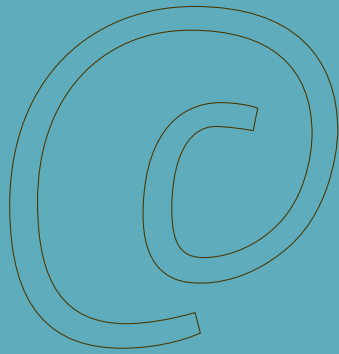


Eén publiekprivate geïntegreerde aanpak.
Eén sluitende nationale infrastructuur ter
bestrijding van cybercrime.



Jaarbericht 2006

NICC



gology
and
the E
of pe
stanc
scure
arch
et to
sh as
calls
ng the
se ha
spac
aft is
cs S
and
ncy
e the

samen
tegen
cyber-
crime
NICC



Samen tegen cybercrime

ICT is onmisbaar...

Digitaal dataverkeer heeft zich in korte tijd onmisbaar gemaakt. Burgers, overheden en bedrijven zijn ervan afhankelijk.

... maar afhankelijkheid van digitaal dataverkeer maakt ons kwetsbaar...

Met deze nieuwe, digitale manier van werken zag een nieuwe vorm van criminaliteit het licht: cybercrime. Publieke en private instanties proberen, ieder voor zich, cybercriminele dreigingen buiten de deur te houden. Ze verzamelen veel kennis, maar delen die te weinig. Er is onvoldoende inzicht in de aard, omvang en mogelijke dreigingen van cybercrime.

... dus is het tijd om de krachten te bundelen....

Cybercriminelen gaan steeds vernuftiger te werk. Het wordt steeds ingewikkelder om ons daartegen te verdedigen. Gelukkig zijn er instanties die burgers waarschuwen, beveiligingen ontwerpen, of criminele sites opsporen en uit de lucht halen. Het is de hoogste tijd om al die initiatieven te coördineren.

... in één Nationale Infrastructuur tegen Cybercrime:

De stand van zaken in kaart brengen.
Witte vlekken invullen. Taken verdelen.
Kennis en informatie verzamelen en door-
sluizen. Expertise uitwisselen.

Dan kan het NICC niet alleen.

Resultaat door samenwerking

De Nationale Infrastructuur tegen Cybercrime ontstaat alleen als alle partijen met elkaar samenwerken. Niemand kan dit alleen. Iedereen heeft elkaar nodig. Onder het motto 'Learning by doing' zijn het afgelopen jaar de eerste stappen op weg naar een succesvolle aanpak tegen cybercrime gezet.

De Nationale Infrastructuur is nooit af

Het NICC wil in 2007 en 2008 met alle mogelijke partners energiek verder bouwen aan een veilige digitale samenleving. Samen aan het werk zal hierbij het uitgangspunt zijn.

Wat is cybercrime, en waarom moeten we ons daar zorgen over maken?

4 **Cybercrime is criminaliteit met een ICT-component.** In het gunstigste geval veroorzaakt cybercrime enkel wat overlast. Voor bedrijven en overheden kan een cybercrime-aanval echter aanzienlijke gevolgen hebben, zowel financieel als in termen van consumentenvertrouwen. Als het terroristen ooit zou lukken om bijvoorbeeld de energievoorziening in Nederland te verstoren, zijn de maatschappelijke gevolgen niet te overzien.

De bekendste vorm van cybercrime is het **computervirus** dat pc's en netwerken infecteert. Minder bekend zijn de **botnets**, die ongemerkt pc's en bedrijfsnetwerken infiltreren. Via **phishing-sites** stelen en misbruiken cybercriminelen digitale identiteiten van nietsvermoedende burgers. De anonimiteit van het internet is ook een ideale schuilplaats voor criminelen die **kinder pornosites** opzetten. En dan zijn er nog onze vitale infrastructuren, die steeds meer gebruikmaken van ICT om hun systemen aan te sturen. Zij vormen een ideaal doelwit voor **cyberterrorisme**.

Tot nu toe blijft de schade bij bedrijven en overheid min of meer beperkt, dankzij antivirussoftware, patches, stevigere firewalls en het uit de lucht halen van phishing-sites. Maar elke nieuwe beveiliging dwingt cybercriminelen nóg inventiever te worden om de mazen in het systeem te ontdekken en benutten. **Cybercrime is veranderlijk en daardoor lastig aan te pakken.**

Opsporing en vervolging van cybercrime is nodig, maar niet de oplossing om veilig digitaal te kunnen werken. **Alleen als overheid en bedrijfsleven de handen ineenslaan en informatie over dreigingen uitwisselen, blijven we gezamenlijk cybercriminelen een stap voor.** We kunnen daarmee niet wachten totdat we hardhandig wakker geschud worden, bijvoorbeeld door een ernstige cybercrime-aanval die een van onze vitale sectoren stillegt.

