INFORMATIE
BEVEILIGINGS
DIENST

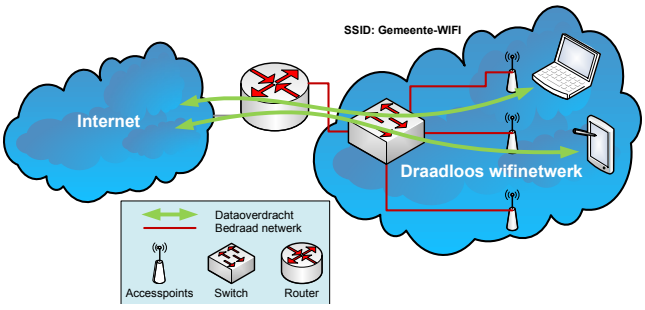
VEILIGE INRICHTING EN TOEPASSING VAN WIFI BINNEN UW GEMEENTE

Vanwege het gebruiksgemak bieden gemeenten steeds vaker wifi aan als standaarddienstverlening voor medewerkers en gasten. Op deze manier kunnen medewerkers en gasten via wifi gebruik maken van e-mail en internet of bedrijfsapplicaties raadplegen. Deze factsheet richt zich op de beveiligingsrisico's die wifinetwerken met zich meebrengen en welke maatregelen gemeenten kunnen nemen om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie te waarborgen en beveiligingsrisico's tot een acceptabel niveau te mitigeren. In deze factsheet wordt achtereenvolgens aandacht besteed aan wifi, de beveiligingsrisico's van wifinetwerken, hoe uw gemeente gebruik kan maken van veilige wifi en tenslotte het IBD advies.

Bij de inrichting van een wifinetwerk bepaalt de gemeente welke dienstverlening zij wil leveren en tegen welke bedreigingen het wifinetwerk en de achterliggende diensten bescherming nodig is. Het doel van deze factsheet is om gemeenten een aanpak en bijpassende maatregelen aan te reiken om te komen tot een gedegen en veilige implementatie van wifinetwerken. De veilige inrichting en het handhaven van de beveiliging van een wifinetwerk vereist continue aandacht. De gemeente dient, na de implementatie, te borgen dat de vereiste beveiliging ook in de toekomst gehandhaafd blijft. Maatregelen dienen niet alleen te worden geïmplementeerd, maar ook te worden gecontroleerd, geactualiseerd en vernieuwd[1].

WAT IS WIFI?

Wifi is een netwerkprotocol om draadloos informatie uit te wisselen, gebaseerd op de IEEE 802.11-standaard. Wifi wordt over het algemeen gebruikt om op locaties waar geen vaste netwerkverbinding beschikbaar is toch een internetverbinding aan te bieden. Inmiddels bieden veel bedrijven, gemeentehuizen, horeca, hotels, openbaar vervoer een wifinetwerk aan voor medewerkers en / of gasten (zie figuur 1). Hierbij communiceert mobiele apparatuur draadloos met accesspoints, die deze mobiele apparatuur verbinden met het achterliggende (bedraad) netwerk. Een groot voordeel van deze flexibele infrastructuur is dat het aantal aansluitingen en capaciteit eenvoudig kan worden uitgebreid.



Figuur 1: Draadloos Wifinetwerk

1 Zie hiervoor het operationele BIG product 'Information Security Management System' van de IBD.

DE VEILIGE INRICHTING EN HET HANDHAVEN VAN DE BEVEILIGING VAN EEN WIFINETWERK VEREIST CONTINUE AANDACHT.

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

WAT ZIJN DE BEVEILIGINGSRISICO'S?

Het grootste gevaar bij wifinetwerken is dat informatie die via het wifinetwerk wordt verstuurd, wordt afgeluisterd of gemanipuleerd. Een ander gevaar is dat via het wifinetwerk ongewenste toegang tot het bedrijfsnetwerk wordt verkregen. Hierbij dient steeds rekening gehouden te worden met dreigingen waar wifinetwerken aan blootstaan. Deze dreigingen, zoals wardriving, rogue accesspoint, spoofen van MAC-adres, Denial-of-Service (DoS), richten zich in het bijzonder op:

- het verstoren van de beschikbaarheid van informatie (Beschikbaarheid);
- het manipuleren van informatie (Integriteit);
- het verkrijgen van ongeautoriseerde toegang tot informatie (Vertrouwelijkheid).

Wardriving: Rondrijden met een computer (bijvoorbeeld een laptop, smartphone of tablet) 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.
Rogue accesspoint: Een nep/illegaal toegangspunt dat niet tot het oorspronkelijke wifinetwerk behoort. Kwaadwillenden plaatsen een rogue accesspoint met de bedoeling informatie af te luisteren of te manipuleren(man-in-the-middle[2]).
Spoofen van Media Access Control (MAC)-adres: Het MAC-adres is een nummer (hardwareadres) dat de netwerkadapter (uniek) identificeert die in je computer of mobiel apparaat geïnstalleerd is. Spoofing van het MAC-adres is het vervalsen van dit kenmerk met als doel om een andere identiteit aan te nemen.
Denial of Service (DoS): Een methode om door middel van 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.

WELKE MAATREGELEN KUNNEN GEMEENTE NEMEN?

