Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Wifi-beveiliging

De onderschatte schakel in netwerkbeveiliging

Versie 1.0

Wifi-beveiliging

De onderschatte schakel in netwerkbeveiliging

Versie 1.0

Nationaal Cyber Security Centrum
Turfmarkt 147 | 2511 DP Den Haag
Postbus 117 | 2501 CC Den Haag
T 070 751 55 55 | F 070 888 75 50
www.ncsc.nl | info@ncsc.nl

Oktober 2013

Nationaal Cyber Security Centrum

Het Nationaal Cyber Security Centrum (NCSC) draagt via samenwerking tussen bedrijfsleven, overheid en wetenschap bij aan het vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein.

Het NCSC ondersteunt de Rijksoverheid en organisaties met een vitale functie in de samenleving met het geven van expertise en advies, response op dreigingen en het versterken van de crisisbeheersing. Daarnaast voorziet het in informatie en advies voor burger, overheid en bedrijfsleven ten behoeve van bewustwording en preventie. Het NCSC is daarmee het centrale meld- en informatiepunt voor ICT-dreigingen en -veiligheidsincidenten.

Het NCSC is een onderdeel van de Directie Cyber Security van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).

Samenwerking en bronnen

Dit Whitepaper is opgesteld door het NCSC. In een samenwerking met deskundigen uit publieke organisaties is dit whitepaper gerealiseerd. Hun inhoudelijke reviews alsmede openbaar toegankelijke bronnen hebben in sterke mate bijgedragen aan de inhoud van dit whitepaper.

Samenvatting

Het gebruik van draadloze netwerken heeft een flinke vlucht genomen. Met een mobiel apparaat, zoals een smartphone, tablet of laptop, heeft iemand op iedere plek ter wereld - waar een wifinetwerk is – potentieel toegang tot zijn/haar informatie. Zo is het tegenwoordig heel normaal dat in de lounge van een vliegveld de zakelijke e-mail op een tablet wordt gelezen. Draadloos werken biedt vele voordelen maar kent – zeker in vergelijking met een netwerk met vaste aansluitingen - ook ernstige en specifieke dreigingen, die de betrouwbaarheid van de informatievoorziening van een organisatie kunnen aantasten.

Het doel van deze whitepaper is om de lezer bewust te maken van de bedreigingen en risico's van draadloze netwerken, en de lezer te helpen met een aanpak om te komen tot een gedegen implementatie en vervolgens bijpassende maatregelen aan te reiken om veilig met draadloze netwerken om te kunnen gaan. Het whitepaper concentreert zich daarbij op de vraag hoe een gekozen beleid voor draadloze communicatie geïmplementeerd kan worden. Het document beperkt zich tot wifi, een wijdverspreide vorm van draadloos netwerken, die wordt ondersteund door vrijwel alle mobiele apparaten zoals smartphones, tablets en laptops.

Veilige inrichting en toepassing van wifi

De veilige inrichting van een wifinetwerk vereist een project- en planmatige aanpak. Het handhaven van de beveiliging van een wifinetwerk vereist echter continue aandacht en zal als de inrichting is afgerond in de lijn moeten worden belegd. Maatregelen moeten immers niet alleen worden geïmplementeerd, ze moeten ook worden gecontroleerd, geactualiseerd en vernieuwd.

Er kan daarom worden gesproken over lifecyclemanagement. In de opzet en het gebruik van een veilig wifinetwerk worden de volgende stappen onderkend: ICT-beleidskeuze op basis van risicoanalyse, architectuurontwerp, implementatie, beheer & onderhoud, doorontwikkeling en ontmanteling

Scenario's voor wifi-gebruik

Het whitepaper beschrijft een aantal scenario's die (IT-)managers, (IT-)beleidsadviseurs, securitycoördinatoren, managers informatiebeveiliging en projectleiders in staat stellen om onderbouwde keuzes te maken als het gaat om het gebruik van wifi binnen hun organisatie. De volgende drie scenario's worden daarbij onderscheiden:

1. De organisatie besluit geen gebruik te maken van wifi, er wordt alleen gebruikgemaakt van een netwerk met vaste (bedrade) aansluitingen. Ook in dit geval moeten maatregelen worden getroffen om de veiligheid van bedrijfsinformatie zeker te stellen.
2. De organisatie besluit onder bepaalde voorwaarden en beperkingen gebruik te maken van wifi. Wifi wordt daarmee gecontroleerd beschikbaar gesteld aan specifieke doelgroepen, met toegang tot geselecteerde applicaties en bijbehorende gegevens.
3. De organisatie maakt geen onderscheid meer tussen het vaste netwerk en het wifinetwerk. De toegang tot en het gebruik van wifi is vrij voor geautoriseerde gebruikers.

Risico's

Een draadloos netwerk is van nature kwetsbaar voor onderschepping van de draadloze communicatie. Ook zijn mobiele apparaten kwetsbaar voor diefstal/verlies, waardoor de erop opgeslagen (bedrijfs)gegevens in vreemde handen kunnen komen. Veel

organisaties die de mogelijkheden van een draadloos netwerk (willen) gebruiken, zijn zich nog onvoldoende bewust van de risico's die dat met zich meebrengt, en hoe deze risico's succesvol weggenomen of beperkt kunnen worden.

Bij de inrichting van een wifinetwerk moeten we goed weten waartegen het netwerk moet worden beschermd. Hierbij dient rekening gehouden te worden met de diverse actoren, de dreigingen waar wifinetwerken aan blootstaan, op welke technologische, menselijke en organisatorische kwetsbaarheden deze zijn gericht en welke risico's en mogelijke gevolgen deze met zich meebrengen.

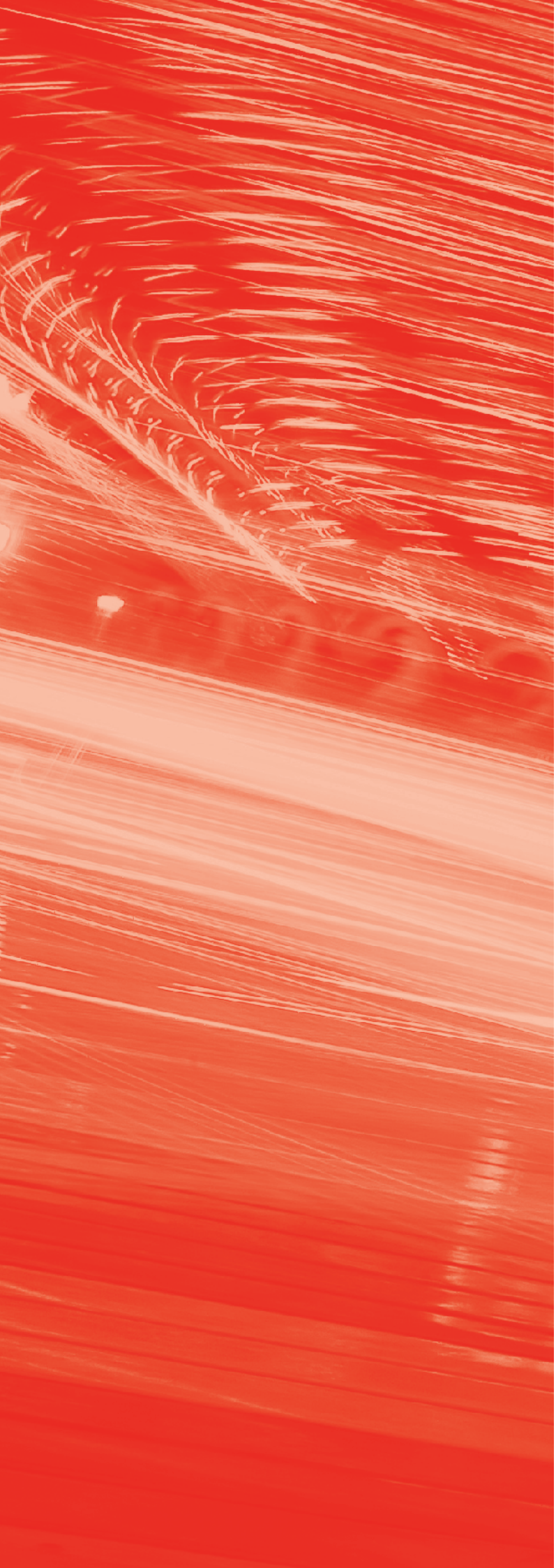
De dreigingen met betrekking tot wifinetwerken, zoals wardriving, rogue accespoints, spoofen van MAC-adressen, Denial-of-Service, richten zich in het bijzonder op:
» het verkrijgen van ongeautoriseerde toegang tot informatie;
» het manipuleren van informatie;
» het verstoren van de beschikbaarheid van informatie.

Maatregelen

Ieder van de scenario's kent specifieke maatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie te waarborgen en de risico's te mitigeren. De top-10 van meest belangrijke maatregelen is als volgt:

1. Zorg ervoor dat de basis van informatiebeveiliging op orde is;
2. Zorg voor een onderbouwde beleidskeuze over het gebruik van wifi;
3. Zorg ervoor dat de juridische risico's zijn onderzocht en afgedekt;
4. Zorg ervoor dat het beheer van de maatregelen goed is ingericht;
5. Zorg ervoor dat gebruikers en beheerders zich bewust zijn van de risico's;
6. Zorg voor een architectuur die past bij de organisatie;
7. Zorg voor methoden van afdoende sterkte voor versleuteling en authenticatie;
8. Zorg voor passende fysieke beveiliging van de netwerkcomponenten;
9. Zorg voor passende beveiliging van de mobiele apparaten;
10. Neem eventueel aanvullende maatregelen op netwerkniveau.

De belangrijkste technische maatregelen voor wifi zijn nader beschreven op basis van best practices. Er wordt hierbij een onderscheid gemaakt tussen het aanbieden van wifi (accesspoint) en het afnemen van wifi (client). «



Inhoud

1 Inleiding

1.1 Waarom een whitepaper over wifibeveiliging?

Wifi biedt vele voordelen, maar kent in vergelijking tot een bedraad netwerk ook ernstige en specifieke dreigingen, die de betrouwbaarheid van de informatievoorziening van een organisatie kunnen aantasten.

Nieuw in dit kader is de opkomst van het fenomeen *consumerization*[1]: de trend dat nieuwe technologieën en toepassingen eerst doorbreken in de consumentenmarkt en van daaruit doordringen in organisaties. Het gebruik van smartphones en tablets, bijvoorbeeld volgens het *Bring Your Own Device* (BYOD)[2] principe, en de inzet van slimme clouddiensten zoals Dropbox zijn hier voorbeelden van.

Het doel van deze whitepaper is om organisaties te helpen de weerbaarheid van hun wifinetwerken te verhogen tegen misbruik.

Een bijzondere constatering daarbij is dat ook een organisatie die het gebruik van wifi niet toe wil staan, gerichte maatregelen moet treffen om dat zeker te stellen.

Deze whitepaper brengt relevante informatie rondom de beveiliging van wifinetwerken in samenhang bij elkaar en geeft aan waar aanvullende informatie is te vinden. Daarnaast bevat het whitepaper een aanpak om te komen tot de juiste beveiliging van een wifinetwerk, en worden drie scenario's uitgewerkt.

1.2 Voor wie is dit document bedoeld?

Dit document is bestemd voor securitycoördinatoren, managers informatiebeveiliging, projectleiders, (IT-beleids)adviseurs, IT-managers en architecten. Het is bedoeld voor de securitycoördinator en manager informatiebeveiliging die belast is met toezicht op de betrouwbaarheid van de informatievoorziening, de projectleider van een project waarbinnen wifi een rol speelt, de (IT-beleids) adviseur en IT-manager die een beeld nodig heeft van beveiligingsaspecten van wifi en de architect die wil weten welke vragen in het ontwerp moeten worden beantwoord.

Deze whitepaper bevat zowel informatie op het niveau van aanpak en scenario's als technische informatie. U kunt als lezer op basis van de leeswijzer kiezen welke informatie voor u relevant is.

1.3 Leeswijzer

Deze whitepaper beschrijft wifibeveiliging in een logische volgorde, van een aanpak voor de implementatie, scenario's voor de inrichting tot meer technische details.

Hoofdstuk 2 geeft een introductie op wifi, met een overzicht van de belangrijkste technische en gebruiksaspecten, de belangrijkste risico's en bijpassende maatregelen.

Hoofdstuk 3 beschrijft een aanpak voor de veilige implementatie van een wifinetwerk en geeft aanbevelingen voor de ontwikkeling, het beheer en de ontmanteling van het wifinetwerk.

Hoofdstuk 4 beschrijft een drietal scenario's waaruit een organisatie kan kiezen voor de implementatie van een wifi-omgeving. Per scenario is beschreven wat de relevante aspecten uit het oogpunt van informatiebeveiliging zijn.

Hoofdstuk 5 beschrijft de inrichting van een wifinetwerk en gaat dieper in op de beveiligingsaspecten: actoren, kwetsbaarheden en dreigingen. Tevens beschrijft dit hoofdstuk best practices die passen bij zowel het beschikbaar stellen als gebruikmaken van een wifinetwerk.

Hoofdstuk 6 beschrijft twee zaken, ten eerste de belangrijkste maatregelen om wifi te beveiligen in de vorm van een top 10 en ten tweede een basisniveau voor de beveiliging van wifi, gebaseerd op best practices.

Een overzicht van alle gebruikte afkortingen en termen staat in **bijlage A**. We hebben voor dit whitepaper diverse literatuurbronnen geraadpleegd. Op plaatsen waar we informatie uit de literatuurbronnen verwerkt hebben, verwijzen we hiernaar in de vorm van[#]. '[#]' verwijst naar een document opgenomen in **bijlage B**.

1.4 Totstandkoming en onderhoud

Dit document is gebaseerd op de huidige stand van zaken rond de beveiliging van wifinetwerken op de datum van de publicatie. De invulling van deze whitepaper is mede gebaseerd op de factsheets en adviezen die het NCSC eerder heeft uitgebracht rond de beveiliging van wifinetwerken.

Dit document is niet uitputtend en zal door het NCSC periodiek worden bijgewerkt wanneer ontwikkelingen rond kwetsbaarheden en dreigingen daartoe aanleiding geven.

Aanvullingen, opmerkingen of informatie over eigen ervaringen ontvangen wij graag via info@ncsc.nl.

1 De NCSC publicatie ´Consumerization en security´gaat nader in op de verschillende facetten van consumerization en de impact daarvan op informatiebeveiliging. (https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/consumerization--security.html)

2 Bring Your Own Device (BYOD) is het beleid om medewerkers, zakelijke partners en andere gebruikers toe te staan om persoonlijk geselecteerde en gekochte (computer)apparatuur - zoals smartphones, tablets en laptops - op de werkplek te gebruiken en met het bedrijfsnetwerk te verbinden.

2 Introductie wifi

2.1 Technologie

Draadloze netwerken worden over het algemeen aangeduid met de afkorting WLAN, wat staat voor Wireless Local Area Network. Hieronder vallen meerdere technieken, zoals wifi, Bluetooth en WiMAX. Tabel 2-1 geeft de verschillen en overeenkomsten tussen deze technieken weer.

Deze whitepaper beperkt zich tot de meest gebruikte vorm van draadloze netwerken, te weten wifi. Wifi is een wijdverspreide vorm van draadloze netwerken, die wordt ondersteund door vrijwel alle mobiele apparaten.

Wifi is een netwerkprotocol om draadloos informatie uit te wisselen, gebaseerd op de zogenaamde IEEE 802.11-standaard. Momenteel is de meest toegepaste (populairste) de 802.11g standaard en het meest recentst is de 802.11ac standaard, die snelheden tot 1 Gbps ondersteunt (in theorie zelfs tot 3,47 Gbps).

Wifi kent drie manieren van communicatie, te weten “infrastructure mode”, “WDS mode” en “ad-hoc mode”.

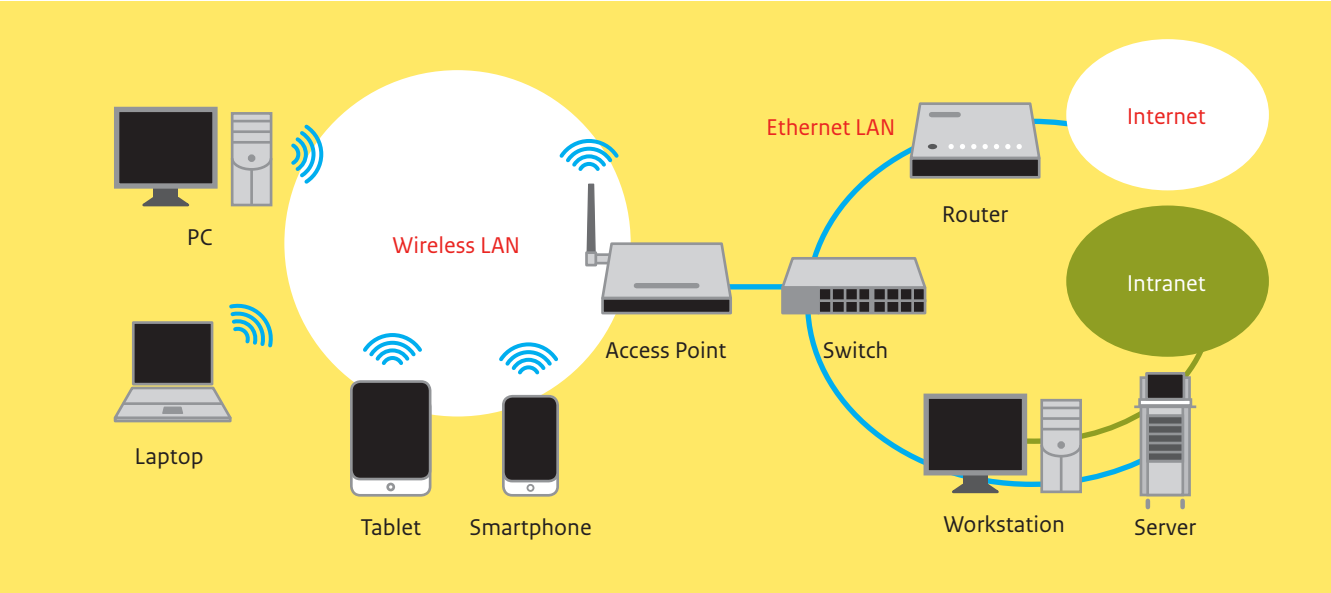
- Bij “infrastructure mode” communiceren de clients draadloos met toegangspunten (accesspoints), die de clients (bijvoorbeeld) koppelen aan het (bedrade) netwerk (zie figuur 2-1).
- De “WDS mode” wordt gebruikt om meerdere netwerken te koppelen. Wireless Distribution System (WDS) wordt bijvoorbeeld gebruikt om connectiviteit van gebouw tot gebouw te realiseren.
- Bij “ad-hoc mode” communiceren de clients (laptops, smartphones, tablets et cetera) onderling draadloos direct met elkaar (zie figuur 2-2).

