White Paper

Hoe maak je wifi-netwerken geschikt voor draadloze stille ontruimingsalarmering volgens de NEN2575-4 norm?

Wifi-netwerken zijn risicovol om te gebruiken voor bedrijfskritieke communicatie, zoals ontruimingsalarmering. Netwerkcomponenten en -verbindingen kunnen uitvallen, bandbreedte op het netwerk is niet gegarandeerd, en er is kans op interferentie op het draadloze netwerk, met name ook van niet-wifi apparaten. Dit maakt dat de betrouwbaarheid van dergelijke netwerken voorheen niet volledig kon worden gegarandeerd, terwijl ziekenhuizen en zorginstellingen juist meer en meer wifi-netwerken gebruiken. In deze whitepaper legt Ascom uit welke maatregelen nodig zijn om wifi-netwerken even betrouwbaar te maken voor ontruimingsalarminstallaties als paging- en (IP-)DECT-systemen.

Alle door de overheid voorgeschreven ontruimingsalarminstallaties voor stil alarm in Nederland moeten voldoen aan de norm NEN2575. Deze norm van het Nederlands Normalisatie Instituut bepaalt de systeem- en kwaliteitseisen en projectierichtlijnen van de installaties die een snelle en ordelijke personele ontruiming van een gebouw of ruimte bewerkstelligen als er een brand of andere calamiteit plaatsvindt. De norm gaat verder dan alleen de producten die de alarmen doorgeven, want de norm kijkt ook naar de autonomie, compatibiliteit en de wijze van installeren, bekabeling en noodvoeding. De norm is in het leven geroepen om de kwaliteit en betrouwbaarheid van ontruimingsalarminstallaties te verbeteren en te garanderen.

Iedere zorginstelling, ziekenhuis en gevangenis heeft een op maat gemaakte aanpak om een dergelijke installatie te implementeren, omdat er specifieke eisen aan worden gesteld: ieder gebouw heeft bijvoorbeeld een eigen indeling, er verblijven en/of werken meer mensen of de behoefte aan het type alarm verschilt. Zo wordt in veel gebouwen gealarmeerd met een luid alarm (slow whoops), zodat iedereen meteen op de hoogte is van een calamiteit. In delen van ziekenhuizen, gevangenissen en zorginstellingen kunnen de bewoners echter vaak niet zelfstandig hun kamer verlaten bij een calamiteit en is ondersteuning door bedrijfshulpverleners noodzakelijk. Dat soort omgevingen met niet-zelfredzame personen vraagt om stille alarmering om paniek te voorkomen.

Verschillende technologieën voor draadloze stille ontruimingsalarmering

In omgevingen met niet-zelfredzame personen worden er voornamelijk drie technologieën gebruikt voor draadloze stille ontruimingsalarmering:

1. Paging

Dit zijn robuuste, op tekstuele communicatie gebaseerde systemen die in zorginstellingen vaak worden gebruikt om zorgoproepen en/of andere alarmeringen door te geven. De zorgmedewerkers of bedrijfshulpverleners hebben kleine mobiele apparaten (pagers) op zak die de tekstberichten tonen, zodat ze een bepaalde ontruimingsprocedure kunnen starten. Het voordeel van deze systemen is dat ze autonoom zijn, specifiek voor alarmering zijn ingericht en daardoor erg betrouwbaar zijn. Een aandachtspunt is echter dat dergelijke systemen vaak alleen voor bedrijfshulpverlening worden gebruikt en dat wel geborgd moet zijn dat het systeem juist in geval van calamiteiten ook echt functioneert. De norm NEN2575 zorgt voor de juiste richtlijnen om deze werking te waarborgen, zoals een indicatie op de pager als de accu leeg dreigt te raken.

2. DECT en IP-DECT

Zorgverleners zijn mobiel en moeten daardoor altijd en overal kunnen communiceren. Met draadloze DECT-systemen wordt communicatie via tekstberichten en spraak (telefonie) gecombineerd tot één apparaat via een eigen infrastructuur. Met de juiste voorzieningen kan een DECT/IP-DECT systeem ook geschikt gemaakt worden voor ontruimingsalarmering. Ten opzichte van een pagingsysteem biedt een DECT/IP-DECT-systeem meer mogelijkheden, maar vereist een grotere investering: er zijn meerdere basisstations nodig om het hele gebouw dekkend te krijgen. IP-DECT is daarentegen zeer betrouwbaar en toekomstvast: IP-DECT com-

ascom

bineert de bewezen DECT-standaard met VoIP, waardoor gebruik kan worden gemaakt van data en kwalitatief hoogstaande spraakverbindingen in combinatie met moderne telefooncentrales.