Bij het ontwerp van een wifinetwerk dient rekening gehouden te worden met adequate beveiliging van het wifinetwerk[3]. De mate van beveiliging zal per situatie vastgesteld dienen te worden op basis van een risicoafweging. Het gaat hierbij niet alleen om de mate waarin bedrijfsinformatie toegankelijk is, maar of het wifinetwerk aan het bedrijfsnetwerk gekoppeld dient te worden en welke beveiligingseisen dan aan deze koppeling gesteld dienen te worden. 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.

Onderstaande vragen kunnen de gemeente helpen om het juiste beveiligingsniveau vast te stellen:

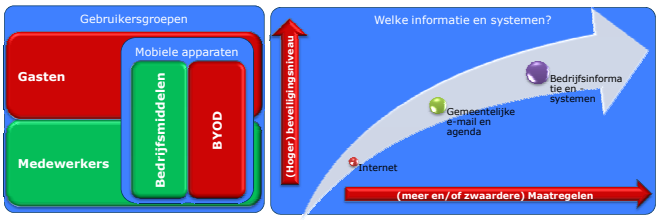
1. Voor welke gebruikersgroepen dient het wifinetwerk beschikbaar te zijn? Is het wifinetwerk alleen toegankelijk voor eigen medewerkers of ook voor gasten? Het gaat hierbij om het onderscheid tussen vertrouwde en niet-vertrouwde personen. De gemeente besluit zelf welke personen zij wil vertrouwen.

2. Met welke mobiele apparaten dient het wifinetwerk bereikbaar te zijn? Is toegang tot het wifinetwerk alleen mogelijk met bedrijfsmiddelen of ook met apparatuur die de gebruiker zelf meeneemt volgens het BYOD-principe[4]? Het gaat hierbij om het onderscheid tussen middelen die wel en die niet door de gemeente worden beheerd[5].

3. Welke bedrijfsinformatie en -systemen via het wifinetwerk beschikbaar dienen te zijn? Per gebruikersgroep dient vastgesteld te worden welke diensten worden geboden. Is alleen internet beschikbaar of zijn ook bedrijfsinformatie en -systemen toegankelijk? Hierbij zijn de volgende scenario's te onderscheiden:

a) Toegang tot internet
b) Toegang tot gemeentelijke e-mail en agenda
c) Toegang tot bedrijfsinformatie en -systemen

Ieder van deze vragen heeft 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 bedrijfsinformatie en -systemen heeft aanzienlijke gevolgen voor de zwaarte van de maatregelen die getroffen dienen te worden. In figuur 2 wordt de samenhang tussen gebruikersgroepen, mobiele apparaten en bedrijfsinformatie en –systemen grafisch weergegeven.



Figuur 2 Samenhang gebruikersgroepen, mobiele apparaten en bedrijfsinformatie en -systemen.

De te nemen maatregelen dienen te passen bij de beveiligingseisen en de geïdentificeerde dreigingen. Een belangrijk uitgangspunt is dat het beheersbaar blijft, dat het integraal kan worden meegenomen in de bedrijfsvoering (efficiency en effectiviteit) en dat de naleving gecontroleerd kan worden. De maatregelen dienen in balans te zijn. Zowel op het vlak van organisatorische, fysieke, procedurele en technische maatregelen als op het vlak van preventieve, reductieve, detectieve en correctieve maatregelen.

2 Man-in-the-middle (mitm), 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.

3 Zie hiervoor ook het whitepaper 'Wifi-beveiliging - De onderschatte schakel in netwerkbeveiliging' van het Nationaal Cyber Security Centrum (NCSC).

4 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.

5 Zie hiervoor het operationele BIG product 'Mobile Device Management' van de IBD.

Beleidskeuzes en risicoafweging

De gemeente dient zowel beleid voor gebruik als beveiliging van wifi te formuleren. Tevens dient de gemeente te zorgen dat gebruikers zich bewust zijn van de risico's van het gebruik van wifi. Risicomanagement is het uitgangspunt voor informatiebeveiliging en de primaire verantwoordelijkheid voor informatiebeveiliging ligt bij het (lijn)management. Wifi biedt gebruikersgemak en informatiebeveiligingsmaatregelen kunnen hierbij een negatieve uitwerking hebben op deze gebruiksvriendelijkheid. De verantwoordelijk manager dient dan ook op basis van een risicoafweging te bepalen hoe om dient te worden gegaan met de vaak tegenstrijdige belangen tussen informatiebeveiliging, efficiëntie en gebruikersgemak.

Iedere gemeente dient een risicoanalyse uit te voeren voordat wordt besloten tot het invoeren van wifi[6]. Uit de risicoanalyse dient naar voren te komen in welke mate de toegang tot (bepaalde categorieën) informatie dient te worden beveiligd[7]. Op basis van de resultaten van de risicoanalyse dient de gemeente te besluiten of en in welke vorm wifi in de ICT-infrastructuur wordt toegepast. Deze keuze wordt bepaald door de classificatie van de data die benaderd wordt of zou kunnen worden via dit wifinetwerk. Het classificatieniveau kan mede afhankelijk zijn van specifieke wet- en regelgeving, zoals de Wet bescherming persoonsgegevens (Wbp).
Hoe hoger de classificatie van verwerkte informatie, hoe zwaarder de beveiligingsmaatregelen. De gemeente kan bijvoorbeeld besluiten om wifi gecontroleerd beschikbaar te stellen aan geautoriseerde gebruikers met toegang tot geselecteerde bedrijfsinformatie en -systemen of de toegang tot het bedrijfsnetwerk via wifi niet toe te staan.

