BELNET JAARVERSLAG 2009

veiliger & efficiënter samenwerken

IN ONDERWIJS EN ONDERZOEK

BELNET

BELNET JAARVERSLAG 2009

veiliger & efficiënter samenwerken

IN ONDERWIJS EN ONDERZOEK

26 – 27
HENRI MALCORPS

"Het KMI heeft een eigen contactpersoon bij BELNET die ons opvolgt en waarmee we regelmatig overleggen."

32 – 33
WIM POUSEELE

38 – 39
PETER STRICKX

48 – 49
HERMAN MOONS

Inhoud

Aan het woord

"Onze systemen en diensten zijn onderdeel van de kritieke infrastructuur van de belangrijkste maatschappelijke instellingen."

PIERRE BRUYÈRE, directeur

WOORD VOORAF
DOOR DIRECTEUR PIERRE BRUYÈRE

Het jaar 2009 stond bij BELNET voor een groot deel in het teken van de veiligheid. Het belang van veilige netwerken kan vandaag nog maar moeilijk overschat worden. Waar computercriminaliteit vroeger vooral een zaak van individuele delinquentie was, moeten we ons nu ook beschermen tegen georganiseerde misdaad en fraude. Door deze verontrustende evolutie zijn veiligheidsmaatregelen een absolute noodzaak.

Daar komt voor BELNET bij dat ons netwerk, met zijn hoge basisbandbreedte van 10 Gbps, op grootschalige manier misbruikt zou kunnen worden. Door één zwakke schakel in het systeem zou onze enorme netwerkcapaciteit in verkeerde handen kunnen vallen. De kennis en de infrastructuur van de onderwijs- en onderzoekssector beschermen is onze prioriteit. Daarom heeft BELNET al enkele jaren geleden een eigen Computer Emergency Response Team (BELNET CERT) opgericht om zijn klanten en gebruikers te sensibiliseren en, waar nodig, te helpen bij de beveiliging van hun werkomgeving. Deze missie hebben we in 2009 versterkt.

HET EERSTE BELGISCHE CONTACTPUNT VOOR NETWERKBEDREIGINGEN

Op vraag van de Federale Overheidsdienst Informatie- en Communicatietechnologie (Fedict) en in samenwerking met

het Belgisch Instituut voor Postdiensten en Telecommunicatie (BIPT) hebben we in 2009 CERT.be opgericht. CERT.be is in ons land het eerste nationale contactpunt voor wie te maken krijgt met bedreigingen op het internet. Met CERT.be richten we ons tot het hele land: veiligheidsexperts, kritieke infrastructuur, bedrijven en alle gewone gebruikers. Dat BELNET werd aangezocht om CERT.be uit te baten, beschouwen we als een blijk van vertrouwen en een belangrijke erkenning van onze ervaring in het domein van de veiligheid.

Om veiligheid als thema weerklank te geven, hebben we in 2009 voor het eerst de BELNET Security Conference georganiseerd. We zullen dit initiatief jaarlijks herhalen. Enerzijds willen we op deze conferenties belangrijke veiligheidstrends bespreken en onze BELNET-diensten presenteren, anderzijds willen we ook een netwerk van veiligheidsdeskundigen opbouwen, ervaringen uitwisselen en feedback op onze diensten verzamelen.

"Terwijl we vroeger vooral tijd en middelen investeerden in de uitbouw van onze netwerkinfrastructuur, concentreren we ons vandaag meer op de ontwikkeling van netwerkdiensten."

"Business continuity is een permanente bekommernis geworden."

NIEUWE DIENSTEN OP EEN HYPERSTABIEL NETWERK

BELNET wil zijn klanten en gebruikers ook helpen bij het beveiligen van netwerken en toepassingen. In 2009 werkten we aan de verbetering van een aantal veiligheidsdiensten, zoals de BELNET Vulnerability Scanner om zwakke plekken in een netwerk op te sporen en de BELNET Digital Certificates Service voor toegangscontrole en authenticatie. Daarnaast werd in tal van andere nieuwe diensten en verbeteringen geïnvesteerd, meestal ter voorbereiding van hun definitieve lancering in 2010. De ontwikkeling van diensten als Videoconferencing en het E-collaboration Platform past in de evolutie die nu al enkele jaren bij BELNET aan de gang is. Terwijl we vroeger vooral tijd en middelen investeerden in de uitbouw van onze netwerk-infrastructuur, concentreren we ons vandaag meer op de ontwikkeling van netwerkdiensten. Om er zeker van te zijn dat deze diensten aan reële behoeften voldoen, houden we regelmatig een peiling bij onze klanten.

Uit de resultaten van onze tevredenheidsenquête in 2008 bleek dat onze klanten tevreden tot uiterst tevreden zijn over onze dienstverlening. Punten die voor verbetering vatbaar waren, werden opgenomen in een actieplan, samen met de

nodige middelen voor de verbetering. We doen ook veel om de diensten die we hebben, bekend te maken en we helpen onze klanten en gebruikers ermee te werken. In dit verband herwerkten we de informatie op onze website, hebben we workshops opgezet en vond opnieuw de jaarlijkse BELNET Networking Conference plaats. Ook namen we in 2009 een productmanager aan om ons dienstenaanbod te stroomlijnen en om ervoor te zorgen dat nieuwe diensten echt vanuit een sterke behoefteanalyse ontwikkeld worden.

VERSTERKING EN PROFESSIONALISERING VAN DE ORGANISATIE

De aandacht voor dienstverlening heeft het aantal medewerkers bij BELNET doen stijgen van 33 naar 39 voltijdsequivalenten. In 2009 troffen we daarom voorbereidingen voor een verhuis naar een nieuwe locatie. De groei van het personeelsbestand vraagt ook om een verhoogde professionalisering

> "Dat BELNET werd aangezocht om CERT.be uit te baten, beschouwen we als een blijk van vertrouwen en een erkenning van onze ervaring in het domein van de veiligheid."

van onze interne structuren. En omdat onze systemen en diensten vandaag onderdelen zijn van de kritieke infrastructuur van de belangrijkste maatschappelijke instellingen, is business continuity een permanente bekommernis geworden.
In 2009 zijn we gestart met de ontwikkeling van een volledig en coherent Business Continuity Plan dat ervoor moet zorgen dat onze netwerken en diensten altijd beschikbaar blijven, ook in extreme omstandigheden, bijvoorbeeld bij brand in onze gebouwen of wanneer zich een andere ramp voordoet.

Onze klanten en gebruikers verwachten dat onze diensten en netwerken permanent beschikbaar zijn, dat we op elk moment van de dag uitmuntende kwaliteit leveren, en dat we de hoogste veiligheid garanderen. Het onderzoek naar de tevredenheid van onze klanten en gebruikers leert dat we deze verwachtingen inlossen. Maar we moeten de veranderende behoeften van onze klanten en gebruikers blijven volgen. Onze aandacht zal de volgende jaren niet alleen naar de BELNET-diensten gaan, maar ook naar de uitbating van BNIX (Belgian National Internet eXchange) en naar de werking van het Belgische CERT. We hebben ook alle voorbereidingen getroffen om een nieuw FedMAN – het netwerk van de federale overheid – te bouwen. Ik twijfel er niet aan dat we voor al die nieuwe uitdagingen de volgende jaren verder mogen blijven rekenen op de inzet van onze medewerkers, onze partners en de leden van de beheerscommissie. Onze oprechte dank aan ieder van hen.

PIERRE BRUYÈRE, directeur

ONZE MISSIE

1

BELNET stimuleert de wetenschappelijke ontwikkelingen door innovatieve netwerkstructuren van hoge kwaliteit met bijbehorende diensten te leveren en te onderhouden, ten voordele van het Belgisch hoger onderwijs en onderzoek.

2

BELNET versnelt dankzij zijn verworven expertise, zijn unieke marktpositie en zijn schaalvoordelen de groei van de kennis- en informatiemaatschappij.

3

BELNET ontplooit activiteiten die het internet in België versterken en zet telematica- en netwerkprojecten op voor overheden, administraties en openbare instellingen.
Tot de activiteiten van BELNET behoren de uitbating van BNIX (Belgian National Internet eXchange), het beheer en de opvolging van FedMAN en de uitbouw van CERT.be (het nationale Computer Emergency Response Team).

ONZE STRATEGISCHE DOELSTELLINGEN

1

BELNET wil de behoeften van onderwijs- en onderzoeksinstellingen en hun eindgebruikers op het vlak van netwerkinfrastructuur en bijbehorende diensten optimaal vervullen.

2

BELNET wil innovatieve netwerken en toepassingen leveren die inspelen op de behoeften van morgen.

3

BELNET wil een sterke, zichtbare organisatie zijn die alle onderwijs- en onderzoeksinstellingen bereikt.

4

BELNET wil zijn middelen en mensen op een effectieve en efficiënte manier inzetten binnen een geoptimaliseerde structuur.

dossier veiligheid

" We zijn eigenlijk de internetbrandweer."

BELNET zet nationaal computerveiligheidsteam op 16

" Trojaanse paarden blijven de grootste bedreiging."

Interview met Luc Beirens, Federal Computer Crime Unit 19

" BELNET is de logische, noodzakelijke partner voor een nationaal CERT."

Daniel Letecheur van Fedict legt uit 22

Het internet heeft veel nieuwe mogelijkheden gecreëerd. In het begin van de 21ste eeuw werd steeds duidelijker dat die niet allemaal altijd op een positieve manier gebruikt worden.

BELNET wees er al vroeg op dat gebruikers en netwerken zich moeten beschermen tegen allerlei vormen van cybercriminalititeit. Sinds de lancering van het nationale Computer Emergency Response Team (CERT.be) in augustus 2009 speelt BELNET ook formeel een belangrijke rol in die bescherming.

Computerveiligheid verdient **meer aandacht**

MEER BEDREIGINGEN

Hoewel lang niet alles gemeten wordt, lijkt het aantal misdaden op het internet internationaal te stijgen. Het grensoverschrijdende karakter van de technologie en het lage veiligheidsbewustzijn bij gebruikers werken die evolutie in de hand. In 2009 deden zich een aantal opmerkelijke incidenten voor. Zo kreeg het kabinet van de Zwitserse minister van Buitenlandse Zaken een cyberaanval te verwerken, en ook banken werden het slachtoffer van criminelen, die trouwens steeds professioneler te werk gaan. Maar niet alleen grote bedrijven of overheden vormen aantrekkelijke doelwitten. Elke internetgebruiker kan vandaag te maken krijgen met ongewenste mail (spam), valse websites (phishing), verborgen functies in programma's (Trojaanse paarden) en andere vormen van cybercriminaliteit.

NATIONALE BEVEILIGING NOODZAKELIJK

Zowel internationaal als nationaal worden diverse initiatieven genomen om overheden, ondernemingen en burgers te beschermen. In België zette de overheid eCops op, een website waar gevallen van cybercriminaliteit gemeld kunnen worden. In 2009 startte BELNET CERT.be op, het nationale Computer Emergency Response Team dat in de eerste plaats kritieke economische sectoren als die van het transport, de energie en de telecommunicatie beter wil beschermen. Als bedrijven in dergelijke sectoren het slachtoffer worden van een grote aanval, kan dat economisch verstrekkende gevolgen hebben. Ook het grote publiek wordt aangesproken. Het is voornamelijk de bedoeling om veiligheidsproblemen te voorkomen, maar CERT.be treedt ook op in noodgevallen. Het geeft informatie over incidenten door aan de politie, die vervolgens misdadigers kan opsporen en voor het gerecht brengen. Maandelijks behandelt het nationale CERT tussen de 50 en 100 ernstige incidenten. Vermits netwerkbedreigingen ook van buiten België komen, werkt CERT.be binnen een wereldwijd netwerk van computerbeveiligingsexperts. ■

Jan Torreele (links), technisch directeur bij BELNET en Lionel Ferette (rechts), CERT.be-coördinator bij BELNET

"Je moet ons zien als de brandweer die blust, **assisteert**, **coördineert** en **sensibiliseert.**"

BELNET beschouwt veiligheid op het internet als een topprioriteit. Om de veiligheid van zijn klanten en gebruikers te bevorderen, richtte het zes jaar geleden al een eigen Computer Emergency Response Team (CERT) op. Nu is BELNET ook verantwoordelijk voor CERT.be, het eerste nationale computerveiligheidsteam van België.

JULLIE HADDEN VÓÓR CERT.BE AL HEEL WAT ERVARING IN DE EIGEN COMMUNITY. IS VEILIGHEID DAAR EEN BELANGRIJKE KWESTIE?

Jan Torreele, technisch directeur bij BELNET: "We beheren een netwerk voor universiteiten en hogescholen. Op dat netwerk zitten dus heel wat studenten informatica met tijd, kennis en zin om te experimenteren. De hackercultuur spreekt sommigen onder hen aan, en zij tasten graag de grenzen van de technologie af. Vanuit die optiek is veiligheid een permanente bekommernis. Een ander aspect is de kracht van ons

netwerk. Het heeft een geweldige capaciteit en er zijn heel wat krachtige computers op aangesloten. Als je die in handen krijgt, kun je massaal veel schade toebrengen, bijvoorbeeld door grote hoeveelheden data naar één bepaald doelwit te sturen, zodat alles daar vastloopt. Een eigen CERT was dus voor ons heel belangrijk. Ook klanten vroegen ernaar. Ik herinner me nog een IT-manager van een universiteit die me jaren geleden zei dat hij nog liever had dat we bij gevaar zijn hele netwerk afsloten dan dat hij nadien een paar duizend besmette pc's moest herstellen. We hebben daarom relatief vroeg eigen resources vrijgemaakt voor een eigen CERT."

BELNET WAS MET DIE VOORGESCHIEDENIS DE LOGISCHE KANDIDAAT OM EEN NATIONAAL CERT UIT TE BOUWEN?

Jan Torreele: "Niet alleen omwille van die ervaring met het eigen CERT. We waren vroeger de facto ook al het internationale aanspreekpunt voor alles wat met netwerkbeveiliging te maken had. Alleen hadden we toen noch het mandaat, noch de middelen. We konden dus alleen maar bij ernstige gevallen op een best-effortbasis werken. We waren dan ook blij dat de minister van Informatisering uiteindelijk aan Fedict de vraag stelde om formeel een nationaal initiatief op te starten. Fedict heeft dan aan ons gevraagd om in samenwerking met het BIPT het nationale CERT daadwerkelijk uit te bouwen. Wij hebben de ervaring en de juiste expertise. Als openbare instelling garanderen wij bovendien neutraliteit en zijn we een stabiele factor. Er zijn in ons domein niet veel spelers die al meer dan vijftien jaar meegaan."

