VO RAAD Vereniging van scholen in het voortgezet onderwijs

PO RAAD

Kennisnet

Handreiking internetverbinding

Adviezen en achtergrondinformatie voor ict-coördinatoren en inkopers in het primair en voortgezet onderwijs

Laat ict werken **voor het onderwijs**

Inhoudsopgave

Inleiding

De internetverbinding is een belangrijke schakel in de ict-voorzieningen van je school. Deze verbinding is niet alleen nodig om op of rond de school internettoegang via wifi te kunnen bieden aan leerlingen, medewerkers en ouders. Een goed functionerende internetverbinding is ook essentieel voor het gebruik van moderne digitale leermiddelen of andere toepassingen in de cloud. Daarmee is het een belangrijke randvoorwaarde voor digitaal onderwijs geworden. Soms is het nodig de internetverbinding aan te passen of tegen het licht te houden. Dat kan zijn omdat je school meer gebruik gaat maken van digitale leermiddelen of van andere toepassingen in de cloud zoals bijvoorbeeld een officepakket als Office 365 of G Suite for Education. Of omdat je school meer mobiele devices als tablets, chromebooks of laptops gaat inzetten.

Zodra je je internetverbinding wilt uitbreiden, aanpassen of nieuw wilt inrichten, heb je kennis van de belangrijkste elementen en afwegingen nodig. Deze handreiking biedt die relevante achtergrond-informatie en bevat concrete adviezen die de ict-coördinator en de inkoper in po en vo helpen om een leverancier te selecteren en opdracht te verlenen. Deze handreiking gaat natuurlijk in op bandbreedte, beschikbaarheid en de kwaliteit van de verbinding. Maar ook belangrijke voorzieningen als de internetrouter, de firewall, vaste IP-adressen, DNS en beveiliging worden besproken.

Deze handreiking heeft alleen betrekking op de internetverbinding. Voor het interne - vaste en/of draadloze - netwerk is een *aparte handreiking* beschikbaar. Het is aan te raden bij aanpassing van de internetverbinding ook te controleren of het interne netwerk nog geschikt is om die goed te kunnen benutten.

Een toekomstvaste internetverbinding is van glasvezel

Op de korte termijn is voor sommige kleinere schoollocaties een internetverbinding gebaseerd op een consumentenproduct op basis van coaxkabel wellicht nog voldoende. Maar voor de meeste scholen is dat nu, en zeker binnen vijf jaar, onvoldoende. Vanwege de groei van het gebruik van digitale leermiddelen en cloudomgevingen is meer nodig. Zakelijke producten op basis van glasvezel bieden de gewenste capaciteit en betrouwbaarheid en kunnen de verbinding beter beveiligen en beschermen tegen verstoringen als DDoS-aanvallen. Dit alles is technisch niet onmogelijk met een coax-infrastructuur maar glasvezel is geschikter, zoals verderop in deze handreiking zal blijken. Glasvezel is ook een betere investering voor de langere termijn. In paragraaf *Wat en waar koop je in?* wordt ingegaan op de opties als er geen glasvezel aanwezig is bij je school.

Advies

Baseer indien mogelijk de internetverbinding op een glasvezeldienst van een zakelijke aanbieder.

1

Belangrijkste eigenschappen van een internet-verbinding

De meest in het oog springende eigenschap van een internetverbinding is de *bandbreedte*. Deze bandbreedte (ook wel *capaciteit* genoemd) wordt uitgedrukt in aantallen megabit per seconde (Mbps) en geeft de snelheid aan waarmee gegevens over de internetverbinding verzonden of ontvangen kunnen worden. Bandbreedte is echter niet de enige eigenschap die van belang is. Ook de *beschikbaarheid* (hoe vaak is de verbinding uit de lucht?) en de *kwaliteit van de verbinding* zijn belangrijk. Dit hoofdstuk gaat in op alle drie deze aspecten.

Bij het bepalen van de benodigde bandbreedte, beschikbaarheid en kwaliteit is het belangrijk dat je school verder kijkt dan vandaag. In de meeste gevallen zal het gebruik van internet en internettoepassingen (zoals digitale leermiddelen, cloudomgevingen en administratieve toepassingen) en het aantal devices niet gelijk blijven met de huidige situatie. Daarom is het belangrijk uit te gaan van de behoefte over drie tot vijf jaar. Omdat de ontwikkelingen in het gebruik van technologie in het onderwijs snel gaan, is de precieze behoefte niet altijd goed te voorspellen, dus flexibiliteit in de internetverbinding is tevens van belang; bijvoorbeeld het eenvoudig en stapsgewijs kunnen *opschalen* (uitbreiden van de bandbreedte).

Overigens moet bij het bepalen van de behoefte niet alleen gekeken worden naar de onderwijstoepassingen en devices, maar ook naar administratieve toepassingen, de ontwikkeling van leerlingaantallen en de behoefte om leerlingen, leraren en/of ouders buiten de lesuren of zelfs buiten schooltijd van internettoegang via wifi te voorzien.

Wees je ervan bewust dat meer bandbreedte, beschikbaarheid en kwaliteitsgaranties vaak ook leiden tot hogere kosten. Weeg in de afweging tussen prijs en kwaliteit ook de (kosten van) verloren (onderwijs-)tijd en frustratie van leraren en leerlingen mee en welke kwaliteit passend is voor de ambities die je school heeft met het gebruik van ict in het onderwijsproces.

Advies

- Ga bij het inrichten van je internetverbinding uit van de behoefte van je school over drie tot vijf jaar. Let daarbij niet alleen op bandbreedte maar ook de vereiste kwaliteit en beschikbaarheid.
- Neem daarin het gebruik van onderwijstoepassingen, administratieve toepassingen, aantallen devices, leerling-aantallen en de behoefte aan internettoegang via wifi mee.
- Zorg voor een flexibele internetverbinding, waarmee je eenvoudig en stapsgewijs kunt opschalen.

De uitgangspunten en adviezen uit dit hoofdstuk zijn mede gebaseerd op een marktconsultatie die Kennisnet uitvoerde in 2017 in het kader van de uitwerking van producten en diensten van de inkoop-coöperatie, aangevuld met een second opinion van Stratix, advies-bureau op het gebied van netwerkinfrastructuur.

Bandbreedte

Bij het bepalen van de benodigde bandbreedte (of capaciteit) is het belangrijk eerst een aantal specifieke aspecten van bandbreedte te doorgronden: symmetrie, gelijktijdig gebruik en overboeking. Deze worden hier daarom eerst behandeld.

Download- en uploadbandbreedte: symmetrie is toekomstvast

De beschikbare bandbreedte van de internetverbinding wordt gebruikt om gegevens te ontvangen *(download)* en gegevens te versturen *(upload)*. Traditioneel was in internetverbindingen vooral bandbreedte gereserveerd voor download en was er maar beperkte bandbreedte voor upload. Voor gewoon internetgebruik is dat vaak prima. Maar cloudtoepassingen als digitale leermiddelen of digitale toetsen vragen ook voldoende uploadbandbreedte. Daarom is een (meer) symmetrische verbinding nodig om soepel te kunnen werken. Sommige aanbieders leveren een internetverbinding met een upload-bandbreedte die tot een factor 10 kleiner is dan de down-load-bandbreedte en dat is onvoldoende. Een volledig symmetrische verbinding heeft net zoveel bandbreedte voor upload als voor down-load beschikbaar en is daardoor veel beter geschikt voor werken met digitale leermiddelen in de cloud. Symmetrische verbindingen vereisen typisch glasvezel als onderliggende technologie.

