stn Telecom & Internet

sTN Whitepaper

DECEMBER 2016

Wifi zonder problemen.

Hoe zet u een goed, veilig en betrouwbaar draadloos netwerk op?

Managementsamenvatting

Draadloze of wifi-netwerken blijven zonder periodieke aandacht niet optimaal werken. Een draadloos netwerk is immers onderdeel van een dynamische omgeving. Storende elementen voor het netwerk komen en gaan, maar ook het gebruik van netwerk door de werknemers verandert in de loop van de tijd.

Door permanent, of op zijn minst regelmatig, het gebruik en de prestaties van het netwerk in kaart te brengen, kunnen problemen worden voorkomen. Daarmee voorkomt u frustraties bij de werknemers en verlies aan productiviteit. Maar een goed ingericht netwerk kan ook zorgen voor nieuwe inkomstenstromen. In deze whitepaper leest u waar u op moet letten.

Inleiding

Een draadloos (wifi) bedrijfsnetwerk; het lijkt al zo gewoon als elektriciteit uit de muur en water uit de kraan. Toch worstelen veel organisaties met de prestaties van hun wifi-netwerk.

Ook goedwerkende wifi-netwerken kampen na verloop van tijd met teruglopende prestaties. Het wordt dan

ook steeds drukker op netwerken. Werknemers hebben niet meer alleen een laptop maar ook mobieltjes, tablets en andere draadloze apparatuur zoals wifi-gebaseerde 'vaste' telefoons die ze tijdens het werk moeten of willen gebruiken.

Leeswijzer

Het hoofdstuk **'Problemen voorkomen'** maakt duidelijk dat het inrichten van een draadloos netwerk geen kwestie is van aanschaffen en aansluiten.

Het hoofdstuk **'Dekking'** benadrukt het belang van een dekkingsplan met goede onderbouwing. Het hoofdstuk 'Apparatuurkeuze' gaat in op de aandachtspunten die van belang zijn in het overleg met de leverancier.

Het hoofdstuk **'Storingen en kanaalkeuze'** demonstreert dat een eenmaal aangelegd netwerk niet vanzelf probleemloos blijft functioneren. De relatief nieuwe 5 GHz-frequentieband biedt 'lucht'.

Het hoofdstuk **'Meten is weten'** behandelt het belang van monitoringsoftware. Niet alleen om de Quality of Service te bewaken, maar ook als onderdeel van de beveiliging.

Het hoofdstuk **'Bedrade netwerk'** laat zien dat een draadloos netwerk eigenlijk maar voor een deel zijn naam eer aan doet. Veel belangrijke overwegingen hebben juist te maken met keuzes in het bedrade deel van het netwerk.

Het hoofdstuk **'Beveiliging'** vraagt aandacht voor een aantal essentiële aandachtspunten met betrekking tot de bescherming van bedrijfsdata en privacygevoelige gegevens.

Het hoofdstuk **'Voordelen benutten'** wijst op mogelijkheden die veel organisaties vergeten: Het netwerk kan een rol spelen in marketing en sales.

Het hoofdstuk **'Wie weet er meer'** verwijst naar de mogelijkheden het beheer van het bedrijfsnetwerk volledig aan een externe partij uit te besteden.

Inhoudsopgave

Maar ook het gebruik van het netwerk verandert. Real time-applicaties zoals video vergen meer capaciteit. Apps op smartphones en tablets starten vaak hun updateroutines zodra ze verbinding met een wifi-netwerk signaleren.

Door een combinatie van deze factoren ontstaan makkelijk problemen met de prestaties van het netwerk. Het aanmelden verloopt moeizaam en de programma's reageren niet snel genoeg. Het gevolg is frustratie bij werknemers of gasten en verlies aan productiviteit. Een suboptimaal ingericht netwerk kan ook makkelijk een beveiligingsrisico opleveren. Bedrijfsdata komen onbedoeld via het draadloos netwerk terecht bij onbevoegden of, erger, worden doelbewust ontvreemd door kwaadwillenden.

Tenslotte vergeten veel organisaties dat het draadloos netwerk ook mogelijkheden biedt voor marketing- en upsell-activiteiten. Maar daar moet de infrastructuur wel goed op worden ingericht.

Aandacht voor uw wifi-netwerk loont dus. Niet alleen om te voorkomen dat het een kostenpost wordt maar ook om het in te zetten voor het bereiken van de bedrijfsdoelen. In deze whitepaper staat een aantal belangrijke aandachtspunten op een rij.

