Stratix

Stratix Rapport

Beveiliging OTT-communicatiediensten (NI-ICS)

RAPPORT

Rapport uitgebracht aan
Rijksinspectie Digitale Infrastructuur

Hilversum, 22-5-2023

Managementsamenvatting

Stratix heeft voor de Rijksinspectie Digitale Infrastructuur (RDI) de markt in Nederland onderzocht voor Number-Independent Interpersonal Communication Services (NI-ICS), ook wel aangeduid als OTT (Over-The-Top)-communicatiediensten. Hieronder vallen bijvoorbeeld communicatie-apps zoals WhatsApp en Telegram, en webmail diensten zoals Gmail en Microsoft Outlook.

De door RDI gestelde onderzoeksvraag luidt: **Wat zijn de belangrijkste NI-ICS diensten in Nederland als het gaat om beveiliging?**

RDI heeft gevraagd deze vraag te beantwoorden door een methode te ontwikkelen en die vervolgens uit te voeren, waarmee de onderstaande deelvragen beantwoord kunnen worden:

A. Wat zijn de meest gebruikte NI-ICS diensten in Nederland?
B. Welke NI-ICS diensten zijn het belangrijkst als het gaat om beveiliging?

Resultaat
Dit onderzoek geeft als resultaat een methode om deze diensten te inventariseren en te scoren op de impact die beveiligingsincidenten met zich mee kunnen brengen voor gebruikers. Dit leidt tot een lijst van NI-ICS die in Nederland gebruikt worden, gesorteerd naar het belang met betrekking tot beveiliging.

De belangrijkste diensten ten aanzien van beveiliging op deze lijst zijn, in alfabetische volgorde: Facebook Messenger, FaceTime, Gmail, Google messages (android), iMessage, Instagram, Outlook (voorheen Hotmail), Signal, Snapchat, WhatsApp, Zivver en Zoom.

De gehanteerde methode
De lijst is opgesteld aan de hand van data uit app-stores, literatuuronderzoek, een survey en enkele interviews. Er is gekozen voor deze combinatie van methoden, omdat het niet haalbaar bleek om te starten met een volledige lijst van alle mogelijke diensten en deze stapsgewijs af te lopen en te classificeren. Daarvoor zijn er simpelweg teveel verschillende diensten. De gebruikte combinatie van methoden leidt tot een lijst waarin in ieder geval de meest gebruikte of anderszins relevante diensten zijn opgenomen.

De ordening van diensten vanuit beveiligingsoogpunt kent zes factoren: (aantallen) gebruikers, vervangbaarheid, beschikbaarheid, authenticiteit, vertrouwelijkheid en integriteit. Deze factoren resulteren in een score die uitdrukt wat de impact van een mogelijk beveiligingsincident is. Met deze score kunnen de diensten worden gerangschikt.

Beoordeling methode
De methode geeft antwoord op de onderzoeksvraag, maar kent beperkingen. Vanwege de kwalitatieve opzet is het resultaat vatbaar is voor discussie, met name voor de minder bekende diensten. Een nauwkeuriger resultaat is te verkrijgen door betere data-verzameling. Dit kan bijvoorbeeld door het opvragen van aantallen gebruikers bij de aanbieders, of door het uitzetten van een grootschalig gebruikersonderzoek.

Executive summary

Stratix conducted this research for the Dutch Authority for Digital Infrastructure (RDI) on the Dutch market for Number-Independent Interpersonal Communication Services (NI-ICS), also known as OTT (Over-The-Top)-communication services. Some examples of NI-ICS are communication apps such as WhatsApp and Telegram, and webmail services such as Gmail and Microsoft Outlook.

This report answers the following research question: **What are the most important NI-ICS services in The Netherlands in terms of security?**

RDI has issued to answer this question by developing and executing a method that answers the following sub-questions:

A. What are the most used NI-ICS services in The Netherlands?
B. Which NI-ICS services are most important in terms of security?

Result
This research resulted in a method for identifying and scoring NI-ICS, based on the impact security incidents can have on users. This results in a ranking of NI-ICS services used in the Netherlands, sorted by importance in terms of security.

According to this method, the most important services regarding security are, in alphabetical order: Facebook Messenger, FaceTime, Gmail, Google messages (android), iMessage, Instagram, Outlook (formerly Hotmail), Signal, Snapchat, WhatsApp, Zivver and Zoom.

The method used
The main list with services was compiled using data from app-stores, deskresearch, a survey and a few interviews. This combination of methods is chosen as it was not feasible to start with a complete list of all possible services and ticking them off by classifying them one by one. There are simple too many services. The combination of methods results in a list that includes the most used or otherwise relevant services.

The method used for ranking the services from a security point of view is based on six factors: (number of) users, replaceability, availability, authenticity, confidentiality and integrity. These factors result in a score that expresses the impact of a potential security incident and thus makes it possible to rank the services.

Assessment of the method
Though the method answers the research question, it has its limitations. Due to the qualitative design, the results can be subject to discussion, especially for less well-known services. The accuracy can be improved by improving the data collection, for example by requesting data from providers or by conducting a broad user survey.

Stratix

Inhoudsopgave

1 Aanleiding en achtergrond 5
1.1 Inleiding 5
1.2 Achtergrond, doel en vraagstelling 5
1.3 Aanpak 6
1.4 Afbakening NI-ICS 6
1.5 Leeswijzer 8
2 Deelvraag A: Wat zijn de meest gebruikte NI-ICS diensten in Nederland? 9
2.1 Algemene benadering 9
2.2 Analyse van app stores 9
2.3 Deskresearch 10
2.4 Survey 10
2.5 Interviews 10
2.6 Welke NI-ICS-diensten worden het meest gebruikt in Nederland? 11
3 Deelvraag B: Welke NI-ICS diensten zijn het belangrijkst als het gaat om beveiliging? 12
3.1 Maatschappelijk domeinen NI-ICS 12
3.2 Meest gebruikte functionaliteiten van NI-ICS diensten 13
3.3 Ordening, categorisering en methodiek 14
3.4 Ordening van diensten bepalen met beperkte informatie 15
3.5 Ordening van NI-ICS 15
3.6 Factoren voor de ordening 16
4 Resultaten, conclusies en aanbevelingen 22
4.1 Uitwerking van de methode 22
4.2 Beschouwing van de resultaten 23
4.3 Aanbevelingen voor vervolgonderzoeken en conclusie 26
Annex A Definitie NI-ICS 31
Annex B Methode - analyse Google Play Store 35
Annex C Profiel expert 37
Annex D Uitwerking methodiek ranking 38
Annex E Survey 40

1 Aanleiding en achtergrond

1.1 Inleiding

Stratix heeft de markt in Nederland onderzocht voor Number-Independent Interpersonal Communication Services (NI-ICS), ook wel aangeduid als OTT (Over-The-Top)-diensten. Hieronder vallen onder andere communicatie-apps zoals WhatsApp en Telegram, en webmail diensten zoals Gmail en Microsoft Outlook. In dit rapport gebruiken we de internationale afkorting NI-ICS, die zowel enkelvoud als meervoud kan zijn.

Dit onderzoek beschrijft een methode om NI-ICS te inventariseren. Ook beschrijft het onderzoek een manier om deze diensten te scoren op de impact die beveiligingsincidenten met zich mee kunnen brengen voor gebruikers. Dit leidt tot een lijst van NI-ICS die in Nederland gebruikt worden, gesorteerd naar het belang met betrekking tot beveiliging. De diensten met de hoogste scores worden gezien als de belangrijkste diensten als het gaat om beveiliging.

1.2 Achtergrond, doel en vraagstelling

'Traditionele' communicatiediensten zoals post en telefonie hebben een (eeuwen-)lange geschiedenis van overheidsingrijpen, met als doel om zoveel mogelijk te voorkomen dat essentiële delen van deze diensten uitvallen. NI-ICS hebben die geschiedenis nog niet, terwijl sommige ervan massaal gebruikt worden en daarom naar verwachting belangrijk zullen zijn voor de samenleving.

Het maatschappelijk belang van veilige communicatiediensten is door de Europese Commissie onderkend en onderdeel gemaakt van de Telecomcode[1]. Zo beoogt die om bij te dragen aan de beveiliging van NI-ICS, in overeenstemming met hun maatschappelijk en economisch belang[2].

Het ministerie van Economische Zaken en Klimaat heeft de Telecomcode geïmplementeerd in de Telecommunicatiewet[3]. Hierdoor vallen nu ook de aanbieders van NI-ICS diensten onder de zorg- en meldplicht rondom beveiliging (conform artikelen 11a.1 en 11a.2 van de Telecommunicatiewet).

Waar de aanbieders van bijvoorbeeld telefoniediensten (inclusief "moderne" telefonie als VoIP en nummergebaseerde OTT-diensten) verplicht zijn om zich te registreren bij de Autoriteit Consument & Markt (ACM), ontbreekt een dergelijke verplichting voor aanbieders van NI-ICS. Daardoor is er geen goed overzicht beschikbaar van NI-ICS aanbieders en hun diensten. De Rijksinspectie Digitale Infrastructuur (RDI) wilde daarom een dergelijk overzicht verkrijgen, met daarbij een gedocumenteerde methode die indien nodig herhaald kan worden.

---

[1] Zie Richtlijn (EU) 2018/1972, in de rest van dit rapport aangeduid als de Telecomcode.
[2] Zie overweging 95 uit de Telecomcode
[3] Zie de Wet Implementatie Telecomcode, https://zoek.officielebekendmakingen.nl/stb-2022-83.html

De door RDI gestelde onderzoeksvraag luidt:

Wat zijn de belangrijkste NI-ICS diensten in Nederland als het gaat om beveiliging?

RDI heeft gevraagd deze vraag te beantwoorden door een methode te ontwikkelen waarmee de onderstaande deelvragen beantwoord kunnen worden (en deze methode uit te voeren):

A. Wat zijn de meest gebruikte NI-ICS diensten in Nederland?
B. Welke NI-ICS diensten zijn het belangrijkst als het gaat om beveiliging?

1.3 Aanpak

Voor het onderzoek hebben wij een combinatie gebruikt van deskresearch, interviews, analyse en synthese. Deze paragraaf beschrijft in grote lijnen de aanpak per deelvraag; verdere details zijn in de volgende hoofdstukken te vinden.

1.3.1 Deelvraag A: Wat zijn de meest gebruikte NI-ICS diensten in Nederland?

De eerste stap is om een groslijst te maken van diensten die mogelijkerwijs worden aangemerkt als NI-ICS. Vervolgens zijn deze diensten getoetst aan de criteria voor NI-ICS, afgeleid uit de definities in artikel 2 van de Telecomcode, de bijbehorende overwegingen in de Telecomcode, de implementatie van dit deel van de Telecomcode in de Telecommunicatiewet en de bijbehorende Memorie van Toelichting[4]. Deze criteria worden hieronder kort behandeld en uitgebreider besproken in Annex A.

1.3.2 Deelvraag B: Welke NI-ICS diensten zijn het belangrijkst als het gaat om beveiliging?

Deze vraag bestaat uit twee delen. Eerst moet het maatschappelijk belang (sociaal, economisch, veiligheid) van verschillende NI-ICS in kaart worden gebracht. Hiervoor putten wij uit het literatuuronderzoek dat in deelvraag A is gedaan, aangevuld met actuele, relevante voorbeelden. Hier gaan wij ook in op de belangrijkste functionaliteiten van de meest gebruikte diensten.