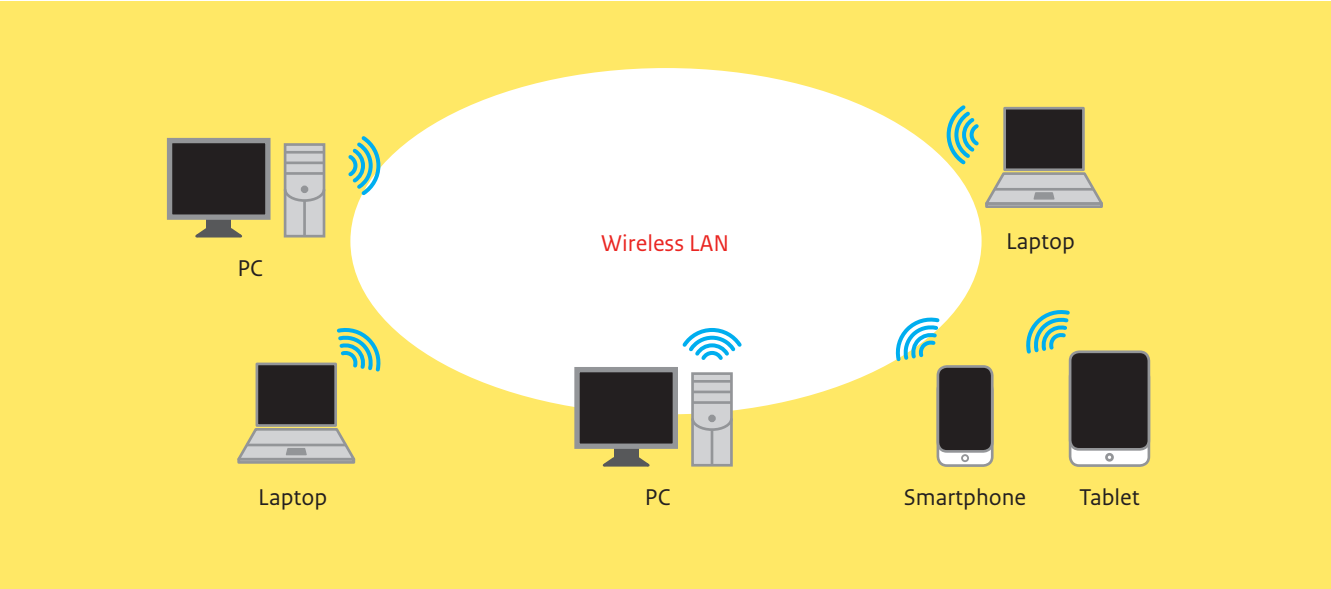
Infrastructure mode is de meest voorkomende variant, waarmee wifi binnen gebouwen beschikbaar wordt gesteld.

	Bluetooth	wifi	WiMAX
Gebruik	**Korte afstanden**	**Lokale verbindingen**	**Stedelijke verbindingen**
Frequentie(s)	2,400 tot 2,483.5 MHz	2.4 Ghz en/of 5.0 Ghz	2 Ghz – 66 Ghz (afh. licentie)
Snelheid (max theoretisch)	v1.2: 1 Mbps v2.1 + EDR: 3 Mbps v3.0 + HS: 24 Mbps	802.11g: 54 Mbps 802.11n: 450 Mbps 802.11ac: 3,47 Gbps	5 Mbps - WiMAX 2: 100 Mbps 802.16m: 300 Mbps
Bereik (+/-)	10 meter	100 meter	10 kilometer

Tabel 2-1 Draadloze netwerken

Figuur 2-1 Infrastructure mode





Figuur 2-2 Ad-hoc mode

2.2 Gebruik van wifi

Vrijwel alle moderne mobiele apparaten (laptops, smartphones, tablets et cetera) kunnen communiceren via wifi. Modems die door de Internet Service Provider (ISP) bij een internetabonnement wordt geleverd ondersteunen steeds vaker wifi en hierdoor is wifi ook thuis steeds vaker gemeengoed. Daarnaast bieden hotels, cafés et cetera wifi aan, soms betaald maar veelal gratis als onderdeel van de dienstverlening.

Juist vanwege het gemak bieden organisaties wifi aan voor eigen medewerkers en bezoekers. Zo kunnen zij via wifi hun e-mail op hun mobiele apparaat lezen, internet gebruiken of zelfs bedrijfsapplicaties raadplegen. Door medewerkers en bezoekers wordt het veelal als positief ervaren en steeds meer als standaarddienstverlening gezien.

Bedrijfsmatig gezien biedt wifi nog meer voordelen. Het is een flexibele infrastructuur die eenvoudig kan worden uitgebreid qua aantal aansluitingen en capaciteit. Dit in tegenstelling tot de traditionele bedrade netwerken waarbij uitbreiding lastiger is omdat dat vaak bouwkundige aanpassingen vereist en daarmee een stuk duurder is.

Het is te voorzien dat in de komende jaren een steeds groter deel van de netwerkcommunicatie zal verlopen via draadloze verbindingen in plaats van via bedrade verbindingen. De wifipenetratie zal de komende jaren wereldwijd enorm toenemen, volgens Strategy Analytics zal het totale aantal wifihuishoudens bijna 800 miljoen bereiken in 2016, een penetratiegraad van 42 procent [1]. Naast de voordelen qua kosten, flexibiliteit en gebruiksgemak zullen moderne mobiele apparaten standaard alleen van een draadloze aansluiting worden voorzien. Volgens de Wireless Broadband Alliance (WBA) zal door het toenemend aantal smartphones en tablets het aantal wereldwijde hotspots in 2015 stijgen naar 5,8 miljoen een toename van 350% ten opzichte van 2011 [2]. Zie ook het kader 'Thuismodem wordt wifihotspot'

Thuismodem wordt wifihotspot

Alle Ziggo-routers worden WiFi-hotspots [3]
Ziggo is druk bezig om overal waar het bedrijf internet aanbiedt, routers van Ziggo-klanten beschikbaar te stellen als wifihotspots (zogenaamde WifiSpots) voor andere klanten. Die gebruiken daarvoor een gereserveerd stukje op de routers van andere klanten die daarmee beschikbaar worden gesteld voor andere Ziggo-klanten. Met WifiSpots kunnen Ziggo-klanten onbeperkt gebruik maken van draadloos internet, op de plekken waar wifimodems van Ziggo staan. Zo hebben Ziggo-klanten met WifiSpots buitenshuis op meer dan 1 miljoen locaties in Nederland de beschikking over een wifiverbinding.

KPN-routers worden Fon wifi-hotspot [4]
KPN maakt in navolging van Ziggo zijn routers tot hotspots, maar doet dit in samenwerking met Fon. Alle nieuwe breedbandklanten van KPN krijgen later dit jaar een Fon-router, zodat een deel van hun bandbreedte kan worden gedeeld met andere zogenaamde 'Foneros'.

In ruil voor het delen van bandbreedte krijgt de klant toegang tot alle andere Fon-routers wereldwijd, ruim 7 miljoen. Fon wordt dus standaard, maar de klant kan zich afmelden.

2.3 Risico's en maatregelen

Het grootste gevaar bij draadloze netwerken is dat ongewenste toegang tot het bedrijfsnetwerk wordt verkregen en/of dat de informatie wordt afgeluisterd of gemanipuleerd. Daarnaast is de informatie die op een mobiel apparaat is opgeslagen kwetsbaar voor diefstal of verlies.

De risico's op misbruik zijn groter dan bij bedrade netwerken omdat toegang tot het bedrijfsnetwerk mogelijk is zonder dat men fysiek hoeft te zijn aangesloten. Omdat alle informatie met een zender wordt uitgezonden/ontvangen, is het voldoende om in de buurt van een accesspoint te zijn. Een voorbeeld hiervan is posten op een parkeerplaats in de buurt van een gebouw met een wifinetwerk, of met gevoelige antennes nog veel verder weg. Tegelijkertijd betekent dit dat (fysieke) controle op de betrouwbaarheid van gebruikers een stuk lastiger, zo niet onmogelijk is.

Bij het ontwerp van een wifinetwerk moet er rekening mee worden gehouden dat het netwerk zelf redelijk goed te beveiligen is, maar dat dit voor de mobiele apparaten veel moeilijker is. Een mobiel apparaat kan buiten het beveiligde netwerk gebruikt zijn en daardan ook besmet zijn geraakt met malware (kwaadaardige software). Uit dit risico wordt gelijk duidelijk dat niet alleen het netwerk beveiligd moet worden, maar ook de mobiele apparaten die van het netwerk gebruik maken moeten beveiligd worden. De mate van beveiliging zal per situatie vastgesteld moeten worden op basis van een risicoafweging.

Voor de beveiliging van wifi worden allerlei technieken gebruikt. Gescheiden netwerken, versleutelen van de communicatieverbinding en sterke authenticatie zijn bekende maatregelen. Voor wifi geldt dat naast gebruik van de juiste technieken, het gedrag van de gebruiker veel invloed heeft op de veiligheid van een wifinetwerk. Om een wifinetwerk afdoende te beveiligen moet daarom aandacht worden geschonken aan het complete scala van organisatorische, procedurele, fysieke en technische maatregelen. Tabel 2-2 geeft een voorbeeld van maatregelen voor ieder van deze vier invalshoeken. In de volgende hoofdstukken worden de risico's en bijbehorende maatregelen uitgediept aan de hand van een aantal scenario's en best practices.

Organisatorische maatregelen	Formuleer beleid voor de wijze waarop de organisatie met draadloze netwerken wil omgaan en formuleer beveiligingsbeleid voor wifi. Zorg ervoor dat gebruikers zich bewust zijn van de risico's van het gebruik van draadloze netwerken.
Procedurele maatregelen	Beschrijf de procedures voor veilig beheer van de wifivoorzieningen, inclusief monitoring, controles et cetera. Beschrijf de richtlijnen voor veilig gebruik van de wifivoorzieningen door gebruikers, bezoekers et cetera. Hierbij kan worden verwezen naar bestaande richtlijnen, zoals: » Baseline Informatiebeveiliging Rijksdienst Tactisch Normenkader (TNK) » Baseline Informatiebeveiliging Rijksdienst Operationele Baseline (OB) » SANS (SysAdmin, Audit, Network, Security) Security Project[3] » NIST (National Institute for Standards and Technology) – Special Publication 800-48 Rev 1- Guide to Securing Legacy IEEE 802.11 Wireless Networks [5] » NIST (National Institute for Standards and Technology) – Special Publication 800-153 Guidelines for Securing Wireless Local Area Networks [6]
Fysieke maatregelen	Zorg voor fysieke beveiliging van de wifi-accesspoints om te voorkomen dat deze kunnen worden misbruikt.
Technische maatregelen	Zorg ervoor dat een veilige versleutelmethode wordt gebruikt voor het versleutelen van de draadloze communicatie. Zorg ervoor dat de identiteit van gebruikers voldoende betrouwbaar wordt vastgesteld.

Tabel 2-2 Organisatorische, procedurele, fysieke en technische maatregelen

3 http://www.sans.org/projects/

3 Veilige inrichting en toepassing van wifi

De veilige inrichting van een wifinetwerk vereist een planmatige aanpak. Dit hoofdstuk helpt degene die verantwoordelijk is voor de inrichting, meestal een projectleider, met handreikingen voor dit plan. Het hoofdstuk beschrijft niet alleen de aanpak voor de keuze en implementatie van de juiste maatregelen, maar ook de borging daarvan tijdens de gebruiksfase.

3.1 Levenscyclus van een wifinetwerk

Het inrichten van een veilig wifinetwerk kan projectmatig worden aangepakt. Het handhaven van de beveiliging van een wifinetwerk vereist echter continue aandacht en zal als de inrichting is afgerond in de lijn moeten worden belegd. Maatregelen moeten immers niet alleen worden geïmplementeerd, ze moeten ook worden gecontroleerd, geactualiseerd en vernieuwd.

Er kan daarom worden gesproken over *lifecyclemanagement*. Er worden vaste stappen doorlopen bij de implementatie en iedere (substantiële) wijziging, totdat het wifinetwerk uiteindelijk wordt ontmanteld. In de opzet en het gebruik van een veilig wifinetwerk worden de volgende stappen onderkend:

1. ICT-beleidskeuze op basis van risicoanalyse
2. Architectuurontwerp
3. Implementatie
4. Beheer & onderhoud
5. Doorontwikkeling
6. Ontmanteling

Het kan zijn dat van deze stappen onderdelen al zijn geadresseerd binnen een organisatie. In deze gevallen kan dezelfde aanpak worden gebruikt, waarbij per stap een check op de noodzaak wordt uitgevoerd en reeds bestaande zaken worden hergebruikt.

In de navolgende paragrafen zijn de stappen nader beschreven.

3.2 ICT-beleidskeuze op basis van risicoanalyse

Informatiebeveiliging is primair een verantwoordelijkheid van het management. Het uitvaardigen van informatiebeveiligingsmaatregelen kan op gespannen voet komen te staan met het gemak van draadloze communicatie. Alleen de verantwoordelijk manager kan daarom verantwoord beslissen over de vaak tegenstrijdige belangen tussen informatiebeveiliging, efficiëntie en gebruiksvriendelijkheid.

In elke organisatie is het nodig om, voordat men besluit tot het invoeren van wifi, een risicoanalyse uit te voeren. Uit de risicoanalyse volgt onder meer in welke mate de toegang tot (bepaalde categorieën) informatie moet worden afgeschermd. Uitgaande van het risicoprofiel besluit een organisatie of en in welke vorm wifi in de ICT-infrastructuur wordt toegepast. Deze keuze is voornamelijk afhankelijk van de classificatie van de data die benaderd wordt casu quo zou kunnen worden met dit draadloze netwerk. Deze classificatie kan bepaald zijn aan de hand van specifieke wet- en regelgeving, zoals de Wet bescherming persoonsgegevens (Wbp)[4], de Telecommunicatiewet[5], de Wet bescherming staatsgeheimen[6] en het Voorschrift Informatiebeveiliging Rijksdienst (VIR)[7]. Hoe hoger de classificatie van verwerkte informatie, hoe eerder een organisatie zal besluiten draadloze netwerken volledig te verbieden.

Op basis van de resultaten van de risicoanalyse kan een onderbouwde keuze worden gemaakt of wifi geschikt is voor de organisatie en of de voordelen opwegen tegen de nadelen (risico's, kosten et cetera).

Vervolgens dient een organisatie op basis van de risicoanalyse een wifibeleid te bepalen. Op basis van dit beleid kan vervolgens worden besloten welk wifiscenario wordt gehanteerd. Hiervoor moet een antwoord worden geformuleerd op onder meer de volgende vragen:

- Wat is het hoogste vertrouwelijkheidsniveau waarvoor het gebruik van mobiele apparaten in combinatie met draadloze communicatie wordt toegestaan en mogelijk gemaakt?
- Welke gebruikersgroepen worden (zowel in- als extern) onderkend en welke faciliteiten wil men deze groepen bieden met draadloze communicatie?
- Met welke mobiele apparaten wordt toegang tot het wifinetwerk toegestaan? Betreft dit alleen apparaten die door de eigen organisatie worden beheerd of ook een apparaat dat de gebruiker zelf meeneemt (BYOD)?
- Hoe wil de organisatie omgaan met het afdwingen van bepaalde regels voor het gebruik van mobiele apparaten via wifinetwerken?

3.3 Architectuurontwerp

Als besloten is op welke wijze wifi in de ICT-infrastructuur van de organisatie wordt opgenomen, moet de juiste balans worden gevonden tussen beveiliging en gebruik. Een gedegen architectuurontwerp is noodzakelijk om het keuzeproces te ondersteunen, onderbouwen en borgen. Op basis van het architectuurontwerp wordt het detailontwerp gemaakt en wordt de implementatie van het wifinetwerk gerealiseerd.

Zoals hiervoor is benoemd, vereist de beveiliging van een wifinetwerk een combinatie van organisatorische, procedurele, fysieke en technische maatregelen. Bij het opzetten van een architectuur voor wifi kan worden uitgegaan van bestaande principes, best practices en standaarden welke deze vier soorten maatregelen verenigen.

