Wifi in de retailomgeving

Overview van de diverse aspecten waarmee een retailer te maken krijgt bij de aanleg en exploitatie van een Wifinetwerk

MOB - WEE	Auteurs	Versie - Datum
Werkstroom *Wifi in de Retailomgeving*	Michel van Bommel *(Detailhandel Nederland)* Peter Kleppe *(Betaalvereniging Nederland)*	1.0 DEF 13 juni 2018

Inhoud

Wifi in de retailomgeving

Aanleiding, Samenvatting en Leeswijzer

Een belangrijke ontwikkeling van de laatste jaren in het winkeldomein is de grootschalige implementatie van Wifinetwerken. Deze draadloze netwerken geven de ondernemer veel mogelijkheden om zijn eigen bedrijfsprocessen te ondersteunen, maar ook om de consument te faciliteren en om betalingsverkeer via de Wifinetwerken af te wikkelen. Zowel aan de fysieke en virtuele toonbank is continuïteit van het betalingsverkeer van essentieel belang. Geconstateerd werd, dat retailondernemers soms weinig kennis hebben van kansen en mogelijkheden van Wifinetwerken, maar ook van zwakheden en bedreigingen ervan. Dat is aanleiding geweest om een rapport op te stellen met betrekking tot het gebruik van Wifinetwerken voor betalingsverkeer.

Een retailer die in zijn winkel een Wifinetwerk wil installeren en onderhouden, zal rekening moeten houden met een aantal aandachtspunten. Belangrijkste daarvan zijn:

- Beschikbaarheid (maximaal);
- Misbruik en fraude (minimaal);
- Juridische aspecten.

Voor elk van deze aandachtspunten zal hij organisatorische, procedurele, fysieke en technische maatregelen moeten nemen.

In de hoofdtekst van dit document worden al deze punten nader toegelicht.
In Bijlage 1 worden genoemde punten in meer detail uitgewerkt. In Bijlage 2 worden Wifi-ontwikkelingen geschetst, zoals die zich voordoen in het publieke domein. In Bijlage 3 is een korte Q&A opgenomen betreffende de belangrijkste privacyaspecten. Tot slot is aan het eind van het document, als Bijlage 4, een checklist opgenomen die een individuele retailer kan gebruiken wanneer hij overweegt een Wifinetwerk te (laten) installeren.
Dit rapport is bedoeld voor Detailhandel Nederland en haar achterban. Het geeft een uitgewerkt overzicht van alle bovengenoemde aandachtspunten.

Inleiding

De fysieke winkel anno 2018 is niet meer te vergelijken met de winkel van 10 jaar geleden. O.a. de ontwikkelingen op het gebied van telecommunicatie zijn niet voorbij gegaan aan de retailsector. Telecommunicatie is noodzakelijk geworden voor voorraadmanagement, locatiebeveiliging, kassabeheer, toegang tot de winkelapp, volgen van klantbewegingen binnen de winkel, communicatie met de klant, en ook voor het afhandelen van betalingen. Een ondernemer die maximaal gebruik maakt van telecommunicatiediensten heeft een duidelijke voorsprong op een ondernemer die dat niet doet.

Dit document benoemt een aantal van deze ontwikkelingen en beschrijft op hoofdlijnen welke kansen en bedreigingen deze ontwikkelingen geven voor de detailhandel. Daarbij wordt ingezoomd op de mogelijkheden van WLAN-technologie en de implicaties voor een ondernemer om hier optimaal gebruik van te maken.

WLAN en Wifi

Draadloze lokale netwerken worden over het algemeen aangeduid met de afkorting WLAN, wat staat voor Wireless Local Area Network. Hieronder vallen meerdere technieken, zoals Wifi en Bluetooth.

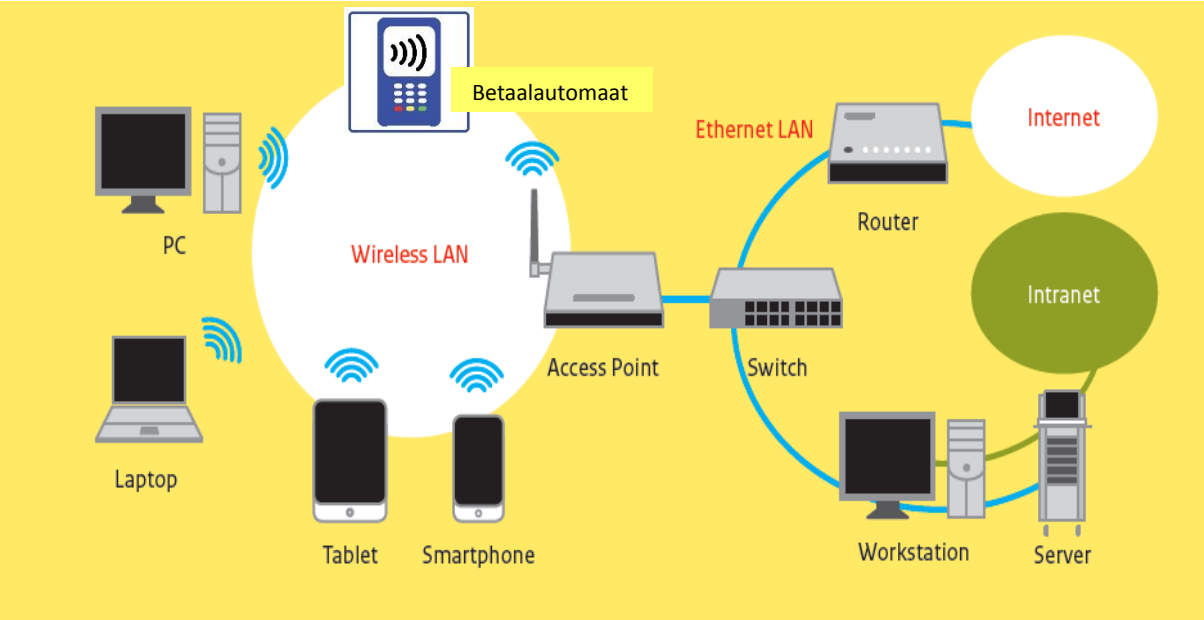
In de meest eenvoudige uitvoering bestaat een WLAN uit een draadloze router die een draadloze verbinding kan maken met een betaalautomaat, een kassasysteem, desktop en ook met smartphones van klanten. In de meest complexe vorm bestaat het WLAN uit heel veel routers, die onderling verbonden zijn en vele soorten diensten kunnen verwerken (videostreaming, “gewoon” internetverkeer, betalingen, IoT-verkeer, …), zoals die in semi-publieke ruimtes worden geïnstalleerd, als voetbalstadions, stations, festivalterreinen, grote winkelcentra e.d.

Om het onderwerp verder in te kaderen, worden hieronder alleen ontwikkelingen beschreven in de Wifi-technologieën. Andere draadloze technologieën die veelvuldig gebruikt worden op de winkellocatie, zoals (Low Energy) Bluetooth en iBeacon blijven buiten beschouwing. Deze technologieën worden overigens niet gebruikt om betaaltransacties af te wikkelen, en zijn ook om die reden niet direct relevant voor dit rapport.

Wifi bestaat uit twee smaken; Wifi dat gebruik maakt van de 2,4 GHz band (smalband) en Wifi dat gebruik maakt van de 5 GHz band (breedband).[1] Voor de retailer lijkt Wifi met Access Points op 5GHz het meest relevant.