WAT ZIJN DE EERSTE ERVARINGEN MET CERT.BE?

Lionel Ferette, CERT.be-coördinator: "We zijn met CERT.be natuurlijk nog maar pas begonnen, maar het is duidelijk dat veel mensen veel verwachten. Soms zijn de verwachtingen zelfs onrealistisch hoog. Wij kunnen bijvoorbeeld niemand met slechte bedoelingen 'van het internet gooien'. Dat kunnen we niet, dat mogen we niet en dat willen we niet. We werken binnen het kader van een rechtsstaat en hebben niet het mandaat dat toebehoort aan de politie of het gerecht."

Jan Torreele: "Je moet ons eerder zien als de brandweer die blust, assisteert, coördineert en sensibiliseert. Daarbij richten we ons in eerste instantie op de kritieke infrastructuren van onze samenleving: de banken, de transportsector, de overheid, ... Daar moeten we nu eerst bekendheid en vertrouwen opbouwen, want veel organisaties staan niet te springen om een veiligheidsincident te melden. Als het vertrouwen er is en als mensen zien dat wij nuttig werk verrichten, gaan ze dat hopelijk wel doen. Uiteindelijk zouden we graag zien dat elke grote onderneming een eigen CERT-functie in het leven roept. Een gemandateerde persoon die de problematiek kent en waarmee we in vertrouwen kunnen samenwerken, is belangrijk. Het grote publiek informeren en sensibiliseren, dat willen we ook doen, maar pas in tweede instantie."

HOE ZIEN JULLIE DE TOEKOMST?

Jan Torreele: "We zien een evolutie van individuele hackers naar georganiseerde criminaliteit en

"We hebben niet **het mandaat** van de politie of het gerecht."

doelgerichte aanvallen op organisaties. Vaak wil men informatie of geld stelen, soms richt men zijn pijlen vanuit politiek activisme op de overheid. En doordat de overheid meer online gaat, wordt ze natuurlijk ook vanzelf meer online aangevallen. De criminaliteit zou zich in de toekomst ook kunnen verplaatsen naar smartphones en tabletcomputers."

Lionel Ferette: "We krijgen meer en meer te maken met advanced persistent threats. Criminelen willen de zaken niet platleggen maar proberen via achterpoortjes systemen binnen te dringen en daar dan zolang mogelijk ongemerkt te blijven om zoveel mogelijk te stelen. De tijd van de hackers die voor het plezier en hun eigen glorie iets kapotmaakten, is grotendeels voorbij. Nu probeert men integendeel onzichtbaar te blijven. Het is een van de taken van het CERT.be om die onzichtbare problematiek zichtbaar te maken, om de patronen in kaart te brengen en te analyseren, zodat de samenleving er beter tegen kan optreden."

NEEMT BELNET NOG ANDERE INITIATIEVEN?

Jan Torreele: "Voor BELNET is beveiliging niet beperkt tot CERT.be. Omdat bewustmaking een belangrijk aspect is, zette BELNET in 2009 de eerste BELNET Security Conference op. Deze conferentie vindt voortaan jaarlijks plaats. Met de BELNET Security Conference wil BELNET zijn klanten en gebruikers nog beter informeren over veiligheid op het internet. Het programma bestaat uit presentaties en keynote speeches over veiligheidskwesties en -trends. Er komen onder meer praktische veiligheidstips, oplossingen en diensten aan bod. Verder kunnen BELNET-klanten een beroep doen op een groeiend aantal diensten om hun netwerk en computers te beveiligen, zoals Vulnerability Scanner en Digital Certificates Service, dat digitale certificaten aflevert waarmee een klant de toegang tot zijn eigen websites kan beveiligen." ■

Internetcriminaliteit in 2009. Een paar cijfers.

- **945 euro**
bedroeg het gemiddelde schadebedrag per schadegeval van de aan de politie gemelde internetfraude.

- **9.891**
strafbare feiten van internetcriminaliteit werden vastgesteld.

- **15 botservers**
werden uit de lucht gehaald door de FCCU (Federal Computer Crime Unit).

- in **1.740 gevallen**
werd overgegaan tot de identificatie van malafide internetgebruikers, meer bepaald gebruikers van e-mailadressen, IP-adressen en pseudoniemen. Dat betekende een stijging met ongeveer 400 % in vergelijking met 2002.

- **230.000 kredietkaarten**
werden geblokkeerd na misbruik. Dat is een verviervoudiging ten opzichte van 2008.

2009

Bron: FCCU, directie Bestrijding van de Economische en Financiële Criminaliteit, Federale gerechtelijke politie

"Trojaanse paarden blijven de grootste bedreiging."

Als hoofd van de Federal Computer Crime Unit weet Luc Beirens beter dan wie ook welke computergevaren er op ons af komen. Bij het internetbankieren blijven de inbreuken beperkt, maar over andere domeinen maakt hij zich meer zorgen.

WAT ZIJN DE GROOTSTE GEVAREN WAAR U MEE TE MAKEN KRIJGT?

Luc Beirens: "Trojaanse paarden blijven de grootste bedreiging. Het principe is eenvoudig: bij slachtoffers wordt ongemerkt kwaadaardige software geïnstalleerd, bijvoorbeeld wanneer ze klikken op een link of een zogenaamde update van een programma installeren. Zo'n stiekem programmaatje kan door de cybercriminelen worden gebruikt om informatie van je pc af te halen maar ook om toepassingen op je pc te gebruiken. Met behulp van Trojaanse paarden zijn criminelen er in de voorbije jaren bijvoorbeeld wereldwijd in geslaagd om geld van de bankreke-

ningen van hun slachtoffers af te halen. Het is een business waar wereldwijd miljoenen in omgaan. Trojaanse paarden kunnen ook automatisch informatie over de geïnfecteerde pc en over de werkwijze van zijn gebruiker overmaken naar databanken die onder controle staan van de criminelen. Op die manier krijgen criminelen onder meer zicht op het surfgedrag, op de e-mails, maar ook op wachtwoorden, logins en allerlei zeer persoonlijke gegevens. We zien meer en meer dat deze informatie te gelde wordt gemaakt via oplichting of door afpersing. Trojaanse paarden zijn dus ideale werktuigen om economische, industriële of andere vormen van spionage te plegen. Bovendien gaan de meeste computers door het Trojaanse paard ook deel uitmaken van een botnet."

WAT ZIJN BOTNETS?

Luc Beirens: "Dat zijn netwerken van computers die door een Trojaans paard geïnfecteerd zijn en via tussenstations (botnetservers) door de cybercriminelen kunnen worden aangestuurd. Het criminele gebruik van botnets dook voor het eerst op in 2004 en is sindsdien steeds frequenter waargenomen. Wij hebben met de Federal Computer Crime Unit in 2009 vijftien botnetservers uit de lucht gehaald, dit jaar wordt dat aantal minstens verdubbeld. Botnetservers zijn belangrijke knooppunten in een botnet. Als je een server weghaalt, verstoor je de werking van het botnet maar daarmee is het botnet nog niet ontmanteld. Als iedereen wereldwijd echter voor zijn eigen deur veegt, is de straat wel proper."

WAT KAN JE ER ALS GEBRUIKER TEGEN DOEN?

Luc Beirens: "Mensen moeten waakzamer worden voor alles wat ze op hun pc en het internet zien en doen. Ze moeten in de eerste plaats hun pc gezond houden door het besturingssysteem, de noodzakelijke beveiligingssoftware en alle andere toepassingen regelmatig bij te werken naar de nieuwste versies. Maar zelfs dat volstaat niet. Ze moeten twee keer nadenken vooraleer ze op een link klikken, bijvoorbeeld om software te installeren. Vaak zien

Internetcriminaliteit door de jaren heen

In 2004

wordt een Britse site die is gespecialiseerd in weddenschappen virtueel afgeperst en bedreigd. Omdat ze niet de gevraagde som betaalt, wordt een denial-of-service attack ingezet: via een botnet van gekraakte computers worden massaal veel data naar de website verstuurd, waardoor die volledig lam komt te liggen.

In 2007

worden kritieke infrastructuren in Estland met botnets aangevallen door cyberterroristen. Ook banken worden virtueel aangevallen. De overheid besluit om alle dataverkeer met het buitenland af te sluiten.

In 2008

verhuist de website van de Georgische president Michail Saakasjvili naar de Verenigde Staten. Dat gebeurt nadat (vermoedelijk Russische) hackers met een botnet hebben geprobeerd de servers in Georgië plat te leggen.

In 2009

verspreidt het Conflicker-virus zich in enkele dagen tijd wereldwijd over miljoenen computersystemen en veroorzaakt enorm veel schade in bedrijven en overheidsdiensten.

we ook dat slachtoffers de meest elementaire veiligheidsmaatregelen niet hebben nageleefd: onveilige wachtwoorden, geen back-up, ... De oorzaak van die gevaarlijke onzorgvuldigheid hoef je niet ver te zoeken. Er wordt hen op school en in de bedrijven veel te weinig geleerd over de gevaren van het gebruik van computers en het internet en over hoe je die gevaren kan minimaliseren."

HOE DOET BELGIË HET TEN OPZICHTE VAN HET BUITENLAND?

Luc Beirens: "Wat betreft de veiligheid van internetbankieren hebben we een voorsprong. Het aantal dossiers rond fraude bij e-banking dat we in 2009 hebben behandeld, is heel beperkt en stijgt zeker niet, in tegenstelling tot wat soms wordt beweerd in de media. De kans om beroofd te worden via internetbankieren is véél kleiner dan de kans om beroofd te worden aan het loket. Belgische banken hebben hun maatregelen verstrengd en zijn meer dan behoorlijk beveiligd. Bij sommige buitenlandse banken is een login en een wachtwoord nog steeds voldoende om aan e-banking te doen, in ons land zijn banken binnenkort verplicht om met een speciale kaartlezer of Digipass te werken. Dat maakt het risico op misbruik een stuk kleiner."

WAAR MOET ER NOG WEL VEEL GEBEUREN?

Luc Beirens: "Onze versnipperde aanpak maakt ons kwetsbaar. Er is in ons land niemand die echt verantwoordelijk is voor een globale aanpak van de cyberdefensie. Die verantwoordelijkheid is verdeeld over instanties als de krijgsmachten, de politie, Fedict, en de federale overheidsdiensten Binnenlandse Zaken, Justitie, Buitenlandse Zaken en Economie. In de VS en in het Verenigd Koninkrijk is er al wel een gecentraliseerde aanpak. Die is ook hier nodig: als er zich een incident voordoet, moet er snel en gecoördineerd worden opgetreden. En een incident is zeker niet uitgesloten. In 2007 werd Estland door hackers aangevallen. De Estse overheid moest snel handelen en heeft toen zelfs beslist om alle dataverkeer van en naar het buitenland te blokkeren."

De Federal Computer Crime Unit (FCCU)

De FCCU pakt diverse vormen van internet- en computercriminaliteit aan, zoals phishing, malafide loterijen, hacking, fraude op sociale netwerken en verkoop van gestolen kredietkaartnummers.

Ze helpt internetfraude en aanvallen op kritieke IT-infrastructuren voorkomen en bestrijden. De FCCU beheert ook het meldpunt www.eCops.be waar onder meer kinderpornosites en phishingwebsites kunnen gemeld worden.

De FCCU behoort tot de Federale gerechtelijke politie en werkt in de strijd tegen de cybercriminelen heel vaak samen met buitenlandse politiediensten.

IS HET DOOR BELNET OPGERICHTE CERT.BE EEN GOEDE ZAAK?

Luc Beirens: "Ik ben blij dat het nationale CERT eindelijk is opgericht. Het is iets waar ik altijd voor heb gepleit. Nu hebben bedrijven en personen die geen klacht willen neerleggen bij de politie uit vrees voor negatieve publiciteit tenminste een aanspreekpunt waar ze met hun informatie en vragen omtrent cybercrime en ernstige ICT-incidenten terecht kunnen. Het feit dat het nationale CERT is opgericht onder voogdij van BELNET, omdat zij reeds over een expertise terzake beschikten, is goede zaak, want wij als politie kunnen alleen optreden in het kader van een gerechtelijk dossier. CERT.be is in de eerste plaats een analyse- en meldpunt omtrent bedreigingen van de kritieke infrastructuur. Daarom lijkt het mij belangrijk het team van CERT.be verder uit te bouwen en overheidsinstellingen en bedrijven in de kritieke infrastructuur aan te zetten – of zelfs te verplichten – om incidenten te melden aan CERT.be. We zijn er dus nog niet." ■

" BELNET is de **logische, noodzakelijke partner** voor een nationaal CERT."

Cybercriminaliteit is alomtegenwoordig. Op het internet vind je programma's waarmee je kan proberen gebruikersaccounts te kapen of kritieke diensten uit te schakelen. CERT.be is een antwoord op dergelijke bedreigingen. Elke maand verwerkt het Computer Emergency Response Team tot 100 ernstige informatica-incidenten in ons land. Een blik achter de schermen van een stille, angstaanjagende oorlog.

In 2007 krijgt Estland te maken met een cyberaanval die het land bijna tot stilstand brengt. De Estse overheid heeft het over de '11 september van de informatica'. In april 2010 bedreigt een cyberaanval in de Verenigde Staten het volledige elektriciteitsnet. Dat voedt de angst voor een grootschalig offensief dat in enkele uren de grootste wereldmacht kan lamleggen.

CERT-BEWAKING IN DE HELE WERELD

Deze twee incidenten haalden wereldwijd de voorpagina's. Honderden andere, minder ernstige, gevallen worden nauwlettend opgevolgd door CERTs. Specialisten observeren de incidenten, analyseren ze en houden de gevoeligste sectoren op de hoogte: de

CERT.be sinds de oprichting

augustus 2009

Het nationale CERT wordt opgericht. Fedict neemt de leiding, BELNET staat in voor de operationele werking. Het doel: kritieke bedrijven en de administratie informeren over informaticarisico's en incidenten behandelen (opsporen, analyseren, actie ondernemen en informeren).

september 2009

CERT.be wordt door de overheid aangekondigd.

januari 2010

CERT.be richt zich ook tot het grote publiek via zijn website. Daarop zijn algemene veiligheidsadviezen te vinden voor 'best practices' en links naar informatiebronnen.

banken, de ziekenhuizen, de overheidsadministraties, de energiebedrijven, ...

