

OPEN GRENZEN



nieuwe uitdagingen voor de ICT-dienstverlening

Grenzen vervagen, zoals de grens tussen de werkomgeving en thuis.

De wereld was overzichtelijk. De instelling bood voorzieningen aan die in de samenleving slechts beperkt beschikbaar waren. En de grens tussen binnen en buiten was helder en meestal waren beide goed van elkaar afgesloten.

Open grenzen, vrij verkeer van personen en goederen. We zijn er binnen Europa al aan gewend geraakt. De drijfveer was primair van economische aard. Maar het was ook een afspiegeling van onze kleiner wordende wereld.

In ICT-land voltrekt zich een vergelijkbaar proces. De informatiewereld wordt kleiner en beperkingen worden niet geaccepteerd, zeker niet door studenten. Dat geeft nieuwe problemen maar bovenal ook nieuwe mogelijkheden.

Een aantal aspecten van deze ontwikkeling wordt in deze bijdrage belicht. Aansluitend worden enkele aanbevelingen gedaan die samenhangen met de beschreven trends.

GRENZEN VERVAGEN

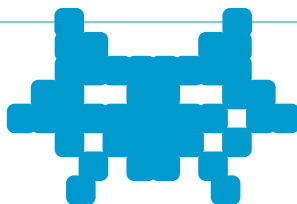
Enige decennia geleden, in de begintijd van pc en netwerk, zag de ICT-wereld er voor een universiteit of hogeschool overzichtelijk uit. De instelling stelde faciliteiten beschikbaar in de vorm van pc-werkplekken met daarop een aantal applicaties en – soms met tegenzin – internet toegang. Een deel van de studenten had weliswaar een computer thuis maar dat betekende hoogstens dat met een floppy disk bestanden over en weer werden meegenomen. Dit laatste werd overigens gezien als een aanzienlijk beveiligingsrisico en werd daarom zeker niet overal zonder meer toegestaan. De wereld was overzichtelijk. De instelling bood voorzieningen aan die in de samenleving slechts beperkt beschikbaar waren. En de grens tussen binnen en buiten was helder en meestal waren beide goed van elkaar afgesloten.

Open grenzen, vrij verkeer van personen en goederen. We zijn er binnen Europa al aan gewend geraakt. De drijfveer was primair van economische aard. Maar het was ook een afspiegeling van onze kleiner wordende wereld. In ICT-land voltrekt zich een vergelijkbaar proces. De informatiewereld wordt kleiner en beperkingen worden niet geaccepteerd, zeker niet door studenten. Dat zorgt voor nieuwe uitdagingen en bovenal nieuwe mogelijkheden. In zijn bijdrage belicht Hendriks een aantal aspecten hiervan en geeft enkele aanbevelingen die samenhangen met de beschreven trends.



CHRIS HENDRIKS
Consultant ICT

Hoe houd je ongewenste elementen (personen, email, applicaties) buiten de deur als de grenzen door samenwerking steeds opener worden?



Maar de wereld veranderde. Het pc-bezit werd normaal evenals de toegang tot internet. In de laatste jaren verschoof daarbij het accent van traditionele vormen van internetgebruik – email en het raadplegen van informatie – naar (real-time) communicatie en actief aanwezig zijn op het web. In samenhang met het toenemende aantal apparaten en gebruiksvoorwerpen met internettoegang is de digitale wereld een onderdeel van de persoonlijke omgeving geworden. Deze verandering loopt dwars door alle aspecten van het leven heen. Grenzen vervagen, zoals de grens tussen de werk-omgeving en thuis. Maar niet alleen vervaagt de grens vanuit het gebruikersperspectief. Ook vanuit het perspectief van de organisatie is de afbakening minder eenduidig. Samenwerkingsverbanden worden aangegaan in verschillende vormen, variërend van een gezamenlijk project of een opleiding die door twee of meer instellingen wordt opgezet, tot verschillende niveaus van bestuurlijk samengaan. Een derde oorzaak van het vervagen van (ICT)grenzen is het gegeven dat ICT-afdelingen vanuit een bedrijfseconomisch perspectief in toenemende mate zullen kiezen voor het inkopen van diensten bij derden. Hierbij kan de leverancier een commerciële partij zijn, een vraagbundelingsorganisatie zoals SURFnet of een andere (ho) organisatie.