Advies

Zorg voor een volledig symmetrische internetverbinding.

Gegarandeerde bandbreedte en overboeking

De bandbreedte waarmee de aanbieder adverteert is in de praktijk niet altijd de daadwerkelijk beschikbare bandbreedte. Dit fenomeen heet *overboeking*[1]. Bij overboeking gaat de aanbieder er van uit dat binnen een groep klantaansluitingen niet alle klanten tegelijk de maximale bandbreedte van hun eigen aansluiting zullen benutten. De totale beschikbare bandbreedte voor die groep klanten is dus lager dan de som van de individuele bandbreedtes. Gangbare overboekingsverhoudingen zijn 1:4 en 1:10, waarbij de laatste betekent dat een tiende van geadverteerde bandbreedte gereserveerd wordt voor de klant. De geadverteerde bandbreedte staat je school dus niet altijd ter beschikking. Dit verklaart mede de soms grote prijsverschillen tussen producten (naast verschillen in bijvoorbeeld beschikbaarheid). Wanneer er geen sprake is van overboeking dan wordt dit ook wel aangeduid met 1:1.

Overboeking verschilt per type aansluiting:

- Aansluitingen met coaxkabel maken vrijwel altijd gebruik van een gedeelde kabel, die dus gedeeld wordt met andere aansluitingen. Daardoor zijn geen bandbreedtegaranties mogelijk.
- Bij zakelijke glasvezelverbindingen is er altijd exclusief gebruik van het medium. Daardoor is de overboeking vaak te kiezen. Daardoor kan je school garanties krijgen op de beschikbare capaciteit of juist voor overboeking kiezen als garanties minder belangrijk zijn en kosten bespaard moeten worden.
- FttH-aansluitingen (*fiber-to-the-home*, dit zijn glasvezelnetwerken die alle adressen in een gebied aansluiten) kennen veelal een (hoge) overboeking en bandbreedtegaranties zijn soms mogelijk.
- Bij ADSL en VDSL hangt naast overboeking de daadwerkelijk beschikbare capaciteit ook nog sterk af van de afstand tussen de schoollocatie en de centrale van de aanbieder.
- Bij draadloze verbindingen zoals 3G en 4G spelen naast overboeking ook de dekking en bereik (zowel binnen als buiten) een belangrijke rol bij de daadwerkelijk bruikbare capaciteit.

Alleen bij glasvezel kan dus een bandbreedtegarantie gegeven worden. Daarom is dat de aan te bevelen optie als internettoegang en de benodigde bandbreedte cruciaal zijn voor het onderwijs in jullie school.

Advies

- Controleer of de overboeking en bandbreedtegaranties van de internetverbinding aansluiten bij de behoefte van je school.
- Kies voor glasvezel zodra bandbreedtegarantie belangrijk is.

Bepalen van de benodigde capaciteit

Voldoende bandbreedte is een belangrijke voorwaarde om de investeringen in devices en digitale leermiddelen tot hun recht te laten komen. Beknibbelen op bandbreedte is dan ook zonde van die investeringen. Hoeveel bandbreedte jouw school nodig heeft is natuurlijk afhankelijk van hoeveel digitale leermiddelen en cloudtoepassingen

1 In strikt technische zin is er bij coaxkabel infrastructuur geen sprake van overboeking. Hierbij wordt het beschikbare frequentiespectrum dynamisch over abonnees verdeeld. Dat geeft voor de eindgebruiker toch grotendeels dezelfde uitkomst.

je school gebruikt en hoe vaak. Ook het algemeen internetgebruik vraagt bandbreedte. Dit gaat dan niet alleen over het gebruik door leerlingen, maar ook dat van leraren en staf op de locatie.

Aan de basis ligt een inschatting van de hoeveelheid capaciteit die een actieve leerling nodig heeft. Uit Kennisnet onderzoek blijkt dat dit op dit moment in het po gemiddeld 1 Mbps is en in het vo gemiddeld 2 Mbps:

- uitgaande van gegarandeerde bandbreedte (dus zonder overboeking)
- zowel up- als downstream
- dit is inclusief een marge voor het gebruik van leraren en staf en het klassikale internetgebruik via bijvoorbeeld smartboards
- dit is inclusief 25% marge om de internetverbinding niet boven de 75% te belasten (omdat dat leidt tot kwaliteitsverlies zoals *verderop* beschreven).

De benodigde capaciteit per actieve leerling zal de komende vijf jaar toenemen:

- wanneer je school in de nabije toekomst intensiever gebruik gaat maken van digitale leermiddelen in het curriculum en/of door migratie van toepassingen naar de cloud
- door autonome groei, omdat de bestaande leermiddelen en cloudtoepassingen rijkere functionaliteit krijgen (interactiever en/of multimedialer). Deze autonome groei was de afgelopen jaren gemiddeld genomen ongeveer 20% per jaar. Die lijn voortzettend zou door groei op groei na een periode van 5 jaar de benodigde capaciteit dus ongeveer 250% van de oorspronkelijke capaciteit zijn geworden (na 3 jaar is dat 175%).

Als je de totale benodigde capaciteit van de internetverbinding zou bepalen door het aantal leerlingen van je school te vermenigvuldigen met de bovenstaande 1 Mbps (po) of 2 Mbps (vo) dan kom je veel te hoog uit. Niet alle leerlingen zijn namelijk tegelijk actief. Dat wil zeggen: ze gebruiken niet allemaal op hetzelfde moment daadwerkelijk een device om leermiddelen of cloudtoepassingen via de internetverbinding te benaderen. Je zult voor de capaciteitsberekening uit moeten gaan van aantallen gelijktijdige gebruikers.

Belangrijk is het om je te beseffen dat gelijktijdig gebruik niet hetzelfde is als het aantal *aanwezige devices.* Typisch varieert het aantal aanwezige devices per leerling in het po nu van 1:5 tot 1:2 en is de verwachting dat dit de komende vijf jaar zal toenemen naar 1:1. In het vo wordt een groei verwacht van 1:2 à 1:1 nu naar 2:1 tot 3:1 over vijf jaar; meerdere aanwezige devices per leerling dus[2].

Het aantal *gelijktijdig actieve devices* kent een heel andere ontwikkeling. Gemiddeld genomen is op dit moment het gelijktijdig gebruik in het po ongeveer 1:3 (maximaal een op de drie leerlingen is redelijkerwijs tegelijk actief op een device). De verwachting is dat dit in het po de komende vijf jaar ongeveer met een factor 3 gaat toenemen (dus naar ongeveer 1:1). In het vo is het gelijktijdig gebruik nu ongeveer 1:2 en wordt een toename met een factor 2 verwacht (dus naar 1:1 over vijf jaar). Hoewel het vo toegroeit naar een situatie dat er meer devices dan leerlingen zijn, ligt het voor de hand dat die devices niet allemaal tegelijk gebruikt zullen worden (of in elk geval per device minder intensief).

