Uitdagingen bij het op de markt brengen van **IoT-oplossingen**

zorgen over veiligheid, schaalbaarheid en de concurrentie

Figuur 1. De Europese Commissie heeft onderzocht of de grote spelers op het gebied van spraakassistenten, de favoriete gebruikersinterface voor het smart home, de concurrentie tegenwerken (bron: ShutterStock/Gorodenkoff).

Stuart Cording (Elektor)

Het Internet of Things (IoT) bestaat al meer dan 20 jaar en er zijn tal van draadloze technologieën ontwikkeld om de toepassing ervan te ondersteunen. In huis zijn spraakassistenten inmiddels de primaire gebruikersinterface voor een reeks slimme apparaten. Ondanks deze vooruitgang komt meer dan een derde van de IoT-projecten nooit verder dan de *proof-of-concept* fase. Bovendien vreest de Europese Commissie dat een gebrek aan concurrentie in sommige toepassingsgebieden de markttoegang voor EU-bedrijven belemmert. Wat zijn dus de echte uitdagingen en hoe kunt u een IoT-oplossing in Europa uitrollen?

Als u de technologieën achter het Internet of Things (IoT) wilt leren kennen, is het niet moeilijk om een hele reeks geschikte projecten te vinden. Zoek gewoon op "IoT" en het prototype-platform van uw voorkeur, en u wordt bedolven door ontelbare pagina's met projecten, cloud-platforms, vergelijkingen van technologieën en talloze ideeën. Elektor is ook een geweldige bron van informatie. Sinds de term IoT meer dan 20 jaar geleden werd bedacht, hebben we op onze website meer dan 600 artikelen verzameld over of gerelateerd aan dit onderwerp [1].

Er gaapt echter een diepe kloof tussen een prototype-platform dat het kernconcept van een IoT-oplossing demonstreert, en de praktische verwerkelijking ervan. Het IoT Insights-rapport van Microsoft [2] ondervroeg meer dan 3.000 IoT-professionals in 2021. Het bleek dat 35% van de IoT-projecten mislukt tijdens de test- of de proof-of-concept fase, een toename van 5% ten opzichte van hun enquête van een jaar eerder. Als reden voor mislukking in deze fase worden vooral de hoge kosten van schaalvergroting genoemd. Andere redenen zijn dat er te veel platforms zijn om te testen, te veel use cases om te bewijzen, en een gebrek aan middelen. Een separate studie van Cisco [3] meldde dat slechts 26% van de ondervraagde bedrijven hun IoT-initiatieven succesvol vonden. Uit de reacties op het onderzoek bleek dat de meeste IoT-projecten er op papier goed uit zien, maar in de praktijk complexer blijken dan aanvankelijk gedacht.

Ondanks deze sombere feedback over het IoT in het algemeen, zijn er sectoren waar het IoT aan een enorme opmars bezig is en voor toenemende inkomsten zorgt.

EU-Commissie bekijkt IoT-consumentensector

EU-burgers hebben het aanbod van IoT-oplossingen voor consumenten de afgelopen jaren verwelkomd. Zozeer zelfs dat een rapport over *smart homes* van Statista [4] voorspelt dat de daarmee samenhangende inkomsten zullen verdubbelen van ongeveer 17 miljard euro in 2020 tot ongeveer 38,1 miljard euro in 2025. Bezorgd dat de concurrentie in deze sector wellicht wordt gesmoord, heeft de Europese Commissie een onderzoek ingesteld als onderdeel van haar digitale strategie [5]. In het verslag, dat in januari 2022 werd vrijgegeven, werden reacties verzameld van fabrikanten van draagbare apparaten, *connected* consumentenapparaten die in het smart home worden gebruikt, en van degenen die diensten verlenen via zulke slimme apparaten. Bovendien heeft de Commissie de normalisatie-instellingen om hun mening gevraagd. Bij lezing blijkt echter dat veel paragrafen van de analyse de *voice assistants* (VA) betreffen die de gebruikersinterface vormen voor veel IoT-producten en -diensten (**figuur 1**). Na analyse van het smart home-landschap blijkt uit het rapport [6] dat in Europa *Google Assistant* van Google, *Alexa* van Amazon en *Siri* van Apple de belangrijkste VA's voor algemeen gebruik zijn. Er bestaan ook andere VA's, maar die hebben meestal een beperktere functionaliteit en zijn gericht op de ondersteuning van één enkel product of app van een dienstverlener. Volgens ZDNet biedt Amazon het hoogste niveau van compatibiliteit van de drie grote oplossingen, met ondersteuning voor ongeveer 7.400 merken [7]. Ter vergelijking, Google ondersteunt er ongeveer 1.000, terwijl Apple zeer exclusief blijft, met ondersteuning voor niet meer dan ongeveer 50 merken.