Grenzen vervagen, zoals de grens tussen de werkomgeving en thuis. Samenwerkingsverbanden worden aangegaan in verschillende vormen, variërend van een gezamenlijk project of een opleiding die door twee of meer instellingen wordt opgezet, tot verschillende niveaus van bestuurlijk samengaan.

Stel dat we het wegvallen van de grens tussen studie en privé, tussen de campus en thuis, als uitgangspunt nemen, wat betekent dit dan voor de universiteit of hogeschool die ICT-voorzieningen aanbiedt? En, in combinatie hiermee, wat zou je als instelling moeten willen aanbieden?

De grens tussen werk en privé vervaagt

Traditioneel bestond er een vrij sterke scheiding tussen werkomgeving en privé. Men nam soms een dossier mee naar huis, maar vooral de werkgerelateerde communicatie was gebonden aan werkplek en werktijd. Zoals vaak het geval is, versterken techniek en cultuur elkaar: iemand privé bellen met een vraag over het werk deed men slechts bij hoge uitzondering. Als er echter iets veranderd is de laatste jaren, dan is dat wel de manier waarop we met elkaar communiceren. Zowel de manier waarop, als de timing: altijd en overal is het uitgangspunt.

De mate waarin werk en privé verweven raken varieert met de aard van het werk – de accountmanager die afhankelijk is van klanten wil altijd bereikbaar zijn, en met de leeftijd, veel jongeren hebben een diversiteit aan communicatievormen in hun leven ingepast. Een groep die hierin zeker voorop loopt, zijn de studenten. Zowel voor de communicatie die betrekking heeft op de studie als voor de privécontacten geldt: altijd en overal en bij voorkeur real-time en met beeld.

Studenten kiezen daarbij graag zelf hun communicatievormen en hun apparatuur. Zij zitten daarbij niet te wachten op specifieke voorzieningen binnen de onderwijsinstelling. Een werkplek is prettig – vanwege het gewicht van een notebook – maar ze zouden daarbij het liefst in hun vertrouwde internetomgeving werken. Een webinterface is alles wat ze nodig hebben.

Stel dat we het wegvallen van de grens tussen studie en privé, tussen de campus en thuis, als uitgangspunt nemen, wat betekent dit dan voor de universiteit of hogeschool die ICT-voorzieningen aanbiedt? En, in combinatie hiermee, wat zou je als instelling moeten willen aanbieden?

Apparatuur

Het aanbieden van draadloze internettoegang zonder beperkingen is voor een onderwijsinstelling vanzelfsprekend, zolang de door providers aangeboden vormen nog duur en kwalitatief beperkt zijn. Uitgangspunt hierbij is meestal dat niet alleen de eigen studenten maar ook bezoekers hiervan gebruik kunnen maken.

Voor pc-werkplekken wordt de vraag lastiger. Indien we de werkplekken met specifieke applicaties buiten beschouwing laten kun je de pc zien als een onderdeel van het meubilair dat beschikbaar gesteld wordt om studenten een werkplek te geven. Voor de manier waarop deze vervolgens door de student gebruikt wordt, zouden dezelfde regels en uitgangspunten moeten gelden als voor de notebook die gebruik maakt van het draadloze netwerk.

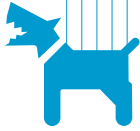
Applicaties en dataopslag

De applicaties die door een student gebruikt worden, vallen uiteen in een aantal categorieën:

- De communicatiegerelateerde internetapplicaties zoals email, MSN, Skype, Hyves en dergelijke. Deze applicaties worden met voldoende kwaliteit en een gunstig prijsniveau (veelal gratis) op internet beschikbaar gesteld. De universiteit of hogeschool kan hier geen significante toegevoegde waarde bieden. Bovendien beschikken veel studenten bij binnenkomst al over een eigen communicatieomgeving. Weliswaar wordt email op dit moment nog door (vrijwel) alle instellingen aan de studenten aangeboden, maar de verwachting is dat deze dienstverlening in de toekomst overbodig wordt. Hierbij zijn verschillende scenario's mogelijk. Het voor de korte termijn meest waarschijnlijke scenario is het gezamenlijk betrekken van email en aanverwante functies bij een grote aanbieder, met behoud van de instellingsidentiteit.
- De klassieke elektronische leeromgeving is primair een omgeving voor contentlevering en communicatie. Voor beide functies geldt dat deze in voldoende mate op internet beschikbaar worden gesteld. Desondanks zal een eigen ELO-omgeving nog wel enige tijd een meerwaarde bieden door de samenhang tussen de verschillende functies en de relaties met de administratieve omgeving.
- Algemene pc-gebaseerde kantoorapplicaties. Met de activiteiten van SURFdiensten op dit gebied wordt in voldoende mate tegemoet gekomen aan de behoefte van studenten om tegen een aantrekkelijke prijs een basispakket te kunnen aanschaffen. De universiteit of hogeschool kan hier geen toegevoegde waarde leveren.
- Specifieke beroepsapplicaties. Hierop zijn meestal tamelijk rigide licentievoorwaarden van toepassing. Daardoor is het veelal aantrekkelijk als deze applicaties door de instelling worden aangeboden. Daarnaast zijn de kosten vaak zo hoog dat van privéaanschaf geen sprake kan zijn.

Organisatorische grenzen vervagen

De gebruikers van ICT-diensten zullen in toenemende mate een diffuse groep vormen. Zo wordt het draadloze netwerk al op veel plaatsen opengesteld voor medewerkers en studenten van andere onderwijsinstellingen. Dit laatste uiteraard met differentiatie van de functionaliteit die via het draadloze netwerk beschikbaar komt. Ook de gebruikersgroep van applicaties en data wijzigt. Samenwerkingsverbanden worden gevormd en beëindigd. De omvang ervan kan variëren van een project tot een gezamenlijke opleiding of een mate van bestuurlijke eenwording. Deze samenwerkingsverbanden leiden tot wisselende gebruikersgroepen die voor een groot deel vanaf externe locaties toegang vragen tot applicaties en data.



Hoe houd je ongewenste elementen (personen, email, applicaties) buiten de deur als de grenzen door samenwerking steeds opener worden?

Er zou dus een gezamenlijk beveiligingsbeleid voor het ho moeten komen, dat een vertaling krijgt naar een implementatie op nationaal (lees SURFnet) niveau.

Naast de vervagende grenzen van de 'klanten' van de ICT-afdeling vervaagt ook de grens van de ICT-afdeling zelf. Diensten in de vorm van applicaties, opslag of verwerkingscapaciteit worden betrokken van derden. Tevens worden in toenemende mate data gedeeld met derden. Dit kan zowel administratieve gegevens betreffen (denk aan identificerende gegevens), als onderwijsinhoud.

Gevolgen voor de inrichting van de ICT-omgeving

Het belangrijkste terrein waarop het diffuser worden of verdwijnen van de afbakening van de ICT-omgeving zich manifesteert is de beveiliging van gegevens en apparatuur. Naast het bieden van een voldoende mate van beschikbaarheid betreft dit vooral de toegangsbeveiliging van applicaties, data en op het netwerk aangesloten apparatuur. Hierbij zijn het niet alleen personen die zich mogelijkwijs toegang proberen te verschaffen, maar ook elders geïnstalleerde schadelijke applicaties. De vraag is dus: hoe houd je ongewenste elementen (personen, email, applicaties) buiten de deur als de grenzen door samenwerking steeds opener worden. De vergelijking met het Schengenakkoord dringt zich op bij het beantwoorden van deze vraag: als de binnengrenzen wegvallen ten behoeve van een vrijer verkeer van personen en goederen, is het zaak de controle aan de buitengrenzen te verbeteren. Vertaald naar de ICT-omgeving kan de ho-gemeenschap gezien worden als het Schengengebied: de binnengrenzen zijn de grenzen van de individuele instelling en de buitengrens wordt gevormd door de grens van SURFnet en alles wat daarop (binnen Nederland) direct is aangesloten. Er zou dus een gezamenlijk beveiligingsbeleid voor het ho moeten komen, dat een vertaling krijgt naar een implementatie op nationaal (lees SURFnet) niveau. Dit laat onverlet dat iedere instelling nog steeds zorg moeten dragen voor de toegangsbeveiliging van zijn applicaties en data: binnen de Schengenlanden doet iedereen ook nog steeds zijn voordeel op slot. Maar een versterking van de buitengrenzen ten gunste van meer open binnengrenzen leidt tot vereenvoudiging van de onderlinge toegang bij een verlaging van de kosten voor beveiliging.