Op basis van de resultaten van de risicoanalyse kan een onderbouwde keuze worden gemaakt of wifi geschikt is voor de gemeente en of de voordelen (gebruiksgemak) opwegen tegen de nadelen (risico's, kosten et cetera). Vervolgens dient de gemeente op basis van de risicoanalyse een wifibeleid te bepalen. Op basis van dit wifibeleid kan de gemeente bepalen welk wifiscenario het beste kan worden geïmplementeerd. Om vast te stellen welk wifiscenario voor de gemeente het beste kan worden toegepast dienen de volgende vragen beantwoord te worden:

- Wat is het hoogste vertrouwelijkheidsniveau waarvoor het gebruik van wifi wordt toegestaan?
- Welke gebruikersgroepen worden (zowel in- als extern) onderkend en welke diensten wil de gemeente deze gebruikersgroepen via wifi aanbieden?
- Met welke mobiele apparaten wordt toegang tot het wifinetwerk toegestaan? Gaat het alleen om mobiele apparaten die door de gemeente worden beheerd of ook om mobiele apparaten die door gebruikers zelf worden meegenomen (BYOD)?
- Hoe wil de gemeente omgaan met het afdwingen van bepaalde regels voor het gebruik van mobiele apparaten via wifi?

6 Zie hiervoor het operationele BIG product 'Diepgaande Risicoanalysemethode gemeenten' van de IBD.

7 Zie hiervoor ook het operationele BIG product 'Handreiking Dataclassificatie' van de IBD.

Technische maatregelen

Voor de beveiliging van wifi kunnen allerlei diverse technische maatregelen worden toegepast. Veel toegepaste maatregelen zijn: gescheiden netwerken, versleutelen van de communicatieverbinding en sterke authenticatie et cetera.

1. Koppeling tussen het wifinetwerk en het bedrijfsnetwerk

Zolang alleen toegang is vereist tot publieke informatie kan volstaan worden met een koppeling van het wifinetwerk aan het internet. Zodra toegang tot bedrijfsinformatie nodig is, dient het wifinetwerk aan het bedrijfsnetwerk te worden gekoppeld. Een dergelijke koppeling kan gerealiseerd worden met een beveiligd koppelvlak. 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 beveiligd koppelvlak.

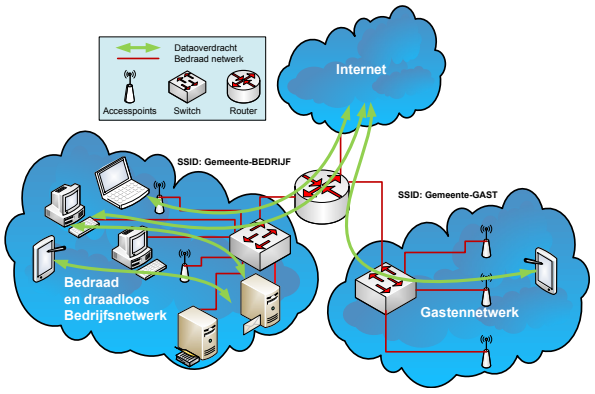
2. Verbinding met het juiste wifinetwerk

Belangrijk is dat gebruikers verbinding hebben met het juiste wifinetwerk. Bijvoorbeeld medewerkers met het bedrijfsnetwerk en gasten met het gastennetwerk. De gemeente zal gasten duidelijk dienen te maken welk wifinetwerk de gast mag gebruiken. Dit kan bijvoorbeeld door gasten te informeren over het te gebruiken wifinetwerk (SSID), of het wifinetwerk een dusdanige naam te geven dat direct duidelijk is dat dit het wifinetwerk voor gasten is.

3. Scheiding van netwerken

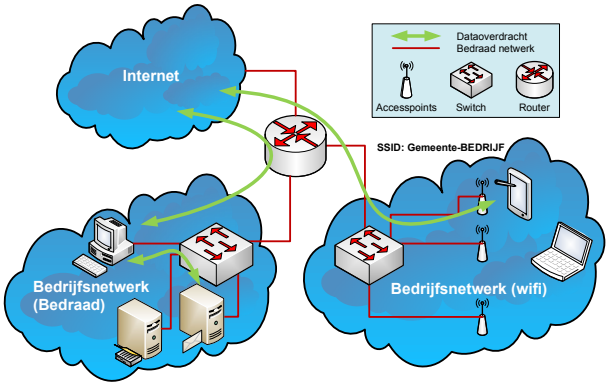
Het wifinetwerk dient, net zoals het internet, te worden beschouwd als een onvertrouwd netwerk van waaruit aanvallen plaats kunnen vinden. Om het interne bedrijfsnetwerk hiertegen te beveiligen dienen deze netwerken van elkaar gescheiden te zijn. De volgende vormen van netwerkscheiding kunnen worden toegepast:

- Scheiding van gast- en bedrijfs-wifinetwerk
  Om zeker te zijn dat ongeautoriseerde gebruikers geen toegang krijgen tot het bedrijfsnetwerk kunnen twee gescheiden wifinetwerken worden aangeboden (zie figuur 3). Op deze manier maken gasten gebruik van het gasten-wifinetwerk (internet) en maken medewerkers gebruik van het bedrijfs-wifinetwerk. Het bedraad en draadloos netwerk voor medewerkers is op deze manier niet van elkaar gescheiden. Dit kan risico's met zich mee brengen



