Onderzoek scenario's voor Nationaal Diensten Centrum

Auteurs	André den Breejen (Opdrachtverantwoordelijke)
	Frank van Dam
	Michelle Custers

Opdrachtgever	Kevin Joosten (Ministerie van OCW)
Versie	1.1 Definitief
Datum	5-3-2024

Departementaal vertrouwelijk - Dep-V

Inhoudsopgave

1 Voorwoord 4

2 Managementsamenvatting 5

3 Inleiding 10

3.1 Vraagstelling vanuit OCW 10

3.2 Veilig Internet en Nationale Diensten Centrum 11

3.3 Aanpak van het onderzoek 11

3.4 Leeswijzer 11

4 Beschrijving van de dienst 12

4.1 Dienst Veilig Internet (VI) 12

4.2 Nationaal Dienstencentrum (NDC) 12

4.3 NDC in relatie tot scope onderzoek 12

4.4 NDC afhankelijkheden en scenario's 15

4.5 Tussenconclusie 1 16

5 Techniek, security, beveiliging en processen 18

5.1 Opzet interne review 18

5.2 Techniek, security en beveiliging 18

5.3 Proces en organisatie 19

5.4 Marktconformiteit 19

5.5 Scenario's en mogelijkheden schoolbesturen 20

5.6 Tussenconclusie 2 22

6 Interviews schoolbesturen 23

6.1 Opzet interviews schoolbesturen 23

6.2 Uitkomsten interviews schoolbesturen 23

6.3 Tussenconclusie 3 25

7 Juridische en financiële kaders 26

7.1 Juridische kaders voor verplichting 27

7.2 Tussenconclusie 4 27

7.3 Financiële kaders 27

7.4 Tussenconclusie 5 28

8 Kosten, baten en prognose aansluitgraad 29

8.1 Kosten en prognose 29

8.2 Kosten en tarieven Veilig Internet 31

8.3 Overige baten van het NDC 31

8.4 Tussenconclusie 6 32

Departementaal vertrouwelijk - Dep-V

9 Argumenten no go / go besluit 33
9.1 Argumenten no go besluit 33
9.2 Argumenten go besluit 33
10 Scenario's no go/go 35
10.1 Scenario no go 35
10.2 Scenario go 36
11 Bijlage: Interviewleidraad schoolbesturen en tabel met bevindingen 37
12 Bijlage: Onderzoek techniek en processen 42
13 Bijlage: Alternatieven voor beveiligingsmaatregelen 45
14 Bijlage: Kosten en prognose NDC (bron: Kennisnet) 48

Departementaal vertrouwelijk - Dep-V

1 Voorwoord

In gezamenlijkheid met de betrokken organisaties is gewerkt aan dit onderzoek. Dit levert nadere inzichten in de kwaliteit en opbouw van de techniek en processen van het NDC. Daarnaast is indicatief een beeld opgehaald bij een aantal schoolbesturen, waarmee de context en de beleving beter geduid kan worden. Onze dank gaat uit naar alle betrokken partijen die hebben meegewerkt aan het onderzoek.

Voor een betere duiding van draagvlak voor een technische voorziening zoals het NDC, zal uitgebreider en nader onderzoek nodig zijn. De geschetste beelden in dit rapport zijn op een beperkt aantal waarnemingen gebaseerd.

In deze rapportage wordt gesproken over additionele middelen en financiering of structurele financiering vanuit OCW. Het uitgangspunt voor dit onderzoek is geweest het onderzoeken van mogelijkheden en scenario's voor de toekomst van het NDC na het aflopen van de huidige (eenmalige) subsidieverlening. In de bijgestelde afspraken over deze subsidie is vastgelegd dat de bestaande subsidie doorloopt tot en met 2026.

Departementaal vertrouwelijk - Dep-V

2 Managementsamenvatting

Het ministerie van Onderwijs, Cultuur en Wetenschap (OCW) is voornemens een besluit te nemen over de financiering van een centrale voorziening voor Veilig Internet (VI) in het Funderend Onderwijs (FO). OCW heeft tot op heden het Nationale Diensten Centrum (NDC) gefinancierd door een eenmalige subsidie beschikbaar te stellen aan Kennisnet. Deze eenmalige subsidie is toereikend tot 2027. Omdat scholen de zekerheid wordt geboden een driejarig contracten af te sluiten is het ministerie voornemens begin 2024 een besluit te nemen over het al dan niet continueren van de financiering van het NDC.

ICTU heeft in opdracht van het ministerie van OCW ter voorbereiding aan deze besluitvorming onderzoek gedaan naar de volgende onderdelen:

Beschrijving van de dienst NDC

- Schoolbesturen zijn zelf verantwoordelijk voor het goed organiseren van veilig internet, het Normenkader Informatiebeveiliging en Privacy (IBP) voor het Funderend Onderwijs (FO) is hierbij helpend.
- De veiligheid voor internettoegang zoals deze door schoolbesturen wordt georganiseerd, kent een groot aantal varianten en bijbehorende afhankelijkheden waarmee geen eenduidig beeld geschetst kan worden over de werking en veiligheid daarvan. De meest voorkomende varianten, naast het NDC, zijn in twee aanvullende alternatieven uitgewerkt.
- De voorziening die voor het NDC is opgebouwd, biedt het meest complete pakket aan beveiligingsmaatregelen.
- Alle schoolbesturen in het FO kunnen gebruik maken van het NDC, de techniek en de aansluitvoorwaarden zijn hierop ingericht en op dit aspect voldoet het NDC aan de voorwaarden voor een publieke dienst.
- Bij het wegvallen van het NDC als keuzemogelijkheid zijn er alternatieven beschikbaar voor schoolbesturen voor het organiseren van veilig internet.
- De kosten voor het NDC zijn afhankelijk van het volume van het verkeer wat wordt gebruikt. Dit volume hangt samen met het aantal leerlingen en devices.
- Grotere schoolbesturen met name in het VO kennen een grotere uitdaging in het beheer en organiseren van veilig internet omdat ook de leerlingen met hun eigen devices gebruik maken van het internet. Daarbij komt het op VO-scholen vaker voor dat leerlingen een dreiging vormen, onder andere door cyberaanvallen op de eigen school.

Techniek

- Is de dienst veilig genoeg, vergeleken met de huidige beschikbare technologie in de markt?
- Is de dienst voldoende schaalbaar voor toekomstige groei?

Op basis van interviews bij Kennisnet kunnen de bovenstaande vragen **positief** worden beantwoord.

Processen

- Heeft Kennisnet een gedegen set aan beheersmaatregelen getroffen voor de dienst?
- Zijn de beheersmaatregelen in opzet voldoende ingericht?

Op basis van interviews bij Kennisnet kunnen de bovenstaande vragen **positief** worden beantwoord.

Departementaal vertrouwelijk - Dep-V

Marktconformiteit

Op basis van onderzoek bij soortgelijke organisaties zien de door ICTU ingezette externe deskundigen dezelfde technische bouwblokken die de dienst creëren. Voor beide onderwerpen (technisch en organisatorisch) hebben de interviewers voldoende indicatie gekregen dat het aannemelijk is dat een commerciële organisatie een soortgelijke dienst op gelijke wijze zou opzetten. Dit draagt bij aan een professionele en tevens uniforme opzet van de dienst. Alternatieven voor de scholen voor een soortgelijke dienst zijn er in twee categorieën, enerzijds eenvoudige en met beperkte beveiligingsmaatregelen, anderzijds gelijkwaardige dienstverlening van een commerciële ICT-dienstverlener, met een aanzienlijk hogere prijs. Er zijn alternatieven voor schoolbesturen in de markt beschikbaar, bij een enigszins vergelijkbaar dienstenniveau en beveiligingsniveau tegen hogere kosten.

Interviews met schoolbesturen

Op basis van 9 interviews bij schoolbesturen (groot/middelgroot/klein, PO/VO, aangesloten/niet aangesloten) is het algemene beeld dat men positief is over de dienst zolang scholen er niet extra voor hoeven te betalen en zolang het niet verplicht is. De dienst wordt door de schoolbesturen vooral gezien als bedoeld voor het VO en niet voor het PO of kleine éénpitters. Er zijn schoolbesturen die eigen vergelijkbare oplossingen hebben (inclusief toegang tot internet via SURF) al dan niet in samenwerkingsverband met meerdere schoolbesturen.

Juridisch

Afname/gebruik van NDC kan vanuit wetgeving en vanuit het Normenkader IBP FO niet verplicht worden. Om marktfalen aan te tonen is nader onderzoek naar de alternatieven voor scholen nodig. Schoolbesturen hebben naar eigen zeggen vergelijkbare oplossingen. Door OCW moet nog uitgezocht worden of financiering van het NDC in de huidige context gezien kan worden als staatssteun.

Financiering

Twee andere vormen van financiering van het NDC (dus in plaats van aanvullende financiering door OCW) zijn besproken met financiële deskundigen van OCW. Dit zijn (deels) afromen van de lumpsum en via een tariefheffing door SIVON. Tariefheffing door SIVON kan relevant zijn bij een no go beslissing, afromen van de lumpsum bij een no go niet. De conclusie van de bespreking was dat deze andere vormen van financiering bij een no go beslissing niet kunnen of niet haalbaar zijn.

Kosten, baten en prognose aansluitgraad

De kosten voor het veilig maken van een internetaansluiting is per leerling ongeveer 32 euro per jaar[1] indien een soortgelijk dienst bij een marktpartij zou worden afgenomen. De kosten per leerling per jaar met een centrale voorziening kunnen bij een aansluitpercentage van meer dan 30% van de schoolbesturen dalen naar 12 euro per aangesloten leerling per jaar. Bij 30% wordt ook het optimale kostenniveau bereikt van het NDC, een hoger aansluitpercentage zal geen voordelig effect hebben per aangesloten leerling.
Zonder de beschikking over een NDC, betekent dit dat het FO zelf een voorziening voor veilig internet moet gaan regelen. Een indicatieve berekening leert dat alternatieven (zie onderdeel Markconformiteit hierboven) neerkomen op ongeveer 32 euro per leerling per jaar, exclusief niet kwantificeerbare restrisico's. Deze indicatieve berekening is gebaseerd op een behoorlijk aantal aannames, zie daarvoor paragraaf 5.5 en bijlage 13.

[1] Dit is exclusief de kosten voor access bij de internetaanbieder

Departementaal vertrouwelijk - Dep-V

Op basis van de cijfers aangeleverd door Kennisnet met betrekking tot de kosten van het NDC komen de kosten per leerling vanaf een aansluitpercentage van 30% op ongeveer 12 euro per jaar.

Vanaf 2027 is aanvullende financiering nodig. Het benodigde bedrag aan additionele middelen hangt af van de ambitie qua aansluitgraad en afspraken die daarover gemaakt worden. De baten vertalen zich naar een efficiënte, toekomst vaste, schaalbare en gecentraliseerde (deskundig personeel en technische kennis) oplossing voor veilig internet. Voor een kleiner schoolbestuur met één of twee locaties is het zelf inrichten van een voorziening zoals het NDC niet haalbaar in verband met de hoge (eenmalige) kosten voor het opzetten van een dergelijke oplossing. Bij het continueren van het NDC in de toekomst is het ook voor kleinere schoolbesturen mogelijk zich aan te sluiten op een dienst die veilig internet voor hen regelt.

Betekenis voor go/no-go besluit

Bovenstaande analyses leiden tot de volgende overwegingen, onderverdeeld naar techniek, beveiliging, financiën, transitie en rollen en verantwoordelijkheden:

Argumenten voor een go besluit NDC

- Techniek: Kwaliteit/marktconformiteit van het NDC voldoet. Er is vooralsnog geen vergelijkbaar aanbod voor schoolbesturen, tenzij zij dit (in gezamenlijkheid) zelf faciliteren. Veilig internet is hiermee in de vorm van het NDC voor alle FO-schoolbesturen beschikbaar.
- Beveiliging: OCW laat zien werk te maken van een digitaal veilige leeromgeving voor elke leerling in het FO door te investeren in de dienst waarop het Programma Digitaal Veilig Onderwijs voortbouwt.
- Beveiliging: Een centrale voorziening waar (bijna) alle scholen op zijn aangesloten biedt mogelijkheden om additionele beveiligingsdiensten (zoals monitoring, incident-response etc.) op te bouwen.
- Financiën: Veilig internet is een basisvoorziening waarover elke school anno 2023 moet kunnen beschikken. Door dit vanuit de overheid te faciliteren én te financieren komt OCW tegemoet aan de oproep van scholen dat digitalisering steeds hogere kosten met zich meebrengt en dat ze daar niet voor gecompenseerd worden.
- Financiën: Eén centrale voorziening voor de hele sector is doelmatiger dan wanneer scholen dit zelf gaan inkopen. Het NDC dient als referentie, heeft een beheersbare kwaliteit en is toekomst vast. Bij voldoende aansluitgraad zijn de kosten minder dan 1 euro per aangesloten leerling per maand. De kosten (inspanning) van een vergelijkbare voorziening voor een zelfstandig schoolbestuur (zelf organiseren) zijn door de beperktere schaal minimaal twee keer zo groot.
- Transitie: Een aansluitgraad van 30% lijkt haalbaar gezien de gegeven condities en verkregen informatie. Voor een (veel) hogere aansluitgraad zullen additionele kosten noodzakelijk zijn.

Argumenten voor een no go besluit

- Techniek: Aansluiting op de dienst kan niet verplicht worden. Daarmee kan niet afgedwongen worden dat iedere school ook daadwerkelijk gebruik maakt van de dienst. Het Normenkader IBP FO beschrijft te nemen cybersecuritymaatregelen, niet hoe of op welke manier dit gedaan moet worden. Vanuit de interviews met schoolbesturen blijkt er weinig draagvlak voor het verplichten van NDC gebruik (hoe), wel voor het verplichten van het Normenkader IBP FO (wat).
- Techniek: Door het aanbieden van een centrale voorziening vanuit de overheid, is deze ook verantwoordelijk voor beheer en doorontwikkeling. Dit kan leiden tot aansprakelijkheidsstelling of politiek afbreukrisico.

- Beveiliging: Een centrale infrastructurele voorziening is niet noodzakelijk om additionele beveiligingsdiensten voor scholen aan te bieden, wel makkelijker. Een voorbeeld van een gezamenlijke centrale voorziening (op vrijwillige basis) zien we in SURFsoc. In de markt zijn meerdere partijen die additionele beveiligingsdiensten aanbieden.
- Financiën: Het aansluiten van **alle** 2.500.000 leerlingen in het FO op de dienst Veilig Internet wordt ingeschat door Kennisnet op ongeveer € 30 mln per jaar. Deze kosten zijn 5x zoveel als programma Digitaal Veilig Onderwijs (€ 6 mln per jaar), zonder duidelijkheid over het effect op veiligheid voor het FO in zijn geheel. Bij het organiseren van veiligheid geldt over het algemeen dat de zwakste schakel bepalend is voor de sterkte van de keten. Om een sterke beveiliging te organiseren zijn de onderdelen mens, techniek en organisatie nodig. Naast een voorziening als het NDC, zal er ook aandacht besteed moeten worden aan mens en organisatie, zie hiervoor ook de bijbehorende maatregelen in het Normenkader IBP FO.
- Financiën: Het risico dat de EC de NDC financiering ziet als verpakte staatssteun.
- Transitie: Het aanbod van internetbeveiligingsdiensten in de markt ontwikkelt zich snel. Scholen kunnen hier (al dan niet in samenwerkingsverbanden) zelf gebruik van maken en doen dit in sommige gevallen ook al. Of er sprake is van marktfalen moet uit een nadere analyse blijken.

Scenario go

Bij een go besluit zorgt OCW voor additionele middelen waardoor er financiële zekerheid is voor de periode van 2027 tot minimaal 2030, omdat SIVON 3-jarige contracten afsluit met schoolbesturen voor aansluiting op het NDC. De enige voor de hand liggende manier van financiering op dit moment lijkt een additionele subsidie aan Kennisnet om het NDC te blijven exploiteren.

Tot nu toe blijft het aansluitpercentage achter bij gemaakte afspraken, onduidelijk is waar dit precies door komt. Vaak wordt genoemd looptijd huidige contracten, overstappen gaat langzamer dan verwacht, er is al een werkende voorziening, niet aantrekkelijk voor de doelgroep PO, etc. Over het te realiseren aansluitpercentage, zullen in de aansturing en voorwaarden, met Kennisnet nadere afspraken gemaakt moeten worden. Het benodigde bedrag aan additionele middelen hangt af van de ambitie en afspraken die gemaakt worden over het aansluitpercentage van schoolbesturen op het NDC en vervolgens de sturing daarop. Een hoog aansluit percentage (van 80%) lijkt op redelijke termijn niet haalbaar en wordt ook niet onderbouwd door de aangeleverde informatie. Een aansluitgraad van 30% lijkt realistisch en haalbaar op redelijke termijn.