Er is dringend één Nationale Infrastructuur ter bestrijding van Cybercrime nodig. Liever vandaag dan morgen. Dat is de missie van het programma NICC.

Wat onderneemt het NICC zelf tegen cybercrime?

Niets. **Bestrijding en beveiliging van cybercrime is de verantwoordelijkheid van alle betrokken publieke en private partijen.**

Wat doet het NICC dan wel?

Het NICC ondersteunt en financiert initiatieven van andere publieke en private partijen die bijdragen aan een veiliger manier van digitaal werken.

Het NICC brengt publieke en private partijen bij elkaar om samen verder te bouwen aan de Nationale Infrastructuur. De bouwstenen die zij daar zelf voor aandragen zijn hun eigen kennis en ervaring.

Het NICC houdt de vinger aan de pols: het verzamelt informatie en geeft die door, en stimuleert publieke en private partijen om kennis met elkaar te delen.

Het NICC luistert naar de markt en handelt vraaggestuurd, in nauwe samenwerking met partijen die concrete en werkbare initiatieven aandragen.

Het NICC is dynamisch en flexibel. Wat gisteren noodzakelijk was, is morgen achterhaald. Het NICC houdt overzicht en scherpt de speerpunten continu aan op basis van de laatste informatie.

Het NICC ondersteunt concrete, overzichtelijke projecten en experimenten. Geen lange aanlooptijden en ingewikkelde structuren, niet eindeloos overleggen. Gewoon beginnen, al doende leren en waar nodig bijstellen.

Het Nationaal Platform Criminaliteitsbeheersing (NPC) heeft in het kader van het Actieplan Veilig Ondernemen II (AVO II) de aanzet gegeven voor de Nationale Infrastructuur ter bestrijding van Cybercrime, kortweg NICC. Dit programma loopt van 1 januari 2006 tot eind 2008. Het NICC brengt publieke en private partijen bij elkaar als eerste stap op weg naar een effectieve en geïntegreerde aanpak van cybercrime, zowel wat betreft preventie als opsporing. In de loop van 2007 zal het NICC worden ondergebracht bij het ministerie van Economische Zaken.

Extremisten en terroristen beheersen de kunst van het communiceren via internet beter dan Amerikaanse overheidsinstellingen; zij maken meer gebruik van multimedia en hun websites zijn interactiever (chatrooms en online fora). Als het gaat om het bouwen van een gemeenschap laten zij de overheden ver achter zich.



NICC: samen bouwen aan één Nationale Infrastructuur ter bestrijding van Cybercrime

8

De Nationale Infrastructuur is een krachtenbundeling van alle functies op het gebied van de bestrijding van cybercrime. Het is de hoogste tijd dat publieke en private partijen samen hun maatregelen op het gebied van digitale veiligheid inventariseren, op elkaar afstemmen en waar nodig aanvullen.

Veel van de functies voor de bestrijding van cybercrime zijn al ingevuld, bijvoorbeeld het Meldpunt Cybercrime én de High Tech Crime Unit van de KLPD en de Waarschuwingsdienst van GOVCERT. Andere functies zijn volop in ontwikkeling. Beheerders van vitale systemen ontwikkelen bovendien zelf intern ook beveiligingsmaatregelen.

De cybercrime-bestrijding op nationaal niveau is gefragmenteerd. Een compleet overzicht van alle initiatieven ontbreekt. De rolverdeling is onduidelijk en van een gezamenlijke, publiek-private en geïntegreerde aanpak is geen sprake. Kortom: **de 'landkaart' van cybercrime-bestrijding vertoont overlappingen en witte vlekken.**

Het NICC inventariseert de stand van zaken op het gebied van cybercrime-bestrijding, signaleert overlappingen en ondersteunt activiteiten die leiden tot het opvullen van witte vlekken. Op basis van de eerste inventarisaties is duidelijk geworden welke functies op de landkaart nog niet, of niet voldoende, zijn ingevuld. **Het NICC stimuleert anderen om de witte vlekken in de nationale infrastructuur in te vullen.**