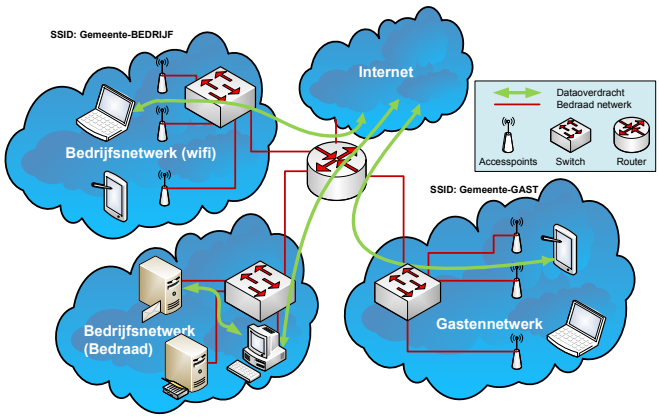
Figuur 3 Scheiding van gast- en bedrijfs-wifinetwerk

- Fysieke scheiding wifi en bedraad bedrijfsnetwerk
  Om zeker te zijn dat het wifi en het bedraad bedrijfsnetwerk niet met elkaar verbonden zijn, is het advies om beide netwerken volledig fysiek te scheiden met ieder een eigen implementatie (zie figuur 4). Beide netwerken hebben hun eigen switches, routers en bekabeling. Daarnaast heeft het wifinetwerk de noodzakelijke accesspoints. Vanwege de zekerheid dat beide netwerken gescheiden zijn is dit een effectieve oplossing tegen misbruik. Daar diverse netwerkcomponenten dubbel uitgevoerd zijn, is dit wel een relatief dure oplossing.



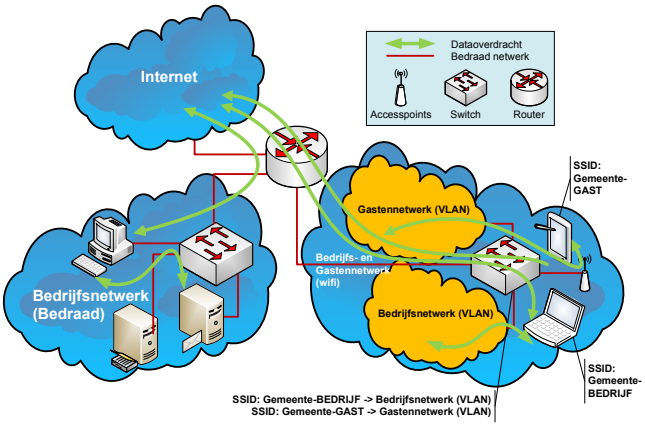
- Segmentering van het netwerk
  Als de gemeente wifi aan gasten wil aanbieden, dient dit gastennetwerk gescheiden te zijn van het wifi en bedraad bedrijfsnetwerk. Gasten mogen toegang hebben tot het internet en niet tot het bedrijfsnetwerk.

Figuur 4 Fysieke scheiding wifinetwerken en bedraad bedrijfsnetwerk



Figuur 5 Fysieke scheiding wifinetwerken en bedraad bedrijfsnetwerk

Het advies is dan ook om verschillende gescheiden wifinetwerken naast elkaar aan te bieden (zie figuur 5). Bijvoorbeeld voor gasten en medewerkers. Elk afzonderlijk wifinetwerk krijgt een eigen naam (Service Set Identifier (SSID)) en loginprocedure. Afhankelijk van de gebruikte netwerkapparatuur is het zelfs mogelijk om te configureren wat de gebruiker van de wifiverbinding wel en niet mag.



Figuur 6 Draadloos bedrijf- en gastennetwerk met VLAN

Een variant op de fysieke scheiding van wifinetwerk en bedraad netwerk is een virtuele scheiding op basis van virtuele LANs (VLANs). Beide netwerken maken hierbij grotendeels gebruik van dezelfde fysieke netwerkcomponenten zoals switches en routers. Op logisch netwerkniveau worden VLANs gedefinieerd waardoor 'virtueel' gescheiden netwerken worden gecreëerd. Een apart VLAN voor het bedrijfs-wifinetwerk en een apart VLAN voor het gasten-wifinetwerk levert twee logisch gescheiden netwerken op (zie figuur 6). Dit kan nog verder worden doorgevoerd door naast de twee aparte VLANs voor de wifinetwerken een apart VLAN op te zetten voor het bedraad bedrijfsnetwerk. Deze VLAN-oplossing is een beproefde technologie en is goedkoper dan een volledige fysieke scheiding. Beheersmatig vereist deze oplossing meer specifieke 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 (bedraad)bedrijfsnetwerk, dan dient de onderlinge communicatie via een beveiligd koppelvlak te verlopen (zie figuur 7).
  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) om te alerteren zodra een potentieel malafide activiteit plaatsvindt binnen het netwerk of het actief blokkeren van een aanval met een Intrusion Prevention System (IPS)[8].