De rollen en verantwoordelijkheden bij een go zijn als volgt verdeeld, NDC als voorziening voor veilig internet, OCW voorziet in additionele middelen en afspraken, Kennisnet zorgt voor de techniek en organisatiecapaciteit van het NDC passend bij de afspraken. Schoolbesturen blijven zelf verantwoordelijk voor veilig internet en mogen zelf bepalen bij wie ze zorgen voor veilig internet.

Scenario no go

Een no go besluit betekent geen additionele middelen vanuit OCW. Op dit moment heeft Kennisnet nog een groot deel van het subsidiebedrag (ongeveer € 22 miljoen, voor minimaal 3 jaar NDC exploitatie) in reserve. Hiermee kan een afbouwscenario worden gefaciliteerd. Het eventuele resterende bedrag zal terugvloeien naar OCW.

De rollen en verantwoordelijkheden bij dit scenario zijn als volgt verdeeld, schoolbesturen zijn zelf verantwoordelijk voor veilig internet en kiezen uit de markt (mogelijk gezamenlijk) een

Departementaal vertrouwelijk - Dep-V

oplossing, Kennisnet voorziet in een afbouw en migratie scenario. OCW blijft investeren en sturen op Digitaal Veilig Onderwijs en de implementatie van het Normenkader IBP FO.

Departementaal vertrouwelijk - Dep-V

3 Inleiding

3.1 Vraagstelling vanuit OCW

Het ministerie van Onderwijs, Cultuur en Wetenschap (OCW) is voornemens een besluit te nemen over structurele financiering van een centrale voorziening voor Veilig Internet (VI) in het Funderend Onderwijs (FO). OCW heeft tot op heden het Nationale Diensten Centrum (NDC) gefinancierd door een eenmalige subsidie beschikbaar te stellen aan Kennisnet. Deze eenmalige subsidie is toereikend tot 2027. Omdat scholen de zekerheid wordt geboden een driejarig contract af te sluiten is het ministerie voornemens begin 2024 een besluit te nemen over het al dan niet continueren van de financiering van het NDC.

ICTU is door het ministerie van OCW gevraagd om ter voorbereiding aan deze besluitvorming invulling te geven aan de volgende opdracht:

Stel op basis van al beschikbare informatie (deskresearch en workshops met Kennisnet en SIVON) minimaal drie en maximaal vijf scenario's op, waarbinnen in ieder geval de volgende scenario's vallen:

- Continueren en uitbouwen van het huidige NDC als publieke dienst voor het hele funderend onderwijs
- Stopzetten van het huidige NDC als publieke dienst

Bij de scenario's wordt aangegeven:

- Schematische weergave van de oplossing, op basis van de architectuur uit het document "Dienstbeschrijving Veilig Internet", SIVON, maart 2022.
- Beschrijving van rollen en verantwoordelijkheden van de schoolbesturen, de markt, de publieke dienstverleners en OCW; wie doet wat ten aanzien van de dienst en de dienstverlening.
- Beschrijving van de bijbehorende dienst(verlening), gedacht vanuit de onderstaande componenten;
    - Technologie: beschrijf of met de beoogde oplossing potentieel alle scholen kunnen worden bediend en onder welke voorwaarden, en of de geschetste oplossing toekomstvast is ten aanzien van mogelijke uitbreiding naar een landelijk SIEM/SOC.
    - Security/beveiliging: beschrijf de beveiligingsrisico's van het geschetste scenario zowel vanuit het oogpunt van de individuele school als voor de sector als geheel.
    - Financiën: geef een globale schatting van de kosten en baten zowel voor een individuele school als voor de sector als geheel.
    - Transitie: geef aan wat er nodig is om van de huidige situatie naar het geschetste scenario te komen en definieer de haalbaarheid (op basis van kosten, technische complexiteit en organisatorische haalbaarheid).
- Geef de voor- en de nadelen, de kosten en de baten van deze scenario's weer.

Deze scenario's worden, in samenspraak met OCW, afgestemd met de belangrijkste stakeholders (Kennisnet, SIVON, PO-Raad en VO-raad).

Departementaal vertrouwelijk - Dep-V

3.2 Veilig Internet en Nationale Diensten Centrum

Het ministerie van OCW streeft naar een onderwijssector waarin elke leerling digitaal veilig kan leren en medewerkers in een digitale werkomgeving veilig kunnen werken. Dit beleidsdoel wordt verder ondersteund door de recente lancering van het Normenkader Informatiebeveiliging en Privacy (IBP) voor het Funderend Onderwijs. Het normenkader biedt de benodigde richtlijnen en normen om de verantwoordelijke schoolbesturen en medewerkers te helpen bij een doordachte gegevensverwerking en gegevensbeveiliging in het onderwijs (bron: Normenkader IBP FO).

Een middel om een deel van dit beleidsdoel, namelijk veilige internettoegang, te verwezenlijken is de dienst Veilig Internet (VI), geleverd door SIVON en Kennisnet. Schoolbesturen hebben zelf de vrijheid om de dienst af te nemen of om elders (veilige) internettoegang af te nemen. Het Nationaal Dienstencentrum (NDC) is een onderdeel van de dienst VI en is eenvoudig gezegd de internet wasstraat, waarin onder meer maatregelen zijn getroffen tegen aanvallen van buitenaf of maatregelen om te voorkomen dat obscure sites (per ongeluk) bezocht worden. In hoofdstuk 4 van deze rapportage wordt nader stilgestaan bij Veilig Internet en het NDC in relatie tot het uitgevoerde onderzoek.

3.3 Aanpak van het onderzoek

Voor dit onderzoek heeft ICTU in nauwe afstemming met OCW de volgende informatie verzameld. Samen met Kennisnet en SIVON is gewerkt aan het opstellen van de verschillende scenario's en het nader invullen daarvan. Er is onderzoek gedaan naar de techniek, processen en marktconformiteit van het NDC in de vorm van een interne review. En er zijn interviews afgenomen bij diverse schoolbesturen, meer of minder bekend met het NDC, naar de behoefte en draagvlak van een centrale voorziening voor veilig internet. Daarnaast is samen met OCW naar de juridische- en financiering bepalingen en randvoorwaarden gekeken.

Ten slotte is onderhavige rapportage opgesteld waar de verschillende onderzoeksgebieden in zijn samengevat en waarin de verschillende scenario's zijn voorzien van voor- en nadelen, kosten en baten ter onderbouwing van een besluit voor de (toekomstige) financiering van het NDC.

De afzonderlijke deelrapportages zijn eerst ter validatie (feitelijke onjuistheden en begrijpelijkheid) voorgelegd aan Kennisnet en SIVON en deels ook OCW (Juridisch en financiële aspecten). De rapportage is in zijn geheel gereviewd door de betrokken QA collega's en de opdrachtgever. Daarna is de definitieve rapportage opgeleverd ter ondersteuning van verdere afstemming en besluitvorming door de opdrachtgever.

3.4 Leeswijzer

Hoofdstuk 4 behandelt de beschrijving van de dienst VI en het NDC en de varianten voor gebruik van internet op een schoollocatie. Hoofdstuk 5 gaat in op de interne review van techniek, security, processen en organisatie, evenals marktconformiteit en alternatieven voor scholen. Hoofdstuk 6 bespreekt de opzet en uitkomsten van de interviews met schoolbesturen. Hoofdstuk 7 belicht de juridische kaders voor verplichtingen en financiën. Hoofdstuk 8 richt zich op kosten, baten en aansluitgraad. In hoofdstuk 9 worden argumenten voor een no go / go besluit behandeld. Hoofdstuk 10 bevat de scenario's voor no go / go. Bijlagen 11 t/m 14 bevatten documentatie over respectievelijk de interviews met schoolbesturen, het onderzoek naar techniek en proces, alternatieven voor beveiligingsmaatregelen en kosten en prognoses van Kennisnet.

4 Beschrijving van de dienst

4.1 Dienst Veilig Internet (VI)

Veilig Internet van SIVON biedt scholen een veilige internetverbinding met aangepaste snelheid en betrouwbaarheid, inclusief professioneel beheerde firewall tegen bedreigingen zoals DDoS-aanvallen. SIVON neemt het aanbestedingsproces voor scholen (met aanbestedingsverplichtingen) op zich, waardoor deze scholen volledig ontzorgd worden. Verder neemt SIVON verantwoordelijkheid voor vragen rond leverancierskeuze, netwerkstabiliteit en beveiliging. Naast Veilig Internet biedt SIVON ook andere services, ter ondersteuning van digitalisering van het FO aan. De dienst VI waarborgt veiligheid door aansluiting op het NDC. Hierbij kan elke school een eigen firewall instellen en extra beveiligingsmaatregelen implementeren. Op figuur 1 wordt de architectuur van de dienst Veilig Internet conceptueel weergegeven.

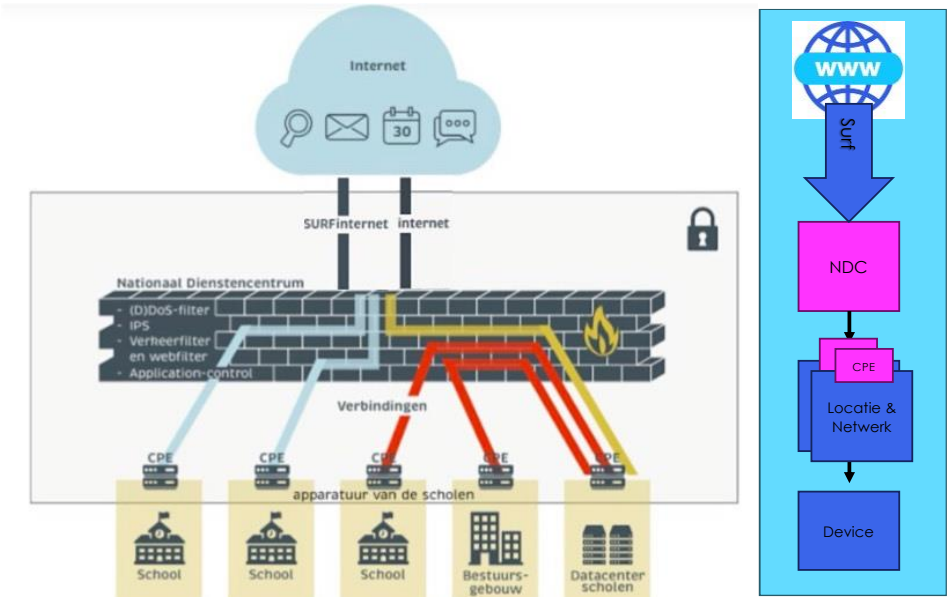
4.2 Nationaal Dienstencentrum (NDC)

Het NDC is onderdeel van de dienst Veilig Internet en is een verzameling diensten, die communicatie via het internet en toegang tot het internet op een veilige en betrouwbare manier mogelijk maakt, waaronder internettoegang, anti-DDoS-maatregelen, IP- en DNS-filtering. In samenwerking met technologiepartners Cisco en Fortinet bouwt, levert, en beheert Axians de komende jaren een centrale beveiligde omgeving, waarbij PO- en VO-schoollocaties via SD-WAN technologie worden ontsloten. Het beoogde resultaat is een van de grootste beveiligde netwerken in Nederland. Het NDC wordt tot op heden door OCW gefinancierd middels een startsubsidie aan Kennisnet.

4.3 NDC in relatie tot scope onderzoek

Figuur 1 geeft een overzicht van de opbouw en alle onderdelen die nodig zijn om veilige internettoegang te realiseren en rechts daarvan een conceptuele weergave. Het omkaderde deel in het linker plaatje en het roze gekleurde deel in het rechter plaatje van figuur 1 laat de scope van dit onderzoek zien. Hierbij gaat het specifiek over de componenten van de dienst Veilig Internet die door OCW gefinancierd worden. Dit betreft het NDC met de specifieke diensten die zorgen voor veiligheid en de CPE die op de scholen geïnstalleerd wordt. De verbindingen (connectiviteit) is buiten scope, omdat dit een andere dienst is die door SIVON wordt aangeboden. Onder figuur 1 wordt een toelichting gegeven op de onderdelen.

Departementaal vertrouwelijk - Dep-V



Figuur 1: Architectuur Veilig Internet (bron: Kennisnet) met conceptuele weergave

Van onder naar boven (van de school naar uiteindelijk de internettoegang) zien we:

CPE, Client Premises Equipment (eindpunt van de connectiviteitsketen op de school)

- Dat is een device op de schoollocatie om aanvullend op de centrale firewall specifiek verkeer te kunnen filteren en detectie te kunnen doen over de gehele keten bij incidenten.
- De levering en plaatsing van de benodigde hardware maakt onderdeel uit van de NDC-dienstverlening. Scholen betalen daar nu dus zelf niets voor, de CPE wordt vanuit OCW gefinancierd.

Access (verbinding vanaf de school tot aan het NDC)

- De aansluiting op het NDC wordt gerealiseerd door een verbinding te leggen tussen de schoollocatie (gebouw) en het datacenter van het NDC. Per schoollocatie is een verbinding noodzakelijk, rechtstreeks naar het NDC of via een door het schoolbestuur beheerd centraal netwerk. SIVON biedt aanvullend ook services aan schoolbesturen om het centrale netwerk te beheren eventueel aangevuld met het beheer van de WiFi voorziening (WaaS – Wifi-as-a-Service). Deze aanvullende services zijn buiten scope van dit onderzoek.
- Beveiligde tunnels (IP-sec en Q-in-Q) van schoolnetwerk tot aan het NDC, i.p.v. openbaar internet, end-to-end beveiliging.
- De toegang tot het NDC is zodanig (technisch) ingericht dat de dienst werkt, zowel via een door SIVON aangeboden verbinding, als via een door een schoolbestuur gekozen verbinding buiten de mantel van SIVON om. Hiermee typeert het NDC zich als publieke dienst voor FO-schoolbesturen. Eind 2023 maakten vrijwel alle aangesloten schoolbesturen gebruik van de door SIVON aangeboden mantels voor verbindingen. Twee schoolbesturen zijn met eigen verbindingen aangesloten op het NDC. Alle aangesloten schoolbesturen maken gebruik van SURFinternet van SIVON.
- Schoolbesturen die lid zijn van SIVON kunnen gebruik maken van de mantels die SIVON heeft afgesloten en daaronder een contract met een leverancier afsluiten. SIVON begeleidt deze minicompetitie. Besturen die geen lid zijn dienen zelf met een marktpartij een contract af te sluiten.
- Schoolbesturen betalen zelf voor Access (al dan niet bij één van de mantelpartijen via SIVON).

Departementaal vertrouwelijk - Dep-V

NDC (Nationaal Diensten Centrum)

- Firewall; filteren van verkeer en mogelijkheden om preventief in te grijpen op basis van dreigingsinformatie door het achterliggend scholennetwerk af te sluiten voor bepaald type verkeer.
- Webfiltering; het afschermen van specifieke content, toegang tot ongewenste websites wordt beperkt op basis van geïnstalleerde filterstandaarden (blacklist).
- Secure DNS; internetgebruikers weten zeker dat de IP-adressen, die ze voor een bepaalde domeinnaam terugkrijgen naar de juiste servers wijzen.
- Anti-DDoS voorziening; filtert verkeer op DDoS-aanvallen, die als doel hebben zoveel verkeer af te vuren op een bepaalde server, dat er een file ontstaat en deze onbereikbaar wordt.
- De werking van deze specifieke anti-DDoS voorziening voor het onderwijs is gebaseerd op de grote hoeveelheden gedeelde internet capaciteit die SURF beschikbaar heeft, waardoor relatief makkelijk voorkomen wordt dat er files ontstaan. Bij een commercieel aanbod voor anti-DDoS, zullen de kosten voor de aanvullende internet capaciteit in rekening worden gebracht, wat over het algemeen een verdubbeling van de kosten voor internet tot gevolg heeft.

Aansluiting en capaciteit NDC

- De kenmerken voor een groter schoolbestuur zijn dat deze over het algemeen meerdere locaties zijn verdeeld, centrale voorzieningen delen(efficiëntie) en een groot aantal (duizenden) leerlingen en leerkrachten faciliteren. Het aantal componenten wat hiervoor nodig is maakt het beheer complexer. Dit vraagt een professionele beheerorganisatie in eigen beheer of uitbesteed.
- Kleine schoolbesturen beschikken over één of enkele locaties, maken over het algemeen geen gebruik van centrale voorzieningen en faciliteren een kleiner aantal (honderden) leerlingen en leerkrachten in een relatief eenvoudige netwerkomgeving. De beheerinspanning is beperkt en kan in eigen beheer worden gedaan of uitbesteed.
- Er is een behoorlijk verschil in de capaciteit van internet(bandbreedte) op schoollocaties tussen het PO en het VO. Anders dan in het PO, is in het VO is het aantal devices veel groter per schoollocatie, ook de leerlingen (op eigen devices, laptop en mobiel) krijgen toegang tot internet als faciliteit vanuit het schoolbestuur. In het PO worden devices veelal gedeeld door leerlingen.
- Het VO heeft naast dreigingen van buitenaf door cybercriminelen ook te maken met dreigingen van binnenuit. Een boze of kwaadwillende leerling kan vrij eenvoudig een DDoS aanval opzetten tegen de school[2], de DDoS voorziening van het NDC is hierop berekend.
- De capaciteit (bandbreedte) van de door een schoolbestuur gebruikte dataverbinding bepaalt hoeveel leerlingen en leerkrachten gebruik kunnen maken van het internet op die locatie. Het NDC is zo ingericht dat de benodigde capaciteit per aangesloten locatie beschikbaar is. De omvang (en bijbehorende kosten) van het NDC is daarmee afgestemd op het aantal aangesloten leerlingen en leerkrachten en daarmee het aantal devices (apparaten) wat een verbindingen maakt met het internet.