[1] Aan het onderscheid tussen Access Points op 2,4 GHz en 5 GHz kan een hele paragraaf gewijd worden. Belangrijk hier is, dat de 5 GHz-technologie een aantal specifieke karakteristieken heeft die relevant zijn voor de retailer. Ten eerste is het bereik van de AP’s veel kleiner. Dat betekent, dat op een winkellocatie eerder gebruik zal moeten worden gemaakt van Wifiversterkers, om het hele vloeroppervlak van de winkel af te dekken. Voordeel van het kleinere bereik is wel, dat het Wifinetwerk lastiger bereikt kan worden buiten de winkel, wat de veiligheid vergroot. Bijkomend voordeel is ook, dat interferentie met Wifinetwerken van winkels in de nabije omgeving veel minder groot is, wat de betrouwbaarheid van het eigen netwerk weer vergroot. Daarnaast is de datasnelheid (bandbreedte) van AP’s op 5 GHz veel groter dan de AP’s op 2,4 GHz. Vanwege deze voordelen en ook vanwege de prijsdaling van de AP’s op 5 GHz, zien we de laatste paar jaar een grote substitutie van 2,4 GHz naar 5 GHz AP’s. Zie hiervoor ook de publicatie van het Agentschap Telecom: https://www.agentschaptelecom.nl/onderwerpen/wifi/nieuws/2017/december/6/wifi-gebruik-5ghz-routers-verdrievoudigd Relevant is hierbij op te merken, dat nog niet alle smartphones 5 GHz ondersteunen. Om een verbinding met een 5 Ghz netwerk te kunnen maken, moet de netwerkkaart van de smartphone geschikt zijn (dual band). Alle smartphones van na 2015 ondersteunen dual band.

In Wifi-terminologie worden de draadloze routers meestal Access Points (AP's) genoemd. Via het AP zijn alle lokale apparaten en dat kan ook een betaalautomaat met kassakoppeling zijn, gekoppeld met "de buitenwereld". Zie ook het onderstaande figuur. Hierin is bovenin een Wifi-betaalautomaat getekend.



Figuur 1: Voorbeeld WLAN Netwerk[2]

Een Wifinetwerk op een winkellocatie zal vaak toegankelijk moeten zijn voor bezoekende consumenten, al dan niet via een toegangscode, maar moet ook door medewerkers van de winkel gebruikt kunnen worden voor toegang tot bedrijfsapplicaties of voor de toegang tot betaalsystemen. Juist vanwege dit multidisciplinair gebruik van het Wifinetwerk zal aan de implementatie en het beheer van een Wifinetwerk op een winkellocatie specifiek aandacht gegeven moeten worden aan een aantal belangrijke punten. Het is duidelijk, dat het gebruik van het Wifinetwerk door eigen personeel strikt gescheiden (fysiek of logisch) dient te zijn van het gebruik door consumenten. Daarbij heeft de afwikkeling van betaaltransacties via het Wifinetwerk nog weer extra aandacht nodig.

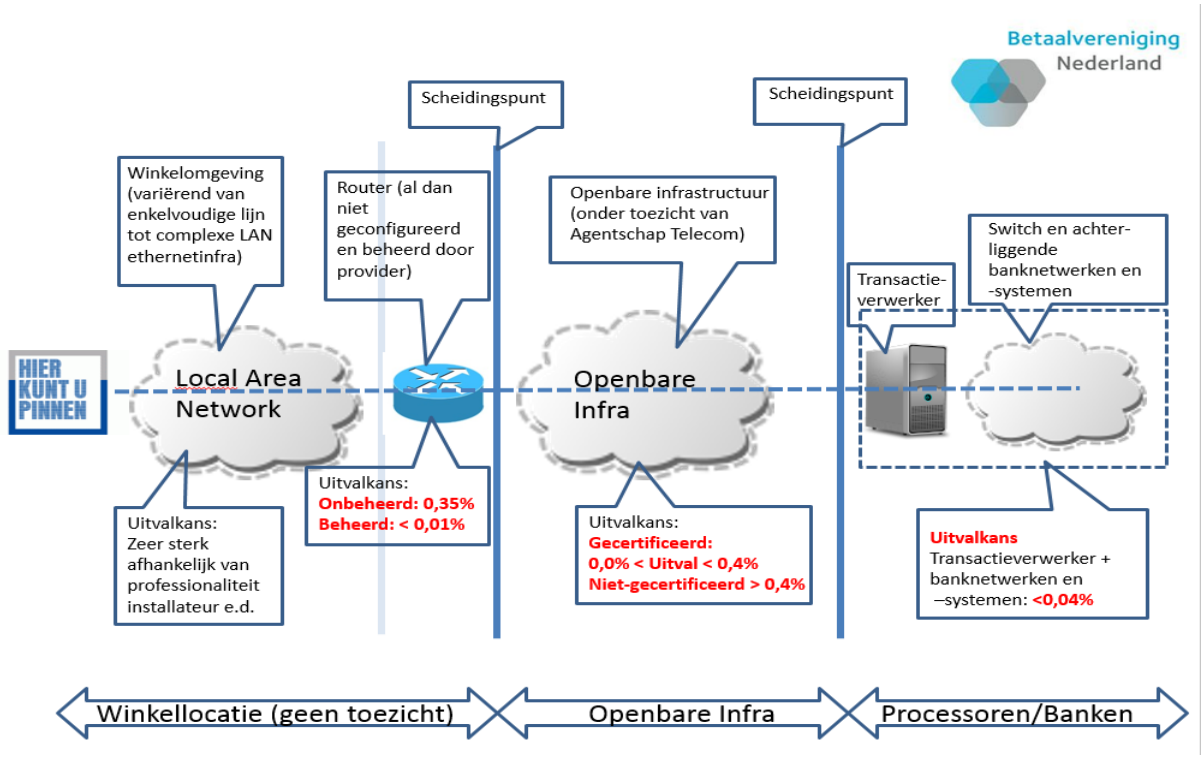
Verschillende publicaties beschrijven welke mogelijkheden Wifinetwerken kunnen geven aan een winkelier. Daarbij worden applicaties beschreven als: Wifitracking, gebruik van beacons en heatmaps, allerlei ander gebruik van Wifi-statistieken, toegang tot winkelapps, … Op al deze mogelijkheden wordt hier niet verder ingegaan. Wel wordt ingegaan op voor de ondernemer relevante aandachtspunten bij de aanleg en inzet van Wifi. Relevant zijn in dit verband de bestaande of toekomstige regelgeving waarmee de ondernemer te maken kan krijgen, de juridische aspecten en de kwaliteit van het Wifinetwerk, die goeddeels wordt bepaald door de kwaliteit van de installatiewerkzaamheden en van het reguliere beheer.

[2] Figuur afkomstig van een publicatie van het NCSC: *Wifi-beveiliging, De onderschatte schakel in netwerkbeveiliging* (oktober 2013). Later zijn nog updates verschenen van delen van dit NCSC-rapport. Ook in de verdere tekst van dit document is gebruik gemaakt van dit NCSC-rapport.

Winkelnetwerk in de totale betaalketen

Uit eerder onderzoek is [3]vastgesteld, dat het betalingsverkeer[4] gevoelig is voor de kwaliteit van het stuk datacominfrastructuur dat zich in de winkel bevindt. Dat is het stuk tussen de betaalautomaat (of een ander apparaat, dat het toegangspunt vormt tot de relevante betaalinfrastructuur) en de (al dan niet draadloze) router die de verbinding met de openbare datacominfrastructuur verzorgt. Zie onderstaande figuur, waarin schematisch de pin-betaalinfrastructuur is weergegeven. Ook worden in de figuur globaal de uitvalkansen gegeven van de verschillende elementen uit die betaalinfra. Aan de linkerkant staat het (W)LAN op de winkellocatie. Om te kunnen garanderen dat betalingen probleemloos gedaan kunnen worden, is het cruciaal, dat dit (W)LAN van goede kwaliteit is.