Vervolgens is van belang in welke mate diensten een kritieke functie vervullen in de maatschappij en wat de impact is van beveiligingsincidenten. Voor het in kaart brengen van mogelijke beveiligingsrisico's is een methode uitgewerkt op basis van een aangepaste Failure Mode Effect Analysis (FMEA). Deze methode resulteert voor elk NI-ICS in een score, waarmee kan worden bepaald welke diensten het belangrijkst zijn als het gaat om beveiliging.

1.4 Afbakening NI-ICS

Om een lijst van NI-ICS op te kunnen stellen, dienen de criteria waaraan NI-ICS moeten voldoen duidelijk te zijn. De formele grondslag voor die criteria is in eerste instantie artikel 2 van

[4] Zie https://zoek.officielebekendmakingen.nl/kst-35865-3.html

de Telecomcode, met de bijbehorende overwegingen. Voor de verdere interpretatie hebben wij daarnaast gebruik gemaakt van de implementatie in de Telecommunicatiewet[5] en de bijbehorende Memorie van Toelichting[6].

Artikel 2 van de Telecomcode definieert een nummeronafhankelijke interpersoonlijke communicatiedienst (NI-ICS) als volgt:

> *7) „nummeronafhankelijke interpersoonlijke communicatiedienst": een interpersoonlijke communicatiedienst die geen verbinding maakt met openbaar toegewezen nummervoorraden, namelijk een nummer of een aantal nummers in nationale of internationale nummerplannen, of die geen communicatie mogelijk maakt met een nummer of een aantal nummers in nationale of internationale nummerplannen;*

In datzelfde artikel wordt interpersoonlijke communicatiedienst als volgt gedefinieerd;

> *5) „interpersoonlijke communicatiedienst": een gewoonlijk tegen vergoeding aangeboden dienst die directe persoonlijke en interactieve uitwisseling van informatie via elektronischecommunicatienetwerken [sic] tussen een eindig aantal personen mogelijk maakt, waarbij de personen die de communicatie starten of eraan deelnemen, bepalen welke de ontvangers zijn, en die geen diensten omvat die persoonlijke en interactieve communicatie mogelijk maken als een louter bijkomstig kenmerk dat onlosmakelijk verbonden is met een andere dienst;*

Kernbegrippen uit de combinatie van deze twee definities zijn de volgende:

- **Dienst**
- **Gewoonlijk tegen vergoeding aangeboden**
- **Directe persoonlijke en interactieve uitwisseling van informatie**
- **Via elektronische communicatienetwerken**
- **Tussen een eindig aantal personen**
- **Waarbij de personen die de communicatie starten of eraan deelnemen, bepalen welke de ontvangers zijn**
- **Die geen diensten omvat die persoonlijke en interactieve communicatie mogelijk maken als een louter bijkomstig kenmerk dat onlosmakelijk verbonden is met een andere dienst**
- **Die geen verbinding maakt met openbaar toegewezen nummervoorraden**.

Deze kernbegrippen vormen de basis voor de criteria die wij voor de selectie gehanteerd hebben. Een verdere analyse van deze criteria is te vinden in Annex A.

[5] https://zoek.officielebekendmakingen.nl/stb-2022-83.html
[6] https://zoek.officielebekendmakingen.nl/kst-35865-3.html

1.5 Leeswijzer

In hoofdstuk 2 beschrijven we de methode om tot de groslijst van NI-ICS te komen (deelvraag A). Er wordt duiding gegeven bij de verschillende onderzoeksmethoden.

In hoofdstuk 3 geven we antwoord op deelvraag B: Welke NI-ICS diensten zijn het belangrijkst als het gaat om beveiliging? Op basis van literatuuronderzoek en kwalitatieve methoden bespreken we eerst het algemene maatschappelijk belang van verschillende NI-ICS. Vervolgens beschrijven we de methode om een NI-ICS een score toe te kennen.

Hoofdstuk 4 bespreekt de resultaten van het onderzoek, duidt deze resultaten, vat de conclusies samen en geeft aanbevelingen voor vervolg- of herhaalonderzoek.

2 Deelvraag A: Wat zijn de meest gebruikte NI-ICS diensten in Nederland?

Dit hoofdstuk beschrijft de methode om tot de groslijst te komen met de meest gebruikte NI-ICS. De beschrijving moet de lezer in staat stellen dit proces te repliceren, en daarmee de groslijst bij te werken wanneer dit nodig is. In het laatste, concluderende hoofdstuk beschouwen we de methode en doen we aanbevelingen voor het herhalen van het onderzoek.

De groslijst is uit verschillende bronnen opgesteld. Vervolgens hebben wij deze diensten getoetst aan de hand van de eerder vastgestelde criteria, om vast te stellen of ze NI-ICS zijn.

2.1 Algemene benadering

Voor de lijst hebben we geput uit verschillende bronnen, waaronder analyses van verschillende app stores, deskresearch, een survey, interviews met enkele gebruikers en een expertinterview. Deze methode, waarbij informatie vanuit verschillende bronnen wordt samengebracht, levert nog altijd geen complete lijst op met alle NI-ICS die binnen de definitie vallen. Hiervoor is het aantal diensten (wereldwijd) dat voldoet aan de criteria simpelweg te groot. Wel verwachten wij dat de bekendste, belangrijkste en meest gebruikte diensten op deze wijze in de lijst terecht komen. De diensten die niet in beeld komen zullen veelal nichediensten zijn, met een zeer beperkt aantal gebruikers (in Nederland). Dergelijke diensten zijn dan ook minder relevant met betrekking tot het doel van het onderzoek.

2.2 Analyse van app stores

Het gros van de diensten die binnen de scope van dit onderzoek vallen, zijn in app-vorm terug te vinden in de app stores van Google en Apple. Apple beschermt haar Apple store dusdanig dat het niet mogelijk was om hier data van op te vragen; met de store van Google Play was dit wel mogelijk.

De Google Play store is toegankelijker voor app-ontwikkelaars, en bevat zodoende ook meer apps. Bijna alle apps die in de Apple App Store staan, zijn ook terug te vinden in de Play store. Daarom geeft Google Play al een goed beeld van de in gebruik zijnde diensten. Relevante diensten die alleen in de Apple store voorkomen (dat zijn met name de eigen diensten van Apple) zijn via andere bronnen in kaart gebracht.

Hieronder beschrijven we kort de methode om de voor ons relevante apps te vinden in de Google Play store. Een uitgebreidere en meer technische beschrijving is opgenomen in Annex B.

De analyse van de Google Play store is gedaan door ‘onder water’ op de website te kijken. Hiermee hebben wij een lijst gegenereerd met alle apps in een aantal specifieke categorieën. Dit vormt het eerste filter. Wij hebben apps opgehaald uit de categorieën voorpagina-, communicatie-, sociale netwerken-, overheid-, zakelijk-, date-, juridisch-, en zorgapps.

Het tweede filter is op basis van trefwoorden. De lijsten met beschrijvingen van applicaties hebben we doorzocht met trefwoorden die passen bij NI-ICS. De volgende trefwoorden zijn gebruikt: messaging/chat, Voice Call (VOIP), video call/videoconference, location sharing, mail, filesharing, .NL en SIM. De apps die hieruit volgden zijn opgenomen in de groslijst.

2.3 Deskresearch

We hebben verschillende relevante onderzoeken en rapportages gebruikt voor verdere aanvulling van de groslijst. Enkele van deze bronnen zijn ook gebruikt bij het definiëren van de criteria. Een volledige lijst van gebruikte literatuur is te vinden in de bijlage.

Er is beperkt literatuur beschikbaar die specifiek kijkt naar het Nederlandse gebruik van communicatiediensten. Bruikbare stukken zijn onder andere de rapportage *Communication behaviour of Dutch consumers* van Telecompaper (Telecompaper, 2022), dat in een vaste frequentie verschijnt. Rapportages als deze bevatten vaak enkel de meest gebruikte diensten, die grotendeels al via de analyse van de Google Play store naar voren kwamen. Wel geeft de rapportage beter inzicht in de aantallen gebruikers in Nederland, data die niet via de Google Play store kan worden verkregen. Deze informatie is relevant bij het vaststellen van de meest gebruikte en dus meest belangrijke diensten in Nederland.

Naast Nederlandse bronnen hebben wij ook internationale bronnen geraadpleegd. Dergelijke rapporten zijn niet één op één voor Nederland toepasbaar, maar bieden wel context en achtergrond bij de beantwoording van de onderzoeksvragen. Voorbeelden zijn recent werk van de Oostenrijkse RTR (RTR, 2020), BEREC (BEREC, 2016) en (BEREC, 2021a), en de Duitse Bundesnetzagentur (BNetzA, 2020). Deze bronnen geven ook informatie over de definitie, gebruik en soort gebruik van communicatiediensten, waarbij de Oostenrijkse en Duitse onderzoeken vooral betrekking hebben op de situatie in die landen. Alle gebruikte literatuur staat in de literatuurlijst.

2.4 Survey

Naast de eerder gebruikte methoden die op 'grote schaal' communicatiediensten onderzoeken, hebben we een survey gebruikt die is verspreid binnen het netwerk van Stratix. De survey en de resultaten zijn opgenomen in de groslijst.

Doel van de survey was om ook nichediensten te vinden en diensten die niet als app in Google Play zijn terug te vinden. De survey geeft ook een indicatie van het belang van de betreffende diensten. De vragen van de survey zijn te vinden in Annex E.

2.5 Interviews

Tot slot hebben we een expert gevraagd om de groslijst met diensten verder aan te vullen en mogelijke blinde vlekken in de onderzoeksopzet te voorkomen, met name waar het gaat over jongeren en kinderen. Het profiel van deze expert is opgenomen als Annex C.

Ook hebben wij een aantal jongeren in onze eigen omgeving geïnterviewd, om na te gaan of zij diensten gebruiken die nog niet op de lijst stonden.

De resultaten van de interviews leverden geen diensten op die nog niet bij ons bekend waren, maar wel nadere inzichten die in het rapport zijn verwerkt.

2.6 Welke NI-ICS-diensten worden het meest gebruikt in Nederland?

Om vanuit de groslijst tot de lijst met meest gebruikte NI-ICS te komen, is het aantal actieve gebruikers de meest geschikte indicator. Deze informatie is echter niet openbaar beschikbaar.

BEREC geeft ook een aantal indicatoren voor de mate van gebruik (BEREC, 2021a), maar ook die indicatoren zijn niet openbaar en dus voor dit onderzoek niet beschikbaar.

We beschikken wel over de aantallen gebruikers vanuit het onderzoek van Telecompaper (Telecompaper, 2022), gesteund door onze eigen analyse, survey en interviews. Op basis daarvan hebben wij de lijst met veelgebruikte diensten opgesteld.

3 Deelvraag B: Welke NI-ICS diensten zijn het belangrijkst als het gaat om beveiliging?

Het tweede deel van dit onderzoek is het identificeren van de belangrijkste diensten als het gaat om beveiliging. Op basis van literatuuronderzoek en kwalitatieve methoden bespreken we eerst de maatschappelijke domeinen waarbinnen NI-ICS van belang zijn. Vervolgens benoemen we de belangrijkste functionaliteiten.

Hierna volgt de methode die is gebruikt voor de ordening van diensten. Uit verschillende factoren wordt een score berekend. Voor een aantal NI-ICS is deze scoring verder uitgewerkt in Annex D, om de methode te illustreren.

3.1 Maatschappelijk domeinen NI-ICS

Het maatschappelijke belang van verschillende NI-ICS is de rode draad in dit rapport. We onderscheiden drie factoren in de onderzoeksvraag: sociaal, economisch en veiligheid. Deze paragraaf beschrijft aan de hand van die drie pijlers het maatschappelijke belang dat NI-ICS diensten in het algemeen hebben.