[2] Bron: Dreigingsbeeld Funderend Onderwijs 2023, Kennisnet

Departementaal vertrouwelijk - Dep-V

Financiering

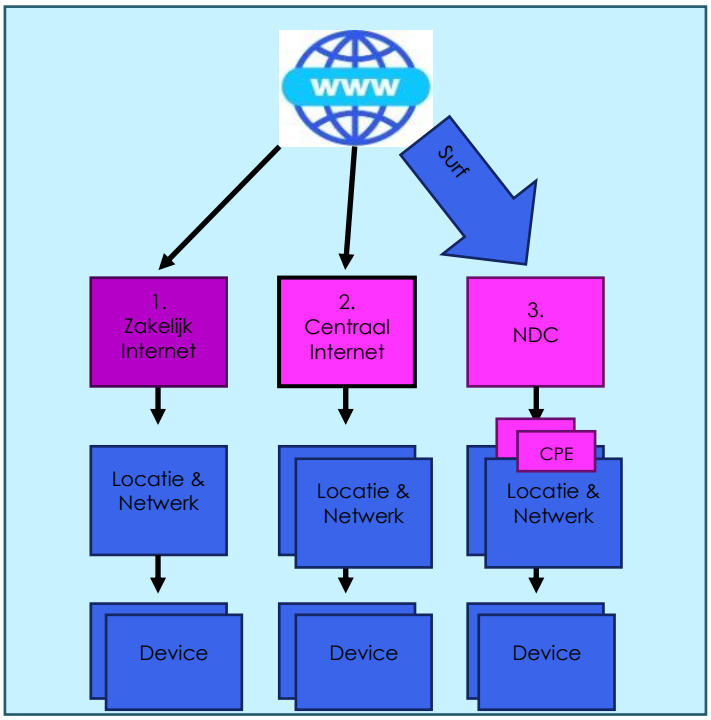
- Het NDC wordt geleverd door Kennisnet en is eenmalig via een startsubsidie door OCW gefinancierd.

Rollen en verantwoordelijkheden in relatie tot het NDC.

- Schoolbesturen; zijn zelf verantwoordelijk voor het organiseren van veilig Internet.
- Het Normenkader IBP FO is bedoeld om schoolbesturen te helpen met het versterken van hun informatiebeveiliging.
- SURF-internet
  - De verbinding naar het internet via SURF is beschikbaar voor schoolbesturen die lid zijn van SIVON. SIVON is lid van SURF en op die manier kunnen scholen gebruik maken van toegang via SURF.
  - Filtering van vaak voorkomend risicovol verkeer (aanvallen) op door SURF vastgestelde drempelwaardes en poorten.
  - Directe peerings (koppelingen) met o.a. Microsoft/Azure, zodat deze bereikt kunnen worden middels het "interne netwerk" van SURF/SIVON/KN. Met hogere kwaliteit en minder hubs.
- Leverancier-internet; voor scholen die geen lid zijn van SIVON, wordt de internet toegang niet via SURF maar via een andere provider georganiseerd. Er is een variant ontwikkeld waarbij NDC ook kan werken met een andere internet toegang dan via SURF internet. Bij het uitvoeren van dit onderzoek was er nog geen schoolbestuur bekend die van deze variant gebruik maakt.

4.4 NDC afhankelijkheden en scenario's

Bij het uitvoeren van het onderzoek naar het NDC komt naar voren dat om gebruik te kunnen maken van het NDC er een aantal afhankelijkheden zijn. Daarnaast is er een beeld ontstaan hoe schoolbesturen de toegang tot internet organiseren als er geen gebruik gemaakt wordt van het NDC. Hiermee wordt inzicht verkregen in de alternatieven die er zijn bij een eventueel no go scenario. De variant waarbij het NDC wordt geschetst is passend bij het go scenario (besluit om NDC te continueren). In onderstaand plaatje zijn de drie varianten voor gebruik van internet op een schoollocatie geschetst zoals die tijdens het onderzoek naar voren zijn gekomen.



Figuur 1: Mogelijkheden om gebruik te maken van internet

Departementaal vertrouwelijk - Dep-V

De drie varianten zoals in dit onderzoek naar voren zijn gekomen om gebruik te maken van internet op een schoollocatie zijn;

1. Door per schoollocatie gebruik te maken van (lokaal) aanbod van een aanbieder van zakelijk internet,
2. Door gebruik te maken van een gezamenlijke of centrale internetaansluiting door samenwerkende schoolbesturen,
3. Door gebruik te maken van het aanbod van SIVON op connectiviteit inclusief de dienst Veilig Internet en het NDC.

De eerste variant wordt toegepast door schoolbesturen die over één of enkele locaties beschikken, of niet beschikken over een eigen netwerk. In de meeste gevallen wordt gebruik gemaakt van een MKB zakelijk abonnement, waarbij de voorzieningen voor veilig internet door het schoolbestuur zelf aanvullend georganiseerd dienen te worden. Ook hierin zijn weer diverse varianten te vinden, van zeer beperkte maatregelen tot een passend service contract met een professionele ICT-service aanbieder. Een enkel schoolbestuur organiseert dit zelf.

De tweede variant komt onder andere voor bij schoolbesturen die betrokken zijn bij een initiatief voor een gezamenlijke (glasvezel)netwerkvoorziening. Deze variant zien we met meerdere schoolbesturen en ook in gezamenlijkheid met gemeentelijke instanties terug. Kenmerk is dat door een eenmalige investering (in het verleden) relatief goedkoop gebruik gemaakt kan worden van een netwerkverbinding met internet. Door de grote schaal van het netwerk zijn er centrale voorzieningen voor veilig internet aanwezig. In een aantal gevallen is SURF ook betrokken als partner en loopt het internetverkeer via SURF.

De derde variant (NDC) is in gebruik bij grotere (samenwerkende) schoolbesturen met meerdere locaties, die grote aantallen leerlingen en leerkrachten voorzien van een internetverbinding. Een meerderheid van VO-scholen maakt gebruik van deze variant en enkele grotere PO-schoolbesturen.

Voor al deze drie varianten geldt dat er uitzonderingen op zijn en dat er combinaties mogelijk zijn op onderdelen. Gezien de scope en diepgang van het onderzoek is daarmee de onderlinge vergelijkbaarheid van deze mogelijkheden beperkt en moet als indicatief worden gezien.

4.5 Tussenconclusie 1

- Schoolbesturen zijn zelf verantwoordelijk voor het goed organiseren van veilig internet, het Normenkader IBP FO schrijft niet voor hoe dit gedaan moet worden.
- De veiligheid voor internettoegang zoals deze door schoolbesturen wordt georganiseerd, kent een groot aantal varianten en bijbehorende afhankelijkheden waarmee geen eenduidig beeld geschetst kan worden over de werking en veiligheid daarvan. De meest voorkomende varianten, naast het NDC, zijn in twee aanvullende alternatieven uitgewerkt.
- De voorziening die voor het NDC is opgebouwd, biedt het meest complete pakket aan beveiligingsmaatregelen.
- Alle schoolbesturen in het FO kunnen gebruik maken van het NDC, de techniek en de aansluitvoorwaarden zijn hierop ingericht en op dit aspect voldoet het NDC aan de voorwaarden voor een publieke dienst.
- Bij het wegvallen van het NDC als keuzemogelijkheid zijn er alternatieven beschikbaar voor schoolbesturen voor het organiseren van veilig internet.
- De totaalkosten voor het NDC zijn afhankelijk van het volume van het verkeer wat wordt gebruikt. Dit volume hangt samen met het aantal leerlingen en devices.
- Grotere schoolbesturen, met name in het VO, kennen een grotere uitdaging in het beheer en organiseren van veilig internet omdat ook de leerlingen met hun eigen

Departementaal vertrouwelijk - Dep-V

devices gebruik maken van het internet. Daarbij komt het op VO-scholen vaker voor dat leerlingen een dreiging vormen, onder andere door cyberaanvallen op de eigen school.

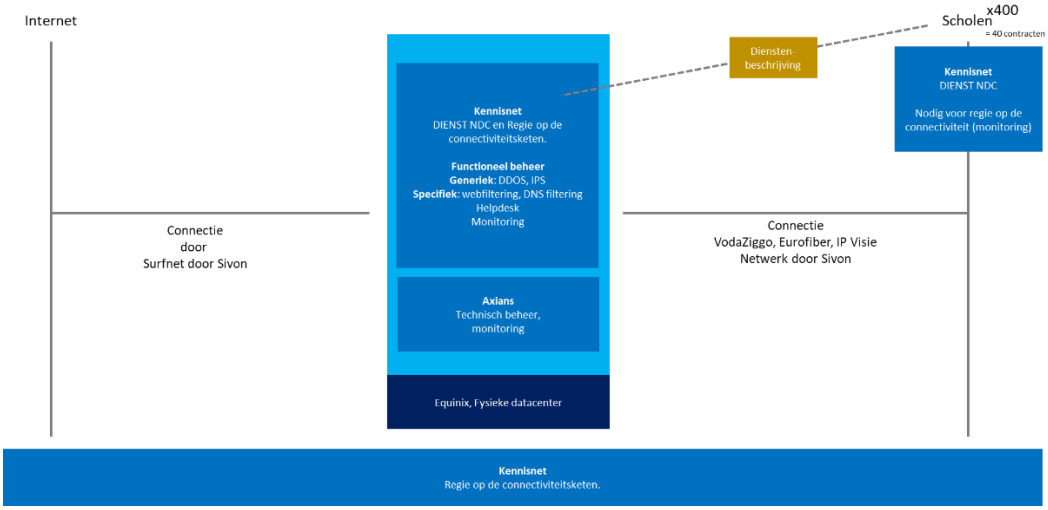
Departementaal vertrouwelijk - Dep-V

5 Techniek, security, beveiliging en processen

5.1 Opzet interne review

Om inzicht te krijgen in de opzet van de dienst VI van Kennisnet heeft ICTU samen met Kennisnet een interne review uitgevoerd. Deze review was primair gericht op de technische en organisatorische beheersmaatregelen in het kader van informatiebeveiliging en privacy. De interne review beperkt zich tot de werkzaamheden en de technische infrastructuur die Kennisnet heeft ingericht en uitvoert voor de dienst NDC en 'regie op de keten'. Een interne review betekent dat de inrichting van de dienst als eerstelijns kwaliteitsreview is bekeken. Dit beperkt de diepgang van de review. Er is in beperkte mate in de systemen gekeken. De meeste informatie is ingewonnen op basis van aangeleverde documentatie of door middel van interviews met betrokkenen. Er is niet gekeken naar leveranciers die ook onderdeel zijn van de keten, anders dan de wijze waarop ze aan de orde komen binnen de processen van Kennisnet zelf.

De dienst die Kennisnet aanbiedt aan scholen is onderdeel van een dienst genaamd Veilig Internet van de organisatie SIVON. Het onderdeel van Kennisnet beslaat het grootste gedeelte van de totale dienst. In de basis beslaat de dienst het leveren van een internetverbinding aan scholen met enkele aanvullende beveiligingsmaatregelen zoals het filteren van internetstromen en bescherming van aanvallen van buitenaf. Onderstaande figuur geeft een schematische weergave van de dienst weer.



Figuur 3: Schematische weergave dienst NDC van Kennisnet

5.2 Techniek, security en beveiliging

De toetsvragen voor het onderdeel techniek van de interne review zijn:

- Is de dienst veilig genoeg, vergeleken met de huidige beschikbare technologie in de markt?
- Is de dienst voldoende schaalbaar voor toekomstige groei?

Beide vragen kunnen **positief** worden beantwoord.

De technische oplossing maakt gebruik van een marktconform, commercial off the shelf (COTS) firewall product (Fortinet) dat gebruikt wordt door Internetproviders, grote gebruikers van Internet, overheden en financiële instellingen.

Departementaal vertrouwelijk - Dep-V

De oplossing is voorzien van Unified Threat Management (UTM) dat bescherming biedt tegen onder meer aanvallen via (kwaadaardige) webservers, botnets en Denial of Service. De deelnemende scholen zijn onderling van elkaar gescheiden om 'kruisbesmetting' van de ene school naar de andere te voorkomen. Alleen met expliciete toestemming van beide scholen kan onderling verkeer worden uitgewisseld. Ook dit onderlinge verkeer wordt door de firewall gecontroleerd.

De huidige implementatie biedt voldoende ruimte voor groei, zowel voor bandbreedte als voor verwerkingscapaciteit. De huidige inrichting en opschaling is gebaseerd op een groter aantal deelnemers dan op dit moment actief is. Bij sterke groei kan de huidige inrichting worden gekopieerd waardoor er voldoende ruimte voor groei beschikbaar blijft.

Kennisnet werkt aan de doorontwikkeling van de huidige oplossing, met name op het gebied van beheersbaarheid. Dit geeft aan dat Kennisnet tijd, kennis en middelen blijft investeren in de oplossing, ook om deze toekomstvast te houden.

5.3 Proces en organisatie

De toets vragen vanuit organisatorisch perspectief zijn:

- Heeft Kennisnet een gedegen set aan beheersmaatregelen getroffen voor de dienst?
- Zijn de beheersmaatregelen in opzet voldoende ingericht?

Op beide vragen is de conclusie **positief**.

Door het ontbreken van een vooraf bepaald normenkader is als eerste stap samen met de betrokkenen een raamwerk opgesteld, wat de verschillende onderwerpen bevat die relevant zijn voor een goed beheer en beheersing van cybersecuritymaatregelen voor de dienst NDC. Voor de volledigheid is het goed om te vermelden dat Kennisnet ook in het bezit is van een ISO 27001 certificaat. Bij het opgestelde raamwerk is per onderwerp een risico inschatting vastgesteld, in de onderverdeling hoog, midden of laag. Per onderwerp zijn een aantal controls geformuleerd, waarbij in de uitgevoerde review op basis van de interviews is bepaald of voldaan wordt aan de eisen zoals deze in de control zijn geformuleerd (zie bijlage 12). Hierbij zijn de volgende onderwerpen onderscheiden;

Onderwerp	Risicoklasse	Aantal controls	Resultaat
ISMS	Midden	5	Voldoet
Logische toegangsbeveiliging	Hoog	9	Voldoet
Wijzigingsbeheer	Midden	9	Voldoet
Netwerk operations	Midden	6	Voldoet
Software Ontwikkeling	Laag	5	Voldoet
End-user computing	Laag	3	Voldoet
Back-up, Recovery & Incident management	Hoog	9	Voldoet
Specifieke applicatiecontroles	NVT	8	Voldoet
AVG	Laag	0	Buiten scope
Leveranciersmanagement	Hoog	1	Voldoet
Servicemanagement	Midden	1	Voldoet
Configuratiebeheer	Midden	1	Voldoet

In bijlage 12 staat het overzicht met de uitwerking van de 57 controls.

5.4 Marktconformiteit

Naast de onderzoeksresultaten die inzicht geven in het technische en organisatorische perspectief is ook gekeken naar de marktconformiteit van de opzet van de dienst van kennisnet. De vraag die daarbij is gesteld is of een commerciële organisatie deze dienst op

Departementaal vertrouwelijk - Dep-V

dezelfde wijze zou opzetten en/of er andere alternatieven beschikbaar zijn voor de scholen. Voor beide onderwerpen (technisch en organisatorisch) hebben de interviewers voldoende indicatie gekregen dat het aannemelijk is dat een commerciële organisatie een soortgelijke dienst op gelijke wijze zou opzetten. Op basis van onderzoek bij soortgelijke organisaties zien de interviewers dezelfde bouwblokken die de dienst creëren. Systemen zoals bijvoorbeeld Fortinet, Microsoft Azure of Confluence samen met Jira software zijn gemeengoed in deze markt en dragen bij aan een professionele en tevens uniforme opzet van de dienst.

Alternatieven voor de scholen voor een soortgelijke dienst zijn er, naar verwachting zijn deze in twee categorieën in te delen (zie ook de conceptuele beschrijving hiervan in hoofdstuk 4.4):

1) Een eenvoudigere dienstverlening van internet (denk hierbij aan een MKB-internet aansluiting) met beperkte aanvullende beveiligingsmaatregelen (bijvoorbeeld geen geavanceerde filtering van verkeer).
2) Een gelijkwaardige dienstverlening bij een commerciële organisatie, hoogstwaarschijnlijk met een aanzienlijk prijsverschil ten opzichte van de eerste optie.