De figuur heeft betrekking op de situatie, dat de router op de winkellocatie gekoppeld is aan een *vast* netwerk. Dat kan koper zijn, of coax of glas. Een andere mogelijkheid is, dat de betaalautomaat via een *mobiel* netwerk (GSM, UMTS, LTE en straks 5G) is gekoppeld aan de transactieverwerker. Dit is een andere situatie dan de betaalautomaat die middels een Wifinetwerk is gekoppeld aan de transactieverwerker. Enerzijds kan, zeker voor de kleinere retailer, een mobiele oplossing goedkoper zijn dan een Wifi-oplossing. Maar anderzijds kunnen via mobiel minder functionaliteiten worden ondersteund. Bovendien kennen mobiele netwerken, zeker in drukke stedelijk centra, een mindere beschikbaarheid dan vaste aansluitingen. Voor de retailer zal vooral de verhouding prijs/kwaliteit een belangrijke afweging zijn. Mobiele netwerken blijven in dit rapport verder buiten beschouwing.



Figuur 2: Betaalinfrastructuur op een winkellocatie (conceptueel)

[3] Zie o.a. het eindrapport van het onderzoek van McKinsey: *Naar een robuustere Pinketen in Nederland* (oktober 2009) en de MOB-nota van 1 mei 2013, die in de voorjaarsvergadering 2013 van het MOB is besproken. Genoemde onderzoeken zijn ook input geweest voor verbeteracties die door de Stichting Bevorderen Efficiënt Betalen, in het kader van de Nadere Overeenkomst II, zijn/worden uitgevoerd.

[4] In dit document wordt geen onderscheid gemaakt tussen verschillende vormen van betalingen, zoals de consument die doet in de winkel. Het kunnen (debet- of credit)kaartbetalingen zijn, credittransfers, iDEAL, mobiele betalingen, betalingen middels allerlei apps, etc. Voor de kwaliteit van de lokale infrastructuren maakt het niet wezenlijk uit welk betaalproduct door de consument gebruikt wordt. Alle betaaldata moet uiteindelijk via het lokale winkelnetwerk en de openbare netwerken verstuurd worden naar de transactieverwerker.

Aspecten van de kwaliteit van Wifinetwerken

Het implementeren van een Wifinetwerk voor professioneel gebruik op de winkelvloer vereist specialistische kennis. Enerzijds moet het Wifinetwerk alle gewenste functionaliteiten ondersteunen, anderzijds moet een aantal belangrijke risico's ondervangen worden. De risico's zijn te clusteren in de volgende categorieën:

- Beschikbaarheid van het Wifinetwerk;
- Misbruik en fraude;
- Privacy risico's.

Beschikbaarheid

Bij beschikbaarheid van het Wifinetwerk moet gedacht worden aan factoren als robuustheid, storingsgevoeligheid, beschikbare bandbreedte e.d. Een hoge beschikbaarheid kan o.a. gerealiseerd worden door voldoende transmissiecapaciteit van het Wifinetwerk, maar ook door kritische diensten zoals het betalingsverkeer via een aparte poort op het AP af te wikkelen, of door prioriseringsmechanismen voor dit type tijdkritische en fraudegevoelige diensten te implementeren. Hierdoor wordt voorkomen, dat niet-tijdkritische applicaties die veel bandbreedte vergen, andere wel-tijdkritische diensten (zoals betalingen of alarmeringsverkeer) wegdrukken.

Misbruik en fraude

Het grootste gevaar bij draadloze netwerken is dat ongewenst toegang tot het bedrijfsnetwerk wordt verkregen en/of dat de informatie wordt afgeluisterd of gemanipuleerd. De risico's op misbruik zijn groter dan bij vaste 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 AP 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 daar dan ook besmet zijn geraakt met malware. Uit dit risico wordt gelijk duidelijk dat niet alleen het netwerk beveiligd moet worden, maar ook de eigen mobiele apparaten die van het netwerk gebruik maken moeten beveiligd worden. Mobiele apparatuur van consumenten valt buiten de verantwoordelijkheid van de winkelier. Maar het Wifinetwerk dient voldoende robuust te zijn, zodat de performance niet beïnvloed kan worden door de smartphone van de consument. De mate van beveiliging zal per situatie vastgesteld moeten worden op basis van een risicoafweging.

Misbruik en fraude in het betalingsverkeer

Via het lokale Wifinetwerk is het mogelijk om toegang te krijgen tot de betaalinfrastructuren. Voor Pinnen zijn dan de bekende authenticatiemiddelen nodig (bankpas + pincode) nodig. Voor iDEAL, Internetbankieren en Mobiel bankieren zijn de andere, bankspecifieke, authenticatie-*credentials* nodig. Het gebruik van deze authenticatiemiddelen is onafhankelijk van het gebruikte (W)LAN. Het maakt dus niet uit of de betalende consument gebruik maakt van een betaalautomaat dat via een vaste bekabeling is verbonden met een router, of via een mobiel netwerk of via een Wifi-netwerk.

Voor wat betreft iDEAL, IB en MB is de situatie iets anders, wanneer de consument gebruik maakt van een Wifinetwerk op een winkellocatie. In een niet goed beveiligd Wifinetwerk bestaat de mogelijkheid om een frauduleus AP in het Wifinetwerk te plaatsen. Hiermee is het mogelijk om *man-in-the-middle* aanvallen uit te voeren. Het risico hierop is door de banken onderkend, en de inschatting is dat de kans op misbruik door deze aanvalswijze minimaal is. Dat is de reden dat dit risico door de banken vooralsnog is geaccepteerd.
Een andersoortig risico betreft het verzenden van betaalverzoeken van een frauduleuze persoon naar een andere, goedwillende consument. Bij een niet-optimaal afgeschermd Wifinetwerk is het mogelijk dat allerlei persoonsgegevens van goedwillende consumenten bekeken kunnen worden door een hacker. Theoretisch zou de hacker die gegevens kunnen misbruiken om een betaalverzoek te versturen naar de goedwillende maar onoplettende consument. Hoewel ook dit risico zeer beperkt is, en actieve medewerking van het slachtoffer vereist, is zo'n situatie natuurlijk zeer ongewenst. Het belang om het Wifinetwerk goed "dicht" te houden wordt hiermee nog eens benadrukt. Dit komt verderop in dit document nog uitgebreider aan de orde.

Maatregelen

Om de beschikbaarheid van een Wifinetwerk te optimalieren en om misbruik en fraude te minimaliseren, worden allerlei maatregelen genomen. Dat kunnen organisatorische, procedurele, fysieke en technische maatregelen zijn. Onderstaande tabel geeft een voorbeeld van maatregelen voor ieder van deze vier invalshoeken.

1. Organisatorische maatregelen	Voorbeelden: formuleer beleid voor de wijze waarop de organisatie met draadloze netwerken wil omgaan en formuleer beveiligingsbeleid voor Wifi. Zorg ervoor dat de eigen gebruikers zich bewust zijn van de risico's van het gebruik van draadloze netwerken.
2. Procedurele maatregelen	Voorbeelden: beschrijf de procedures voor veilig beheer van de Wifivoorzieningen, inclusief monitoring, controles op functionaliteiten en dekking et cetera.
3. Fysieke maatregelen	Voorbeeld: zorg voor fysieke beveiliging van de Wifi-accesspoints om te voorkomen dat deze kunnen worden misbruikt.
4. Technische maatregelen	In deze categorie vallen alle technische maatregelen, die de maximale beschikbaarheid en minimale misbruik en fraude moeten waarborgen.

De risico's met betrekking tot beschikbaarheid, misbruik en fraude en de maatregelen die genomen kunnen worden om die te minimaliseren, zijn in meer detail beschreven in Bijlage 1.
De robuuste, veilige inrichting en exploitatie van een Wifinetwerk vereist specifieke en specialistische aandacht. In Bijlage 1 worden een aantal handvatten gegeven om deze aspecten gestructureerd aan te pakken. Daarbij is ernaar gestreefd om de belangrijkste aspecten hierbij te benoemen. Er is niet gestreefd naar volledigheid.