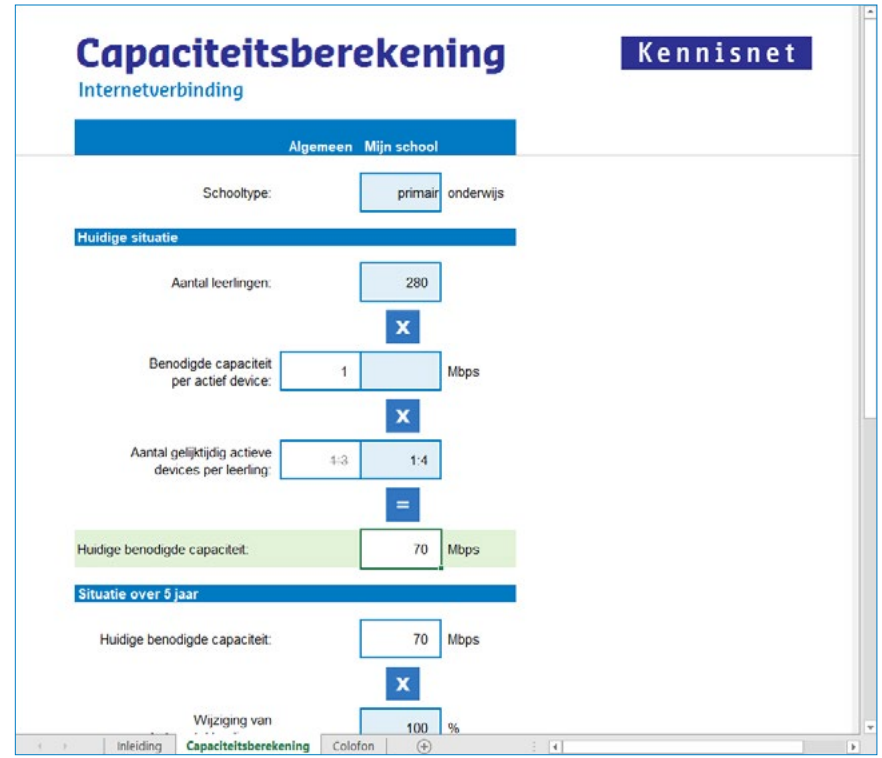
2 Het aantal aanwezige devices heeft geen directe impact op de benodigde capaciteit voor de internetverbinding. Het beïnvloedt wel het aantal benodigde IP-adressen in het interne netwerk.

Samengevat geeft dit de volgende verhoudingsgetallen:

	po		vo	
	nu	over 5 jaar	nu	over 5 jaar
aantal *aanwezige* devices per leerling	1:5 à 1:2	1:1	1:2 à 1:1	2:1 à 3:1
aantal *gelijktijdig actieve* devices per leerling	1:3	1:1	1:2	1:1

Deze verhoudingsgetallen zijn indicaties[3]. Mogelijk wijkt de situatie van je school hiervan af, afhankelijk van didactische en organisatorische keuzes. Wanneer je dit verhoudingsgetal zelf in wil schatten, ga dan uit van het *redelijkerwijs maximale* gelijktijdige gebruik. Als op jullie school regelmatig 1 device per 5 leerlingen (1:5) gelijktijdig wordt gebruikt, maar soms ook 1 device per 2 leerlingen (1:2), dan moet je van dit laatste uitgaan. Ook kan het helpen om de actuele gebruikte capaciteit in de praktijk vast te stellen en te bewaken. In *de paragraaf over capaciteitsbeheer* staat beschreven hoe dat moet.

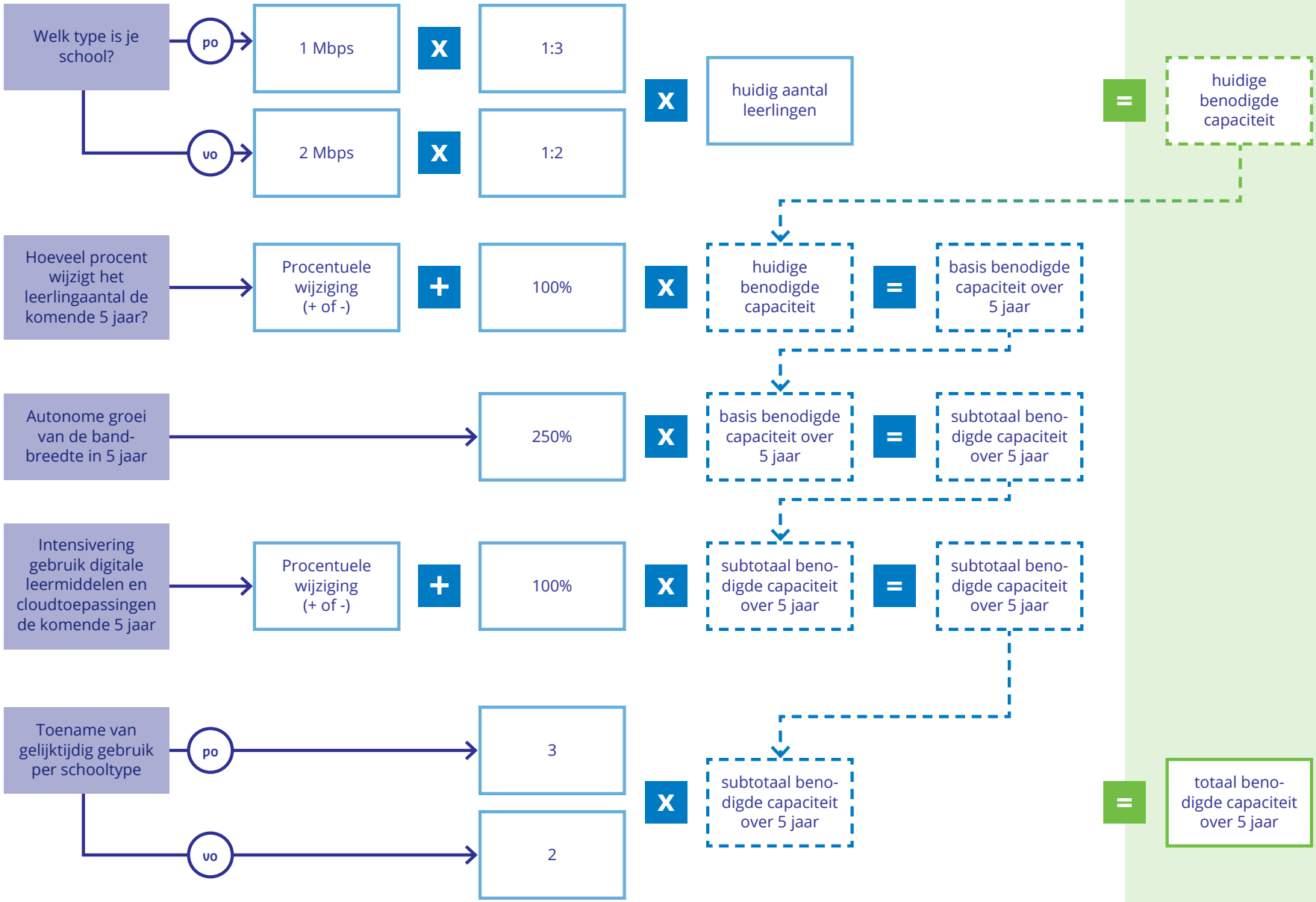
De bandbreedte die je school nu en over vijf jaar nodig heeft, kun je berekenen volgens het schema op de volgende pagina, op basis van bovengenoemde vuistregels en/of de vuistregels die voor jouw school bekend zijn. Om je te helpen die berekening te maken en om spelenderwijs de consequenties te kunnen doorgronden van alle aspecten is er een apart *spreadsheet* beschikbaar waarin de berekening is uitgewerkt.