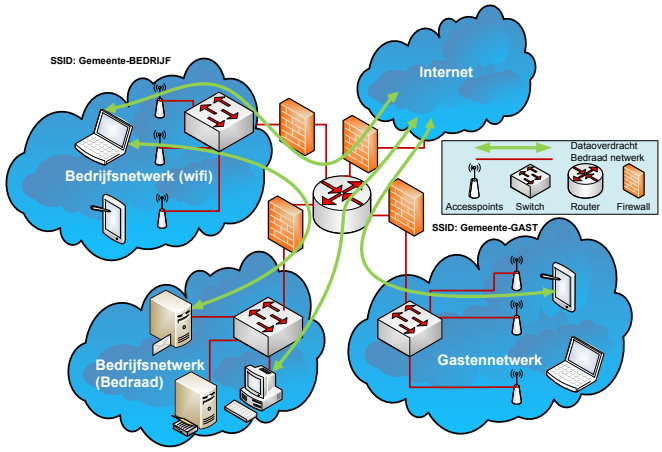
  Maatregelen die in dit beveiligd koppelvlak genomen dienen te worden zijn bijvoorbeeld:

  - 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

8 Zie hiervoor ook de 'Handreiking voor implementatie van detectie-oplossingen' van het Nationaal Cyber Security Centrum (NCSC).

en software versies, van het bedrijfsnetwerk vrijgegeven naar het (externe) wifinetwerk.
- alleen toegang geven tot een kopie van de informatie;
- gebruik maken van een stepping-stone server;
- informatie over de inkomende en uitgaande datastromen wordt gelogd en geanalyseerd door geautoriseerde personen.

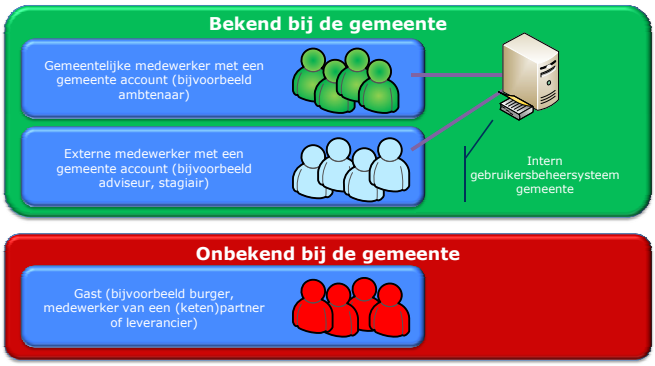
De koppeling naar het internet zou ook via een beveiligd koppelvlak dienen te lopen, in verband met aanvallen vanaf of naar het internet. De gemeente is in eerste instantie aansprakelijk voor internetaanvallen die zijn wifi-gebruikers uitvoeren; het is daarom verstandig om te zorgen dat ook uitgaande 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.



Figuur 7 Beveiligd koppelvlak

4. authenticatie van gebruikers (en apparaten);

Alleen legitieme gebruikers en apparatuur mogen via het wifinetwerk communiceren. In figuur 8 worden de verschillende soorten gebruikers weergegeven. Het doel van (client-)authenticatie is het voorkomen van ongeautoriseerde toegang tot het wifinetwerk.
In verband met gebruiksgemak en beheersbaarheid, is het wenselijk om voor de authenticatie van eigen medewerkers gebruik te maken van de eigen authenticatiesystemen. Bijvoorbeeld een koppeling met het interne gebruikersbeheersysteem (zoals Active Directory (AD), Lightweight Directory Access Protocol (LDAP) et cetera).



Figuur 8 Verschillende soorten gebruikers

Hoe en met welke sterkte de authenticatie dient te worden ingericht is vooral afhankelijk van het vertrouwelijkheidsniveau van de (bedrijfs)informatie die door bekende personen kan worden benaderd. Er dienen adequate authenticatiemiddelen te worden ingezet als het wifinetwerk is gekoppeld aan het bedrijfsnetwerk of vertrouwelijke (bedrijfs)informatie kan worden benaderd. Als aan bekende personen alleen toegang tot internet wordt geboden is er geen sterk authenticatiemechanisme vereist, maar blijft het advies dit te koppelen aan het bestaande authenticatiesysteem.

Bij de inrichting van authenticatie dient van het volgende te worden uitgegaan:

- De toegang tot een bedrijfsnetwerk dient persoonlijk te zijn, zodat per uniek identificeerbaar persoon toegang kan worden gegeven en ingetrokken.
- Maak binnen een bedrijfsomgeving gebruik van geautomatiseerde methoden voor wederzijdse authenticatie (conform het IEEE 802.1X-raamwerk). Hierbij wordt een authenticatieserver gebruikt om tweezijdige authenticatie te realiseren. De authenticatieserver kan de gebruiker (via gebruikersnaam/wachtwoorden of certificaten) en/of het systeem (via certificaten of MAC-adres) verifiëren.

5. versleuteling van de netwerkverbinding

Versleuteling van het wifinetwerkverkeer dient te voorkomen dat de informatie die over het wifinetwerk wordt verzonden kan worden afgeluisterd en gemanipuleerd.

Bij voorkeur richt de gemeente voor eigen (vertrouwde) medewerkers een geavanceerd mechanisme in voor versleuteling, zonder dat het de medewerkers in het gebruik belemmerd. Voor (incidentele) gasten ligt dat anders. Er kan worden gekozen voor onversleutelde communicatie of het gebruik van een (handmatig) gedeeld wachtwoord. De gemeente kan ook kiezen om gebruik te maken van tijdelijk geldige privésleutels, dit brengt wel een grotere beheerlast met zich mee. Omdat sprake is van geen tot beperkte beveiliging wordt aanbevolen om het wifinetwerk voor gasten af te scheiden van het wifinetwerk voor eigen medewerkers. Omdat over een onversleutelde of eenvoudig versleutelde verbinding wordt gewerkt zal een disclaimer getoond dienen te worden die de gast ervoor waarschuwt dat zijn/haar data mogelijk kan worden afgeluisterd.