5.5 Scenario's en mogelijkheden schoolbesturen

Zoals in voorgaande paragraaf geschetst zijn er op hoofdlijnen drie mogelijkheden voor schoolbesturen om aanvullende beveiligingsmaatregelen toe te passen. De bovengenoemde twee (bij een no-go scenario) of gebruik maken van het NDC (go scenario). Onderstaand wordt een indicatieve uitwerking geschetst van deze mogelijkheden, waarbij ook een aantal aannames worden gedaan en toegelicht om een vergelijking met het NDC te maken.

Het eerste alternatief gaat uit van een beperkte aanvulling op beveiligingsmaatregelen, waarbij slechts een beperkte filtering van het internetverkeer wordt gedaan (standaard instellingen van een MKB-internet aansluiting). Het tweede alternatief gaat uit van de eerste oplossing, aangevuld met een adequaat ingerichte firewall, waarbij (proactief) het internetverkeer wordt gefilterd en gemonitord. De vergelijking tussen de alternatieven is in de onderstaande tabel weergegeven.

Departementaal vertrouwelijk - Dep-V

Indicatief vergelijk alternatieven	Alternatief 1 No-go scenario	Alternatief 2 No-go scenario	Alternatief 3 Go scenario
Beschrijving	Eenvoudige internetaansluiting, zonder additionele beveiliging met reactief beheer	Internetaansluiting met additionele beveiliging, zoals firewalll en beheercontract	Beveiliging via NDC
Firewall	Zeer beperkt mogelijk in alternatief 1	Eenmalig ingericht en mogelijk onderhouden[3]	Afgestemd op FO
Anti-DDoS	Niet inbegrepen in alternatief 1	Mogelijk, tegen hoge kosten[4]	Afgestemd op FO[5]
Web filtering	Zeer beperkt mogelijk in alternatief 1	Eenmalig ingericht en onderhouden[3]	Afgestemd op FO
Secure DNS	Zeer beperkt mogelijk in alternatief 1	Eenmalig ingericht en onderhouden[3]	Afgestemd op FO
Beschermingsniveau	Laag	Gemiddeld	Hoog
Beveiligings risico	Gemiddeld, restrisico's	Gemiddeld-Laag	Laag
Beschikbaarheid Internet	Gemiddeld[6]	Hoog	Hoog
Kosten	Gemiddeld (uren)	Gemiddeld(uitbesteed)	Laag
Jaarkosten beveiliging per leerling exclusief access (indicatief)	0 euro[7]	32 euro, wordt lager bij meerdere locaties	12 euro, vanaf 30% aansluitpercentage
Schaalbaar	Nee	Ja, bij meerdere locaties	Algemene voorziening voor FO

De onderbouwing van deze onderdelen is gebaseerd op een aantal aannames, waardoor deze als indicatief moeten worden beschouwd. In bijlage 13 Alternatieven voor beveiligingsmaatregelen zijn deze aannames verder toegelicht en uitgewerkt.

Wat duidelijk wordt aan de hand van deze tabel, is dat het NDC een goede en adequate oplossing is voor veilig internet voor het FO. Maar ook dat een samenwerkingsverband met meerdere locaties een vergelijkbare oplossing kan implementeren, weliswaar gezien de schaal tegen hogere kosten en mogelijke restrisico's. Bij het wegvallen van het NDC als alternatief, kunnen schoolbesturen zich of verenigen en een eigen gezamenlijk internetvoorziening opzetten, of er kan gebruikt gemaakt worden van bestaande marktaanbod, waarbij op een kleine schaal de inspanning en bijbehorende kosten relatief hoog zullen zijn, vergeleken met een gezamenlijke/centrale voorziening.

[3] Afhankelijk van het afgesloten beheercontract.
[4] Deze voorziening zal specifiek ingericht en ingeleerd moeten worden voor de school die dit afneemt.
[5] De anti-DDoS voorziening van NDC is specifiek ingericht voor het onderwijs.
[6] Door de beperkte veiligheidsvoorzieningen en reactief beheer is te verwachtten dat er verstoringen optreden in de internet verbinding.
[7] Bij dit alternatief, zijn er verhoogde reactieve beheerkosten te verwachtten, omdat de beveiliging beperkt is

Departementaal vertrouwelijk - Dep-V

5.6 Tussenconclusie 2

- De dienst NDC biedt voldoende veiligheid, vergeleken met de huidige beschikbare technologie in de markt. De dienst is voldoende schaalbaar voor toekomstige groei.
- Kennisnet heeft een gedegen set aan beheersmaatregelen getroffen voor de dienst, deze beheersmaatregelen zijn in opzet voldoende ingericht.
- Het is aannemelijk is dat een commerciële organisatie een soortgelijke dienst gaat opbouwen gebruikmakend van vergelijkbare componenten.
- Er zijn alternatieven voor schoolbesturen in de markt beschikbaar, bij een enigszins vergelijkbaar dienstenniveau en beveiligingsniveau tegen hogere kosten, ingeschat op basis van aannames op gemiddeld 32 euro per leerling per jaar.

Departementaal vertrouwelijk - Dep-V

6 Interviews schoolbesturen

6.1 Opzet interviews schoolbesturen

Om inzicht te verkrijgen in de behoefte aan en draagvlak voor een centrale voorziening voor veilig internet, zijn er interviews gehouden met diverse schoolbesturen. Er zijn in totaal negen schoolbesturen geïnterviewd die in meer of mindere mate bekend zijn met het NDC. Deze groep omvat drie PO-schoolbesturen, drie VO-schoolbesturen en drie PO- en VO-schoolbesturen van verschillende omvang. Van de negen schoolbesturen zijn er vijf aangesloten of in de aansluitfase en vier niet-aangesloten. Het is belangrijk om op te merken dat de interviews een indicatief beeld geven dat niet representatief is voor de gehele groep schoolbesturen. Voor herkenbaarheid voor scholen hebben we gesproken over de dienst Veilig Internet in plaats van het NDC.

In de volgende paragraaf wordt een samenvatting gegeven van de uitkomsten. De interviewleidraad en een tabel met een overzicht van de interviewresultaten zijn in bijlage 11 te vinden.

6.2 Uitkomsten interviews schoolbesturen

6.2.1 Algemeen beeld

Van de negen geïnterviewde schoolbesturen zijn er acht bekend met de dienst VI, waarbij er vijf zijn aangesloten bij de dienst VI.

Er kwamen verschillen naar voren tussen VO- en PO- schoolbesturen, waarbij VO-schoolbesturen vaak meer bewust zijn van de dienst VI en online veiligheid, terwijl PO-schoolbesturen hier minder bewust van zijn. Een aantal schoolbesturen schetsen het beeld dat PO-schoolbesturen vaak kleinschaliger zijn en nog gebruik maken van een abonnement zoals Ziggo Zakelijk zonder extra beveiliging. Het gevoel van urgentie voor internetdreigingen lijkt minder aanwezig in het PO, wat bijvoorbeeld bleek bij een scholengemeenschap waarbij VO- scholen aangesloten zijn bij VI, maar PO-directeuren moeilijk te overtuigen waren van de noodzaak van deze investering en daarmee ook geen gebruik maken van VI maar van een eigen oplossing.

6.2.2 Grootte van scholen

De drie kleinere schoolbesturen variëren in aansluiting, waarbij een schoolbestuur is aangesloten, en de andere twee eigen oplossingen hebben via een commerciële partij of een stichting waar ze niet uit kunnen stappen. De middelgrote scholengemeenschappen zijn allemaal aangesloten bij de dienst VI. De grotere scholengemeenschappen hebben vaak een eigen ICT-afdeling. Een schoolbestuur zit in de aansluitingsfase bij de dienst VI, de andere twee hebben hun eigen beveiligingsoplossingen ontwikkeld op basis van een aansluiting bij SURF Internet. Axians voert bij een van deze twee schoolbesturen de beheerwerkzaamheden uit, waarmee een oplossing is gerealiseerd die erg lijkt op die van het NDC.

6.2.3 Motivatie aansluiting

De motivatie voor aansluiting varieert, waarbij sommige schoolbesturen de dienst VI beschouwen als een collectieve oplossing. Dergelijke beveiligingsmaatregelen zijn volgens hen te complex en kostbaar om individueel te realiseren. De dienst VI wordt ook gezien als een opstap naar een uitgebreider dienstenpakket dat volgens hen door de overheid georganiseerd zou moeten worden om te voldoen aan het Normenkader IBP FO. Anderen zijn meer kosten gedreven: de dienst (connectiviteit) is goedkoper dan het alternatief. Voor één schoolbestuur was het technisch niet mogelijk om aan te sluiten.

Departementaal vertrouwelijk - Dep-V

6.2.4 Dienstverlening SIVON

De aangesloten schoolbesturen zijn over het algemeen tevreden over de dienstverlening van VI/SIVON, met positieve opmerkingen over proactieve communicatie, snelle reactie op problemen, meedenken en het meenemen van feedback over technische verbeteringen. Dit wordt door een bestuurder in contrast geplaatst met eerdere negatieve ervaringen met Ziggo. Een schoolbestuur benoemd wel dat er verbeteringen mogelijk zijn qua techniek en functionaliteiten.

6.2.5 Normenkader IBP FO en bestuurlijke agenda

Online veiligheid en het Normenkader IBP FO staan hoog op de bestuurlijke agenda van vrijwel alle scholen, met nulmetingen, concrete stappenplannen tot 2026 en bewustwordingsprogramma's. Sommige schoolbesturen wensen meer ondersteuning van OCW, zowel financieel als in termen van uitleg en advies in de organisatie.

6.2.6 Kosten

De aangesloten schoolbesturen zijn over het algemeen tevreden over de huidige kosten. Met name een aantal middelgrote en grotere schoolbesturen zijn zich bewust van de kosten van online veiligheid en vinden een marktconforme prijs acceptabel, met het besef dat veiligheid niet gratis is. Daar wordt wel bij benadrukt dat het binnen het budget moet blijven passen, omdat het anders ten koste gaat van het onderwijs. Overstappen door niet-aangesloten schoolbesturen wordt overwogen als de dienst goedkoper wordt door collectieve deelname of bij voortzetting van de subsidie na 2026.

Randvoorwaarden om de dienst te blijven afnemen tegen een marktconforme prijs zijn een goede dienstverlening, snel optreden bij calamiteiten, meegaan met technologische ontwikkelingen en een goede prijs ten opzichte van functionaliteiten, flexibiliteit, licenties en beheerkosten.

6.2.7 Contractduur

De meerderheid van de schoolbesturen geeft de voorkeur aan contracten van 4-5 jaar voor een balans tussen stabiliteit en flexibiliteit. Overstappen naar een nieuwe dienst wordt vaak als duur en complex beschouwd, waardoor kortlopende contracten door een aantal schoolbesturen als riskant worden ervaren. Daartegenover staat dat een zekere mate van flexibiliteit als belangrijk wordt beschouwd met het oog op snelle technologische ontwikkelingen.

6.2.8 Verplichting

Schoolbesturen staan over het algemeen open voor een algemene verplichting rond online veiligheid, maar zijn terughoudend tegenover een verplichting voor de dienst VI. Ze benadrukken het belang van keuzevrijheid. Daarnaast zou de dienst gratis of niet te duur moeten zijn wanneer dit verplicht zou worden. Een algemene verplichting zou volgens een PO-bestuurder helpen bij het overtuigen van PO-directeuren om meer te investeren. Daar zouden wel duidelijke eisen bij gesteld moeten worden en advies over waar men dit goedkoop en slim kan organiseren.

6.2.9 Aanbevelingen door geïnterviewde schoolbesturen

Aanbevelingen vanuit de interviews omvatten verbeterde communicatie en bekendheid rondom de dienst VI en het NDC en het aanbieden van bredere dienstverlening. Daarnaast kwam er ook het advies aan SIVON om zich niet alleen te richten op bestuurders, maar ook op de laag ICT-managers onder de bestuurders, die inhoudelijke kennis hebben en invloed

Departementaal vertrouwelijk - Dep-V

kunnen uitoefenen. Er is ook een wens geuit om niet te hoeven veranderen van Internet Service Provider bij overstap.

6.3 Tussenconclusie 3

- Het algemene beeld is dat men positief is over de beveiliging die de NDC-dienst biedt zolang scholen er niet voor hoeven te betalen en zolang afname niet verplicht is.
- Aangesloten schoolbesturen zijn over het algemeen tevreden over de dienstverlening.
- De dienst wordt door de geïnterviewde schoolbesturen vooral gezien als bedoeld voor het VO en niet voor het PO of kleine éénpitters.
- Er zijn schoolbesturen die eigen vergelijkbare oplossingen hebben (inclusief toegang tot internet via SURF) al dan niet in samenwerkingsverband met meerdere schoolbesturen.

Departementaal vertrouwelijk - Dep-V

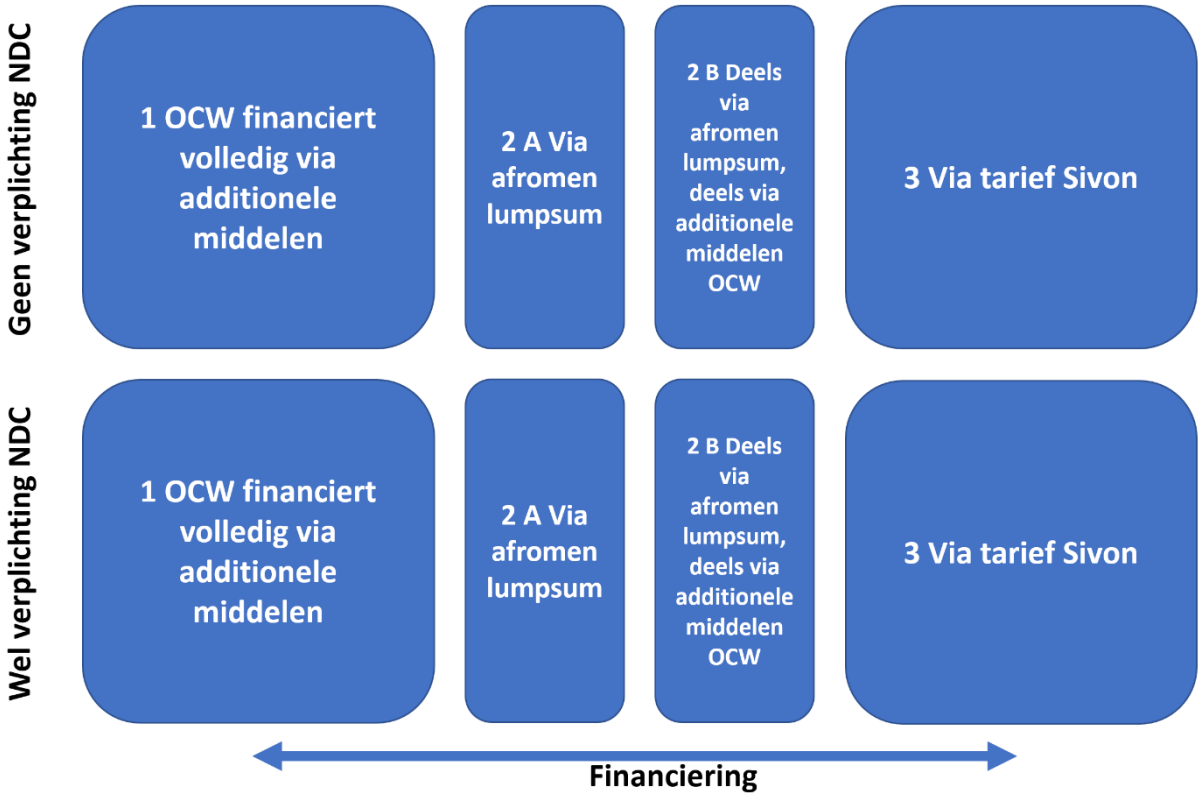
7 Juridische en financiële kaders

In samenwerking met het ministerie van OCW is gekeken naar juridische kaders voor een mogelijke verplichting van het NDC voor scholen. Daarnaast is er gekeken naar financieringsmogelijkheden.

Vanuit het al dan niet verplichten in combinatie met de wijze van financieren, ontstaat onderstaand figuur 4.

In het figuur zijn de verschillende mogelijkheden voor financiering van het NDC geschetst. De mogelijkheden voor financiering lopen van links volledige additionele middelen door OCW, naar deels additionele middelendoor OCW (beide een uitwerking een go besluit) naar geen additionele middelenrechts (een no go). Bij een no go is gekeken of een alternatief mogelijk is, zoals de kostendekking van het NDC laten lopen via een tariefheffing door SIVON bij de aangesloten schoolbesturen of door het afromen van de lumpsum. Bij deels additioneel financieren is gekeken naar de rest deels afromen van de lumpsum.

Bij het verplichten is gekeken naar de mogelijkheid om scholen verplicht gebruik te laten maken van het NDC.