Spreadsheet om de benodigde capaciteit te berekenen.

3 De gehanteerde verhoudingsgetallen zijn een combinatie van devices van de school en devices die leerlingen zelf meenemen. Dit geeft een zo reëel mogelijke inschatting van de benodigde capaciteit voor probleemloos gebruik van digitale leermiddelen en cloudtoepassingen, ongeacht op welk device deze gebruikt worden..

Rekenhulp voor de benodigde capaciteit van de internetverbinding
(nu en over vijf jaar)



Dat betekent bijvoorbeeld:

	aantal leerlingen	huidige benodigde gegarandeerde capaciteit van de internetaansluiting (indicatief)[1]	benodigde gegarandeerde capaciteit van de internetaansluiting over 5 jaar (indicatief)[1, 2]
gemiddelde po school	270	90 Mbps	675 Mbps
gemiddelde vo school	740	740 Mbps	3700 Mbps

[1] Dit is inclusief 25% marge om de kwaliteit van de verbinding te behouden en is zonder overboeking en zowel up- als downstream beschikbaar. De overboekingsfactor kan een grote invloed hebben op de benodigde capaciteit als die niet gegarandeerd is (zie *Gegarandeerde bandbreedte en overboeking*). Als de provider van de aansluiting voor de gemiddelde po school uit de tabel bijvoorbeeld een overboekingsfactor van 1:4 toepast, dan moet de huidige benodigde capaciteit zijn: 4x 90 Mbps = 360 Mbps.

[2] Bij gelijkblijvende leerlingaantallen, zonder uitbreiding van de inzet van digitale leermiddelen in het curriculum.

Advies

- Beknibbel niet op bandbreedte.
- Ga voor de huidige bandbreedte uit van 1 Mbps per leerling in het po en 2 Mbps per leerling in het vo.
- Houd voor de benodigde bandbreedte over vijf jaar rekening met de ontwikkeling van leerlingaantallen, de autonome groei, de uitbreiding van inzet van digitale leermiddelen en de toename van het gelijktijdig gebruik van devices.
- Ga uit van 1 *aanwezige* device per leerling in het po en 2 à 3 *aanwezige* devices per leerling in het vo over 5 jaar.
- Ga uit van 1 actief device per leerling in zowel het po als het vo over 5 jaar.

Capaciteitsbeheer: monitoren van het gebruik en de beschikbare capaciteit

Een overbelaste internetverbinding wordt snel langzamer. Dat geeft symptomen als een trage reactie van digitale leermiddelen of andere cloudtoepassingen, haperend beeld of geluid bij multimedia en het wegvallen van de verbinding bij *VoIP (Voice-over-IP* of IP-telefonie). Dit gebeurt typisch als meer dan 75% van de capaciteit van de verbinding wordt gebruikt, zoals *verderop* toegelicht.

Door regelmatig de daadwerkelijk beschikbare bandbreedte en het capaciteitsgebruik te meten (dit noemen we *capaciteitsbeheer*) kan je dit voorkomen. Doordat je het eerder signaleert als er in je school een grotere capaciteitsbehoefte ontstaat, heb je de tijd om maatregelen te nemen voordat er problemen ontstaan.

Capaciteitsbeheer kan doorlopend en geautomatiseerd worden gedaan met behulp van zogenoemde *monitoringtools*. Die kun je zelf inrichten (in of rond de router) of dit kun je door je it-dienstverlener of soms ook door de aanbieder van de internetverbinding laten doen. Een rapportage over het internetverkeer gedurende een schooldag en de ontwikkeling daarin per week of per maand is veelal voldoende.

Om incidenteel een indicatie te krijgen van de daadwerkelijk beschikbare bandbreedte op een bepaald moment (indien je school een overboekte verbinding heeft) kun je gebruik maken van een toepassing op internet, een zogenoemde *speedtest*. Zo'n speedtest zegt niets over het daadwerkelijke gebruik of over de kwaliteit van de verbinding (zie *Kwaliteitsaspecten van de verbinding*) maar enkel over de beschikbare bandbreedte.

Het meest betrouwbare resultaat van zo'n speedtest krijg je wanneer:

- er geen andere toepassingen zijn die de verbinding ook gebruiken, dus in ieder geval buiten schooltijd
- er zo min mogelijk beperkende schakels in het interne netwerk doorlopen worden, dus niet meten vanaf een laptop die via wifi met het vaste netwerk en internet verbonden is.

Advies

- Richt structureel capaciteitsbeheer in met monitoringtools om niet verrast te worden door een overbelaste internetverbinding.
- Controleer ook incidenteel de daadwerkelijk beschikbare bandbreedte via speedtests (indien je school een overboekte verbinding heeft).

Beschikbaarheid

Hoe belangrijker de toegang tot internet is voor de onderwijsprocessen en de administratieve processen op jullie school, hoe belangrijker het is dat die toegang ook gegarandeerd is. Dit stelt eisen aan de beschikbaarheid van de internetverbinding. Hoewel dit nu nog niet voor alle po- en vo-scholen al het geval is brengt de structurele inzet van digitale leermiddelen en grotere aantallen devices onvermijdelijk ook investeringen in beschikbaarheid met zich mee. Het wordt immers reëel om te streven naar een maximale beschikbaarheid (100%) tijdens reguliere schooluren. Dit is te realiseren door goede servicelevelafspraken met de internetprovider, waarin een beschikbaarheidsgarantie en maximale hersteltijd afgesproken is en een redundante of back-up-verbinding.

Advies

Zorg voor een internetverbinding met goede beschikbaarheidsgaranties door een back-up- of een redundante aansluiting, afhankelijk van het belang van internetgebruik in je school.

Servicelevelafspraken

Hoe belangrijker de beschikbaarheid van internet voor je school is, hoe belangrijker het is om garanties af te spreken in een zogeheten *service level overeenkomst* of *service level agreement*. Omdat uitval van de verbinding toch af en toe kan plaatsvinden, is het ook belangrijk om goede afspraken te maken over de hersteltijd.

Aanbieders hanteren in hun consumentenaanbod geen beschikbaarheidsgaranties. Ook aanbieders voor de kleinzakelijke markt zijn hiermee terughoudend. Onderstaande service levels zijn reëel in het zakelijke aanbod van internetproviders:

	servicelevelgarantie
service window	24x7
beschikbaarheid	99,8% gedurende service window
hersteltijd bij prioriteit 1 incidenten	12 uur (90% binnen 8 uur)
gepland onderhoud	tussen 22:00 en 6:00 uur op schooldagen of op niet-schooldagen

Advies

Maak over de beschikbaarheid van de internetverbinding concrete servicelevelafspraken met de internetprovider.

Redundantie of back-up-verbinding

De beschikbaarheid van de internetverbinding kan verstoord worden door calamiteiten zoals een kabelbreuk door graafwerkzaamheden. Dergelijke calamiteiten zijn op te vangen door:

- de enkelvoudige aansluiting te combineren met een (mobiele) verbinding die als back-up kan dienen in geval van calamiteiten. In verband met de kosten heeft een back-up-verbinding meestal een niet-volledige capaciteit. Daarom heeft de school beleid nodig welk internetverkeer in geval van calamiteiten prioriteit krijgt. Dit beleid kan in sommige gevallen mogelijk technisch afgedwongen worden met technieken als QoS en CoS of het blokkeren van netwerksegmenten. Deze technieken worden beschreven in de *Handreiking netwerk en wifi in de school*.
- een redundante internetverbinding door twee verschillende aansluitingen met dezelfde capaciteit (op twee verschillende plaatsen in het gebouw) te laten aanleggen.