4 http://wetten.overheid.nl/BWBR0011468/
5 http://wetten.overheid.nl/BWBR0009950/
6 http://wetten.overheid.nl/BWBR0002074/
7 http://wetten.overheid.nl/BWBR0022141/

Denk aan:

- Pas het 'security by design' principe toe, security is hierbij integraal onderdeel van het ontwerp van het wifinetwerk.
- Maak gebruik van erkende en bewezen (open) standaarden, zoals de 802.11x standaard[8] voor authenticatie.
- Beveilig naast het netwerk, ook de clients, zowel voor de instellingen als voor de gegevens die er mogelijk op worden verwerkt en opgeslagen. Houdt er rekening mee dat gebruikers zelf aangeschafte apparatuur (willen) gebruiken in hun werkomgeving.
- Fysieke beveiliging van netwerkcomponenten moet onderdeel zijn van de architectuur.
- Maak, zeker bij een grote organisatie, gebruik van apparatuur en software voor grootschalig zakelijk gebruik. Dit zorgt voor veilige, schaalbare en beheersbare oplossingen in een complexe infrastructuur.
- Implementeer naast preventieve maatregelen ook maatregelen die gericht zijn op detectie van inbraken op het wifinetwerk, zoals Wireless Intrusion Detection systemen (WIDS).

De onderwerpen die onderdeel moeten zijn van het architectuurontwerp zijn beschreven in hoofdstuk 4.

3.4 Implementatie

De implementatie van een wifinetwerk kent voor de beveiliging specifieke aandachtspunten. Zowel bij een nieuwe implementatie als bij een migratie moeten onderstaande zaken worden bereikt.

- Het beleid rond het gebruik en de beveiliging van het wifinetwerk is beschreven, vastgesteld en wordt uitgedragen naar de organisatie en gasten/leveranciers. Gebruikers worden bijvoorbeeld via opleidingen bewust gemaakt van de beveiligingsaspecten van draadloos werken met mobiele apparaten.
- De implementatie van beveiliging omvat de vier belangrijkste onderdelen van een wifi-infrastructuur: het wifinetwerk, de mobiele apparaten, de eventuele koppeling met internet en de eventuele koppeling met het interne bedrijfsnetwerk.
- Een geaccordeerde en werkende governancestructuur voor de wifi-dienstverlening is ingericht. Denk aan zaken zoals eenduidig belegd eigenaarschap, (escalatie)procedures voor het afhandelen van veiligheidsincidenten en Service Level Agreements (SLA's) met leveranciers inclusief organisatie van de aansturing van deze leveranciers.
- De faciliteiten voor adequaat beheer van de wifi-infrastructuur zijn ingericht en de beheerders zijn opgeleid om hiermee te werken.

In de hoofdstukken 4 en 5 worden de inhoudelijke details van de implementatie verder uitgewerkt.

3.5 Beheer & onderhoud

Het beheer en onderhoud vormen een belangrijke factor in de betrouwbaarheid van een wifinetwerk. Het beheer en onderhoud moeten ervoor zorgen dat de maatregelen goed blijven functioneren. Specifiek voor het wifinetwerk betreft dit onder meer de onderstaande zaken, waarbij onderscheid wordt gemaakt tussen activiteiten die bij het dagelijks beheer horen (de continue activiteiten) en activiteiten die periodiek moeten worden uitgevoerd.

Continue activiteiten:

- Onderzoek reguliere meldingen van incidenten en problemen bij zaken die te maken hebben met of van invloed zijn op de beveiliging van het wifinetwerk.
- Controleer de logging van de (wifi)netwerkapparatuur periodiek om pogingen tot misbruik te herkennen en waar nodig maatregelen te treffen. Sluit deze bij voorkeur aan op bestaande Security Information and Event Management (SIEM)[9]-oplossingen. Correleer deze logging tevens met de logging van andere ICT-componenten (netwerkcomponenten, servers en applicaties et cetera) zodat tussen de verschillende logs verbanden kunnen worden gelegd.
- Controleer de integriteit van het wifinetwerk. De configuratie van de eigen accesspoints moet bijvoorbeeld conform afspraken zijn en er mogen geen nep/illegale toegangspunten (rogue accesspoint) op het netwerk zijn aangesloten.

Periodieke activiteiten:

- Evalueer de beveiligingsmechanismen die worden gebruikt op hun effectiviteit. Dit betreft bijvoorbeeld een controle op de voor de versleuteling van het draadloze netwerkverkeer gebruikte standaarden.
- Controleer of de lijst met geautoriseerde gebruikers overeenkomt met de lijst gebruikers die daadwerkelijk toegang heeft tot het wifinetwerk.
- Laat gerichte testen (zogenaamde penetratietesten[10]) uitvoeren op het wifinetwerk om gaten in de beveiliging te ontdekken en te repareren.
- Controleer de dekking van het wifinetwerk. Deze moet ruim genoeg zijn om gebruikers goedwerkende toegang te verlenen, maar tegelijkertijd niet té uitgebreid zijn om kwaadwillenden buiten de deur te houden.

De omvang van de beheerwerkzaamheden wordt in belangrijke mate bepaald door de fysieke omvang van het wifinetwerk, de doelgroepen die worden onderscheiden en het niveau van beveiliging dat is vereist. Het niveau van beveiliging vertaalt zich in specifieke maatregelen die van invloed zijn op de beheerlast. Bij een

8 802.1X is een IEEE beveiligingsstandaard voor poortgebaseerde authenticatie (port-based Network Access Control (PNAC)) op laag 2 van het Open Systems Interconnection (OSI)-model. De authenticatie vindt plaats nog voor de gebruiker toegang krijgt tot het netwerk. Dit heeft als voordeel dat er op basis van de authenticatie een verschillende laag 2 toegekend kan worden en er zo een policy toegelegd kan worden op het type gebruiker. Dit alles kan - afhankelijk van de gebruikte hardware - zowel bekabelde Ethernet-netwerken en draadloze 802.11-netwerken. (http://www.ieee802.org/1/pages/802.1x-2010.html)

9 Security Information and Event Management (SIEM) systemen bieden real-time-analyse van securitywaarschuwingen gegenereerd door bijvoorbeeld netwerksystemen, hardware of applicaties. SIEM-oplossingen verzamelen encorreleren meldingen en worden gebruikt om beveiligingsgegevens te loggen en rapporten te genereren voor onder meer het afleggen van verantwoording.

10 Zie voor meer informatie met betrekking tot penetratietesten het NCSC whitepaper 'Penetratietesten – doe je zo' (https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/pentesten-doe-je-zo.html)

hoog beveiligingsniveau wordt bij de periodieke activiteiten bijvoorbeeld een hogere frequentie aangehouden dan bij een lager beveiligingsniveau.

Het beheer van de beveiligingsaspecten kan in grote mate worden ondersteund met geautomatiseerde hulpmiddelen. Denk bijvoorbeeld aan hulpmiddelen die het wifinetwerk continu controleren op inbraakpogingen, zoals een WIDS. Dit vereist op zijn beurt een hoger kennis- en ervaringsniveau van de beheerders.

Details van de zaken die onderdeel moeten zijn van het beheer komen in de volgende hoofdstukken aan de orde.

3.6 Ontmanteling

Ook bij een ontmanteling van het netwerk moet rekening worden gehouden met zaken die specifiek zijn voor wifi. Denk daarbij tenminste aan de onderstaande zaken.

- Informeren van gebruikers dat het wifinetwerk niet (meer) actief zal zijn, om te voorkomen dat zij slachtoffer worden van een nep wifinetwerk.
- Het wissen van netwerkapparatuur, zoals de accesspoints, om te voorkomen dat instellingen (configuratie, wachtwoorden, logs et cetera) in verkeerde handen vallen.
- Het opheffen (onklaar maken) van de koppelingen waarmee het wifinetwerk met het internet en eventueel het bedrijfsnetwerk was verbonden.

Ongeacht de wijze waarop het wifinetwerk wordt voortgezet – vervanging of afbouw – zijn maatregelen noodzakelijk voor een goede beveiliging. Zie hiervoor het volgende hoofdstuk.

4 Scenario's voor wifi-gebruik

In de voorgaande hoofdstukken is wifi geïntroduceerd en is een aanpak beschreven voor de implementatie van een wifi-infrastructuur. Dit hoofdstuk beschrijft drie verschillende scenario's waaruit een organisatie kan kiezen voor de implementatie van wifi. De drie scenario's zijn:

1. **Open wifi:**
   wifi vrijgeven aan iedereen, ondersteund door een (minimale) set maatregelen.
2. **Geen wifi:**
   Totaal verbod van wifi. De nadruk ligt hierbij op handhaving van het verbod.
3. **Gecontroleerd wifi:**
   wifi aanbieden op basis van doelgroepen en/of een selectie van applicaties.

Scenario's 1 en 2 zijn de twee uiterste scenario's. Scenario 3 kent de meeste ruimte in de uitvoering, van een heel restrictief beleid tot een veel ruimer beleid ten aanzien van de doelgroepen waarvoor wifi wordt aangeboden en het type applicaties dat benaderd kan worden met een draadloze verbinding.

4.1 Scenario 1 – Open wifi

Bij dit scenario wordt ervan uitgegaan dat alle doelgroepen vrij gebruik mogen maken van het wifinetwerk. In de regel wordt dit slechts toegepast wanneer er alleen toegang wordt verleend tot openbare (bedrijfs)informatie. Ook bij dit scenario moeten echter maatregelen worden genomen om de betrouwbaarheid van de informatievoorziening te garanderen.

Denk aan de volgende maatregelen bij gebruik van open wifi:

- Voorkom dat vanaf het wifinetwerk toegang mogelijk is tot de vertrouwelijke bedrijfsinformatie. Dit kan bijvoorbeeld door:
  1. het wifinetwerk niet aan het bedrijfsnetwerk te koppelen;
  2. wanneer er wel een koppeling nodig is, deze afdoende te beveiligen tegen inbraak vanaf het wifinetwerk;
  3. de vertrouwelijke gegevens zelf goed te beveiligen tegen inzage of wijziging, bijvoorbeeld met versleuteling.

- Informeer gebruikers (bijvoorbeeld door middel van een startscherm) dat zij voor eigen risico gebruik maken van het wifinetwerk en aansprakelijk zijn voor hun eigen gedragingen op het wifinetwerk en het aangesloten internet.
- Voorkomen dat rogue accesspoints op het netwerk worden aangesloten. Deze controle kan door middel van visuele inspectie gebeuren of met elektronische middelen zoals een WIDS en netwerk toegangscontrole (zie paragraaf 6.4.6).

Hou er rekening mee dat ook in het geval er geen gevoelige informatie benaderbaar is via het wifinetwerk, er nog steeds beveiligingsrisico's bestaan. Dat betreft het onbereikbaar maken van het wifinetwerk of het misbruik van het wifinetwerk voor oneigenlijke of strafbare activiteiten.

4.2 Scenario 2 – Geen wifi

Een verbod op het gebruik van wifi zal in de meeste gevallen voortkomen uit hoge eisen die worden gesteld aan de vertrouwelijkheid van gegevens binnen een organisatie. Het voorkomen van de ontsluiting van gegevens via wifi heeft vooral te maken met reguleren en handhaven. Binnen de eigen muren is handhaving mogelijk, daarbuiten is dat slechts in beperkte mate het geval.

Het beleid moet daarom gericht zijn op het onmogelijk maken van het draadloos verbinden met het bedrijfsnetwerk zodat wordt voorkomen dat data buiten de muren van de organisatie gebruikt kan worden via draadloze verbindingen. Dit voorkomt tevens dat deze data verwerkt kan worden op mobiele gegevensdragers die de mogelijkheid hebben draadloos te communiceren. Denk daarbij aan data op laptops, tablets, smartphones et cetera.

Handhaving van het beleid heeft vooral te maken met:

- Voorkomen dat rogue accesspoints op het bedrijfsnetwerk worden aangesloten zodat het bedrijfsnetwerk alsnog wordt voorzien van draadloze toegang. Deze controle kan door middel van visuele inspectie gebeuren of met elektronische middelen zoals een WIDS.
- Indien een rogue accesspoint mogelijk gebruikt wordt voor bedrijfsspionage, is het verstandig hier aangifte van te doen bij de politie en een forensisch expert in te schakelen.
- Medewerkers bewust maken van het beleid en wat van hen wordt verwacht om dit te ondersteunen. Zij moeten bekend zijn met de risico's, beperkingen, sancties et cetera.
- De mogelijkheid voor gebruikers om van het beleid afwijkende zaken te melden.
- De wifi mogelijkheden van mobiele apparaten beperken dan wel uitschakelen zodat de risico's worden beperkt. In het uiterste geval wordt apparatuur met wifi verboden en alleen apparatuur zonder wifi-aansluiting aangeschaft. Het gebruik van door gebruikers meegenomen apparatuur (BYOD) met gebruik van wifi wordt niet toegestaan.

Om op afstand werken wel mogelijk te maken kan de organisatie toegang via bijvoorbeeld UMTS wel toestaan.

4.3 Scenario 3 – Gecontroleerd wifi

Voor het gecontroleerd beschikbaar stellen van wifi kunnen verschillende varianten worden onderkend, die van invloed zijn op de inrichting van het wifinetwerk.

Daarbij dienen onderstaande vragen te worden beantwoord:

1. Voor welke doelgroepen is het wifinetwerk beschikbaar? Is het wifinetwerk alleen toegankelijk voor eigen medewerkers of ook voor bezoekers, leveranciers, onbekenden et cetera? Het gaat hierbij om het onderscheid tussen vertrouwde en niet-vertrouwde personen. Een organisatie besluit zelf welke personen zij wil vertrouwen.
2. Met welke apparaten is het wifinetwerk bereikbaar? Is toegang tot het wifinetwerk alleen mogelijk met bedrijfsmiddelen of ook met apparatuur die de gebruiker zelf meeneemt volgens het BYOD-principe? Het gaat hierbij om het onderscheid tussen middelen die door de organisatie worden beheerd en middelen die niet door de organisatie worden beheerd.
3. Welke applicaties zijn via het wifinetwerk beschikbaar? Per doelgroep moet worden vastgesteld welke faciliteiten exact worden geboden. Is alleen internet beschikbaar of zijn ook de bedrijfsapplicaties toegankelijk? Vaak worden vier soorten toegang onderscheiden, te weten:
   a) Toegang tot internet
   b) Toegang tot internet en algemene informatie van de organisatie
   c) Toegang tot e-mail en agenda van de organisatie
   d) Toegang tot bedrijfsapplicaties

   Het gaat in hoofdlijn om het onderscheid tussen toegang tot openbare informatie en toegang tot bedrijfsinformatie: "*openbaar*" versus "*vertrouwelijk*". Bij vertrouwelijk kunnen verschillende classificatieniveaus worden onderscheiden. De overheid onderscheidt bijvoorbeeld *Departementaal VERTROUWELIJK* en drie categorieën staatsgeheim (Stg): *Stg. CONFIDENTIEEL*, *Stg. GEHEIM* en *Stg. ZEER GEHEIM* [7]. In welke "vertrouwensklasse" een soort toegang valt, is verschillend per organisatie. Een reële vraag is bijvoorbeeld: is de e-mail van onze organisatie openbaar, vertrouwelijk of zeer vertrouwelijk (geheim)?

Ieder van deze vragen heeft een substantiële invloed op de eisen die aan de beveiliging van het wifinetwerk worden gesteld. In het bijzonder de stap van alleen toegang verlenen tot het internet naar het verlenen van toegang tot (algemene) bedrijfsinformatie heeft aanzienlijke gevolgen voor de zwaarte van de maatregelen die moeten worden getroffen.

Het gaat hierbij niet alleen om de mate waarin (algemene) bedrijfsinformatie toegankelijk is, maar überhaupt of het wifinetwerk aan het bedrijfsnetwerk is gekoppeld en hoe de beveiliging van deze koppeling is ingericht.

Op basis van voornoemde vragen kunnen zes varianten worden onderscheiden voor de toegang tot informatie via een wifiverbinding. In tabel 4-1 zijn deze zes varianten met nummers aangegeven. Organisaties kunnen combinaties van varianten naast elkaar toepassen, bijvoorbeeld omdat je voor verschillende doelgroepen verschillende varianten hanteert.

Varianten voor toegang via wifi			
Doelgroep	**Middel**	**Toegang tot openbare informatie**	**Toegang tot vertrouwelijke informatie**
Vertrouwd	Beheerd	(1)	(2)
	Niet-beheerd	(3)	(4)
Niet-vertrouwd	Niet-Beheerd	(5)	(6)

Tabel 4-1 Varianten voor toegang via wifi

(1) Toegang tot openbare informatie via een wifiverbinding vanaf een door de organisatie beheerd apparaat zal in de meeste gevallen worden toegestaan. Denk aan iemand die met een bedrijfslaptop via een wifiverbinding toegang heeft tot het intranet van de organisatie.

(2) Toegang tot vertrouwelijke informatie via een wifiverbinding vanaf een door de organisatie beheerd apparaat kan worden toegestaan mits de juiste maatregelen worden getroffen, passende bij het vertrouwelijkheidsniveau van de informatie.

(3) Toegang tot openbare informatie vanaf een niet door de organisatie beheerd apparaat zal in de meeste gevallen worden toegestaan. Belangrijk aandachtspunt hierbij is of en hoe het wifinetwerk – vanuit het oogpunt van beveiliging – is gekoppeld aan het bedrijfsnetwerk. Denk aan iemand die met zijn eigen smartphone toegang heeft tot het intranet van de organisatie.

(4) Dit betreft toegang tot vertrouwelijke informatie vanaf een apparaat dat niet door de organisatie wordt beheerd. De vraag voor een organisatie is of deze variant – het benaderen van vertrouwelijke informatie op een niet-beheerd apparaat – wordt toegestaan. Dit zal niet zozeer een kwestie zijn bij informatie met een laag vertrouwelijkheidsniveau, maar zeker gelden bij informatie met een hoge eis aan de vertrouwelijkheid. Er kan sprake zijn van gradaties, bijvoorbeeld een situatie waarbij de gebruiker die een eigen apparaat meeneemt een zekere mate van centraal beheer moet toestaan. Zo kan (technisch) worden afgedwongen dat een zelf aangeschaft apparaat van een wachtwoord moet zijn voorzien om toegang tot bedrijfsmail te hebben.