Als we kijken naar het bestaande IoT-landschap, is het duidelijk dat er zakelijke kansen in overvloed zijn, ongeacht of u zich richt op oplossingen voor de consument of voor de industrie.

Weinig ruimte voor VA-nieuwkomers

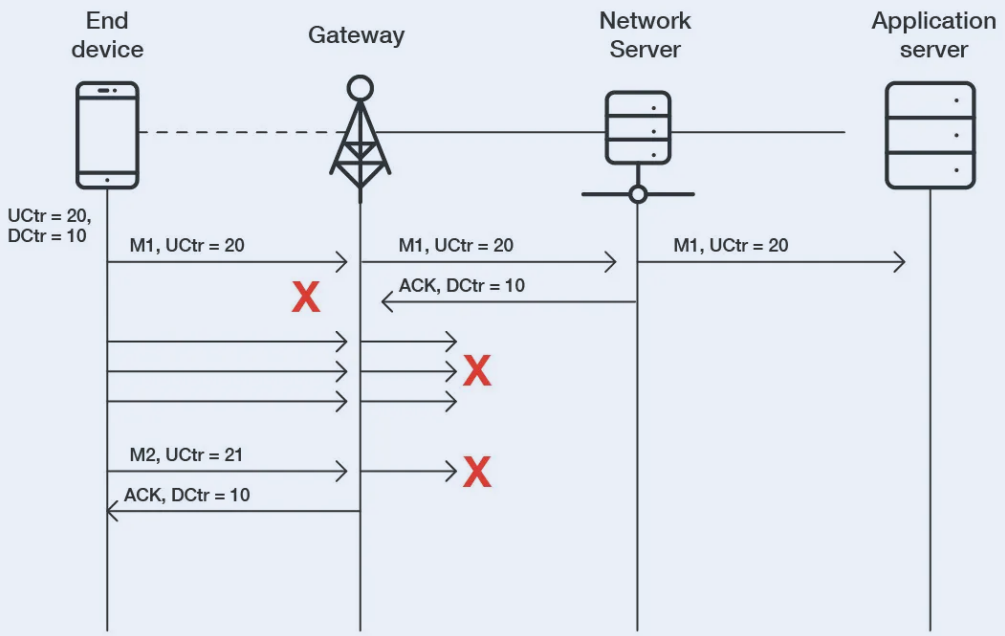
Met zulke machtige en gevestigde spelers is er weinig ruimte voor nieuwkomers, en de technologiecurve om een concurrerende VA te ontwikkelen verloopt zeer steil. Als u dus gebruik wilt maken van spraaksturing voor uw IoT-oplossing, moet u zich conformeren aan de regels die door de grote drie zijn opgesteld. Een alternatieve aanpak zou zijn om een VA in licentie te nemen. Sommige van de ondervraagde fabrikanten meldden echter dat de licentievoorwaarden hun mogelijkheden beperkten. Deze varieerden van exclusiviteit of restricties om te voorkomen dat meer dan één VA tegelijkertijd wordt gebruikt, tot licenties die verplichten tot de opname van andere soorten software of toepassingen, waardoor de VA-technologie niet standalone kan worden gebruikt.