HOGESNELHEIDSVERBINDINGEN - NIET ALLEEN VOOR WETENSCHAPPERS

Het 'traditionele' internet bestaat uit een netwerk waarop pakketten individueel gerouteerd worden. Dat wil zeggen dat ieder pakket een adres heeft, op basis waarvan het pakket van het ene naar het andere schakelapparaat doorgestuurd wordt, totdat de bestemming bereikt is.

Enige jaren geleden is aan dit netwerk een tweede toegevoegd: het lambda- of lichtpadennetwerk. Het lichtpadennetwerk bestaat uit door glasvezel verbonden schakelapparatuur. Deze apparatuur schakelt echter geen pakketten maar golflengten waarvan er meerdere gelijktijdig over glasvezels verzonden kunnen worden. Op ba-

sis hiervan worden door de schakelaars end-to-end-verbindingen opgebouwd. Deze verbinding kan statisch zijn of een tijdelijk karakter hebben en staat volledig ter beschikking van de servers aan beide uiteinden van de verbinding. Op de verbinding kan data zonder verdere routinginformatie verstuurd worden. Ook het protocol is niet van belang en de beveiliging van dit privépad is in principe volledig gewaarborgd.

Het lichtpadennetwerk wordt door SURFnet sinds 2006 aangeboden en heeft vertakkingen naar lichtpadnetwerken elders op de wereld. In welke situaties heeft het lichtpadennetwerk voordelen boven het pakketgerouteerde internet? Toepassingen van het eerste uur liggen vooral op onderzoeksterrein. Een bekend voorbeeld is het Lofar project. Hierin wordt een extreem gevoelige radiotelescoop gerealiseerd door tienduizenden kleine antennes over een gebied met een diameter van 350 kilometer onderling door glasvezel te verbinden en te koppelen aan een supercomputer. Maar ook buiten dit gebied zal het lichtpadennetwerk verder zijn diensten gaan bewijzen. Voorbeelden daarvan zijn ondermeer: het Digitaal Bevolkingsonderzoek Borstkanker (DigiBOB), CineGrid – het Europese knooppunt in het wereldwijde initiatief voor 4K-cinema, en het optisch private netwerk voor de Open Universiteit Nederland.¹

Tot slot willen we wijzen op een nieuwe toepassing die bij uitstek de kracht van het lichtpaden netwerk laat zien:

Iedere universiteit of hogeschool heeft één of meerdere datacentra. De afhankelijkheid van deze datacentra is groot. Een hoge beschikbaarheid van het datacentrum is daarom één van de belangrijkste ontwerpcriteria. Brandblusinstallaties en noodstroomvoorzieningen behoren dan ook tot de standaard inrichting van het datacentrum. Toch is een calamiteit nooit helemaal uit te sluiten, met als mogelijk gevolg het voor kortere of langere tijd uitvallen van het datacentrum. Een grote brand, een ontploffing, sabotage, de kans erop is klein maar niet nul. En omdat het onderzoek- en onderwijsbedrijf stil ligt zodra het datacentrum uitvalt, realiseren universiteiten en hogescholen uitwijkvoorzieningen. Deze voorzieningen zijn echter duur, temeer omdat ze waarschijnlijk nooit gebruikt worden. Het ligt dan ook in de rede om uitwijkvoorzieningen te delen met anderen. Tot op heden gebeurt dit echter nog niet. Een mogelijk scenario is het realiseren van een gezamenlijke uitwijkvoorziening voor alle universiteiten en hogescholen. Dit combineert een hoge beschikbaarheid met een eveneens hoge mate van kosteneffectiviteit. Eventueel kunnen hierin naast elektriciteit en koeling ook opslag- en verwerkingscapaciteit aanwezig zijn. Als een instelling dan genoodzaakt is gebruik te maken van de uitwijkvoorziening, dan wordt een lichtpad opgebouwd tussen het netwerk van de instelling en de uitwijklocatie. Het lichtpad biedt een hoge bandbreedte en staat volledig ter beschikking van de instelling. Hierdoor vormt het op geen enkele wijze een beveiligingsrisico. Het kan in

omdat het onderzoek- en onderwijsbedrijf stil ligt zodra het datacentrum uitvalt, realiseren universiteiten en hogescholen uitwijkvoorzieningen. Deze voorzieningen zijn echter duur, temeer omdat ze waarschijnlijk nooit gebruikt worden. Het ligt dan ook in de rede om uitwijkvoorzieningen te delen met anderen. Dit combineert een hoge beschikbaarheid met een eveneens hoge mate van kosteneffectiviteit.