Privacyrisico's

Wanneer klanten middels een smartphone contact maken met een Wifinetwerk, worden allerlei persoonsgegevens uitgewisseld tussen het AP en de smartphone. Deze elementen maken, dat een ondernemer die Wifi inzet voor bedrijfsdoeleinden, te maken gaat krijgen met de Wet bescherming persoonsgegevens (Wbp) en straks (vanaf 25 mei 2018) met de Algemene Verordening Gegevensbescherming, de AVG.

Wifi en privacy hebben veel met elkaar te maken. Een smartphone die zich opengesteld heeft voor de ontvangst van Wifi-signalen, zendt permanent zijn eigen, unieke MAC-adres uit. Met dat MAC-adres kan de beheerder van de Wifi-router heel veel. In wezen kan met het MAC-adres een klant gealloceerd worden, kan de ondernemer gebruik maken van Wifi-tracking, maar kan hij ook specifieke informatie naar de bezitter van de smartphone sturen. En wanneer het MAC-adres in een databestand van de ondernemer voorkomt, kan hij die informatie ook *customizen*.

De huidige Wbp geeft aan dat een persoonsgegeven elk gegeven is over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Een telefoonnummer, maar ook een MAC-adres van een smartphone wordt gezien als een persoonsgegeven. Dat betekent, dat een ondernemer die MAC-adressen of telefoonnummers van consumenten verwerkt, rekening moet houden met de Wbp.
Wifi wordt vaak geassocieerd met *tracking*. Winkeliers gebruiken deze methode om te kijken hoe mensen zich door hun winkel bewegen. Onder de AVG is deze manier van volgen alleen toegestaan als mensen toestemming geven of als de gegevens worden geanonimiseerd.
Organisaties die *tracking*-gegevens verzamelen zouden kunnen volstaan met het informeren van mensen en door hen erop te wijzen dat zij hun apparaat uit kunnen zetten als ze niet willen worden gevolgd. De toezichthouders vragen de Europese Commissie te bevorderen dat er een technische standaard voor mobiele apparaten wordt ontwikkeld waarmee mensen automatisch kunnen aangeven niet op deze manier te willen worden gevolgd (*privacy by design* en *privacy by default*).
Factoren die dan relevant worden zijn: *ondubbelzinnige toestemming* van de betrokkene voor het verwerken van de persoonsgegevens, *noodzakelijkheid* (is het verwerken van persoonsgegevens noodzakelijk voor het bereiken van het doel van de onderneming?), *proportionaliteit* (zijn de inbreuken op de belangen van de betrokkenen niet onevenredig in verhouding tot het met de verwerking te dienen doel?), *subsidiariteit* (kan het doel waarvoor de persoonsgegevens worden verwerkt niet op een andere, voor de betrokkenen minder nadelige wijze worden verwezenlijkt?) en *dataminimalisatie* (worden niet meer persoonsgegevens verwerkt dan strikt noodzakelijk is voor de gestelde doelen?).
Met het van kracht worden van de AVG worden bovengenoemde factoren nog verder uitgewerkt. Tevens worden boeteregelingen duidelijk verzwaard en krijgen partijen die persoonsgegevens verwerken te maken met de Wet Datalekken. Sinds 1 januari 2016 geldt een meldplicht voor datalekken. Deze meldplicht houdt in dat organisaties (zowel bedrijven als overheden) direct een melding moeten doen bij de Autoriteit Persoonsgegevens zodra zij een ernstig datalek hebben. En soms moeten zij het datalek ook melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt). De meldplicht datalekken blijft onder de AVG grotendeels hetzelfde.

De AVG stelt wel strengere eisen aan de eigen registratie van de datalekken die zich in een organisatie hebben voorgedaan.[5]

Nog een aanvullende opmerking t.a.v. Wifitracking: naast AVG krijgen we in Nederland ook de maken met de aanstaande nieuwe *Europese ePrivacy act*. Die is in ontwikkeling en zal in de loop van 2018/2019 z'n beslag krijgen. Hij gaat over gebruik van cookies etc., maar ook over Wifitracking. In de concepttekst van deze Act wordt de term 'tracking users' gebruikt (dus technologie onafhankelijk). Waar eerder nog ruimte werd geboden voor tracking zonder toestemming van de eindgebruiker, neigt de nieuwe Act nu naar strengere regels (vooraf toestemming van de klant), in lijn met de AVG.[6] Deze *Europese ePrivacy act* kan op termijn dus gevolgen hebben voor de implementatie en exploitatie van Wifinetwerken.

Tot slot: in Bijlage 3 zijn de belangrijkste vragen geformuleerd waarmee een retailer geconfronteerd kan worden betreffende privacyaspecten. Daarbij zijn ook antwoorden van ICT-jurist Arnoud Engelfriet geformuleerd.

Wifi in het publieke domein

Eerder genoemde aspecten die relevant zijn bij de implementatie en exploitatie van Wifinetwerken in het domein van de retailer, zijn veelal ook relevant voor het publieke domein. Te denken valt hierbij aan bv. Wifinetwerken op universiteitsterreinen, of voor ministeries of andere publieke bestuursorganen. Hiervoor zijn door leveranciers specifieke oplossingen ontwikkeld: Eduroam en , Govroam. In Bijlage 2 worden enkele karakteristieken van deze beide diensten verder uitgewerkt. Tevens wordt daar ingegaan op een dienst die momenteel voor het private domein wordt ontwikkeld: Publicroam.

[5] Verdere uitwerking van alle bovengenoemde privacy-elementen is te vinden op de website van de AP: https://autoriteitpersoonsgegevens.nl/nl. De formele wetteksten zijn hier te vinden: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:NL:PDF

[6] Zie amendement 26 op voorstel van de Europese Commissie op pagina 29 van de concepttekst: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FNONSGML%2BCOMPARL%2BPE-606.011%2B01%2BDOC%2BPDF%2BV0%2F%2FEN)

Bijlage 1: Beschikbaarheid en Veiligheid

Wifi en PCI DSS Compliance

Ondernemers die online betaaldiensten aanbieden aan hun klanten, krijgen te maken met PCI DSS-regelgeving. Dit is een algemene regelgeving, die los staat van hoe een winkelier/ondernemer zijn betaalketen heeft ingericht. Maar de kans dat PCI DSS-regelgeving geraakt wordt is bij het gebruik van Wifi groter dan bij het gebruik van vaste bekabelde netwerken.
PCI DSS staat voor Payment Card Industry Data Security Standard. Dit is een internationale beveiligingsstandaard, opgesteld door de diverse betaalkaartmaatschappijen (zoals Mastercard en Visa). De standaard probeert betaalkaartgegevens te beschermen en zo misbruik van kaartgegevens, en daarmee schade, te voorkomen. PCI DSS stelt eisen aan het verwerken, doorsturen en opslaan van kaartgegevens. In principe moeten alle bedrijven die creditcards en internationale debet kaarten accepteren, voldoen aan het veiligheidsvoorschrift PCI DSS. Schending van de regels kan enorme gevolgen hebben voor de betrokken onderneming.
Wanneer een ondernemer een Wifinetwerk realiseert waarover ook betaaltransacties worden afgewikkeld, heeft hij dus met PCI DSS te maken. En zal hij daarom aanvullende maatregelen moeten nemen om zijn netwerk zodanig te beschermen, dat misbruik en diefstal van kaartgegevens uitgesloten is. Praktisch gesproken betekent dit , dat het Wifinetwerk gesegmenteerd moet worden middels SSID-(Service Set Identifier) technologie. SSID maakt het mogelijk om draadloze computernetwerken van elkaar te scheiden, door elk draadloos netwerk een aparte naam (SSID) te geven. Dat betekent, dat de Wifi-routers zodanig geconfigureerd moeten worden, dat het betaalverkeer op logisch of fysiek niveau volledig is gescheiden van de rest van het Wifi-verkeer, zodat het niet mogelijk is om ongeautoriseerd toegang te krijgen tot dit deel van de Wifi-router.