3. Wifi
Veel zorginstellingen en ziekenhuizen investeren in wifi-netwerken met het oog op een grote verscheidenheid aan toepassingen. Er worden steeds vaker mobiele apparaten gebruikt, zoals tablets en smartphones. Medewerkers kunnen hiermee overal toegang krijgen tot bijvoorbeeld het intranet, het internet, videobeelden van bewakingscamera's en patiëntdossiers. Ook patiënten en bezoekers willen gebruik kunnen maken van het draadloze netwerk. De investeringen die nodig zijn voor de wifi-infrastructuur zijn relatief hoog, maar het toepassingsgebied van wifi is daarentegen zeer breed.

Kritische communicatie moet altijd werken, en altijd blijven werken
De grote uitdaging bij deze technologieën is dat bedrijfskritische communicatie, van zeer groot belang in de zorg, snel moet plaatsvinden en dat het altijd moet functioneren. Paging- en (IP-)DECT-systemen zijn zeer betrouwbaar, maar richten zich vooral op de bedrijfskritische communicatie zelf. De markt beweegt steeds meer richting wifi als gangbare oplossing om een grotere diversiteit aan toepassingen mogelijk te maken. Voor het faciliteren van kritische communicatie via wifi-netwerken zijn er echter extra maatregelen vereist. Het is natuurlijk niet voor niets dat het Agentschap Telecom waarschuwt voor de opstopping van 2,4 GHz-wifi-netwerken door de wildgroei aan hotspots en toenemend dataverkeer. Daardoor bestaat het risico dat draadloze netwerkverbindingen traag of helemaal niet werken, met mogelijk gevolgen voor bedrijfsprocessen, inclusief processen die gebruik maken van kritische communicatie.

Veel wifi-oplossingen worden ontworpen voor de huidige situatie van de instelling. Er wordt vaak niet nagedacht over hoe het systeem moet worden bewaakt en hoe de gebruiker ervoor kan zorgen dat het ook op langere termijn (als er meer of nieuwe apparaten gebruik gaan maken van het netwerk) nog steeds volledig betrouwbaar werkt. Degradatie van de diensten die het netwerk biedt, kunnen gebruikers, en in het bijzonder zorginstellingen, ziekenhuizen en gevangenissen, zich simpelweg niet veroorloven.

Aandachtspunten bij wifi voor draadloze stille ontruimingsalarmering
Bij gebruik van wifi voor draadloze stille ontruiming conform NEN2575-4, zijn er verschillende punten die extra aandacht behoeven:

1. Noodstroomvoorziening
Als de primaire stroomvoorziening wegvalt, moet een noodstroomvoorziening ervoor zorgen dat de ontruimingsalarminstallatie nog minimaal twaalf uur blijft functioneren. Een wifi-infrastructuur maakt gebruik van decentrale componenten (access points), die worden ontsloten vanuit één of meerdere technische ruimten. Noodstroom moet beschikbaar zijn voor de gehele infrastructuur.

2. Autonomie
Voor de werking van de ontruimingsalarminstallatie mag er geen afhankelijkheid van andere systemen zijn. Zo kan bij een brand het telefonieplatform uitvallen, maar de ontruimingsalarmering moet gewaarborgd blijven. Ook mogen gekoppelde systemen die een andere toepassing dienen, de werking van de ontruimingsalarminstallatie niet negatief beïnvloeden. Bedrade, fysieke netwerken kunnen gebruik maken van logische netwerken om dit te bewerkstelligen. Wifi is eveneens een gedeeld medium, waarop allerlei apparaten aanspraak op kunnen maken. Apparaten hebben hierbij de eigenschap dat ze zoveel mogelijk capaciteit van het netwerk willen benutten. De wifi-infrastructuur moet in staat zijn om het gebruik van het gedeelde medium goed te coördineren, zodat de ontruimingsalarmeringstoepassing niet in het gedrang komt.