Bij de inrichting van de versleuteling dient van het volgende te worden uitgegaan:

- Zet het mechanisme voor versleuteling zodanig op dat het past bij de gebruikersgroepen en het vertrouwelijkheidsniveau van de verwerkte informatie.
-
- Maak gebruik van adequate methoden voor versleuteling en authenticatie, nu WPA2 met AES-versleuteling omdat oudere methoden kwetsbaarheden bevatten. Geïmplementeerde beveiligingsprotocollen dienen nu maar ook in de toekomst een adequate beveiliging te blijven bieden. Door de steeds toenemende rekenkracht van computers hebben versleutelmethoden een beperkte houdbaarheid.

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

WPA/WPA2 (Wifi Protected Access) zijn beveiligingsstandaarden die als opvolgers van WEP (Wired Equivalent Privacy) zijn ontwikkeld. WEP is simpelweg geen veilige optie meer en WPA wordt als kwetsbaar gezien. WPA2 is de opvolger van WPA en maakt gebruik van het sterkere versleutelprotocol. In deze factsheet wordt dan ook alleen aandacht besteed aan WPA2.

WPA2 onderkent twee varianten, die beide zowel versleuteling als authenticatie bieden. Dit zijn Personal of Small Office Home Office (SOHO) en Enterprise.

WPA2-Personal is met name bedoeld voor thuisgebruik of kleine organisaties. Hierbij wordt voor authenticatie gebruik gemaakt van een gedeeld wachtwoord voor authenticatie, de Pre-Shared key (PSK).

WPA2-Enterprise is bedoeld voor (grotere) organisaties. Hierbij wordt gebruik gemaakt van het 802.1x-authenticatieraamwerk, het Extensible Authentication Protocol (EAP) en een authenticatieserver om tweezijdige authenticatie te realiseren. Het is belangrijk dat gemeente hierbij een koppeling met reeds bestaande authenticatiemiddelen (bijvoorbeeld gebruikersbeheersystemen zoals LDAP en Active Directory) leggen. Hiermee wordt het beheer vereenvoudigd.

WPA2-Enterprise maakt het mogelijk om veilige wifinetwerken op te zetten. De standaard specificeert de beveiligingsmechanismen bij het tot stand brengen van toegang tot een wifinetwerk. WPA2-Enterprise impliceert de toepassing van een aantal andere standaarden, met name:

- EAP: Standaard voor authenticatie over een point-to-point-verbinding, bijvoorbeeld tussen een wifi-gebruiker en een accesspoint.
- 802.1X: Standaard om EAP te gebruiken op een wifinetwerk.
- RADIUS[9]: Maakt het mogelijk om toegang te verlenen door de identiteit van een gebruiker, die toegang wenst tot een netwerk, te kunnen vaststellen.

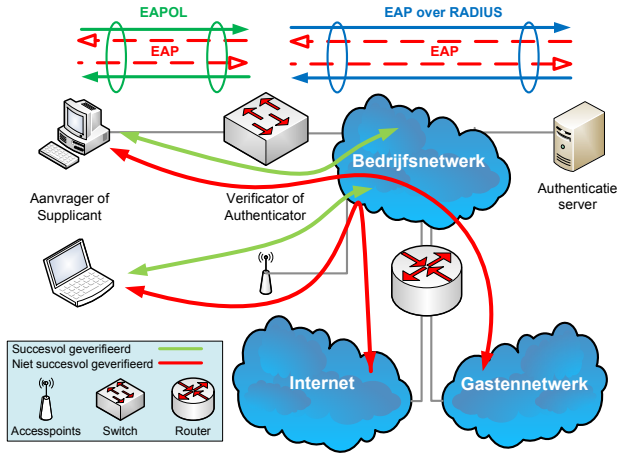
Uitsluitend WPA2-Enterprise (in combinatie met de andere genoemde standaarden) biedt een afdoende hoog beveiligingsniveau voor toegang tot wifinetwerken. WPA2-Enterprise is sinds begin 2016 opgenomen op de lijst met verplichte open standaarden voor de gehele publieke sector ('pas-toe-ofleg-uit-lijst') van het Forum Standaardisatie.

9 RADIUS staat voor: Remote Authentication Dial In User Service en 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.

802.1x-standaard

Het protocol dat gebruikt wordt voor authenticatie in de 802.1x-standaard is het Extensible Authentication Protocol (EAP). EAP ondersteunt verschillende authenticatiemethoden voor zowel bedrade als wifinetwerken. De drie basiscomponenten binnen de 802.1x-standaard zijn: de supplicant (een gebruiker of systeem), de authenticator (accesspoint of switch) en de authenticatieserver (Remote Authentication Dial In User Service(RADIUS)-server).
De authenticator geeft de authenticatieberichten tussen de supplicant en de authenticatieserver door (zie figuur 9). De authenticator heeft alleen bij het starten en stoppen van het EAP-authenticatieproces een actieve rol, in de tussenliggende periode is de authenticator eigenlijk een doorgeefluik tussen de supplicant en de authenticatieserver. EAP is niet ontwikkeld om in een IP-netwerk te worden gebruikt. Om dit toch mogelijk te maken worden de EAP-pakketten op twee manieren getransporteerd over het IP-netwerk:

- EAP over LAN (EAPOL) tussen supplicant en authenticator;
- EAP over RADIUS tussen authenticator en de authenticatie server.