Deze maatregelen lopen op in effect, maar ook in benodigde investering. Het kan zijn dat de internetaanbieder om een hoge beschikbaarheidsgarantie te bieden juist ook een van deze maatregelen voorschrijft. De eerder genoemde servicelevels zijn veelal zonder redundante verbindingen te garanderen door de internetprovider.

Advies

- Overweeg voor een extra hoge beschikbaarheid de inzet van een back-up internetverbinding of de aanleg van een redundante internetverbinding.
- Bepaal bij een back-up-verbinding het beleid voor internetgebruik tijdens calamiteiten (om de veelal lagere capaciteit optimaal te kunnen benutten) en implementeer indien mogelijk technische maatregelen om dit beleid af te dwingen.

Kwaliteitsaspecten van de verbinding

Naast bandbreedte en beschikbaarheid bepaalt ook de kwaliteit van de verbinding het effectief gebruik van met name multimedia via internet. Interactieve multimedia (zoals VoIP, Skype en FaceTime) stellen de hoogste eisen, maar ook niet-interactieve multimedia zoals animaties en filmpjes in digitale leermiddelen of digitale toetsen stellen hoge eisen. Hoe geschikt een verbinding is voor interactief en multimediaal gebruik, wordt bepaald door drie kwaliteitsaspecten: latency, jitter en packet loss.

Latency is de vertraging (uitgedrukt in milliseconden, ms) die optreedt tussen de toepassing in de cloud en de browser van de gebruiker. Een hoge latency (veel vertraging; typisch meer dan 150 ms) veroorzaakt toepassingen die traag reageren, zoals bijvoorbeeld een trage terugkoppeling van een leermiddel wanneer een leerling antwoord geeft bij een toets of oefening. Lage latency is van extra belang voor conferencing-toepassingen.

Jitter is de variatie in latency. Hoe groter de jitter, hoe meer kans dat beeld of geluid hapert of dat toepassingen (onvoorspelbaar) traag reageren.

Packet loss geeft aan hoe vaak een stukje informatie opnieuw verstuurd moet worden omdat het verloren ging. Enige packet loss is een normaal verschijnsel waar je vaak niets van merkt. Een packet loss van meer dan 1 procent is wel merkbaar bij interactieve multimediale communicatie: beeld of geluid hapert of de verbinding valt weg. Deze haperingen treden juist op bij een overbelaste internetverbinding (meer dan 75% van de capaciteit benut). Naast het inkopen van voldoende capaciteit helpt het ook om voor belangrijke multimediale toepassingen (zoals VoIP) bandbreedte te reserveren. Meer informatie daarover staat in de *Handreiking netwerk en wifi in de school*.

Voor een soepel gebruik van interactieve multimedia in digitale leermiddelen of toepassingen gelden de volgende kwaliteitseisen:

latency	jitter	packet loss
< 150 ms	< 20 ms	< 0,5 %

In de praktijk voldoen verbindingen via glasvezel, coaxkabel, DSL en 3G/4G veelal allemaal aan deze eisen. Echter, garanties hierop worden meestal alleen gegeven door zakelijke aanbieders. Glasvezel is dan vrijwel altijd noodzakelijk. Als deze kwaliteitseisen voor je school belangrijk zijn, neem ze dan op in de servicelevelafspraken.

Als de verbinding van je internetprovider aan deze eisen voldoet, is dat in theorie nog geen garantie dat de totale verbinding (van je school naar de aanbieder van het digitale lesmateriaal of de cloudtoepassing) ook aan deze eisen voldoet. Dat is namelijk mede afhankelijk van de kwaliteit van de overige schakels in het internet, waaronder de internetverbinding van de aanbieder van het digitale lesmateriaal of de cloudtoepassing. Maak met deze aanbieders daarom ook afspraken over kwaliteit en beschikbaarheid. Achterhaal ook welke (minimale) eisen deze aanbieders stellen aan de internetverbinding van een leerling om hun producten goed te kunnen benutten.

Advies

Bepaal of garanties op deze kwaliteitseisen belangrijk zijn voor je school. Zo ja, oriënteer je dan vooral op het aanbod in de (groot-)zakelijke markt en maak met de aanbieders van digitaal lesmateriaal of cloudtoepassingen ook afspraken over kwaliteit en beschikbaarheid.

2

Belangrijke voorzieningen voor een internet-verbinding

Router

Het netwerk van de school wordt met het internet verbonden door een router. De internetprovider levert en beheert deze router meestal, maar niet altijd. Het is belangrijk na te gaan welke aansluitmogelijkheid de internetprovider biedt en of dat extra investeringen noodzakelijk maakt in bestaande of aanvullende netwerkapparatuur van de school. Bij snelheden tot 500 Mbps is de aansluitmogelijkheid doorgaans kopergebaseerd zodat de router direct op het schoolnetwerk aangesloten kan worden met CAT6-bekabeling en een RJ-45 stekker. Vanaf 1 Gbps is de aansluitmogelijkheid steeds vaker optisch in de vorm van een SFP *(small form-factor pluggable)*; dit biedt de grootste betrouwbaarheid. De router die je zelf aanschaft (of laat inrichten en beheren door de beheerder van het interne schoolnetwerk) moet in de juiste aansluitmogelijkheid (kunnen) voorzien.

Een RJ-45 aansluiting in een router

Daarnaast kunt u ervoor kiezen de router een aantal belangrijke functies te laten vervullen op het schoolnetwerk, zoals het uitdelen van IP-adressen aan devices. Bij grotere netwerken is het gebruikelijk dat dit niet door de internetrouter maar door netwerkswitches gedaan wordt.

Advies

Als de internetprovider geen router levert, controleer dan of de aansluitmogelijkheid van de bestaande of aan te schaffen router overeenkomt met wat de internetprovider vereist.

Sommige router-apparaten, veelal meegeleverd bij consumenten-verbindingen, kunnen ook werken als wifi-toegangspunt. De capaciteit, dekking en kwaliteit van dergelijke wifi-functionaliteit is niet geschikt voor gebruik in een school en verhoogt bovendien de kans op verstoringen en beveiligingsincidenten op de internetverbinding. Daarom moet deze wifi-functionaliteit uitgeschakeld worden. Wat er nodig is voor een betrouwbare wifi-voorziening voor je school, is terug te vinden in de *Handreiking Netwerk en wifi in de school.*

Advies

Schakel eventuele wifi-functionaliteit op de internetmodem/router uit.

Beheer van de router

Om de beschikbaarheid van de internetverbinding te kunnen (blijven) garanderen, moet de router beheerd worden. Dit omvat installatie-, onderhouds- en configuratiewerkzaamheden en zo nodig vervanging. Proactieve monitoring is ook van belang en houdt in dat de aanbieder storingen zelf opmerkt en herstelt. Dit beheer is onderdeel van het aanbod van de internetprovider, of je doet het zelf of laat het over aan de beheerder van het schoolnetwerk. De router kan ook een rol spelen bij rapportages voor *capaciteitsbeheer*.

Advies

Zorg voor beheer en proactieve monitoring van de router, ofwel door de internetprovider, door de beheerder van het schoolnetwerk, of doe het zelf.