België richtte CERT.be op in augustus 2009. "We hadden geen nationaal Computer Emergency Response Team, terwijl hier heel wat belangrijke internationale instellingen gevestigd zijn en België meer en meer e-governmenttoepassingen ontwikkelt. Er drong zich een structuur op die incidenten behandelt, assisteert bij problemen en advies geeft omtrent best practices", zegt Daniel Letecheur, information security analyst bij Fedict.

Meer dan 6 maanden na de lancering van CERT.be hebben de CERT.be-medewerkers geen gebrek aan werk. Per maand behandelen ze gemiddeld meer dan 300 aangiften, onderwerpen ze 150 tot 200 incidenten aan een nader onderzoek en beoordelen ze 50 tot 100 van die incidenten als 'ernstig'. "Meer dan de helft van de aanvallen zijn vandaag gericht op gebruikersaccounts of systemen", zegt Daniel Letecheur.

FEDICT, PROJECTINCUBATOR

De telecomwetgeving verplicht de staat zijn telecominfrastructuur te beschermen. Vanuit die verplichting is CERT.be ontstaan. De oprichting ervan werd toevertrouwd aan Fedict, de federale overheidsdienst die nieuwe technologie binnen het bereik van iedereen wil brengen. Fedict lanceerde diensten als Tax-on-web, het meldpunt PoliceOnWeb, eID (de elektronische identiteitskaart) en eBirth (voor de aangifte van geboorten).

"Bij de oprichting van CERT.be werd een beroep gedaan op BELNET en de solide expertise die het toen al had opgebouwd. Oorspronkelijk bestond CERT.be uit vier medewerkers, allemaal informatici met een grondige kennis van netwerken en beveiliging. Vandaag telt het team zes specialisten; in 2013 of 2014 zullen dat er tien zijn."

BELNET, NATUURLIJKE PARTNER

"BELNET was een logische, noodzakelijke partner", zegt Daniel Letecheur. "BELNET maakt deel uit van

de administratie en we wilden het nationale CERT binnen de openbare sector houden. Bovendien had BELNET ervaring met de materie. BELNET houdt zich al meer dan vijftien jaar bezig met netwerken van Belgische universiteiten en administraties en had al een eigen CERT om zijn netwerk te bewaken en zijn gebruikers te informeren.

We hebben een uitstekende relatie met BELNET. Elke maand krijgen we een gedetailleerd verslag over de activiteiten van de afgelopen periode en de verschillende soorten incidenten die zich hebben voorgedaan. We plannen samen activiteiten, zoals de publicatie van informatie op het web, het bezoek aan partners of prospects, of meetings met instellingen en bedrijven om hen het nationale CERT voor te stellen."

EEN COMPLEX INFORMATIENETWERK

"In heel de wereld stijgt het aantal aanvallen op informaticasystemen", zegt Daniel Letecheur. "Ze komen van overal. Op het internet zijn programma's te vinden waarmee je kan proberen gebruikersaccounts te kapen of kritieke diensten uit te schakelen. Die informatie staat op het net, criminelen hoeven ze slechts op te zoeken en te gebruiken. Met dit zwaard van Damocles boven het hoofd wisselen CERTs in heel de wereld kritieke informatie uit.

De informatie waarover CERT.be beschikt, komt van verschillende bronnen. CERT-partners delen hun informatie met CERT.be, zeker als België betrokken partij is. Ook de bedrijven en overheidsadministraties wisselen info uit met CERT.be. De banken bijvoorbeeld hebben intern al een eigen responscapaciteit opgebouwd, maar ze kunnen ons nog altijd een incident melden, zoals een geval van e-bankingfraude. Wij kunnen dan een onderzoek instellen en, indien nodig, voorstellen om via tussenkomst van de gerechtelijke autoriteiten een bankrekening af te sluiten. Daarvoor werkt CERT.be nauw samen met de FCCU (Federal Computer Crime Unit)."

DE AANPAK VAN CERT.BE

De toekomst van CERT.be zit in die aanpak, in de samenwerking en uitwisseling met andere betrokken partijen in de strijd tegen cybercriminaliteit. "We gaan de operationele capaciteit van onze dienst verhogen zodat we de meerderheid van de incidenten binnen korte tijd kunnen behandelen. Die doelstelling moeten we tegen half 2012 halen", zegt Daniel Letecheur. Voor het overige wil CERT.be voordeel halen uit de integratie en coördinatie van verschillende actoren in het domein. "Er bestaat vandaag een militair CERT, maar ook een Federal Computer Crime Unit, en dan is er nog Justitie. Het is de bedoeling dat die allemaal nog meer gaan samenwerken." ■

CERT.be in cijfers

2009

- 200 tot 300
rapporten per maand

- 150 tot 200
incidenten per maand

- 50 tot 100
ernstige incidenten per maand. Een ernstig incident is een geval van fraude, een poging tot fraude of een (poging tot) identiteitsdiefstal in de banksector.

Veilig op het internet

Gebruik een firewall

Met een firewall kunt u uw computers beter beschermen tegen aanvallen via het internet.

Reageer nooit op spam

De term 'spam' wordt gebruikt om ongewenste e-mails aan te duiden. Spam wordt in eerste instantie verzonden aan enorme aantallen automatisch gegenereerde e-mailadressen. Als u reageert op een spambericht, weet de verzender dat uw adres actief is; u krijgt dan gegarandeerd nog veel meer ongewenste elektronische post.

Gebruik veilige wachtwoorden

Voor de toegang tot sommige toepassingen en informatie is een wachtwoord vereist. Een veilig wachtwoord bestaat uit minstens acht tekens, bij voorkeur een mix van cijfers, hoofdletters en kleine letters. U kunt ook leestekens gebruiken. Gebruik verschillende wachtwoorden en verander ze geregeld.

Klik niet op links in e-mails

Links in e-mails worden vaak gebruikt om nietsvermoedende gebruikers naar een valse website te leiden die een kopie is van een echte website. Via de valse website probeert men dan vertrouwelijke gegevens van de gebruiker te bemachtigen, zoals kredietkaartgegevens of wachtwoorden. Deze malafide techniek heet 'phishing'. Vermijd phishing door adressen van dergelijke websites grondig te verifiëren en vervolgens de u bekende adressen zelf in uw browser in te voeren.

Gebruik een antivirusprogramma dat dagelijks wordt bijgewerkt

Ga altijd na of gedownloade of ontvangen programma's en bestanden veilig zijn alvorens u ze de eerste keer opent. Maak daarbij gebruik van een antivirusprogramma dat real-timebescherming biedt en dat voortdurend wordt geüpdatet.

Installeer de veiligheidspatches

Alle veiligheidspatches voor het besturingssysteem en voor toepassingen moeten geïnstalleerd worden zodra ze beschikbaar zijn.

Verstuur geen vertrouwelijke informatie via e-mail

Verstuur nooit vertrouwelijke informatie, zoals kredietkaartgegevens of wachtwoorden, via e-mail. Bonafide bedrijven vragen nooit via e-mail om dergelijke informatie. Zelfs als u naar een onverdachte bron mailt, is het geen goed idee om vertrouwelijke informatie in uw e-mail op te nemen. E-mails kunnen immers gemakkelijk onderschept worden.

Wees voorzichtig met automatische antwoorden

Zogenaamde out-of-officeberichten geven informatie prijs die nuttig kan zijn voor hackers en spammers. Een automatisch bericht dat vermeldt wanneer u met vakantie bent, bevat interessante informatie voor inbrekers en dieven.

Wees voorzichtig met peer-to-peernetwerken en uitwisselingssoftware

Gebruikers van chatboxen op het internet, instant messaging en tools om bestanden te delen in een P2P-netwerk moeten op hun hoede zijn voor de links en de programma's die worden uitgewisseld. Niet alleen bestaat de kans dat u de wet op het auteursrecht schendt, ook bevatten veel aangeboden bestanden virussen of Trojaanse paarden. Peer-to-peersoftware kan ook spyware, ongewenste adware of beveiligingslekken bevatten.

Meer veiligheidsadviezen op www.cert.be

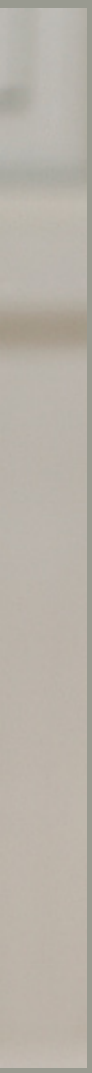
Uit het klantentevreden-heidsonderzoek van 2008 is gebleken dat al onze klanten tevreden tot uiterst tevreden zijn en dat meer dan 41 % ons al meer dan eens heeft aanbevolen.

INNOVATIE

EXPERTISE

AAN HET WOORD

Henri Malcorps

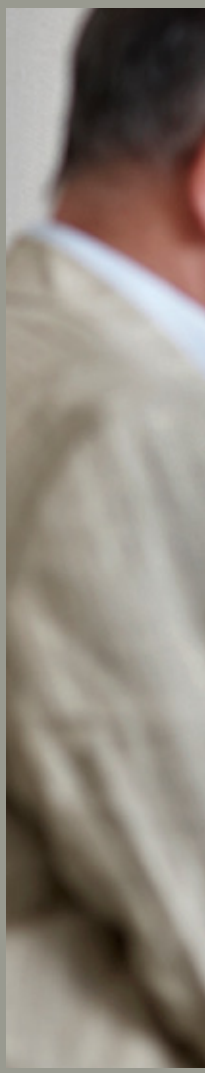


HENRI MALCORPS

ALGEMEEN DIRECTEUR,

KONINKLIJK METEOROLOGISCH INSTITUUT,

OVER BELNET



“Het KMI is waarschijnlijk een van de belangrijkste gebruikers van het BELNET-netwerk. Elk jaar sturen wij meer dan 5.000 weersvoorspellingen en meer dan 100 stormwaarschuwingen naar overheden en diverse gebruikersgroepen. Daartoe moeten we een enorme hoeveelheid informatie verwerken: zo’n 83 miljoen gegevens van waarnemingen in België en zo’n 800.000 radar- en satellietbeelden. En dan zijn er nog de resultaten van numerieke modellen en de gegevens die we uitwisselen met onze buitenlandse collega’s.

Om alles te kunnen verwerken en versturen, hebben we een krachtig netwerk nodig. BELNET weet trouwens ook dat infrastructuur alleen niet volstaat. Het biedt ook veel diensten aan. We werken bijvoorbeeld op het vlak van fijnmazige weervoorspellingen met virtuele teams; daarbij doen we een beroep op het professionele videoconferentiesysteem van BELNET. In de toekomst zullen de federale wetenschappelijke instellingen, zoals de Koninklijke Bibliotheek of de musea, veel digitaliseren om hun verzamelingen toegankelijker te maken voor het publiek. Dit vraagt een enorme opslagcapaciteit en snelle toegang via het internet. De uitgebreide gegevensbanken van het KMI zouden op deze manier toegankelijk gemaakt kunnen worden, maar dit is geen kerntaak van de instelling. We willen een betrouwbare partner die ons een grote opslagcapaciteit kan garanderen, met veiligheidsgaranties die zijn vastgelegd in duidelijke Service Level Agreements. Het dienstenpakket van BELNET zou daarmee in de toekomst uitgebreid kunnen worden.

BELNET zoekt antwoorden op onze vragen en boezemt ons groot vertrouwen in. Het feit dat ze binnen de federale overheid werken en dezelfde uitdagingen kennen als wij versterkt onze relatie. We zitten op dezelfde golflengte. Het KMI heeft een eigen contactpersoon bij BELNET, die ons opvolgt en waarmee we regelmatig overleggen. Dat we verder de klok rond op support kunnen rekenen en dat het BELNET-team zich voortdurend uitbreidt, stemt ons ook heel tevreden. We weten dat de continuïteit gegarandeerd is en zijn echt in de wolken met een partner als BELNET.”

"We zijn in de wolken met een partner als BELNET."

HET KONINKLIJK METEOROLOGISCH INSTITUUT (KMI)
IS EEN FEDERAAL WETENSCHAPPELIJK INSTITUUT DAT INFORMATIE
OVER HET WEER VERZAMELT, ANALYSEERT EN VERSPREIDT.

1.

KLANTEN EN GEBRUIKERS

Eind 2009 waren 193 organisaties aangesloten op het BELNET-netwerk, waaronder alle Belgische hogescholen en universiteiten, een aantal overheidsinstellingen, onderzoeksafdelingen van private ondernemingen, en internationale organisaties. In totaal deden bijna dagelijks ongeveer 700.000 eindgebruikers een beroep op het BELNET-netwerk.

1.1 ONDERWIJS EN ONDERZOEK

Sinds 2008 maken alle Belgische hogescholen en universiteiten gebruik van het BELNET-netwerk en de BELNET-diensten. Tot deze groep behoren erg grote instellingen, zoals het netwerk van Enseignement de la Province de Liège, de Universiteit Gent en de Katholieke Universiteit Leuven (elk met meer dan 40.000 eindgebruikers). Maar BELNET levert zijn diensten ook aan tal van kleinere instellingen, bijvoorbeeld gespecialiseerde publieke of private researchcentra met slechts een tiental medewerkers. Ook de federale wetenschappelijke instellingen zijn klant bij BELNET.

1.2 ANDERE KLANTEN EN GEBRUIKERS

Tot de klanten van BELNET behoren verder een aantal federale, regionale en lokale overheden. Voor de federale overheid zette BELNET het FedMAN-netwerk op. In 2009 bereidde BELNET zich voor op de ontwikkeling van FedMAN3. Als beheerder van BNIX (Belgian National Internet eXchange) werkt BELNET ook voor private internetaanbieders op de Belgische markt. Via BNIX houden wij het internetverkeer in België snel, veilig en betaalbaar. Eind 2009 waren 44 organisaties – hoofdzakelijk aanbieders van internetdiensten en content – aangesloten op BNIX. Er werd in 2009 ook gestart met de vernieuwing van het BNIX-platform.