Figuur 9 802.1x authenticatieproces

Het 802.1x authenticatieproces verloopt via de volgende stappen:

1. De supplicant verstuurt een verzoek om toegang naar de authenticator.
2. De authenticator vraagt de supplicant zich te identificeren.
3. De supplicant verstuurt een identiteitspakket naar de authenticator die dit doorgeeft aan de authenticatieserver.
4. De authenticatieserver controleert het ontvangen identiteitspakket en op basis daarvan zal de authenticatie succesvol zijn of niet. De authenticatieserver kan:
   - een gebruiker op basis van wachtwoorden of certificaten verifiëren
   - een systeem op basis van certificaten of MAC-adres verifiëren.

Bij een geslaagde verificatie stuurt de authenticatieserver een acceptatiepakket terug naar de authenticator die vervolgens de supplicant instelt als geautoriseerd. De supplicant kan nu bijvoorbeeld gebruik maken van het bedrijfsnetwerk et cetera. Bij een niet geslaagde verificatie kan bijvoorbeeld de toegang geheel worden geweigerd of kan de supplicant alleen gebruik maken van het gastennetwerk en/of internet et cetera.

De WPA/WPA2-standaard kan van verschillende EAP/RADIUS-authenticatiemechanismen gebruikmaken[10]. De meest toegepaste en veilige EAP/RADIUS-authenticatiemechanismen worden in tabel 1 weergegeven. Hierbij wordt aangegeven op welke wijze de client (supplicant) en de authenticatieserver zich dienen te authenticeren.

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

Tabel 1: Authenticatiemechanismen

EAP-TLS

EAP-Transport Layer Security (EAP-TLS) wordt op dit moment gezien als één van de veiligste EAP standaarden en maakt gebruik van digitale certificaten waarbij een tweezijdige TLS-authenticatie plaatsvindt[11]. Alle supplicants maar ook de authenticatieserver worden voorzien van een digitaal certificaat. Deze digitale certificaten worden gebruikt om zowel de supplicant als authenticatieserver te authenticeren.

EAP-TTLS
EAP-Tunneled Transport Layer Security (EAP-TTLS) is een uitbreiding op EAP-TLS waarbij een eenzijdige TLS authenticatie wordt geboden in plaats van een tweezijdige TLS-authenticatie. Hierbij authenticeert de authenticatieserver zich met een digitaal certificaat en wordt een versleutelde tunnel opgezet tussen de supplicant en de authenticatieserver. Op het moment dat deze versleutelde tunnel is opgezet vindt de tweede authenticatie plaats van de supplicant naar de authenticatieserver. Hierbij kan gebruik gemaakt worden van verschillende authenticatiemethoden zoals wachtwoorden[12] en digitale certificaten. De authenticatiegegevens van de supplicant worden via de opgezette versleutelde tunnel (versleuteld) uitgewisseld.

PEAP
Protected Extensible Authentication Protocol (PEAP) is vergelijkbaar met EAP-TTLS. Ook hier vindt eenzijdige TLS authenticatie plaats. Op het moment dat de authenticatieserver zich met een digitaal certificaat heeft geauthenticeerd en de versleutelde tunnel is opgezet, tussen de supplicant en de authenticatieserver, vindt de tweede authenticatie plaats van de supplicant naar de authenticatieserver. Hierbij kan alleen gebruik gemaakt worden van de authenticatiemethode op basis van gebruikersnaam en wachtwoorden. De authenticatiegegevens van de supplicant worden zo versleuteld uitgewisseld.

Digitale clientcertificaten zijn veiliger dan gebruikersnamen en wachtwoorden, maar de distributie vereist wel meer beheerinspanning. Het digitaal certificaat dient bijvoorbeeld op een systeem te worden geïnstalleerd.

Voor wachtwoorden geldt dat een sterk wachtwoord gekozen dient te worden (minimaal 8 vrij te kiezen tekens, waarvan tenminste 1 kleine letter, 1 hoofdletter, 1 cijfer en 1 vreemd teken)[13]. De gebruiker dient op een veilige manier met het wachtwoord om te gaan maar tevens dient de uitgifte en het beheer van deze inloggegevens goed te zijn geregeld.

6. detectie en preventie.

Detectie en preventie dienen onder andere te voorkomen dat kwaadwillenden zich toegang verschaffen tot computersystemen en/of schadelijke handelingen uitvoeren. Deze controle kan door middel een Wireless Intrusion Detection System (WIDS). Een Wireless Intrusion Prevention System (WIPS) biedt de mogelijkheid om 'inbrekers' te signaleren en blokkeren voordat deze zich toegang hebben verschaft tot een computersysteem en/of al diverse schadelijke handelingen hebben uitgevoerd.

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 alleen toegang tot publieke 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 deze functionaliteit inmiddels als een Software as a Service (SaaS)-oplossing[14].

7. Architectuurontwerp

Als besloten is om wifi in de ICT-infrastructuur van de gemeente op te nemen, dient de juiste balans te worden gevonden tussen beveiliging en gebruikersgemak. Een gedegen architectuurontwerp is noodzakelijk om het keuzeproces te ondersteunen, onderbouwen en borgen. Bij het opzetten van een architectuur voor wifi kan worden uitgegaan van bestaande principes, best practices en standaarden. Denk hierbij 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[15] voor authenticatie.