feite gezien worden als een eigen glasvezelverbinding tussen het netwerkknooppunt van de instelling en het uitwijkcentrum. Een belangrijk voordeel is dat het lichtpad in een fractie van een seconde opgezet kan worden en relatief goedkoop is omdat de kosten gedeeld worden met andere toepassingen die er op andere momenten gebruik van maken. Uiteraard is het noodzakelijk de lokale schakelapparatuur en de kritieke lokale bekabeling zodanig redundant uit te voeren dat de calamiteit die het datacentrum trof niet tevens het lokale netwerk buiten bedrijf stelt.

Terug naar het thema: open grenzen. Een lichtpadennetwerk tussen servers op verschillende instellingen is alleen mogelijk als we afzien van controle op de 'binnengrenzen'. Traditionele vormen van 'grenscontrole', zoals de firewall waarbij de 'bagage van de reiziger' - de inhoud van de datapakketten - wordt doorzocht alvorens deze toe te laten, volstaan niet als we met minimale vertraging willen reizen. Dat is immers het doel van lichtpaden: het doen verdwijnen van fysieke afstanden.

HET VERANDEREND PROFIEL VAN HET REKENCENTRUM

Naarmate ICT meer een commodity wordt en minder een factor die bepalend is voor het onderscheidend vermogen, neemt de wens toe om meer bedrijfseconomisch naar de ICT-dienstverlening te kijken.

Deze bedrijfseconomische invalshoek leidt al snel tot de conclusie dat schaalgrootte een belangrijke parameter is om kwaliteit beschikbaar te krijgen tegen aanvaardbare kosten. Dit geldt weliswaar niet voor alle, maar toch zeker voor een aantal van de diensten die de verschillende ICT-afdelingen leveren. De reden is dat ICT-diensten over het algemeen een hoge basislast (nullast) hebben en relatief beperkte incrementele kosten bij een toenemend aantal gebruikers. Zo dragen vooral de eenmalige installatiekosten en de continue investering in kennis bij tot de hoogte van de nullastkosten.

Inmiddels heeft vrijwel elke ho-instelling de bestuurlijke ambitie om de schaal van de ICT-dienstverlening te vergroten. Meestal gebeurt dit door de vorming van zogenoemde shared service centra. Dit proces is bij veel van de instellingen nog in volle gang. Het veranderingsproces gaat bovendien niet zonder pijn. De toegenomen afstand tussen de gebruiker en de dienstverlener, het zoeken naar de juiste balans tussen doorbelasting en administratieve overhead en vooral de aanloopproblemen zorgen ervoor dat de migratie naar een shared service centrum niet op voorhand een succesverhaal is. Toch is men het er over het algemeen over eens dat het centraal aanbieden van generieke ICT-diensten via een shared service centrum een onomkeerbare stap is in de evolutie van de ICT-dienstverlening.

De positionering van het shared service centrum binnen de organisatie is niet bij alle ho-instellingen gelijk. De belangrijkste onderscheidende parameter daarbij is de vorm van financiering en daarmee samenhangend de mate van organisatorische onafhankelijkheid van het centrum. Vooral bij kleinere, meer centraal gestuurde organisaties is overwegend sprake van inputfinanciering: de ICT-dienst krijgt een hoeveelheid geld en wordt verwacht daar een zo goed mogelijke dienstverlening mee te realiseren. De omvang van het budget is vooral historisch bepaald. Naarmate organisaties daarentegen bestaan uit meer autonome eenheden (faculteiten en diensten), met een eigen financiële verantwoordelijkheid, is meer sprake van shared service centra als interne leveranciers, al dan niet met verplichte winkelniering. Vaak ook tref je mengvormen aan: de infrastructurele voorzieningen worden centraal gefinancierd en zijn als zodanig voor ieder 'kosteloos' beschikbaar terwijl de diensten die bovenop de infrastructuur worden aangeboden, betaald worden door de afnemer. Veel universiteiten en hogescholen gaan uit van een dergelijke mengvorm en zoeken daarbij nog naar een balans tussen enerzijds inputfinanciering en anderzijds een financiering op basis van afname en, in relatie daarmee, een mate van afnameplicht.