Relevante aspecten[7]

Het inrichten van een robuust en veilig Wifinetwerk is specifiek en specialistisch werk. Het handhaven van de maximale beschikbaarheid en veiligheid van een Wifinetwerk vereist daarna continue aandacht en zal als de inrichting is afgerond, 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. Keuze van het lokale netwerk op basis van gewenste functionaliteiten en een risicoanalyse
2. Architectuurontwerp
3. Implementatie
4. Beheer & onderhoud
5. Ontmanteling

In de navolgende paragrafen zijn de stappen nader beschreven.

[7] Bij de invulling van deze paragraaf is gebruik gemaakt van het concept, zoals in het eerder genoemde rapport van het NCSC is beschreven.

Vervolgens wordt ingegaan op een aantal specifieke aandachtspunten, die niet altijd even duidelijk zijn te relateren aan bovengenoemde lifecyclefasen:

- Scheiding van netwerken
- Beveiligd koppelvlak
- Sterke versleuteling en authenticatie
- Detectie en Preventie
- Logging en monitoring
- Veranderen van de naam van het Wifinetwerk
- Signaaloptimalisatie
- Accesspoint beveiligen
- Veilig configureren van accesspoints

Beleidsdocument: gewenste functionaliteiten, risicoanalyse en keuze van het Wifinetwerk

Voordat een retailer besluit om een Wifinetwerk te implementeren en exploiteren, zal een beleidsdocument opgesteld dienen te worden. Daarin wordt geformuleerd welke klant- en bedrijfsprocessen ondersteund moeten worden en over welke functionaliteiten het Wifinetwerk dientengevolge moet beschikken. In een beleidsdocument worden ook zaken opgenomen als: wie beslist over het inwerking stellen van maatregelen (voor zover niet automatisch) naar aanleiding van detectie van problemen. Ook zal opgenomen moeten worden wie geïnformeerd moet worden zodra maatregelen (al dan niet automatisch) in werking treden.
In elke organisatie, dus ook in de winkelorganisatie, is het nodig om, voordat men besluit tot het invoeren van Wifi, een inventarisatie te maken van de gewenste functionaliteiten die ondersteund moeten worden, de gewenste kwaliteit (bv. in termen van beschikbaarheid) van de oplossing, kosten, etc., en daarbij een risicoanalyse uit te voeren. Uit de risicoanalyse volgt onder meer in welke mate de toegang tot (bepaalde categorieën) informatie moet worden afgeschermd, of dat bepaalde netwerkelementen dubbel uitgevoerd moeten worden. Uitgaande van het risicoprofiel besluit een organisatie of en in welke vorm Wifi wordt toegepast. Hiervoor moet een antwoord worden geformuleerd op onder meer de volgende vragen:

- Welke eisen worden gesteld aan de beschikbaarheid en de maximale storingsduur?
- Welke gebruikersgroepen worden (zowel in- als extern) onderkend en welke faciliteiten wil men deze groepen bieden?
- Met welke mobiele apparaten wordt toegang tot het Wifinetwerk toegestaan?

Het is zinvol om tijdens dit vooronderzoek, wat leidt tot een beleidsdocument, al gesprekken te hebben met één of meerdere leveranciers/installateurs.

Architectuurontwerp

Als besloten is op welke wijze Wifi in de winkelorganisatie wordt opgenomen, moet de juiste balans worden gevonden tussen beveiliging en gebruik. Een goed architectuurontwerp is daarbij noodzakelijk. 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. Concreet kan dit betekenen:

- Pas het 'security by design' principe toe, security is hierbij integraal onderdeel van het ontwerp van het Wifinetwerk;
- Maak, zeker bij een grote winkelorganisatie, gebruik van apparatuur en software voor grootschalig zakelijk gebruik. Dus geen consumentenproducten. Dit zorgt voor veilige, schaalbare en beheersbare oplossingen in een complexe infrastructuur.
- Omdat op het Wifinetwerk wellicht ook beveiligingsapparatuur (brandalarm, inbraakalarm, …) wordt aangesloten, is het zinvol om de specifieke eisen hiervoor in het architectuurontwerp mee te nemen.

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:

- 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;
- Het beheer van de Wifi-infrastructuur is professioneel ingericht en de beheerders zijn opgeleid om hiermee te werken.

Vanwege de vele specifieke aandachtspunten, zullen de installatiewerkzaamheden in het algemeen niet door de retailer zelf worden gedaan, maar zullen die worden uitbesteed aan een daartoe gespecialiseerd installatiebedrijf. Gespecialiseerde installatiebedrijven zijn vaak aangesloten bij de koepelorganisatie voor installateurs, Uneto-VNI. Ook kan een installatiebedrijf geselecteerd worden dat door Betaalvereniging Nederland is beoordeeld op kwaliteit van installatiewerkzaamheden[8]. Dat geeft enige garantie, dat installatiewerkzaamheden volgens *best practices* worden uitgevoerd. Wanneer gebruik gemaakt wordt van een dergelijke installateur wordt ook de garantie verstrekt, dat het opgeleverde Wifinetwerk voldoet aan de eisen van de alarmeringsbranche, zodat ook alarmeringsapparatuur kan worden aangesloten op het Wifinetwerk. Er zijn vanzelfsprekend ook andere installateurs die kwalitatief goed installatiewerk verrichten. In zo'n geval is het vragen om èn het checken van een referentielijst zinvol.
Er bestaan geen algemeen erkende installatierichtlijnen wanneer het om de implementatie van Wifinetwerken gaat. In NEN-verband wordt wel aan normering gewerkt, en in de loop van 2018 zal daartoe de NTA8085 verschijnen. Maar naar verwachting zal het daarna nog meerdere jaren kosten voordat die NTA is uitgewerkt tot een volledige NEN-standaard.
Samenvattend betekent dit, dat de implementatiewerkzaamheden het beste kunnen worden uitbesteed aan een installatiebedrijf dat gespecialiseerd is in dit soort werk, en ook is aangesloten bij een koepelorganisatie. Er bestaan echter (nog) geen door de markt erkende kwaliteitskeurmerken.

Kwaliteit van bekabeling en koppelingen tussen netwerkelementen

Dit is een algemeen aandachtspunt. Kwalitatief goede bekabeling en koppelingen bepalen voor een belangrijk deel de beschikbaarheid van het eindresultaat: het integrale Wifinetwerk in de winkel. Voor bekabeling en koppelingen bestaan normen, die bij voorkeur gebruikt dienen te worden. Ook de feitelijke installatiewerkzaamheden dienen bij voorkeur door een gecertificeerde installateur, of een bekende telecomprovider verricht te worden. Certificeringen die hier relevant zijn, zijn

[8] Zie: https://www.betaalvereniging.nl/wp-content/uploads/breedband_installateurs_pinnen.pdf

bijvoorbeeld SECT-certificaten, terwijl grotere, professionele opleidingsinstituten, opleiden verzorgen tot door de markt erkende Wifi-certificaten.

Beheer en onderhoud

Het is van belang om de implementatiewerkzaamheden en het beheer en onderhoud van een Wifinetwerk niet te verwarren. Het is in de praktijk heel wel mogelijk, dat het installatiewerk geheel volgens het architectuurontwerp (zie boven) wordt gerealiseerd, maar dat omtrent beheer en onderhoud niets is afgesproken. Vanzelfsprekend is dit een ongewenste situatie. Het beheer en onderhoud vormen belangrijke factoren in de betrouwbaarheid van een Wifinetwerk. Het beheer en onderhoud moeten ervoor zorgen dat de maatregelen goed blijven functioneren. Hierbij is onderscheid te maken tussen continue activiteiten en periodieke activiteiten.