De factoren sociaal, economisch en veiligheid en de functionaliteit van een dienst worden kwalitatief bepaald en kunnen zodoende ter discussie staan. Ze worden gebruikt om de beoordeling van diensten van context te voorzien. Om dit transparant en herhaalbaar te maken, zijn voor deze factoren en voor de functionaliteit enkele kernkenmerken vastgesteld. Deze zijn gekoppeld aan een label (S1, E1, V1, etc.); deze labels worden genoemd bij de scores. Zo is in één oogopslag duidelijk in welk domein de betreffende dienst zich bevindt en wat de functionaliteiten zijn ten tijde van het opstellen van deze rapportage.

3.1.1 Sociaal

Gebruikers communiceren via NI-ICS over een veelheid aan onderwerpen. De belangrijkste diensten, zoals WhatsApp, bedienen vele gebruikers. Digitaal contact blijft toenemen, vooral onder ouderen[7]. Bij storingen worden ze nog wel gedeeltelijk vervangen door 'ouderwetse' diensten, zoals SMS. KPN heeft dat gezien tijdens een WhatsApp storing in 2022[8].

Het sociaal belang van diensten wordt voor een belangrijk deel bepaald door het aantal gebruikers van een bepaalde dienst. Wanneer veelgebruikte NI-ICS die voornamelijk in een sociale context worden gebruikt uitvallen, heeft dat meer impact dan wanneer minder gebruikte diensten uitvallen.

Het te onderscheiden kenmerk van het sociale domein is zodoende:

[7] Een jaar met corona (kennisbanksportenbewegen.nl)
[8] https://www.overons.kpn/nieuws/sms-verkeer-piekt-tijdens-storing/

S1 – de mate van sociaal gebruik, hoe meer sociaal gebruik, hoe belangrijker

3.1.2 Economisch

Ook in het werkende leven worden NI-ICS gebruikt. Hieronder vallen maildiensten, berichtendiensten maar ook diensten waarin beide (en vaak nog meer functies) in zijn geïntegreerd. Slack is een voorbeeld van een dienst in de laatste categorie. Wanneer een dergelijke dienst geheel of gedeeltelijk uitvalt, kan dit economische gevolgen hebben.

Ook voor het economisch belang geldt dat het aantal gebruikers invloed heeft op de impact van niet-beschikbaarheid. Daarnaast kennen diensten met een hoge functie integratie, zoals veel maildiensten en diensten als Slack, een groter economisch belang dan diensten met beperktere functionaliteit.

De te onderscheiden kenmerken van het economisch domein zijn zodoende:

E1 – de mate van zakelijk gebruik, hoe meer zakelijk gebruik, hoe belangrijker

E2 – de mate van functie-integratie, hoe hoger, hoe belangrijker

3.1.3 Veiligheid

Bij verschillende diensten ligt het maatschappelijk belang in het domein veiligheid. Veiligheid betekent hier maatschappelijke veiligheid en stabiliteit. Incidenten bij dergelijke diensten hebben mogelijk invloed op de gezondheid, het functioneren van de overheid of het functioneren van de rechtsstaat. Bijvoorbeeld bij Zivver, een beveiligde e-mail in het domein van de gezondheidszorg. Andere diensten waarbij de veiligheid in het geding is bij incidenten zijn bijvoorbeeld veelgebruikte diensten binnen overheden. Dit geldt bijvoorbeeld voor sommige video-call diensten. Ook diensten die gebruikt worden in het geval van nood, bijvoorbeeld de 112NL App, hebben bij uitval gevolgen voor de veiligheid. Diensten die binnen dit domein vallen, zijn over het algemeen minder goed vervangbaar en hebben vaak ook minder gebruikers dan de meeste NI-ICS.

De te onderscheiden kenmerken van het domein veiligheid zijn zodoende:

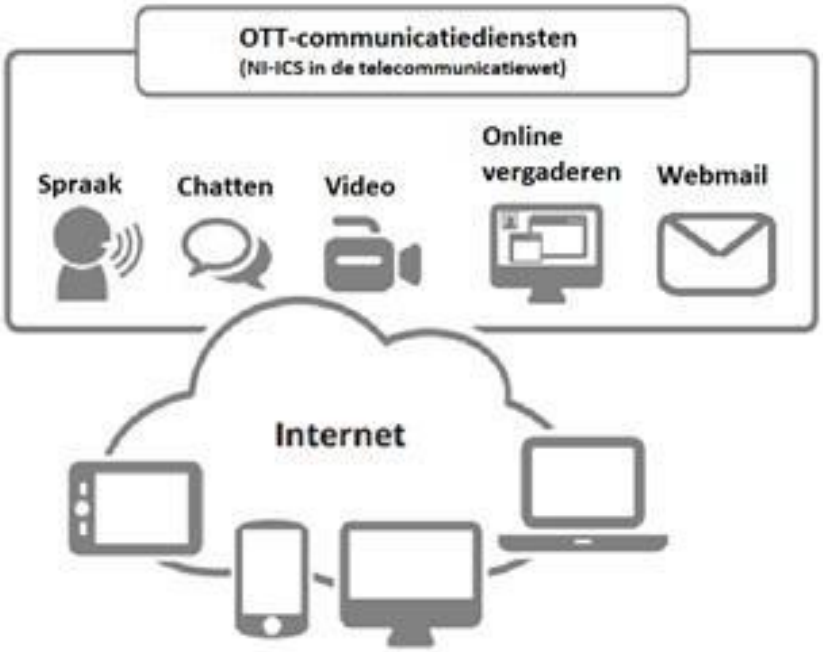
V1 – de dienst kent een specifieke functie gericht op veiligheid (zorg, hulpdiensten)

V2 – de dienst wordt veel gebruikt binnen overheden

3.2 Meest gebruikte functionaliteiten van NI-ICS diensten

NI-ICS kunnen een veelheid aan functionaliteiten bevatten. De functionaliteiten zijn al gedeeltelijk besproken in andere delen van het rapport. Deze paragraaf benoemt dan ook enkel de belangrijkste.

De meest gebruikte functionaliteiten van NI-ICS diensten, zoals beschreven in de eerder aangehaalde literatuur, zijn; messaging/chat, voice call, video call, video conference en e-mail, zoals te zien in onderstaande afbeelding.



De te onderscheiden functionaliteiten zijn zodoende:

F1 – messaging, chat

F2 – voice call, spraak

F3 – video call

F4 – video conference, online vergaderen

F5 – e-mail

3.3 Ordening, categorisering en methodiek

Om te bepalen welke NI-ICS het meest relevant zijn met betrekking tot beveiliging is naast het aantal gebruikers een aantal andere factoren relevant. Het gaat om eigenschappen van de dienst, de manier waarop deze wordt aangeboden en ontsloten, en het gebruik binnen specifieke doelgroepen. Aan de hand hiervan geven wij een praktische en eenvoudige methode voor het bepalen van de relevantie van de dienst in het kader van beveiliging.

De relevantie van NI-ICS wordt bepaald door de gevolgen van eventueel functieverlies in kaart te brengen. Er kunnen problemen optreden met de beschikbaarheid, authenticiteit, vertrouwelijkheid of integriteit. Hiervoor gebruiken we een vereenvoudiging van het 'failure mode effect analysis' (FMEA) model, waarbij we kijken naar bepaalde vormen van functieverlies. Dit model gaat uit van een foutmodus (hoe gaat het fout?), de ernst en de herkenbaarheid als basis voor een ranking.

Dit deel van het onderzoek gaat in op de methode en de voor de beoordeling relevante factoren. In Annex D wordt aan de hand van drie voorbeelden de methode uitgewerkt.

3.4 Ordening van diensten bepalen met beperkte informatie

De meest relevante diensten vanuit het oogpunt van beveiliging zijn lastig te bepalen zonder 'onder de motorkap' te kunnen kijken. Er zijn in elk geval twee benaderingen mogelijk.

De eerste benadering kijkt naar gebruikersaantallen, functie en relevantie in het maatschappelijk verkeer. De tweede benadering kijkt naar de diensten die op technisch gebied de meeste aandacht vragen, aan de hand van bekende beveiligingsincidenten, door specifieke eigenschappen, architectuur en de staat van de systemen.

Het complete plaatje ontstaat bij het gebruik van beide benaderingen. Tegelijkertijd zijn de technische aspecten van een dienst niet openbaar. Bij beperkte informatie dienen we terughoudend te zijn in ons oordeel.

Daarom ordent dit onderzoek de diensten door primair te kijken naar het effect van eventueel functieverlies. In dit perspectief worden ook de sociaaleconomische kenmerken en veiligheidsaspecten betrokken.

3.5 Ordening van NI-ICS

Om NI-ICS diensten te kunnen ordenen op belang van beveiliging is het goed om te kijken naar de significantie van mogelijk beveiligingsincidenten. ENISA, het Europees agentschap voor informatiebeveiliging, geeft enkele handreikingen voor het bepalen van de ernst van een incident. De ENISA *Technical Guideline on Incident Reporting under the EECC* (ENISA, 2021) geeft echter niet aan wat 'significant' is, maar laat die keuze aan de lidstaten. Als suggestie worden parameters meegegeven. De relevantie van een incident kan volgens de ENISA op nationaal niveau worden bepaald aan de hand van onder andere:

- het aantal gebruikers geraakt door het incident
- de duur van het incident
- de geografische reikwijdte van het incident
- de invloed op het functioneren van het netwerk of de dienst
- de invloed op economische en sociale activiteiten

In dit onderzoek ligt de nadruk echter niet op het classificeren van incidenten, maar op het ordenen van de diensten naargelang belang van beveiliging. Hierom komen de duur en de geografische reikwijdte van het incident niet terug in de in het onderzoek gebruikte methode.

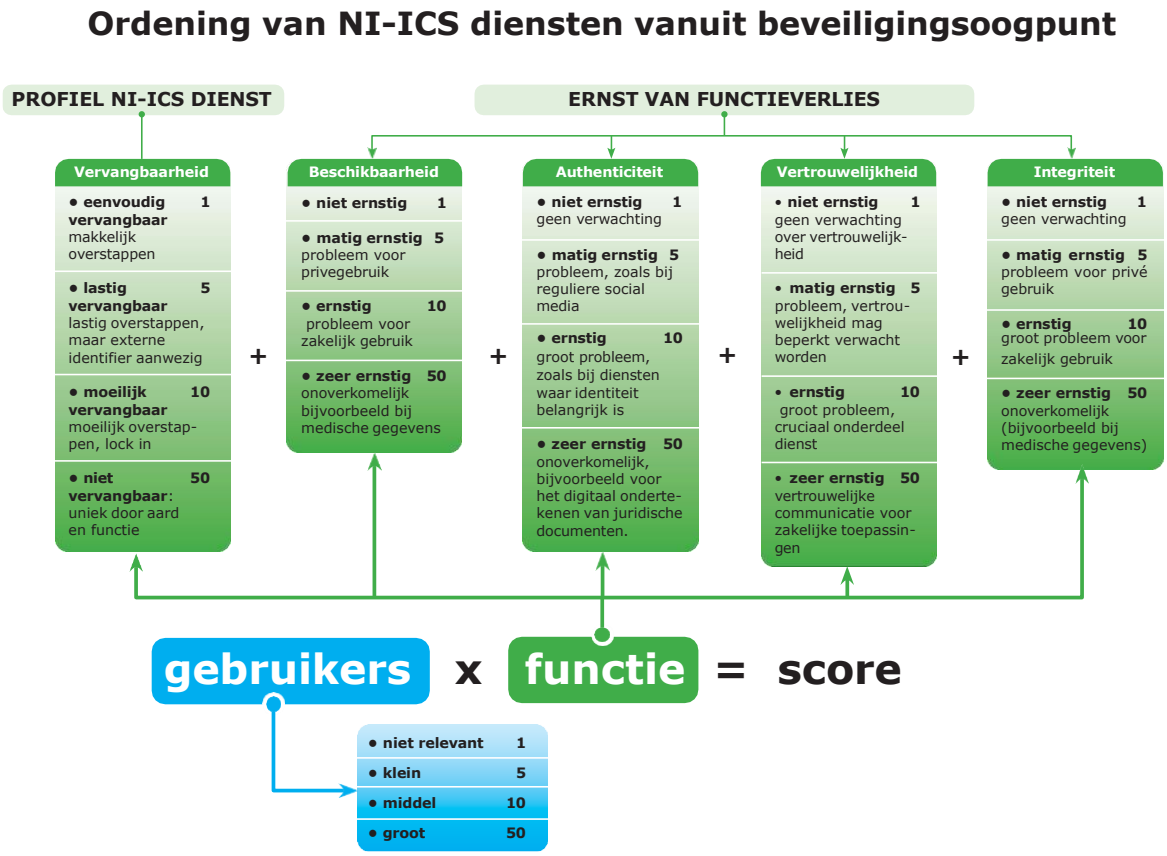
Via een formule op basis van een vereenvoudiging van de FMEA zijn NI-ICS te ordenen naar belang van beveiliging. Foutmodi zijn gedefinieerd op basis van een aantal eigenschappen en functies en gecombineerd tot een score.

