure servicenummers. Bij een recent incident in China zorgde een fake antivirus-app voor malware op de smartphone, die automatisch sms-berichten met URL-links ging verspreiden naar persoonlijke contacten. Meer dan een miljoen gebruikers raakten geïnfecteerd en de kosten liepen hoog op.
Om het dialerprobleem tegen te gaan, houden operators het verbruik van klanten in de gaten. Zodra dit boven een bepaalde drempel komt, is er vaak iets verdachts aan de hand. Verder kunnen de sms-berichten binnen het netwerk worden gecontroleerd op kwaadaardige content middels filtering en blacklisting. Een alternatieve, nog niet gehanteerde methode is het gebruik van whitelisting voor legitieme servicerequests. Hierbij zijn de lijsten vaak beter beheersbaar dan bij blacklisting, omdat illegale services doorgaans geen lang leven beschoren is en de onbetrouwbare adressen dus vaak veranderen.

Denial of service

Het tweede serieuze probleem voor operators vormen de DoS-aanvallen. Malware of specifiek geconstrueerde sms-berichten kunnen toestellen dermate van slag brengen dat ze niet meer functioneren. Behalve ongemak voor de gebruiker veroorzaken dergelijke acties ook een extra belasting voor de operator, die wordt ingeschakeld om het probleem te verhelpen. Het kan zelfs zo ver gaan dat een grootschalige aanval op toestellen van een bepaalde operator wordt opgezet om uiteindelijk die operator te kunnen afpersen. Hij moet dan betalen om van het probleem af te komen.
Met zijn zogenoemde SMS-o'-death heeft Collin Mulliner aangetoond dat het sturen van een sms'je naar diverse dedicated toestellen voldoende is om ze te laten crashen. De doods-sms blijkt door zijn binaire formaat tevens lastig te filteren op het operatornetwerk. Ook via malware op het toestel kan een kwaadwillende vanaf een willekeurige plek op aarde je toestel laten blokkeren of zelfs stukmaken. Met een beetje creativiteit kun je allerlei toepassingen bedenken voor zo'n aanval.
Als je specifiek de operator dwars wil zitten, zijn er alvast twee mogelijkheden. Ten eerste kun je de simlock van het toestel omzetten naar een andere operator, zodat het toestel geen verbinding meer kan krijgen met zijn eigen netwerk. Ten tweede kun je de sim blokkeren door verkeerde pin- en PUK-codes in te voeren. Dit leidt niet alleen tot een groot aantal dure helpdeskcalls, maar de operator moet dan zelfs een nieuwe simkaart uitgeven, wat nog meer kosten met zich meebrengt.
Om te voorkomen dat de gevolgen van zo'n aanval voor gebruiker en operator uit de hand lopen, kun je denken aan een alternatieve oplossing: een automatische herstart van het toestel of een geforceerde terugkeer naar de fabrieksinstellingen nadat voor de zoveelste maal een verkeerde PUK-code is ingegeven. Hierdoor blijft in ieder geval de functionaliteit van de smartphone behouden.

Nieuwe oplossingen

Waar de meeste artikelen over smartphone security tegenwoordig de nadruk leggen op de risico's voor de gebruiker, is de rol van de operator vaak nog onderbelicht. Telecomoperators zullen echter te maken krijgen met bekende dreigingen in een nieuw jasje, zoals dialers en DoS, die ze in de gaten moeten houden en waarvoor ze nieuwe oplossingen moeten bedenken.
Er wordt wel degelijk gewerkt aan manieren om malware voor smartphones en internettablets tegen te gaan. Zo zijn de Trusted Computer Group (TCG) en het Open Mobile Terminal Platform (OMTP) bezig om het platform robuuster te maken, maar dat zie je nog niet terug op de markt. Er is daarom reden om de ogen open te houden en toe te werken naar goede oplossingen, anders blijven we beperkt tot lapmiddelen en kunnen de kosten voor de operators aardig uit de hand lopen. De toenemende onveiligheid kan voor operators ook aanleiding zijn om zich van concurrenten te onderscheiden door extra voorzieningen op securitygebied. Natuurlijk kunnen ze hun toevlucht nemen tot maatregelen die we kennen uit de pc-wereld, zoals databackups, biometrie en dergelijke. Aan de andere kant kan men ook zoeken naar nieuwe maatregelen die specifiek voor smartphones geschikt zijn. Een beveiligingsoplossing die beschikbaar is als app in de appstores, wellicht?

Ir. Frank Fransen (frank.fransen@tno.nl), **ir. Tim Hartog** (tim.hartog@tno.nl), **ir. Frank Muller** (frank.muller@tno.nl) en **dr. ir. Thijs Veugen** (thijs.veugen@tno.nl), zijn allen werkzaam bij TNO op het gebied van information security.

Bronnen

Trojan targets mobile phones running Java applications op *www.kaspersky.com/news?id=180984542*, Kaspersky, 28 februari 2006

Golde, N. en Mulliner, C., *SMS-o'-death. From analyzing to attacking mobile phones on a large scale* op *www.mulliner.org/security/sms/feed/smsodeath_mulliner_golde_cansecwest2011.pdf*, Vancouver, 9 maart 2011

Hogben, G., met Dekker, M., *Smartphones. Information security risks, opportunities and recommendations for users* op *www.enisa.europa.eu/act/it/oar/smartphones-information-security-risks-opportunities-and-recommendations-for-users/at_download/fullReport*, ENISA, december 2010

Janssen, R., *Sms-trojan schrikt de Androidwereld op!* op *www.androidworld.nl/37236/sms-trojan-schrikt-de-android-wereld-op*, Androidworld, 9 augustus 2010

Prince, B., *Mobile malware targets Chinese users* op *http://securitywatch.eweek.com/mobile_malware/mobile_malware_targets_chinese_users.html*, eWeek, 12 november 2010