Figuur 4: Juridische en financiële scenario's

Departementaal vertrouwelijk - Dep-V

7.1 Juridische kaders voor verplichting

In de bespreking met de deskundige van OCW is het volgende aan de orde gekomen:

Een volledige verplichting voor scholen om het NDC af te nemen is juridisch gezien lastig aangezien het hier niet gaat om bepaalde beveiligingsnorm maar afname van één type dienst door één aanbieder op dit moment via een lidmaatschap bij een coöperatie. Tijdens de bespreking is ook overwogen wat de implicaties zouden zijn als het als een wettelijke taak bij Kennisnet als instituut wordt neergelegd. Een wettelijke taak is altijd gekoppeld aan een verplichting. Dit is echter ook een uitdaging, omdat je bij de Europese Commissie moet bewijzen dat er dan sprake is van marktfalen.

Een meer haalbare optie lijkt een algemene verplichting voor digitale veiligheid te zijn, net zoals sociale en fysieke veiligheid ook in de Wet op het primair onderwijs en Wet op het voortgezet onderwijs is vastgelegd. Op deze manier raak je niet de vrijheid van inrichting (Artikel 23). Onder deze algemene verplichting zou het NDC wel aanbevolen kunnen worden.

Een andere mogelijkheid is om via het Normenkader IBP FO, waarbij de intentie is om dit in 2027 verplicht te stellen, een voorschrift/norm te creëren voor een bepaalde mate van internetveiligheid die lijkt op het NDC.

7.2 Tussenconclusie 4

- Een verplichting voor scholen om het NDC via de huidige constructies af te nemen is niet haalbaar.
- Het als wettelijk taak beleggen bij Kennisnet (met bijbehorende verplichte afname) wordt lastig omdat OCW dan marktfalen moet kunnen aantonen.
- Enige mate van sturing richting NDC afname (maar niet verplichting) is via een verdere uitwerking van het Normenkader IBP FO of het toevoegen van een algemene verplichting voor digitale veiligheid aan de zorgplicht van scholen (passend bij Artikel 9).

7.3 Financiële kaders

Op dit moment krijgt Kennisnet 13,5 miljoen structureel aan instellingssubsidie. Hier zitten geen wettelijke taken/verplichtingen in. Indien men ervoor kiest om een algemene verplichting voor digitale veiligheid in te voeren, met de aanbeveling van het NDC als dienst, moet er onderzocht worden of een dergelijke (extra) structurele financiering levensvatbaar is. Het is de vraag of men dan niet ingrijpt in de markt in de vorm van staatssteun. Dit moet verder uitgezocht worden door OCW in het staatsrecht. Structurele financiering wordt elke 5 jaar herzien.

De dekking van de kosten voor het NDC halen uit de lumpsum wordt experimenteel en komt (bijna) nooit voor. Ook niet als de lumpsum daarvoor eerst verhoogd zou worden. Dan moet er sprake zijn van een wettelijke verplichting of het moet goedgekeurd worden door de Tweede Kamer. Een andere mogelijkheid is dat er middelen zitten in de lumpsum die je kunt afromen, maar dit wordt ook lastig omdat per 1 januari de vereenvoudiging van bekostiging is ingetreden. Er zitten geen geoormerkte middelen voor digitale veiligheid in de lumpsum.

Departementaal vertrouwelijk - Dep-V

7.4 Tussenconclusie 5

- Bij een algemene verplichting voor digitale veiligheid met de aanbeveling om NDC als dienst af te nemen, moet worden uitgezocht door OCW of additionele structurele financiering niet wordt gezien als staatsteun.
- Structurele financiering wordt elke 5 jaar herzien.
- Financiering via de lumpsum lijkt niet haalbaar.
- Financiering via het tarief van SIVON is niet goed besproken behalve dat dan verwacht wordt dat veel schoolbesturen afhaken in verband met de hoge tarieven en dat bij de huidige aansluitingsgraad de kosten voor die scholen dusdanig hoog zijn dat ze dit helemaal niet meer bereid zijn om te betalen.
- Financiering door OCW met additionele middelen, bijvoorbeeld in combinatie met het verlengen van het overgebleven budget is een waarschijnlijke optie (linksboven in figuur 4).

De informatie ten aanzien van de juridische en financiële kaders zal ten behoeve van verdere besluitvorming worden aangevuld door inhoudelijke juridische en financiële experts van OCW (denk aan de staatssteun analyse en de check of de bekostiging van veilig internet al in de lumpsum zit).

Departementaal vertrouwelijk - Dep-V

8 Kosten, baten en prognose aansluitgraad

8.1 Kosten en prognose

Met Kennisnet zijn gesprekken gevoerd over de opbouw en kosten van de dienst NDC. Om de kosten en baten van het NDC inzichtelijk en vergelijkbaar te kunnen maken en om te voorkomen dat onjuiste conclusies getrokken worden op basis van de gedeeltelijk informatie, is ervoor gekozen om de kosten en de aansluitgraad op hoofdlijnen weer te geven. In onderstaande tabel, aangeleverd door Kennisnet, staan de kosten over de afgelopen jaren en een prognose voor de komende 10 jaar, aangevuld met het aantal leerlingen wat aangesloten is op het NDC. Hierbij is de prognose voor het aantal aansluitingen op korte termijn gebaseerd op gesprekken met schoolbesturen en contracten en toezeggingen. Voor de langere termijn betreft dit een inschatting.

Kosten NDC	2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031	2032	2033
Beheer en onderhoud NDC		€ 80.614	€ 721.652	€ 1.001.399	€ 1.393.464	€ 1.207.986	€ 1.244.226	€ 1.281.553	€ 1.409.887	€ 1.589.632	€ 1.683.531	€ 1.734.037	€ 1.939.056	€ 2.154.816	€ 2.219.460	€ 2.286.044
Investeringen in NDC		€ 157.731	€ 3.091.223	€ 3.342	€ -	€ -	€ -	€ 4.020.669	€ 1.567.994	€ 1.232.704	€ -	€ -	€ 6.477.007	€ 1.817.734	€ 1.429.042	€ -
Beheer en onderhoud besturen en locaties			€ 83.567	€ 219.306	€ 488.778	€ 567.530	€ 958.779	€ 1.344.793	€ 2.153.250	€ 2.859.021	€ 3.610.694	€ 4.381.006	€ 5.160.179	€ 5.942.957	€ 6.582.997	€ 7.131.386
Investeringen aansluitingen NDC			€ 131.963	€ 227.671	€ 463.554	€ 190.865	€ 493.345	€ 550.520	€ 1.014.615	€ 1.041.468	€ 1.069.019	€ 1.068.612	€ 1.056.633	€ 1.043.262	€ 846.221	€ 668.403
Extern personeel	€ 113.649		€ 434.311	€ 833.065	€ 587.449	€ 671.598	€ 691.746	€ 712.498	€ 733.873	€ 755.889	€ 778.566	€ 801.923	€ 825.980	€ 850.760	€ 876.283	€ 902.571
Intern personeel	€ 94.584	€ 335.178	€ 661.536	€ 965.880	€ 899.796	€ 1.322.618	€ 1.485.581	€ 1.657.132	€ 1.837.639	€ 1.892.768	€ 1.949.551	€ 2.008.038	€ 2.068.279	€ 2.130.327	€ 2.194.237	€ 2.260.064
	€ 208.233	**€ 573.522**	**€ 5.124.252**	**€ 3.250.663**	**€ 3.833.041**	**€ 3.960.597**	**€ 4.873.677**	**€ 9.567.165**	**€ 8.717.259**	**€ 9.371.484**	**€ 9.091.361**	**€ 9.993.615**	**€ 17.527.134**	**€ 13.939.855**	**€ 14.148.239**	**€ 13.248.468**

PO	besturen	-	-	2	9	27	47	70	121	168	214	261	308	354	391	419
VO	besturen	-	4	9	19	31	50	70	92	114	137	159	175	188	197	204
Totaal	besturen		4	11	28	58	97	140	213	282	351	420	483	542	588	623
Nieuwe besturen			4	7	17	30	39	43	73	69	69	69	63	59	46	35

PO	verbindingen	-	-	37	159	232	372	532	906	1.258	1.603	1.955	2.307	2.651	2.928	3.138
VO	verbindingen	-	30	41	125	144	232	325	402	498	598	678	747	802	841	870
Totaal	verbindingen	-	30	78	284	376	604	857	1.308	1.756	2.201	2.633	3.054	3.453	3.769	4.008
PO	Nieuwe verbindingen		-	37	122	73	140	160	374	352	345	352	352	344	277	210
VO	Nieuwe verbindingen		30	11	84	19	88	93	77	96	100	80	69	55	39	29
Totaal	Nieuwe verbindingen		30	48	206	92	228	253	451	448	445	432	421	399	316	239
PO	leerlingen	-	-	1.733	40.035	58.482	105.151	150.369	273.174	379.408	483.411	589.645	695.879	799.659	883.128	946.512
VO	leerlingen	-	33.775	45.355	64.184	73.770	175.986	246.998	282.812	380.094	456.516	500.759	570.497	612.833	642.676	664.886
Totaal	leerlingen	-	33.775	47.088	104.219	132.252	281.137	397.366	555.986	759.503	939.926	1.090.404	1.266.376	1.412.491	1.525.805	1.611.397

Figuur 5: Kosten en prognose NDC, bron Kennisnet

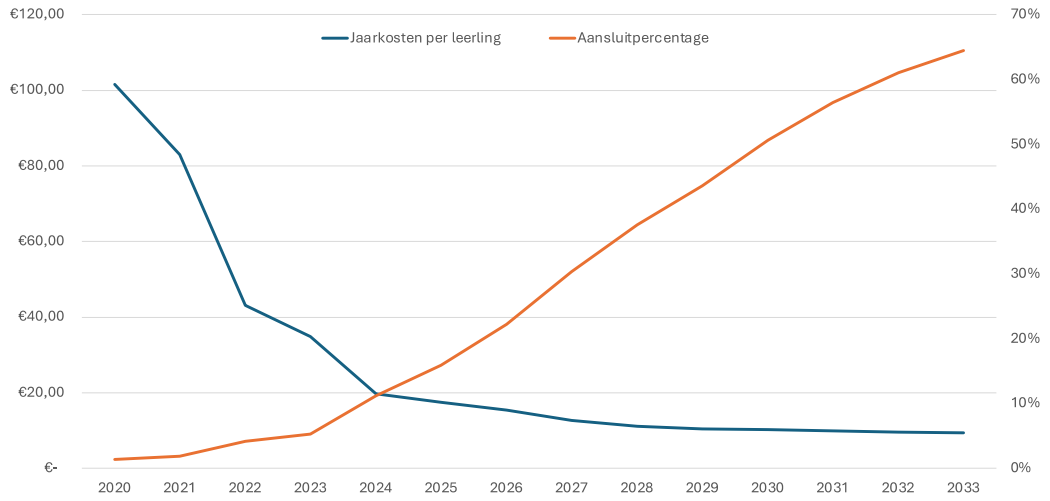
Om de kosten in de bovenstaande tabel (zie ook bijlage 14 voor een beter leesbare versie van deze tabel), aangeleverd door Kennisnet, te kunnen gebruiken voor een inzicht in het verloop over de jaren heen, zijn de investeringskosten omgerekend naar afschrijvingskosten, met een afschrijvingstermijn van 5 jaar. Dit is in de volgende tabel weergegeven. Het aantal aangesloten leerlingen, is uitgerekend in een aansluitpercentage, waarbij gerekend is met in totaal 2.500.000 leerlingen voor het FO.

Jaartal	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031	2032	2033
Kosten	€ 2.800.000	€ 3.251.000	€ 3.833.000	€ 3.961.000	€ 4.874.000	€ 5.567.000	€ 7.217.000	€ 8.171.000	€ 9.091.000	€ 9.993.000	€ 11.000.000	€ 12.000.000	€ 12.700.000	€ 13.248.000
Afschrijving	€ 650.000	€ 650.000	€ 650.000	€ 650.000	€ 650.000	€ 1.400.000	€ 1.400.000	€ 1.400.000	€ 1.400.000	€ 1.400.000	€ 2.000.000	€ 2.000.000	€ 2.000.000	€ 2.000.000
Aantal leerlingen	34.000	47.000	104.000	132.000	281.000	397.000	556.000	760.000	940.000	1.090.000	1.266.000	1.412.000	1.526.000	1.611.000
Jaarkosten	€ 3.450.000	€ 3.901.000	€ 4.483.000	€ 4.611.000	€ 5.524.000	€ 6.967.000	€ 8.617.000	€ 9.571.000	€ 10.491.000	€ 11.393.000	€ 13.000.000	€ 14.000.000	€ 14.700.000	€ 15.248.000
Aansluit percentage	1%	2%	4%	5%	11%	16%	22%	30%	38%	44%	51%	56%	61%	64%
Jaarkosten per leerling	€ 101	€ 83	€ 43	€ 35	€ 20	€ 18	€ 15	€ 13	€ 11	€ 10	€ 10	€ 10	€ 10	€ 9

Figuur 6: Investeringskosten omgerekend naar afschrijvingskosten

Departementaal vertrouwelijk - Dep-V

De omgerekende cijfers zijn gebruikt om een grafiek te maken, met op de ene as de jaarkosten per aangesloten leerling en op de andere as het aansluitpercentage.



Figuur 7: Aansluitpercentage NDC afgezet tegen kosten per leerling per jaar

Uit deze grafiek en tabel kunnen we de volgende zaken afleiden;

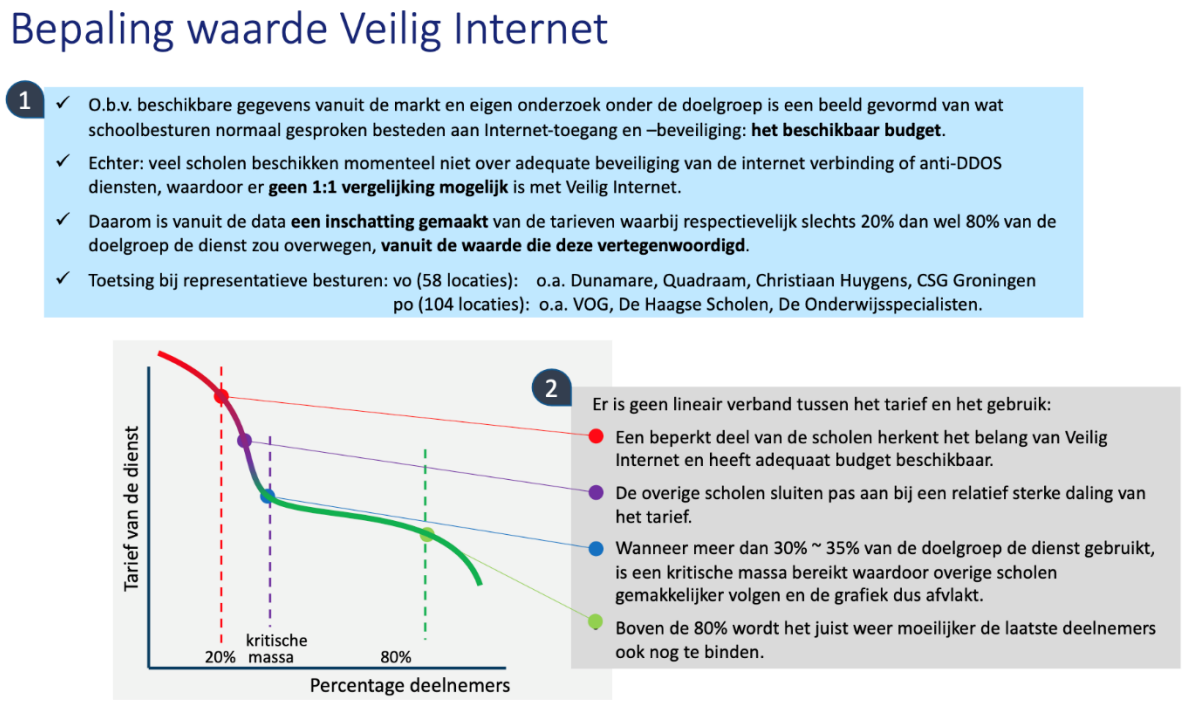
- De afgelopen jaren is er sprake geweest van een matige groei in het aansluitpercentage. Uit de gesprekken met Kennisnet en SIVON komt naar voren dat veel schoolbesturen langlopende contracten hadden afgesloten voor connectiviteit en bijbehorende securitymaatregelen.
- De komende twee jaar zal volgens de grafiek het aansluitpercentage groeien van 5 naar 16%, blijkt uit door Kennisnet aangegeven informatie. Vanuit de gesprekken die zijn gevoerd met de schoolbesturen, kunnen we bevestigen dat er twee grote schoolbesturen in een aansluitfase zitten en een dit overweegt na de afschrijvingsperiode van de apparatuur. De door Kennisnet aangegeven 30% in 2027 wordt door deze aansluitingen niet gerealiseerd. Op verzoek kan Kennisnet inzage geven in de concrete toezeggingen voor aansluitingen de komende periode.
- Kennisnet verwacht de komende twee jaar een fors aantal leerlingen aan te kunnen. Bij een aansluitgraad hoger dan 30%, daalt de prijs per aangesloten leerling naar 12 euro per jaar.
- In het eerste jaar van het NDC waren door de eenmalige investeringskosten en de nog geringe aantal aangesloten leerlingen de kosten per aangesloten leerling ongeveer 100 euro per jaar. Na drie jaar NDC zijn in 2023 de kosten per aangesloten leerling gedaald naar 35 euro per jaar. Vanaf 2027 zullen de kosten per aangesloten leerling (mits het aansluitpercentage van minimaal 30% wordt gerealiseerd) verder dalen tot ongeveer 12 euro per jaar. Bij een verdere groei van het NDC zullen de kosten per aangesloten leerling niet verder dalen.
- Bij een aansluitpercentage van hoger dan 30% is een uitbreiding van de onderliggende infrastructuur van het NDC noodzakelijk om het bijbehorende volume aan aangesloten leerlingen op te vangen. De jaarkosten per leerling zullen hierbij niet veel meer afnemen. Uit de aangeleverde cijfers van Kennisnet blijkt dat het volume van de dienst, bij verdere uitbreidingen, geen effect meer heeft op de kosten per aangesloten leerling. De kosten voor het NDC zijn in een optimale variant, bij een aansluitpercentage van 30% of hoger, 12 euro per leerling.
- Het NDC is bij een aansluitpercentage van meer dan 30% een kosteneffectieve gecentraliseerde beveiligingsoplossing, die in de basis (geredeneerd vanuit de technische opzet) als publieke voorziening kan worden gepositioneerd.