De volgende factoren worden onderscheiden:

- Gebruikers van de dienst
- Vervangbaarheid van de dienst
- Belang van beschikbaarheid
- Belang van authenticiteit
- Belang van vertrouwelijkheid
- Belang van integriteit

Per factor worden punten toegekend. Als deze factor niet of nauwelijks relevant is, krijgt deze één punt. Een klein belang weegt voor vijf punten mee, een groot belang voor tien punten. Als een factor van essentieel belang is vanuit beveiligingsoogpunt, krijgt deze de hoogste score van 50 punten.

Het voordeel van deze weging is dat een dienst met bijzondere eigenschappen of grootschalig gebruik er altijd uitspringt en niet gemist wordt.



Figuur 1: Ordening NI-ICS diensten

3.6 Factoren voor de ordening

De factoren worden hieronder toegelicht en uitgewerkt voor toepassing bij het scoren van NI-ICS.

3.6.1 Gebruikers

Het aantal gebruikers van een dienst is in hoge mate bepalend voor de maatschappelijke relevantie. De maatschappij wordt meer geraakt wanneer een veelgebruikte dienst uitvalt. Deze factor is gescoord op basis van de gevonden informatie in deelvraag A. Diensten zijn verdeeld in vier categorieën, waarbij de kleinste categorie een verwaarloosbaar aantal gebruikers kent en de grootste categorie draait om marktleiders zoals WhatsApp, Gmail en iMessage. De diensten zijn ingedeeld op basis van de beschikbare onderzoeksgegevens, zoals uit het onderzoek van Telecompaper voor de Nederlandse markt. Diensten waarvoor deze bron niet beschikbaar is, worden ingedeeld op basis van een inschatting van de gebruikscijfers in internationale context. Deze informatie was niet voor alle diensten voorhanden. Waar deze informatie niet beschikbaar was zijn diensten gescoord aan de hand van informatie uit de survey, naamsbekendheid en informatie van eigen sites of reviewsites.

Categorieën:

A. Niet relevant (tot 10.000).
B. Klein (tot 300.000).
C. Middel (tot 1,5 miljoen).
D. Groot (vanaf 1,5 miljoen)

Gebruikers	**Punten**
Niet relevant (tot 10.000)	1
Klein (tot 300.000)	5
Middel (tot 1,5 miljoen)	10
Groot (vanaf 1,5 miljoen)	50

3.6.2 Vervangbaarheid

De vervangbaarheid van een dienst bepaalt hoe zeer de gebruikers voor hun communicatie aangewezen zijn op deze dienst en hoe eenvoudig of lastig het is om over te stappen. Wordt een dienst zo aangeboden en ontsloten dat deze eenvoudig inwisselbaar is, dan levert dit een ander risicobeeld op dan wanneer een dienst onderdeel uitmaakt van een volledig gesloten systeem.

De vervangbaarheid van de dienst wordt uitgedrukt op vier niveaus:

A. Eenvoudig vervangbaar: het is voor gebruikers makkelijk om van de ene dienst over te stappen op de andere, ook als deze uitgevallen is.
B. Lastig vervangbaar: het is voor gebruikers lastig om over te stappen, maar niet onmogelijk vanwege externe identifiers.
C. Moeilijk vervangbaar: het is moeilijk om over te stappen, omdat alle communicatie en contacten in de dienst besloten liggen.
D. Onvervangbaar: het is niet mogelijk om over te stappen op een andere dienst, omdat deze door de aard en functie een unieke rol vervult of (vrijwel) onvervangbaar is.

Voorbeelden zijn specifieke diensten voor bepaalde doelgroepen met certificering en/of bijzondere functies.

Vervangbaarheid	**Punten**
Eenvoudig vervangbaar	1
Lastig vervangbaar	5
Moeilijk vervangbaar	10
Onvervangbaar	50

De vervangbaarheid wisselt sterk per type dienst. Bij veel chatdiensten is de vervangbaarheid moeilijker, omdat er afhankelijkheid is van een contactenlijst of van groepen die alleen via de dienst bereikbaar zijn. Dit geldt ook voor e-mail, doordat het mailadres gekoppeld zit aan de domeinnaam van de aanbieder ('@gmail.com'). Bij video-/conferencediensten is de vervangbaarheid makkelijker, omdat het gesprek tot stand komt in de context van andere communicatie en de uitnodigingen meestal vooraf worden aangemaakt.

Uiteindelijk is de inrichting van de dienst doorslaggevend. Zo zijn er email-providers die zich aanprijzen met de mogelijkheid om eenvoudig over te stappen, en een eigen domeinnaam aanbieden bij het abonnement op de dienst.

3.6.3 Ernst van functieverlies

Naast het aantal gebruikers en de vervangbaarheid van de dienst wordt functieverlies gebruikt als factor om de relevantie vanuit het oogpunt van beveiliging te bepalen. In vier soorten functieverlies komt het element 'failure mode' uit de FMEA terug, met als doel het vooraf doen van een uitspraak over de impact als een bepaald type fout zich voordoet.

Functieverlies wordt gezien als een verlies van beschikbaarheid, authenticiteit, vertrouwelijkheid of integriteit van de dienst. De aard van een incident of de oorzaak maakt niet uit voor het effect van het functieverlies.

Het effect van verminderde beschikbaarheid, authenticiteit, vertrouwelijkheid of integriteit kan per dienst verschillen. Bij een berichtendienst voor artsen zijn vertrouwelijkheid en authenticiteit cruciaal, want het gaat om medische gegevens. Voor een dienst die vooral voor privégebruik en vermaak wordt ingezet is dit minder van belang.

Beschikbaarheid

Het langdurig niet beschikbaar zijn van een gehele dienst is een zeldzaamheid, maar eenvoudig te detecteren. De gedeeltelijke beschikbaarheid is lastiger te detecteren. De ernst van het effect van het gedeeltelijk of geheel niet beschikbaar zijn van een dienst wordt uitgedrukt in vier niveaus.

A. Niet ernstig: het is geen probleem als de dienst gedeeltelijk of geheel niet beschikbaar is.
B. Matig ernstig: het is een probleem als de dienst gedeeltelijk of geheel niet beschikbaar is, er zijn effecten op sociaal gebied te verwachten.
C. Ernstig: het is een groot probleem als de dienst geheel of gedeeltelijk niet beschikbaar is. De invloed op sociaal en economisch gebied is groot.
D. Zeer ernstig: het is onoverkomelijk als de dienst geheel of gedeeltelijk niet beschikbaar is (bijvoorbeeld bij medische gegevens). De invloed op sociaal en economisch gebied is zeer groot tot onaanvaardbaar en/of er is grote invloed op de veiligheid van de samenleving.

Beschikbaarheid	**Punten**
Niet ernstig	1
Matig ernstig	5
Ernstig	10
Zeer ernstig	50

Authenticiteit

Authenticiteit heeft te maken met de zekerheid met wie je communiceert. Dit valt uiteen in 'weten met wie je communiceert' en 'steeds met dezelfde persoon communiceren'. Een account kan anoniem zijn, maar wel voorzien van goede authenticatie. Een bijzondere categorie betreft diensten die communicatie over documenten aanbieden, zoals ten behoeve van de ondertekening van officiële aktes. Hiervoor is authenticatie van cruciaal belang voor het functioneren van de dienst.

Authenticiteit is voor het sociale- en economische verkeer net zo relevant als voor de veiligheid, het loopt in elkaar over.

A. Niet ernstig: geen verwachting over authenticiteit, zoals bij de basale versies van IRC of email.
B. Matig ernstig: het is een probleem als de authenticiteit niet betrouwbaar is, zoals bij reguliere sociale media. Er zijn effecten op sociaal gebied te verwachten.
C. Ernstig: het is een groot probleem als de authenticiteit niet betrouwbaar is, bijvoorbeeld bij diensten waar identiteit belangrijk is. Er zijn grote effecten te verwachten op sociaal en/of economisch gebied.
D. Zeer ernstig: het is onoverkomelijk als de authenticatie niet betrouwbaar is, bijvoorbeeld voor het digitaal ondertekenen van juridische documenten. De invloed op sociaal en economisch gebied is zeer groot tot onaanvaardbaar en/of er is grote invloed op de veiligheid van de samenleving.

Authenticiteit	Punten
Niet ernstig	1
Matig ernstig	5
Ernstig	10
Zeer ernstig	50

Vertrouwelijkheid

Een deel van de NI-ICS gebruikt end-to-end versleuteling van de communicatie, wat tot doel heeft de vertrouwelijkheid en de integriteit van de berichtgeving te beschermen. In sommige gevallen beschikt de dienstenleverancier zelf over de encryptiesleutels of is er sprake van een versleutelde verbinding tussen de client en een van de servers van de leverancier. Bij e-mail is de verbinding tussen de client en de server vaak versleuteld, maar gaat het mailbericht zelf als platte tekst over het internet. Bij dergelijke communicatie hoeft er bij de ontvanger geen verwachting te zijn omtrent de vertrouwelijkheid en integriteit, tenzij hier aparte maatregelen voor genomen worden.

De ernst van het effect van het gedeeltelijk of geheel verliezen van de vertrouwelijkheid van de communicatie wordt uitgedrukt in vier niveaus:

A. Niet ernstig: geen verwachting over vertrouwelijkheid, bijvoorbeeld omdat het protocol dit al niet biedt (en ook niet pretendeert te bieden).
B. Matig ernstig: het is een probleem als (een deel van) de communicatie niet vertrouwelijk is, er zijn effecten op sociaal gebied te verwachten.
C. Ernstig: het is een groot probleem als (een deel van) de communicatie niet vertrouwelijk is. De invloed op sociaal en economisch gebied is groot.
D. Zeer ernstig: voor vertrouwelijke communicatie, met end-to-end versleuteling voor zakelijke toepassingen. De invloed op sociaal en economisch gebied is zeer groot tot onaanvaardbaar en/of er is grote invloed op de veiligheid van de samenleving.