Omdat cybercrime veranderlijk is, liggen de speerpunten van het NICC niet vast. Als in de loop van het programma blijkt dat andere onderwerpen voorrang moeten krijgen, dan past het NICC zijn strategie aan. **De ontwikkeling van de infrastructuur is een dynamisch, continu proces waarbinnen het NICC twee lijnen aanhoudt.**

1. Het NICC realiseert een Informatieknooppunt Cybercrime dat het kloppende hart wordt van de Nationale Infrastructuur.

Een cybercrime-aanval op water- en energievoorziening, banken, telecom, transport of chemische industrie kan de samenleving ernstig ontwrichten. Publieke en private instanties in deze vitale sectoren bezitten waardevolle informatie over dreigingen en het verweer daartegen. In de veilige omgeving van het Informatieknooppunt kunnen zij deze gevoelige informatie vrijuit uitwisselen.

2. Het NICC ontwikkelt en ondersteunt experimenten die kennis over cybercrime opleveren en tegelijkertijd een concreet knelpunt oplossen.

Bij gebrek aan inzicht in de aard en omvang van het probleem is de bestrijding van cybercrime nog voornamelijk aanbodgericht. Het is onduidelijk of de bewustwordingscampagnes van de overheid en de beveiligingsproducten die op de markt komen, aansluiten op een reële vraag. Het NICC hanteert 'learning by doing' als motto. Experimenten genereren nieuwe informatie, op basis waarvan het NICC partijen bij elkaar brengt die samen een knelpunt kunnen oplossen. Deze informatie leidt bovendien weer tot nieuwe experimenten op andere terreinen.

Deze twee lijnen lopen parallel en zijn nauw verweven. De uitkomsten van de experimenten voeden het Informatieknooppunt; het Informatieknooppunt levert input voor de experimenten.

Het resultaat is één publiekprivate, geïntegreerde aanpak van veilig digitaal werken, ofwel één sluitende Nationale Infrastructuur ter bestrijding van Cybercrime.

De functies van de Nationale Infrastructuur zijn: aanspreekpunt, meldpunt, trendwatching, monitoren en detecteren, informatieverstrekking, voorlichting, waarschuwen, ontwikkelen, kennis ontwikkelen en delen, toezicht, tegenhouden/stoppen, verstoren, schadebeperking.

Het NICC concentreert zich op vier cruciale functies:

De volgende functies worden op dit moment niet of onvoldoende ingevuld. Het NICC zal het komende jaar met betrokken organisaties verder werken om deze functies in te vullen:

1. kennis ontwikkelen en delen;
2. informatieverstrekking;
3. tegenhouden/stoppen;
4. trendwatching.

Informatieknooppunt Cybercrime

10

Het Informatieknooppunt Cybercrime is het kloppende hart van de Nationale Infrastructuur. Hierin wisselen bedrijven en instanties binnen vitale sectoren gevoelige informatie uit die voor hun collega's van belang kan zijn.

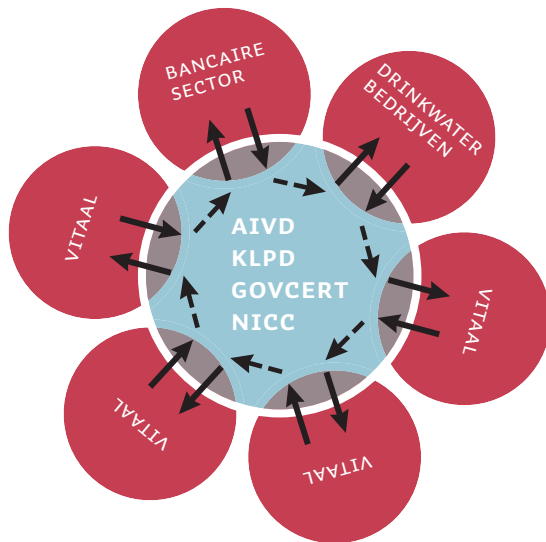
Het Informatieknooppunt is opgebouwd volgens het 'bloemblaadjesmodel'. De kern van de bloem bestaat uit AIVD, KLPD, GOVCERT en NICC. Daaromheen zijn overlegorganen van de vitale sectoren gerangschikt als bloemblaadjes. Binnen elk bloemblaadje wordt informatie gedeeld. Via de kern van de bloem wordt essentiële informatie doorgegeven van het ene bloemblaadje naar het andere, en eventueel aan andere partijen. De sector die informatie aanlevert, bepaalt zelf wat daarvan aan de overige vitale sectoren of andere partijen mag worden bekendgemaakt. Uiteraard onder strikte voorwaarden, en geanonimiseerd.