De ICT-afdeling verandert niet alleen door de uitbreiding van haar taken en haar gewijzigde organisatorische positie. Een belangrijke ontwikkeling zal ook zijn dat zij in toenemende mate diensten zal inkopen ten behoeve van haar klanten. Zij zal zich ontwikkelen van producent van diensten tot inkoper en packager.

De ICT-afdeling verandert overigens niet alleen door de uitbreiding van haar taken en haar gewijzigde organisatorische positie. Een belangrijke ontwikkeling zal ook zijn dat zij in toenemende mate diensten zal inkopen ten behoeve van haar klanten. Zij zal zich ontwikkelen van producent van diensten tot inkoper en packager. Uiteraard geldt dit niet voor geavanceerde ICT-diensten waarbij het ho voorop wil lopen op de markt.

De parallel met de ontwikkeling die productiebedrijven al lang geleden hebben doorgemaakt is voor de ICT-dienstverleners zeker te trekken: het aantal daadwerkelijke producenten neemt af en veel bedrijven positioneren zich ergens in de waardevermeerderingsketen tussen producent en consument.

Enige specifieke ontwikkelingen op dit gebied betreffen:

- Het inkopen van specifieke diensten die in bulk goedkoper kunnen worden gerealiseerd en die gemakkelijk kunnen worden ingepast in de infrastructuur. Voorbeelden zijn dataopslag, back-up en archivering, en dataverwerking daar waar een relatief grote verwerkingscapaciteit vereist is.
- Vraagbundeling bij de aanschaf van software is een functie van de ICT-afdeling en zal dit blijven, in samenwerking met SURFdiensten.
- Het betrekken van applicaties (bijvoorbeeld email) van derden en deze inpassen in de informatie-infrastructuur.
- Het gezamenlijk binnen ho-verband realiseren van specifieke functies zoals uitwijkvoorziening bij calamiteiten.
- Daar waar instellingen op een gezamenlijke campus gehuisvest zijn, zullen zij voor een deel van een gezamenlijke infrastructuur gebruik maken.

In alle gevallen geldt dat een gezamenlijk inkooppunt voordelen heeft voor de organisatie. Dit voordeel kan variëren van (financiële) inkoopvoordelen tot een betere inpassing van de ingekochte dienst in de technische en/of informatie-infrastructuur.

In de praktijk schuilt het beveiligingsrisico niet zozeer in de dikte van de voordeur maar in het bestaan van achterdeuren in bijgebouwen, die toegang kunnen geven tot de ruimten waar het werkelijk om gaat. Dit gevaar is groter naarmate er bij de beveiligingsmedewerkers hiaten zijn in de kennis van het gebouw. Deze situatie kan zowel ontstaan door ondoorzichtigheid van het gebouw zelf als door regelmatige verbouwingen met tijdelijke voorzieningen. Onvoldoende communicatie en/of de onoverzichtelijkheid van de situatie maken dat de verantwoordelijke beveiligers de situatie niet meer kunnen overzien.

DE FUNDERING VAN HET BEVEILIGINGSBOUWWERK

De basis van een goede beveiliging is de beschikbaarheid van een volledig en actueel beeld van het te beveiligen object bij de beveiligingsfunctionarissen. Dit geldt voor de beveiliging van een bankgebouw maar evenzeer voor de beveiliging van de ICT-infrastructuur. Het beschikken over een goede documentatie is daarbij niet voldoende. Hoe belangrijk dit ook is. Het is noodzakelijk dat – in het geval van de ICT-voorzieningen – de beheerders die zorg dragen voor de beveiliging de opbouw van de totale infrastructuur kunnen overzien. Zij moeten derhalve een globaal beeld hebben van alles wat met de infrastructuur en de beveiliging daarvan samenhangt. Voor onderdelen en details kan dan worden teruggevallen op documentatie en ondersteunende systemen. Het is vergelijkbaar met de beveiliging van een bankgebouw. De beveiligingsmensen moeten kunnen overzien wat de structuur is van het gebouw, de onderlinge verbindingen tussen de gebouwdelen, de verbindingen naar andere complexen, de toegangsmogelijkheden en dergelijke. Dan pas kunnen zij beoordelen of en in welke mate beveiligingsrisico's van invloed zijn op het beveiligingsniveau van het totale gebouw.