Vertrouwelijkheid	Punten
Niet ernstig	1
Matig ernstig	5
Ernstig	10
Zeer ernstig	50

Integriteit

Is een bericht compleet en zoals verzonden? De integriteit van de communicatie gaat over de volledigheid en juistheid – niet of het inhoudelijk klopt maar of het exact zo aankomt als de afzender het verzonden heeft. De ernst van een niet volledig of aangepast bericht verschilt tussen soorten communicatie. Dit probleem speelt bijvoorbeeld bij zogeheten 'man in the middle' aanvallen, waarbij iemand de communicatie onderschept, aanpast en als origineel doorstuurt.

De ernst van het effect van het gedeeltelijk of geheel verliezen van de integriteit van de communicatie wordt uitgedrukt in vier niveaus:

A. Niet ernstig: geen verwachting over integriteit, zoals bij de basale versies van IRC of e-mail.
B. Matig ernstig: het is een probleem als de integriteit niet betrouwbaar is, er zijn effecten op sociaal gebied te verwachten.
C. Ernstig: het is een groot probleem als de integriteit niet gewaarborgd is. De invloed op sociaal en economisch gebied is groot.
D. Zeer ernstig: het is onoverkomelijk als de integriteit niet gewaarborgd is, bijvoorbeeld voor het digitaal ondertekenen van juridische documenten. De invloed op sociaal en economisch gebied is zeer groot tot onaanvaardbaar en/of er is grote invloed op de veiligheid van de samenleving.

Integriteit	**Punten**
Niet ernstig	1
Matig ernstig	5
Ernstig	10
Zeer ernstig	50

3.6.4 Ranking

Aan de hand van het profiel[9] van de NI-ICS wordt een score toegekend, waarmee de diensten worden gesorteerd op relevantie vanuit beveiligingsperspectief. Hiermee ontstaat een grof beeld van welke diensten bijzondere aandacht nodig hebben.

$$functie = vervangbaarheid + beschikbaarheid + authenticiteit + vertrouwlijkheid + integriteit$$

$$score = gebruikers \times functie$$

[9] Alle eigenschappen van de dienst die nodig zijn voor het vaststellen van de score.

4 Resultaten, conclusies en aanbevelingen

Dit hoofdstuk bespreekt de resultaten van het onderzoek, duidt deze resultaten, vat de conclusies samen en geeft aanbevelingen voor vervolg- of herhaalonderzoek.

4.1 Uitwerking van de methode

Aan de hand van de methode zijn de diensten geordend vanuit het oogpunt van beveiliging. We lichten de methode toe met een uitgebreide bespreking van een aantal belangrijke diensten. Deze bespreking staat in Annex D. Ten behoeve van de herhaalbaarheid is tevens een overzicht gemaakt van stappen die nodig zijn om dit proces te herhalen.

4.1.1 Ordening

Bij de ordening is voor de volledigheid is ook een aantal diensten meegenomen die niet volledig aan de criteria voor NI-ICS voldoen, maar in het 'grijze gebied' zitten (dit wordt uitgelegd in hoofdstuk 4.2.3). Deze diensten zijn niet opgenomen bij de belangrijkste NI-ICS. De uitwerking waarmee tot de score en de ranking is gekomen is op te vragen bij de onderzoekers.

De NI-ICS die het belangrijkst zijn als het gaat om beveiliging zijn, in alfabetische volgorde: Facebook Messenger, FaceTime, Gmail, Google messages (android), iMessage, Instagram, Outlook (voorheen Hotmail), Signal, Snapchat, WhatsApp, Zivver en Zoom.

In dit rijtje komen zowel diensten voor die veel gebruikers hebben, als diensten die belangrijk zijn vanwege specifieke functies of bijzondere gevoeligheid van gedeelde informatie.

4.1.2 Herhaalbaarheid

Het proces dat heeft geleid tot de bovenstaande indeling kan worden herhaald. Indien er nieuwe NI-ICS op de radar komen, is het interessant om de beoordeling opnieuw te doen. Door het kwalitatieve karakter van de beoordeling is het relevant om meerdere diensten te vergelijken. Zo wordt voor de beoordelaar duidelijk hoe de diensten zich onderling verhouden, welke functies eruit springen en welke waarde deze hebben.

De stappen om de ordening van de NI-ICS te herhalen zijn als volgt:

1- Bij een nieuwe dienst of een herbeoordeling van een bestaande dienst wordt eerst de dienst geïnventariseerd. Wat zijn de eigenschappen, welke diensten worden aangeboden en hoe werken ze? Daarmee kunnen de volgende vragen worden beantwoord:
2- Is de dienst NI-ICS of niet? Ofwel, voldoet de dienst aan de randvoorwaarden voor NI-ICS?
3- Wat is het profiel van de NI-ICS? Hiervoor dient de omvang van het gebruik worden bepaald, bijvoorbeeld met de methodes besproken bij deelvraag A.
4- Wat is de vervangbaarheid van de NI-ICS? Zijn er externe identifiers beschikbaar, wordt de dienst gebruikt in het verlengde van andere communicatie (zoals met

videoconferencing diensten), is er sprake van lock-in mechanismen zoals contactenlijsten of groepen die alleen binnen de dienst beschikbaar zijn?

5- Wat is de ernst van eventueel functieverlies? Die ernst kan worden bepaald aan de hand van de eigenschappen van de dienst. Dit geldt voor de vier factoren beschikbaarheid, authenticiteit, vertrouwelijkheid en integriteit.

Bij het invullen van het model worden de scores zichtbaar. Hier loont het om meerdere diensten te scoren: het model heeft dan de grootste werkingskracht, omdat het om onderlinge verhoudingen gaat.

4.2 Beschouwing van de resultaten

4.2.1 Deelvraag A – Wat zijn de meest gebruikte NI-ICS diensten in Nederland?

Bij het opstellen van de groslijst zijn verschillende opties besproken. Zo is er ook nagedacht over een methode waarbij via een app store een volledige lijst aan communicatiediensten wordt opgevraagd, waarna stapsgewijs de diensten worden verwijderd die niet aan de criteria van NI-ICS voldoen. Dit levert initieel echter een dusdanig grote lijst op (honderdduizenden apps), dat dit binnen het onderzoek geen werkbare methode is. Onder deze lijst vallen bovendien veel diensten met zeer weinig gebruikers (in Nederland). Veel van dit soort diensten, of diensten die om een andere reden onbekend zijn, zouden getoetst moeten worden aan de hand van de criteria, terwijl ze vaak niet relevant zijn voor het onderzoek. Dit kostte te veel tijd om binnen het onderzoek uit te voeren. De huidige methode is minder volledig, maar wel pragmatischer.

Een mogelijkheid om hier mee om te gaan is het stellen van een ondergrens van aantallen gebruikers. Dit brengt echter een aantal problemen met zich mee. Kleine maar zeer belangrijke diensten zouden dan buiten de boot vallen, en bovendien blijkt het niet altijd mogelijk om van een dienst het aantal gebruikers vast te stellen. Dit is vaak alleen te benaderen, bijvoorbeeld door het aantal downloads in app stores. Deze aantallen zijn in de meeste gevallen echter enkel wereldwijd beschikbaar, terwijl het onderzoek zich specifiek richt op gebruikers in Nederland.

Naast de praktische haalbaarheid, is het opvragen van een volledige lijst van diensten met de gebruikte methode alleen mogelijk voor diensten waar ook apps voor zijn. Dit zou neerkomen op het herhalen van de eerste stap in de methode, maar met bredere parameters. Deze methode zou miljoenen apps opleveren die niet eenvoudig te filteren zijn, en nog steeds diensten uitsluiten die niet via een app beschikbaar zijn (zoals sommige maildiensten). Juist deze zijn in beeld gekomen via andere methoden, zoals de survey. Het zou kunnen dat enkele relevante diensten nog ontbreken op de groslijst. Een uitgebreidere survey zou hiervoor een oplossing kunnen zijn, maar paste niet binnen het onderzoek.

4.2.2 Deelvraag B – Welke NI-ICS diensten zijn het belangrijkst als het gaat om beveiliging?

Belangrijk bij deelvraag B is dat de gebruikte methode, conform de opdracht, kwalitatief is, wat inhoudt dat er discussie mogelijk is over de gegeven scores. Om NI-ICS goed te kunnen beoordelen is enige kennis van de dienst wel vereist. Het is niet mogelijk om bijvoorbeeld alleen te vertrouwen op de beschrijving van de dienst in de app stores. Dit zorgt er voor dat de beoordeling arbeidsintensief is. Voor enkele van de facetten, zoals het aantal gebruikers, geldt tevens dat harde cijfers moeilijk te achterhalen zijn en er dus een schatting dient te worden gemaakt. Het verplichten van aanbieders tot het overdragen van de relevante indicatoren zoals die van BEREC (BEREC, 2021a), zou het werk makkelijker maken.

Een ander nadeel van deze kwalitatieve methode is de discussie die kan ontstaan. Dit is goed te illustreren met de vertrouwelijkheid van e-mail-diensten. E-mail kent meestal een mindere mate van beveiliging dan chat-diensten[10], maar de meeste gebruikers zijn niet goed bekend met deze verschillen. Er ontstaat zo dus een discrepantie tussen perceptie en objectieve waardering. De perceptie van gebruikers is echter niet gemeten binnen dit onderzoek, en de beschikbare literatuur betreft slechts enkele specifieke diensten en een internationale context (Abu-Salma et al, 2017), (Al Qahtani et al, 2022). Als dit aspect wel mee wordt genomen (bijvoorbeeld door middel van een bredere survey), wordt het onderzoek en daarmee de resultaten betrouwbaarder.

Naast de facetten die op zijn genomen in de aangepaste versie van de FMEA, is ook het maatschappelijk belang opgenomen in de scoring. Het beschrijven van dit belang (sociaal, economisch, veiligheid) geeft context bij de score. Ook hiervoor geldt dat het een kwalitatieve methode betreft en dat er over de uitkomsten discussie mogelijk is.

Daarnaast kan er een verschil zijn tussen bedoeld gebruik en daadwerkelijk gebruik. Zo zijn veel chat-diensten bedoeld voor sociaal gebruik, maar wordt WhatsApp ook gebruikt voor werk-doeleinden. Dit is enigszins ondervangen door in de survey specifiek te vragen naar diensten die in de privé context en diensten die in professionele context zijn gebruikt, maar een uitgebreidere survey is nodig om hier een betrouwbare uitspraak over te doen.

Tenslotte kan de ordening minder kwalitatief worden gemaakt door als vervolgstap ook technische facetten beter in beeld te brengen. Hiervoor is een combinatie denkbaar van geautomatiseerde scans van via het internet toegankelijke systemen en veiligheidschecks op basis van zelfanalyse door de dienstenaanbieder.

4.2.3 Definitie en grijze gebieden

Om het onderzoek uit te kunnen voeren zijn verschillende facetten uit gangbare definities van NI-ICS gedestilleerd (zie Annex A). Veel diensten voldoen duidelijk aan de criteria uit de

[10] Bij e-mail is de inhoud onversleuteld bij de aanbieder beschikbaar, bij de meeste chat-diensten niet.

Telecomcode, maar er is ook een grijs gebied. Dat blijkt ook uit de literatuur (WIK, 2019a), (WIK, 2019b), (BEREC, 2021b), en uit antwoorden van de Europese Commissie[11].