(5) Toegang tot openbare informatie vanaf een niet door de organisatie beheerd apparaat zal in de meeste gevallen worden toegestaan. Denk aan een bezoeker of leverancier die in de gebouwen van de organisatie via een wifiverbinding toegang heeft om het internet te benaderen en zijn eigen bedrijfsmail te lezen. Belangrijk aandachtspunt hierbij is of en hoe het betreffende wifinetwerk – vanuit het oogpunt van beveiliging – is gekoppeld aan het bedrijfsnetwerk.

(6) Dit betreft toegang tot vertrouwelijke informatie, door een niet vertrouwde persoon vanaf een niet door de organisatie beheerd apparaat. In de regel zal deze variant niet worden toegestaan. Wanneer een externe partij toegang tot vertrouwelijke informatie (lees: bedrijfsinformatie) krijgt, is immers een bepaalde mate van wederzijds vertrouwen nodig en komen varianten (2) en (4) automatisch in beeld.

Ieder van deze varianten moet met passende maatregelen worden beveiligd. Belangrijk is dat daarbij niet alleen de vertrouwelijkheid van informatie wordt belicht, maar dat aan alle drie de aspecten van informatiebeveiliging (beschikbaarheid, integriteit en vertrouwelijkheid) de juiste aandacht wordt besteed. Hierna zijn de aspecten beschreven die onderdeel moeten zijn van de beveiliging.
Achtereenvolgens komen aan de orde:

1. authenticatie van gebruikers (en apparaten);
2. versleuteling van de communicatie;
3. gegevens op en toegang tot het mobiele apparaat;
4. fysieke beveiliging;
5. koppeling tussen het wifinetwerk en het bedrijfsnetwerk;
6. de connectie met het juiste wifinetwerk;
7. detectie en preventie.

1. *Authenticatie van gebruikers (en apparaten)*

Alleen legitieme gebruikers en apparatuur mogen via het wifinetwerk communiceren. Het doel van (client-)authenticatie is het voorkomen van ongeautoriseerde toegang tot het wifinetwerk.

Hoe en met welke sterkte de authenticatie moet worden ingericht is vooral afhankelijk van het vertrouwelijkheidsniveau van de informatie die kan worden benaderd. Dit brengt in de regel met zich mee dat hogere eisen aan de authenticatie worden gesteld wanneer het wifinetwerk is aangesloten op een bedrijfsnetwerk.

In een bedrijfsomgeving is het, uit het oogpunt van gebruiksgemak en beheersbaarheid, wenselijk om voor de authenticatie van eigen medewerkers gebruik te maken van de al bestaande systemen voor authenticatie. Denk daarbij bijvoorbeeld aan een koppeling met het interne gebruikersbeheersysteem (bijv. Active Directory (AD), Lightweight Directory Access Protocol (LDAP) et cetera). Daarmee loopt de authenticatie (als het goed ingericht is) gelijk met de medewerkers die volgens de in- en uitdienstprocedure toegang mogen hebben.

De hiervoor beschreven varianten voor toegang tot wifi kunnen worden ingevuld zoals beschreven in tabel 4-2.
Er wordt hierbij vanuit gegaan dat varianten 4 (met hoge eisen aan de vertrouwelijkheid) en 6 (dat is de toegang tot vertrouwelijk informatie vanaf apparaten die niet in beheer zijn bij de organisatie) onwenselijk zijn.

In hoofdstuk 6 is detailinformatie over authenticatiemechanismen voor wifi opgenomen.

2. *Versleuteling van de communicatie*

Versleuteling van het draadloze netwerkverkeer moet voorkomen dat de informatie die over het wifinetwerk wordt verzonden kan worden afgeluisterd en gemanipuleerd. Bij de inrichting van de versleuteling moet van het volgende worden uitgegaan:

- Zet het mechanisme voor versleuteling zodanig op dat het past bij de doelgroepen en het vertrouwelijkheidsniveau van de verwerkte informatie.
- Maak gebruik van adequate methoden voor versleuteling en authenticatie, nu WPA2 met AES-encryptie (zie paragraaf 6.3.2 voor detailinformatie) omdat oudere methoden kwetsbaarheden bevatten.
- Maak binnen een bedrijfsomgeving gebruik van geautomatiseerde methoden voor wederzijdse authenticatie (conform het IEEE 802.1X-framework). Hierbij wordt een authenticatieserver gebruikt om tweezijdige authenticatie te realiseren. De authenticatieserver kan de gebruiker (via wachtwoorden of certificaten) en/of het systeem (via certificaten of MAC-adres) verifiëren.

Voor eigen (vertrouwde) medewerkers kan een geavanceerd mechanisme voor versleuteling worden ingericht, zonder dat het de medewerkers in het gebruik hoeft te belemmeren.

Voor (incidentele) bezoekers ligt dat anders. Er kan worden gekozen voor onversleutelde communicatie of het gebruik van een sleutel die (handmatig) wordt gedeeld. Een organisatie kan ook tijdelijk geldige privésleutels gebruiken. Omdat sprake is van geen tot

Tabel 4-2 Authenticatie van gebruikers (en apparaten) voor de verschillende varianten

Variant(en)	Invulling
Toegang door bekende personen tot openbare informatie (varianten 1 en 3)	Er is geen sterk authenticatiemechanisme vereist, maar het is wel wenselijk dat deze gekoppeld is aan de authenticatiesystemen in de bestaande infrastructuur.
Toegang door bekende personen tot vertrouwelijke informatie (variant 2)	Er moeten adequate versleutel- en authenticatiemiddelen worden ingezet. De gebruikersvriendelijkheid van de wifitoegang is belangrijk, maar staat niet op de eerste plaats.
Toegang door bekende personen die inloggen met eigen apparaten (variant 4)	lage eisen aan de vertrouwelijkheid. Er kan sprake zijn van gradaties, bijvoorbeeld een situatie waarbij de gebruiker die een eigen apparaat meeneemt een zekere mate van centraal beheer moet toestaan. Zo kan (technisch) worden afgedwongen dat een zelf aangeschaft apparaat van een wachtwoord moet zijn voorzien om toegang tot bedrijfsmail te hebben.
Toegang voor bezoekers die inloggen met eigen apparaten (variant 5)	Het wifinetwerk biedt in de regel minder functionaliteit en stelt daarom lagere eisen aan de beveiliging, maar moet wel eenvoudig te beheren en gebruiken zijn. De gemiddelde bezoeker moet immers in staat zijn om zonder hulp van de IT-afdeling gebruik van het wifinetwerk te maken. Enige vorm van authenticatie, een disclaimer en logging van het gebruik zijn dan het meest relevant om de gebruiker te wijzen op zijn verantwoordelijkheden bij het wifi gebruik.

beperkte beveiliging wordt aanbevolen om het wifinetwerk voor bezoekers af te scheiden van het wifinetwerk voor eigen medewerkers. Omdat over een onversleutelde of eenvoudig versleutelde verbinding wordt gewerkt zal een disclaimer moeten worden getoond die de bezoeker ervoor waarschuwt dat zijn/haar data potentieel kan worden afgeluisterd.

In alle gevallen is het (ook voor bezoekers) raadzaam om met behulp van een 'eigen' versleutelmechanisme (bijvoorbeeld een Virtual Private Network (VPN)) de `end to end' communicatie te beveiligen.

3. Gegevens op en toegang tot het mobiele apparaat

Gebruik van een wifinetwerk en mobiele apparaten betekent in veel gevallen dat op deze mobiele apparaten gegevens worden opgeslagen. Bij bedrijfsapparatuur zal dit primair bedrijfsgegevens betreffen en bij BYOD waarschijnlijk ook privégegevens van de gebruikers. Denk bij gegevens aan e-mail, contactgegevens, locatiegegevens (waar het mobiele apparaat is geweest), foto's, applicaties en mogelijk documenten.

Een uitgangspunt kan zijn dat het mobiele apparaat waar mogelijk zo is ingericht dat geen bedrijfsgegevens worden opgeslagen ('zero footprint'). indien zero footprint (nog) niet realiseerbaar is, of functioneel onwenselijk is, dient bij het beveiligen van gegevens op mobiele apparaten rekening te worden gehouden met onder meer de volgende zaken:

- De mate waarin beveiliging van gegevens op mobiele apparaten nodig is, is afhankelijk van het vertrouwelijkheidsniveau van de betreffende gegevens. Dit vertrouwelijkheidsniveau wordt bepaald door de eigenaar van de gegevens, dus de werkgever voor wat betreft bedrijfsgegevens of de eindgebruiker in het geval van privégegevens.
- De maatregelen zijn voor een groot deel gebonden aan het mobiele apparaat en daarom specifiek per soort apparaat, het merk en de versie van het besturingssysteem.
- In een bedrijfsomgeving kan gebruik worden gemaakt van een beheerde architectuur, waarbij de instellingen van mobiele apparaten centraal worden beheerd (Mobile Device Management – (MDM)).
- Bij BYOD is de privacy van de eigenaar een belangrijke factor. Wanneer een medewerker via zijn eigen apparaat toegang heeft tot bedrijfsgegevens (bijvoorbeeld e-mail) moeten goede afspraken worden gemaakt over maatregelen die op het apparaat moeten worden getroffen. Hiermee wordt voorkomen dat deze gegevens in de openbaarheid komen, bijvoorbeeld na diefstal van het apparaat. Zie hiervoor ook de whitepaper 'Consumerization en security' [8] en de 'Beveiligingsrichtlijnen voor mobiele apparaten' van het NCSC [9].

4. Fysieke beveiliging

De netwerkapparatuur van vaste netwerken is meestal opgesteld in beveiligde ruimten. De netwerkapparatuur van draadloze netwerken (de accesspoints) moet echter zodanig worden opgesteld dat het draadloze signaal zo min mogelijk wordt verstoord. Dit brengt risico's met zich mee omdat kwaadwillenden meer kans van slagen hebben wanneer zij fysieke toegang hebben tot een apparaat. Zorg er in het ontwerp voor dat de draadloze netwerkapparatuur niet (eenvoudig) fysiek toegankelijk is.

Ook voor mobiele apparaten die verbinden met het netwerk is fysieke beveiliging van belang. Het is belangrijk dat gebruikers zorgvuldig omgaan met mobiele apparaten waar bedrijfsgegevens op staan, temeer omdat voornoemde maatregelen (authenticatie en versleuteling) geen garantie geven dat gegevens niet kunnen worden uitgelezen door een kwaadwillende die een mobiel apparaat in handen heeft gekregen.

5. Koppeling tussen het wifinetwerk en het bedrijfsnetwerk

Zolang alleen toegang is vereist tot openbare informatie kan wellicht worden volstaan met een koppeling van het wifinetwerk aan het internet. Zodra toegang tot bedrijfsinformatie nodig is, moet het wifinetwerk aan het bedrijfsnetwerk worden gekoppeld. Gezien de risico's van een wifinetwerk brengt de koppeling aan het bedrijfsnetwerk extra eisen ten aanzien van de beveiliging met zich mee. Dit betreft zowel eisen aan het wifinetwerk zelf als eisen aan het koppelvlak.

Wanneer hoge eisen aan de vertrouwelijkheid van de informatie op het bedrijfsnetwerk worden gesteld is alleen variant 2 acceptabel, vertrouwde personen met beheerde apparatuur, alleen wanneer de eisen laag zijn komt variant 4, vertrouwde personen met onbeheerde apparatuur, in beeld.
Zodra een veilig beheerde omgeving wordt geïmplementeerd (app) op een niet beheerd apparaat van gebruikers zelf, is sprake van variant 2. Met behulp van deze implementatie wordt een scheiding aangebracht tussen het zakelijke gebruik en de privé gebruiksmogelijkheden van het apparaat. De bedrijfsgegevens zijn alleen te benaderen via deze veilig beheerde omgeving.

Bij beveiliging van het koppelvlak kan bijvoorbeeld worden gedacht aan een firewall om selectief netwerkverkeer door te laten, netwerkverkeer op virussen te scannen et cetera. Dit koppelvlak vraagt om gericht beheer en wellicht aanvullende systemen zoals een Intrusion Detection System (IDS).

6. De connectie met het juiste wifinetwerk

Belangrijk is dat de juiste medewerkers connectie hebben met het juiste netwerk: medewerkers met het bedrijfsnetwerk en bezoekers met het bezoekersnetwerk. Tegelijkertijd moet worden voorkomen dat ongewenste gebruikers eenvoudig toegang hebben tot een wifinetwerk. De reikwijdte (dekking) van het wifinetwerk moet dus zo goed mogelijk overeenstemmen met de plekken waar legitieme gebruikers toegang mogen krijgen. Voorbeelden zijn alleen het eigen gebouw bij bedrijven of juist de hele campus in het geval van een onderwijsinstelling. Fysieke wijzigingen kunnen invloed hebben op het bereik van een wifinetwerk, en het is daarom van belang om periodiek metingen uit te voeren ter controle.

Wanneer de ICT-afdeling alle ICT-middelen beheert en het wifinetwerk alleen voor medewerkers is bedoeld, kan de ICT-afdeling de

werkplekken en andere apparatuur van medewerkers zodanig configureren dat deze standaard een verbinding maken met het juiste wifinetwerk.

Maken bezoekers gebruik van het wifinetwerk dan worden de ICT-middelen normaal gesproken niet geconfigureerd door de ICT-afdeling. De bezoeker zal zijn eigen apparaat moeten instellen. De organisatie zal daarom duidelijk moeten maken welk wifinetwerk de bezoeker mag gebruiken. Dit kan bijvoorbeeld door de bezoeker een brief te geven met naam van het netwerk (Service Set Identifier (SSID)) erop, en het netwerk een dusdanige naam te geven dat direct duidelijk is dat dit het netwerk voor bezoekers is, of de bezoeker te 'verleiden' een bepaald wifinetwerk te gebruiken. Het verleiden kan door bijvoorbeeld één wifinetwerk zonder versleuteling aan te bieden waar de andere wifinetwerken wel van versleuteling zijn voorzien.

7. *Detectie en Preventie (van rogue accesspoints)*

Detectie en preventie moeten voorkomen dat rogue accesspoints op het bedrijfsnetwerk worden aangesloten. Dit gebeurt bijvoorbeeld door het actief controleren op rogue accesspoints die in het bedrijfsnetwerk zijn opgenomen. Deze controle kan door middel van visuele inspectie gebeuren of met elektronische middelen zoals een WIDS. Daarnaast kan ongeautoriseerde apparatuur worden geweerd door (fysiek) toegangsbeheer toe te passen.

Een Wireless Intrusion Prevention System (WIPS) biedt de mogelijkheid om 'inbrekers' te signaleren voordat deze zich toegang hebben verschaft tot een computersysteem en/of al diverse schadelijke handelingen hebben uitgevoerd. Deze functionaliteit kan een uitbreiding zijn op het bestaande Intrusion Prevention System (IPS) voor het vaste netwerk.

De toepassing van WIDS/WIPS is vooral belangrijk voor grote organisaties die te maken hebben met een complexe wifinetwerkinfrastructuur en het wifinetwerk gebruiken voor meer dan toegang tot openbare informatie. Een WIDS/WIPS kan een aanzienlijke investering zijn en vereist professioneel beheer om daadwerkelijk effectief te zijn. Om hieraan tegemoet te komen bieden bepaalde partijen dezelfde functionaliteit inmiddels als een Software as a Service (SaaS)-oplossing [10].

5 Risico's bij wifi-gebruik

Bij de inrichting van een wifinetwerk moeten we goed weten waartegen het netwerk moet worden beschermd. Dit hoofdstuk beschrijft daarom met welke actoren rekening moet worden gehouden, de dreigingen waar wifinetwerken aan blootstaan, op welke kwetsbaarheden deze zijn gericht en welke risico's deze met zich meebrengen.

Vervolgens wordt in hoofdstuk 6 een top tien van de meest belangrijke maatregelen benoemd evenals de best practices bij het aanbieden en het gebruik van een wifinetwerk.

5.1 Actoren en aanvalsscenario's

Een 'actor' is een rol die een partij speelt op het gebied van informatiebeveiliging. Actoren worden gekenmerkt door een bepaalde intentie en een bepaald profiel [11]. Voor iedere organisatie zullen de actoren die geïnteresseerd zijn om misbruik te maken het wifinetwerk verschillend zijn. Het is dus belangrijk dat een organisatie kiest tot op welk niveau men zich wil verdedigen. Kwetsbaarheden kunnen immers worden misbruikt door zowel relatief onschuldige actoren met weinig middelen[11] als actoren met veel middelen (staten[12] en interne actoren zoals medewerkers, ingehuurde krachten en ex-medewerkers).

Naast de middelen van een actor is specifiek voor wifi de manier waarop actoren misbruik kunnen maken van het wifinetwerk. Op hoofdlijnen kunnen de navolgende situaties worden onderkend.

- wifi leent zich voor aanvallen waarbij actoren zich richten op personen die een externe locatie bezoeken, bijvoorbeeld een vliegveld, restaurant of hotel.
- Een kwaadwillende kan binnen de gebouwen van een organisatie het wifinetwerk compromitteren, zowel fysiek als draadloos. Evident is dat de kwaadwillende hiervoor toegang tot deze gebouwen moet verkrijgen.
- Een wifinetwerk kan kwetsbaar zijn als het buiten de gebouwen van een organisatie toegankelijk is. Een actor kan dan draadloos toegang proberen te verkrijgen tot het wifinetwerk zonder fysiek toegang tot de gebouwen van de organisatie te hebben.

5.2 Kwetsbaarheden

De definitie van een kwetsbaarheid luidt:

Een 'kwetsbaarheid' is een eigenschap van een samenleving, organisatie of informatiesysteem (of een onderdeel daarvan) die die kan worden misbruikt voor ongewenste activiteiten.

De meest evidente kwetsbaarheden van draadloze netwerken zijn technisch van aard. Er zijn echter ook menselijke en organisatorische kwetsbaarheden te benoemen waarmee terdege rekening moet worden gehouden. Deze drie invalshoeken, technologisch, menselijk en organisatorisch, zijn opgenomen in tabel 5-1 en uitgewerkt in de volgende paragrafen.