Departementaal vertrouwelijk - Dep-V

- Met een beperkte aanvullende financiering (ten opzichte van de start subsidie) is het mogelijk het NDC te laten voortbestaan en daarmee voor het gehele FO een alternatief beschikbaar te hebben voor een centrale voorziening voor veilig internet.

8.2 Kosten en tarieven Veilig Internet

Uit onderzoek door SIVON en Kennisnet naar de tariefstelling van de NDC dienst komt naar voren dat er een viertal verbanden zijn tussen het tarief en het gebruik van het NDC[8]. Hierbij worden de totale kosten voor het NDC verdeeld over het aantal aangesloten schoolbesturen en leerlingen. Bij een lager aansluitpercentage zijn er hoge kosten voor het beperkt aantal aangesloten scholen. Bij een aansluitpercentage van 30% of hoger is te zien dat de kosten niet veel meer afnemen per aansluiting. Deze 30% aansluitpercentage komt overeen met het in de vorige alinea aangegeven aansluitpercentage op basis van kosten en prognose NDC. Anders gezegd, bij een aansluitpercentage van 30% of hoger heeft het NDC het meest optimale prijsniveau, bij een hoger aansluitpercentage, zullen de kosten per aangesloten leerling niet lager worden.



Figuur 8: Bepaling waarde Veilig Internet

8.3 Overige baten van het NDC

Naast bovengenoemde kwantitatieve baten, is er nog een aantal kwalitatieve baten die voortkomen uit de opzet van het NDC. Dat zijn:

- De technische opzet van het NDC, wordt (mede op basis van het uitgevoerde technisch onderzoek) gezien als een referentie voor het aanbieden van een gecentraliseerde oplossing voor beveiligingsmaatregelen. Door deze referentie op te nemen in het

[8] Resultaten onderzoek beschikbaar gesteld door SIVON/Kennisnet in een presentatie, met de titel: Kosten en tarieven Veilig Internet

Departementaal vertrouwelijk - Dep-V

Normenkader IBP FO (als voorkeur uitwerking) wordt deze oplossing voor alle betrokkenen in het FO bruikbaar en hanteerbaar.

- Door de centrale opzet van het NDC, wordt er slim en efficiënt gebruik gemaakt van (de schaars in de markt aanwezige) expertise en ervaring op cyber-securitygebied.
- Het NDC kan als bouwsteen dienen voor het Programma Digitaal Veilig Onderwijs, waarbij op basis van deze bouwsteen, aanvullende diensten als monitoring, logging, SOC en SIEM diensten kunnen worden gekoppeld. Deze aanvullende diensten kunnen vervolgens een opmaat zijn voor diensten als CISO-as-a-service, voor aangesloten schoolbesturen die zelf geen CISO kunnen of willen aanstellen.
- Doordat schoolbesturen kunnen kiezen voor een aansluiting op het NDC worden zij ontzorgd, zijn ze minder afhankelijk van specifieke kennis en expertise binnen het eigen schoolbestuur en kunnen zij de aandacht richten op hun primaire taak; goed (digitaal) onderwijs organiseren en geven. Los van de rol van het NDC, blijven schoolbesturen zelf verantwoordelijk voor het organiseren van de beveiliging.

8.4 Tussenconclusie 6

- De afgelopen jaren is er sprake geweest van een matige groei in het aansluitpercentage, Kennisnet en SIVON verwachten dat het aansluitpercentage komende 2 jaar zal groeien van 5% naar 16% van de schoolbesturen.
- Bij een aansluitgraad hoger dan 30% daalt de prijs per leerling naar 12 euro per jaar. Hiermee wordt voor het NDC het meest optimale kostenniveau per aangesloten leerling bereikt.
- De baten vertalen zich naar een efficiënte, toekomstvaste, schaalbare en gecentraliseerde (deskundig personeel en technische kennis) oplossing voor veilig internet.
- Een centrale opzet van het NDC maakt slim en efficiënt gebruik van (schaarse) cybersecurity expertise en ervaring. Scholen worden ontzorgd en kunnen zich richten op het goed (digitaal) onderwijs organiseren en geven
- Het NDC kan dienen als bouwsteen voor het Programma Digitaal Veilig Onderwijs, waarop aanvullende diensten kunnen worden gekoppeld.

Departementaal vertrouwelijk - Dep-V

9 Argumenten no go / go besluit

De uitkomsten van de gemaakte analyses leiden tot de volgende argumenten voor een no go of go besluit van het NDC.

9.1 Argumenten no go besluit

- Techniek: Aansluiting op de dienst kan niet verplicht worden. Daarmee kan niet afgedwongen worden dat iedere school ook daadwerkelijk gebruik maakt van de dienst. Het Normenkader IBP FO schrijft het gebruik van (een dienst voor) veilig internet niet direct voor. Vanuit de interviews met schoolbesturen blijkt weinig draagvlak voor verplichten NDC gebruik (hoe), wel voor het verplichten van het Normenkader IBP FO (wat).
- Techniek: Door het aanbieden van een centrale voorziening vanuit de overheid, is deze ook verantwoordelijk voor beheer en doorontwikkeling. Dit kan leiden tot aansprakelijkheidsstelling of politiek afbreukrisico.
- Beveiliging: Een centrale infrastructurele voorziening is niet noodzakelijk om additionele beveiligingsdiensten voor scholen aan te bieden, wel makkelijker. Een voorbeeld van een gezamenlijke centrale voorziening (op vrijwillige basis) zien we in SURFsoc. In de markt zijn meerdere partijen die additionele beveiligingsdiensten aanbieden.
- Financiën: Het aansluiten van **alle** 2.500.000 leerlingen in het FO op de dienst Veilig Internet wordt ingeschat door Kennisnet op ongeveer € 30 mln per jaar. Deze kosten zijn 5x zoveel als programma Digitaal Veilig Onderwijs (€ 6 mln per jaar), zonder duidelijkheid over het effect op veiligheid voor het FO in zijn geheel. Bij het organiseren van veiligheid geldt over het algemeen dat de zwakste schakel bepalend is voor de sterkte van de keten. Om een sterke beveiliging te organiseren zijn de onderdelen mens, techniek en organisatie nodig. Naast een voorziening als het NDC, zal er ook aandacht besteed moeten worden aan mens en organisatie, zie hiervoor ook de maatregelen in het Normenkader IBP FO.
- Financiën: Het risico dat de EC de NDC financiering ziet als verpakte staatssteun.
- Transitie: Het aanbod van internetbeveiligingsdiensten in de markt ontwikkelt zich snel. Scholen kunnen hier (al dan niet in samenwerkingsverbanden) zelf gebruik van maken en doen dit in sommige gevallen ook al. Of er sprake is van marktfalen moet uit een nadere analyse blijken.

9.2 Argumenten go besluit

- Techniek: Kwaliteit/marktconformiteit van het NDC voldoet. Er is vooralsnog geen vergelijkbaar aanbod voor schoolbesturen, tenzij zij dit (in gezamenlijkheid) zelf faciliteren. Veilig internet is hiermee in de vorm van het NDC voor alle FO-schoolbesturen beschikbaar.
- Beveiliging: OCW laat zien werk te maken van een digitaal veilige leeromgeving voor elke leerling in het FO door te investeren in de dienst waarop het Programma Digitaal Veilig Onderwijs voortbouwt.
- Beveiliging: Een centrale voorziening waar (bijna) alle scholen op zijn aangesloten biedt mogelijkheden om additionele beveiligingsdiensten (zoals monitoring, incident-response etc.) op te bouwen.
- Financiën: Veilig internet is een basisvoorziening waarover elke school anno 2023 moet kunnen beschikken. Door dit vanuit de overheid te faciliteren én te financieren komt OCW tegemoet aan de oproep van scholen dat digitalisering steeds hogere kosten met zich meebrengt en dat ze daar niet voor gecompenseerd worden.
- Financiën: Eén centrale voorziening voor de hele sector is doelmatiger dan wanneer scholen dit zelf gaan inkopen. Het NDC dient als referentie, heeft een beheersbare kwaliteit en is toekomstvast. Bij voldoende aansluitgraad zijn de kosten minder dan 1 euro per aangesloten leerling per maand. De kosten (inspanning) van een

Departementaal vertrouwelijk - Dep-V

vergelijkbare voorziening voor een zelfstandig schoolbestuur (zelf organiseren) zijn door de beperktere schaal minimaal twee keer zo groot.

- Transitie: Een aansluitgraad van 30% lijkt haalbaar gezien de gegeven condities en verkregen informatie. Voor een (veel) hogere aansluitgraad zullen additionele inspanningen noodzakelijk zijn.

Departementaal vertrouwelijk - Dep-V

10 Scenario's no go/go

10.1 Scenario no go

Een no go besluit betekent geen additionele middelen vanuit OCW. Op dit moment heeft Kennisnet nog een groot deel van het subsidiebedrag (zo'n € 22 mln, voor minimaal 3 jaar NDC exploitatie) in reserve. Hiermee kan een afbouw-scenario worden gefaciliteerd, zowel voor Kennisnet zelf als voor het helpen van bestaande klanten bij het zoeken naar een alternatief. Het eventuele resterende bedrag aan het einde van 2027 zal terugvloeien naar OCW. Nieuwe schoolbesturen zullen zich niet meer kunnen aanmelden en zoals gezegd zullen bestaande klanten op zoek moeten naar een alternatief. In de tussentijd blijft Kennisnet de dienstverlening op het afgesproken niveau leveren. Een effect kan ook zijn reputatieschade bij OCW door deze dienst niet verder te financieren en daarmee op dit punt niet verder te willen zorgen voor de veiligheid van het FO, zo kan worden geredeneerd. Een dergelijk besluit zal goed moeten worden uitgelegd aan de raden en overige stakeholders.

10.1.1 Rollen en verantwoordelijkheden bij een no go

Bij een no go besluit blijft Kennisnet verantwoordelijk voor het leveren van de dienst aan de huidige klanten van NDC voor de duur van het contract. Daarnaast is Kennisnet verantwoordelijk voor het afbouwen van de dienst, denk aan het opzeggen van contracten zoals met SURF, Axians, Equinix.

OCW blijft streven naar een onderwijssector waarin elke leerling digitaal veilig kan leren en medewerkers in een digitale werkomgeving veilig kunnen werken. Bij een no go verwacht OCW dat schoolbesturen de diensten zoals geleverd door NDC bij marktpartijen kunnen afnemen conform het Normenkader IBP FO.

Schoolbesturen blijven zelf verantwoordelijk hoe ze invulling geven in het algemeen aan het Normenkader IBP FO en specifiek aan veilig internet. Bij het afsluiten van contracten met marktpartijen bijvoorbeeld voor access moeten schoolbesturen daarin de diensten rondom veilig internet meenemen.

Departementaal vertrouwelijk - Dep-V

10.2 Scenario go

Bij een go besluit zorgt OCW voor additionele middelen waardoor er financiële zekerheid is voor de periode van 2027 tot minimaal 2030, omdat SIVON 3-jarige contracten afsluit met schoolbesturen voor aansluiting op het NDC. De enige voor de hand liggende manier van financiering op dit moment lijkt een additionele subsidie aan Kennisnet om het NDC te blijven exploiteren.

Tot nu toe blijft het aansluitpercentage achter bij gemaakte afspraken, het is niet volledig duidelijk waar dit precies door komt. Vaak wordt genoemd de looptijd van huidige contracten, overstappen gaat langzamer dan verwacht, er is al een werkende voorziening, niet aantrekkelijk voor de doelgroep PO, etc.

Over het te verwachtten aansluitpercentage, zullen in de aansturing en financiering van Kennisnet nadere afspraken gemaakt moeten worden. Het benodigde bedrag aan additionele middelen hangt af van de ambitie en afspraken die gemaakt worden over het aansluitpercentage van schoolbesturen op het NDC en vervolgens de sturing daarop. Een aansluitgraad van minimaal 30% binnen redelijke termijn lijkt realistisch en haalbaar.

Een hoger percentage aangesloten schoolbesturen lijkt niet haalbaar:

- Dienst lijkt vooral voor grotere VO-scholen aantrekkelijk
- Dienst lijkt een overkill te zijn voor PO en kleinere éénpitters
- Sommige (grote) schoolbesturen of groepen van schoolbesturen hebben een soortgelijke dienst al zelf ingericht of gekocht
- Sommige schoolbesturen zitten in een juridische constructie (een stichting) met commitment naar andere schoolbesturen die ook in die constructie zitten. Vaak zijn dit soort stichtingen ontstaan toen gezamenlijk breedband internet (glasvezel) werd aangelegd.

10.2.1 Rollen en verantwoordelijkheden bij een go

Bij een go wordt het NDC als middel om te zorgen voor veilig internet voor het FO voortgezet. OCW voorziet in additionele middelen en maakt afspraken met SIVON en Kennisnet over gewenste aansluitpercentages van schoolbesturen en stuurt daarop.

Kennisnet zorgt dat de techniek en organisatiecapaciteit voldoende is om de afgesproken percentages aan te kunnen. SIVON brengt het NDC onder de aandacht bij schoolbesturen en stuurt op de met OCW afgesproken aansluitpercentages.

Schoolbesturen blijven zelf verantwoordelijk en mogen zelf bepalen hoe en bij wie ze zorgen voor veilig internet. Dit kan via SIVON/Kennisnet maar kan ook bij een marktpartij.

Departementaal vertrouwelijk - Dep-V

11 Bijlage: Interviewleidraad schoolbesturen en tabel met bevindingen

Interviewleidraad voor schoolbesturen aangesloten bij het NDC

Inleiding + achtergrondinformatie

- Namen, functies, organisatie
- Introductie en uitleg (architectuur plaatje)

Motivatie aansluiting

- Waarom heeft deze school besloten om zich aan te sluiten bij de dienst Veilig Internet en het NDC (daarna NDC)?
- Sluit de dienst VI/NDC tot nu toe aan bij je verwachtingen?

Tevredenheid over de dienst VI/NDC algemeen

- Hoe kijk je aan tegen de dienst VI/NDC?
- Kun je ons vertellen over je ervaring met VI/het NDC?
  - Wat loopt er goed?
  - Wat kan verbeterd worden?
  - Wat zijn de voordelen/nadelen?
  - Hoe worden afspraken nagekomen en vastgelegd?
  - Hoe zou je de algehele tevredenheid omschrijven?

Online veiligheid

- Hoe belangrijk is online veiligheid van (FO) in jouw ogen? / Staat dit (hoog) op de bestuurlijke agenda?
- Hoe kijk je aan tegen het Normenkader IBP FO, waar staan jullie als schoolbestuur?
- Hoe belangrijk is de rol van VI/het NDC daarin gezien vanuit jouw eigen organisatie/onderdeel? Heeft het bijgedragen aan het verbeteren van de online veiligheid (bijv. voorkomen van DDoS aanvallen?)

Financiële overwegingen

- In hoeverre ben je tevreden over de kosten van VI/het NDC? (Wat zijn deze kosten?)
- Zijn deze kosten hoger, gelijk of lager dan wat je hiervoor betaalde bij een commerciële partij?
- Zou je bij VI/het NDC aangesloten blijven indien de prijzen hoger worden (ivm wel/niet stoppen van OCW met NDC)? Wat zou daar dan tegenover moeten staan?
- Tot welke prijs ben je bereid aangesloten te blijven bij VI/het NDC?