Problemen voorkomen

Waarom is het zo lastig voor de meeste organisaties hun wifi op orde te krijgen? Het probleem is dat het inrichten geen kwestie is van apparatuur kopen, aansluiten en het werkt. Een optimale dekking vraagt om een goed gefundeerd plan. Bovendien blijft een eenmaal ingericht netwerk aandacht vragen. Het netwerk is immers onderdeel van een omgeving die niet constant is. Ruimtes worden op een andere manier gebruikt, door meer, of juist minder gebruikers. Het verkeer over het netwerk verandert van intensiteit. Of de behoefte aan quality of service neemt toe door het gebruik van toepassingen die geen vertraging verdragen, zoals spraak en video. Elementen die makkelijk storing veroorzaken - metalen kasten bijvoorbeeld - worden in de ruimten gebracht of worden verplaatst.

Experts omschreven het inrichten van een wifi-netwerk wel als "meer een 'kunst' en een 'gevoel' dan als een exacte wetenschap". Gelukkig komen er steeds meer hulpmiddelen om er grip op te krijgen.

Dekking

Een goede dekking van een wifi-netwerk begint met een goed ontwerp. Daarvoor is het noodzakelijk de ruimten in kaart te brengen waar het netwerk wordt gebruik. Er bestaat geavanceerde meetapparatuur die de belangrijkste storende elementen identificeert. Dergelijke software heeft daarbij mogelijkheden om accespoints te simuleren en te zien wat het effect is op de dekking. Ook biedt ze gereedschappen om analyses te maken en deze grafisch weer te geven en te presenteren in rapporten. Het is zeer aan te raden een dienstverlener zoals bijvoorbeeld sTN in te schakelen om met professionele apparatuur een optimale plaatsing van accespoints in kaart te brengen.

Ook een gebruiksanalyse is belangrijk. Hoeveel mensen moeten gelijktijdig op een bepaalde plek in de ruimtes gebruik kunnen maken van het netwerk? Wat gaan ze op dat moment doen? Zijn het zware datagebruikers of gaat het om het bekijken van simpele tekstbestanden? Voor het in kaart brengen van het gebruik kunnen enquêtes worden ingezet, maar het netwerk zelf geeft veel, heel betrouwbare informatie. Ook hier kan uw IT-dienstverlener u het beste overzicht geven met behulp van professioneel analysegereedschap.

Een analyse van het netwerkgebruik zou eigenlijk periodiek terug moeten komen om de optimale prestaties van het netwerk te blijven garanderen. Om regelmatig inzicht te krijgen in het gebruik van het netwerk, kan het netwerk het best worden verbonden met een centrale computer. Deze registreert constant het gebruik van het netwerk en verstrekt de noodzakelijke

rapportage. De eigenaar van het wifi-netwerk ontvangt hiervoor een inlognaam en wachtwoord voor verbinding met de centrale computer. De rapportage omvat o.a. het gebruik en aantal gasten per toegangspunt, het totale gebruik over de dag, het soort verkeer en de verbonden apparaten.

U kunt de netwerkanalyse uitbesteden aan een dienstverlener maar voor dit doel bestaan ook wel verschillende softwaretools die een indicatie kunnen geven van netwerkverkeer. Microsoft heeft bijvoorbeeld een packetanalyzer genaamd Microsoft Network Monitor[1]. OpenNMS[2] is een open source hulpmiddel voor professioneel network management. Zo zijn er enkele tientallen gratis en betaalde applicaties met ieder eigen voor- en nadelen. GFI Software heeft een handzaam overzicht[3] gemaakt van de top 20 gratis netwerkmonitor en -analyse tools. Stanford University[4] houdt een iets minder toegankelijk gepresenteerde lijst bij van nagenoeg alle hulpmiddelen.

Apparatuurkeuze

Is het netwerkontwerp klaar, dan komt het moment er de juiste apparatuur bij te zoeken. Hoewel het aanbod voor consumenten of small office home office (SoHo) accesspoints prijstechnisch aantrekkelijk lijkt is het toch niet verstandig deze apparatuur in te zetten voor een groter bedrijfsnetwerk. Dergelijke consumentenapparatuur mist de betrouwbaarheid van de professionele tegenhangers. Ze ontbeert bovendien de mogelijkheden voor geavanceerde netwerkconfiguratie, monitoring, beheer en beveiliging.

Router vs Accespoint

De basis van een wifinetwerk bij consumenten bestaat vaak uit een enkel apparaat waarin een router, een switch en een of meerdere antennes in een behuizing zijn gecombineerd. Het apparaat staat doorgaans ergens op heup- of borsthoogte opgesteld, meestal langs een muur. Dat is per definitie een suboptimale situatie vanwege de hoeveelheid objecten tussen de antenne en de apparatuur van de gebruikers die storing of demping veroorzaken.