Het NICC wil eind 2007 zes van de twaalf vitale sectoren aan het informatieknooppunt verbonden hebben: de bancaire sector, drinkwaterbedrijven, energie, telecom, chemie en transport. In deze sectoren speelt ICT namelijk een essentiële rol.

In oktober 2006 sloot de bancaire sector zich als eerste bloemblaadje aan op het Informatieknooppunt. Op 30 november 2006 vond het eerste overleg plaats tussen dertien organisaties uit de financiële wereld. De deelnemers bespraken in strikte vertrouwelijkheid de dreigingen in de sector en deelden informatie over oplossingen. Een van die oplossingen is **Notice and Take Down** (zie ook pagina 14), waarmee phishing-sites uit de lucht gehaald worden.

De elf waterbedrijven die zijn aangesloten bij de Vereniging van Waterbedrijven in Nederland (VEWIN) vormen het tweede bloemblaadje van het Informatieknooppunt. Het eerste overleg, in april 2007, staat in het kader van SCADA/procesautomatisering. Het productieproces van waterbedrijven wordt in toenemende mate op afstand aangestuurd via internetverbindingen. Dat maakt de sector kwetsbaar: er moet voorkomen worden dat kwaadwillenden via internet de drinkwatervoorziening kunnen verstoren. TNO en KEMA brengen momenteel samen met het ministerie van Economische Zaken de dreigingen en kwetsbaarheden voor de drinkwatersector overzichtelijk in kaart. De uitkomsten van dit onderzoek worden besproken in de eerste vergadering van de waterbedrijven. Onderwerp voor een volgende bijeenkomst zijn de uitkomsten van een meting: wat komt er daadwerkelijk aan cybercrime-dreiging binnen op de netwerken?

Het NICC voert momenteel verkennende gesprekken in de sectoren energie, telecom, transport en chemie. Deze sectoren worden in kaart gebracht en vervolgens benaderd voor deelname aan het Informatieknooppunt.



Het Informatieknoppunt Cybercrime is gebaseerd op het informatie-uitwisselingsmodel van het Britse Centre for the Protection of National Infrastructure (CPNI, voorheen NISCC). In dit model overlegt een selecte groep overheidsdiensten met vitale sectoren over de risico's van cybercrime en het nemen van maatregelen. De sector selecteert zelf de deelnemers aan het overleg. Een voorwaarde voor het slagen van het Informatieknoppunt is vertrouwelijkheid. De aangesloten deelnemers moeten binnen hun eigen kring vrijuit kunnen spreken.

Door de toenemende online criminaliteit loopt elektronische commercie gevaar.

Enrique T. Salem van Symantec:

‘Gebruikers zijn kopschuw geworden. Ze weigeren nog langer online formulieren in te vullen. Ook transacties worden steeds vaker gewantrouwd.

Dat houdt de ontwikkeling van nieuwe diensten tegen.’



Experimenten en onderzoek

14

De Nationale Infrastructuur krijgt voeding van experimenten en onderzoek. Deze experimenten pakken een knelpunt aan in de publieke of private sector. Tegelijkertijd genereren ze kennis over cybercrime en nieuwe inzichten in de witte vlekken op de landkaart. Dat leidt weer tot nieuwe, creatieve projecten.

Het NICC benadert de experimenten en onderzoeken als een groeiproces. De cybercrime-dreiging is zeer veranderlijk, dus moet ook de aanpak ervan actief en dynamisch zijn. Een interessant idee wordt meteen omgezet in een experiment, zonder lange aanlooptijd. Mochten er gaandeweg aanpassingen nodig zijn, dan wordt daar snel en flexibel op ingespeeld.

Het NICC beheert de ontstane beveiligingsoplossingen niet zelf. Na de ontwikkelfase neemt een van de betrokken partijen het beheer op zich.

Het NICC brengt partijen bij elkaar; het ondersteunt initiatieven en vragen uit de publieke en private sector. Een onderzoek naar een waarschuwingssysteem voor kleine community's is bijvoorbeeld totstandgekomen op initiatief van het onderwijs. De opgedane kennis en ervaring zijn weer toe te passen in andere afgebakende community's, zoals gemeenten of het midden- en kleinbedrijf.