Contracten

- De contractduur kan een bottleneck zijn hebben we begrepen. Is dat bij jullie ook een issue geweest?

Verplichting

- Hoe sta je tegenover een verplichting van VI/het NDC voor alle scholen in het FO?
- Wat zijn dan de randvoorwaarden?

Aanbevelingen of suggesties

- Heb je mogelijke aanbevelingen of suggesties voor verbetering van VI/het NDC?

Afsluiting

- Kunnen we je benaderen voor extra input op een later moment?

Departementaal vertrouwelijk - Dep-V

Interviewleidraad voor schoolbesturen niet-aangesloten bij het NDC

Inleiding + achtergrondinformatie

- Namen, functies, organisatie
- Introductie en uitleg (architectuur plaatje)

Motivatie niet-aansluiting

- Ben je bekend met SIVON en de dienst VI/het NDC?
  - Zo ja, hoe kijk jij aan tegen VI/het NDC?
  - Zo ja, kun je ons vertellen waarom deze school niet is aangesloten bij VI/het NDC? Welke overwegingen hebben geleid tot deze beslissing?
- Zo nee, uitleggen wat SIVON, VI en het NDC is.

Online veiligheid

- Hoe belangrijk is online veiligheid (van FO) in jouw ogen? / Staat dit (hoog) op de bestuurlijke agenda?
- Hoe kijk je aan tegen het Normenkader IBP FO, waar staan jullie als schoolbestuur?
- Welke beveiligingsmaatregelen heeft deze school momenteel getroffen voor veilig internet?
- Zijn deze maatregelen in jouw ogen voldoende?

Tevredenheid huidige aanbieder

- In hoeverre ben je tevreden over deze huidige beveiligingsmaatregelen bij jullie huidige aanbieder?

Financiële overwegingen

- Wat zijn de kosten van de huidige beveiligingsmaatregelen?
- In hoeverre ben je tevreden over de kosten van deze beveiligingsmaatregelen?
- Voor welke prijs ben je bereid over te stappen naar de diensten van VI/het NDC? (Huidige prijs benoemen?)

Contracten

- De contractduur kan een bottleneck zijn hebben we begrepen. Is dat bij jullie ook een issue geweest?

Verplichting

- Hoe sta je tegenover een verplichting van VI/het NDC voor alle scholen in het FO?
- Wat zijn dan de randvoorwaarden?

Aanbevelingen of suggesties

- Wat zou er volgens jou moeten veranderen of verbeteren zodat deze school zich aansluit bij VI/het NDC?

Afsluiting

- Kunnen we je benaderen voor extra input op een later moment?
- OCW gebruikt dit voor besluitvorming, we sturen het gespreksverslag nog naar je toe.

Departementaal vertrouwelijk - Dep-V

Samenvatting geïnterviewde scholen

PO

	Schoolbestuur 1	Schoolbestuur 2	Schoolbestuur 3
Grootte school	Klein PO éénpitter 400 leerlingen en 95 medewerkers	Middelgroot PO 23 scholen en 5500 leerlingen en 550 medewerkers	Groot 68 PO scholen, 20 peuterspeelzalen en 1 Pabo 22.000 leerlingen en 2500 medewerkers
Aangesloten bij SIVON	Nee	Ja	Nee
Aangesloten bij NDC/VI	Nee	Ja	Nee
Motivatie (niet) aansluiting	Niet bekend en niet overwogen.	Bestuurder met ICT-kennis, betere beveiliging, betrouwbaarheid, leverancierszekerheid, collectief dragen.	Hebben eigen oplossing waar ze tevreden over zijn.
Alternatieve beveiliging	Zakelijke glasvezel leverancier. Wifi en firewall bij commerciële partij. Hebben een groep 'ICT-ouders' die ondersteunen.	n.v.t.	Beheren eigen netwerk in samenwerking met Axians. Firewalls, monitoring en filtering. Internetaansluiting Ziggo Zakelijk.
Tevredenheid dienstverlening SIVON	n.v.t.	Tevreden. Wordt meegedacht.	n.v.t.
Bestuurlijke agenda en Normenkader IBP FO	Staat op de bestuurlijke agenda. Actief bezig met Normenkader IBP FO en met bewustwording.	Staat op de bestuurlijke agenda.	Staat op agenda, maar primaire proces blijft lesgeven. Gebruiken Normenkader IBP FO voor HO door de Paboschool. Nu in vastleggingsfase en volgend jaar een externe audit.
Kosten en eventueel overstappen	Ze betalen €100 per maand en zijn tevreden over dit relatief lage bedrag. Investeren liever in onderwijs.	VI is duurder dan wat er voorheen werd betaald en inkoop was niet gemakkelijker. Maar veiligheid woog zwaarder.	Prijs zou moeten passen binnen de begrotingen. Geen reden om over te stappen tenzij er een zwaarwegend incident zou plaatsvinden.
Contracten	Liever langlopende contracten dan kortlopende contracten. Geeft zekerheid in financiën.	Minimaal 5 jaar voor zekerheid.	Ongeveer 5 jaar.
Verplichting	Zijn tegen een algemene verplichting, scholen voelen zich verantwoordelijk. Zijn ook tegen een verplichting van de dienst VI en benadrukken keuzevrijheid.	Voor een algemene verplichting, maar dan wel duidelijke eisen stellen en doorverwijzen naar waar je dit goed kan regelen. Tegen een verplichting van de dienst VI.	Tegen verplichtingen. Benadrukken belang van keuzevrijheid.
Aanbevelingen	Bekendheid en communicatie van VI en SIVON vergroten, met als goed voorbeeld Kennisnet. Voelen zich als eenpitter niet vertegenwoordigd door de raden.	Dienstverlening voor PO zou breder moeten zijn. PO-scholen willen doorgaans liever alles van begin tot einde bij één partij afnemen.	Geen aanbevelingen.

Departementaal vertrouwelijk - Dep-V

VO

	Schoolbestuur 4	Schoolbestuur 5	Schoolbestuur 6
Grootte school	Klein 1310 leerlingen	Klein VO éénpitter 1700 leerlingen en 200 medewerkers	Groot VO 45 locaties en 12 instellingen 33.000 leerlingen en 4300 medewerkers
Aangesloten bij SIVON	Ja	Ja	?
Aangesloten bij NDC/VI	Nee, zijn aangesloten bij stichting waar ze zelf eigenaar van zijn.	Ja	Nee
Motivatie (niet) aansluiting	Niet lang op de hoogte van NDC en zijn tevreden over eigen oplossing.	Eerdere contract liep af na 15 jaar. De dienst VI had de beste prijs.	Overwogen maar technisch niet compatibel met eigen oplossing die al langer bestond dan VI. Tevreden over eigen oplossing.
Alternatieve beveiliging	Virusscanner en eigen glasvezelring met SURF-internet met o.a. DDoS protectie.	n.v.t.	Eigen glasvezelnetwerk met SURF-internet met o.a. DDoS protectie. Eigen firewall.
Tevredenheid dienstverlening SIVON	Tevreden. Netwerkbeheerder via SIVON geregeld.	Erg tevreden. Communicatie over onderhoud en storingen goed. SIVON denkt mee en geeft advies.	n.v.t.
Bestuurlijke agenda en Normenkader IBP FO	Hoog op de bestuurlijke agenda. Stappenplan tot 2026.	Staat op de bestuurlijke agenda. Er is een stuurgroep ICT. Binnenkort aan de slag met Normenkader IBP FO i.s.m. SIVON.	Hoog op de bestuurlijke agenda. Binnenkort een deep dive om niveau te bepalen.
Kosten en eventueel overstappen	Tevreden over huidige kosten. Mocht VI veel goedkoper worden dan zou het overwegen.	Kosten gedreven. Kijken naar wat het voordeligste is. Als VI duurder zou worden zouden ze opnieuw opties overwegen.	Tevreden over huidige kosten bij SURF. Zouden overwegen om over te stappen naar VI als dit goedkoper is. Huidige contract loopt tot 2026. Duidelijkheid over subsidie is wenselijk.
Contracten	3-4 jaar gebruikelijk	3-5 jaar. Hebben negatieve ervaring met langlopende contracten (15 jaar). Ze betaalden te veel voor weinig, technologische ontwikkelingen hadden het contract ingehaald.	Het liefst minimaal 5 jaar. Zekerheid van leverancier en diensten belangrijk wegens complexiteit en risico's.
Verplichting	Voor een algemene verplichting, tegen een verplichting van de dienst VI.	Voor een algemene verplichting en een dienst zoals VI. Mocht het duurder worden moet het wel mogelijk zijn om over te stappen.	Voor een algemene verplichting, tegen een verplichting van de dienst VI. Stelselverantwoordelijkheid OCW belangrijk.
Aanbevelingen	Is er wel goed vooronderzoek gedaan naar de behoeften van scholen?	Geen aanbevelingen.	Duurzame strategie belangrijk voor VI. Duidelijkheid over subsidie en de dienst belangrijk in keuze om over te stappen. Aan welke kosten moeten ze denken als de subsidie stopt?

Departementaal vertrouwelijk - Dep-V

PO en VO

	Schoolbestuur 7	Schoolbestuur 8	Schoolbestuur 9
Grootte school	Middelgroot 7 VO en 1 PO 7000 leerlingen en 1200 medewerkers	Middelgroot 16 PO en 6 VO 9740 leerlingen en 1295 medewerkers	Groot 47 PO, 33 VO en 7 speciaal onderwijs 38.000 leerlingen en 4600 medewerkers
Aangesloten bij SIVON	Ja	Ja	Ja
Aangesloten bij NDC/VI	Ja, aansluitingsfase	Ja, gedeeltelijk. VO-scholen wel, PO-scholen niet.	Ja, aansluitingsfase
Motivatie (niet) aansluiting	Zien aansluiting als opstap om aan IBP-normen-kader te voldoen en om risico's af te dekken.	Samenwerking komt prijs, kwaliteit en continuïteit ten goede.	Hadden al goede oplossing maar overgestapt om collectief te dragen.
Alternatieve beveiliging	Hebben nu nog firewalls die worden afgeschaald.	PO-scholen gebruiken nog een zakelijke internetverbinding zonder extra beveiliging.	Eigen glasvezel via stichting met eerder een SURF-internet verbinding.
Tevredenheid dienstverlening SIVON	Tevreden	Tevreden, alles verloopt goed. Proactieve communicatie door SIVON.	Tevreden over dienstverlening maar VI heeft beperkte technische mogelijkheden t.o.v. eigen oude oplossing
Bestuurlijke agenda en Normenkader IBP FO	Hoog op de bestuurlijke agenda. Verander-programma, awareness en roadmap voor Normenkader IBP FO.	Hoog op de bestuurlijke agenda. Hebben externe audits laten doen en pakken vervolg op.	Met pieken en dalen hoog op de bestuurlijke agenda. Nulmeting en meerjarenplan tot 2027.
Kosten en eventueel overstappen	Tevreden over de kosten van VI. Willen volledig ontzorgd zijn. Bereid om meer te betalen als het doorgroeit naar een SIEM/SOC oplossing.	Investeringen nodig, bereid om wat extra te betalen maar kunnen deze kosten niet alleen dragen. Samenwerking is nodig.	Marktconforme prijzen is voldoende. Wanneer VI veel duurder zou worden dan eigen firewall wordt het ingewikkeld.
Contracten	Geen duidelijke mening over contractduur. Geven wel aan dat verandering ingrijpend is.	Een mate van flexibiliteit in contracten is belangrijk i.v.m. snelle technologische ontwikkelingen.	Geen uitspraken over. Geven wel aan dat verandering ingrijpend is.
Verplichting	Staan positief tegenover verplichtingen voor online veiligheid en het NDC. Veiligheid is belangrijk.	Staan positief tegenover verplichtingen voor online veiligheid en het NDC. Verplichting zou helpen in het overtuigen van PO-directeuren om over te stappen. Dit is op dit moment lastig.	Niet blij met verplichtingen, maar misschien nodig om kleinere besturen te beschermen tegen zichzelf.
Aanbevelingen	Uitgroeien naar completere dienst, meer beheermogelijk-heden, liever geen wisseling van ISP, koppeling VI en SURF-CERT loslaten	Differentiatie in aanbod PO en VO. Firewall wordt nu aangeboden maar hebben scholen vaak al. Niet efficiënt. SIVON zou zich ook moeten richten op ICT-managers met invloed.	Behoefte aan meer functionaliteiten en inzicht in logging en systemen.

Departementaal vertrouwelijk - Dep-V

12 Bijlage: Onderzoek techniek en processen

Er bestaan twee versies van het document met de onderzoeksresultaten, te weten een short-form (tot en met Bijlage A) en een long-form (tot en met bijlage D). De short-form is geschikt voor verspreiding buiten de betrokken organisaties en is gebruikt voor deze bijlage. De long-form heeft een hogere classificatie van vertrouwelijkheid en is bedoeld voor de direct betrokkenen.

Onderzoeksmethode

Het onderzoek heeft plaats gevonden als interne review. Dit betekent dat de inrichting van de dienst als eerstelijns kwaliteitsreview is bekeken. Het beperkt de diepgang van de review. Er is in beperkte mate in de systemen gekeken. De meeste informatie is ingewonnen op basis van aangeleverde documentatie of door middel van interviews met betrokkenen. De interviews zijn afgenomen door twee zeer ervaren securityspecialisten in de rol van expert en auditor.

Technisch onderzoek

Dit document bevat de belangrijkste resultaten, bevinding en aanbevelingen die als resultaat van de review van de technische implementatie van de dienst "Veilig Internet" voor het funderend onderwijs. De belangrijkste toets vragen zijn:

- Is de dienst veilig genoeg, vergeleken met de huidige beschikbare technologie in de markt?
- Is de dienst voldoende schaalbaar voor toekomstige groei?

Beide vragen kunnen positief worden beantwoord.

De technische oplossing maakt gebruik van een marktconform, commercial off the shelf (COTS) firewall product (Fortinet) dat gebruikt wordt door Internetproviders, grote gebruikers van Internet, overheden en financiële instellingen.

De oplossing is voorzien van Unified Threat Management (UTM) dat bescherming biedt tegen onder meer aanvallen via (kwaadaardige) webservers, botnets en Denial of Service. De deelnemende scholen zijn onderling van elkaar gescheiden om 'kruisbesmetting' van de ene school naar de andere te voorkomen. Alleen met expliciete toestemming van beide scholen kan onderling verkeer worden uitgewisseld. Ook dit onderlinge verkeer wordt door de firewall gecontroleerd.

De huidige implementatie biedt voldoende ruimte voor groei, zowel voor bandbreedte als voor verwerkingscapaciteit. De huidige inrichting en opschaling is gebaseerd op een groter aantal deelnemers dan op dit moment actief. Bij sterke groei kan de huidige inrichten worden gekopieerd waardoor er voldoende ruimte voor groei beschikbaar blijft.

Kennisnet werkt aan de doorontwikkeling van de huidige oplossing, met name op het gebied van beheersbaarheid. Dit geeft aan dat Kennisnet tijd, kennis en middelen blijft investeren in de oplossing, ook om deze toekomstvast te houden.