In een professioneel wifi-netwerk worden daarom de verschillende onderdelen uit elkaar gehaald. Centraal in het netwerk staat een router voor het regelen van de verkeersstromen, de beveiliging, en het toepassen van het toegangsbeleid. De router is via een bedraad netwerk verbonden met verschillende 'accesspoints' voor het afhandelen van van het dataverkeer. Maar dezelfde netwerkkabel kan ook de benodigde stroom leveren, ook wel aangeduid met het begrip Power-over-Ethernet (PoE). Met PoE is het niet nodig naast de datakabel ook nog een stroomdraad naar het accespoint te leggen, wat aanzienlijk in de aanleg- en onderhoudskosten kan schelen.

Het accesspoint verzorgt alleen het radiogedeelte van de verbinding en zendt het dataverkeer naar een of meer gekoppelde antennes. Het accesspoint speelt in sommige gevallen ook een rol bij de beveiliging. Accespoints in kantoor- of fabrieksomgevingen hangen zoveel mogelijk aan het plafond, waarbij ze in een straal van 360 graden naar beneden stralen. Met zo'n opstelling is de invloed van storende objecten doorgaans minimaal.

[1] www.microsoft.com/en-us/download/details.aspx?id=4865
[2] www.opennms.org
[3] www.gfi.com/blog/the-top-20-free-network-monitoring-and-analysis-tools-for-sys-admins/
[4] www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html

Professionele apparatuur biedt bovendien meer technische mogelijkheden. Zo ondersteunt ze bijvoorbeeld vaak de mogelijkheid om niet alleen signalen rondom (360 graden) te zenden, maar ook een aantal smalle bundels naast elkaar uit te sturen met behulp van verschillende antennes (beamforming). Die eigenschappen helpen bij het invullen van de optimale dekkingskaart. Daarnaast is al deze apparatuur voorzien van netwerkpoorten met een hoge doorvoercapaciteit in de orde van gigabits per seconde (Gbps) voor de koppeling met het bedrade netwerk. Die poorten zijn nodig om de groeiende stroom dataverkeer naar het internet of naar de bedrijfsservers te leiden. Om op de toekomst voorbereid te zijn is het tegenwoordig zelfs al verstandig uit te kijken naar accespoints die een 2,5 of 5 Gbps poort hebben of de mogelijkheid twee Gbps-poorten te combineren tot één. Het voordeel van de eerste optie is dat in veel gevallen de bestaande ethernetbekabeling naar de accesspoints niet aangepast hoeft te worden.

Een relatief nieuwe ontwikkeling is het inzetten van verschillende antennes tegelijk om te communiceren met de apparatuur van een gebruiker op het netwerk. Dat levert een stabielere verbinding op door gebruik te maken van de karakteristieken van de doorgaans twee tot vier antennes. Dit wordt wel aangeduid met Multiple Input Multiple Output (MIMO). Tot voor kort kon het netwerk slechts MIMO inzetten voor de communicatie met één enkele gebruiker (Single User MIMO of SU-MIMO). Door die data-uitwisseling per gebruiker heel erg kort te houden, is het toch mogelijk veel gebruikers of 'clients' tegelijk te bedienen. Nu biedt een nieuwe standaard (802.11ac Wave 2) ook de mogelijkheid MIMO in te zetten voor de communicatie met meer gebruikers tegelijk (Multiple User MIMO of MU-MIMO). Daardoor neemt de bruikbaarheid van het netwerk sterk toe. Echter niet alle leveranciers ondersteunen deze nieuwe vorm van MIMO al.

Antennes

Een aandachtspunt bij het kiezen van de wifi-accesspointapparatuur is de mogelijkheid er verschillende typen antennes op aan te sluiten. Het aanbod aan antennes is heel divers. Elk antennetype heeft eigen karakteristieken. Die kunnen helpen de dekking en capaciteit van het netwerk op specifieke plekken in ruimtes optimaal in te richten.

Hoewel antennes een belangrijke invloed hebben op de dekking van de capaciteit van het wifi-netwerk, bestaat ook de valkuil het netwerk in te richten met een beperkt aantal krachtige antennes. Daarmee lijkt de dekking goed geregeld. De metingen aan de signaalsterkte in het netwerk hebben echter meestal alleen betrekking op het verkeer van het accespoint naar de gebruikersapparatuur. Echter, de apparatuur van de gebruikers moet zorgen voor het retourkanaal. Het gevolg is dat deze gebruikersapparatuur in een situatie met een gering aantal accesspoints alles uit de kast moet halen om de ontvanger te bereiken. Dat kost

veel energie. Eindgebruikers merken dat aan het tempo waarmee hun accu uitgeput raakt. Daarom is het aan te bevelen - waar mogelijk - de dekking van het netwerk in te richten met extra accesspoints, liever dan de inzet van een beperkt aantal krachtige antennes.

