Veiligheid van de mobiele werkplek

Een white paper van RAM Mobile Data

Schrijver: Hans Heising
24-07-2008

Inhoudsopgave

Mobiele datacommunicatie en beveiliging: geen vanzelfsprekendheid

De businessomgeving van de meeste organisaties kenmerkt zich vandaag de dag in toenemende mate door flexibiliteit. Mobiel werken met behulp van GPRS-/UMTS-netwerken en het daarmee gepaard gaande gebruik van devices als mobiele telefoons, smart phones en PDA's wordt meer en meer een vanzelfsprekendheid. Maar dat geldt niet voor de beveiliging van het vaak bedrijfskritische dataverkeer. Het is de ervaring van RAM Mobile Data dat de meeste organisaties hun mobiele medewerkers uitrusten met standaard mobiele communicatievoorzieningen die gebruikmaken van het vrij toegankelijke publieke internet, zonder daarbij veel aandacht te schenken aan het beveiligingsaspect.

Mobiel dataverkeer onder vuur
Een dergelijke aanpak is zeker niet zonder gevaar! Reeds in 2005 was er binnen de wereld van de mobiele datacommunicatie sprake van een aantal virussen en wormen, zoals Cabir, Duts, Skulls en Comwar. Hoewel daarbij geen grote of onherstelbare schade ontstond, gaf dit wel aan dat kwaadwillenden toen al druk bezig waren manieren te ontwikkelen om aanvallen uit te voeren op het mobiele dataverkeer en de achterliggende technologie.

Het internationale onafhankelijke onderzoeksbureau Forrester verwacht dat dergelijke aanvallen zich in de toekomst vooral zullen richten op drie gebieden:
1. verstoren van lokale mobiele netwerken door het gebruik van wormen, virussen en spyware;
2. overnemen van mobiele telefoons om daarmee SMS-en te versturen en telefoongesprekken te voeren;
3. stelen van informatie op PDA's.

Goede beveiligingsstrategie cruciaal
Organisaties mogen dergelijke waarschuwingen zeker niet in de wind slaan. Zij zullen actie moeten ondernemen en niet bij voorbaat mogen vertrouwen op de informatie van leveranciers van mobiele operating systems zoals Microsoft en Nokia. Ondanks de geruststellende woorden dat hun operating systems 100% veilig zijn, is de realiteit vaak weerbarstiger. Zo heeft Microsoft in theorie slechts één Windows Mobile-platform, in werkelijkheid bestaan er maar liefst meer dan 250 variaties die kunnen worden geconfigureerd. Dat grote aantal maakt een goede beveiliging er bepaald niet gemakkelijker op!
Dit alles illustreert dat u goed moet nadenken over het formuleren van een beveiligingsstrategie voor uw mobiele dataverkeer. Stel u daarbij eens de volgende vragen:

- Waarom zou u eigenlijk gebruikmaken van mobiele datacommunicatie?
- Welke bedrijfsprocessen worden ondersteund en hoe bedrijfskritisch zijn die?
- Welke risico's loopt u als uw gegevens in verkeerde handen terechtkomen?
- Voor welke medewerkers is mobiel werken essentieel en voor welke maar bijzaak?

De antwoorden op die vragen verschaffen u belangrijke informatie over het belang van het beveiligen van uw mobiele dataverkeer.

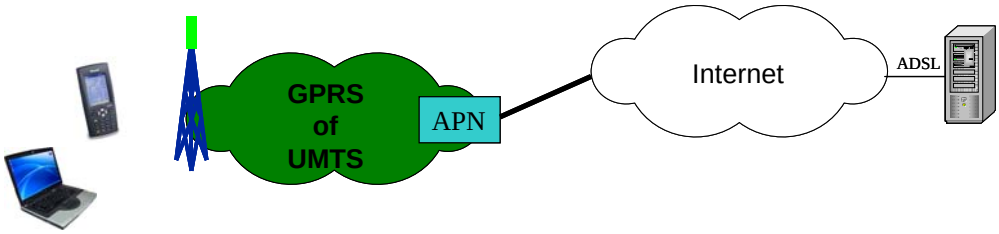
Twee basisconfiguraties

Voor een beter begrip van de inhoud van dit whitepaper is het goed om te weten dat er in principe twee basisconfiguraties bestaan om een mobiel GPRS-/UMTS-toestel verbinding te laten maken met een centrale serverlocatie:

- Standaard GPRS-/UMTS-aansluiting via het publieke internet
- GPRS-/UMTS-aansluiting via Private APN

Standaard GPRS-/UMTS-aansluiting via het publieke internet

In de meest simpele vorm kan een mobiele terminal verbinding maken met een centrale server, door beide systemen aan te sluiten op het publieke internet met behulp van een standaard GPRS- of UMTS-abonnement.



Als u op deze manier een mobiel device via een GPRS- of UMTS- verbinding aansluit, worden de poorten van dit device binnen een paar minuten gescand door zogenaamde poortscanners of internetapplicaties die de verbinding willen gebruiken om niet alleen goedwillende, maar ook kwaadwillende redenen. Daar komt nog bij dat de gebruiker betaalt voor dit verkeer!

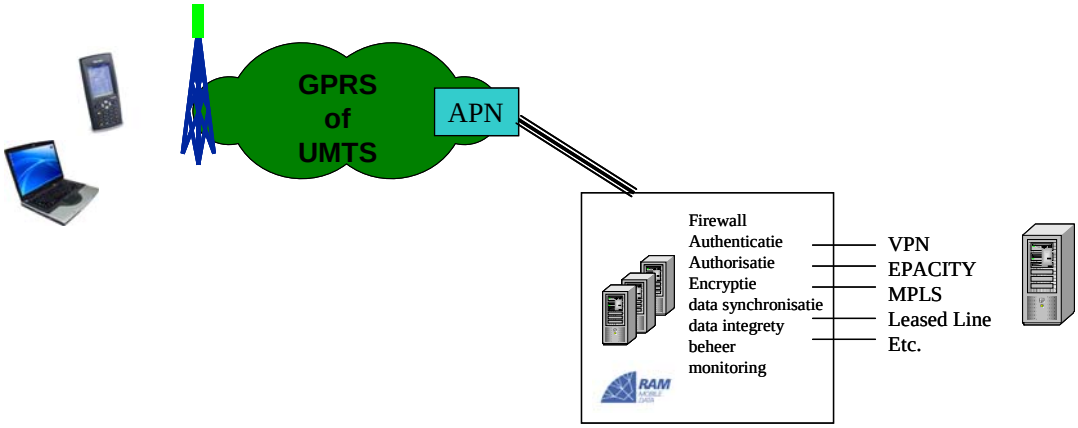
Dat betekent in de praktijk dat u voor de beveiliging van zowel het mobiele device als de server een groot aantal maatregelen zult moeten treffen.

GPRS-/UMTS-aansluiting via Private APN

Een tweede optie voor mobiel dataverkeer bestaat uit het gebruik van een Private APN (Access Point Name). Een Private APN is een directe, beveiligde en gesloten verbinding tussen een mobiel netwerk en het hostsysteem, geheel buiten internet om. Die beveiliging wordt gegarandeerd door de mogelijkheid verschillende beveiligingsmechanismen in te bouwen. Deze komen later in dit whitepaper uitgebreid aan bod.

Om te voorkomen dat een GPRS-/UMTS -toestel toch een verbinding opbouwt met het internet (en zo toegankelijk wordt voor andere internetgebruikers) moet u het device zodanig configureren dat het contact zoekt met een Private APN. Op de SIM-kaart van de mobiele gebruiker wordt dan aangegeven tot welke Private APN's deze toegang

heeft. Deze technologie maakt het mogelijk de verbindingen naar mobiele devices op een veilige manier te beheren.



Belangrijke beveiligingsvragen

Zoals gezegd, de enorme flexibiliteit van mobiele communicatiesystemen dwingt organisaties ertoe maatregelen te treffen om ervoor te zorgen dat er geen misbruik wordt gemaakt van die systemen, bijvoorbeeld door ongewenste aanvallen van virussen, spam en spyware.