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 (bijvoorbeeld maandelijks; frequentie is o.a. afhankelijk van het aantal inlogpogingen op het Wifinetwerk en het aantal eigen gebruikers) om pogingen tot misbruik te herkennen en waar nodig maatregelen te treffen. Logging geeft ook inzicht in mogelijke uitval van het Wifinetwerk;
- 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;
- Controleer het Wifinetwerk op aspecten als continue beschikbaarheid, bandbreedte (snelheid van het Wifinetwerk), de segmentering etc;
- Controleer of alle gewenste functionaliteiten voor de consument nog op het gewenste niveau functioneren. Dit kan gebeuren door iemand in de rol van consument alle functionaliteiten te laten testen.

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 eigen gebruikers overeenkomt met de lijst gebruikers die daadwerkelijk toegang heeft tot het Wifinetwerk;
- 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 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 (zie verderop in deze bijlage).

Beheer en onderhoud van een Wifinetwerk vergt heel veel kennis en aandacht. In hoeverre bovenstaande activiteiten door een eigen organisatie kunnen worden uitgevoerd hangt vanzelfsprekend af van het kennisniveau van de organisatie. Vaak kan het beheer worden uitgevoerd door een daartoe gespecialiseerd ICT-bedrijf. Er bestaan echter geen specifieke normeringen of kwaliteitsgaranties op dit vlak. Wanneer activiteiten worden uitbesteed, dienen bovengenoemde aandachtspunten allemaal afgedekt te zijn.

Accesspoint opnemen in beheerprocessen

Een Wifi-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 AP op te nemen in een aantal bedrijfsprocessen, zoals patch-, wijzigings- en configuratiemanagement. Patchmanagement zorgt ervoor dat de accesspoints regelmatig worden voorzien van firmware-updates. 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.

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.

- 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.

Hieronder worden een aantal aspecten beschreven, die relevant zijn bij het ontwerpen, implementeren en onderhouden van een Wifinetwerk op een winkellocatie, waarbij de focus ligt op veiligheidsaspecten.

Scheiding van netwerken

Het Wifinetwerk moet, net zoals het internet, worden beschouwd als een *open* netwerk, en is dus kwetsbaar voor aanvallen van buitenaf. Om het interne winkelbedrijfsnetwerk hiertegen te beveiligen moeten deze netwerken van elkaar gescheiden zijn. Dat kan op twee manieren.

1. *Fysieke scheiding Wifinetwerk en bedraad netwerk*
   Om zeker te zijn dat het Wifinetwerk en het bedrade 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 de zekerste 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.

2. *Segmentering van het netwerk*
   Een variant op de fysieke scheiding van het Wifinetwerk en bedrade 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.

Beveiligd koppelvlak

Als er een koppeling nodig is tussen het Wifinetwerk en het bedrijfsnetwerk, dan moet de onderlinge communicatie via een beveiligd koppelvlak verlopen. De koppeling naar het internet zou ook via een beveiligd koppelvlak moeten lopen, in verband met aanvallen vanaf of naar het internet.

Sterke versleuteling en authenticatie

Geïmplementeerde beveiligingsprotocollen moeten een voldoende beveiliging bieden. De onderliggende versleutelmethoden hebben in de regel een beperkte houdbaarheid omdat deze met de toenemende beschikbaarheid van rekenkracht op termijn kunnen worden gekraakt.
WEP (Wired Equivalent Privacy) was de eerste versleutelmethode die werd aangeboden voor Wifi apparatuur. WEP is tegenwoordig binnen 1 minuut te kraken; WEP is daarom 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. WPA2 is de vernieuwde versie van WPA en maakt gebruik van een veel sterker versleutelprotocol. Waar mogelijk dient WPA2 gekozen te worden.[9]

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 WPA2, 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.[10]
Door periodiek het Wifinetwerk te analyseren/scannen kunnen deze problemen worden ontdekt. Belangrijke aandachtspunten hierbij zijn:

---

[9] Eind 2017 hebben Belgische onderzoekers een kwetsbaarheid in WPA2 aangetoond ("Krack-aanval"). Dit onderzoek heeft veel publiciteit gekregen, omdat de indruk werd gewekt, dat door de kwetsbaarheid WPA2 niet langer bruikbaar zou zijn. Later hebben de onderzoekers hun resultaten flink genuanceerd. Met enkele eenvoudige maatregelen is WPA2 nog steeds toepasbaar. Meer informatie hierover: https://www.security.nl/posting/535615/KRACK-aanval+op+WPA2-beveiliging+wifi-netwerken%3A+Een+Q%26A

[10] Hier moet het risico op Man-in-the-middle attack worden genoemd. Een man-in-the-middle-aanval (MITM-aanval) is een aanval waarbij informatie tussen twee communicerende partijen onderschept wordt zonder dat beide partijen daar weet van hebben. Hierbij bevindt de computer van de aanvaller zich tussen de twee communicerende partijen. De berichten kunnen daarbij mogelijk gelezen en veranderd worden. Ook kunnen berichten worden verzonden die niet door de andere partij zijn geschreven. Bij een MITM-aanval kan bv. een zgn. PineApple gebruikt worden. Zie bijvoorbeeld: *https://www.wifipineapple.com/*

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

Wireless Intrusion Detection System/Wireless Intrusion Prevention 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 IDS.
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.
Een WIDS/WIPS is een substantiële investering. Daarnaast gaan de kosten zeker niet alleen 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 of IPS zal de stap naar een WIDS of WIPS minder groot zijn.

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. Vanzelf-sprekend moeten dan de logbestanden op een andere plaats worden opgeslagen dan op het AP zèlf. Zodra het AP gecompromitteerd is, zou de aanvaller als eerste zijn sporen willen wissen. Opslaan op een externe/andere locatie is weer een extra beveiligingsobstakel die hij dan moet doorbreken.

Juridische consequenties loggen en monitoren van netwerkverkeer
Wanneer de eigenaar/beheerder van het Wifinetwerk netwerkverkeer gaat loggen, loopt hij al heel snel tegen de Wbp/AVG aan. Het netwerkverkeer 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 privacy-inbreuk 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.

Veranderen van de naam van het Wifinetwerk

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 één 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.
De standaard ingestelde SSID die het accesspoint in de fabriek heeft gekregen moet bij installatie worden veranderd. Er staan op het internet lijsten van merken accesspoints met hun bijbehorende standaardwaarde voor de SSID en wachtwoord. 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 winkel) kan vanuit het oogpunt van gebruikersgemak veel waarde hebben, terwijl de beveiliging gegarandeerd wordt door in het SSID op geen enkele manier melding te maken van het merk van het accesspoint.

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. 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 mogelijk ongewenste uitbreiding zouden kunnen veroorzaken van het dekkingsgebied.
Overigens leidt deze maatregel op zijn best tot een enigszins verminderd risico. Kwaadwillenden kunnen, indien de ondernemer het zendvermogen van de Wifi-router verlaagt, gebruik maken van een gevoelige antenne om het signaal toch te ontvangen. Indien absoluut geen straling naar buiten mag komen zijn er speciale oplossingen denkbaar.

Niet-bedoeld gebruik van Wifinetwerk

In de praktijk blijkt het voor te komen, dat Wifinetwerken, waarvan de dekking zich uitstrekt tot buiten de feitelijke winkellocatie, gebruikt worden door ongewenste personen, om zo gratis toegang tot internet te krijgen. Vanzelfsprekend is dat niet de bedoeling van de retailer, omdat het hem netwerkcapaciteit kost. Voor de retailer zal het niet direct juridische problemen opleveren, dat bv. allerlei “verkeerde” websites bezocht worden. Maar er zijn voldoende redenen om dit soort misbruik te willen minimaliseren. De eenvoudigste oplossing is er voor te zorgen, dat de dekking van het Wifinetwerk zo strak mogelijk afgebakend is. Daarnaast is het afsluiten van het Wifinetwerk buiten winkelopenstellingstijden een eenvoudige en doeltreffende oplossing.