Een ander groot punt van zorg is de toegang tot data. Als derde partij die op een VA-aanbieder vertrouwt, hebt u slechts beperkte toegang tot de verzamelde gegevens. De aanbieder heeft toegang tot de audio-opnames en weet ook hoeveel mislukte pogingen er zijn geweest om de voor uw apparaat geselecteerde opdrachten te geven. Uw eigen team krijgt echter geen toegang tot die opnames, dus u moet veeleer wachten op feedback van gebruikers om te ontdekken dat uw keuze van spraakopdrachten suboptimaal is in een groep die groter is dan die welke voor het testen is gebruikt. Omdat de VA-provider alle mondeling gegeven opdrachten kan analyseren, is het bovendien denkbaar dat hij deze gegevens gebruikt om een oplossing te ontwikkelen die met de uwe concurreert of om de gebruikerservaring van uw IoT-oplossing te gebruiken om zijn eigen diensten te verbeteren.

Een ander probleem doet zich voor wanneer de VA-provider ook reclameservices aanbiedt. In theorie zou de spraak-invoer van uw gebruikers de leverancier kunnen helpen die reclame nauwkeuriger af te stemmen op de demografie van uw klantenbestand.

Tenslotte is er het verlies van merkherkenning en ervaring. Uw zorgvuldig vervaardigde oplossing is overgeleverd aan de grillen en barmhartigheid van de VA. Als zij een belangrijke wijziging doorvoeren, zoals de gebruikte stem, het wekwoord, of zelfs de uitrol van wijzigingen in de functionaliteit die leiden tot een afname van het aantal gebruikers, zult u onvermijdelijk ook de gevolgen ondervinden.

In het verslag worden ook vele andere relevante gebieden onderzocht, waaronder interfaces voor applicatieprogrammering (API's), normen, interoperabiliteit, het gebrek aan machtsevenwicht tussen veel externe ontwikkelaars van IoT-apparaten en de grote



Figuur 2. Onderzoekers ontdekten een Denial-of-Service (DoS)-aanval in LoRa 1.0. Door een eerdere succesvolle gegevensoverdracht opnieuw af te spelen, wordt een LoRaWAN-knooppunt belemmerd bij het verzenden van verdere gegevenspakketten (bron: Trend Micro).

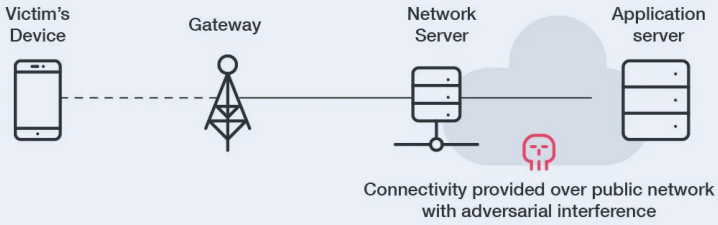
aanbieders van cloud-platform services, en clausules om contracten te beëindigen.
Het verslag bevat geen aanbevelingen. In de conclusies staat echter dat de inhoud van het verslag zal bijdragen aan de standaardiseringsstrategie van de Commissie en wordt meegenomen in het wetgevingsdebat over de Digital Markets Act (DMA).