10 Zie voor meer achtergrondinformatie het document 'Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i' van het National Institute of Standards and Technology (NIST)

11 Zie hiervoor het operationele BIG product 'Encryptiebeleid (PKI)' van de IBD

12 Afhankelijk van de authenticatiemethode worden de wachtwoorden niet zelf verzonden maar worden aan beide zijde challenges (berekeningen met het wachtwoord) uitgevoerd

13 Zie hiervoor het operationele BIG product 'Wachtwoordbeleid' van de IBD.

14 Zie hiervoor zowel het operationele BIG product als de factsheet 'Cloud Computing' van de IBD

15 802.1X 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)

- Beveilig naast het netwerk, ook de apparatuur van de gebruikers, zowel voor de instellingen als voor de gegevens die er mogelijk op worden verwerkt en opgeslagen. Er dient rekening mee gehouden te worden dat gebruikers zelf aangeschafte apparatuur (willen) gebruiken in hun werkomgeving.
- Fysieke beveiliging van netwerkcomponenten dient onderdeel te 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 (meestal) complexe infrastructuur
- Implementeer naast preventieve maatregelen ook maatregelen die gericht zijn op detectie van inbraken op het wifinetwerk, zoals een WIDS.

8. Beheer & onderhoud

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

Continue activiteiten:

- Onderzoek incidentmeldingen en problemen 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)-oplossingen[16]. 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 dient bijvoorbeeld conform afspraken te 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 wifinetwerkverkeer 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[17]) uitvoeren op het wifinetwerk om gaten in de beveiliging te ontdekken en te repareren.
- Controleer de dekking van het wifinetwerk. Deze dient ruim genoeg te zijn om gebruikers goedwerkende toegang te verlenen, maar tegelijkertijd niet te ruim 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 gebruikersgroepen 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 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.

16 Security Information and Event Management (SIEM) systemen bieden real-time-analyse van security waarschuwingen 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.

17 Zie hiervoor het operationele BIG product 'Handreiking penetratietesten' van de IBD.

ADVIES IBD MET BETREKKING TOT WIFINETWERKEN

De IBD geeft het advies om onderstaande maatregelen te implementeren om zodoende de beschikbaarheid, integriteit en vertrouwelijkheid van informatie bij het gebruik van wifinetwerken te waarborgen en de risico's te mitigeren:

- Zorg ervoor dat de basis van informatiebeveiliging op orde is;
- Zorg ervoor dat de risico's van wifi zijn onderzocht;
- Zorg voor een onderbouwde beleidskeuze over het gebruik van wifi;
- Zorg voor een architectuur die past bij de gemeente;
  - Zorg voor de juiste balans tussen beveiliging en gebruikersgemak.
  - Zorg voor een adequate scheiding/segmentering van netwerken. Denk hierbij aan een fysieke of virtuele (VLAN) scheiding.
  - Zorg voor beveiligde koppelvlakken tussen deze netwerken. Denk hierbij aan firewalls, malware detectie et cetera.
  - Zorg voor detectie maatregelen. Denk hierbij aan logging en monitoring, (Wireless) Intrusion Detection Systemen ((W)IDS) et cetera.
- Zorg voor methoden van afdoende sterkte voor versleuteling en authenticatie;
  - Maak gebruik van bestaande interne gebruikersbeheer-/authenticatiesystemen.
  - Maak gebruik van WPA2-Enterprise (Wifi Protected Access).
  - Maak gebruik van het 802.1X-raamwerk voor wederzijdse authenticatie.
  - Maak gebruik van een veilige verbinding om gegevens uit te wisselen (bijvoorbeeld VPN).
- Zorg ervoor dat het beheer en onderhoud van de maatregelen goed is ingericht;
  - Maak hierbij onderscheid tussen dagelijkse (continue) en periodieke beheeractiviteiten.
- Zorg ervoor dat gebruikers en beheerders zich bewust zijn van de risico's;
- Zorg voor passende fysieke beveiliging van de netwerkcomponenten;
- Zorg voor passende beveiliging van de mobiele apparaten;
- Neem eventueel aanvullende maatregelen op netwerkniveau.

MEER INFORMATIE

MEER INFORMATIE OVER ONZE DIENSTVERLENING VINDT U IN DE ANDERE FACTSHEETS VAN DE IBD EN OP DE WEBSITE WWW.IBDGEMEENTEN.NL. HIER KUNNEN GEMEENTEN BOVENDIEN VIA DE COMMUNITY RELEVANTE INFORMATIE MET ELKAAR DELEN, VRAGEN AAN ELKAAR STELLEN EN DOCUMENTEN UITWISSELEN. DE HELPDESK VAN DE IBD IS TE BEREIKEN TIJDENS KANTOORUREN VAN 9:00 TOT 17:00 UUR OP HET NUMMER 070 373 8011 OF VIA HET E-MAILADRES INFO@IBDGEMEENTEN.NL. TIJDENS DEZE KANTOORUREN REAGEERT DE IBD BINNEN 30 MINUTEN OP EEN INCIDENTMELDING. BUITEN KANTOORUREN IS DE IBD OP HETZELFDE NUMMER BEREIKBAAR VOOR SPOEDEISENDE MELDINGEN EN ZAL DE IBD BINNEN 60 MINUTEN REAGEREN OP EEN TELEFONISCHE OPROEP.