Vaste IP-adressen

Het is aan te bevelen om geen toepassingen te gebruiken die servers in je school vergen (zie *Toepassingen in de school van buiten benaderen*). Mocht er toch sprake zijn van toepassingen op servers in je school die via het internet benaderbaar moeten zijn, dan kan je deze benaderbaar maken met behulp van vaste IP-adressen. Zakelijke aanbieders bieden vrijwel altijd een of meer vaste IP-adressen. In het consumentenaanbod ontbreekt dit vrijwel altijd. Tegen vergoeding verstrekken zakelijke aanbieders veelal extra vaste IP-adressen. Om deze toepassingen makkelijker te kunnen benaderen is het mogelijk

hiervoor een domeinnaam aan te vragen (zie *Domeinnaamregistratie en DNS*). Servers in de school die van buiten zijn te benaderen, kunnen een groot veiligheidsrisico opleveren, waarvoor maatregelen genomen moeten worden (zie *Demilitarized zone*).

Als de servers in de school beveiligingscertificaten gebruiken, dan moeten deze bij wijziging van het vaste IP-adres worden vervangen.

Advies

Indien servers in je school echt noodzakelijk zijn, inventariseer hoeveel vaste IP-adressen nodig zijn en controleer of deze geboden worden in het aanbod van de leverancier.

Domeinnaamregistratie en DNS

Als je school een website heeft, een cloudtoepassing gebruikt die onder een eigen webadres benaderbaar moet zijn of diensten op servers in de school heeft, die ook vanuit internet bereikbaar moeten zijn, dan kunnen deze benaderbaar gemaakt worden met een eigen domeinnaam (bijvoorbeeld: https://leeromgeving.onzeschool.nl). Naast gebruiksgemak heeft dit ook het voordeel dat de toepassing via de domeinnaam vindbaar blijft als deze verhuist (en daardoor een ander IP-adres krijgt). Dit geldt ook voor eventuele servers en toepassingen op de schoollocatie.

De aanvraag (registratie) van een dergelijke naam wordt vaak door de internetprovider verzorgd of kan anders via een zogeheten *registrar* worden gedaan. De school blijft eigenaar van deze naam en bij verandering van internetprovider kan deze naam meeverhuisd worden. Door de verhuizing door te geven in de *Domain Name Service* (DNS) blijft de domeinnaam naar het actuele IP-adres verwijzen. Browsers gebruiken deze DNS om het IP-adres van een toepassing te achterhalen.

Advies

Overweeg om toepassingen in de cloud en/of op servers in de school benaderbaar te maken via een eigen domeinnaam vanwege gebruiksgemak en continuïteit.

3 Beveiliging van de internet-verbinding

Firewall

Een *firewall* is een essentieel onderdeel van de internetbeveiliging. Het filtert het verkeer tussen het internet en het schoolnetwerk om ongeautoriseerde toegang tot het schoolnetwerk vanaf het internet te belemmeren en om onwenselijk verkeer vanaf het schoolnetwerk naar internet tegen te gaan.

Verkeer blokkeren of toestaan

Een firewall bevat instellingen die bepalen welk soort internetverkeer is toegestaan. In de meest basale vorm werkt dit met *port blocking*: een instelling die bepaalt welk soort internetverkeer is toegestaan, zoals bijvoorbeeld het verkeer tussen een website en een webbrowser.

Een zogenoemde *next generation* firewall gaat verder. Deze kan per toepassing en/of gebruiker(sgroep) het verkeer blokkeren of een lagere prioriteit geven. Denk dan aan het blokkeren van Netflix, torrents en de Tor-browser of het toekennen van een lagere prioriteit aan Snapchat. Deze regels kunnen zelfs verschillen voor groepen leerlingen en leraren, als de firewall gekoppeld is met de directory service van je school (zoals Windows Active Directory of LDAP).

Door zorgvuldig het beleid voor internetverkeer te kiezen beveilig je het interne netwerk niet alleen tegen ongewenst verkeer van buitenaf, maar ook tegen bewust en onbewust schadelijk verkeer van binnenuit en de aansprakelijkheid daarvoor.

Inbreuken voorkomen

Een *intrusion prevention system (IPS)* gaat nog wat verder dan het blokkeren van ongeautoriseerde toegang. Zo'n systeem bewaakt ook

of geautoriseerd internetverkeer dat niet kwaadwillend is. Een next generation firewall met IPS-functionaliteit zoekt naar patronen in het netwerkverkeer die wijzen op een computervirus, malware of andere ongewenste activiteiten. Als zulke patronen zich voordoen, dan blokkeert de firewall dit specifieke (of alle) netwerkverkeer. Omdat steeds nieuwe malafide patronen ontdekt worden, moet de IPS-functionaliteit een abonnement hebben op automatische updates.

Demilitarized zone (DMZ)

Het is aan te bevelen om geen toepassingen te gebruiken die servers in je school vergen (zie *Toepassingen in de school van buiten benaderen*). Mocht er toch sprake zijn van servers in je school die via het internet benaderbaar moeten zijn, dan kan in de firewall een zogeheten *demilitarized zone (DMZ)* worden ingericht. Dit zorgt ervoor dat enkel die servers van buitenaf te benaderen zijn, en niet het hele schoolnetwerk. Hiervoor zijn *vaste IP-adressen* nodig.

Beheer

Het inrichten en beheren van een firewall is specialistisch werk, zeker bij een *next generation* firewall. Doe dit alleen zelf wanneer de school hier specifieke kennis van heeft en laat het anders over aan de beheerder van het schoolnetwerk of de internetprovider (indien deze dat biedt).

Advies

- Richt een firewall in tussen het interne schoolnetwerk en het internet.
- Bepaal het beleid voor toegestaan internetverkeer.
- Overweeg het gebruik van een firewall met IPS.
- Laat de firewall inrichten en beheren door een specialist.

Bescherming tegen DDoS-aanvallen

Een *DDoS-aanval (Distributed Denial of Service aanval)* is een gecoördineerde aanval op een website, server of ander systeem vanaf zeer veel verschillende locaties op het internet. Doordat de aanval van zoveel verschillende kanten komt, is het niet mogelijk om in het schoolnetwerk technische tegenmaatregelen te nemen. Dat kan de internetprovider in zijn netwerk wel. Het is belangrijk om een DDoS-protocol op te stellen met de aanbieder, waarin staat wie welke taken uitvoert indien zich een DDoS-aanval voordoet en waar de aanval gemeld moet worden (bijvoorbeeld bij de ict-dienstverlener, internetprovider, de politie en/of het Nationaal Cyber Security Center).

DDoS-aanvallen zijn een reële bedreiging, juist vanuit leerlingen: zij kunnen eenvoudigweg voor enkele euro's een zo'n aanval bestellen op het internet om bijvoorbeeld een digitale toets te frustreren. Doelwit van de aanval kan dan de school of de toetsleverancier zijn. Dit speelt al in het vo en binnen enkele jaren zal dit ook in het po een reële bedreiging vormen met de toename van zelfstandig ict-gebruik door leerlingen.

Advies

- Richt nu in overleg met de internetprovider maatregelen in tegen DDoS-aanvallen als je school een vo-school betreft. Overweeg dit te gaan doen als je school een po-school is.
- Stel een DDoS-protocol op in overleg met de aanbieder van de DDoS-bescherming.