Beveiligingsproblemen baren zorgen bij IoT-implementaties

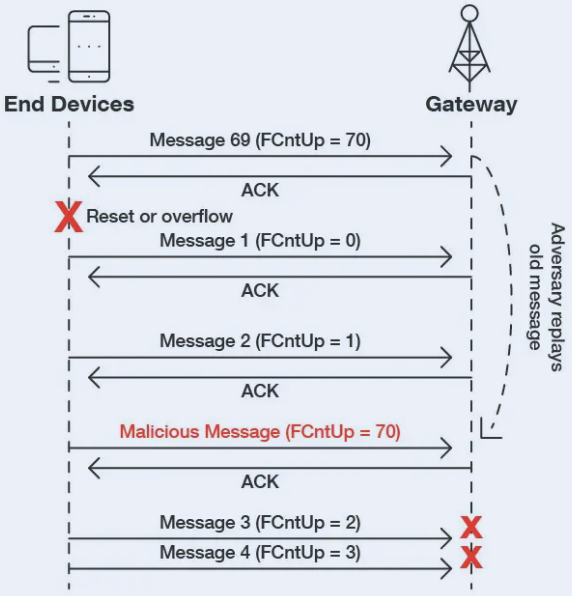
Als we kijken naar de gegevens die zijn verzameld in het IoT Insights-rapport van Microsoft, blijkt dat IoT-beveiliging hoog op de lijst van zorgen staat. Deze kwestie is met name van belang voor degenen die IoT-oplossingen plannen, waarbij 29% aangeeft dat de bijbehorende beveiligingsrisico's hen ervan weerhouden meer gebruik te maken van het IoT. Het rapport legt ook uit dat ongeveer een derde van de organisaties zich zorgen maakt over de veiligheidsrisico's van het IoT, met name datalekken. Om dit tegen te gaan, wordt *outsourcing* genoemd als de beste manier om de gemoedsrust te verbeteren.
Hoewel veel ingenieurs de uitdrukking *"obscurity is not security"* kennen, zijn slechts weinigen op dit gebied bekwaam genoeg om ervoor te zorgen dat een oplossing *end-to-end* beschermd is tegen aanvallers. En hoewel leveranciers van halfgeleiders een reeks enkelchip-beveiligingsoplossingen aanbieden, moeten ontwikkelaars nog steeds leren hoe ze die correct kunnen gebruiken om te voorkomen dat ze onbedoeld nieuwe zwakke punten in de beveiliging introduceren.
In de afgelopen decennia hebben *low-power wide-area network* (LPWAN) oplossingen zoals LoRa en Sigfox zich gevestigd als belangrijke draadloze IoT-technologieën die communicatie over lange afstand ondersteunen. Met een bereik van tientallen kilometers vormen ze een alternatief voor cellulaire draadloze netwerken zoals LTE Cat-M1 en NB-IoT dankzij hun superieure prestaties bij een laag stroomverbruik voor geringe datavolumes [8]. Maar hoe veilig zijn ze?

LoRaWAN onder de loep

LoRa en LoRaWAN zijn bijzonder kritisch bekeken door de beveiligings- en hackers-community. Sébastien Dudek van Trend Micro, een onderneming die zich richt op IT-beveiligingsoplossingen, is een van de onderzoekers die uitvoerig heeft geschreven over een aantal van de potentiële problemen. In een reeks van drie technische artikelen [9][10][11] schetst hij een reeks problemen bij de implementatie, en mogelijke aanvallen. Deze variëren van *Denial of Service* (DoS) (**figuur 2**) en afluisteren tot *bit-flipping* (**figuur 3**) en *spoofing* van ontvangstbevestigingen (**figuur 4**). De gevolgen van dergelijke aanvallen variëren van de onmogelijkheid om met nodes te communiceren en de reductie van de levensduur van de batterij tot het wijzigen van applicatiegegevens.
Veel van de gemelde problemen werden verholpen tussen versie 1.0.2 en 1.1 van de LoRaWAN-norm. Verdere uitdagingen doen zich echter voor wanneer LoRaWAN-knooppunten worden gebruikt met gateways die verschillende versies van de specificatie gebruiken. In dergelijke gevallen is het nodig om wijzigingen aan te brengen om beveiligde achterwaartse compatibiliteit tussen eindapparaten en het back-end te garanderen, zoals benadrukt in een paper uit 2018 van Tahsin C. M. Dönmez [12].
Naast het hacken van de draadloze verbinding is er ook het probleem van kwaadwillenden die de hardware stelen en die rechtstreeks onder handen nemen. Sébastien Dudek gaat ook in op dit beveiligingsaspect. In het geval van LoRaWAN maken veel oplossingen gebruik van een microcontroller (MCU) en een draadloze module van Semtech. Aangezien deze via SPI met elkaar zijn verbonden, kunnen gegevens die tussen de twee worden



Figuur 3. Door de bekende vaste structuur van LoRaWAN-datapakketten is het mogelijk bits om te draaien (bit-flipping attack) in de inhoud zonder dat het bericht hoeft te worden ontcijferd. Hiervoor is toegang nodig tot de netwerkserver die de gegevens ontvangt (bron: Trend Micro).