1.3

BELNET CUSTOMER SURVEY

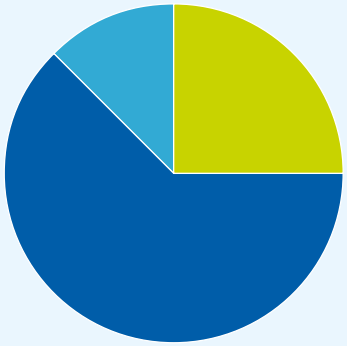
Begin 2009 publiceerde BELNET de resultaten van een grootschalig klantentevredenheidsonderzoek dat werd uitgevoerd in het laatste kwartaal van 2008. We onderzochten zowel de tevredenheid bij onze gebruikers als het belang dat zij hechtten aan diverse aspecten van onze dienstverlening als de mate waarin gebruikers bereid zijn om onze diensten aan te bevelen. Uit het onderzoek bleek dat onze klanten tevreden (25 %), zeer tevreden (62,5 %) tot uiterst tevreden (12,5 %) zijn.
De combinatie van lage kostprijs, hoge bandbreedte en grote bedrijfszekerheid waarderen onze klanten heel erg. Klanten staan positief tegenover BELNET en zijn bereid ons aan te raden. Punten voor verbetering werden geanalyseerd en opgenomen in een actieplan dat werd uitgevoerd in 2009. Begin 2010 werd een nieuw onderzoek gelanceerd om de werkelijke verbeteringen te meten.

1.4

BELNET-CONFERENTIES, BELNET-WORKSHOPS EN WEBSITE

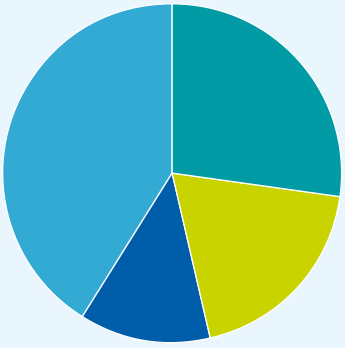
BELNET nam verschillende initiatieven om klanten en gebruikers te informeren over zijn diensten, om de diensten meer toegankelijk te maken, en om gebruikers te helpen om de diensten maximaal te benutten. Inmiddels klassieke evenementen in dit verband, zoals de BELNET Workshops en de BELNET Networking Conference, werden ook in 2009 georganiseerd. Op de conferentie en tijdens de workshops worden ideeën en ervaringen uitgewisseld, en de gebruikers kunnen er BELNET-medewerkers ontmoeten en kennismaken met nieuwe ontwikkelingen. De BELNET Networking Conference 2009 was met 180 deelnemers een succes. In de voormiddag werden de recentste evoluties in e-technologieën en de rol van een onderzoeks- en onderwijsnetwerk belicht, met nadruk op het innovatieve gebruik ervan binnen hoger onderwijs en onderzoekscentra. Er werd ook over de grenzen heen gekeken, onder meer naar de impact van onderzoeksnetwerken in technologiearme landen. In de namiddag werden praktische voorbeelden en toepassingen gepresenteerd en kwamen nieuwe BELNET-diensten aan bod. In 2009 organiseerden we ook een tweede conferentie, de BELNET Security Conference. Daarnaast hebben we de informatie over onze diensten verbeterd, onder meer door onze website te herwerken. De nieuwe website werd in januari 2010 gelanceerd.

TEVREDENHEID VAN DE BELNET-GEBRUIKER



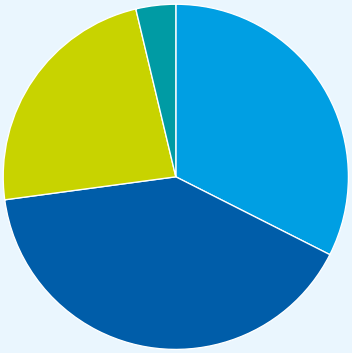
Uiterst tevreden	12,50 %
Zeer tevreden	62,50 %
Tevreden	25,00 %
Weinig tevreden	0 %
Niet tevreden	0 %

GEBRUIKERS DIE BELNET IN DE 6 MAANDEN VOOR HET TEVREDENHEIDSONDERZOEK HEBBEN AANBEVOLEN



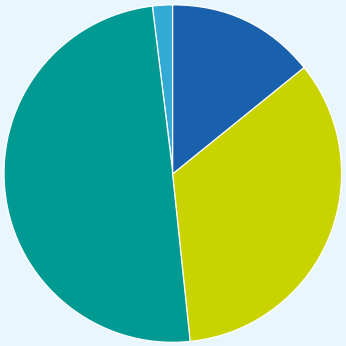
Heeft het al meer dan eens gedaan	41,10 %
Heeft het één keer gedaan	12,50 %
Heeft het nog niet gedaan, maar gaat het zeker doen in de toekomst	19,00 %
Heeft het nog niet gedaan, maar zou het zeker doen als iemand erom vraagt	27,40 %
Heeft het nog niet gedaan en zou het zeker ook niet doen	0 %

AANTAL INSTELLINGEN PER KLANTENGROEP, EIND 2009



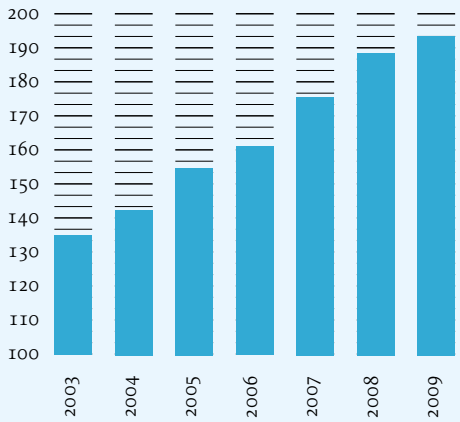
Onderzoek	66	34,20 %
Hoger onderwijs [inclusief universiteiten]	76	39,38 %
Overheid en administraties	43	22,27 %
Regionale netwerken	8	4,15 %
Totaal	**193**	**100,00 %**

VERDELING VAN DE AANSLUITINGEN VOLGENS TOEGANGSCAPACITEIT



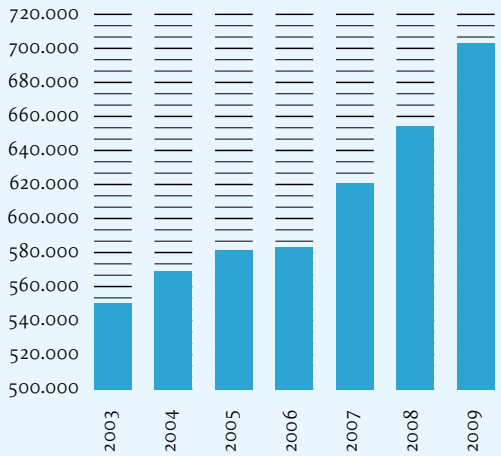
	Aantal actieve aansluitingen	Aantal back-up-aansluitingen	Mbps	% van het totaal
10 Mbps Ethernet	34	6	400	14,43 %
100 Mbps Fast Ethernet	81	13	9.400	33,94 %
1 Gbps Ethernet	121	17	138.000	49,82 %
10 Gbps Ethernet	4	1	50.000	1,81 %
Totaal	**240**	**37**	**197.800**	**100,00 %**

AANTAL KLANTEN EN GROEI IN % TEGENOVER VOORGAAND JAAR



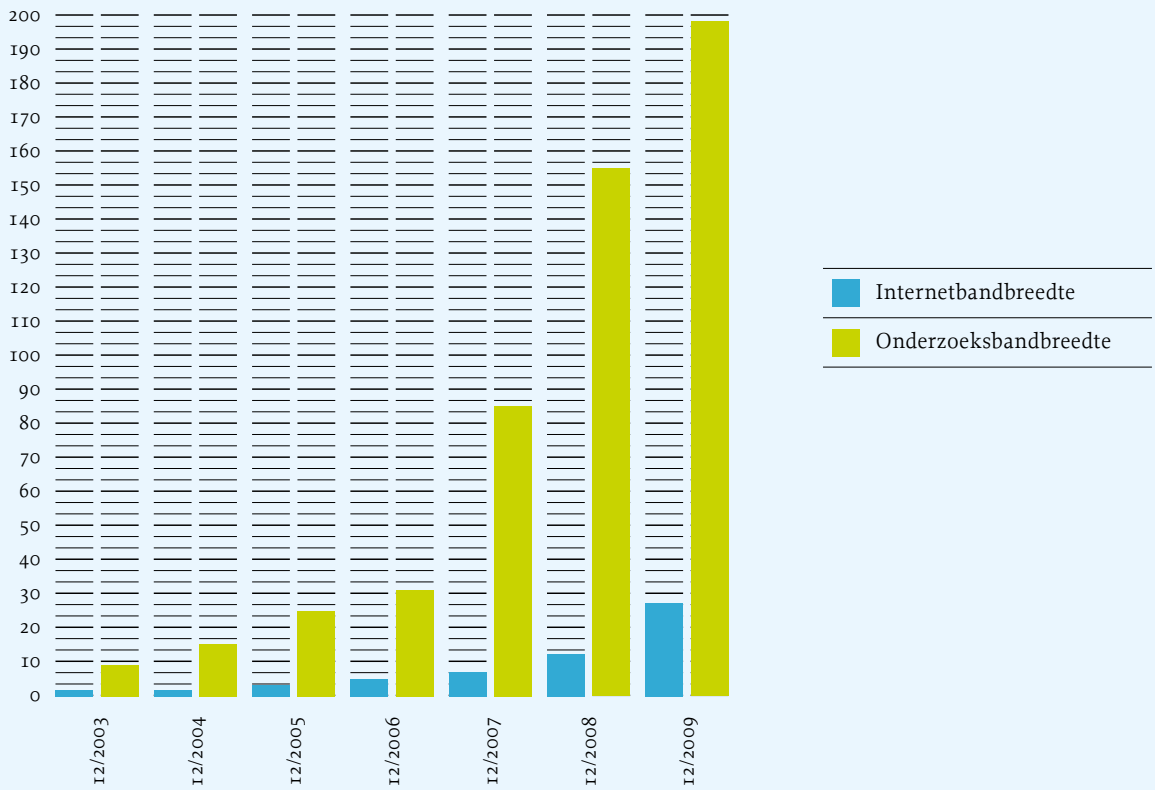
2003	135	
2004	142	5,19 %
2005	155	9,15 %
2006	161	3,87 %
2007	176	9,32 %
2008	188	6,82 %
2009	**193**	**2,66 %**

AANTAL EINDGEBRUIKERS EN GROEI IN % TEGENOVER VOORGAAND JAAR



2003	550.000	
2004	575.000	4,55 %
2005	584.000	1,57 %
2006	585.600	0,27 %
2007	620.100	5,89 %
2008	655.600	5,72 %
2009	**700.374**	**6,83 %**

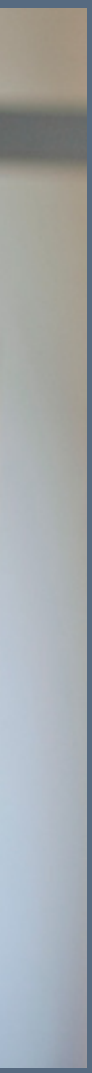
EVOLUTIE VAN DE TOTALE TOEGANGSCAPACITEIT VAN BELNET-KLANTEN, IN GBPS



BELNET neemt voortdurend initiatieven om klanten en gebruikers te informeren over de bestaande diensten en peilt naar de behoeften om vervolgens nieuwe diensten te ontwikkelen.

AAN HET WOORD

Wim Pouseele



WIM POUSEELE

IT INFRASTRUCTUUR MANAGER,

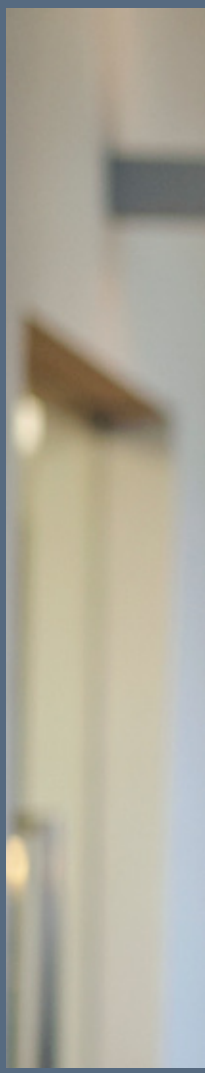
VLERICK LEUVEN GENT MANAGEMENT SCHOOL,

OVER BELNET

“De samenwerking met BELNET begon toen we in Gent naar een andere campus verhuisden. De jaren nadien zijn we voor meer en meer diensten bij hen gaan aankloppen, zoals voor onze intercampusconnectie tussen Gent en Leuven. Vroeger hadden we voor het intercampusverkeer een eigen VPN-connectie, maar nu zit alles bij BELNET. Dat betekent dat we de connectie niet meer zelf moeten beheren en dat we geen eigen investeringen in hardware meer hoeven te doen.

We maken ook veel gebruik van de dienst Videoconferencing van BELNET. Voor videoconferencing tussen twee toestellen op onze campussen hebben we een eigen oplossing, maar zodra er een derde partij bij komt, is Videoconferencing van BELNET absoluut noodzakelijk. Zonder dat systeem zouden we zelf al het materiaal moeten kopen en complexe firewalls moeten opzetten. Nu is dat allemaal niet nodig. Onze medewerkers en studenten gebruiken de dienst verschillende keren per week. Ook onze Board of Directors gebruikt Videoconferencing bij overleg tussen Leuven, Gent en Sint-Petersburg. Dat loopt goed: we kunnen bij BELNET een reservatie maken en daarna direct starten.

Basisdiensten als DNS-registratie en certificering zijn ook heel belangrijk voor ons. Met die diensten kunnen we hier de overload beperken. Ook een goed punt is de invoering van de 24/7-helpdesk. Voordien was het soms lastiger om een probleem op te lossen. Je kan je eigenlijk geen betere provider wensen. Eigenlijk is BELNET ook veel meer dan een provider. De BELNET-medewerkers denken mee, zoeken mee naar oplossingen en zijn niet bang om serieuze inspanningen te leveren. Ik ben heel tevreden.”



"De BELNET-medewerkers denken mee, zoeken mee naar oplossingen en zijn niet bang van serieuze inspanningen."

WIM POUSEELE IS VERANTWOORDELIJK VOOR DE IT-INFRASTRUCTUUR EN DE IT-VEILIGHEID VAN DE VLERICK LEUVEN GENT MANAGEMENT SCHOOL.

2.