Roaming

Vrijwel alle wifi-accesspoints voor zakelijke toepassingen zijn tegenwoordig in staat 'roaming service' te leveren. Dat betekent dat gebruikers met hun laptop, smartphone of tablet rond kunnen lopen in het gebouw zonder dat ze in de gaten hebben dat ze steeds van het ene naar het andere accesspoint overstappen. Dat is zeker van belang wanneer veel gebruik gemaakt wordt van softtelefoons of wifi-telefoons. Gebruikers willen dan kunnen rondlopen zonder dat hun verbindingssessie verbreekt en opnieuw moet worden opgebouwd. Een voorwaarde voor een goedwerkende roaming is wel dat de dekkingsgebieden elkaar allemaal iets overlappen en dat er geen 'witte' vlekken zijn in de dekking op plekken waar de apparatuur van gebruikers moet overstappen naar een ander accesspoint. Een sluitend wifi-netwerkontwerp is daarbij essentieel (zie hoofdstuk Dekking).

Een laatste punt van aandacht bij de selectie van leveranciers en apparatuur is de manier waarop ze beveiliging faciliteren. (zie ook hoofdstuk Beveiliging). De betere leveranciers hebben wel mogelijkheden om te ontdekken of er onbedoeld en ongewenst apparatuur op het netwerk is aangesloten (rogue accesspoints). Dat kan bijvoorbeeld gebeuren wanneer een werknemer zijn eigen accesspoint op het netwerk aansluit met het idee zelf de dekking te verbeteren. Zo'n roque accesspoint vormt echter een lek in de beveiliging van het netwerk.

Storingen en kanaalkeuze

Hoe belangrijk een goed ontwerp en de juiste apparatuurkeuze ook is, ze bieden geen garantie voor een probleemloos functionerend netwerk. Goed in de gaten houden (monitoring) van het verkeer op het wifi-netwerk kan een hoop ergernis voorkomen, mits de instellingen van het netwerk steeds weer op de bevindingen worden aangepast.

De wifi-standaard waaraan de meeste apparatuur voldoet , biedt de mogelijkheid kanalen te gebruiken in twee frequentiebanden, 2,4 GHz en 5 GHz. Beide banden behoren tot het zogeheten vrije spectrum. Mits de zendsterkte binnen wettelijk vastgelegde limieten blijft, mag iedereen gebruik maken van deze frequenties zonder dat daar licentiekosten voor verschuldigd zijn. Voor veel andere frequentiebanden geldt dat niet zoals bijvoorbeeld 1,8 GHz en 2,6 GHz. Die worden door de overheid periodiek via een veiling aan de hoogstbiedende telecomaanbieders in licentie gegeven.
Een nadeel van de vrije banden is dat er veel verschillende toepassingen gebruik van maken. De ene toepassing kan de andere wegdrukken. De 2,4 GHz-band wordt bijvoorbeeld ook gebruikt door Bluetooth, babyfoons, draadloze telefoons, sommige afstandsbedieningen en autoalarmen. Bovendien werkt de magnetron ook met elektromagnetische straling in het 2,4 GHz-gebied. De wanden van de magnetron schermen de gevaarlijk krachtige straling in deze frequentieband weliswaar af, maar afhankelijk van de kwaliteit van de magnetronoven kan deze toch storen op het wifi-netwerk.

5 GHz biedt uitkomst

2,4 GHz was de eerste band die werd gebruikt voor het opzetten van wifi-netwerken. De 2,4 GHz-band biedt 13 kanalen die ook nog eens deels overlappend zijn. Daardoor zitten verschillende wifi-netwerken elkaar snel in de weg. Pas een jaar of zes geleden kwam de eerste apparatuur op de markt waarmee ook de 5 GHz-band kon worden gebruikt voor wifi. Het voordeel van deze band is dat er 23 kanalen beschikbaar zijn die elkaar niet overlappen.

Bovendien zijn er minder andere toepassingen die gebruik maken van de 5 GHz-band. Door de hogere frequentie hebben verbindingen in de 5 GHz-band wel meer last van afscherming door bijvoorbeeld muren of zware metalen voorwerpen.
Netwerkspecialisten raden aan de netwerkapparatuur zo in te richten dat deze gebruikersapparatuur (clients) die in staat is te communiceren over 5 GHz, ook dwingt er gebruik van te maken. Zo blijft de 2,4 GHz-band beter beschikbaar voor de wat oudere wifi-apparatuur die nog geen 5 GHz aan kan.