Systeembeheerders moeten zich in dit verband dan ook een aantal belangrijke vragen stellen:

- Is de mobiele gebruiker wel wie hij zegt dat hij is?
- Tot welke server krijgt de mobiele gebruiker toegang?
- Kunnen vreemden toegang krijgen tot het mobiele device?
- Kan de informatie onderweg afgetapt worden?
- Hoe toegankelijk is de data op het mobiele device?
- Kan er data verloren gaan of verminkt worden?

In dit whitepaper presenteert RAM Mobile Data op basis van haar jarenlange ervaring met deze problematiek een helder overzicht van de verschillende maatregelen die u kunt nemen om bovenstaande vragen afdoende te beantwoorden. Die informatie helpt u een eind op weg om de voor uw organisatie optimale beveiligingsstrategie te ontwikkelen voor uw bedrijfskritische mobiele datacommunicatie.

Is de mobiele gebruiker wel wie hij zegt dat hij is?

Om deze vraag afdoende te beantwoorden is een betrouwbare authenticatieprocedure noodzakelijk, waarbij verificatie van de identiteit van de gebruiker plaatsvindt. Want als een mobiele gebruiker toegang wil verkrijgen tot uw centrale server, moeten u er van uit kunnen gaan dat die gebruiker is wie hij zegt dat hij is. Om dit afdoende te kunnen controleren moet worden voldaan aan drie voorwaarden:

- Geen verbinding via het publieke internet
- Verbinding via Private APN
- Gebruik van Radius authenticatieserver

Geen verbinding via het publieke internet

Als uw verbindingen niet via het publieke internet lopen, is het onmogelijk vanaf internet toegang te verkrijgen tot uw server. Gebruikers die toegang willen krijgen tot de server moeten hun communicatie dan namelijk altijd opzetten vanaf het eigen GPRS-/UMTS-netwerk. Dit beperkt de mogelijkheden tot misbruik al enorm. Als de verbindingen niet via het internet verlopen, wordt namelijk automatisch gebruikgemaakt van een Private APN.

Verbinding via Private APN

Het gebruik van een Private APN als verbinding tussen het GPRS-/UMTS- netwerk en het hostsysteem maakt een betrouwbare authenticatie mogelijk. Immers, alle mobiele gebruikers, van wie bij aanmelding niet is geregistreerd dat ze toegang mogen hebben tot de Private APN, worden simpelweg geweigerd.

Voor uw informatie: RAM Mobile Data beschikt over een Private APN-aansluiting op alle bestaande GPRS/UMTS-netwerken.

Gebruik van Radius authenticatieserver

Alle mobiele gebruikers die toegang aanvragen tot het hostsysteem, ondergaan daarnaast een check in een Radius authenticatieserver. Als daarbij blijkt dat een gebruiker bekend is, deelt deze server een vast IP-adres aan hem uit. Dit betekent dat de serverapplicatie aan het IP-adres altijd kan zien met welke mobiele gebruiker de communicatie plaatsvindt. Dit in tegenstelling tot de standaard GPRS-/UMTS-abonnementen van de telecomoperators die geen vaste IP-adressen gebruiken.

Tot welke server krijgt de mobiele gebruiker toegang?

Naast authenticatie speelt bij optimaal beveiligd mobiel dataverkeer ook autorisatie een belangrijke rol. Want na een succesvol doorlopen authenticatieprocedure, kan vervolgens op IP-nummer/poortniveau ook nog bepaald worden wat een gebruiker wel mag en wat niet: over welke rechten beschikt hij en tot welke systemen krijgt hij toegang?

Op die manier kunt u ook vastleggen of die mobiele gebruiker toegang krijgt tot internet en zo ja, om welke sites het daarbij gaat. Want doordat de internetverbinding nu plaatsvindt via centrale proxy- en firewall-systemen, is er nog steeds sprake van optimale beveiliging.

Kunnen vreemden toegang krijgen tot het mobiele device?