NIEUWE EN VERBETERDE DIENSTEN

De evolutie van netwerkprovider naar dienstenleverancier is bij BELNET al enkele jaren aan de gang en werd in 2009 verdergezet. Onze klanten en gebruikers beschikken allemaal over ruim voldoende bandbreedte, maar hebben nu vooral nood aan nieuwe diensten die hun werk vergemakkelijken en verbeteren. BELNET peilt naar de behoeften en ontwikkelt vervolgens de gepaste diensten. Ook werken wij voortdurend aan de verbetering van bestaande diensten. Kortom, 2009 stond in het teken van tal van voorbereidende acties voor een uitgebreider en beter dienstenaanbod.

2.1 BELNET R&E FEDERATIE

BELNET startte in 2009 met de voorbereidingen van een federatie van universiteiten en dienstenleveranciers. Een gebruiker van een instelling die tot die federatie behoort, zal met zijn eigen gebruikersnaam en wachtwoord in real time toegang krijgen tot bepaalde diensten van een dienstenleverancier van de federatie. Hij hoeft zich dus niet tweemaal te registreren noch zich met verschillende authenticatiegegevens aan te melden. BELNET treedt binnen de federatie op als centraal aanspreekpunt, maar de gegevens van de gebruikers blijven bij de instellingen zelf. Op die manier zijn alle gegevens altijd actueel en kan de privacy van de gebruikers het best gerespecteerd worden.

2.2 DIGITAL CERTIFICATES SERVICE

BELNET verbeterde in 2009 zijn systeem van digitale certificaten. Wij zijn gemachtigd om certificaten voor servers en DNS-namen uit te reiken, waarmee netwerken en servers beschermd worden. De digitale certificaten zijn enkel beschikbaar voor erkende onderzoekscentra, universiteiten en hogescholen die zijn aangesloten op het BELNET-netwerk. De toewijzing ervan gebeurt volgens de regels van TERENA, de vereniging van Europese onderzoeksnetwerken. Er werden in 2009 767 certificaten uitgereikt.

2.3
VULNERABILITY SCANNER

De Vulnerability Scanner van BELNET spoort zwakke schakels in het netwerk van een gebruiker op en signaleert potentiële bedreigingen en kwetsbaarheden. De Vulnerability Scanner verhindert geen aanvallen, maar maakt het mogelijk de beveiliging van het netwerk in kwestie beter te evalueren. De aanzet voor een verbeterde en meer uitgebreide versie van de Vulnerability Scanner – met support ter plaatse – werd in 2009 gegeven.

2.4
VIDEOCONFERENCING

Door de toenemende internationalisering van onderwijs en onderzoek blijft het aantal videoconferenties stijgen. De BELNET-videoconferentiedienst werd in 2008 al 332 keer gebruikt, in 2009 steeg dat aantal tot 637. Wij verbeterden ons systeem voor MCU-Videoconferencing. De Multipoint Control Unit (MCU) stelt gebruikers in staat om een videoconferentie van hoge kwaliteit met meer dan twee geografisch verspreide partijen op te zetten. De beelden worden uitgewisseld via het BELNET-netwerk.

2.5
E-COLLABORATION PLATFORM

In 2009 testte BELNET een nieuw E-collaboration Platform, een virtuele ontmoetingsruimte voor medewerkers, studenten en docenten. Met behulp van een gebruiksvriendelijke webtool kunnen op eender welk moment en vanop eender welke locatie online lessen en virtuele vergaderingen opgezet worden. Het systeem is eenvoudiger dan videoconferencing maar zeer flexibel. Men kan bijvoorbeeld ook toegang tot de eigen computer verlenen en gemakkelijk documenten uitwisselen. Een computer, een webcam en een headset volstaan om ermee te werken. Deze dienst ging begin 2010 van start als een pilootproject.

2.6
BELNET-HUURLIJN

Sommige BELNET-klanten kunnen enkel via een afzonderlijke huurlijn op het BELNET-netwerk. Tot voor kort moesten ze voor die huurlijn een beroep doen op een derde partij. In 2008 besloot BELNET een gedetailleerde studie uit te voeren naar de mogelijkheden om klanten connectiviteit met een huurlijn in één pakket aan te bieden. In het eerste kwartaal van 2009 werd deze dienst gelanceerd. BELNET-klanten hoeven sindsdien geen aparte leverancier meer te zoeken; ze betalen door het schaalvoordeel dat BELNET biedt in de meeste gevallen een lagere prijs. In de eerste helft van 2009 bezorgde BELNET al meteen een twintigtal klanten een huurlijn.

2.7

STANDAARDPAKKET EN PLUS-DIENSTEN

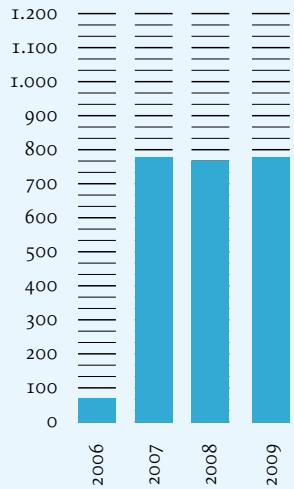
BELNET bracht zijn diensten onder in een standaardpakket en een reeks optionele Plus-diensten. Deze indeling is officieel ingevoerd begin 2010. Het standaardpakket omvat de aansluiting en een aantal extra diensten waarvoor de klant niets hoeft bij te betalen. Het bestaat uit:

- Connectiviteit
- IP-adressering (zowel IPv4 als IPv6)
- DNS-diensten
- Kloksynchronisatie
- Softwarearchief
- Bandbreedtestatistieken
- BELNET CERT
- 24/7 helpdesk
- Support en advies
- Workshops en conferenties

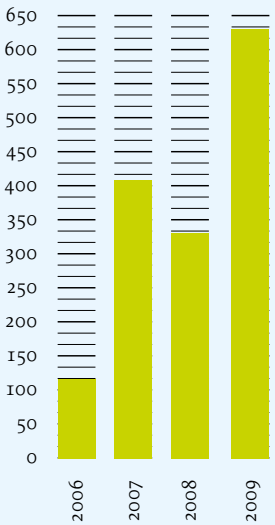
Met de BELNET Plus-diensten kan de gebruiker het comfort, de veiligheid en de bedrijfszekerheid van zijn aansluiting verder verhogen. Plus-diensten zijn onder meer:

- Back-up connectiviteit
- IPv6 connectiviteit
- Multicast
- Domeinnaamregistratie
- Instant Messaging
- Digital Certificates Service
- Vulnerability Scanner
- Videoconferencing
- BEgrid
- eduroam
- BELNET-huurlijn
- E-collaboration Platform
- Interconnectiviteitsdienst

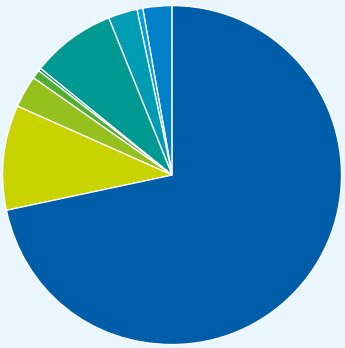
DIGITAL CERTIFICATES SERVICE – AANTAL AFGELEVERDE CERTIFICATEN SINDS DE START IN 2006



VIDEOCONFERENCING – AANTAL SESSIES

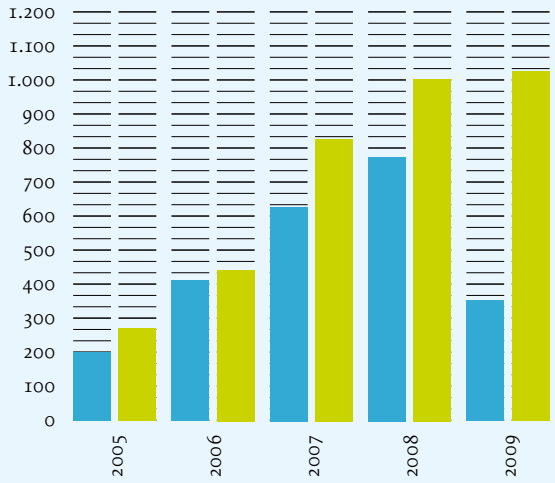


BELNET CERT – INCIDENTEN PER TYPE IN 2009



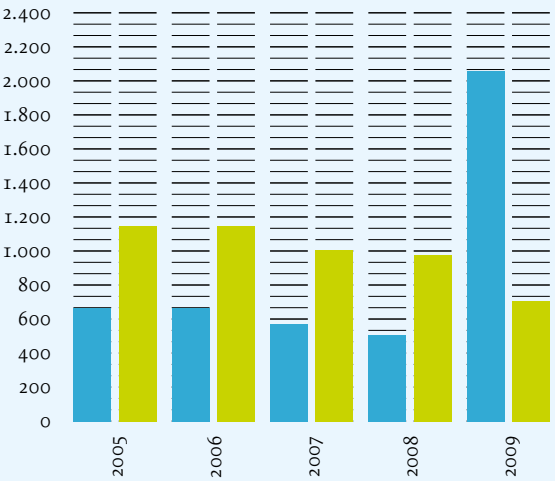
Spam	1.333
System compromise	184
Query	56
Scan	16
Denial of service	1
Piraterij	150
Virussen/wormen	51
Phishing	3
Andere	50

BEGRID – GRIDCOMPUTING



Aantal certificaten	354
Aantal CPU's	1.016

BELNET CERT – WAARSCHUWINGEN EN VEILIGHEIDSADVIEZEN

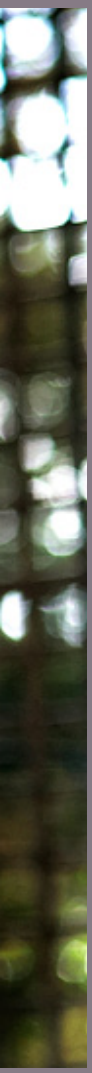


Aantal waarschuwingen	2.074
Aantal veiligheidsadviezen	717

BELNET beheert het FedMAN-netwerk, dat de basis vormt voor alle e-government-toepassingen in België. Het werd in 2009 onder meer geschikt gemaakt voor IPv6.

AAN HET WOORD

Peter Strickx



PETER STRICKX

TECHNOLOGISCH DIRECTEUR

BIJ FEDICT, OVER BELNET

"In 2001 hadden we bij de federale overheidsdiensten een eerder primitief netwerk, maar het jaar nadien veranderde dat. We hadden voor e-government een betrouwbaar en krachtig netwerk nodig en klopten aan bij BELNET. BELNET had met zijn eigen onderzoeksnetwerk al veel ervaring en was daarom voor ons een logische keuze. Er zitten bij de organisatie heel wat competente mensen. En BELNET is zelf een overheidsdienst, wat de samenwerking vanzelfsprekend een stuk makkelijker maakt.

De bandbreedte en de betrouwbaarheid van ons netwerk zijn er dankzij BELNET fors op vooruitgegaan. We halen nu 1 gigabit per seconde, terwijl de snelheid in 2001 bij sommige diensten nog tussen 192 en 512 kbps was. Dat is een verbetering met een factor 5.000. Ook de betrouwbaarheid heeft een enorme evolutie doorgemaakt. Alle aansluitpunten zijn nu via twee onafhankelijke telecomoperatoren aangesloten op het netwerk, wat resulteert in een effectieve beschikbaarheid van 99,99 %. Ook de toegang en de informatieveiligheid zijn sterk verbeterd. Vroeger had elke overheidsdienst zijn eigen internetverbinding en stond alles los van mekaar. Nu verbindt het FedMAN-netwerk alle federale overheidsdiensten en is er één enkele gemeenschappelijke, snelle en beveiligde toegangspoort tot het internet.

In 2006 startte BELNET de tweede fase van het FedMAN-netwerk. Een belangrijk testproject in dat verband is de overgang van IPv4 naar IPv6. Door de groei van het internet dreigt er een tekort aan IP-adressen, en dat lost IPv6 definitief op. Met dit project kijkt BELNET niet de kat uit de boom, maar loopt het voor op de zaken. Contracten in de telecomwereld duren al snel enkele jaren en dan moet je op lange termijn kunnen denken. BELNET doet dat. Door die proactiviteit, die innovatie en die expertise speelt BELNET, als partner van Fedict, een sleutelrol bij het realiseren van een 'virtual connected government'."

"BELNET speelt een sleutelrol bij het realiseren van een virtual connected government."

FEDICT IS VERANTWOORDELIJK VOOR DE IMPLEMENTATIE EN DE ONDERSTEUNING VAN E-GOVERNMENT IN ONS LAND.

3.

NETWERKEN EN GRIDS

BELNET beheert drie fysiek gescheiden netwerken: BELNET, BNIX en FedMAN. De optische infrastructuur van het BELNET-netwerk die in 2008 in gebruik werd genomen, heeft zich het voorbije jaar sterk bewezen, onder meer als facilitator van de Vlaamse supercomputer en als fundament van BEgrid. De aanzet tot de vernieuwing van BNIX werd in 2009 gegeven. Een vernieuwing van het FedMAN-netwerk vanaf 2011 werd reeds voorbereid.