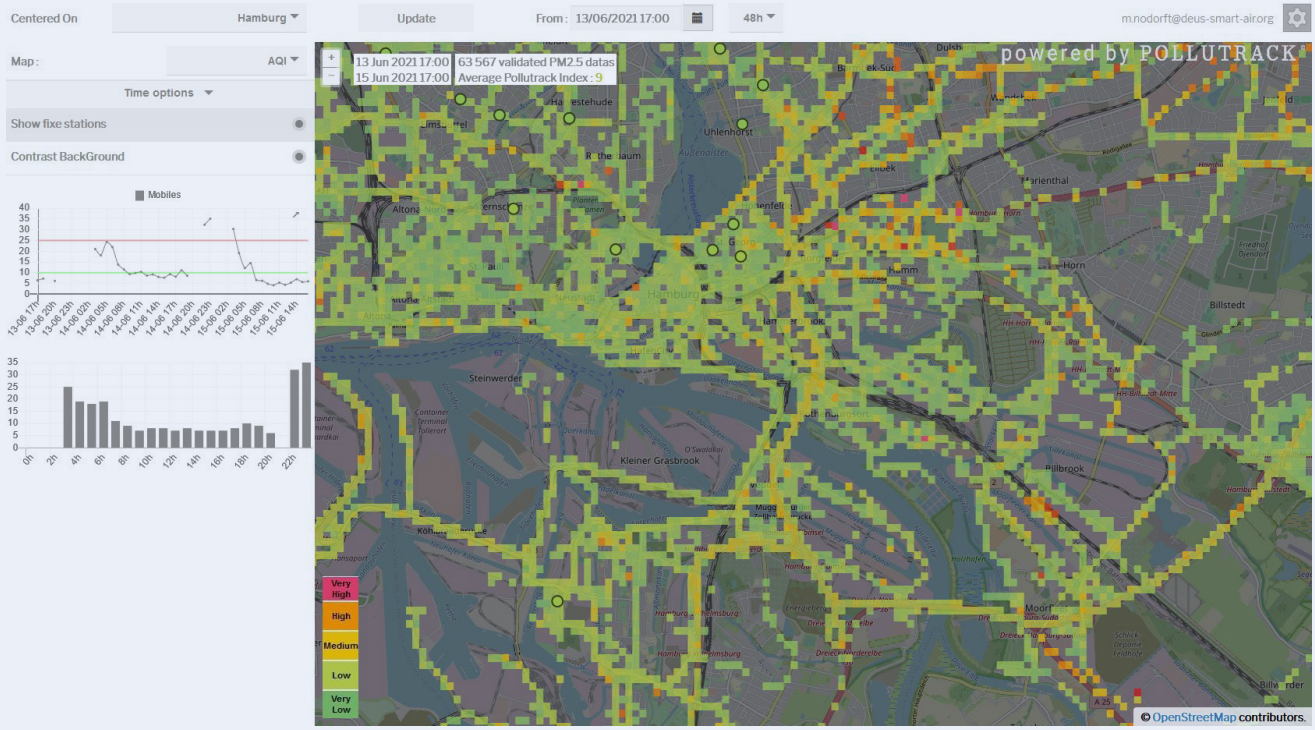
Figuur 4. Verstoring van de draadloze verbinding heeft tot gevolg dat het LoRaWAN-knooppunt de pakketoverdracht tot zeven keer herhaalt, waardoor de batterij minder lang meegaat. Als de aanvaller ook acknowledge-datapakketten (ACK) opvangt en herhaalt, denkt het knooppunt dat de verbinding nog functioneel is omdat ACK-pakketten niet aangeven welk bericht ze bevestigen (bron: Trend Micro).