Grootgebruikers liever aan een kabel

Veel moderne netwerkapparatuur is tegenwoordig in staat verschillende kanalen tegelijk te gebruiken. Die aanpak wordt ook wel 'channel bonding' genoemd. In plaats van 20 MHz per gebruiker is er dan 40 MHz

beschikbaar. De eindgebruiker krijgt zo dus ook de dubbele doorvoercapaciteit tot zijn beschikking. Het is de vraag of het zinvol is die mogelijkheid in te zetten. De capaciteit van een enkel kanaal bedraagt tegenwoordig namelijk wel 150 tot 300 Mbps. Die capaciteit is dus veel groter dan die van de verbinding van de organisatie naar het internet. Die bedraagt immers vaak niet meer dan 100 of 200 Mbps. Het vergroten van de wifi- doorvoercapaciteit door het bundelen van kanalen heeft dus alleen zin wanneer er vaak lokaal grote bestanden moeten worden uitgewisseld.
Het nadeel van bundelen is dat andere gebruikers op het netwerk minder capaciteit tot hun beschikking krijgen. Het is daarom zinvoller de datagrootgebruikers op het netwerk aan te sluiten met een ethernetkabel (bedraad) in plaats van draadloos (via wifi).

Meten is weten

De netwerkmanagementsoftware besproken onder het hoofdstuk Dekking levert in de exploitatiefase van het netwerk waardevolle informatie over de prestaties van het netwerk gemeten in de tijd. Zo biedt de software in veel gevallen mogelijkheden een Quality of Service-drempel in te stellen. Netwerkbeheer krijgt dan een waarschuwing wanneer niet aan de gemaakte afspraken wordt voldaan.

De managementsoftware levert tevens een overzicht van de gebruiksstatistieken op piektijden en over langere tijd gemeten. Doorsnee gebruikers halen doorgaans veel meer data op dan dat zij versturen over het netwerk. Dat kan een reden zijn om het netwerk ook asymmetrisch in te richten, liefst per gebruikerstype. Zo komt er meer ruimte beschikbaar om downloadacties soepel te laten verlopen terwijl er genoeg ruimte overblijft voor het uploadkanaal. Internetaanbieders hanteren bij ADSL-verbindingen op dezelfde manier een asymmetrische capaciteit.

Beleid

In elke groep zijn er grootgebruikers en kleine afnemers. Binnen een werkomgeving hangt dat doorgaans samen met aard van de werkzaamheden van de betrokken werknemers. Maar in sommige gevallen eigenen mensen zich privileges toe die eigenlijk niet voor hen zijn bestemd. Zo lang de productiviteit er niet onder lijdt en de andere werknemers er geen last van ondervinden, hoeft dat geen probleem te zijn. Maar wanneer bijvoorbeeld het opstellen van de maandrapportages vertraagt door excessief YouTube-gebruik, is er een grens overschreden. Het is handiger zo'n situatie te voorkomen met goede gebruiksregels (policies) die op de netwerkapparatuur worden ingesteld. Dergelijke policies worden gekoppeld aan gebruikersgroepen of aan de profielen van individuele gebruikers. Met goede monitoringsoftware is na te gaan welke groepen of individuele eindgebruikers de zwaarste belasting vormen voor het netwerk. Zo'n analyse is een goed vertrekpunt voor het opstellen van de beleidsregels.

Een andere mogelijkheid om het verkeer in te dammen, is het instellen van time-limited sessions. In dat geval breekt de netwerkapparatuur de sessie af na een vooraf bepaalde tijd. Deze onvriendelijke methode wordt vaak toegepast bij gratis openbare netwerken en is niet zo geschikt voor reguliere bedrijfsnetwerken.

Wanneer het netwerk niet alleen door eigen werknemers wordt gebruikt, maar ook door gasten, kan er verstoring optreden door overbelasting of onvoldoende beveiliging. Een oplossing hiervoor is het inrichten van de configuratie van een gescheiden wifi-netwerk bestemd voor gastgebruik. Daardoor hebben de gasten geen toegang tot het bedrijfsnetwerk. Zo wordt de veiligheid en de beschikbare capaciteit op het bedrijfsnetwerk gegarandeerd.

Storingen en verlies aan capaciteit treden ook op door fysieke problemen in de netwerkapparatuur. Tenzij er een voortdurende monitoring op de werking van het netwerk is ingericht, kan het nog wel eens even duren voordat de ergernis over een slecht werkend netwerk

wordt herleid tot een uitgevallen accesspoint. Wanneer de dekking van een aantal accesspoints elkaar redelijk overlapt zal gebruikersapparatuur immers automatisch overschakelen op een ander accesspoint dat wel werkt. Het probleem van storingen in de netwerkapparatuur kan worden opgelost door de toepassing van intelligente zelfherstellende technieken in de apparatuur.

Hierbij worden veel voorkomende storingen automatisch herkend. De apparatuur doet vervolgens zelf een poging de storing te verhelpen. Ook de door sTN toegepaste methode van Centrale monitoring en foutmelding biedt een adequate oplossing. Hierbij staat de apparatuur via internet permanent in verbinding met een centrale server waardoor foutsituaties meteen worden herkend en gerapporteerd door de centrale netwerkbeheerder. Daarmee kan proactief onderhoud worden gedaan, dus voor de gebruikers werkelijk problemen ervaren.