Kwetsbaarheden wifi	
Technologisch	» Informatie kan worden onderschept en/of gemanipuleerd » Geen zekerheid of gebruikers/systemen zijn wie zij claimen te zijn » Misbruik wifinetwerk door toegang tot netwerkcomponenten » Inbreuk op vertrouwelijkheid van bedrijfsinformatie
Menselijk	» Gebrek aan beveiligingsbewustzijn bij gebruikers » Toegang tot bedrijfsdata en bedrijfsnetwerken door verlies/diefstal mobiel apparaat
Organisatorisch	» Ontbreken van beleid ten aanzien van wifi gebruik » Geen of onvoldoende controle op misbruik van wifinetwerk

Tabel 5-1 Kwetsbaarheden wifi

5.2.1 *Technologische kwetsbaarheden*

Informatie kan worden onderschept en/of gemanipuleerd

Een wifinetwerk is kwetsbaar wanneer geen of onvoldoende veilige versleuteling wordt gebruikt. Draadloze communicatie is van nature kwetsbaar voor onderschepping van de informatie die wordt uitgewisseld. Om te voorkomen dat data door ongewenste personen wordt gelezen, moet deze versleuteld worden uitgewisseld. Omdat versleutelmethoden in de loop van de tijd achterhaald raken, moet steeds een actuele standaard worden gekozen om het hoofd te bieden aan misbruik van kwetsbaarheden in deze achterhaalde methoden. Tevens moeten in een zakelijke omgeving methoden worden gebruikt die zijn toegespitst op zakelijk gebruik.

Geen zekerheid of gebruikers/systemen zijn wie zij claimen te zijn

Een wifinetwerk is kwetsbaar voor toegang door niet-geautoriseerde personen, zeker wanneer een onvoldoende veilig en beheersbaar authenticatiemechanisme wordt gebruikt. Omdat de gebruiker anders dan bij vaste netwerken niet fysiek op het bedrijfsnetwerk hoeft te zijn aangesloten, kan niet worden vertrouwd op de aanwezigheid van sociale controle en/of toegangscontrole tot een gebouw.

Misbruik wifinetwerk door toegang tot netwerkcomponenten

De kern van een wifinetwerk bestaat uit fysieke onderdelen, de zogenaamde accesspoints. Een accesspoint is (uitgaande van

11 Onder middelen vallen de capaciteiten en instrumenten waarover een actor beschikt of kan beschikken om een aanval uit te voeren.

12 Onder 'staten' verstaan we in dit verband actoren die onderdeel vormen van de overheid van een bepaald land

infrastructuurtype) enerzijds een zender/ontvanger waar mobiele apparaten mee communiceren en anderzijds een koppelpunt met het bedrade netwerk. Wanneer een ongeautoriseerde persoon fysiek toegang krijgt tot een accesspoint kan hij de configuratie van het apparaat zodanig wijzigen dat hij eenvoudiger controle kan krijgen over de draadloze verbindingen.

Inbreuk op vertrouwelijkheid van bedrijfsinformatie
Wanneer ongeautoriseerd toegang wordt verschaft tot een wifinetwerk bestaat de mogelijkheid dat deze niet-geautoriseerde personen toegang krijgen tot bedrijfsinformatie wanneer het wifinetwerk is gekoppeld aan het bedrijfsnetwerk. De beveiliging van het koppelvlak tussen het wifinetwerk en het bedrijfsnetwerk is dus van belang.

5.2.2 *Menselijke kwetsbaarheden*

Gebrek aan beveiligingsbewustzijn bij gebruikers
Het wifinetwerk is kwetsbaar voor misbruik wanneer gebruikers zich onvoldoende bewust zijn van de risico's en bijvoorbeeld niet zorgvuldig omgaan met authenticatiemiddelen of de toegang tot onvertrouwde wifinetwerken accepteren.

Toegang tot bedrijfsdata en bedrijfsnetwerken door verlies/diefstal mobiel apparaat
Los van mogelijke wifi-risico's staat het verlies of de diefstal van de mobiele apparaten of gegevensdrager zelf. Diefstal of verlies komt vaker voor en brengt zoals altijd risico's op het gebied van vertrouwelijkheid en privacy met zich mee. Wanneer een mobiel apparaat in handen is van een kwaadwillende, is het voor hem relatief eenvoudig om toegang tot de opgeslagen gegevens te verkrijgen of op afstand in te loggen op een bedrijfsnetwerk via de mogelijkheden die deze mobiele apparaten bieden. Indien de data zelf geen waarde heeft kan het bekendmaken van het in bezit hebben van die data (via de media) een bedrijf imagoschade berokkenen.

5.2.3 *Organisatorische kwetsbaarheden*

Ontbreken van beleid ten aanzien van wifigebruik
Een wifinetwerk is kwetsbaar voor misbruik wanneer duidelijke afspraken over de inrichting, het gebruik en het beheer ontbreken. Een organisatie moet een eenduidige richting kiezen ten aanzien van het gebruik van wifi: past het bij ons type organisatie, willen we gebruikers en bezoekers faciliteren of willen we het juist beperken? De inrichting van beveiligingsmaatregelen en de borging daarvan moet zijn gebaseerd op de gemaakte beleidskeuzes.

Geen of onvoldoende controle op misbruik van wifinetwerk
Een wifinetwerk kan op allerlei manieren worden aangevallen. Het netwerk is kwetsbaar wanneer onvoldoende aandacht wordt besteed aan het monitoren van de punten waarop het netwerk kwetsbaar is en kan worden misbruikt.

5.3 Dreigingen

De definitie van een dreiging luidt:

Een 'dreiging' is een ongewenste gebeurtenis die kan plaatsvinden. De dreiging kan zowel van buiten als van binnen komen. Een dreiging kan werkelijkheid worden als er een kwetsbaarheid is die door de dreiging kan worden misbruikt. Als de dreiging werkelijkheid wordt dan resulteert dit in schade aan waardevolle eigendommen en/of verstoring van waardevolle processen.

Hierna zijn de voor wifinetwerken meest relevante dreigingen beschreven, waarbij de focus ligt op technologie. De dreigingen zijn allen qua opzet en uitvoering verschillend, maar zijn uiteindelijk letterlijk gericht op de drie invalshoeken:
- het verkrijgen van ongeautoriseerde toegang tot informatie;
- het manipuleren van informatie;
- het verstoren van de beschikbaarheid van informatie.

Wardriving
Met vrij verkrijgbare software is het relatief eenvoudig om vast te stellen of er wifinetwerken in de buurt actief zijn, die niet of onvoldoende beveiligd zijn tegen ongeautoriseerd gebruik. Rondrijden met een laptop met wifi ondersteuning en de juiste software is voldoende om deze netwerken te vinden. Deze activiteit wordt *wardriving* genoemd. Na ontdekking van een onvoldoende beveiligd netwerk kan een actor pogen om in te breken op deze netwerken. Hiermee krijgt een actor niet alleen gratis toegang tot het internet, maar onder omstandigheden ook toegang tot het (bedrijfs)netwerk dat gebruikmaakt van deze internetverbinding. Potentieel kan een "wardriver" deze toegang misbruiken, enerzijds om informatie op het interne netwerk te manipuleren en anderzijds om illegale praktijken op het internet uit te voeren. De eigenaar van het wifinetwerk loopt dus potentieel aanzienlijke risico's.

Rogue accesspoint
Een rogue accesspoint is een nep/illegaal toegangspunt dat wordt toegevoegd aan een vast of draadloos netwerk. Het is een accesspoint dat niet door de eigen organisatie wordt beheerd en door kwaadwillenden wordt gebruikt om informatie van nietsvermoedende gebruikers te onderscheppen. Een rogue accesspoint kan ook (onopzettelijk) door een eigen medewerker worden geïmplementeerd, waardoor het bedrade netwerk van buitenaf toegankelijk wordt. Vormen van rogue accesspoints zijn bijvoorbeeld:
- Geplaatst door een medewerker om flexibeler te kunnen werken in en om het kantoor, zich daarbij al dan niet bewust zijnde van de risico's en het beleid ten aanzien van wifi.
- Geplaatst door kwaadwillenden die uit zijn op het bespioneren van de organisatie door gegevens te manipuleren. Deze accesspoints zullen goed verstopt zijn en niet bekend worden als er niet actief naar wordt gezocht.
- Rogue accespoints kunnen zowel binnen de kantooromgeving als daarbuiten voorkomen, zoals vliegvelden, hotels en conferenties.
- Er kan een accesspoint worden geplaatst om bijvoorbeeld een ruimte van tijdelijke netwerkaansluitpunten te voorzien. Een

speciale vergadering, een project, een demoruimte of een testruimte zijn vaak de aanleiding om daartoe een netwerk aan te leggen gebruikmakend van wifi. Wanneer de netwerkbeheerder niet is betrokken, is sprake van een rogue accesspoint.
- Een accesspoint dat door een aanvaller is overgenomen. Wanneer een accesspoint fysiek te benaderen is, kan dit gereset worden naar de fabrieksinstellingen. De inbreker kan dit vervolgens naar believen configureren.
- Verschillende soorten apparatuur met een wifi-interface kunnen ingezet worden als accesspoint, bijvoorbeeld laptops of smartphones.
- Een rogue accesspoint dat niet op het bedrijfsnetwerk is aangesloten, maar door de eigen medewerkers als legitiem wordt gezien omdat het zich presenteert met de naam van het bedrijfsnetwerk. Hiermee kan een Man-in-the-Middle-aanval (MitM) worden uitgevoerd.

Spoofen van MAC-adressen

Een MAC-adres (Media Access Control) is een hardware-adres dat elke computer en elk mobiel apparaat met een bedrade of draadloze netwerkaansluiting uniek identificeert. Bij MAC-spoofing neemt een aanvaller het MAC-adres van een legitieme gebruiker over. Dit is voornamelijk van belang als het accesspoint alleen bepaalde MAC-adressen toestaat op het netwerk (MAC-adresfiltering). Als MAC-adresfiltering de enige beveiligingsmaatregel is die het accesspoint toepast, kan door middel van MAC-spoofing eenvoudig netwerktoegang verkregen worden.
MAC-spoofing (het nadoen van het MAC-adres) begint met het meeluisteren op een wifiverbinding om het MAC-adres van de geautoriseerde gebruiker te achterhalen. Dit MAC-adres heeft men nodig als het accesspoint gebruikmaakt van MAC-adresfiltering. Alleen geautoriseerde clients staan in de ACL (Access Control List) van het accesspoint en alle andere clients die niet in deze lijst voorkomen krijgen geen toegang tot het accesspoint. In de praktijk is het eenvoudig om een MAC-adres te manipuleren.
Na het succesvol uitvoeren van deze aanval is de aanvaller in staat om "legitiem" toegang te krijgen tot het wifinetwerk en is hij daarmee een bedreiging voor beschikbaarheid, integriteit en vertrouwelijkheid van de gehele informatievoorziening op de betreffende infrastructuur.

Besmetting mobiele apparaten

Mobiele apparaten kunnen ook geïnfecteerd worden met schadelijke content of malware. Naast de beveiliging van communicatie via wifi en de toegang tot wifinetwerken moet daarom ook rekening worden gehouden met de risico's van de communicatie op zich. Via een rogue accesspoint kan bijvoorbeeld malware worden verspreid of door content in de browsercache van een telefoon te plaatsen kunnen ongewenst acties worden uitgevoerd.

Naburige wifinetwerken

Het kan voorkomen dat een mobiel apparaat verbinding maakt met een naburig onbeschermd netwerk dat geen onderdeel uitmaakt of uit zou mogen maken van het wifinetwerk waarop automatisch een connectie mee kan worden gemaakt.

In de wifi-standaard wordt altijd met het accesspoint verbonden dat het sterkste signaal uitzendt als er geen bekend accesspoint in de buurt is. Niemand hoeft dat in de gaten te hebben, het kan helemaal automatisch gaan zonder een enkele waarschuwing.

Indien het een laptop betreft en deze een onbeveiligde (zonder wachtwoord) gedeelde map (share) open heeft staan, kunnen alle computers die aangesloten zijn op dat naburige netwerk meekijken op de harde schijf van die computer. Zelfs met een versleutelde harde schijf is het soms mogelijk om de data te benaderen, want het besturingssysteem is al operationeel en de encryptiesleutel is al ingevoerd.

Op deze manier is het onbewust weglekken (datalek) een groot risico dat niet onderschat mag worden, temeer omdat de eigenaar van de data helemaal niets in de gaten hoeft te hebben.

Ongeautoriseerde toegang

Een algemene dreiging is dat een ongeautoriseerde client netwerktoegang krijgt. Daarmee wordt het bijvoorbeeld mogelijk om het interne netwerk aan te vallen, of om misbruik te maken van een internetverbinding.

Gasten of kwaadwillenden kunnen het wifinetwerk misbruiken voor het downloaden van illegale content of het versturen van spam. De organisatie die de wifiverbinding beschikbaar stelt kan hier vervolgens op worden aangesproken. Bij misbruik kan ook gedacht worden aan het onevenredig gebruiken van de beschikbare internetbandbreedte.

Netwerkaanvallen naar de client

Wanneer een client een draadloze netwerkverbinding opzet, wordt het mogelijk om deze client via het netwerk aan te vallen. Voorbeelden zijn een Denial-of-Service (DoS) aanval die de volledige processorkracht van een laptop verbruikt, of dat al het geheugen in beslag wordt genomen. In het ergste geval maakt de aanvaller misbruik van een kwetsbaarheid in een programma dat luistert naar netwerkverkeer, om zo volledige toegang tot het systeem te krijgen.

Berichtinjectie

Voor aanvallers kan het interessant zijn om (netwerk-)berichten te maken of te wijzigen. Doel kan bijvoorbeeld zijn om netwerkroutering aan te passen voor een MitM-aanval. In een berichtinjectieaanval kan een hacker gebruikmaken van accesspoints om netwerkcommando's het bedrade netwerk achter het accesspoint in te sturen. De hacker injecteert bijvoorbeeld commando's om het netwerk opnieuw te configureren die routers, switches en intelligente hubs kunnen beïnvloeden. Op deze manier kan een compleet netwerk onbeschikbaar worden waarna dit opnieuw moet worden opgestart. Het kan zelfs betekenen dat alle intelligente netwerkonderdelen opnieuw geprogrammeerd moeten worden.

Aanpassen van berichten

Message modification (het aanpassen van berichten) werkt met behulp van een MitM-aanval. Een nietsvermoedende gebruiker

denkt in te loggen op het wifinetwerk, maar in werkelijkheid wordt via een rogue accesspoint ingelogd. Nadat de verbinding met dit rogue accesspoint is gemaakt, wordt de verbinding doorgezet naar het echte netwerk, maar nu zit er een station tussen die al het netwerkverkeer voorbij ziet komen, maar ook kan manipuleren, tegenhouden, veranderen, opslaan enzovoort. MitM-aanvallen worden mogelijk gemaakt door software als LANjack of AirJack, die deze vorm van hacking automatiseren en eenvoudig uitvoerbaar maken voor mensen die niet zoveel kennis hebben van het (ingewikkelde) protocol dat ervoor nodig is. Hotspots zijn hierbij de uitgelezen locatie om deze vorm van aanval uit te voeren, omdat er weinig of geen beveiliging is, wat het inbreken eenvoudig maakt.

Denial-of-Service

Een DoS-aanval vindt plaats als een aanvaller het wifinetwerk onbruikbaar maakt. Dat kan een aanvaller bijvoorbeeld doen door een bombardement van nepverzoeken te zenden naar een accesspoint. Het accesspoint is vervolgens niet meer in staat om te communiceren met andere stations en daarom is het draadloze netwerk niet meer beschikbaar. Deze methode kan door netwerkbeheerders ook worden gebruikt om rogue accesspoints te blokkeren. Er dient wel rekening gehouden te worden met het feit dat het uitvoeren van een DoS-aanval juridische consequenties kan hebben bijvoorbeeld als het een legitiem systeem is van een derde partij. Er zijn veel methoden waarop DoS-aanvallen kunnen worden uitgevoerd, en verschillende lagen in de protocol stack zijn kwetsbaar. Een protocol stack is een reeks bij elkaar horende lagen die het mogelijk maakt een bepaalde communicatie-architectuur te gebruiken, zoals het Open Systems Interconnection (OSI)-model[13]. Indien het handshake protocol tussen wificlient en accesspoint in de verkeerde volgorde of qua timing bewust verkeerd wordt uitgevoerd, kan de communicatie stilgelegd worden. Nog voordat de verbinding daadwerkelijk tot stand is gekomen verzendt de aanvaller al een bericht dat de connectie succesvol is verlopen of een bericht dat de connectie niet tot stand is gebracht. Door consequent de volgorde van verzenden van berichten (handshake) in de verkeerde volgorde of te snel of te langzaam te verzenden is het accesspoint continu bezig met het afwikkelen van al die verzoeken tot connectie zonder nog capaciteit over te houden voor de authentieke gebruikers. Gevolg: het accesspoint is onbereikbaar geworden, of het netwerk crasht volledig.

Tegen aanvallen op de fysieke laag, het radioverkeer, zijn geen goede maatregelen te nemen. De methode gaat uit van het storen van de zender door het uitzenden met een groot vermogen op dezelfde frequentie met een richtantenne naar het accesspoint om interferentie te veroorzaken. Deze methode valt onder de categorie grof geschut maar is wel effectief. Deze methode kan ook ongewild of onbewust ontstaan, vooral op de 2,45MHz band, omdat deze vrije band een veelgebruikte frequentie is voor Digital Enhanced Cordless Telecommunications (DECT)-telefoons[14], magnetrons en beveiligingsapparatuur.