3. Functiebehoud
Na het uitbreken van brand, moet het systeem nog minimaal dertig minuten blijven functioneren. Functiebehoud bij brand is vastgelegd in de Nederlandse praktijkrichtlijn NPR-2576 voor bekabeling, ophanging en montage van transmissiewegen. Wanneer een kabel naar een access point doorbrandt, functioneert het access point niet meer en is er geen communicatie mogelijk. Het heeft de voorkeur om bekabeling in vloeren en wanden aan te leggen (nieuwbouw), of om

gebruik te maken van functiebehoud E30 bekabeling en ophanging. Als deze opties niet mogelijk of gewenst zijn, dan kan het aanleggen van een tweede netwerk overwogen worden. ‘Dubbele dekking’ kan gezien worden als een manier om functiebehoud te realiseren. Bij een tweede wifi-netwerk komt echter een groot interferentie-probleem om de hoek kijken, omdat de toename aan access points ook meer interferentie genereert. De access points hebben maar een bepaald aantal kanalen per frequentie (2,4 GHz of 5 GHz) ter beschikking, waardoor ze elkaar overlappen en dus storen.
Dit probleem is gedeeltelijk te ondervangen met kanaalplanning, zodat access points een bepaald kanaal krijgen toegewezen, om zo min mogelijk overlap per kanaal te krijgen. Kanaalplanning voor een netwerk met enkele dekking kan erg uitdagend zijn, zeker in gebouwen met meerdere bouwlagen en met weinig demping tussen deze bouwlagen. Een goede kanaalplanning voor een netwerk met dubbele dekking is nauwelijks realiseerbaar met wifi. Daarbij zal de kwaliteit van een dergelijk netwerk te wensen overlaten, waardoor berichten trager of helemaal niet door kunnen komen. Een oplossing kan zijn om twee aparte wifi-infrastructuren aan te leggen, waarbij één infrastructuur gebruik maakt van de 2.4 GHz frequentieband en de andere infrastructuur gebruik maakt van de 5 GHz frequentieband. Ook kunnen er twee infrastructuren aangelegd worden, waarbij de access points worden ‘geknepen’ (minder vermogen). Hierdoor is er minder storing tussen de infrastructuren. Als één infrastructuur uitvalt bij een calamiteit, dan schaalt de andere infrastructuur op in vermogen. Dit lijkt op het eerste gezicht een doeltreffende oplossing, maar de realiteit is dat organisaties een duur netwerk aanleggen dat eigenlijk nooit de volledige mogelijkheden van het netwerk benut. Het tweede probleem is dat moet worden vertrouwd op het opschalen van het netwerk tijdens een calamiteit; het systeem moet zich dus in zeldzame gevallen anders gedragen, terwijl juist op dat moment zekerheid is gewenst.

4. Bewaking
Vanuit de NEN2575-norm moeten ontruimingsalarminstallaties worden bewaakt. Juist voor wifi-netwerken brengt dit een uitdaging met zich mee. Niet alleen het uitvallen van een access point of centrale apparatuur (incl. routers, switches e.d.) moet worden bewaakt, maar juist ook de werking van het draadloze netwerk moet bewaakt worden. Zijn er geen stoorbronnen aanwezig, die de werking van de ontruimingsalarminstallatie kunnen beïnvloeden? Is er voldoende bandbreedte aanwezig op het wifi-netwerk, ook geruime tijd na de ingebruikname van het systeem?

Dit zijn vier belangrijke uitdagingen waar leveranciers van wifi-netwerken voor ontruimingsalarminstallaties tot voor kort geen volledig antwoord op hadden. Sommige leveranciers

bieden wifi-netwerken die beperkt bewaakt worden, onvoldoende zekerheid geven op het correct (blijven) functioneren of waarbij de volledige mogelijkheden van de infrastructuur niet worden benut.

Nieuw totaalconcept als antwoord op de aandachtspunten
Dat het ook anders kan, bewijst Ascom nu samen met Fortinet (voorheen Meru Networks), leverancier van wifi-infrastructuren. De beide partijen bedachten samen een totaaloplossing om wifi-netwerken geschikt te maken voor ontruimingsalarmering, waarbij eerdergenoemde aandachtspunten geadresseerd worden.

1. Aan de basis van dit nieuwe concept staat een fundament waarin noodstroom voor de wifi-infrastructuur voorzien is vanuit de centrale apparatuur. Access points worden vanuit één of meerdere centrale ruimtes door middel van ‘Power over Ethernet’ gevoed met een NEN-EN54-4 gecertificeerde voeding.