Bedrade netwerk

Tot nog toe behandelde deze whitepaper vooral aandachtspunten om het draadloze (radio) gedeelte van het netwerk te optimaliseren. Een cruciaal deel van een draadloos netwerk is echter het bedrade netwerk. Een switch die de basis vormt van een intensief gebruikt draadloos netwerk, moet eigenlijk op alle poorten een capaciteit van 1 Gbps kunnen leveren om de pieken in capaciteitsvraag goed aan te kunnen. De poorten waarop de accesspoints zijn aangesloten moeten ook allemaal voorzien zijn van Power over Ethernet (PoE). Op die manier hoeft er alleen een ethernetkabel naar de accesspoints getrokken te worden en kan de investering in een aparte stroomvoorziening en het onderhoud ervan, achterwege blijven.

DUS:

DATALIMIETEN X AANTALLEN APPARATEN GELIJKTIJDIG OP HET NETWERK = MINIMUM BANDBREEDTE NAAR DE EXTERNE NETWERKAANBIEDEN.

Tenslotte is ook de verbinding naar buiten toe een punt van aandacht. Hoewel een deel van het verkeer binnen het lokale netwerk blijft, wordt de capaciteit naar buiten toe steeds belangrijker. Denk daarbij bijvoorbeeld aan het toenemend gebruik van diensten van cloudaanbieders, maar ook aan videovergaderingen en andere toepassingen die veel bandbreedte vergen. Een goede stelregel voor het bepalen van de capaciteit is het aantal apparaten dat gelijktijdig gebruik maakt van het netwerk, vermenigvuldigd met de datalimieten die voor die apparaten zijn ingesteld in de beleidsregels.

Beveiliging

Aandacht voor beveiliging moet een topprioriteit zijn bij het inrichten van een wifi-netwerk. Alleen met voldoende alertheid kan worden voorkomen dat onbevoegden het netwerk binnen komen en gevoelige bedrijfsgegevens in verkeerde handen vallen of kwaadaardige software (malware, zoals virussen of Trojan Horses) wordt geïnstalleerd.

De standaard beveiliging die elk draadloos netwerk moet hebben, is de versleuteling (codering) van al het verkeer dat over het netwerk gaat. Alleen bevoegde ontvangende apparatuur bevat de sleutel waarmee de gegevens weer gedecodeerd kunnen worden. Hoewel wifi-apparatuur nog vaak verschillende protocollen aanbiedt zoals WEP en WPA, is WPA2 het enige protocol dat nog voldoende zekerheid biedt tegen indringers. Wanneer een toegangscode wordt gebruikt, wordt de informatie gecodeerd vanaf het wifi-toegangspunt tot de internetmodem. Verdergaande beveiliging is mogelijk door directe verbinding van het verbonden apparaat en internet. Hierbij is geen onderling verkeer mogelijk tussen de met het netwerk verbonden apparaten hetgeen bescherming biedt tegen MITM (man in the middle) aanvallen.

Nog veiliger is het gebruik van Virtual Private Networks (VPN's), vooral als bijvoorbeeld voor het gebruik van het netwerk op een andere vestiging of bij het gebruik van een extern datacentrum of clouddienst, een deel van de verbinding over het publieke internet loopt. In dat geval wordt als het ware een tunnel gecreëerd voor de datacommunicatie vanaf de computer van de gebruiker tot servers die via het internet worden benaderd.

Daarnaast hoort elk bedrijfsnetwerk - draadloos en bedraad - te zijn voorzien van gebruikersprofielen. Niet elke werknemer heeft toegang nodig tot alle uithoeken van het netwerk, zoals de servers van de financiële administratie, die voor het personeelssysteem of de planning en controle. Door de werknemers in groepen

in te delen en daar specifieke rechten aan te verbinden, krijgen zij bij het inloggen op het netwerk automatisch de juiste rechten (user policies) toegewezen voor toegang, maar ook voor het bandbreedtegebruik, zoals eerder besproken.

Een bijzondere groep zijn de gasten op het netwerk, zoals bezoekers, werknemers van partners en andere tijdelijke gebruikers van het netwerk, zoals bijvoorbeeld de gasten in een horecagelegenheid. Met user policies kunnen gastgebruikers speciale rechten en beperkingen worden toegekend. Een van de voor de hand liggende beperkingen is bijvoorbeeld dat het bepaalde groepen gebruikers niet is toegestaan buiten kantoortijden op het netwerk in te loggen (access schedules).

De wensen van de verschillende groepen gastgebruikers lopen nogal uiteen. Zo zal een externe consultant misschien toegang willen hebben tot strategiedocumenten maar een medewerker van een toeleveringsbedrijf wil toegang juist tot de productieplanning en logistiek. Met gebruikersprofielen zijn deze rechten heel nauwkeurig vast te leggen. Gasten van een horecagelegenheid hoeven waarschijnlijk helemaal geen servers op het bedrijfsnet te benaderen en zijn al tevreden met een goede verbinding naar internet. In dat geval kan het aanleggen van een volledig gescheiden netwerk voordelen bieden omdat daarmee een optimale beveiliging van de bedrijfsprocessen- en gegevens kan worden bereikt.