4.2.4 Ontwikkelingen

De definitie uit de Telecomcode (en de uitwerking in de Telecommunicatiewet) is goed genoeg om de meeste diensten eenduidig te beoordelen. Zoals gezegd zijn er echter nu al diensten die in een grijs gebied vallen, en het is voorstelbaar dat er in de toekomst meer van komen. Daarom bespreken we enkele ontwikkelingen die de huidige definitie onder druk kunnen zetten. Hiermee hopen we te ondervangen dat de definities en methoden in dit onderzoek op korte termijn niet meer relevant of bruikbaar zijn.

4.2.4.1 Manier van communiceren

In de Telecomcode wordt gesproken van inter*persoonlijke* communicatie. In het verlengde hiervan gaat het ook om *personen* die een communicatie starten, *personen* die beslissen wie aan de communicatie deelneemt, en om communicatie tussen een eindig aantal *personen*. Deze manier van definiëren klinkt logisch, maar er zijn nu al diensten die hier niet goed bij aansluiten. Een voorbeeld hiervan is BeReal. Deze dienst laat vrienden met elkaar communiceren door op willekeurige momenten de gebruiker een notificatie te sturen, waarna de gebruiker vijf minuten de tijd heeft om een foto van zijn of haar huidige situatie te maken (en zodoende laat zien wat er 'echt' gebeurt, in tegenstelling tot de 'gefilterde' wereld op andere diensten). Feitelijk gezien is het hierbij dus niet de *persoon* die de communicatie start, maar de dienst. Zodoende sluit de definitie in dit geval niet goed aan bij de manier waarop wordt gecommuniceerd. BeReal voldoet verder wel aan alle criteria en wordt in dit onderzoek wel beschouwd als NI-ICS.

Er komen steeds meer manieren waarop applicaties min of meer de communicatie, en de rol van personen daarin, ondersteunen of gedeeltelijk overnemen. Michiel Kalverda (TMI, zie Annex C), als expert geïnterviewd voor dit onderzoek, verwacht bijvoorbeeld dat communicatie in toenemende mate inspeelt op de behoeftes van de gebruiker, bijvoorbeeld door de inzet van AI (Artificial Intelligence) voor tekstsuggesties. Meerdere e-maildiensten maken hier al gebruik van. Het is dan de vraag in hoeverre nog kan worden gesproken van interpersoonlijke communicatie, wanneer AI de antwoorden voorkauwt, of juist op basis van een paar steekwoorden uitwerkt[12]. Belangrijk om hierbij ook te noemen is de Open AI ChatGPT, die eind 2022 werd uitgebracht en veel indruk maakt binnen de tech-wereld[13].

In het interview kwam ook terug dat het zeker voor jongeren ook niet altijd uitmaakt of ze met een persoon of met een AI/bot chatten. Dit is ook niet altijd even makkelijk vast te stellen, en het ligt voor de hand dat dit in de toekomst alleen maar moeilijker wordt. Communicatiediensten waarbij alleen met bots wordt gecommuniceerd passen niet binnen de huidige

[11] Zie https://www.euractiv.com/wp-content/uploads/sites/2/2021/01/20201027_ePrivacy-derogation_follow-up-questions-COM_0611-clean.pdf
[12] Zie ook (WIK, 2019a).
[13] https://www.nporadio1.nl/nieuws/wetenschap-techniek/3f163607-85a1-4927-af4d-11ea48a9ab60/techwereld-in-ban-van-chatgpt

definitie van NI-ICS, maar er zullen steeds meer gevallen zijn waarbij het voor de gebruiker niet eens duidelijk is of men met een persoon of een bot communiceert.

4.2.4.2 Metaverse

Een manier van communiceren die de definitie in toekomst nog verder onder druk kan zetten is de Metaverse. De Metaverse is een door verschillende techbedrijven voorspelde online omgeving die min of meer functioneert als een kopie van de echt wereld. Deze 'immersive' omgeving, die door veel techgiganten als de volgende grote ontwikkeling wordt gezien, kan worden opgevat als één grote dienst. Een dergelijke digitale omgeving vormt als het ware een soort schil rond mogelijke NI-ICS en andere diensten, die binnen de Metaverse worden aangeboden. Het is niet duidelijk of de Metaverse er komt en hoe deze er uit gaat zien, maar de geschetste toekomstbeelden laten een wereld zien die niet goed aansluit bij de huidige denkwijze over NI-ICS en andere diensten.

4.2.4.3 Games

Veel games bevatten een chat-functie of anderzijds een manier om onderling te communiceren. Voor dit onderzoek hebben we games niet meegenomen, aangezien we deze functies zien als een 'bijkomstig kenmerk' zoals beschreven in criterium 7. Er zijn echter al veel gebruikers voor wie communicatie via games al in grote mate communicatie via diensten als WhatsApp vervangt. Bovendien zijn er games die een dusdanig uitgebreide chatfunctie hebben dat deze bijna als een op zichzelf staande dienst kan worden beschouwd. Bij games als Habbo Hotel of Roblox maakt onderling communiceren in grote mate deel uit van het spel. Deze en andere voorbeelden worden door gamers dan ook veelvuldig gebruikt voor communicatie die niet enkel gericht is op het spel zelf. Ook spellen waarbij gamers voorafgaand aan het 'echte' spel in een lobby met elkaar kunnen communiceren worden, zeker onder jongeren, gebruikt als vervanger voor 'traditionele' communicatiemiddelen. De mate waarin de communicatiefunctie nog een "bijkomstig kenmerk" is, kan daardoor verschuiven. Het antwoord op de vraag of communicatiefuncties binnen games tot NI-ICS behoren, zal dus regelmatig per dienst beoordeeld moeten worden.

4.3 Aanbevelingen voor vervolgonderzoeken en conclusie

De aanbevelingen voor vervolg- of herhaalonderzoek hebben we deels al hierboven benoemd. Voor een betrouwbaarder resultaat dient de dataverzameling voor de groslijst en het scoren te worden verbeterd.

De belangrijkste stap in het opstellen van de groslijst is de analyse van de appstores. Hiermee komen de meest gebruikte diensten in Nederland in ieder geval naar boven. Deze analyse is mogelijkerwijs in te ruilen voor soortgelijke analyses, bijvoorbeeld via een sites die aantallen gebruikers per land bijhouden. Een voorbeeld van een site die dit lijkt te doen is https://app.sensortower.com/top-charts. Stratix heeft echter niet kunnen verifiëren via welke werkwijze ze dit doen en of de data dus betrouwbaar is; op het eerste gezicht lijkt de informatie niet goed aan te sluiten bij andere bronnen.

De dataverzameling kan ook worden verbeterd door het opvragen van informatie bij aanbieders, bijvoorbeeld over aantallen gebruikers, maar ook gedetailleerdere informatie over

beveiliging. Dit is vaak concurrentiegevoelige informatie die dan ook niet gemakkelijk door een onderzoeksbureau kan worden verkregen. Overheden hebben hier meer mogelijkheden voor.

Als in Nederland actieve aanbieders worden gevraagd om een overzicht van de infrastructuur, kan deze informatie worden opgenomen in een geautomatiseerd systeem dat controleert op bekende kwetsbaarheden en veel voorkomende configuratiefouten.

Een voorbeeld hiervan is OpenKAT, de Kwetsbaarheden Analyse Tool die door het Ministerie van Volksgezondheid, Welzijn en Sport is gepubliceerd. Dit systeem kan rapportages toesturen en automatisch alerts genereren als er bevindingen zijn.

Verder is het opzetten van een periodieke representatieve survey een manier om meer inzicht te krijgen in welke, en de manier waarop diensten worden gebruikt. Dit maakt het niet alleen makkelijk om de diensten te scoren, maar brengt ook onbekende diensten in beeld. Daarnaast geeft dit context bij het maatschappelijk belang.

Het expertinterview bleek vooral van belang voor de duiding van de huidige onderzoeksresultaten. Het interview leverde geen diensten op die niet al via andere wegen in beeld kwamen. Het lijkt dus niet zinvol om, met het oog op de groslijst, dit interview te herhalen bij een volgend onderzoek. Ook de overige interviews hebben niet tot additionele diensten geleid.

De Failure Mode Effect Analysis, waaruit de methode voor het sorteren van NI-ICS is voortgekomen, biedt indien uitgevoerd door de aanbieders veel meer mogelijkheden voor het doen van een goede analyse. Er kan worden ingezoomd op realistische fouten, incidenten uit het directe verleden kunnen worden betrokken en per fout kunnen ook mitigerende maatregelen worden benoemd en uitgevoerd.

Deze analyses zijn marginaal te toetsen: het is goed herkenbaar of de analyse door de betrokken technici en het management naar behoren zijn uitgevoerd. Daarnaast zijn ook bevindingen uit bijvoorbeeld OpenKAT mogelijke input voor een FMEA, en vice versa.

Het is lastig om uitspraken te kunnen doen over hoe vaak een herhaalonderzoek nodig is. Er verschijnen regelmatig nieuwe diensten, maar van jaar tot jaar verandert de groslijst weinig. In de looptijd van het onderzoek (circa 8 maanden) is er één noemenswaardige dienst bijgekomen (BeReal). Het jaarlijks herhalen van het eerste gedeelte van de analyse en eventueel een survey lijkt dus ruim voldoende. Nieuwe diensten kunnen vervolgens volgens dezelfde methode worden gescoord.

Voor bestaande diensten geldt dat zaken als aantallen gebruikers, betrouwbaarheid en vervangbaarheid aan verandering onderhevig kunnen zijn. Dat betekent dat diensten periodiek opnieuw moeten worden beoordeeld. Het gebruik van informatie die direct van aanbieders komt, draagt bij aan een exactere score.

Concluderend geeft de methode antwoord op de onderzoeksvraag, maar kent vanwege de kwalitatieve opzet beperkingen waardoor het resultaat vatbaar is voor discussie. Deze beperkingen zijn te ondervangen door betere data-verzameling. Dit gaat bijvoorbeeld over het opvragen van aantallen gebruikers bij aanbieders of het uitzetten van een representatief

gebruikersonderzoek. Hiermee worden zowel de resultaten van deelvraag A als van deelvraag B betrouwbaarder.