Antivirus

Om de systemen op je schoolnetwerk te beschermen tegen virussen en andere malware, is antivirussoftware nodig op de devices. Deze software moet dagelijks bijgewerkt worden om up-to-date te blijven. Een next generation firewall met IPS-functionaliteit (zie *aldaar*) helpt voorkomen dat virussen en malware worden gedownload, maar maakt antivirusbescherming op devices niet overbodig.

Het beheer van zo'n gecoördineerde antivirusinstallatie op de systemen in een netwerk is specialistisch werk voor je netwerkbeheerder. Een aantal internetproviders biedt deze diensten ook aan.

Advies

- Installeer antivirussoftware op alle systemen in het netwerk.
- Beheer deze software zelf of laat dit doen door de netwerkbeheerder of internetprovider.

URL- en contentfiltering

Met URL-filtering bepaal je welke websites wel en niet mogen worden bezocht door specifieke groepen gebruikers. Dit kunnen websites met ongewenste inhoud zijn, maar ook malafide websites die systemen kunnen besmetten met malware en computervirussen. Contentfiltering zorgt ervoor dat de gebruikers geen ongewenste inhoud kunnen benaderen of schadelijke bestanden (bijvoorbeeld met computervirussen) kunnen downloaden. Dit begint met het vaststellen van beleid en kan geïmplementeerd worden met gedragsafspraken of via een dienst voor URL-/contentfiltering. Zo'n dienst moet up-to-date worden gehouden via een abonnement en kan als optie op een next generation firewall ingekocht worden.

Advies

- Stel beleid op welke websites en content gebruikers mogen raadplegen en welke niet en wat de gevolgen zijn in geval dat dit alsnog geprobeerd wordt.
- Overweeg om een dienst voor URL- en contentfiltering te gebruiken om dit beleid te implementeren of maak gedragsafspraken binnen de school.

Mailfiltering

Met mailfiltering kunnen e-mails die phishingmails of spam zijn of die een computervirus of andere malware bevatten van het interne netwerk geweerd worden. Mailfilteringfunctionaliteit moet up-to-date blijven via een abonnement. Deze functionaliteit kan als beheerde dienst uit de cloud worden afgenomen van een marktpartij, bijvoorbeeld in combinatie met Microsoft Office 365 of Google Mail.

Advies

Richt mailfiltering in via een beheerde clouddienst.

4 Specifieke overwegingen

Toepassingen in de school van buiten benaderen

Als je school (een deel van) het digitaal leermateriaal en toepassingen als e-mail en bestandsopslag niet in de cloud heeft, maar op servers in de school, dan zijn deze niet zonder meer door thuiswerkende medewerkers en leerlingen te benaderen. Om te beginnen zijn toepassingen op servers in de school vanwege de hogere kosten voor beheer en beveiliging en de grotere risico's op storingen onwenselijk. Migreren naar de cloud of hosting in een extern datacenter is de beste oplossing. De toepassingen zijn daarmee meteen ook buiten school te benaderen.

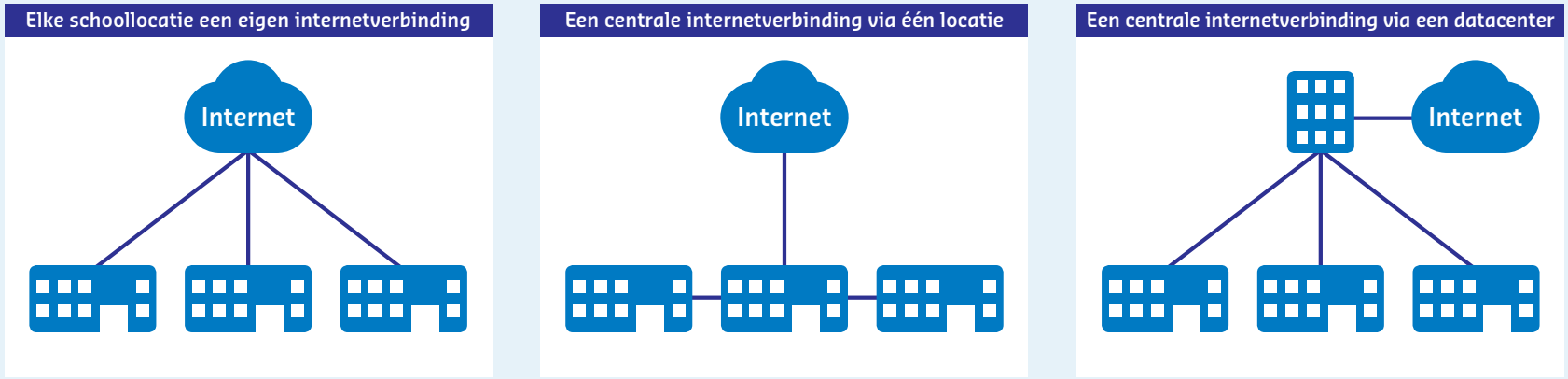
Mocht migratie naar de cloud of datacenter nog niet kunnen, dan zijn servers in de school veilig benaderbaar te maken via het internet zonder de rest van het interne netwerk openbaar te maken. Hiervoor zijn *vaste IP-adressen* en een *DMZ* nodig.

Advies

- Overweeg om toepassingen die vanaf buiten de school te gebruiken moeten zijn te migreren naar de cloud of naar een extern datacenter.
- Indien dit echt niet mogelijk is, zorg dan voor vaste IP-adressen en richt een DMZ in.

Een internetverbinding per school of per schoollocatie?

Als je school uit meerdere schoollocaties bestaat, doemt de vraag op of je op elke schoollocatie een eigen internetverbinding laat



aanleggen, of dat je dit centraal regelt via één van de locaties of via een datacenter. Het inrichten en beheren van de internetverbinding, firewalls en voorzieningen tegen DDoS-aanvallen is kostbaar en vergt specialistische expertise. Het centraliseren hiervan bespaart kosten en maakt de ict op de schoollocaties eenvoudiger. Je school kan toe met minder beheerders. Dit effect speelt natuurlijk ook bij het centraliseren van (administratieve) toepassingen en leermiddelen. Hiervoor geldt dat migreren naar de cloud de beheerkosten nog veel verder kan terugbrengen.

Bij een centrale internetverbinding geldt dat de capaciteits- en kwaliteitseisen natuurlijk moeten aansluiten bij wat alle achterliggende schoollocaties gezamenlijk nodig hebben. Omdat de impact van een storing in dit geval nog groter is (immers, alle locaties worden getroffen in plaats van slechts één) zijn de garanties die de leverancier geeft nog belangrijker dan bij individuele internetverbindingen per locatie. Ook speelt bij centralisatie de kwaliteit van de netwerkverbinding tussen de schoollocaties en de centrale locatie of het datacenter een belangrijke rol. Over het algemeen voldoen deze aan de kwaliteitsaspecten (zie voor meer informatie over deze verbindingen de *Handreiking Netwerk en wifi in de school*). Je kunt overwegen monitoring in te (laten) richten om de kwaliteit van deze verbindingen te bewaken.

Advies

- Overweeg om de internetverbinding via één centrale locatie of datacenter te laten lopen.
- Overweeg om monitoring in te (laten) richten voor de netwerkverbindingen naar de centrale locatie of datacenter.

Wat en waar koop je in?

Zoals gesteld bieden zakelijke producten op basis van glasvezel de gewenste capaciteit en betrouwbaarheid en kunnen deze de verbinding beter beveiligen en beschermen tegen verstoringen als DDoS-aanvallen. Glasvezel als onderliggende technologie is de beste investering voor de langere termijn.