3.1 BELNET

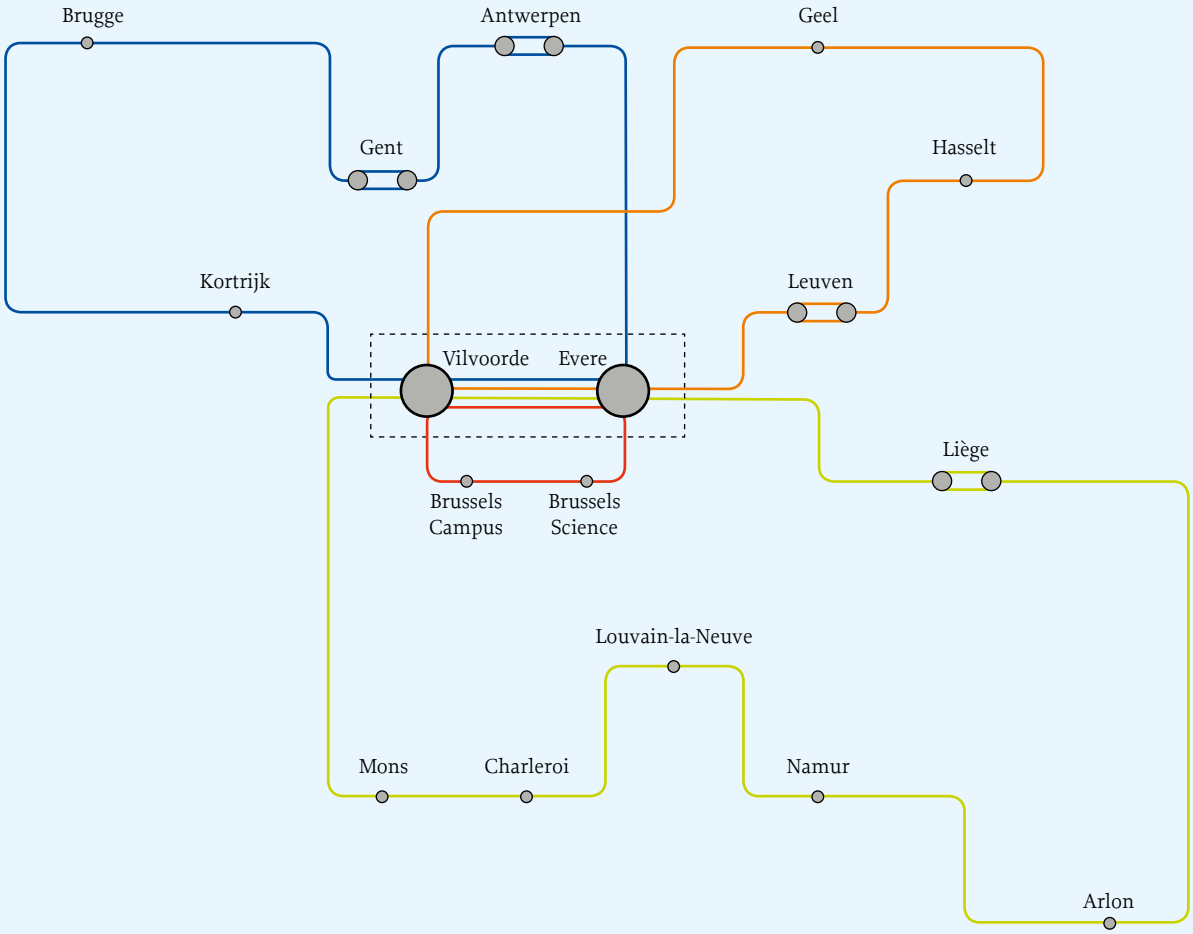
Het BELNET-netwerk dat in 2008 in gebruik werd genomen, is hyperstabiel en van een hoge kwaliteit en levert uitstekende prestaties. Het netwerk verenigt alle Belgische universiteiten en hogescholen in één hoogtechnologische omgeving. Het uitbaten ervan blijft wel een dynamisch proces. Een deel van het netwerk werd in 2009 verbeterd, onder meer door een aantal netwerkversterkers te vervangen. Om het dataverkeer van en naar onze klanten via de meest kwaliteitsvolle weg te kunnen leiden, is BELNET in 2009 ook begonnen met een nieuw project rond netwerkanalyse en -beveiliging. BELNET wil verder de centrale optische ring van het netwerk in Brussel door twee bijkomende carrierneutrale datacentra laten lopen en begon dit project in 2009 voor te bereiden.

3.2 FEDMAN

Sinds 2001 is BELNET verantwoordelijk voor het ontwerp, de implementatie, het beheer, de ontwikkeling en de ondersteuning van het FedMAN-netwerk. Dit netwerk van de federale overheid is de basis waarop alle Belgische e-governmenttoepassingen gebouwd zijn. In 2009 voerde BELNET op eigen initiatief of in opdracht van Fedict verschillende projecten uit.

- FedMAN werd geschikt gemaakt voor IPv6. Deze nieuwste versie van het Internet Protocol (IP) lost het probleem van het beperkte aantal IPv4-adressen op.
- Een aantal overheidsinstellingen kregen een hogere bandbreedtecapaciteit van 100 Mbps toegewezen.
- De procedure om de Federal Computer Crime Unit (FCCU) op het FedMAN-netwerk aan te sluiten werd opgestart.
- BELNET stond in voor de connectiviteit van het Federaal Agentschap voor de Veiligheid van de Voedselketen (FAVV) tijdens de verhuizing van dit agentschap.
- De aansluitingen van de FOD Economie werden ontdubbeld.
- BELNET werkte een businesscase uit voor het toekomstige FedMAN3-netwerk.

HET BELNET-NETWERK



Met het BELNET-netwerk is datacommunicatie via lichtpaden mogelijk. Lichtpaden zijn directe optische verbindingen tussen twee punten zonder tussenkomst van routers. Een hoge capaciteit, kwaliteit en betrouwbaarheid zijn de belangrijkste troeven.

3.3

BNIX

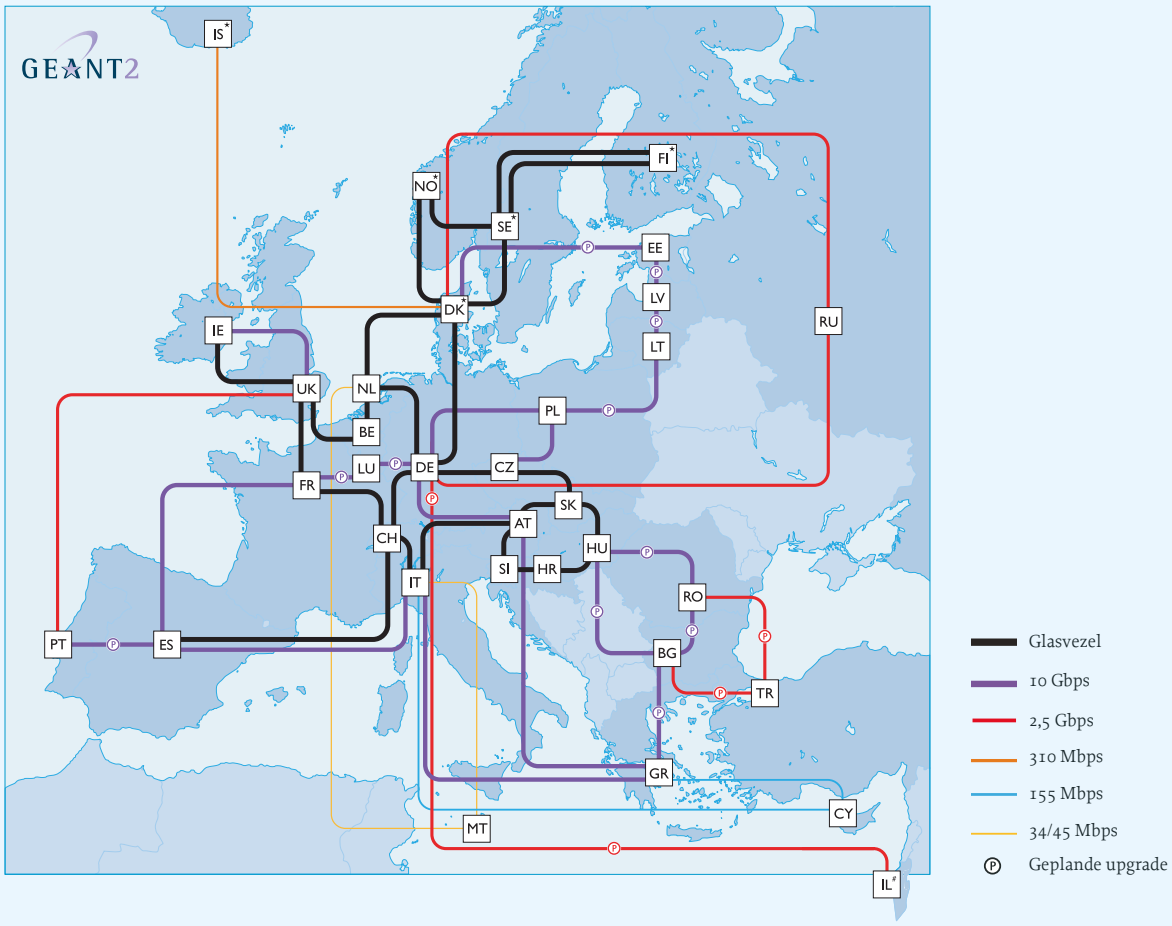
Het BNIX-platform (Belgian National Internet eXchange) is een fysiek platform dat IP-netwerken van Belgische internetaanbieders, contentproviders en andere bedrijven met mekaar verbindt, waardoor het lokale internetverkeer in ons land sneller, veiliger en goedkoper kan verlopen. BNIX helpt BELNET de tarieven voor zijn klanten laag te houden. BELNET baat het platform uit en begon in 2009 de vernieuwing ervan voor te bereiden, vooral om te kunnen inspelen op toekomstige evoluties.

3.4

INTERNATIONALE NETWERKTOEGANG EN SAMENWERKING

Het BELNET-netwerk is verbonden met internationale onderzoeksnetwerken, wat de internationale samenwerking tussen onderwijs- en onderzoeksinstellingen bevordert. Het BELNET-netwerk maakt deel uit van het Europese onderzoeksnetwerk Géant2 en biedt toegang tot andere onderzoeksnetwerken, zoals het Amerikaanse Internet2-netwerk. Verder is BELNET lid van TERENA, de Europese vereniging van onderzoeks- en onderwijsnetwerken. Op de TERENA Conference van 2009 zette BELNET zijn visie over de aanpak van een Network Operations Center (NOC) en de procedures van een NOC uiteen. Deze uiteenzetting bracht heel wat discussie teweeg en leidt mogelijk tot een internationale NOC Task Force.

HET GÉANT2-NETWERK



Het BELNET-netwerk is verbonden met de grote internationale onderzoeksnetwerken. Samen vormen ze het Géant2-netwerk.

De kern van het netwerk bestaat uit meervoudige 10 Gbps-aansluitingen. Deze worden grotendeels door glasvezelverbindingen tot stand gebracht.

3.5

VLAAMS SUPERCOMPUTER CENTRUM (VSC)

Het BELNET-netwerk heeft nieuwe toepassingen mogelijk gemaakt, zoals de Vlaamse supercomputer, een cluster van computers op verschillende locaties, die nu via ons netwerk aan elkaar geschakeld zijn. Het Vlaams Supercomputer Centrum maakt gebruik van speciaal toegewezen 10 Gbps-lijnen via lichtpaden. Het is een samenwerking van vijf Vlaamse academische associaties: de Associatie K.U.Leuven, de Associatie Universiteit Gent, de Universitaire Associatie Brussel, de Associatie Universiteit & Hogescholen Antwerpen en de Associatie Universiteit-Hogescholen Limburg. Het VSC wordt gefinancierd door het departement Economie, Wetenschap en Innovatie van de Vlaamse overheid.

3.6

BEGRID

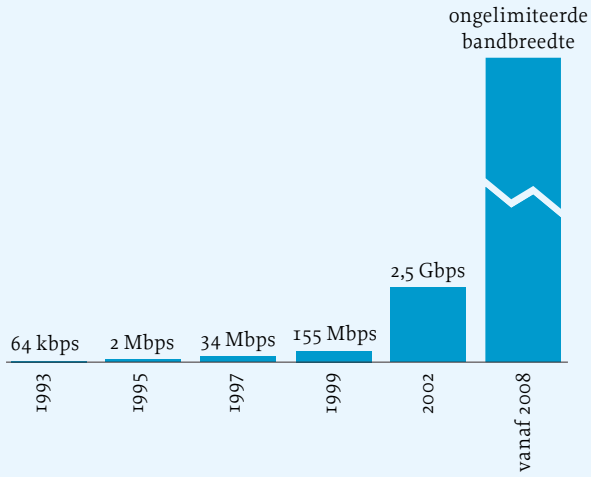
BEgrid is een verzameling computerprocessoren (CPU's) die door het BELNET-netwerk met elkaar verbonden zijn en die samen een enorme rekencapaciteit aanbieden. In 2009 bestond BEgrid uit 1.016 CPU's. Voor sommige experimenten kan ook op het Nederlandse gridsysteem een beroep gedaan worden, wat het aantal CPU's verhoogt tot 4.952. BELNET levert de nodige certificaten af aan klanten die willen gebruikmaken van de rekencapaciteit van BEgrid. In 2009 waren dat er 354.

3.7

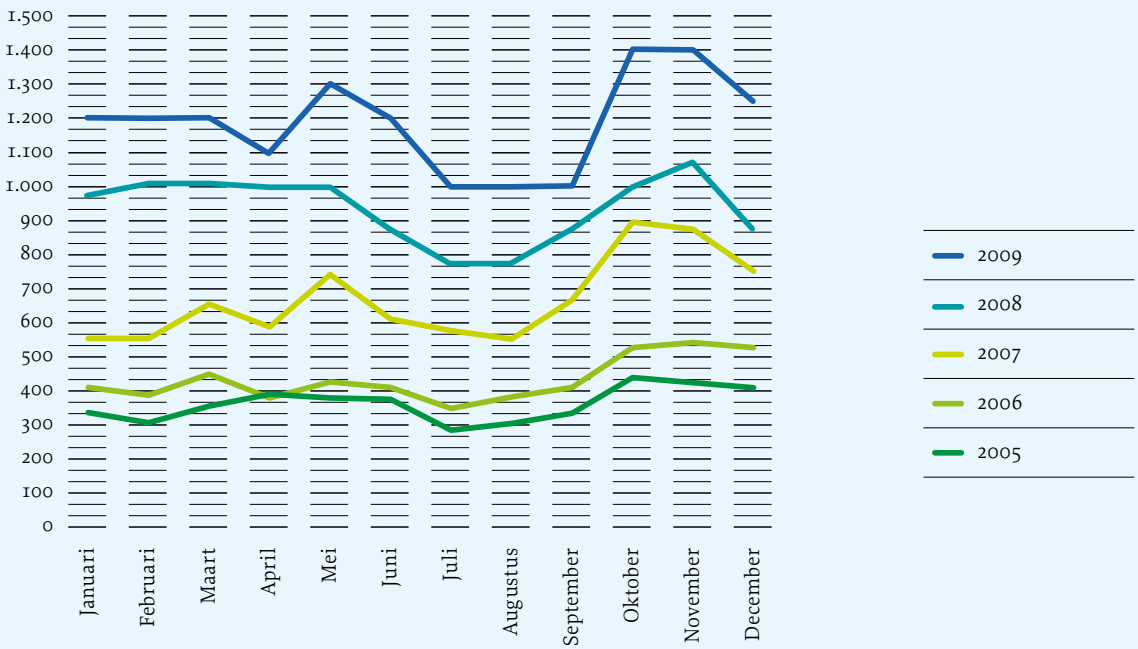
EUROPEAN GRID INITIATIVE

BELNET vertegenwoordigt sinds 2009 België bij het European Grid Initiative (EGI). Het EGI is een consortium dat Europese landen met een gridinfrastructuur samenbrengt, met het oog op meer samenwerking over de landsgrenzen heen. Per land wordt slechts één partner toegelaten.