Wat betekent dit uitgangspunt voor de opbouw en het beheer van de infrastructuur?

Twee dingen:

- 1 Ontwerp de infrastructuur op basis van een eenduidige en eenvoudige architectuur. In de praktijk betekent dit dat de infrastructuur wordt opgebouwd uit onderdelen met een minimale onderlinge verwevenheid. Zo is, vanuit overwegingen van overzichtelijkheid, een sterstructuur te prefereren boven een vermaasde structuur. Daar waar redundantie wordt aangebracht om de kwetsbaarheid te verminderen die ontstaat door single points of failure, moet voorkomen worden dat de complexiteit hierdoor vergroot wordt. Bij een goed ontworpen infrastructuur zijn de grensvlakken tussen de samenstellende onderdelen zodanig eenvoudig dat de onderdelen door verschillende beheergroepen min of meer onafhankelijk van elkaar beheerd kunnen worden.
- 2 Hanteer een rigide change management-systeem. Voorkom dat tijdelijke voorzieningen bedoeld om een acuut probleem of een urgente vraag op te lossen sluipend een structureel karakter krijgen. Goede procedures voor change management stellen uiteraard ook hun eisen aan de capaciteit en de expertise van het beheerpersonnel.

Indien de fundering in de vorm van een gedegen technische en procedurele structuur is gerealiseerd kan het verdere beveiligingsbouwwerk worden opgebouwd. Technieken en producten hiertoe zijn in voldoende mate beschikbaar. Bij elke toepassing ervan moet echter beseft worden dat zij ook een keerzijde hebben. In het algemeen leidt het aanbrengen van redundantie – teneinde de beschikbaarheid te vergroten – en het gebruik van beveiligingsgereedschappen tot een vergroting van de complexiteit en een verhoging van de beheerlast. Beide vormen een gevaar voor de fundering van het beveiligingsbouwwerk. Daarom zal bij elke uitbreiding van de infrastructuur met het doel de beveiliging te vergroten de vraag moeten worden gesteld of de vergroting van de complexiteit acceptabel is en of de beheerorganisatie in capaciteit en expertise in staat is met de toegenomen complexiteit om te gaan. Zo niet, dan is het netto effect van een op zich waardevol gereedschap negatief.

AANBEVELINGEN

Aanbeveling SURF/SURFnet

- Ontwikkel een structuur voor beveiliging van de buitengrenzen van de SURFnet gemeenschap en combineer deze structuur met daarop afgestemde aansluitvoorwaarden en aanbevelingen voor de interne beveiliging van de instellingen.
- Onderzoek de haalbaarheid van een gezamenlijke uitwijkvoorziening.

Aanbeveling instellingen

- Realiseer een intern beveiligingsbeleid dat ervan uitgaat dat de instelling een relatief open omgeving is. Verschuif het accent daarbij van de extern georiënteerde firewall naar een beveiliging van individuele servers.
- Ga na of en waar lichtpaden een rol kunnen spelen in de instellingsinfrastructuur en voor de connectiviteit met anderen.
- ICT-diensten zouden een leidende rol moeten nemen in de verdere bedrijfseconomische optimalisatie van de ICT-dienstverlening door daar waar mogelijk het inkopen van diensten af te zetten tegen het zelf aanbieden van deze diensten. Een gezamenlijke inkoop kan daarbij de inkoopvoorwaarden gunstig beïnvloeden.
- Draag er zorg voor dat de infrastructuur homogeen wordt opgezet en maximaal homogeen blijft. Expliciteer op basis daarvan welke kennis bij wie aanwezig moet zijn.

Referentie

- ¹ Meer informatie over de verschillende projecten is te vinden via de website van SURFnet (<http://www.surfnet.nl/>).