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 ze 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.

Veilig configureren 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. Dit is een belangrijk aandachtspunt tijdens de initiële installatie van het Wifinetwerk.[11]

[11] Een mogelijk risico dat hier genoemd kan worden is de zgn. WPS-aanval. WPS-staat voor 'Wifi Protected Setup' en is een methode om gemakkelijk apparaten met elkaar te verbinden via Wifi. De technologie geeft in veel routers beveiligingsproblemen en kan relatief eenvoudig gekraakt worden. Een WPS-aanval is een aanval die misbruik maakt van een kwetsbaarheid op AP's. Hiermee zijn ook beveiligingssleutels van WPA2 beveiligde netwerken te achterhalen. Aanbevolen wordt dan ook, om WPS standaard uit te zetten.
Zie achter deze link: *http://archive.hack.lu/2014/Hacklu2014_offline_bruteforce_attack_on_wps.pdf* .

Bijlage 2: Wifinetwerken in het publieke, semi-publieke en private domein (Eduroam, Govroam en Publicroam)

Retailers die Wifi aanbieden hebben te maken met vergelijkbare problemen als onderwijs-instellingen en overheden. In die sectoren wordt breed gebruik gemaakt van gestandaardiseerde Wifi-roamingdiensten: *eduroam* voor het onderwijs en *govroam* voor de overheid. Deze diensten vergroten de veiligheid en met name ook het gemak voor de eindgebruiker. Alle geregistreerde studenten en alle geregistreerde ambtenaren kunnen, waar ook in Nederland, inloggen op Wifinetwerken, die volgens het concept van *eduroam* of *govroam* zijn ingericht. Alle aspecten m.b.t. veiligheid, beschikbaarheid en privacy zijn centraal geïmplementeerd.
Omdat *eduroam* en *govroam* alleen beschikbaar zijn voor onderwijs en overheid, wordt momenteel een nieuwe dienst ontwikkeld, *publicroam,* voor gebruik in openbare Wifi-gastnetwerken (beschikbaar voor zowel publieke als private partijen).

Het concept achter de beide diensten *eduroam* en *govroam* kan zinvol zijn voor de retail. Om deze reden wordt in deze bijlage nader ingegaan op deze Wifidiensten.

Hoe werkt het?
De diensten werken op basis van een netwerk van gekoppelde RADIUS-servers die authenticatieverzoeken routeren. Een organisatie die deelneemt aan *eduroam, govroam* of *publicroam* koppelt haar Wifinetwerk aan een centrale radius-server. Wanneer een eindgebruiker zich aanmeldt, wordt aan de hand van gebruikersnaam/wachtwoord gecontroleerd of hij recht heeft op toegang tot het Wifinetwerk. Bij *eduroam* en *govroam* worden deze inloggegevens (ID) verstrekt door de organisatie waar men werkt of studeert. Bij *publicroam* gebeurt dit via een SMS-dienst. Organisaties die de roamingdiensten afnemen, houden hun netwerken in eigen beheer. De diensten worden op een onafhankelijke manier aangeboden, separaat van telecomaanbieders. Ze zijn een toevoeging aan een bestaand Wifinetwerk.

Gemak
Een belangrijk voordeel voor gebruikers is het gemak. Na de eerste keer aanmelden kunnen zij veilig en snel online bij alle deelnemende organisaties. Dus zonder steeds opnieuw in te loggen. Dit draagt bij aan de gastvrijheid. Een apparaat gaat direct online op alle locaties waar één van de Wifinetwerken wordt aangeboden. Eindgebruikers hoeven niet meer te zoeken naar een Wifinetwerk en de wijze van aanmelden.

Bewezen technologie
De onderliggende technologie is uitgebreid getest op veiligheid en het wordt positief beoordeeld door eindgebruikers. *Eduroam* bestaat al bijna 15 jaar, het is wereldwijd in gebruik bij onderwijs- en onderzoeksinstellingen en heeft ruim 20 miljoen eindgebruikers per dag. *Govroam* is in Nederland in gebruik bij ruim 200 overheidsorganisaties in Nederland, waaronder bijna alle ministeries, de belastingdienst, vele gemeenten en waterschappen. *Eduroam* is ontwikkeld door SURFnet, een Nederlandse telecomspecialist, die gespecialiseerd is in het ontwikkelen van telecomapplicaties voor het (hoger) onderwijs.

Veiligheid en privacy

De roamingdiensten zijn ontwikkeld vanuit de principes ‘security by design’ en ‘privacy by design’. Ze maken gebruik van WPA2-Enterprise (sterke versleuteling en authenticatie). Door centrale logging en monitoring wordt de veiligheid vergroot. De diensten werken vanuit een geüniformeerd privacy kader waarmee de deelnemende organisaties voldoen aan de eisen van de Wbp/AVG. De organisatie hoeven hier dus niet afzonderlijk invulling aan te geven.

Bovengenoemde aspecten maken het zinvol om ontwikkelingen op dit vlak, specifiek van de nieuwe dienst *publicroam*, actief te blijven volgen. Wellicht kunnen winkelcentra, maar ook grote winkelketens het concept gebruiken, teneinde Wifinetwerken en de functionaliteiten daarvan verregaand te standaardiseren en de veiligheid en privacy centraal te implementeren.

Bijlage 3: Korte Q&A betreffende privacy[12]

In deze bijlage zijn de belangrijkste vragen geformuleerd waarmee een retailer geconfronteerd kan worden betreffende privacyaspecten. Daarbij zijn ook antwoorden van ICT-jurist Arnoud Engelfriet, die een zekere autoriteit heeft in dit werkveld, geformuleerd.

Vraag: Is een ondernemer verantwoordelijk en aansprakelijk voor wat consumenten doen op zijn Wifinetwerk?
Antwoord: wie de dienst internettoegang aanbiedt, is niet aansprakelijk voor de inhoud of handelingen die over die internettoegang plaatsvinden. Dat staat in de wet (art. 6:196c BW) en is de basis waarom partijen als Ziggo of XS4All niet elke dag aansprakelijk worden gesteld voor klantgedrag. In de wet staat niet dat dit beperkt is tot bedrijven die tegen betaling internet aanbieden. Daarom gelden deze regels ook voor particulieren.
Een aanbieder van internettoegang hoeft geen informatie te loggen. De aanbieder moet gegevens bewaren die hij kreeg in het kader van zijn bedrijfsvoering. Had de aanbieder bijvoorbeeld geen namen en adressen nodig voor zijn bedrijfsvoering (internet via prepaidkaart) dan was dat goed. Maar had de Wifi-aanbieder die namen wel (bv. uit de bankoverschrijvingen) dan moet hij dat bewaren.
Natuurlijk kan de Wifi-aanbieder in de praktijk de nodige overlast krijgen van mensen die de verbinding dichttrekken of van wangedrag bij sites die het IP-adres van de aanbieder een blokkade opleveren. Ook kan het gebeuren dat een politieteam aan de deur komt omdat via het Wifinetwerk wellicht illegale activiteiten zijn verricht. Maar aansprakelijk hiervoor is de Wifi-aanbieder dus niet.