Literatuurlijst

Abu-Salma et al, R. (2017). Obstacles to the Adoption of Secure Communication Tools. *IEEE Symposium on Security and Privacy.*

Al Qahtani et al, E. (2022). User Perceptions of Gmail's Confidential Mode. *Proceedings on Privacy Enhancing Technologies.*

BEREC. (2016). *BEREC Report on OTT services.* Opgehaald van https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-ott-services

BEREC. (2021a). *Report on harmonised definitions for indicators regarding OTT services.* Opgehaald van https://www.berec.europa.eu/en/document-categories/berec/reports/berec-report-on-harmonised-definitions-for-indicators-regarding-over-the-top-services-relevant-to-electronic-communications-markets

BEREC. (2021b). *Report on the interplay EECC and DMA on NI-ICS.* Opgehaald van https://www.berec.europa.eu/sites/default/files/files/document_register_store/2021/6/BoR_%2821%29_85_Report_on_the_interplay_EECC-DMA_on_NI-ICS_-_Clean_%28final%29.pdf

BNetzA. (2020). *Nutzung von OTT-Kommunikationsdiensten in Deutschland.* Opgehaald van https://www.bundesnetzagentur.de/SharedDocs/Mediathek/Berichte/2020/OTT.pdf

Bundeskartellamt. (2021). *Sektoruntersuchung Messenger- und Video-Dienste.* Opgehaald van https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Sektoruntersuchungen/Sektoruntersuchung_MessengerVideoDienste_Zwischenbericht.pdf

ENISA. (2021). *Technical Guideline on Incident Reporting under the EECC.* Opgehaald van https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eecc/@@download/fullReport

EU. (2018). *Richtlijn (EU) 2018/1972 (Telecomcode).* Opgehaald van http://data.europa.eu/eli/dir/2018/1972/2018-12-17

RTR. (2020). *Monitoring Interpersonelle Kommunikationsdienste mit Fokus auf Instant Messaging.* Opgehaald van https://www.rtr.at/TKP/aktuelles/publikationen/publikationen/Monitoring_Interpersonelle_Kommunikationsdienste_mit.en.html

Telecompaper. (2022). *Communication behaviour of Dutch consumers.*

WIK. (2019a). *WIK-440: Auswirkungen von OTT-1-Diensten auf das Kommunikationsverhalten.* Opgehaald van https://www.wik.org/uploads/media/WIK_Diskussionsbeitrag_Nr_440.pdf

WIK. (2019b). *Future of voice.* Opgehaald van https://www.wik.org/fileadmin/Konferenzbeitraege/2019/Gigabit_society/Rene_Arnold_20191014_future_of_voice_v4.pdf

Annex A Definitie NI-ICS

In hoofdstuk 1 is de scope van het onderzoek beschreven, onder andere bestaande uit een definitie van NI-ICS, waarbij acht kernbegrippen uit de definitie in de Telecomcode zijn genoemd:

- **Dienst**
- **Gewoonlijk tegen vergoeding aangeboden**
- **Directe persoonlijke en interactieve uitwisseling van informatie**
- **Via elektronische communicatienetwerken**
- **Tussen een eindig aantal personen**
- **Waarbij de personen die de communicatie starten of eraan deelnemen, bepalen welke de ontvangers zijn**
- **Die geen diensten omvat die persoonlijke en interactieve communicatie mogelijk maken als een louter bijkomstig kenmerk dat onlosmakelijk verbonden is met een andere dienst**
- **Die geen verbinding maakt met openbaar toegewezen nummervoorraden**.

Vanuit deze kernbegrippen, en de bijbehorende uitleg in de Telecomcode en de Nederlandse implementatie daarvan, komen wij op de volgende criteria:

1. Dienst

Er moet een dienst geleverd worden. Dat klinkt triviaal, maar niet elke communicatievorm is een dienst: een programma (app) dat rechtstreeks contact maakt met andere apparaten is geen dienst. Na publicatie van de software heeft de leverancier in dat geval geen bemoeienis meer met het gebruik van de software. In het geval van een dienst speelt de leverancier nog wel een rol na publicatie. Dit kan bijvoorbeeld door het beheren van servers waar de dienst gebruik van maakt, en door het faciliteren van beveiliging en encryptie.

Een voorbeeld: vanaf een Android telefoon kan een gebruiker via Bluetooth berichten en bestanden sturen naar andere telefoons in de omgeving. Deze functionaliteit is onderdeel van het Android besturingssysteem. Er is hierbij geen sprake van een dienst, aangezien de leverancier niet betrokken is, en daarmee dus ook niet van een NI-ICS.

iMessage, waarmee Apple-gebruikers berichten kunnen versturen, biedt onder andere encryptie en synchronisatie tussen verschillende apparaten van de gebruiker aan, via een server van Apple. De leverancier of aanbieder speelt dus ook na publicatie van de software nog een rol. iMessage is daarmee dus wel een dienst.

2. Gewoonlijk tegen vergoeding aangeboden

Er moet "gewoonlijk" een vergoeding staan tegenover het leveren van de dienst. Dit hoeft geen (monetaire) betaling door eindgebruikers te zijn, maar kan ook een verdienmodel op basis van advertenties, donaties, subsidies of data zijn. Het ontvangen van advertenties en

het prijsgeven van persoonlijke data hebben immers waarde, en zijn daarmee ook vormen van vergoeding[14].

"Gewoonlijk" impliceert bovendien dat ook een dienst die incidenteel zonder vergoeding wordt aangeboden, toch een interpersoonlijke communicatiedienst kan zijn als er meestal wel een vergoeding gevraagd wordt.

Het is niet altijd duidelijk op welke manier een dienst te gelde wordt gemaakt. Het is ook niet noodzakelijk dat een gebruiker actief bijdraagt aan het ten gelde maken van een dienst.

Diensten die via open source software worden aangeboden, worden vrijwel nooit tegen welke vergoeding dan ook aangeboden. Deze diensten zijn strikt gezien geen NI-ICS, maar zijn wel meegenomen in groslijst.

3. Directe persoonlijke en interactieve uitwisseling van informatie

De dienst moet een "directe" uitwisseling mogelijk maken. Direct moet hier worden opgevat als 'zonder tussenkomst van anderen'. Het versturen en ontvangen van berichten moet dusdanig direct zijn dat er van interactieve communicatie kan worden gesproken. Dat komt neer op vrijwel elke hedendaagse elektronische communicatiedienst.

Ook het soort informatie dat wordt uitgewisseld, kan verschillen tussen en binnen diensten. Voorbeelden van soorten informatie die via NI-ICS worden gedeeld zijn geluid, tekst, afbeeldingen, videobestanden en locatiegegevens.

4. Via elektronische communicatienetwerken

Het gaat uitsluitend om diensten via elektronische communicatienetwerken, zoals gedefinieerd in de Telecomcode. Daaronder vallen vrijwel alle moderne diensten (ook als het een glasvezelnetwerk betreft), maar bijvoorbeeld niet een koeriersdienst. Merk op dat het niet om *openbare* netwerken hoeft te gaan; een (openbare) NI-ICS kan dus ook via een privaat netwerk geleverd worden. Met name diensten die binnen een bedrijf gebruikt worden lopen vaak geheel of gedeeltelijk via de private netwerken van dat bedrijf.

5. Tussen een eindig aantal personen

Hoewel hel aantal personen zeer groot kan zijn, moet het om een eindig aantal personen gaan. De intentie daarvan is duidelijk niet dat de communicatie met "iedereen" of met "alle gebruikers van de dienst" is. Dit sluit platformen zoals Twitter uit (afgezien van de "direct message" functie van die platformen).

Enkele populaire diensten, waaronder Instagram en SnapChat, bieden niet alleen communicatie naar 'vrienden', geaccepteerde volgers of een anderszins afgebakende groep personen. Ze kunnen ook communicatie aanbieden die in principe door iedere gebruiker te lezen of bekijken is. Op 'Mijn verhaal' van SnapChat en Reels van Instagram zijn de foto's en filmpjes (met de juiste instellingen) voor iedere gebruiker te zien. Deze manier van communicatie lijkt al in grote mate op de manier waarop platformen als Twitter werken. Het is echter niet de primaire functie, waardoor SnapChat en Instagram wel gelden als NI-ICS, maar Twitter niet (zie ook

[14] Zie Overweging 16 uit de Telecomcode

criterium 7).Twitter bevindt zich wel in het 'grijze gebied' en wordt meegenomen in het onderzoek.

6. Waarbij de personen die de communicatie starten of eraan deelnemen, bepalen welke de ontvangers zijn

Ook hieruit is duidelijk dat het om besloten communicatie moet gaan, in een door de deelnemers bepaalde groep.

Niet alle diensten tussen een eindig aantal personen voldoen hieraan: de 112NL app verbindt de gebruiker bijvoorbeeld altijd met de 112 alarmcentrale, dus kan de gebruiker feitelijk niet bepalen welke de ontvangers zijn. Die dienst voldoet dus niet aan dit criterium.

Een ander bijzonder geval is Omegle; bij deze app kan de gebruiker met een willekeurige persoon communiceren. Hij kan dus niet bepalen wie de ontvanger is, terwijl de dienst in alle andere opzichten op een NI-ICS lijkt.

7. Die geen diensten omvat die persoonlijke en interactieve communicatie mogelijk maken als een louter bijkomstig kenmerk dat onlosmakelijk verbonden is met een andere dienst

Soms is de communicatie alleen een bijkomstig kenmerk van een andere dienst. Volgens overweging 17 van de Telecomcode dient het begrip "bijkomstig" hierbij restrictief uitgelegd te worden. Dus een dienst die samen met andere (niet NI-ICS) diensten geleverd wordt, kan nog steeds een zelfstandige NI-ICS zijn. Dat levert een grijs gebied op: de spraakcommunicatie in gaming diensten is bijvoorbeeld primair bedoeld als ondersteunend ("bijkomstig") kenmerk bij het spel, maar kan ook als zelfstandige dienst gebruikt worden. Overweging 17 van de Telecomcode geeft dan ook expliciet aan het communicatiekanaal in online spellen in principe, afhankelijk van de kenmerken van de dienst, buiten het bereik van de definitie *zou kunnen vallen*. Er kunnen dus ook gevallen zijn waarbij het er wel binnen valt.

Ook diensten als Instagram en SnapChat, die al eerder genoemd zijn, bieden verschillende soorten van communicatie binnen hun app aan. Het valt niet altijd goed vast te stellen wat het primaire doel of gebruik van een dergelijke dienst is. Hier komt bij dat er een verschil kan zitten tussen het bedoelde gebruik en het daadwerkelijke gebruik. Zo wordt de populaire app Wordfeud, een op Scrabble gelijkend spel, door veel gebruikers ook als communicatiemiddel gebruikt. De Telecomcode maakt geen onderscheid tussen bedoeld gebruik en daadwerkelijk gebruik.

Het kan andersom ook voorkomen dat een initieel als NI-ICS bedoelde dienst ook voor andere middelen wordt ingezet. Zo wordt Slack, bedoeld om chatgesprekken in groepen en teams te faciliteren en vooral gebruikt in een professionele setting, steeds meer als een soort intranet gebruikt. De dienst als geheel overstijgt op die manier de definitie van NI-ICS, maar de communicatiefunctie blijft NI-ICS.

Een andere categorie diensten die onduidelijkheid op kunnen leveren zijn datingapps. Gebruikers van deze apps zijn een groot gedeelte van het gebruik bezig met het bekijken van

profielen en daarop te reageren. Het hoofddoel van de app is echter wel het communiceren met matches. De meeste dating apps zullen zodoende wel binnen dit criterium vallen.[15]

8. Die geen verbinding maakt met openbaar toegewezen nummervoorraden

De dienst heeft geen koppeling met openbare telefoonnummers en met de daarop gebaseerde netwerken (zoals de diensten SkypeIn en SkypeOut dat wel hebben). Er zijn wel NI-ICS die telefoonnummers als unieke identiteit gebruiken (zoals WhatsApp). Deze diensten, waarbij het telefoonnummer alleen als identificerende eigenschap gebruikt wordt maar niet voor de verbinding, gelden als nummeronafhankelijk.[16]