uitgewisseld gemakkelijk worden afgevangen en geanalyseerd. Daarnaast is er ook nog de kwestie van de beveiliging van de MCU zelf. Eén aanvalsmethode haalt domweg de firmware uit het flashgeheugen, zodat de code kan worden geanalyseerd. Als de beveiligingssleutels zich ook in de firmware bevinden, kan een aanvaller deze gebruiken om nodes te ontwikkelen waarmee authentieke eindapparatuur kan worden nagebootst. De aanbeveling om dit tegen te gaan is het gebruik van Secure Elements (SE), single-chip authenticatie-voorzieningen die encryptiesleutels veilig opslaan. Een aanpak met de ATECC608A van Microchip [13] is een van de vele waarvoor voorbeeldcode beschikbaar is. Hoewel voorbeeldprojecten laten zien hoe de cryptografische sleutels kunnen worden beschermd, wordt de veilige opstartfunctie van dit authenticatiemiddel niet gebruikt. Als dezelfde aanpak voor een product zou worden gebruikt, zou het authenticatiemiddel dus kunnen worden verwijderd en gebruikt als SE met een andere MCU en nieuwe firmware.

Veiligheidsproblemen over de hele linie

LoRaWAN-eindapparaten bieden slechts een beperkte gegevensbandbreedte en zijn niet adresseerbaar, omdat ze geen IP-adres hebben zoals een WiFi-module. Als zodanig vormen ze een minimaal risico voor bedrijfsnetwerken. Er zijn echter potentiele risico's verbonden aan toepassingen die op dergelijke draadloze technologieën zijn gebaseerd. Deze kunnen gevolgen hebben voor mensenlevens en het milieu als er iets misgaat. Als onderdeel van een smart city-netwerk kunnen op LoRa gebaseerde sensoren bijvoorbeeld verantwoordelijk zijn voor het bewaken van het waterpeil om overstromingen te voorkomen. Als de gegevens van de sensoren worden geblokkeerd, kunnen beveiligingssystemen tegen overstromingen eventueel uitvallen. Omgekeerd kunnen verkeerd geïnjecteerde gegevens ertoe leiden dat waterkeringen

Figuur 5. DEUS POLLUTRACK fijnstof-sensoren verzamelen gegevens van stationaire en mobiele IoT-eenheden. De gegevens worden aan het back-end geleverd met behulp van 4G en 5G cellulaire netwerken (bron: DEUS POLLUTRACK).



Figuur 6. Een cloud-gebaseerd dashboard toont het niveau van verontreinigende stoffen in de lucht, in dit voorbeeld de stad Hamburg in Duitsland. Lokale overheden gebruiken dergelijke gegevens om beslissingen te nemen over vervoersoplossingen (bron: DEUS POLLUTRACK).

reageren op een gebeurtenis die niet plaatsvindt, met mogelijk even desastreuze gevolgen.

En hoewel we hier LoRa en LoRaWAN hebben belicht, worden ook andere LPWAN-technologieën onderzocht, waaronder Sigfox en NB-IoT. In een paper van Florian Laurentiu Coman et al. [14] worden verschillende proof-of-concept aanvallen op draadloze netwerken naast LoRaWAN beschreven. In een technisch artikel van Deutsche Telekom [15] wordt gesteld dat de implementatie van Sigfox en LoRaWAN "zonder [een SE] zelfs end-to-end encryptie nutteloos [kan] maken." Er wordt uitgelegd dat NB-IoT daarentegen profiteert van LTE-beveiligingsfuncties die zich bewezen hebben, zoals authenticatie en veilige sleutelgeneratie en -uitwisseling. Het maakt echter ook duidelijk dat end-to-end encryptie niet standaard is en, indien nodig geacht, moet worden besproken met de netwerkoperator.