EVOLUTIE VAN DE BACKBONEBANDBREEDTE SINDS 1993



HET BELNET-NETWERK – EVOLUTIE VAN DE EXTERNE TRAFIEK, IN TERABYTE (TB) PER MAAND



HET BELNET-NETWERK – CUSTOMER TROUBLE TICKETS IN 2009

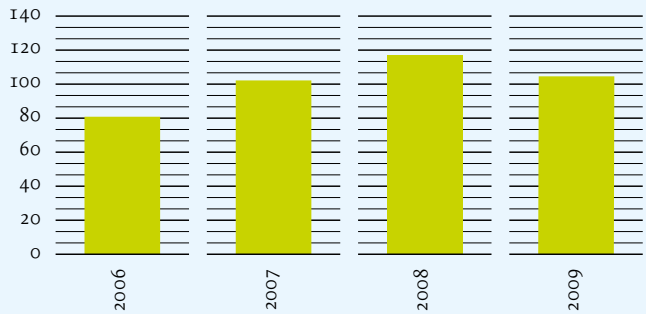
Type	Jan	Feb	Maart	April	Mei	Juni	Juli	Aug	Sept	Okt	Nov	Dec
S1	0	0	0	0	0	0	0	2	0	1	0	0
S2	5	0	4	2	2	4	6	5	16	5	7	4
S3	19	9	15	16	16	13	5	6	34	18	16	13
S4	2	1	7	4	2	7	4	7	1	8	8	2
Totaal	**26**	**10**	**26**	**22**	**20**	**24**	**15**	**20**	**51**	**32**	**31**	**19**

HET BELNET-NETWERK – SURVEILLANCE AND FAULT MANAGEMENT

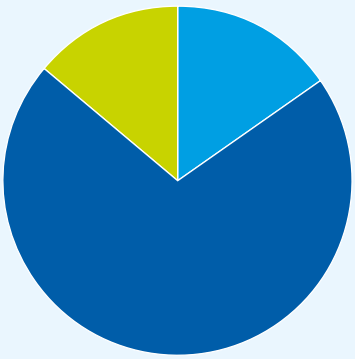
Type	Jan	Feb	Maart	April	Mei	Juni	Juli	Aug	Sept	Okt	Nov	Dec
S1	0	0	1	1	0	0	0	0	0	0	0	0
S2	18	15	26	20	13	22	11	13	20	10	7	6
S3	7	9	12	18	17	19	25	17	10	20	7	6
S4	4	2	2	1	2	8	4	3	2	10	2	3
Totaal	**29**	**26**	**41**	**40**	**32**	**49**	**40**	**33**	**32**	**40**	**16**	**15**

S1	Volledig backbonefalen. Point of Presence buiten gebruik.
S2	Verminderde werking (met invloed op de dienstverlening)
S3	Probleem met de redundantie, zonder invloed op de dienstverlening
S4	Informatieaanvraag

HET FEDMAN-NETWERK – AANTAL INCIDENTEN

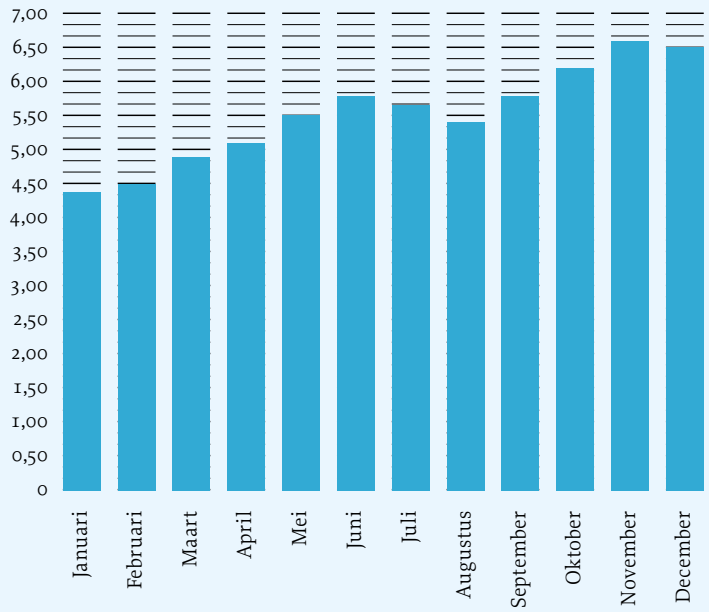


HET BNIX-NETWERK – AANTALLEN EN TYPES AANSLUITINGEN



	2002	2003	2004	2005	2006	2007	2008	**2009**
100 Mbps Fast Ethernet	47	44	38	32	21	20	13	**10**
1 Gbps Ethernet	13	20	28	33	41	44	49	**46**
10 Gbps Ethernet					1	5	7	**9**
Totaal aantal aansluitingen	60	64	66	65	63	69	69	**65**
Klanten			47	46	47	47	44	**44**

HET BNIX-NETWERKVOLUME IN 2009, IN PETABYTE (PB) PER MAAND



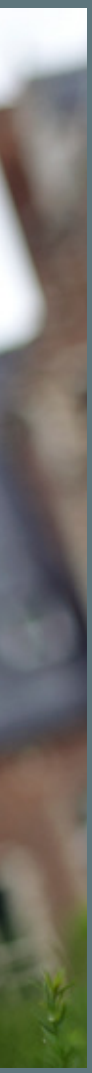
BELNET verhuist in 2010 naar een nieuwe locatie, o.a. om de groei van het aantal medewerkers in de komende jaren op te vangen.

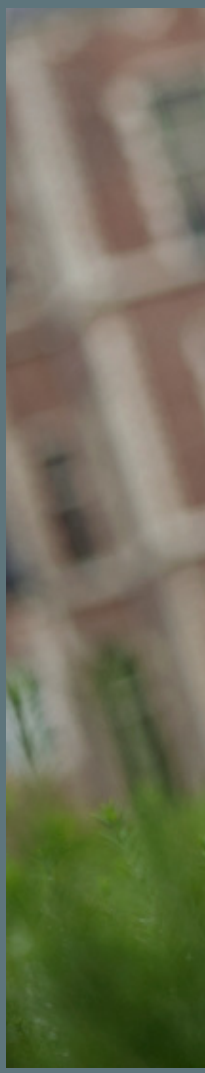
EFFICIENT

PARTNERS

AAN HET WOORD

Herman Moons





HERMAN MOONS

DIENSTHOOFD CENTRALE

ICTS INFRASTRUCTUUR, K.U.LEUVEN,

OVER BELNET

“Ik heb al contact met BELNET van toen ze zich enkel met netwerkinfrastructuur bezighielden. Ik was destijds bij KULeuvenNet verantwoordelijk voor het netwerk. Vroeger was de aanpak van BELNET vooral op de korte termijn gericht en lag de nadruk op de technologie zelf. Vandaag primeren de lange termijn en de dienstverlening. Vooral vanaf 2005 is BELNET diensten met een toegevoegde waarde beginnen aanbieden.

Een mooi voorbeeld is eduroam. Die dienst geeft studenten en onderzoekers via de logingegevens van hun eigen instelling toegang tot netwerken van andere instellingen. Het nieuwste project van BELNET, dat in de lijn van eduroam ligt, is de R & E Federatie (research & education). Een dergelijk systeem wordt al enige tijd intensief gebruikt binnen de Associatie K.U.Leuven, waar het zijn nut reeds heeft bewezen. Een gebruiker van een instelling die tot de federatie behoort, kan met zijn eigen wachtwoord en gebruikersnaam toegang krijgen tot de diensten van een andere instelling van de federatie. Hij hoeft zich geen twee keer te registreren en heeft niet langer meerdere logingegevens nodig. Dit project wordt ondertussen nationaal uitgerold voor andere organisaties en hogescholen, waarbij BELNET instaat voor de overkoepelende diensten.

Een andere dienst met toegevoegde waarde is Digital Certificates Service, voor certificaten die veilige toegang tot websites en internetdiensten garanderen. Vroeger moesten we vanuit de K.U.Leuven die certificaten zelf aanvragen bij instanties als Globalsign of Verisign. Nu zorgt BELNET daarvoor. Het is een extra service die heel handig is. Ze maakt het ons veel gemakkelijker. Bij onze universiteit alleen al hebben we ongeveer zeshonderd van die certificaten.”

"Bij BELNET primeren de lange termijn en de dienstverlening."

HERMAN MOONS IS BIJ DE K.U.LEUVEN
VERANTWOORDELIJK VOOR HET DATACENTER,
HET NETWERK EN DE CENTRALE IT-SYSTEMEN.

4.

ADMINISTRATIE, FINANCIËN & HR

De afdeling Administratie, Financiën & HR staat in voor de boekhouding, het financieel beheer, de rekrutering van personeel, de opvolging van de reglementering van de overheidsopdrachten, het onthaal en andere ondersteunende taken. Zij vervult een belangrijke rol bij de verdere professionalisering van BELNET, onder meer via de ontwikkeling van prestatie-indicatoren voor het personeel.

4.1 DIRECTIE EN BEHEERSCOMMISSIE

BELNET wordt geleid door directeur Pierre Bruyère. Hij wordt bijgestaan door een beheerscommissie. Zij zijn verantwoordelijk voor de uitvoering van het kaderprogramma, de begroting, het investeringsprogramma, de rekeningen, de tarieven, de overheidsopdrachten en de aanwervingen.

4.2 MEDEWERKERS

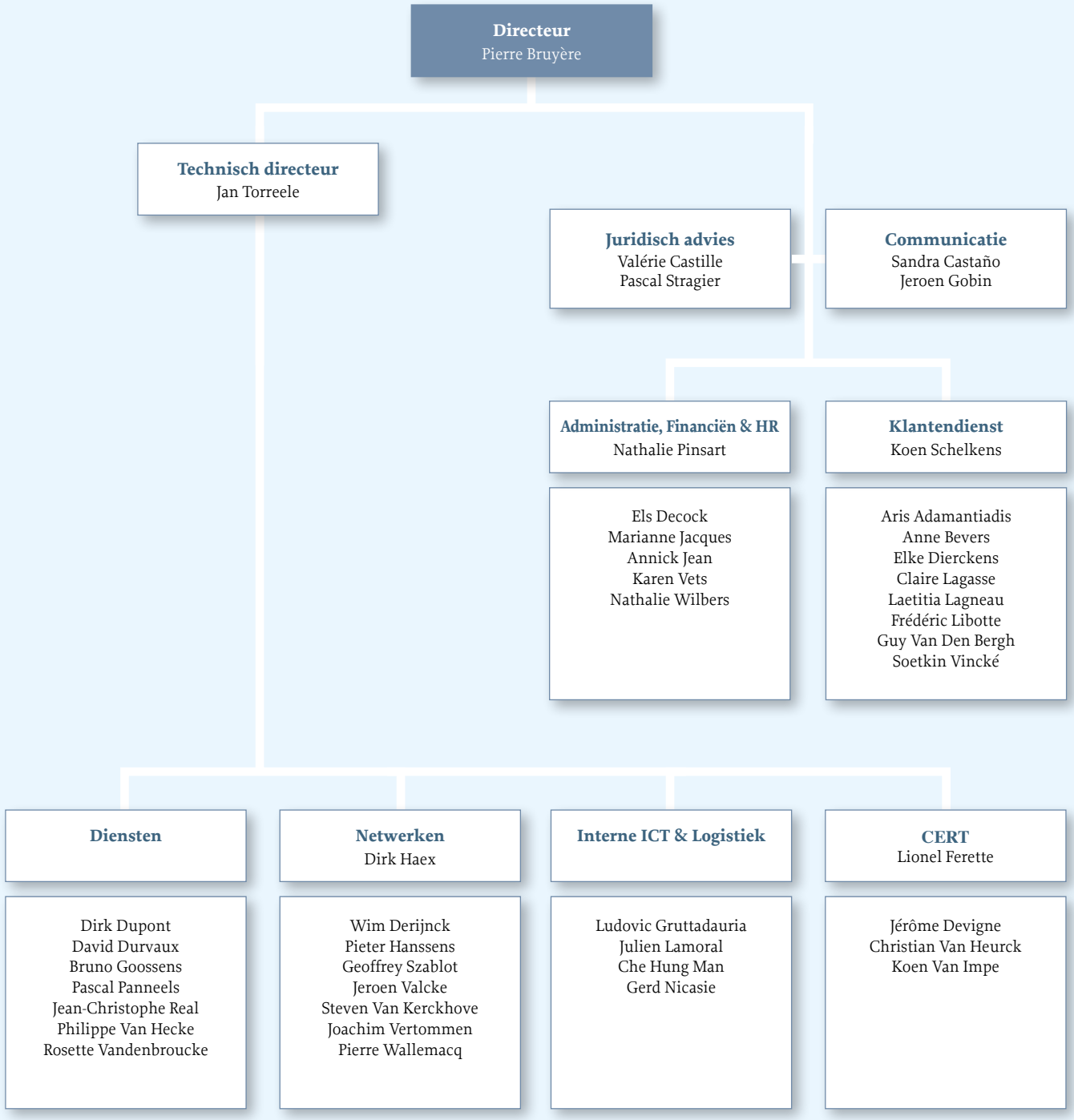
Het aantal medewerkers steeg van 33 tot 39 voltijdsequivalenten, voornamelijk als gevolg van de uitbreiding van onze dienstverlening.
De tewerkstelling gebeurt rechtstreeks door BELNET (82 %), via het Federaal Wetenschapsbeleid (12 %) en via outsourcing (6 %). Zo'n 50 % van de medewerkers is technisch personeel. Ongeveer een derde van onze werknemers zijn vrouwen. Er werken nagenoeg evenveel Franstaligen als Nederlandstaligen bij BELNET. De meeste werknemers zijn jonger dan 40 jaar (75 %) en tewerkgesteld op niveau A (77 %). De grote meerderheid van het personeel komt met het openbaar vervoer naar het werk (86 %). Zo'n 47 % van de medewerkers werkt geregeld 1 dag per week van thuis uit, 31 % doet af en toe aan telewerken.