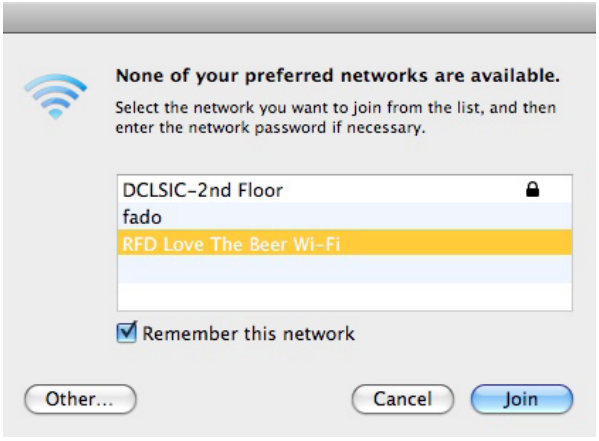
Opsporing wordt belangrijker

De aandacht van moderne IT-beveiliging verschuift steeds meer van het buiten houden van ongewenste activiteiten (het kasteel-model) naar het vroegtijdig detecteren en neutraliseren ervan. Geen enkele beveiligingstechnologie biedt namelijk een 100 procent garantie waterdicht te zijn. Maar afwijkende verkeerspatronen en verdachte activiteiten zijn vaak wel automatisch te detecteren. Monitoring speelt dus ook in de beveiliging van het netwerk een belangrijke rol. Ontwikkelingen in machine learning en kunstmatige intelligentie helpen om deze monitoringsoftware steeds geavanceerder te maken. De software leert zelf wat de gangbare verkeerspatronen en acties zijn op het netwerk en slaat alarm wanneer er afwijkingen worden gesignaleerd. Een van de veel voorkomende afwijkingen is wanneer een werknemer of gast probeert een eigen accesspoint aan het netwerk te verbinden. Soms is dat gewoon voor het gemak, maar het komt ook regelmatig voor dat ze worden geïnstalleerd om makkelijker van buitenaf toegang te krijgen tot het bedrijfsnetwerk. Dergelijke 'rogue networks' moeten dus snel worden ontdekt en verwijderd.

Zoals bij alle beveiligingsvraagstukken is het actueel houden van de apparatuur een aandachtspunt dat zo voor de hand ligt dat het eigenlijk geen aandacht zou hoeven krijgen. Het controleren dat steeds de laatste firmwareupdates zijn geïnstalleerd, moet een topprioriteit zijn van elke beheerder. Alleen op die manier is er zekerheid dat kwaadwillende hackers niet via bekende zwakke plekken het netwerk kunnen binnendringen.

Voordelen benutten

Veel organisaties beseffen niet dat het wifi-netwerk niet alleen een functioneel bedrijfsmiddel is, maar ook een handig gereedschap voor marketing en zelfs voor sales. Erg voor de hand ligt het slim gebruik van de naamgeving van het netwerk (de SSID). Een netwerk dat 'Vandaag 2e koffie gratis bij lunchroom Corry' heet,



vormt een gratis advertentie voor iedereen binnen het bereik van het netwerk. De naam 'Netgear386729C' daarentegen zegt bijzonder weinig.

Het kiezen van de SSID met een ondoorgrondelijke naam of zelfs het onzichtbaar maken van de naam, kan onderdeel zijn van een beveiligingsstrategie. Maar hoe effectief dat onderdeel van de strategie is, valt te betwijfelen. Met professionele scannerapparatuur is het tegenwoordig een koud kunstje elk netwerk te peilen of nu de SSID is afgeschermd of niet. Een goede herkenbare netwerknaam daarentegen verhoogt de herkenbaarheid van de organisatie.

Wifi-net biedt mogelijk nieuwe inkomstenstromen

In de hotelbranche is het heel gebruikelijk klanten die contact leggen met het netwerk automatisch eerst een welkomspagina te presenteren. Zo'n pagina wordt ook wel een portalpagina genoemd. De portal biedt bijvoorbeeld informatie over de organisatie maar kan ook dienen voor de aanvraag van een tijdelijk gastaccount. Wanneer er een betaalsysteem gekoppeld wordt aan de portalsite is het zelfs mogelijk met de (premium) gastaccounts een aparte inkomstenstroom te genereren. Gasten krijgen dan bijvoorbeeld op basis van vouchers voor een beperkte tijd toegang tot het netwerk, waarbij de snelheid van de verbinding is opgedeeld in verschillende klassen met een bijbehorend prijskaartje. Voor de leden van branchevereniging Koninklijke Horeca Nederland is zelfs een pakket ontwikkeld waarmee zo'n gelaagd wifi-voucheraanbod eenvoudig te realiseren is, via de telecomorganisatie van de vereniging die door sTN is opgezet. sTN kan dit pakket ook aan leden van andere brancheverenigingen aanbieden[5].