IoT-oplossingen voor de hele stad

Bezorgdheid over de veiligheid in LPWAN-netwerken beïnvloedde de technologiekeuzes van DEUS POLLUTRACK Smart City GmbH i.G. voor hun IoT-platform [16]. Hun team ontwikkelt al meer dan een decennium IoT-sensornetwerken om fijnstof in steden te monitoren. De technologie wordt ingezet in meer dan 15 Europese steden en stelt lokale bestuurders in staat om weloverwogen milieubeslissingen te nemen met betrekking tot luchtvervuiling. Hun gepatenteerde optische deeltjestellers (OPC) kunnen tot en met de ultrafijne deeltjesclassificatie (UFP) (minder dan 0,1 µm) monitoren. Terwijl grotere deeltjes zoals PM10 als gevaarlijk voor de longen worden beschouwd, kunnen UFP's via ingeademde lucht in de bloedbaan terechtkomen en naar andere organen worden getransporteerd.

De sensortechnologie van DEUS (**figuur 5**) maakt gebruik van een combinatie van stationaire en mobiele sensoren, in een netwerk gekoppeld aan back-end dashboards die de verzamelde gegevens visualiseren. Steden als Marseille en Parijs gebruiken 40 stationaire sensoren, aangevuld met 300 mobiele sensoren [17]. Mobiele sensoren worden gemonteerd op voertuigen van partners, zoals de bestelauto's van DPD, die toch al vaak onderweg zijn in de doelstad. Deze sensoren herkalibreren zichzelf aan de hand van gegevens die zijn verkregen van de stationaire sensoren die ze passeren, om de vereiste nauwkeurigheid te garanderen. Dit alles vereist een robuuste, betrouwbare en veilige LPWAN-keuze.

Mede-oprichter Marc Nodorft legt uit dat tijdens de vroege ontwikkelingsfasen zowel Sigfox als LoRaWAN werden overwogen. Sigfox bood een connectiviteits-infrastructuur die de implementatie van systemen vereenvoudigde, maar geen van beide bood de vereiste gegevensdoorvoer. LoRaWAN was op dat moment niet veilig genoeg en zonder infrastructuur-partners in de steden waar de technologie zou worden ingezet, zou het nodig zijn om gateways te gebruiken die via cellulaire netwerken met het back-end verbonden waren. Daarom werd gekozen voor een 4G en later 5G cellulaire aanpak, waarmee de problemen op het gebied van dekking, betrouwbaarheid en het vereiste beveiligingsniveau werden opgelost.

Nodorft vertelt ook dat er weliswaar veel goedkope elektronische oplossingen voor IoT beschikbaar zijn, maar dat die niet robuust genoeg zijn voor langdurige inzet in de omgevingen waarin hun producten worden geïnstalleerd. Vandaar de keuze om te ontwikkelen volgens industriële standaarden – nog een overweging voor wie zijn eigen IoT-producten plant.

Een ander aspect is het gebruik van het back-end, dat specifiek is ontwikkeld voor de behoeften van hun IoT-implementatie (**figuur 6**). In de toekomst moeten open-source rapportagedashboards worden ondersteund, zodat overheidsinstanties die het

systeem gebruiken zowel als burgers toegang kunnen krijgen tot de gegevens; daarvoor is een cloud-serviceprovider nodig. En hoewel er keuze te over is, wordt de provider even belangrijk gevonden als de technische oplossing. Er wordt dus gezocht naar een provider die persoonlijke ondersteuning kan bieden en niet alleen een onpersoonlijke chatbot voor de klantenservice gebruikt.
Met zoveel ervaring in significante IoT-implementaties en met veel kennis over de technische uitdagingen, vroeg ik me af welk ander advies Nodorft zou kunnen geven aan degenen die IoT-oplossingen willen implementeren. “We zijn altijd trouw gebleven aan onze visie,” antwoordt hij, “wat vaak heeft vereist dat we de aanpak moesten veranderen.” Dat betekende het evalueren van verschillende technologieën, het werken met verschillende partners en het aanpassen van de verkoopstrategie op hun weg naar succes.