De hierboven beschreven authenticatie- en autorisatieprocessen hebben tot doel te voorkomen dat onbevoegden toegang kunnen krijgen tot de serverapplicatie. Maar daarmee zijn nog niet alle potentiële bedreigingen afdoende afgewend.
Door gebruik te maken van een Private APN is, zoals eerder in dit whitepaper aangegeven, rechtstreekse toegang vanaf internet naar de mobiele devices niet langer mogelijk. Om daarnaast te voorkomen dat onbevoegden toegang krijgen tot de mobiele devices via de systemen die contact moeten hebben met de mobiele devices, is een geavanceerd firewall-systeem een absolute must, inclusief voorzieningen zoals Intrusion Detection Systems.

Kan de informatie onderweg afgetapt worden?

Als u alle mogelijke beveiligingsmaatregelen hebt genomen voor het vaste GPRS-/UTMS-netwerk, kunnen kwaadwillenden altijd nog proberen het radiosignaal af te tappen. Standaard maken GPRS en UMTS al gebruik van steeds wisselende cyphering keys, waardoor de informatie die door de lucht gaat, altijd versleuteld is. Voor aanvullende beveiliging kunt u er voor kiezen extra encryptie toe te voegen op de data tussen het mobiele device en het hostsysteem, zodat ook de informatie tussen dat systeem en de APN-verbinding versleuteld is.

Hoe toegankelijk is de data op het mobiele device?

Als een mobiel device in handen valt van een onbevoegde, moet u voorkomen dat op dat moment ook alle bedrijfskritische gegevens, zoals klant- of patiëntgegevens, toegankelijk zijn.

Een goede beveiliging is mogelijk door (een gedeelte van) die gegevens lokaal te versleutelen. Daarvoor zijn tegenwoordig goede middleware-systemen beschikbaar, die ontwikkeld zijn om op correcte wijze om te gaan met de onvolkomenheden van mobiele communicatieoplossingen. Bij geavanceerde systemen is het mogelijk deze versleuteling per veld in te stellen, zodat gevoelige gegevens nooit door onbevoegden te ontcijferen zijn. En dat terwijl de impact van deze maatregel op de performance minimaal blijft.

Kan er data verloren gaan of verminkt worden?

Tot slot is er de integriteit van de data. Helaas is het in het standaard Internet Protocol (IP) mogelijk dat data verloren gaat of dat informatie verminkt overkomt. Om dergelijke problemen in de datatransmissie te voorkomen wordt op de transportlaag (OSI laag 4) doorgaans het Transmission Control Protocol (TCP) toegevoegd.

Maar dan is het op sessie- en applicatieniveau nog steeds mogelijk dat data onvolledig overkomt, bijvoorbeeld doordat een mobiel device tijdens de datatransmissie buiten het bereik van het netwerk komt.
Mobiele middleware-systemen, zoals Navara. houden rekening met dit soort problemen door op applicatieniveau te controleren of de data goed is aangekomen. De verzendende partij onthoudt daarbij welke data verstuurd is, totdat hij een terugmelding ontvangt van de ontvangende partij dat de datatransmissie correct heeft plaatsgevonden. Dit proces voltrekt zich op een efficiënte wijze op de achtergrond, zodat de gebruiker hier geen last van ondervindt.

Samenvatting

Om te anticiperen op de kwetsbaarheden in uw mobiele communicatie-omgeving moet u een beveiligingsstrategie ontwikkelen die is toegespitst op uw specifieke bedrijfsomgeving. Op die manier blijft de communicatie met uw mobiele devices beheersbaar en veilig. En dat stelt u in staat uw applicaties eenvoudig en optimaal beveiligd mobiel te ontsluiten.

RAM Mobile Data is daarbij een voorstander van het gebruik van Private APN's. Op die manier bent u in staat alle benodigde beveiligingsmaatregelen centraal in te richten en te beheren. Centrale firewalls en Radius-servers vormen daarbij de basis voor waterdichte authenticatie- en authorisatieprocedures.

Tenslotte beveelt RAM Mobile Data het gebruik van middleware-systemen aan, die rekening houden met de onvolkomenheden van mobiele communicatie.

Vragen?

Indien u vragen heeft naar aanleiding van deze whitepaper, dan kunt u contact opnemen met de heer P. Groot via telefoonnummer 0302390385 of via de e-mail pgroot@ram.nl.