Tools

Er zijn verschillende vrij verkrijgbare tools die door een aanvaller kunnen worden gebruikt om misbruik te maken van de kwetsbaarheden van wifi. Dit betekent dat ook mensen met beperkte kennis misbruik kunnen maken van wifi.
Deze tools kunnen uiteraard ook door netwerkbeheerders van het wifinetwerk worden ingezet om kwetsbaarheden te sporen.

Op het moment van schrijven van dit document zijn bekende tools bijvoorbeeld:

- Firesheep, op open wifinetwerken de inloggegevens van gebruikers achterhalen;
- Reaver, brute force attack op WPA(2) encrypted wifinetwerken;
- Kismet, passieve sniffer van wifinetwerken

13 http://nl.wikipedia.org/wiki/OSI-model
14 http://nl.wikipedia.org/wiki/Digital_Enhanced_Cordless_Telecommunications

6 Maatregelen om wifi te beveiligen

Dit hoofdstuk beschrijft twee zaken, ten eerste de belangrijkste maatregelen om wifi te beveiligen in de vorm van een top tien en ten tweede een basisniveau voor de beveiliging van wifi, gebaseerd op best practices.

6.1 Top tien maatregelen

Hieronder zijn de belangrijkste maatregelen beschreven die onderdeel moeten zijn van het raamwerk om wifi te beveiligen.

6.2 Best practices

In deze paragraaf zijn de belangrijkste technische maatregelen voor wifi nader beschreven op basis van best practices. Er wordt hierbij een onderscheid gemaakt tussen het aanbieden van wifi (accesspoint) (paragraaf 6.3, 6.4 en 6.5) en het afnemen van wifi (client) (paragraaf 6.6).

Maatregelen organisatie en mens

1. Zorg ervoor dat de basis van informatiebeveiliging op orde is. Zowel qua proces als technologie moet de beveiliging van de informatievoorziening op orde zijn om de risico's van draadloze communicatie te beperken.
2. Zorg voor een onderbouwde beleidskeuze voor de vorm waarin wifi wel of niet wordt toegestaan binnen de organisatie. Zorg ervoor dat deze beleidskeuze binnen de organisatie wordt gecommuniceerd.
3. Zorg ervoor dat de juridische risico's zijn onderzocht en afdoende zijn afgedekt. Zo is het verstandig om bij een open wifinetwerk, bijvoorbeeld voor bezoekers, iedere gebruiker expliciet akkoord te laten gaan met de verantwoordelijkheden die deze toegang met zich meebrengt.
4. Zorg er niet alleen voor dat de juiste technische en fysieke maatregelen zijn geïmplementeerd, maar zorg er ook voor dat het beheer daarvan goed is ingericht, inclusief de monitoring en controle op de goede en veilige werking.
5. Zorg ervoor dat gebruikers en beheerders zich bewust zijn van de risico's van draadloos en mobiel werken en welke eisen die risico's aan hun gedrag stellen. Denk daarbij ook aan leveranciers en bezoekers die toegang hebben tot een draadloos netwerk.

Maatregelen technisch

1. Zorg voor een architectuur voor het draadloze netwerk die past bij de organisatie. In alle gevallen moet de juiste afweging worden gemaakt tussen de maatregelen die nodig zijn om draadloos werken te beveiligen en de impact die dat heeft op de functionaliteit, het gemak en de flexibiliteit. Leidend hierbij zijn de eisen die aan de betrouwbaarheid van de informatievoorziening van de organisatie worden gesteld.
2. Zorg voor afdoende sterke methoden voor versleuteling en authenticatie, passend bij de organisatie. Versleuteling dient om gegevens tijdens opslag en transport te beveiligen en authenticatie dient om de toegang tot mobiele apparaten, netwerken en gegevens te beveiligen. Maak bij bedrijven/organisaties gebruik van producten voor zakelijk gebruik en zorg voor aansluiting op bestaande voorzieningen voor versleuteling en authenticatie.
3. Zorg voor passende fysieke beveiliging van de draadloze netwerkcomponenten (accesspoints et cetera) om te voorkomen dat kwaadwillenden eenvoudig toegang hebben tot de bedrijfsinfrastructuur.
4. Zorg voor passende beveiliging van mobiele apparaten. Denk aan een virusscanner op een laptop en hardening van een smartphone en tablet.
5. Tref aanvullende maatregelen op netwerkniveau wanneer de eisen aan de betrouwbaarheid van de informatievoorziening dat rechtvaardigen. Denk aan:
   - middelen voor aanvullende controle op netwerktoegang zoals Network Access Control (NAC) en Network Access Protection (NAP);
   - middelen voor het detecteren van inbraak, Wireless Intrusion Detection System (WIDS);
   - middelen voor het voorkomen van inbraak, Wireless Intrusion Prevention Systems (WIPS).

Maatregel	Beveiligingsniveau Laag	Midden	Hoog
aanbieden van wifi			
Scheiding van netwerken (zie paragraaf 6.3.1)	W	N	N
Sterke versleuteling en Authenticatie (zie paragraaf 6.3.2)	W	N	N
Detectie en preventie (zie paragraaf 6.4) **Wireless Intrusion Detection System (6.4.1)** **Wireless Intrusion Prevention System (6.4.2)**	O	W	N
Logging en monitoring (zie paragraaf 6.4.3)	W	W	N
SSID broadcasting beperken (zie paragraaf 6.4.4)	O	W	N
Signaaloptimalisatie (zie paragraaf 6.4.5)	O	W	N
Network Access Control (zie paragraaf 6.4.6)	O	W	N
Accesspoint fysiek beveiligen (zie paragraaf 6.5.1)	O	W	N
Accesspoint hardenen (zie paragraaf 6.5.2)	O	W	N
Accesspoint opnemen in processen (zie paragraaf 6.5.3)	W	N	N
afnemen van wifi			
Bewustzijn bij gebruikers (zie paragraaf 6.6.1)	N	N	N
Personal firewall gebruiken (zie paragraaf 6.6.2)	W	N	N
Met het juiste netwerk verbinden (zie paragraaf 6.6.3)	W	N	N
Clientcache / browsercache legen (zie paragraaf 6.6.4)	W	W	N
Shoulder surfing voorkomen (zie paragraaf 6.6.5)	W	W	N
Toepassen van VPN-verbinding (zie paragraaf 6.6.6)	W	W	N
wifi-adapter tijdelijk uitschakelen (zie paragraaf 6.6.7)	O	W	N

Legenda: O=optioneel, W=wenselijk, N=noodzakelijk

Tabel 6-1 Technische maatregelen

Tabel 6-1 geeft richting aan het belang van maatregelen door deze te koppelen aan een laag, midden en hoog beveiligingsniveau.

In de volgende paragrafen worden de verschillende maatregelen verder uitgewerkt.

6.3 Aanbieden wifi: Infrastructuur

6.3.1 Scheiding van netwerken

Het wifinetwerk moet, net zoals het internet, worden beschouwd als een onvertrouwd netwerk van waaruit aanvallen plaats kunnen vinden. Om het interne bedrijfsnetwerk hiertegen te beveiligen moeten deze netwerken van elkaar gescheiden zijn.

De navolgende vormen van scheiding kunnen worden toegepast:

Scheiding van gast-wifinetwerk en bedrijfs-wifinetwerk.

Om zeker te zijn dat ongeautoriseerde personen geen toegang krijgen tot het bedrijfsnetwerk kunnen twee gescheiden wifinetwerken worden aangeboden. Op deze manier maken gasten/leveranciers gebruik van het gast-wifinetwerk en maken de medewerkers gebruik van het bedrijfs-wifinetwerk.

Fysieke scheiding wifinetwerk en bedraad netwerk

Om zeker te zijn dat het wifinetwerk en het bedraad netwerk niet met elkaar verbonden zijn, dienen beide netwerken een volledig fysiek gescheiden eigen implementatie te hebben. Beide netwerken hebben hun eigen switches, routers en bekabeling en het wifinetwerk daarnaast nog zijn accesspoints. Dit is een zekere oplossing om beide netwerken gescheiden te houden, maar omdat diverse netwerkcomponenten dubbel uitgevoerd moeten worden, is dit ook een dure oplossing. Deze aanpak is zeer effectief tegen misbruik.

Segmentering van het netwerk

Een variant op de fysieke scheiding van wifinetwerk en bedraad netwerk is een virtuele scheiding, bijvoorbeeld op basis van virtuele LAN's (VLAN's). Beide netwerken delen grotendeels hun fysieke componenten zoals switches en routers. Op logisch netwerkniveau worden VLAN's gedefinieerd waarmee feitelijk gescheiden netwerken worden gecreëerd. Een apart VLAN voor het wifinetwerk en een apart VLAN voor het bedrade netwerk levert twee logisch gescheiden netwerken die grotendeels gebruikmaken van dezelfde fysieke infrastructuur. Deze oplossing is goedkoper dan een volledige fysieke scheiding. Beheersmatig vereist deze oplossing meer kennis en introduceert daarmee een kans op fouten in de implementatie en operatie. Deze oplossing is minder veilig dan de strikte fysieke scheiding.

Beveiligd koppelvlak

Als er wel een koppeling nodig is tussen het wifinetwerk en het bedrijfsnetwerk, dan moet de onderlinge communicatie via een beveiligd koppelvlak verlopen.

De maatregelen die in dit beveiligd koppelvlak worden genomen zijn bijvoorbeeld:

- koppelvlak heeft een default deny policy;
- alleen geautoriseerd dataverkeer is toegestaan;
- alleen toegang geven tot bepaalde systemen;
- alleen toegang geven tot systemen via een proxy in het koppelvlak;
- netwerkverkeer wordt gescand op aanwezigheid van malware;
- netwerkverkeer wordt gescand op (netwerk gebaseerde) aanvallen;
- er worden geen gegevens, zoals IP-adressen en software versies, van het bedrijfsnetwerk vrijgegeven naar het (externe) wifinetwerk.
- alleen toegang geven tot een kopie van de informatie;
- informatie over de inkomende en uitgaande datastromen wordt gelogd en geanalyseerd door geautoriseerde personen.

De koppeling naar het internet zou ook via een beveiligd koppelvlak moeten lopen, in verband met aanvallen vanaf of naar het internet. Het bedrijf is in eerste instantie aansprakelijk voor internetaanvallen die zijn wifi-gebruikers uitvoeren; het is daarom verstandig om te zorgen dat ook uitgaande DoS-aanvallen, wormen, spam en dergelijke door het koppelvlak worden tegengehouden. Daarnaast is het raadzaam om het wifinetwerk te beschermen tegen vergelijkbare aanvallen die vanaf het internet op de werkplekken worden gericht.

6.3.2 *Sterke versleuteling en authenticatie*

Geïmplementeerde beveiligingsprotocollen moeten nu maar ook in de toekomst een adequate beveiliging blijven bieden. De onderliggende versleutelmethoden hebben in de regel een beperkte houdbaarheid omdat deze met de toenemende beschikbaarheid van rekenkracht worden gekraakt.

Afkorting	Omschrijving	Stand van zaken
WEP	Wired Equivalent Privacy	Onveilig
WPA-PSK (TKIP)	wifi Protected Access Personal/SOHO	Onveilig
WPA2-PSK (CCMP)	wifi Protected Access II Personal/SOHO	Beperkt veilig geacht
WPA-EAP (TKIP)	wifi Protected Access Enterprise	Kwetsbaar
WPA2-EAP (CCMP)	wifi Protected Access II Enterprise	Veilig geacht

Tabel 6-2 Versleutelmethoden

Tabel 6-2 geeft de huidige stand van zaken weer.

WEP (Wired Equivalent Privacy) was de eerste versleutelmethode die werd aangeboden voor wifi apparatuur. Het WEP-protocol maakt gebruik van RC4-versleuteling. Door een verkeerde implementatie van het RC4-algoritme, waarbij de zwakheden van RC4 niet worden omzeild, is de versleuteling kwetsbaar voor aanvallen berustend op statistische evaluatie van ontvangen pakketten. Door genoeg draadloos netwerkverkeer te verzamelen, kan de WEP-key worden bepaald. WEP is binnen 1 minuut te kraken en er is tegenwoordig praktisch geen netwerk verkeer meer nodig omdat je dit als aanvaller zelf kunt genereren. WEP is simpelweg geen veilige optie meer, ook niet voor thuisgebruikers.

WPA/WPA2 (wifi Protected Access) zijn beveiligingsstandaarden die als opvolgers van WEP zijn ontwikkeld. WPA is als een tijdelijke standaard geïntroduceerd om de problemen met WEP snel het hoofd te bieden. WPA kan RC4 of Advanced Encryption Standard (AES) als versleutelalgoritme gebruiken. WPA2 is de vernieuwde versie van WPA en maakt gebruik van het sterkere versleutelprotocol AES met CCMP (Counter-mode CBC MAC Protocol) als variant. Waar mogelijk dient WPA2 gekozen te worden.

WPA en WPA2 onderkennen ieder 2 modes: Enterprise en Personal. Beide voorzien in versleuteling en authenticatie.

- Personal/SOHO mode is bedoeld voor thuisgebruik of kleine omgevingen (Small Office Home Office) waar authenticatieservers niet voorhanden zijn. Er wordt een Pre-Shared key (PSK) gebruikt voor authenticatie.
- Enterprise mode is bedoeld voor (grotere) organisaties. Er wordt gebruikgemaakt van het 802.1x-authenticatieframework, het Extensible Authentication Protocol (EAP) en een authenticatie-server om tweezijdige authenticatie te realiseren. In deze context is het tevens belangrijk dat een koppeling met reeds bestaande authenticatiemiddelen (bijvoorbeeld gebruikersbeheersystemen zoals LDAP en Active Directory) wordt gelegd. Hiermee wordt het beheer vereenvoudigd.

Bij zowel Personal/SOHO mode als Enterprise mode zijn twee verschillende protocollen voor versleuteling in gebruik. WPA maakt gebruik van het TKIP/MIC-protocol (TKIP=Temporal Key Integrity Protocol. MIC = Message Integrity Check) en WPA2 maakt gebruik van het AES-CCMP protocol. De laatste wordt veiliger geacht. CCMP is een versleutelmechanisme dat veiliger is dan TKIP en sinds 2006 verplicht voor Wi-Fi-gecertificeerde apparaten door de Wi-Fi Alliance[15].

Veelgebruikte en sterke RADIUS-authenticatiemechanismen worden in tabel 6-3 weergegeven. RADIUS (Remote Authentication Dial In User Service) is een AAA (authenticatie, autorisatie en accounting) systeem. Het systeem wordt gebruikt om de identiteit van een gebruiker die toegang wenst tot een netwerk, te kunnen vaststellen.

	Clientauthenticatie	Serverauthenticatie
EAP-Transport Layer Security (EAP-TLS)	Certificaat	Certificaat
EAP-Tunneled Transport Layer Security (EAP-TTLS)	Naam/wachtwoord of certificaat	Certificaat
Protected Extensible Authentication Protocol (PEAP)	Naam/wachtwoord	Certificaat

Tabel 6-3 RADIUS-authenticatiemechanismen

Clientcertificaten zijn veilig omdat ze niet te raden zijn, maar de distributie vereist meer beheerinspanning dan bij gebruikersnamen en wachtwoorden. Het certificaat moet bijvoorbeeld op een systeem (softwarecertificaten) of op een smartcard worden geplaatst.

Een gebruikersnaam/wachtwoordcombinatie kan ook veilig zijn mits er een sterk wachtwoord wordt gekozen (minimaal acht tekens, niet gebaseerd op woorden, variatie in hoofd- en kleine letters, en met speciale karakters). Tevens is het van belang dat de gebruiker op een veilige manier met het wachtwoord omgaat en niet in de laatste plaats dat de uitgifte en het beheer van deze inloggegevens goed is geregeld.

6.4 Aanbieden wifi: Detectie en Preventie

Door configuratiefouten, handelingen van gebruikers of aanvallers kan het zijn dat de integriteit van het wifinetwerk gecompromitteerd wordt. Een accesspoint dat per ongeluk WEP gebruikt in plaats van WPA, een intern rogue accesspoint dat door een medewerker op het netwerk is aangesloten of een extern rogue accesspoint waarmee een aanvaller gebruikers probeert te lokken zijn hier voorbeelden van.

Door periodiek het wifinetwerk te analyseren/scannen kunnen deze problemen worden ontdekt. Belangrijke aandachtspunten hierbij zijn:

- Controleer of alle accesspoints nog functioneren;
- Controleer of de accesspoints niet (fysiek) zijn gemanipuleerd;
- Controleer of er rogue accesspoints zijn.

Wireless Intrusion Prevention Systems (WIPS) kunnen toegepast worden om automatisch rogue accesspoints te detecteren en blokkeren. Een WIPS kan ook verschillende aanvallen (zoals DoS-aanvallen en spoofing) herkennen, dit maakt het mogelijk om snel actie te ondernemen om een aanval te stoppen.

6.4.1 *Wireless Intrusion Detection System*

IDS staat voor Intrusion Detection System. Waar een firewall te vergelijken is met een solide voordeur met inbraakwerend hang- en sluitwerk, is een IDS te vergelijken met een inbraakalarm, als de voordeur toch niet heeft kunnen voorkomen dat een inbreker is binnengekomen.

WIDS staat voor Wireless Intrusion Detection System en is een uitbreiding van de bestaande IDS'en. Hiermee komen de volgende mogelijkheden binnen bereik:

- Identificatie van de fysieke locatie van alle draadloze apparatuur binnen het gebouw en de directe omgeving;
- Detectie van ongeautoriseerde peer-to-peercommunicatie (ad-hoc mode) binnen het draadloze netwerk die niet zichtbaar is binnen het bedrade netwerk;
- Analyse van draadloze communicatie en monitoring van de 802.11-frequentieband en het genereren van een alarm als ongeautoriseerde configuratiewijzigingen worden waargenomen;
- Detectie van rogue accesspoints met alarmeringsfunctie;
- Bepaalde implementaties kennen de mogelijkheid om een rogue accesspoint te bestrijden door middel van een DoS-aanval[16];
- Vroegtijdige detectie van DoS–aanvallen en pogingen tot injectie van netwerkverkeer;
- Een WIDS kan worden aangesloten op een correlatiesysteem. Een dergelijk systeem combineert realtime de uitvoer van de sensoren van bijvoorbeeld de firewalls, virusdetectiesystemen en IDS'en. Deze correlatiesystemen zijn in staat om geconsolideerde realtimerapportages te genereren.
- Verzorgen van gecentraliseerde monitoring en beheer van het wifinetwerk, met de mogelijkheid van integratie met het bestaande IDS voor monitoring en rapportage.