Teams van deskundigen en partnerschappen vereist

Als we kijken naar het bestaande IoT-landschap, is het duidelijk dat er zakelijke kansen in overvloed zijn, ongeacht of u zich richt op oplossingen voor de consument of voor de industrie. De weg van concept naar implementatie is echter vol uitdagingen. Hoewel ontwikkelaars van embedded systemen goed thuis zijn in de ontwikkeling van hard- en firmware, en misschien zelfs ervaring hebben met draadloze technologieën, kunnen IoT en de bijbehorende beveiligings- en schaalbaarheidsuitdagingen te veel zijn voor een organisatie om alleen aan te pakken.
Volgens het verslag van de Europese Commissie hebben grote organisaties ook de overhand in zakelijke relaties als het gaat om diensten en platforms. Kleine spelers en start-ups zullen moeite hebben om in eigenregie voldoende steun te krijgen die nodig is in deze asymmetrische relaties. Zonder twijfel is expertise, ingehuurd of geleend, essentieel om verder te komen dan voorbeeldtoepassingen, demonstratie-dashboards en het testen van IoT-diensten. Tot slot is het van vitaal belang om uw visie vast te leggen en tegelijkertijd wendbaar te blijven bij alle aspecten van de implementatie, van technologiekeuze tot doelmarkt, om deze te vervullen.

220053-03

Een bijdrage van
Tekst: **Stuart Cording**
Redactie: **Jens Nickel, C. J. Abate**
Vertaling: **Eric Bogers**
Layout: **Harmen Heida**

Vragen of opmerkingen?
Hebt u technische vragen of opmerkingen naar aanleiding van dit artikel? Stuur een e-mail naar de auteur via stuart.cording@elektor.com of naar de redactie van Elektor via redactie@elektor.com.

WEBLINKS

[1] Elektor IoT-artikelen: www.elektormagazine.com/select/internet-of-things-IoT
[2] “IoT Insights, Edition 3,” Microsoft/Hypothesis, October 2021: https://bit.ly/3rxMk3a
[3] “The Journey to IoT Value,” Cisco, May 2017: https://bit.ly/3GzdJWS
[4] Dr. J. Lasquety-Reyes, “Smart Home - revenue forecast in Europe from 2017 to 2025,” Statista, June 2021: https://bit.ly/3LlGiuG
[5] “Sector inquiry into the Consumer Internet of Things,” European Commission, January 2022: https://bit.ly/3Lgw9iE
[6] “Final report - sector inquiry into consumer Internet of Things,” European Commission, January 2022: https://bit.ly/3B2Htu9
[7] “The best voice assistant,” ZDNet, September 2021: https://zd.net/3rxf6Rt
[8] L. Tan, “Comparison of LoRa and NBIoT in Terms of Power Consumption,” KTH Royal Institute of Technology, January 2020: https://bit.ly/3JafsUb
[9] S. Dudek, “Low Powered and High Risk: Possible Attacks on LoRaWAN Devices,” Trend Micro, January 2021: https://bit.ly/3rA02Tg
[10] S. Dudek, “Gauging LoRaWAN Communication Security with LoraPWN,” Trend Micro, February 2021: https://bit.ly/3LhV0T5
[11] S. Dudek, “Protecting LoRaWAN Hardware from Attacks in the Wild,” Trend Micro, March 2021: https://bit.ly/3rxquge
[12] T.C.M. Dönmez, “Security of LoRaWAN v1.1 in Backward Compatibility Scenarios,” Elsevier, 2018: https://bit.ly/3GtzKq0
[13] Microchip Product Page - ATECC608A: https://bit.ly/3B7zIms
[14] F.L. Coman et al., “Security issues in internet of things: Vulnerability analysis of LoRaWAN, sigfox and NB-IoT,” IEEE, June 2019: https://bit.ly/3uwhUQX
[15] “NB-IoT, LoRaWAN, Sigfox: An up-to-date comparison,” Deutsche Telekom AG, April 2021: https://bit.ly/3uyUydj
[16] DEUS Pollutrack-website: https://bit.ly/3sHL9O5
[17] DEUS Sensor Measurement Network: https://bit.ly/3Gzjbcc