2. Het is een autonoom systeem dat allereerst niet afhankelijk is van andere systemen. Essentieel in het concept is dat het wifi-systeem zelf de controle heeft over het gebruik van het draadloze netwerk en niet de apparaten die gebruik willen maken van het netwerk. Op deze manier bepaalt het systeem welke apparaten en welke toepassing bandbreedte krijgen; dit wordt niet aan de willekeur van wifi-apparaten en de grote diversiteit aan mogelijke wifi-toepassingen overgelaten. De access points worden aangestuurd door een controller als een soort dirigent en het systeem bepaalt zelf wanneer welke apparaat ‘aan de beurt’ is. De ‘dirigent’ zorgt ervoor dat de draadloze apparaten niet de baas over het netwerk zijn, maar het draadloze netwerk zelf. Het wifi-systeem

bepaalt dus wanneer (en hoelang) een apparaat toegang krijgt tot het netwerk. Het systeem en de draadloze handsets die gebruikt worden voor ontruimingsalarmering geven bovendien prioriteit aan ontruimingsalarmeringen.

3. Daarnaast is er een continue bewaking van de prestaties van het netwerk. Dat gaat veel verder dan het detecteren of een access point is uitgevallen: het systeem kan zelfs problemen voortijdig signaleren. Het systeem peilt zelf of het systeem werkt en of er voldoende bandbreedte is. Zo ontstaat een beter beeld van de prestatie van het netwerk over een langere periode en kan proactief worden gehandeld om mogelijke problemen te verhelpen. Het systeem wordt dus niet alleen handmatig ieder jaar gecontroleerd, maar die controle wordt automatisch gedaan. Het wifi-systeem is daarmee een zelf-verifiërend systeem.

4. Het systeem detecteert stoorbronnen die de prestaties van het netwerk tijdelijk of permanent negatief beïnvloeden. Sensoren ‘luisteren’ naar apparaten die de werking van het wifi-netwerk kunnen verstoren. Zo kan het bijvoorbeeld zijn dat tijdens de aanleg van het systeem het aantal stoorzenders beperkt is, maar dat dat aantal groeit als er bijvoorbeeld andere netwerkapparatuur in de omgeving geplaatst wordt.

5. Als functiebehoudkabeling en aanleg van bekabeling in wanden en vloeren niet gewenst of mogelijk zijn, is een wifi-netwerk met dubbele dekking mogelijk. Om interferentie te voorkomen of te minimaliseren, wordt er gebruik gemaakt van de unieke mogelijkheid van “channel layering”. Er worden twee volledig dekkende netwerken gerealiseerd, waarbij elk netwerk gebruik maakt van een eigen kanaal/frequentie. Alle access points van één netwerk werken op hetzelfde kanaal en interfereren daarbij niet met het andere netwerk Deze oplossing vergt weliswaar een grote investering, maar deze investering wordt tijdens normaal gebruik van het netwerk volledig benut: het systeem biedt namelijk een dubbele capaciteit, omdat de capaciteit van beide netwerk niet wordt ‘geknepen’.

Voor veel zorginstellingen is het voldoende om te kiezen voor paging- en DECT-systemen als ontruimingsalarminstallaties, maar als men kiest voor wifi is dit totaalconcept de meest betrouwbare oplossing. Dit concept is uniek, omdat het een zelf-verifiërend, voorspellend netwerk is, dat continu mogelijke stoorbronnen detecteert. De dirigent-functie zorgt voor een gecontroleerde toegang tot het netwerk. Indien de andere opties (functiebehoudbekabeling of aanleg van bekabeling in wanden en vloeren) niet mogelijk zijn, is het mogelijk om een netwerk met dubbele dekking te realiseren. Het totaalconcept is een stap verder dan wat andere leveranciers op het gebied van wifi bieden, maar dat is geen overbodige luxe als het gaat om ontruimingsalarmering. Ascom ziet het zelfs als een voorwaarde voor een volledig betrouwbaar wifi-netwerk.

Wilt u meer informatie over deze totaaloplossing om wifi-netwerken te laten voldoen aan de NEN2575-norm? Neem dan contact op met Ascom en mail naar info@ascom.nl.

Ascom (Nederland) B.V.
Postbus 40242 | 3504 AA Utrecht
T (030) 240 91 00 | F (030) 241 19 46
info@ascom.nl | www.ascom.nl