Een WIDS is een substantiële investering. Houdt er bovendien rekening mee dat de kosten zeker niet alleen gaan zitten in de aanschaf en implementatie van dergelijke systemen. Er zullen tevens goed opgeleide securityprofessionals moeten worden ingehuurd of opgeleid om deze systemen te bedienen, de alarmen te kunnen opvolgen en rapportages te kunnen beoordelen en te aggregeren naar hogere rapportageniveaus. Indien al gebruik wordt gemaakt van een IDS zal de stap naar een WIDS minder groot zijn.

15 http://www.wi-fi.org

16 Het uitvoeren van een DoS kan juridische consequenties hebben als het bijvoorbeeld een legitiem systeem is van een derde partij.

6.4.2 Wireless Intrusion Prevention System

IPS staat voor Intrusion Prevention System, WIPS staat voor Wireless IPS. Een WIPS is een systeem om inbrekers te detecteren voordat ze zich toegang hebben verschaft tot een computersysteem en/of al diverse schadelijke handelingen hebben uitgevoerd. Tevens kan een WIPS automatisch tegenmaatregelen nemen (preventie). Een WIPS dient als aanvulling op een IDS én als uitbreiding van een bestaand Intrusion Prevention Systeem, maar dan voor het draadloze netwerk.

6.4.3 Logging en monitoring

Het loggen en monitoren van gebeurtenissen biedt voordelen voor drie niveaus van bescherming tegen incidenten: preventie, detectie en respons.

Wanneer kwaadwillenden weten dat aanvallen worden opgemerkt heeft dit een afschrikkende werking. Als, door actief monitoren, een aanval wordt opgemerkt kan daar snel actie op worden ondernomen. Mocht de aanval pas later worden ontdekt, dan kan met behulp van de gelogde informatie wellicht de aard van de aanval worden achterhaald en kunnen daartegen passende maatregelen worden geïmplementeerd.

Voorbeelden van bronnen voor logging zijn systeem- en applicatie-logs en logs van netwerkverkeer. Het loggen van netwerkverkeer kan zich beperken tot informatie over de verbindingen en hoeft niet de inhoud van de pakketten te bewaren.

Juridische consequenties loggen en monitoren van netwerkverkeer[17].

Het loggen van netwerkverkeer loopt al heel snel tegen de Wet bescherming persoonsgegevens (Wbp) aan. Dit is immers gekoppeld aan IP- of MAC-adressen en dat zijn meestal persoonsgegevens (als ze gebruikt worden door een persoon). Hoofdregel is dat je "duidelijk" toestemming moet vragen, bijvoorbeeld door een melding bij het aanmeldscherm.

Als er niet om toestemming gevraagd kan worden en de privacyinbreuk gering is, mag zonder toestemming gewerkt worden. Op deze grond mogen bijvoorbeeld MAC-adressen worden gelogd voor beveiligingsdoeleinden. Beveiliging is een eigen dringende noodzaak en loggen van zulke gegevens is geen ernstige inbreuk op de privacy. Zorg dat in deze situatie zo terughoudend mogelijk wordt gewerkt. Werk zoveel mogelijk met automatische scripts in plaats van met handmatige controles door mensen. Er zijn programma's voor het realtime analyseren van logs, die een melding maken van (mogelijke) incidenten zonder dat een medewerker continu de loginformatie moet analyseren.

6.4.4 SSID broadcasting beperken

Binnen de 802.11–standaard voor wifi wordt de zogenaamde Service Set Identifier (SSID) gedefinieerd waarmee draadloze netwerken van elkaar worden onderscheiden en ieder netwerk een eigen naam heeft (het SSID). Het SSID is een identificatie in de vorm van een naam van minimaal een en maximaal 32 tekens. Om een wifinetwerk te herkennen door middel van een SSID, is het belangrijk dat bij het implementeren elk accesspoint dezelfde SSID bevat.

Veranderen van de SSID

De standaard ingestelde SSID die het accesspoint in de fabriek heeft gekregen moet worden veranderd. Er staan op het internet lijsten van merken accesspoints met hun bijbehorende standaardwaarde voor de SSID. Hackers kennen deze standaardwaardes en hebben eenvoudig toegang tot het netwerk wanneer er geen andere wijzigingen zijn gemaakt. Ook is het niet verstandig om in een SSID melding te maken van merk en versie van het accesspoint. Een beschrijvend SSID (bijvoorbeeld de naam van de organisatie) kan vanuit het oogpunt van gebruikersgemak echter zeer veel waarde hebben, ten opzichte van de marginale beveiligingswaarde van een niet-beschrijvend SSID

Er zijn daarnaast programma's die aanvallers gebruiken om een verborgen SSID te achterhalen. Deze maatregel verhoogt het beveiligingsniveau daarom maar beperkt.

Maximeren van het Beaconinterval

De 802.11-standaard specificeert het gebruik van "Beacon frames" om de SSID aan de omgeving te melden. De frequentie van het uitzenden van de SSID kan worden ingesteld. Indien het tijdsinterval zo hoog mogelijk wordt gezet (meestal iets van een minuut), dan wordt het iets lastiger voor een wardriver om het netwerk te spotten. Er zijn methodes die dit weten te omzeilen met actieve scanning waarbij niet hoeft te worden gewacht op het uitzenden van een SSID. Deze maatregel verhoogt het beveiligingsniveau maar beperkt.

Uitzetten van de Broadcast SSID-optie

Indien slechts gebruik wordt gemaakt van één accesspoint, dan heeft het uitzenden van de SSID geen meerwaarde omdat roaming niet van toepassing is. Roaming is het overdragen van een bestaande verbinding tussen een client en een accesspoint naar een ander accesspoint waar op dat moment de signaalsterkte groter is. Op deze manier wordt het dus mogelijk het netwerk in een heel gebouw dekkend te krijgen. Lopend door het gebouw blijft de verbinding in stand. Misbruik van deze netwerkverbinding wordt dan lastiger omdat gebruik moet worden gemaakt van passieve scanning om het bestaande netwerkverkeer te analyseren. Ook deze maatregel verhoogt het beveiligingsniveau beperkt.

6.4.5 Signaaloptimalisatie

Met signaaloptimalisatie wordt bedoeld dat het bereik van het draadloze signaal optimaal wordt afgestemd op de locatie van de gebruikers. Alleen op de gewenste locatie (bijvoorbeeld binnen een gebouw) is het draadloze netwerk beschikbaar en daarbuiten niet. Hiermee wordt voorkomen dat kwaadwillenden eenvoudig toegang tot het netwerk hebben. In de praktijk is dit niet exact te realiseren en is aandacht nodig bij wijzigingen zoals een verbouwing.

17 Bron: https://www.security.nl/artikel/44398/Juridische_vraag%3A_mag_ik_WiFi-verkeer_afluisteren%3F.html

Het regelmatig scannen van het bereik is belangrijk om enerzijds te ontdekken of er rogue accesspoints bij zijn gekomen en anderzijds omdat veranderde omstandigheden van de gebouwen een mogelijke ongewenste uitbreiding zouden kunnen veroorzaken van het dekkingsgebied. Een afgebroken bijgebouw, het plaatsen van grotere ramen of het verplaatsen van kasten kan al van veel invloed zijn op het bereik van het wifinetwerk.

Indien absoluut geen straling naar buiten mag komen zijn er speciale oplossingen die ervoor kunnen zorgen dat geen straling het gebouw kan verlaten.

6.4.6 Network Access Control

Een Network Access Control (NAC)–systeem biedt aanvullende controle over netwerktoegang. Op basis van de identiteit van de gebruiker en profielen wordt bepaald welke toegang een gebruiker krijgt. Verschillende leveranciers hebben NAC-systemen in hun netwerk- en serverproducten opgenomen.

Een specifieke vorm is MAC-adresfiltering. Een MAC-adres is een hardware-adres dat elke computer en elk mobiel apparaat op een unieke manier identificeert. Vrijwel elk accesspoint kent de mogelijkheid een ACL (Access Control List) te maken met alleen de MAC-adressen van apparaten die verbinding mogen maken. Indien een MAC-adres niet voorkomt in deze lijst, dan is het niet mogelijk verbinding te krijgen met het accesspoint. Het is echter relatief eenvoudig om door het spoofen van MAC-adressen toch toegang te krijgen. Belangrijk is daarnaast dat het actueel houden van een ACL extra beheerwerkzaamheden met zich meebrengt. Het filteren van MAC-adressen moet dan ook gezien worden als een maatregel die het beveiligingsniveau beperkt verhoogd.

6.5 Aanbieden wifi: Accesspoint

6.5.1 Accesspoint fysiek beveiligen

Vrijwel alle accesspoints zijn door middel van fysieke toegang te ‘resetten’ waarbij de fabrieksinstellingen worden hersteld. Een aanvaller kan hier misbruik van maken, om vervolgens het accesspoint naar wens te configureren tot een rogue accesspoint. Hoewel de prijs van een accesspoint daar geen directe aanleiding toe geeft, is ook diefstal een risico.

Om tegen deze dreigingen te beschermen moeten accesspoints fysiek beveiligd worden, bijvoorbeeld door het accesspoint niet zichtbaar te plaatsen maar boven een systeemplafond. Door ook te monitoren of er voortdurend verbinding is met alle accesspoints kan opgemerkt worden wanneer een accesspoint wordt gereset of verwijderd.

6.5.2 Hardenen van accesspoints

De fabrieksinstellingen van een accesspoint zijn meestal onvoldoende veilig, zeker omdat ze alom bekend zijn. Denk bijvoorbeeld aan een standaardsleutel die gebruikt wordt voor de versleuteling van het dataverkeer, maar ook een standaardwaarde voor gebruikersnaam en wachtwoord van de hoofdgebruiker et cetera. Het wijzigen van deze standaardinstellingen is belangrijk, omdat aanvallers uiteraard op de hoogte zijn van deze fabrieksinstellingen.

Met hardenen, of het veilig configureren van een accesspoint, kunnen verschillende aanvallen worden voorkomen. Deze maatregel is vooral gericht op de beheertoegang van het accesspoint. Voorbeelden van hardening zijn:

- het uitschakelen van Universal Plug & Play (UpnP);
- het veranderen van het standaardwachtwoord voor beheer;
- het beperken van toegang tot de beheerinterface tot het bedrade (beheer-)netwerk;
- alle overbodige functionaliteit uitschakelen;
- maak de firmware en drivers van uw accesspoints en draadloze netwerkkaarten onderdeel van de patchmanagementcyclus;
- maak de instellingen van uw accesspoints onderdeel van uw configuratiemanagement.

6.5.3 Accesspoint opnemen in processen

Een accesspoint is te vergelijken met een willekeurig ander computersysteem; het heeft bijvoorbeeld een configuratie en er verschijnen updates voor de besturingssoftware. Het is daarom goed om het accesspoint op te nemen in een aantal bedrijfsprocessen, zoals patch-, wijzigings- en configuratiemanagement.

Patchmanagement zorgt ervoor dat de accesspoints regelmatig worden voorzien van firmwareupdates. Het aantal kwetsbaarheden waar een aanvaller misbruik van zou kunnen maken wordt daarmee tot een minimum teruggebracht.

Met wijzigings- en configuratiemanagement is het mogelijk om snel de instellingen van een accesspoint te herstellen, omdat de instellingen en wijzigingen daarvan consequent zijn bijgehouden.

6.6 Afnemen wifi

Bij het afnemen van wifi gaat het om het nemen van maatregelen aan de zijde van de client (de gebruikerszijde).

6.6.1 Bewustzijn bij gebruikers

Technische beveiligingsmaatregelen staan nooit op zichzelf. Er zijn vrijwel altijd mensen bij betrokken die de techniek aanvullen, gebruiken, bedienen, monitoren en vervangen als de technische middelen het laten afweten. De mens zal in elk van deze gevallen getraind moeten zijn om naar behoren om te kunnen gaan met de betreffende techniek.

In het kader van wifinetwerken betekent dit dat een aantal partijen binnen een bedrijf bewust gemaakt dienen te worden van het feit dat zij omgaan met een wifinetwerk. Enerzijds betreft dit de beheerders die bijvoorbeeld de accesspoints instellen en detectie van rogue accesspoints uitvoeren. Zij dienen op de hoogte te zijn van de mogelijkheden van de techniek en hoe zij deze op zo veilig mogelijke wijze kunnen instellen en beheren.

Anderzijds betreft het de groep gebruikers binnen de organisatie die voorzien zijn van een laptop met wifi. Zij zullen zich er bewust van

moeten worden dat hun wifi-adapter zich met ieder willekeurig onversleuteld accesspoint kan verbinden. Zij lopen daarmee het risico vertrouwelijke data te versturen over een niet-vertrouwd en onversleuteld wifinetwerk. De gebruiker zal zich dus bewust moeten zijn van de gevaren die het gebruik van een zakelijke laptop op een wifinetwerk met zich mee brengt.

6.6.2 *Personal firewall gebruiken*

Op het moment dat een wifiverbinding wordt gemaakt, zijn systemen in staat om de client te benaderen en aan te vallen. Door een personal firewall te gebruiken (die alleen het noodzakelijke inkomende netwerkverkeer toestaat) wordt de client beveiligd tegen veel netwerkaanvallen.

De meeste netwerkaanvallen zijn gericht op poort 139 en 445, Windows gebruikt deze poorten voor toegang tot gedeelde mappen. Het is daarom belangrijk dat dit netwerkverkeer alleen voor de juiste IP-adressen wordt toegestaan.

6.6.3 *Met het juiste netwerk verbinden*

Bij het verbinden met een wifinetwerk is het belangrijk dat het netwerk met de juiste naam wordt geselecteerd. Als een ander netwerk wordt gekozen (een rogue accesspoint) is het mogelijk dat al het netwerkverkeer van en naar de client wordt afgeluisterd.

6.6.4 *Clientcache / browsercache legen*

Opdrachten die in de cache van een client of browser worden geplaatst kunnen ongewenste acties op een mobiel apparaat doen uitvoeren. Om dit te voorkomen kan ervoor worden gekozen om deze cache steeds te legen voordat deze ongewenste acties kunnen worden opgestart.

6.6.5 *Shoulder surfing voorkomen*

Het voordeel van wifi is dat computergebruik minder plaatsgebonden is. Zo wordt op veel plaatsen gratis internettoegang via wifi aangeboden. Het gevaar dat iemand op het scherm of toetsenbord meekijkt bij het invoeren van bijvoorbeeld wachtwoorden, is dan ook aanwezig. Houdt hier rekening mee; overweeg om een zogenaamd privacyscherm te gebruiken voor laptops.

6.6.6 *Toepassen van VPN-verbinding*

Naast de direct op wifi gerichte beveiligingen uit eerdere paragrafen kan ook voor een aanvullende aanpak gekozen worden. In dat geval wordt niet alleen het wifinetwerk beveiligd, maar wordt er een end-to-endbeveiliging tussen client en applicatie gerealiseerd.

Een VPN biedt bescherming tegen het afluisteren en manipuleren van netwerkverkeer doordat een versleutelde tunnel wordt opgezet tussen de client en de VPN-server. Het is daarom een geschikte beveiligingsmaatregel bij het gebruik van wifi in een onveilige of onvertrouwde omgeving.

Als bijvoorbeeld een bedrijfsapplicatie op het interne bedrijfsnetwerk benaderd moeten worden, dient eerst een VPN-tunnel over het wifinetwerk naar het interne bedrijfsnetwerk opgezet te worden. Hiermee worden onbevoegden geweerd omdat zij geen toegang hebben tot de centrale VPN-voorziening en het netwerkverkeer end-to-end is versleuteld. Deze maatregel heeft aanzienlijke toegevoegde waarde voor beveiliging van de communicatie.

Gebruikersauthenticatie en versleuteling van netwerkverkeer kan zowel door het accesspoint (WPA/WPA2) als door de VPN-software gedaan worden; het grootste verschil is dat voor het opbouwen van de VPN-tunnel al een bestaande netwerkverbinding vereist is. Zonder beveiligingsmaatregelen als WPA/WPA2 betekent dit dat de client gevoelig is voor wifinetwerkaanvallen tussen het moment dat de wifiverbinding is opgezet en het moment dat de VPN-tunnel is gerealiseerd.

WPA(2) heeft daarom de voorkeur, maar als dit niet beschikbaar is, of wanneer sterkere authenticatie nodig is voor toegang tot het (interne) netwerk, dan is het aan te raden om een VPN-verbinding te gebruiken.

6.6.7 *wifi-adapter tijdelijk uitschakelen*

In vrijwel alle huidige laptops en andere mobiele apparaten zit een wifi-adapter. Vaak staat deze adapter nog aan indien het apparaat in de stand-bystand is gezet en opgeborgen is in bijvoorbeeld een auto.

Wanneer de wifi-adapter actief is, is deze eenvoudig en met goedkope apparatuur (een wifi-detector) waarneembaar. Dit wordt gebruikt door inbrekers om laptops uit auto's te ontvreemden. Daarnaast loopt ieder apparaat met een actieve wifi-adapter het risico om gecompromitteerd te worden door directe communicatie naar het mobiele apparaat en kwetsbaarheden op OS-, driver-, firmware- of hardwareniveau.