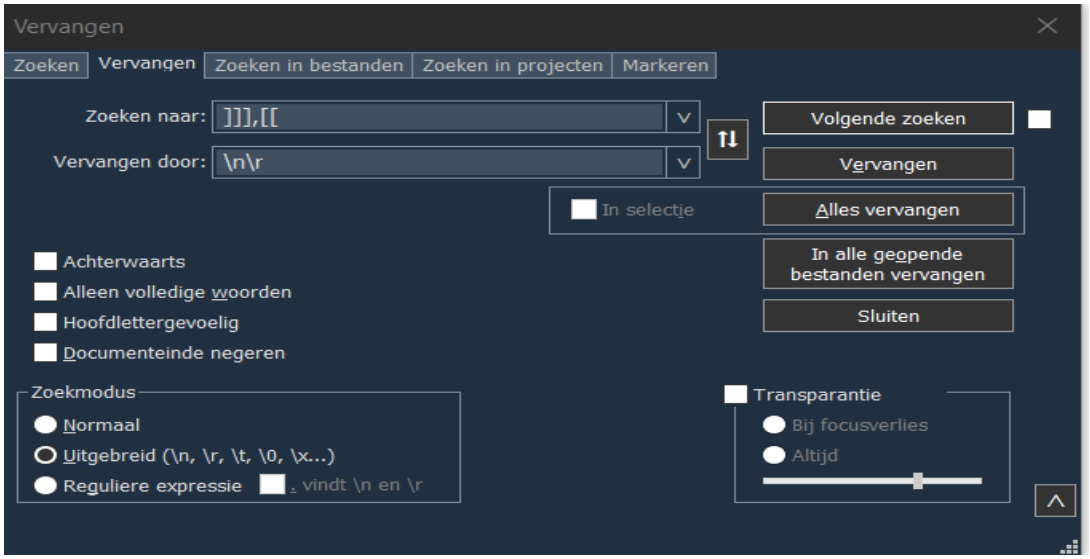
[15] https://www.euractiv.com/wp-content/uploads/sites/2/2021/01/EP-questions-9-October-final.pdf
[16] Zie Overweging 18 uit de Telecomcode

Annex B Methode - analyse Google Play Store

De methode bestaat uit twee stappen. In de eerste stap worden de extensies verzameld die 'onder water' vindbaar zijn per categorie. In de tweede stap wordt alle gegevens opgehaald per app die relevant zijn voor de scope van dit onderzoek. Tijdens dit onderzoek zijn alle gegevens in een tekstdocument verwerkt en geanalyseerd, maar het is ook mogelijk om de gegevens in een database te zetten. De categorieën die onderzocht worden zijn: voorpagina-, communicatie-, sociale netwerken-, overheid-, zakelijk-, date-, juridisch-, en zorgapps. Als alle gegevens van de apps en de categorieën tot één document zijn samengevoegd wordt het document handmatig doorzocht met de volgende trefwoorden: Messaging/chat, Voice Call (VOIP), video call/videoconference, location sharing, mail, files-sharing, .NL en SIM. Hieronder wordt een voorbeeld gegeven waarbij gegevens worden verzamelend bij de categorie "sociale netwerken".

Stap 1: extensies per categorie verzamelen

Ga naar de volgende link https://play.google.com/store/apps/category/ en typ hier je gewenste categorie in bijvoorbeeld: sociale netwerken. Zoek 'onder water' naar de eerste app die je op de pagina linksboven kunt zien. Klik vervolgens drie keer herhaaldelijk op de linkermuisknop om de blok met code te selecteren. Kopieer dit blokje in notepad++ en vervang]]],[[met \n\r zoals in de afbeelding hieronder is weergegeven. Sla dit document vervolgens op als sociale_netwerken_**in**.



Vervolgens wordt het script dat hieronder is weergegeven gebruikt om de extensies klaar te maken voor stap twee. Er ontstaat een nieuwe file genaamd sociale_netwerken_**out** met de desbetreffende extensies voor die categorie. Met het script hieronder weergegeven wordt er automatisch een file sociale_netwerken_**out** aangemaakt. In deze file zitten de extensies en zullen gebruikt worden voor stap 2.

```python
import re

fhandle_in = open("sociale_netwerken_in.txt",'r', encoding="utf-8")  #document met ongefilterde apps
fhandle_out = open("sociale_netwerken_out.txt", 'w', encoding="utf-8") #document met gefilterde apps


for line in fhandle_in:
    deel = line.find(",7],")
    app = line[:deel]
    app = re.sub('[^a-zA-Z0-9 \n\.]', '', app)
    final_app = app.find('null')
    if final_app == -1:
        fhandle_out.write(app+'\n')
        print(app)

fhandle_in.close()
fhandle_out.close()
```

Stap 2: Gegevens per extensie verzamelen

Via de link: https://play.google.com/store/apps/details?id= gecombineerd met een extensie zoals https://play.google.com/store/apps/details?id=com.viki.android kom je bij een app uit. Met het onderstaande script kunnen de gegevens van deze apps opgehaald worden met behulp van de in stap 1 verkregen extensies. De file die eruit komt is in dit geval sociale_netwerken_data. Kopieer de gegevens naar één tekstdocument. Aan dit document zullen ook de gegevens van de apps uit de andere categorieën worden toegevoegd.

```python
from bs4 import BeautifulSoup
import ssl
from urllib.request import Request, urlopen

fhandle_in = open("sociale_netwerken_out.txt",'r', encoding="utf-8")
fhandle_out_data = open("sociale_netwerken_data.txt",'w', encoding="utf-8")

lst = list()

for app in fhandle_in:
    app = str(app)
    stripped = app.rstrip("\n")
    lst.append(stripped)
    print(lst)
ctx = ssl.create_default_context()
ctx.check_hostname = False
ctx.verify_mode = ssl.CERT_NONE

url = "https://play.google.com/store/apps/details?id="

for i in lst:
    url = "https://play.google.com/store/apps/details?id="+i
    uh = Request(url, headers={"User-Agent": "Mozilla/5.0"})
    try:
        webpage = urlopen(uh).read().decode()
        soup = BeautifulSoup(webpage, "html.parser")
        tekst = soup.find(class_="bARER")
        tekst = str(tekst)
        tekst = tekst.replace("<br/>", "\n")
        app = "\n"+"APP TEKST*******************" + i + "***********APP TEKST"
        fhandle_out_data.write(app+"\n")
        fhandle_out_data.write(tekst)
    except:
        continue
fhandle_in.close()
fhandle_out_data.close()
```

Annex C Profiel expert

Michiel Kalverda – Algemeen directeur TMI (https://www.tmi.one/)

Michiel Kalverda is na zijn opleiding journalistiek in 2015 met het nieuwskanaal TMI begonnen en heeft dit middels TMI.academy doorontwikkeld tot een kenniscentrum dat zich richt op het onderwijzen van digitale geletterdheid op scholen. In deze hoedanigheid komt hij veel in aanraking met de manier waarop jongeren met internet en media omgaan. Hij is geïnterviewd als expert op het gebied van communicatiediensten onder jongeren en ontwikkelingen op dit gebied.

Annex D Uitwerking methodiek ranking

WhatsApp

WhatsApp is een chatprogramma dat intensief wordt gebruikt, dit vanwege bijvoorbeeld de mogelijkheid groepen aan te maken en het netwerkeffect van brede adoptie. Het programma kent een externe identifier (telefoonnummer) en bindt gebruikers onder andere door groepsberichten. WhatsApp kent zakelijk en privégebruik, en legt sterk de nadruk op veilige communicatie.

De labels die aan WhatsApp worden toegekend conform paragraaf 3.1 zijn S1 (grote schaal), E1 (zakelijk gebruik), V1 (functies voor veilige communicatie), V2 (gebruik binnen de overheid).

Dat leidt tot de volgende scores: Gebruikers: 50, alomtegenwoordig

Vervangbaarheid: 5, doordat WhatsApp gebruik maakt van telefoonnummers heeft de gebruiker altijd de mogelijkheid zijn contacten via SMS te bereiken.

Beschikbaarheid: 10, WhatsApp wordt gebruikt voor zowel zakelijke als privé communicatie.

Authenticiteit: 10, gekoppeld aan telefoonnummer, actief misbruik door social engineering.

Vertrouwelijkheid: 10, cruciaal onderdeel, relevant voor zakelijk en privégebruik.

Integriteit: 10, verwachting: volledig en correct, mede door end-to-end encryptie.

Zivver

Mail of een add-on voor mail conform NTA7516, een standaard voor incidentele communicatie in de zorg. Zivver heeft weinig gebruikers maar is door de certificering als NTA7516 dienst lastig te vervangen. Door het gebruik voor zorginformatie zijn beschikbaarheid, vertrouwelijkheid en betrouwbaarheid belangrijk. Het lage aantal gebruikers resulteert in een lagere score.

De labels die aan Zivver worden toegekend zijn S2 (vervangbaarheid is laag), E1 (zakelijk gebruik), V1 (functies voor veiligheid), V2 (gebruik binnen de overheid).

Gebruikers: 5 – de schaal van Zivver is erg klein

Vervangbaarheid: 10 – het overstappen op een andere dienst is moeilijk door de aan Zivver gekoppelde certificering.

Beschikbaarheid: 50 – het niet beschikbaar zijn van Zivver leidt tot ernstige problemen in de communicatie tussen medici, bijvoorbeeld bij het uitwisselen patiëntinformatie.

Authenticiteit: 50 – de betrouwbaarheid van de communicatie is cruciaal onderdeel van de dienst.

Vertrouwelijkheid: 50 – vertrouwelijkheid van medische gegevens is cruciaal onderdeel van de dienst.

Integriteit: 50 – de volledigheid en correctheid van de berichten zijn een cruciaal onderdeel van de dienst.

Gmail

Gmail is een gratis e-maildienst die massaal gebruikt wordt. Vervangbaarheid is lastig door lock-in van het e-mailadres (naam@gmail.com). Het is een van de meest gebruikte NI-ICS. Hoewel de perceptie bij gebruikers mogelijk anders is, kunnen door de aard van het protocol (platte tekst email) de authenticiteit, vertrouwelijkheid en integriteit niet gegarandeerd worden. Gmail heeft geen end-to-end beveiliging, waardoor Google en eventueel andere betrokken mailproviders volledig toegang hebben tot de inhoud.

De labels die aan Gmail worden toegekend zijn S1 (grote schaal), S2 (vervangbaarheid is laag), E1 (zakelijk gebruik).

Gebruikers: 50 punten, Gmail is een veel gebruikte emaildienst.

Vervangbaarheid: 10, het mailadres is gebaseerd op name@gmail.com, accounts kunnen niet makkelijk worden vervangen.

Beschikbaarheid: 10, de dienst kent veel dagelijkse zakelijke en privé communicatie.

Authenticiteit: 10, als derden toegang hebben tot de mailboxen is dat een groot probleem voor privé en zakelijk gebruik.

Vertrouwelijkheid: 1 punt, er zijn geen verwachtingen over de vertrouwelijkheid van plaintext email.

Integriteit: 1 punt, er zijn geen verwachtingen over de integriteit van plaintext email.

Annex E Survey

De volgende (open) vragen maakten deel uit van de survey:

Welke communicatiediensten gebruikt u voor uw werk, binnen uw bedrijf? Voorbeelden zijn Microsoft Teams, Slack of WhatsApp.

Welke communicatiediensten gebruikt u voor uw werk, buiten uw bedrijf (klanten, business partners, etc.)? Voorbeelden zijn Microsoft Teams, WhatsApp of Microsoft Outlook.

Welke communicatiediensten gebruikt u privé? Voorbeelden zijn WhatsApp, Instagram of Snapchat.

Welke communicatiediensten zijn dusdanig essentieel voor uw werk dat het uitvallen ervan voor problemen zou zorgen?

Welke communicatiediensten zijn voor u dusdanig essentieel op privégebied dat het uitvallen ervan voor problemen zou zorgen?

Welke communicatiemiddelen zou u niet missen wanneer ze niet meer zouden bestaan?

Stratix B.V.
Villa Looverhoek – Julianalaan 1
1213 AP Hilversum

Telefoon:	+31.35.622 2020
E-mail:	office@stratix.nl
URL:	http://www.stratix.nl
Reg. no.:	57689326
IBAN:	NL85ABNA0513733922
BIC:	ABNANL2A
VAT:	NL8526.92.079.B.01