Vraag: Welke regels gelden er, wanneer een ondernemer gratis internet via Wifi wil aanbieden aan consumenten?
Antwoord: Gratis internet (via Wifi) aanbieden is zo'n onderwerp waar vele mythes over leven. Vaak wordt een bezoeker gedwongen om een vinkje te plaatsen voordat hij het internet op kan. Daarmee worden gebruiksvoorwaarden opgelegd, maar dat gaat bijna altijd mis: dat is alleen rechtsgeldig als de bezoeker die voorwaarden kan ópslaan voordat hij ze accordeert. En meestal staan ze in een scrolvenster, en de consument kan daaruit niets opslaan. Dat vinkje voegt juridisch niets toe, en ook de daarbij gestelde gebruiksvoorwaarden zijn vaak onzinnig.
Wie internet aanbiedt, is niet aansprakelijk voor wat gebruikers/bezoekers doen. Dat geldt voor de grote professionele aanbieders als UPC, Ziggo en KPN, maar ook voor een café of bedrijf dat een gastennetwerk opzet. En daarvoor hoeven bezoekers geen disclaimer te accorderen, dit staat gewoon in de wet (art. 6:196c BW).
Een 'kleine' aanbieder zoals café, bedrijf of winkel hoeft zich niet bij de OPTA of Agentschap Telecom te laten registreren. Wel bestaat de plicht om internet netneutraal aan te bieden; de aanbieder mag dus niet bv. bepaalde websites blokkeren.
Ook hoeft de aanbieder zijn klanten niet te kunnen identificeren, het is toegestaan anoniem internettoegang aan te bieden. Maar ook dat maakt de aanbieder niet aansprakelijk; wel komt Justitie natuurlijk bij hem uit als er problemen zijn maar als hij kan bewijzen dat het een anonieme bezoeker was dan wordt hij verder niet vervolgd (art. 54a Sr en 6:196c BW).

[12] Teksten zijn o.a. gebaseerd op informatie van de ICT-jurist Arnoud Engelfriet (partner van juridisch adviesbureau ICTRecht) die gepubliceerd is op de website Security.nl.

Monitoren van het verkeer mag maar de aanbieder moet rekening houden met de privacy van de bezoekers. Diepgaand monitoren mag alleen met voorafgaande aparte toestemming (dus niet verstopt in de gebruiksvoorwaarden) en moet gericht zijn op een legitiem doel.

Vraag: Is het toegestaan om te meten welke draadloze netwerken er in de buurt zijn? En als deze niet beveiligd zijn, mag iemand dan het dataverkeer daarvan opnemen en analyseren?
Antwoord: Het ontvangen van vrije signalen uit de ether is niet verboden, tenzij je een 'bijzondere inspanning' moet leveren om de signalen te kunnen interpreteren. Onderdeel van het grondrecht vrije meningsuiting is namelijk het mogen vergaren van informatie uit openbare bronnen. Zo is het bijvoorbeeld legaal om mee te luisteren met de politieradio via een scanner. De Hoge Raad oordeelde in 2008 echter dat het gebruik van een snelheidsradardetector niet via dit grondrecht gerechtvaardigd kon worden, omdat radargolven 'geen kennis of gedachten overbrengen', oftewel geen mening of informatie bevatten die onder dit grondrecht vallen.
Als iemand dus alleen maar opneemt wat een netwerkzender zelf uitzendt, en niets bijzonders doet (zoals WPA encryptie kraken of *spoofen* van MAC-adressen) dan handelt hij legaal. Het scannen naar beschikbare Wifinetwerken valt dus onder de uitzondering van vrije signalen. Een computer met Wifi-antenne is gewoon een radio-ontvanger die informatie analyseert en is dus geen niet-toegestaan decodeerapparaat.
Het analyseren van het dataverkeer zelf is riskanter. Het hangt af van het doel dat hiermee bereikt moet worden. Als het gaat om vrije nieuwsgaring is veel toegestaan. Zolang niet geciteerd wordt uit private berichten en mensen niet geïdentificeerd worden, lijkt het legaal.

Bijlage 4: Checklist voor de individuele retailer

Een retailer die op zijn winkellocatie een Wifinetwerk voor zichzelf en voor zijn klanten wil aanleggen, moet rekening houden met een aantal aandachtspunten. Die zijn te clusteren in drie categorieën.

1. Vooronderzoek
2. Installatie
3. Onderhoud

Ad 1: Vooronderzoek

- Stel een beleidsdocument op. Daarin moeten zaken zijn opgenomen als: welke functionaliteiten moeten worden ondersteund, draaien ook eigen bedrijfsprocessen op het netwerk, zijn eigen specialisten in dienst of moet alles (installatie/exploitatie) worden uitbesteed, welke beschikbaarheid en maximale storingsduur worden geëist, wordt ook betalingsverkeer afgewikkeld over het Wifinetwerk, … In een beleidsdocument moet ook opgenomen worden wie beslist over het inwerking stellen van maatregelen (voor zover niet automatisch) naar aanleiding van detectie van problemen. Ook zal opgenomen moeten worden wie geïnformeerd moet worden zodra maatregelen (al dan niet automatisch) in werking treden.
- Bij de exploitatie van een Wifinetwerk krijgt de retailer per definitie te maken met de Algemene Verordening Gegevensbescherming (AVG), die per 25 mei rechtsgeldig wordt. Daarom zal in het vooronderzoek nadrukkelijk ook aandacht besteed dienen te worden aan juridische en privacyaspecten. Welke persoonsgegevens zullen via het Wifinetwerk worden verzameld en verwerkt, hoe worden persoonsgegevens opgeslagen, is de hoeveelheid persoonsgegevens proportioneel met het doel waarvoor ze gebruikt worden etc.

  Het is zinvol om tijdens dit vooronderzoek al gesprekken te hebben met één of meerdere leveranciers/installateurs.

Ad 2: Installatie

- Installeer heldere netwerkarchitectuur en leg die vast in een netwerkadministratie
- Gebruik geen consumentenapparatuur
- Plaats de Wifirouter buiten het zicht
- Gebruik gecertifieerde bekabeling en koppelingen tussen diverse netwerkcomponenten. Doe daarbij navraag bij de installateur
- Wijzig bij installatie alle wachtwoorden
- Installeer bij voorkeur een Wireless Intrusion Detection/Prevention System

Ad 3: Beheer en Onderhoud

- Zorg voor voldoende kennis in de eigen organisatie, zodat elementaire activiteiten (configuratie van poorten, resetten naar bedrijfsinstellingen, bijhouden netwerkadministratie, …) aan het netwerk in eigen beheer kunnen worden gedaan
- Hou een nauwkeurige netwerkadministratie bij
- Controleer Wifinetwerk regelmatig op functionaliteiten en dekking

- Beschrijf richtlijnen, waar het eigen personeel zich aan dient te houden
- Installeer detectiesystemen (WIDS en/of WIPS). Controleer deze regelmatig op functionaliteit, controleer regelmatig de logging. Onderneem actie wanneer onregelmatigheden worden geconstateerd
- Indien bovengenoemde activiteiten niet in eigen beheer worden uitgevoerd, sluit een heldere SLA af met een partij, die dit allemaal afdekt

Uit bovenstaande aandachtspunten blijkt, dat installatie, beheer en onderhoud van een Wifinetwerk heel veel kennis en aandacht vergt. In hoeverre bovenstaande activiteiten door een eigen organisatie kunnen worden uitgevoerd hangt vanzelfsprekend af van het kennisniveau van de organisatie. Vaak kan installatie, beheer en onderhoud worden uitgevoerd door een daartoe gespecialiseerd ICT-bedrijf. Er bestaan echter geen specifieke normeringen of kwaliteitsgaranties op dit vlak. Wanneer activiteiten worden uitbesteed, dienen bovengenoemde aandachtspunten allemaal afgedekt te zijn. Het is daarbij zinvol om een installatiebedrijf in te schakelen, dat is aangesloten bij een brancheorganisatie als Uneto-VNI, of dat door Betaalvereniging Nederland is beoordeeld op kwaliteit van installatiewerkzaamheden[13]. Dat geeft enige zekerheid, dat werkzaamheden volgens *best practices* worden uitgevoerd.

[13] Zie: https://www.betaalvereniging.nl/wp-content/uploads/breedband_installateurs_pinnen.pdf