4.3 PARTNERSHIPS

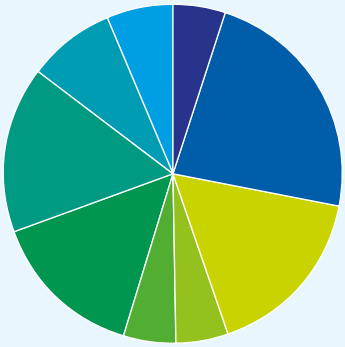
BELNET werkt nationaal en internationaal samen met diverse andere actoren van de kennis- en informatiemaatschappij.

Nationale partners zijn:
- alle Belgische universiteiten, hogescholen en onderzoekscentra
- de Vlaamse overheid en het Waals Gewest
- Fedict, de Federale Overheidsdienst Informatie- en Communicatietechnologie
- ISPA, de Internet Service Providers Association van België
- DNS Belgium

Internationale partners zijn:
- DANTE, dat zorgt voor Géant2, het Europese onderzoeksnetwerk
- Euro-IX, de Europese vereniging van internetknooppunten
- TERENA, de Europese vereniging van onderzoeks- en onderwijsnetwerken

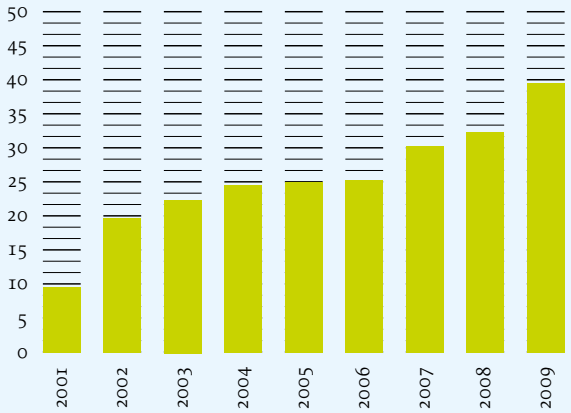

Directeur
Pierre Bruyère
Technisch directeur
Jan Torreele
Juridisch advies
Valérie Castille
Pascal Stragier
Communicatie
Sandra Castaño
Jeroen Gobin
Administratie, Financiën & HR
Nathalie Pinsart
Klantendienst
Koen Schelkens
Els Decock
Marianne Jacques
Annick Jean
Karen Vets
Nathalie Wilbers
Aris Adamantiadis
Anne Bevers
Elke Dierckens
Claire Lagasse
Laetitia Lagneau
Frédéric Libotte
Guy Van Den Bergh
Soetkin Vincké
Diensten
Netwerken
Dirk Haex
Interne ICT & Logistiek
CERT
Lionel Ferette
Dirk Dupont
David Durvaux
Bruno Goossens
Pascal Panneels
Jean-Christophe Real
Philippe Van Hecke
Rosette Vandenbroucke
Wim Derijnck
Pieter Hanssens
Geoffrey Szablot
Jeroen Valcke
Steven Van Kerckhove
Joachim Vertommen
Pierre Wallemacq
Ludovic Gruttadauria
Julien Lamoral
Che Hung Man
Gerd Nicasie
Jérôme Devigne
Christian Van Heurck
Koen Van Impe

HET GEMIDDELDE AANTAL VOLTIJDSEQUIVALENTEN PER DIENST



	2006	2007	2008	**2009**
Communicatie	1,77	2,57	1,79	**2,00**
Klantendienst	2,83	4,44	6,25	**9,05**
Administratie, Financiën & HR	3,90	4,51	5,50	**6,51**
Juridisch advies	1,00	1,00	1,13	**2,00**
Directie	2,00	2,00	2,00	**2,00**
Netwerken	6,50	6,83	6,36	**5,76**
Diensten	5,42	7,21	6,00	**6,12**
Interne ICT & Logistiek	0,00	0,00	2,00	**3,31**
CERT	2,00	1,88	2,00	**2,49**
Totaal	25,42	30,43	33,04	**39,24**

DE EVOLUTIE VAN HET AANTAL MEDEWERKERS, IN VOLTIJDSEQUIVALENTEN



DE BEHEERSCOMMISSIE

VOORZITTER

Dominique Fonteyn, directeur-generaal Onderzoek & Toepassingen, POD Wetenschapsbeleid [1]

ONDERVOORZITTER

Pierre Bruyère, directeur, BELNET [2]

STEMGERECHTIGDE LEDEN

Robert Van de Walle, adviseur-generaal, POD Wetenschapsbeleid [3]
Paul Lagasse, professor aan de Universiteit Gent
Yves Delvaux, directeur operaties & techniek, A.S.T.R.I.D. [4]
Johan Van Helleputte, vice-president, IMEC
Henri Malcorps, directeur van het Koninklijk Meteorologisch Instituut [5]
Marc Acheroy, professor aan de Koninklijke Militaire School [6]

LEDEN MET RAADGEVENDE STEM

Marianne Jacques, rekenplichtige, BELNET
Paul Annicaert, algemeen inspecteur, FOD Financiën

SECRETARIS

Nathalie Pinsart, Administratie, Financiën & HR, BELNET [7]

4.4
FINANCIËLE RESULTATEN

Het algemeen boekhoudkundig resultaat is positief, met 329.606 euro. Door de jaarlijkse indexering nam de werkings- en uitrustingsdotatie in 2009 toe tot 8.474.000 euro. De stijging in gefactureerde prestaties is voornamelijk het gevolg van de verhoging van de opbrengsten uit terugkerende activiteiten met 32 % (2.186.000 euro in 2009 tegenover 1.654.000 euro in 2008). De stijging is ook het gevolg van de toename van het aantal klanten, de vraag naar meer bandbreedte en een aantal nieuwe diensten. Deze stijging werd gedeeltelijk afgeremd door een aanzienlijke daling van de kosten van internetbandbreedte, een daling die BELNET verrekende in zijn tarieven. BELNET factureerde een bedrag van 202.000 euro voor de installatie van CERT.be en de exploitatie ervan vanaf 1 augustus 2009. CERT.be werd door Fedict in het kader van een samenwerkingsprotocol aan BELNET toevertrouwd tot eind 2010; die overeenkomst is verlengbaar tot eind 2014. In vergelijking met 2008 zijn de kosten van diensten en diverse goederen gedaald. BELNET organiseerde in 2008 nog de TERENA-conferentie; de betreffende eenmalige kosten vielen in 2009 weg, net als de installatiekosten van het vernieuwde BELNET-netwerk, dat in 2008 voor het eerst in gebruik werd genomen. Verder daalden de kosten voor de huur en het onderhoud van de lijnen. De personeelskosten namen in vergelijking met vorig jaar toe, vooral door de uitbreiding van het aantal medewerkers in de afdelingen Klantendienst, Interne ICT & Logistiek, CERT en Diensten.

Ondanks de stijging van het gemiddelde uitstaande saldo daalden de financiële opbrengsten in vergelijking met het vorige boekjaar, een gevolg van de sterke daling van de interestvoeten in 2009. Met het oog op een toekomstige toename van de kosten (voornamelijk voor personeel), besliste BELNET om 200.000 euro aan het reservefonds toe te voegen.

4.5
BALANS

De investeringen tijdens het boekjaar 2009 (1.523.000 euro) hebben hoofdzakelijk betrekking op netwerkapparatuur en software voor de verdere ontwikkeling van het BELNET-onderzoeksnetwerk. De afschrijvingen voor boekjaar 2009 bedragen 3.911.216 euro, tegen een jaarlijks afschrijvingspercentage van 25 % voor de computerinfrastructuur, van 20 % voor het rollende materieel en van 10 % voor de overige investeringsgoederen. Tot de vorderingen op ten hoogste één jaar behoort een vordering van 258.000 euro op de btw-administratie. Ze betreft vooral btw-bedragen te recupereren op inkomende facturen ontvangen in de loop van het laatste trimester. De niet aan het algemeen rekeningenstelsel onderworpen externe schulden op ten hoogste één jaar vertonen een stijging, toe te schrijven aan facturen ontvangen in het kader van investeringen in en het onderhoud van het BELNET-onderzoeksnetwerk.

BALANS, IN EURO

Activa	Boekjaar 2008	Boekjaar 2009
Materiële vaste activa	6.874.306	4.502.452
Niet aan rekeningenstelsel onderworpen externe vorderingen op ten hoogste 1 jaar	336.527	314.472
Aan rekeningenstelsel onderworpen externe vorderingen op ten hoogste 1 jaar	46.424	299.425
Schatkistcertificaten en thesauriebewijzen	6.193.000	12.693.000
Bank- en postchequerekeningen – kas, contanten en zegels	3.575.198	360.256
Overlopende activa en wachtrekeningen	1.021.626	1.009.658
Totaal activa	**18.047.081**	**19.179.263**

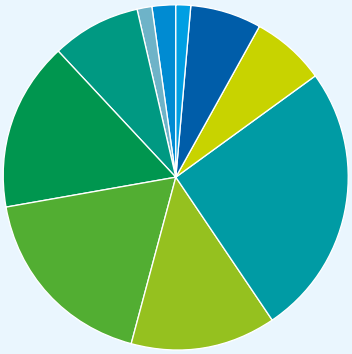
Passiva	Boekjaar 2008	Boekjaar 2009
Nettoactiva of Eigen vermogen of Nettopassiva	16.618.999	17.148.604
Niet aan rekeningenstelsel onderworpen externe schulden op ten hoogste 1 jaar	638.481	1.564.719
Aan rekeningenstelsel onderworpen externe schulden op ten hoogste 1 jaar	124.226	91.420
Overlopende passiva en wachtrekeningen	665.375	374.520
Totaal passiva	**18.047.081**	**19.179.263**

RESULTATENREKENING, IN EURO

Kosten	Boekjaar 2008	Boekjaar 2009
Overig gebruik van consumptiegoederen en externe diensten	6.983.534	5.576.346
Onroerende voorheffing en diverse belastingen	13.188	13.713
Directe en indirecte personeelsvergoedingen	1.444.738	1.907.639
Economische afschrijvingen op huisvestingskosten, immateriële vaste activa en materiële vaste activa	3.235.387	3.911.216
Overdracht van andere inkomsten [uitgaven] dan sociale uitkeringen	64.315	88.226
Waardeverminderingen op bestaande activa en passiva	9.375	3.075
Toevoegingen aan het reservefonds	0	200.000
Algemeen boekhoudkundig resultaat	-132.359	329.606
Totaal kosten	**11.618.178**	**12.029.821**

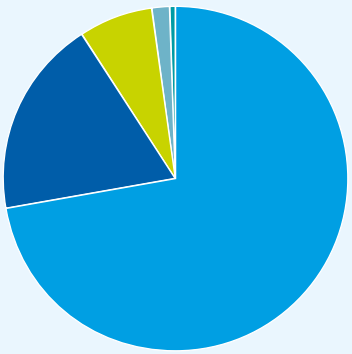
Inkomsten	Boekjaar 2008	Boekjaar 2009
Gefactureerde diensten	2.938.198	3.498.811
Rente en overige financiële inkomsten	243.980	49.905
Uitzonderlijke inkomsten	30.000	7.105
Overdracht van andere inkomsten dan belastingen en sociale bijdragen	8.406.000	8.474.000
Terugname van voorzieningen voor toekomstige risico's en lasten	0	0
Totaal inkomsten	**11.618.178**	**12.029.821**

UITTREKSELS UIT DE BUDGETREKENING: DE UITGAVEN, IN DUIZENDEN EURO



	2008	**2009**
Nationale lijnen	684	**156**
Europese lijnen	684	**636**
Commercieel internet	614	**663**
Onderhoud van netwerkapparatuur en diensten	3.432	**2.428**
Algemene onkosten	1.492	**1.328**
Bezoldigingen	1.285	**1.681**
Andere investeringen	2.035	**1.523**
FedMAN2-project [investeringen inbegrepen]	977	**826**
Beheer van CERT.be	0	**128**
Toevoegingen aan het reservefonds	0	**200**
Totaal	11.203	**9.569**

UITTREKSELS UIT DE BUDGETREKENING: DE INKOMSTEN, IN DUIZENDEN EURO



	2008	**2009**
Dotatie	8.406	**8.474**
Gefactureerde prestaties	1.654	**2.186**
FedMAN2-project	457	**812**
Beheer van CERT.be	0	**202**
Rente	244	**50**
Terugname van voorzieningen en overdracht van ontvangsten	695	**0**
Totaal	11.456	**11.724**

In 2009 ontplooide BELNET heel wat initiatieven om via zijn infrastructuur en diensten een veilige en efficiënte samenwerking in onderwijs en onderzoek te ondersteunen. Van een netwerkprovider evolueren we tot een dienstenleverancier die ervoor zorgt dat zijn klanten en gebruikers onder alle omstandigheden goed en veilig kunnen samenwerken.

We hebben in 2009 ook taken op ons genomen die de wereld van het onderwijs en het onderzoek overstijgen en iedere burger van het land aangaan. CERT.be is daar het meest sprekende voorbeeld van. De lancering van dit nationale veiligheidsteam is aanmoedigend. Ze toont duidelijk aan dat de overheid haar verantwoordelijkheid opneemt voor het beveiligen van de kennis- en informatiemaatschappij die volop in ontwikkeling is.

Het behoort tot onze missie de groei van de kennis- en informatiemaatschappij te bevorderen en met CERT.be en tal van andere initiatieven hebben we dat in 2009 zeker gedaan. In 2010 gaan we op de ingeslagen weg verder, om nog beter onze strategische doelstellingen te realiseren.

2009

BELNET wenst de volgende personen en organisaties hartelijk te danken voor de aangename samenwerking bij de realisatie van dit jaarverslag:

- Luc Beirens en de Federal Computer Crime Unit
- Daniel Letecheur
- Henri Malcorps
- Herman Moons
- Wim Pouseele
- Peter Strickx
- De directie en de medewerkers van The Platinum
- De directie en de medewerkers van de Federale Politie, 'Kroontuinen'

Dit jaarverslag werd gedrukt op papier dat werd vervaardigd uit grondstoffen die afkomstig zijn uit goed beheerde bossen en andere gecontroleerde bronnen.

ISBN 9789056270001
D/2010/12411/1

BELNET

Wetenschapsstraat 4
1000 Brussel
Tel.: +32 2 790 33 33
Fax: +32 2 790 33 34
www.belnet.be

NIEUW ADRES
VANAF DECEMBER 2010

Louizalaan 231
1050 Brussel

Verantwoordelijke uitgever: BELNET, Pierre Bruyère, Wetenschapsstraat 4, 1000 Brussel

Cypres