Het is daarom verstandig om de wifi–functionaliteit uit te zetten wanneer deze niet gebruikt wordt. Dit voorkomt dat de aanwezigheid van een mobiel apparaat kan worden gedetecteerd en dat aanvallen op het mobiele apparaat over het draadloze netwerk worden uitgevoerd. «

7 Bijlage A Afkortingen en definities

Afkorting	Omschrijving
AES	Advanced Encryption Standard (AES), een sterke versleutelingstechniek (encryptie). Het is de opvolger van de Data Encryption Standard (DES).
AD	Active Directory (AD) is een eigen implementatie door Microsoft van de directoryservice LDAP in combinatie met Domain Name System (DNS) en Kerberos voor het gebruik in Windows-omgevingen vanaf Windows 2000.
AP	Accesspoint. Een wifi-basisstation waar draadloos een verbinding mee kan worden gemaakt. Meerdere basisstations kunnen onderling verbonden zijn door een ethernet-infrastructuur om roaming mogelijk te maken.
Bluetooth	Open standaard voor draadloze verbindingen tussen apparaten op korte afstand. De eerste versie had een bereik van 10 meter, de nieuwste versie van 100 meter.
BYOD	Bring Your Own Device (BYOD) is het beleid om medewerkers, zakelijke partners en andere gebruikers toe te staan om persoonlijk geselecteerde en gekochte (computer)apparatuur – zoals smartphones, tablets en laptops – op de werkplek te gebruiken en met het bedrijfsnetwerk te verbinden.
Clear Text	Onversleutelde data die door iedereen kan worden gelezen die toegang heeft tot de data.
DoS-aanval	Denial of Service-aanval. Een methode om d.m.v. het verzenden van heel veel verzoeken om te mogen aansluiten de mogelijkheid ontnemen voor legitieme gebruikers om contact te maken met een netwerk of systeem.
EAP	Extensible Authentication Protocol (EAP), een mechanisme dat meerdere authenticatiemethoden ondersteunt. Wordt binnen het 802.1x-framework gebruikt om de communicatie tussen client en authenticatieserver te beveiligen.
Encryptie	Het versleutelen van gegevens. Met behulp van een wachtwoord of encryptiesleutel kan data versleuteld worden. Alleen met behulp van dit wachtwoord of deze sleutel kan de versleutelde data weer leesbaar worden gemaakt. Encryptie voorkomt het ongeautoriseerd inzien of wijzigen van data.
ETSI	Het European Telecommunications Standards Institute (ETSI) is een onafhankelijke, non-profit, standaardisatie organisatie in de telecommunicatie-industrie (fabrikanten van apparatuur en netbeheerders) in Europa, met een wereldwijde projectie.[18]
Handshake	Het proces van initiatie van netwerkcommunicatie. Dit dient om te verifiëren dat beide partijen klaar zijn om de eigenlijke communicatie te starten. Als de handshake succesvol is verlopen wordt gesproken over een succesvol tot stand gekomen verbinding.
Hotspot	Een accesspoint in de openbare ruimte, meestal geschikt om zonder versleuteling mee te werken, vaak gebruikt voor internettoegang met mobiele apparaten.
(W)IDS	(Wireless) Intrusion Detection System, een mechanisme om inbraak op een (draadloos) netwerk te detecteren.

18 Bron: http://www.etsi.org/ en http://en.wikipedia.org/wiki/European_Telecommunications_Standards_Institute

IEEE	Het Institute of Electrical and Electronics Engineers is, met meer dan 400.000 leden, waarvan meer dan 100.000 student leden, in 160 landen, 's werelds grootste vereniging van professionals zoals ingenieurs, wetenschappers, wiskundigen, informatici, fysici, et cetera De vereniging heeft circa 900 actieve standaarden ontworpen en circa 400 zijn er nu in ontwikkeling met betrekking tot elektronica, elektriciteit en informatica.[19]
(W)IPS	(Wireless) Intrusion Prevention System, een mechanisme om inbraak op een (draadloos) netwerk te voorkomen.
(W)LAN	(Wireless) Local Area Network. Een lokaal netwerk met de omvang van één of meerdere gebouwen.
LDAP	Lightweight Directory Access Protocol (LDAP) is een netwerkprotocol dat beschrijft hoe gegevens uit directoryservices benaderd moeten worden over bijvoorbeeld TCP/IP. LDAP maakt gebruik van het LDAP Data Interchange Format (LDIF). Dit is een ASCII-formaat dat wordt gebruikt om gegevens toe te voegen aan de LDAP-hiërarchische database.[20] Een directory is in dit verband informatie die op een hiërarchische manier, gegroepeerd naar een bepaald attribuut, is opgeslagen. Denk aan een telefoonboek waarin telefoonnummers en adressen van personen per bedrijf worden opgeslagen.
MAC	Media Access Control. Een hardwareadres dat elke computer en elk mobiel apparaat op een unieke manier identificeert.
Malware	Malicious software (kwaadwillende software). Software die als doel heeft om een systeem (waaronder ook mobiele apparaten) te schaden; malware is de verzamelnaam voor wormen, rootkits, Trojaanse paarden, virussen, et cetera
MitM	Man-in-the-Middle-aanval, een type aanval waarbij de aanvaller als tussenpersoon fungeert in de netwerkcommunicatie en daardoor toegang heeft tot de informatie die wordt verzonden en ontvangen door het slachtoffer.
MIC	De Message Integrity Check (MIC) controleert of de inhoud van het pakketje nog steeds klopt.
NAC	Een Network Access Control (NAC) systeem biedt aanvullende controle over netwerktoegang. Op basis van de identiteit van de gebruiker en profielen wordt bepaald welke toegang een gebruiker krijgt.
NAP	Network Access Protection (NAP of netwerktoegangsbeveiliging) is een technologie die is geïntroduceerd in Windows Vista en Windows Server 2008. NAP biedt de mogelijkheid om een beleid voor de beveiligingsstatus op te stellen en handhaven. Dit beleid bepaalt de vereiste software- en systeemconfiguratie voor computers die verbinding maken met uw netwerk.[21]
OSI	Het Open Systems Interconnection (OSI)-model is een gestandaardiseerd middel om te beschrijven hoe data wordt verstuurd over een netwerk. Het zorgt er voor dat er compatibiliteit en interoperabiliteit is tussen de verschillende types van netwerktechnologieën van organisaties over de hele wereld. Dit model deelt de communicatie in zeven lagen in. Daarom wordt dit ook wel het Zevenlagenmodel genoemd. De lagen zijn, van hoog naar laag: toepassing, presentatie, sessie, transport, netwerk, datalink en fysiek. http://nl.wikipedia.org/wiki/OSI-model

19 Bron: http://www.ieee.org/index.html en http://nl.wikipedia.org/wiki/Institute_of_Electrical_and_Electronics_Engineers

20 Bron: http://nl.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol

21 Bron: http://technet.microsoft.com/nl-nl/library/cc730902%28v=ws.10%29.aspx

PNAK	802.1X is een IEEE beveiligingsstandaard voor poortgebaseerde authenticatie (port-based Network Access Control (PNAC)) op laag 2 van het Open Systems Interconnection (OSI)-model. Dit alles kan – afhankelijk van de gebruikte hardware – zowel bekabelde Ethernet-netwerken en draadloze 802.11-netwerken. (http://www.ieee802.org/1/pages/802.1x-2010.html)
PSK	Pre-shared Key (PSK), een sleutel voor encryptie/authenticatie die fysiek wordt gedeeld met gebruikers. Deze dient bijvoorbeeld om bezoekers toegang te geven tot internet.
RADIUS	Remote Authentication Dial In User Service (RADIUS) is een AAA (authenticatie, autorisatie en accounting) systeem. Het systeem wordt gebruikt om de identiteit van een gebruiker die toegang wenst tot een netwerk, te kunnen vaststellen.[22]
Roaming	Roaming is het overdragen van een bestaande verbinding tussen een client en een accesspoint naar een ander accesspoint waar op dat moment de signaalsterkte groter is. Op deze manier wordt het dus mogelijk het netwerk in een heel gebouw dekkend te krijgen. Lopend door het gebouw blijft de verbinding in stand.
Rogue accesspoint	Een nep/illegaal toegangspunt dat niet tot het oorspronkelijke draadloze netwerk behoort. Kwaadwillenden plaatsen een rogue accesspoint met de bedoeling informatie te stelen, af te luisteren of te veranderen.
SaaS	Software as a Service (SaaS) is software die als een onlinedienst wordt aangeboden. De klant hoeft de software niet aan te schaffen, maar sluit bijvoorbeeld een contract per maand per gebruiker, eventueel in combinatie met andere parameters. De SaaS-aanbieder zorgt voor installatie, onderhoud en beheer, de gebruiker benadert de software over het internet bij de SaaS-aanbieder.[23]
SIEM	Security Information and Event Management (SIEM) systemen bieden real-time-analyse van securitywaarschuwingen gegenereerd door bijvoorbeeld netwerksystemen, hardware of applicaties. SIEM-oplossingen verzamelen en correleren meldingen en worden gebruikt om beveiligingsgegevens te loggen en rapporten te genereren voor onder meer het afleggen van verantwoording.
Signaaloptimalisatie	De reikwijdte van het wifi-radiosignaal zodanig instellen dat de gebruikers optimaal toegang hebben, maar kwaadwillenden (van buiten) zo beperkt mogelijk toegang hebben.
SLA	Een Service level agreement (SLA) (Serviceniveau-overeenkomst), is een type overeenkomst waarin afspraken staan tussen aanbieder en afnemer van een dienst of product. Er wordt afgesproken wat de prestatie-indicatoren en kwaliteitseisen zijn van de te leveren dienst of product, om deze later te kunnen toetsen. In een SLA worden de rechten en plichten van beide partijen omschreven. Een SLA kan als afspraak bestaan tussen zowel externe (leverancier) als interne (klant) partijen binnen een organisatie. http://nl.wikipedia.org/wiki/Service_level_agreement
SSID	Service Set Identifier, de identificatie (de naam) van een wifinetwerk.
SSL-VPN	Secure Sockets Layer Virtual Private Network. Een mechanisme om een verbinding end-to-end te beveiligen op basis van SSL.
TKIP	Het Temporal Key Integrity Protocol (TKIP) is een versleutelmechanisme die wordt gebruikt bij WPA. Wordt als onveilig beschouwd.

22 Bron: http://nl.wikipedia.org/wiki/RADIUS

23 Bron: http://nl.wikipedia.org/wiki/Software_as_a_Service

VIR	Het besluit Voorschrift Informatiebeveiliging Rijksdienst (VIR) is op 1 januari 1995 van kracht geworden en regelt de wijze waarop de Nederlandse Rijksoverheid omgaat met de beveiliging van haar informatie. Het VIR is geen lijst met maatregelen die moeten worden doorgevoerd maar geeft een klein aantal basisregels. Het VIR is een doelstellende regeling, die veel overlaat aan de verantwoordelijke beheerders zelf. De regeling stelt minimumeisen aan het te ontwikkelen beveiligingsbeleid binnen een ministerie. Daarnaast worden eisen gesteld aan het stelsel van maatregelen dat dit beleid in de praktijk moet brengen. De beheerder van de informatie moet daartoe een risico-afweging maken waaruit blijkt welke maatregelen getroffen moeten worden. Op basis van die risico-afweging moeten informatiebeveiligingsplannen worden opgesteld. De eerste versie van het VIR (VIR 1994) was geldig van 1 januari 1995 tot 30 juni 2007. Op 1 juli 2007 is vervolgens de nieuwe versie van het VIR (VIR 2007) van kracht geworden. http://wetten.overheid.nl/BWBR0022141/
VPN	Virtual Private Network. Een mechanisme om een verbinding end-to-end te beveiligen.
Wardriving	Rondrijden met een computer (bijvoorbeeld een laptop) met wifi ondersteuning en de juiste software is voldoende om wifinetwerken in de buurt te vinden die actief zijn en die niet of onvoldoende beveiligd zijn tegen ongeautoriseerd gebruik.
WBA	De Wireless Broadband Alliance werd opgericht in 2003. De missie van WBA is het faciliteren van de adoptie van wifi ondersteunde diensten door middel van het verbeteren van gebruikerservaringen, interoperabiliteit en service delivery in technologieën, apparaten en netwerken.
Wbp	De belangrijkste regels voor de omgang met persoonsgegevens zijn vastgelegd in de Wet bescherming persoonsgegevens (Wbp). De Wbp is de Nederlandse uitwerking van de Europese richtlijn bescherming persoonsgegevens en is sinds 1 september 2001 van kracht. http://www.cbpweb.nl/pages/ind_wetten_wbp.aspx
WDS	Wireless Distribution System is een systeem dat het voor APs mogelijk maakt om draadloos verbinding met elkaar te maken.
WEP	Wired Equivalent Privacy. Een verouderde vorm van wifiversleuteling. WEP wordt als onveilig beschouwd en is eenvoudig te kraken.
Wifi	Wi-Fi is een certificatielabel ('logo') voor producten voor draadloze datanetwerken, die werken volgens de internationale standaard IEEE 802.11 (draadloos ethernet of wifi). Producten die volgens deze standaard werken maken gebruik van radiofrequenties in de 2,4GHz- en/of 5,0GHz-band die onder voorwaarden zonder licentie gebruikt mogen worden. De eisen voor dit logo worden vastgelegd door de Wi-Fi Alliance. De Wi-Fi Alliance is een wereldwijde non-profit brancheorganisatie van honderden bedrijven. De naam Wi-Fi staat, in tegenstelling tot wat velen denken, niet voor Wireless Fidelity.[24]
WiMAX	Worldwide Interoperability for Microwave Access is een standaard gebaseerd op de IEEE 802.16 (en ETSI HiperMAN) standaard voor breedbandige draadloze netwerken met middelgroot bereik. IEEE 802.16 staat ook wel bekend onder de naam WirelessMAN. Op 19 oktober 2007 werd WiMAX door het ITU toegevoegd aan de standaard voor 3G-netwerken.[25]
WPA	wifi Protected Access, een protocol dat zorgt voor versleuteling en authenticatie in een wifinetwerk. Een verouderde vorm van wifiversleuteling.
WPA2	wifi Protected Access versie 2, de nieuwste vorm van wifiversleuteling.
802.11	Ook wel wifi genoemd. Omvat een verzameling van standaarden voor draadloze netwerken (Wireless LAN), ontwikkeld door groep 11 van het IEEE LAN/MAN standaarden-comité (IEEE 802).

24 Bron: http://www.wi-fi.org en http://nl.wikipedia.org/wiki/Wi-Fi

25 Bron: http://nl.wikipedia.org/wiki/WiMAX

8 Bijlage B Referenties

Nr	Omschrijving
[1]	Strategy Analytics Connected Home Devices service, 'Broadband and Wi-Fi Households Global Forecast 2012.', de dato maart 2012 http://www.strategyanalytics.com/default.aspx?mod=reportabstractviewer&ao=7215 Achtergrond artikelen in relatie tot bovenstaand rapport: • http://www.businesswire.com/news/home/20120404006331/en/Strategy-Analytics-Quarter-Households-Worldwide-Wireless-Home
[2]	Wireless Broadband Alliance (WBA) Wi-Fi Industry Report: Global Trends in Public Wi-Fi, de dato november 2012 http://www.wballiance.com/wba/wp-content/uploads/downloads/2012/11/WBA_Wi-Fi_Industry_Report_Nov2012_Key-Findings.pdf Achtergrond artikelen in relatie tot bovenstaand rapport: • http://tabtimes.com/news/ittech-stats-research/2011/11/09/smartphone-and-tablet-adoption-drive-increasing-number-wi-fi
[3]	Nu.nl artikel 'Ziggo rolt landelijk wifi-netwerk vanaf 7 mei uit' http://www.nu.nl/internet/3406393/ziggo-rolt-landelijk-wifi-netwerk-7-mei.html Zie ook 'Ziggo WifiSpots' https://www.ziggo.nl/#producten/extra-diensten/wifispots/
[4]	Webwereld.nl artikel 'KPN-routers worden Fon wifi-hotspot' http://webwereld.nl/mobility/59080-kpn-routers-worden-fon-wifi-hotspot Zie ook 'KPN biedt wereldwijd publiek Wi-Fi netwerk via samenwerking met Fon' http://forum.kpn.com/t5/News-stream/KPN-biedt-wereldwijd-publiek-Wi-Fi-netwerk-via-samenwerking-met/ba-p/77406
[5]	NIST – SP 800-48 Rev 1- Guide to Securing Legacy IEEE 802.11 Wireless Networks http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf
[6]	NIST 'SP 800-153 - Guidelines for Securing Wireless Local Area Networks' http://csrc.nist.gov/publications/nistpubs/800-153/sp800-153.pdf
[7]	Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI 2013) http://wetten.overheid.nl/BWBR0033507
[8]	NSCS paper 'Consumerization en security', de dato 14 november 2012 https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/consumerization--security.html
[9]	NCSC 'Beveiligingsrichtlijnen voor mobiele apparaten', de dato 14 november 2012 https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/beveiligingsrichtlijnen-voor-mobiele-apparaten.html
[10]	NCSC whitepaper 'Cloudcomputing', de dato 19 december 2011 https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/whitepaper-cloudcomputing.html
[11]	NCSC 'Cybersecuritybeeld Nederland 2', de dato 6 juli 2012 https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/trendrapporten/cybersecuritybeeld-nederland.html en NCSC 'Cybersecuritybeeld Nederland 3', de dato 3 juli 2013 https://www.ncsc.nl/actueel/nieuwsberichten/cybersecuritybeeld-nederland-kwetsbaarheid-van-ict-onverminderd-hoog.html

Nationaal Cyber Security Centrum
Turfmarkt 147 | 2511 DP Den Haag
Postbus 117 | 2501 CC Den Haag
T 070 751 55 55 | F 070 888 75 50
www.ncsc.nl | info@ncsc.nl

Oktober 2013