In de horeca is klanten laten betalen voor internettoegang steeds minder gebruikelijk, maar zo'n aanpak zal niet voor elke organisatie van toepassing zijn. Inmiddels het gebruik van een portalsite waarop derden de gelegenheid krijgen hun eigen reclameboodschappen te plaatsen om zo een nieuwe inkomstenstroom te genereren wel breder toepasbaar is.

Een alternatief voor de portalsite is een automatische doorlink naar de Facebookpagina van de organisatie. Doorverwijzen naar de Facebookpagina heeft een aantal voordelen. Zo biedt het bedrijf achter het sociale netwerk ook een authenticatiedienst waarmee een gastgebruiker zich makkelijk kan aanmelden op het netwerk met zijn eigen Facebook-inloggegevens.

Facebook zorgt dan voor de validatie van de gegevens van de gastgebruiker. Facebook kan bovendien een aantal extra diensten leveren. Zo kan het bezoek bijvoorbeeld automatisch aan de timeline van de gast op Facebook worden gekoppeld.

De eigenaar van het bedrijfsnetwerk krijgt op zijn beurt van Facebook de mogelijkheid allerlei statistieken te bekijken over het bezoek, zoals het totaal aantal ingelogde personen, fans, bereikt publiek, de verdeling tussen mannelijke en vrouwelijke bezoekers, leeftijdscategorieën, piektijden en meer. Bovendien, hoe hoger de bezoekersaantallen die Facebook registreert, hoe beter de organisatie voorkomt in de zoekopdrachten die via Facebook worden geplaatst.

Wie weet er meer?

Een goed wifi-netwerk opzetten en onderhouden is een activiteit die bij de meeste organisaties niet tot de kerntaken behoort. Met de opkomst van clouddiensten en managed serviceproviders neemt ook het aantal aanbieders toe dat het gehele onderhoud op afstand kan verzorgen. Deze whitepaper geeft een overzicht van de kansen en bedreigingen bij het gebruik van wifi-netwerken. Wellicht zijn er actuele vragen bij u opgekomen. De accountmedewerker van uw netwerk- of internetleverancier is de aangewezen persoon om die vragen voor te leggen.

Maar ook uw brancheverenigingen kan u hierbij zeker bij helpen, onder meer via de kennis en ervaring van sTN. Zoals sTN voor de brancheverenigingen Koninklijke Horeca Nederland de eigen dienstverlener KHN Telecom opzette, kan de dienstverlener deze ervaring ook aan leden van andere brancheverenigingen aanbieden. Denk daarbij aan hulp bij het inrichten van wifi-netwerken - of deelname aan inkoopcombinaties met aantrekkelijke groepskortingen. Aarzel niet hiervoor contact op te nemen met uw brancheverenigingen of sTN.

Conclusie

Een wifi- of draadloos netwerk vergt onderhoud. Goedpresterende netwerken krijgen na verloop van tijd vaak te maken met een verlies aan capaciteit. De oorzaak is de veranderende omgeving waarin het netwerk actief is. Of de gebruikers gaan andere eisen stellen aan gebruik van het netwerk waardoor de capaciteit tekort schiet.

Het aanleggen van een nieuw netwerk of het optimaliseren van een bestaand netwerk begint met het maken van een goed dekkingsplan. Een analyse van het gebruik en de mogelijke storingsbronnen moet eigenlijk altijd een uitgangspunt zijn voor zo'n vernieuwingsslag. Het is aan te raden zo'n dekkingsplan door een professionele dienstverlener uit te laten voeren. Om de prestaties optimaal te houden, is een periodieke herhaling van de gebruiksanalyse nodig. Een permanente monitoring van het verkeer op het netwerk biedt bovendien het voordeel dat afwijkende verkeerspatronen – bijvoorbeeld als gevolg van een beveiligingsprobleem – tijdig worden onderkent.

Tenslotte biedt het wifi-netwerk diverse mogelijkheden voor de organisatie zich beter te presenteren, interactie met de gastgebruikers aan te gaan en zelfs een nieuwe inkomstenstroom te genereren. sTN kan u verder helpen met het maken van de juiste keuzes daarin.

[5] Zie voor aanbod: www.khntelecom.nl

sTN Telecom & Internet
Postbus 627
3447 GW Woerden

Antwoordnummer 2241
3440 VB Woerden
Telefoon: 0348-495051

E-mail: info@stn.nl
Web: www.stn.nl
Twitter: twitter.com/stnnl