Ook al heeft glasvezel de voorkeur, bij de helft van de schoollocaties ligt dit nog niet voor de deur. Geldt dit ook voor jouw school, inventariseer dan of er lokale glasvezelinitiatieven in de regio actief zijn en onderzoek hun aanbod. Eentiende van de schoollocaties heeft daarnaast ook geen toegang tot coaxkabel. Hoort je school hierbij, dan is de subsidieregeling van het Ministerie van OCW mogelijk interessant. Je school kan via die regeling een aanzienlijk deel van het bedrag voor aanleg van glasvezel vergoed krijgen.

Als je school besluit zelf te investeren in het aanleggen van een kabel voor de internetverbinding, dan is glasvezel de meest toekomstvaste investering. De investering wordt over een periode van tien tot vijftien jaar afgeschreven. Ga voor het bepalen van de benodigde capaciteit en/of schaalbaarheid dan ook uit van de behoefte van je school gedurende diezelfde periode.

Als een glasvezelaansluiting in het geheel nog niet mogelijk is, zijn er tussentijdse mogelijkheden om de internetverbinding te verbeteren. Die staan beschreven in een aparte publicatie.

Een groeiende groep po- en vo-besturen werkt samen in een inkoopcoöperatie aan gezamenlijke inkoop van ict-voorzieningen, waaronder ook een beveiligde, symmetrische (waar mogelijk glasvezel gebaseerde) internetverbinding met de vereiste hoge kwaliteitsgaranties. De coöperatie maakt ict-voorzieningen als nutsvoorziening beschikbaar voor scholen. Door hun krachten te bundelen kunnen scholen een goed aanbod uit de markt krijgen. De coöperatie gaat daarbij uit van het 'connectivity-as-a-service' concept. Dat betekent dat een school geen apparatuur aanschaft, onderhoudt, beheert of vervangt, maar een abonnement op connectiviteit heeft. Dit omvat onder meer de internetverbinding, firewall en voorzieningen tegen DDoS-aanvallen. Het gezamenlijk ingekochte aanbod is beschikbaar in de loop van 2018. Meer informatie is te vinden op *www.ictcooperatie.nl.*

Advies

Indien glasvezelaanbod beschikbaar is bij de school:

- Baseer de internetverbinding op een glasvezeldienst van een zakelijke aanbieder.

Indien er nog geen glasvezelkabel bij de school ligt:

- Onderzoek de mogelijkheid aan te sluiten bij een lokaal glasvezelinitiatief.

Indien er geen glasvezel- en geen coaxkabel bij de school ligt:

- Onderzoek de mogelijkheden van de subsidieregeling van OCW.
- Indien je school zelf een kabel moet laten aanleggen, ga dan uit van glasvezel en ga bij het bepalen van de capaciteit en schaalbaarheid van de glasvezel uit van de behoefte gedurende tien tot vijftien jaar.

Informeer je over de mogelijkheden die aansluiting bij de inkoopcooperatie zou kunnen bieden.

Begrippenlijst

De volgende technische begrippen komen in in de tekst voor, of zou de leverancier kunnen gebruiken:

ADSL	Afkorting van Asymetrical Digital Subscriber Line, een breedband verbinding via de telefoonlijn. ADSL is minder snel dan VDSL.
CAT6	Typeaanduiding voor hoge kwaliteit netwerkbekabeling op basis van koper.
DDoS-aanval	Afkorting van Distributed Denial of Service aanval, een aanval op een computersysteem met als doel de werking ervan te frustreren.
DMZ	Afkorting van demilitarized zone, een deel van het netwerk dat te benaderen is vanaf computers van buiten dat netwerk, zonder het hele schoolnetwerk toegankelijk te maken.
DNS	Afkorting van Domain Name Service, een mechanisme waarmee computers en andere apparaten in een netwerk op basis van hun naam gevonden kunnen worden in plaats van het IP-adres.
DSL	Afkorting van Digital Subscriber Line, een breedbandverbinding via de telefoonlijn. Zie ook ADSL en VDSL.
firewall	Apparaat dat het netwerkverkeer tussen het eigen netwerk en het internet bewaakt en filtert ter beveiliging.
FttH	Afkorting van Fiber-to-the-home. Glasvezelnetwerk waarmee alle adressen in een gebied aangesloten worden.
Gbps	Afkorting van Gigabit per seconde, gelijk aan 1000 Mbit ofwel 1 miljard bits per seconde. Eenheid van bandbreedte van netwerkverkeer.
IP	Afkorting van Internet Protocol, een standaard waarmee computers en andere apparaten informatie met elkaar kunnen uitwisselen.
IP-adres	Het unieke adres waarmee computers en andere apparaten in een IP-netwerk gevonden kunnen worden.
IP-telefonie	Modern digitaal telefoonsysteem dat werkt via het computernetwerk / het internet. Zie ook VoIP.
IPS	Afkorting van intrusion prevention system, een functie - veelal in een firewall - die bewaakt of internetverkeer niet kwaadwillend is.
Mbps	Afkorting van Megabit per seconde, ofwel 1 miljoen bits per seconde. Eenheid van bandbreedte van netwerkverkeer.
port blocking	Functie in een firewall om te bepalen welk soort internetverkeer is toegestaan, zoals bijvoorbeeld het verkeer tussen een website en een webbrowser.
RJ-45	Typeaanduiding voor een stekker voor netwerkbekabeling op basis van koper.
SFP	Afkorting van small form-factor pluggable, de glasvezelaansluiting die meestal bij snellere verbindingen door de internetprovider geboden wordt om de router op aan te sluiten.
UTP	Typeaanduiding voor netwerkbekabeling op basis van koper.
VDSL	Afkorting van Very High Bitrate Digital Subscriber Line, een breedbandverbinding via de telefoonlijn. VDSL is sneller dan ADSL.
VoIP	Voice-over-IP. Technologie waarmee telefonie over het computernetwerk / over het internet kan plaatsvinden. Zie ook IP-telefonie.
wifi	Afkorting van Wireless Fidelity, een verwijzing naar de draadloze netwerkverbinding.

Colofon

Handreiking internetverbinding

Deze brochure is ontwikkeld door Kennisnet, in het kader van het Doorbraakproject Onderwijs & ICT. Het Doorbraakproject is een gezamenlijk initiatief van de PO-Raad, VO-raad en de ministeries van Onderwijs, Cultuur en Wetenschap en Economische Zaken.

Datum van uitgave
november 2017

Auteurs
Michael van Wetering, Petra Nederkoorn, Paul Dam

Redactie
Lisa van Ginneken

Uitvoering
Vormgeving: *gloed*communicatie, Nijmegen
Fotografie: iStockphoto

Over Kennisnet
Elke leerling verdient eigentijds, veilig en persoonlijk onderwijs. Daarom ondersteunt Kennisnet scholen met ict. We zorgen voor een landelijke ict-basisinfrastructuur, adviseren de sectorraden en delen onze kennis met het primair onderwijs (po), het voortgezet onderwijs (vo) en het middelbaar beroepsonderwijs (mbo). Kennisnet wordt gefinancierd door het ministerie van Onderwijs, Cultuur en Wetenschap (OCW).

kennisnet.nl

Kennisnet
Paletsingel 32
2718 NT Zoetermeer

T 0800 321 22 33
E support@kennisnet.nl
I kennisnet.nl

Postbus 778
2700 AT Zoetermeer