Organisatorisch onderzoek:

Risico	#	Beheersingsvraag	Bevindingen interne review
De organisatie hanteert een managementsysteem om zicht te krijgen op het wel of niet behalen van	1	Beleidsdocumentatie	Voldoet
	2	Risicoanalyse	
	3	Key Performance Indicatoren	
	4	Interne Audits	

doelstellingen voor informatiebeveiliging. **Risicoscore: Midden**	5	Directiebeoordeling	
Logische toegangsbeveiliging			
1. Eindgebruikers omzeilen systeem afgedwongen autorisaties en functiescheidingsmaatregelen 2. Wachtwoord en/of andere beveiligingsmaatregelen worden omzeild. **Risicoscore: Hoog**	6	Worden rechten op een gecontroleerde wijze ontwikkeld en toegekend rekening houdend met functiescheiding in IT en de lijn?	Voldoet
	7	Hoe worden rechten toegekend, gemuteerd en ontnomen?	Voldoet
	8	Worden rechten periodiek gecontroleerd?	Voldoet
	9	Hoe is functiescheiding toegepast in het systeem en/of het proces?	Voldoet
	10	Is er een systeem eigenaar, hoe is deze betrokken bij de functionaliteiten in het systeem?	Voldoet
	11	Welke toegangscontrole is van toepassing op de applicatie, met welke instellingen?	Voldoet
	12	Op welke wijze is directe toegang tot de database/bron-informatie geblokkeerd of gemanaged?	Voldoet
	13	Welke additionele tooling voor de database is in gebruik?	Voldoet
	14	Hoe zijn stamgegevens en configuratiebestanden beveiligd?	Voldoet
Wijzigingsbeheer			
3. Ongeautoriseerde of onvoldoende geteste wijzigingen worden in productie doorgevoerd waardoor systemen niet meer juist, volledig en tijdig verwerkingen uitvoeren. **Risicoscore: Midden**	15	Is er een wijzigingsproces beschreven relevant voor het systeem?	Voldoet
	16	Worden alle wijzigingen via het proces uitgevoerd?	Voldoet
	17	Hoe worden wijzigingsverzoeken vastgelegd?	Voldoet
	18	Wordt getest en zo ja, hoe wordt de range en diepgang bepaald?	Voldoet
	19	Wie wordt betrokken tijdens het testen en hoe worden bevindingen vastgelegd?	Voldoet
	20	Is een CAB (Change Advisory Board) ingericht? Accorderen ze alle wijzigingen?	Voldoet
	21	Hoe worden wijzigingen naar productie gebracht? Wie mogen dit uitvoeren?	Voldoet
	22	Hoe worden spoedwijzigingen behandeld?	Voldoet
	23	Is er een OTAP omgeving en hoe wordt deze onderhouden?	Voldoet
Netwerk operations			
4. Systeembeheerder rechten worden gebruikt om autorisaties en functiescheidingsbeheersmaatregelen te omzeilen. 5. Wijzigingen in de gegevens opgeslagen in de onderliggende infrastructuur wordt onvoldoende gecontroleerd uitgevoerd. **Risicoscore: Midden**	24	Hoe is het systeem in het netwerk geplaatst? Welke zonering is toegepast?	Voldoet
	25	Hoe worden wijzigingen in de infrastructuur gecontroleerd toegepast (in relatie tot het systeem)	Voldoet
	26	Wordt er op beveiligingsincidenten gecontroleerd en zo ja, hoe wordt er mee om gegaan?	Voldoet
	27	Is fysieke toegangscontrole toegepast (indien nodig?)	Voldoet
	28	Wordt toegang tot het besturingssysteem periodiek gecontroleerd?	Voldoet
	29	Wordt de omgeving gecontroleerd op ongeautoriseerde toegang?	Voldoet
Software Ontwikkeling			
6. Onvoldoende beheerste softwareontwikkeling leidt tot niet betrouwbaar en niet veilige applicatie of systeem. **Risicoscore: Laag**	30	Wordt gewerkt volgens een standaard ontwikkel methodiek?	Voldoet
	31	Wordt versiebeheer toegepast?	Voldoet
	32	Is er een software ontwikkel repository?	Voldoet
	33	Wordt ontwikkeld met de OWASP top-10 als kader?	Voldoet
	34	Ondergaan producten een technische kwetsbaarhedentest voor oplevering?	Voldoet
End-user computing			
7. Gebruikers hebben (te) veel invloed op (grotere) datasets, waardoor	35	Zijn er processtappen waarbij een grote afhankelijkheid bestaat met 'losse' producten	. Voldoet

andere beheersmaatregelen worden omzeild. **Risicoscore: Laag**		zoals excel-sheets, access-databases of overige eenvoudig te manipuleren producten?	
	36	Zijn er procesafspraken gemaakt hoe met deze documenten wordt omgegaan?	
	37	Hoe zijn de autorisaties voor de locaties ingeregeld?	
Back-up, Recovery & Incidentmanagement			
8. Onvoldoende beheersmaatregelen leidt tot het niet garanderen van de continuïteit van de applicatie of de onderliggende infrastructuur. **Risicoscore: Hoog**	38	Is er een back-up procedure van toepassing op het systeem en welk schema wordt gehanteerd?	Voldoet
	39	Waar worden back-up media bewaard?	Voldoet
	40	Worden restore-tests uitgevoerd?	Voldoet
	41	Welke beveiliging is voor de back-up ingericht (encryptie / autorisaties)	Voldoet
	42	Is er monitoring ingericht op het systeem?	Voldoet
	43	Is er een incidentmanagement procedure, welke categorieën worden onderkent?	Voldoet
	44	Is er een continuïteitsplan opgesteld?	Voldoet
	45	Is er een uitwijklocatie beschikbaar (systeem en medewerkers) en wordt deze getest?	Voldoet
	46	Zijn er afspraken gemaakt met leveranciers inzake uitwijk indien het een SaaS applicatie betreft.	Voldoet
Specifieke applicatiecontroles			
9. Ontbrekende beheersing in de applicatie leidt tot onvoldoende waarborg van de beschikbaarheid, integriteit en vertrouwelijkheid van de verwerkte gegevens. **Risicoscore: Niet relevant**	47	Stamgegevens	Voldoet
	48	Invoer controles	
	49	Bestaanbaarheidscontroles	
	50	Verbandscontroles	
	51	Redelijkheidscontroles	
	52	Procuratieschema / mandatenregister	
	53	Functiescheidingcontrols	
	54	Logging	
Algemene verordening gegevens (AVG)			
Uit de review is gebleken dat de dienst geen gegevens verwerkt van tot natuurlijke personen te herleiden gegevens, anders dan de gebruikers c.q. beheerders van de systemen, evenals de contactpersonen vanuit de scholen of leveranciers. Vanwege de beperkte risico's is ervoor gekozen om AVG controls buiten scope te stellen. **Risicoscore: Laag**			
Leveranciersmanagement **Risicoscore: Hoog**	55		Voldoet
Servicemanagement **Risicoscore: Midden**	56		Voldoet
Configuratiebeheer **Risicoscore: Midden**	57		Voldoet

13 Bijlage: Alternatieven voor beveiligingsmaatregelen

Deze bijlage bevat de basis voor de vergelijking van de alternatieven voor beveiligingsmaatregelen. Hierbij zijn diverse aannames gedaan, die inzichtelijk zijn gemaakt in een tabel.

Er kunnen geen harde conclusies getrokken worden uit deze informatie, de inzichten zijn gebruikt voor een indicatief vergelijk tussen de alternatieven.

Alternatief 1: re-actief beheer

Dit alternatief gaat uit van een MKB / zakelijk - internet aansluiting per schoollocatie. Bij een dergelijke aansluiting wordt gebruik gemaakt van de standaard instellingen die door de aanbieder worden meegegeven. In de onderstaande tabel worden de beveiligingsmaatregelen die het NDC biedt vergeleken met dit alternatief.

Vergelijk beveiligingsmaatregelen	Alternatief 1	NDC
Firewall	Zeer beperkt mogelijk in dit alternatief	Afgestemd op FO
Anti-DDoS	Niet inbegrepen in dit alternatief	Afgestemd op FO
Web filtering	Zeer beperkt mogelijk in dit alternatief	Afgestemd op FO
Secure DNS	Zeer beperkt mogelijk in dit alternatief	Afgestemd op FO

Een schoollocatie heeft in deze vergelijking 400 leerlingen (aanname 1). De internetaansluiting wordt gebruikt door de leerlingen en leerkrachten om onderwijs gerelateerde taken uit te voeren waarbij kleine en grote incidenten optreden (aanname 2: dat er kleine en grotere verstoringen optreden, waarbij er tijd gevraagd wordt van een locatiebeheerder) die gemiddeld tussen de 1 tot 2 uur per week vragen (van zowel de leerkracht als de locatiebeheerder) om op te lossen (aanname 3). De kosten die deze vorm van beheer met zich meebrengt komt in totaal uit op ongeveer 32 euro per leerling per jaar en restrisico's met een kans op aanzienlijke schade.

Indicatieve rekensom 1: 42 weken * 3 uur (1,5 uur per week * 2 personen) = 126 uur per jaar voor incidenten en reactief beheer. De kosten voor een uur (alles inbegrepen) worden gesteld op 100,- euro per uur. De totale kosten voor de schoollocatie zijn 12600,- per jaar, per leerling per jaar is ongeveer 32 euro. Daarnaast is door het ontbreken van adequate beveiligingsmaatregelen eventuele schade (uitval en inbreuk) voor een schoollocatie die op deze alternatieve manier gebruik maakt van een internetaansluiting veel groter. In deze vergelijking zijn de bijkomende kosten hiervan niet meegenomen, omdat deze erg verschillend kunnen zijn en daarmee lastig kwantificeerbaar.

Alternatief 2: pro-actief beheer

Dit alternatief bestaat uit een MKB / zakelijk -internet aansluiting per schoollocatie aangevuld met een managed service aanbieder. Bij een dergelijke aansluiting wordt gebruik gemaakt van managed firewall service met aanvullende diensten, waarbij de geleverde kwaliteit en mate van beveiliging afhankelijk is van de ervaring en kennis die deze aanbieder heeft. Het schoolbestuur zal zelf mede moeten aangeven hoe onderdelen als firewall, filtering en secure DNS functioneel moeten worden ingesteld. In de onderstaande tabel worden de beveiligingsmaatregelen die het NDC biedt vergeleken met dit alternatief.

Vergelijk beveiligingsmaatregelen	Alternatief 2	NDC
Firewall	Eenmalig ingericht en mogelijk onderhouden[9]	Afgestemd op FO
Anti-DDoS	Mogelijk, tegen hoge kosten[10]	Afgestemd op FO
Web filtering	Eenmalig ingericht en onderhouden[3]	Afgestemd op FO
Secure DNS	Eenmalig ingericht en onderhouden[3]	Afgestemd op FO

Een schoollocatie heeft in deze vergelijking 400 leerlingen (aanname 1). De internetaansluiting wordt gebruikt door de leerlingen en leerkrachten om onderwijs gerelateerde taken uit te voeren waarbij kleine incidenten optreden (aanname 4: er treden minder grote verstoringen op, door proactief beheer, waarbij de managed service aanbieder de verstoringen verhelpt, in samenwerking met de leerkracht of locatiebeheerder) waarbij een contract gemiddeld 500,- euro per maand kost (aanname 5). Daarnaast zal de incidentafhandeling ook tijd kosten van een leerkracht of locatiebeheerder.

De kosten die deze vorm van beheer met zich meebrengt komt in totaal uit op 30,50 euro per leerling per jaar en restrisico's met een beperkte schade. De kosten per aangesloten leerling kunnen aanzienlijk worden verlaagd, als er sprake is van schoolbesturen met meerdere locaties en er gebruik gemaakt wordt van een centrale managed firewall voor de aansluiting op het internet.

Indicatieve rekensom: 42 weken * 1 uur (1 uur per week voor 1 persoon) = 42 uur per jaar voor incidenten. De kosten voor een uur (alles inbegrepen) worden gesteld op 100,- euro per uur. De eenmalige aanschaf van een firewall (aanname 6), is 6000,- euro, en de eenmalige inrichtingskosten voor de firewall zijn eveneens 6000,- euro. Wat neerkomt op 2400,- euro per jaar bij een afschrijvingstermijn van 5 jaar. De maandelijkse kosten voor de managed serviceprovider zijn gemiddeld 500,- euro per maand. Daarmee zijn de jaarkosten voor uren 4200,- plus 2400,- euro voor de firewall en 6000,- euro voor de serviceprovider. De jaarkosten zijn hiermee 12600,- euro, per leerling per jaar is dit ongeveer 32 euro.

Daarnaast is door bij dit alternatief van beveiligingsmaatregelen de kans op schade (uitval en inbreuk) voor een schoollocatie nog steeds aanwezig, maar kleiner dan in alternatief 1. In deze vergelijking zijn de bijkomende kosten hiervan niet meegenomen, omdat deze erg verschillend kunnen zijn en daarmee lastig kwantificeerbaar.

Tabel met aannames bij deze uitwerking.

#	Aanname
1	Op basis van cijfers Kennisnet, aantal aangesloten leerlingen gedeeld door het aantal dataverbinding, 1 dataverbinding per locatie. Uit cijfers van Kennisnet en DUO komt ongeveer eenzelfde gemiddelde naar voren van 400 – 600 leerlingen per locatie in het PO en VO. Er is echter ook een grote variatie in deze aantallen, waardoor deze gemiddelden beperkt toepasbaar zijn in dit onderzoek.
2	Er treden kleine en grotere verstoringen op, waarbij er tijd gevraagd wordt van een locatiebeheerder om deze te verhelpen, danwel de schade te beperken.

[9] Afhankelijk van het afgesloten beheercontract.
[10] Deze voorziening zal specifiek ingericht en ingeleerd moeten worden voor de school die dit afneemt.

3	Relatief eenvoudig uit te voeren reactief beheer, omdat het aan technische voorzieningen en kennis ontbreekt om pro-actieve maatregelen te nemen. Dit moet meer gezien worden als damage control (schade beperken), zeg maar dweilen met de kraan open.
4	Er treden minder grote verstoringen op, door proactief beheer, waarbij de managed service aanbieder de verstoringen verhelpt op basis van de afgesproken SLA, in samenwerking met de leerkracht of locatiebeheerder
5	Op basis van gemiddelde maandprijzen managed firewall en service contracten met kosten per aangesloten computer op basis van prijslijsten van dienstaanbieders op internet (prijspeil december 2023)
6	Gemiddelde prijs voor een Firewall voor een locatie met ongeveer 500 gebruikers, op basis van prijslijsten van aanbieders op internet (prijspeil december 2023)

Departementaal vertrouwelijk - Dep-V

14 Bijlage: Kosten en prognose NDC (bron: Kennisnet)

Kosten NDC		2018	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031	2032	2033
Beheer en onderhoud NDC			€ 80.614	€ 721.652	€ 1.001.399	€ 1.393.464	€ 1.207.986	€ 1.244.226	€ 1.281.553	€ 1.409.887	€ 1.589.632	€ 1.683.531	€ 1.734.037	€ 1.939.056	€ 2.154.816	€ 2.219.460	€ 2.286.044
Investeringen in NDC			€ 157.731	€ 3.091.223	€ 3.342	€ -	€ -	€ -	€ 4.020.669	€ 1.567.994	€ 1.232.704	€ -	€ -	€ 6.477.007	€ 1.817.734	€ 1.429.042	€ -
Beheer en onderhoud besturen en locaties			€	€ 83.567	€ 219.306	€ 488.778	€ 567.530	€ 958.779	€ 1.344.793	€ 2.153.250	€ 2.859.021	€ 3.610.694	€ 4.381.006	€ 5.160.179	€ 5.942.957	€ 6.582.997	€ 7.131.386
Investeringen aansluitingen NDC			€	€ 131.963	€ 227.671	€ 463.554	€ 190.865	€ 493.345	€ 550.520	€ 1.014.615	€ 1.041.468	€ 1.069.019	€ 1.068.612	€ 1.056.633	€ 1.043.262	€ 846.221	€ 668.403
Extern personeel	€	113.649	€	€ 434.311	€ 833.065	€ 587.449	€ 671.598	€ 691.746	€ 712.498	€ 733.873	€ 755.889	€ 778.566	€ 801.923	€ 825.980	€ 850.760	€ 876.283	€ 902.571
Intern personeel	€	94.584	€ 335.178	€ 661.536	€ 965.880	€ 899.796	€ 1.322.618	€ 1.485.581	€ 1.657.132	€ 1.837.639	€ 1.892.768	€ 1.949.551	€ 2.008.038	€ 2.068.279	€ 2.130.327	€ 2.194.237	€ 2.260.064
	€	**208.233**	€ **573.522**	€ **5.124.252**	€ **3.250.663**	€ **3.833.041**	€ **3.960.597**	€ **4.873.677**	€ **9.567.165**	€ **8.717.259**	€ **9.371.484**	€ **9.091.361**	€ **9.993.615**	€ **17.527.134**	€ **13.939.855**	€ **14.148.239**	€ **13.248.468**

PO	besturen		-	-	2	9	27	47	70	121	168	214	261	308	354	391	419
VO	besturen		-	4	9	19	31	50	70	92	114	137	159	175	188	197	204
Totaal	besturen			4	11	28	58	97	140	213	282	351	420	483	542	588	623
Nieuwe besturen				4	7	17	30	39	43	73	69	69	69	63	59	46	35
PO	verbindingen		-	-	37	159	232	372	532	906	1.258	1.603	1.955	2.307	2.651	2.928	3.138
VO	verbindingen		-	30	41	125	144	232	325	402	498	598	678	747	802	841	870
Totaal	verbindingen		-	30	78	284	376	604	857	1.308	1.756	2.201	2.633	3.054	3.453	3.769	4.008
PO	Nieuwe verbindingen			-	37	122	73	140	160	374	352	345	352	352	344	277	210
VO	Nieuwe verbindingen			30	11	84	19	88	93	77	96	100	80	69	55	39	29
Totaal	Nieuwe verbindingen			30	48	206	92	228	253	451	448	445	432	421	399	316	239
PO	leerlingen		-	-	1.733	40.035	58.482	105.151	150.369	273.174	379.408	483.411	589.645	695.879	799.659	883.128	946.512
VO	leerlingen		-	33.775	45.355	64.184	73.770	175.986	246.998	282.812	380.094	456.516	500.759	570.497	612.833	642.676	664.886
Totaal	leerlingen		-	33.775	47.088	104.219	132.252	281.137	397.366	555.986	759.503	939.926	1.090.404	1.266.376	1.412.491	1.525.805	1.611.397

Departementaal vertrouwelijk - Dep-V