Om identiteitsfraude aan te pakken heeft de bancaire sector het NICC-project Notice and Take Down opgezet. Criminelen verleiden bankklanten om via phishing-sites hun inloggegevens prijs te geven. De banken in Nederland zijn afdoende tegen dergelijke identiteitsfraude beveiligd. Maar verhalen in de media over

buitenlandse phishing-dreigingen kunnen wel het consumentenvertrouwen in veilige e-commerce en internetbankieren schaden. Notice and Take Down heeft in 2006 zes maanden gedraaid en is wegens groot succes met nog eens zes maanden verlengd. In de eerste fase hebben de banken enkele tientallen, merendeels buitenlandse, phishing-sites aangemeld bij GOVCERT. Het is GOVCERT via zijn internationale netwerk gelukt om het grootste deel van deze phishing-sites uit de lucht te laten halen.

Het midden- en kleinbedrijf is nog niet voldoende digitaal beveiligd. In 2006 heeft Syntens in opdracht van het NICC en het Electronic Commerce Platform (ECP) bij vijftig midden- en kleinbedrijven in Flevoland onderzocht in welke mate ze concreet door cybercrime (virussen, malware) worden bedreigd. Ook werd ter plekke gekeken hoe het stond met hun informatiebeveiliging in het algemeen. De ondernemers kregen een rapport inclusief beveiligingsadviezen en een handleiding.

De conclusies uit het onderzoek waren zorgwekkend. Veel ondernemingen gaan er van uit dat het inhuren van een externe ICT-leverancier een garantie voor beveiliging is. Ondanks deze investering blijkt de beveiliging echter onvoldoende. Een van de aanbevelingen is dan ook dat de ICT-branche een goede kwaliteit van dienstverlening herkenbaar gaat maken, bijvoorbeeld door certificering.

Hoe maak je als ICT-coördinator van een school de juiste keuze uit het grote aanbod op het gebied van ICT-beveiliging? Een experiment in het Nederlandse voortgezet onderwijs en in de beroeps- en volwasseneneducatie onderzoekt of

het Britse **Warning, Advise and Reporting Point (WARP)** van nut kan zijn. Dit concept biedt computergebruikers op maat gesneden informatie voor de beveiliging van hun computer die verder gaat dan de algemene waarschuwingen van GOVCERT. Bovendien stimuleert WARP het vormen van community's waarbinnen deelnemers informatie uitwisselen.

De in dit experiment opgedane kennis komt ook van pas in andere sectoren met een vergelijkbare problematiek, bijvoorbeeld het midden- en kleinbedrijf en kleine gemeenten. Het NICC voert het experiment in 2007 uit in samenwerking met Kennisnet en Surfnet.

Gemeenten worden steeds kwetsbaarder voor cybercrime. Het contact van gemeenten met burgers en bedrijven wordt gedigitaliseerd. Interactieve gemeentelijke websites (frontoffice) zijn verbonden met de backoffice-processen en -systemen. Management en bestuur van gemeenten hebben te weinig kennis van en aandacht voor de integrale aanpak van informatiebeveiliging; ze zien dat als een zaak van de gemeentelijke IT-afdeling.

Er staan drie concrete projecten op stapel: een toegankelijk zakboekje over informatiebeveiliging voor management en bestuur, een WARP-experiment en een meta-analyse van het gemeentelijke landschap en cybercrime. Het NICC werkt samen met de Vereniging voor I&A-coördinatoren Gemeenten (VIAG), de Vereniging van Nederlandse Gemeenten (VNG) en de belangrijkste gemeentelijke ICT-leveranciers.

In 2006 heeft de Universiteit van Tilburg een **Onderzoek Convergentie Cybercrime naar identiteitsfraude uitgevoerd**. Het ouderwetse, zichtbare hacken is sluipenderwijs veranderd in onzichtbare infiltratie in computersystemen. Het is een volwassen middel geworden waarmee professionele criminele netwerken identiteitsfraude plegen. Iedereen kan daar, vaak zonder het te merken, slachtoffer van worden. Hoewel de individuele burger vaak slechts voor kleine bedragen wordt opgelicht, gaat het in totaal om aanzienlijke financiële schade. Het accent moet daarom worden verlegd van beveiliging tegen individuele computerfreaks naar de opsporing en aanpak van professionele cybercriminelen. Deze accentverschuiving stelt andere, hogere eisen aan de functies van de Nationale Infrastructuur.

De Nederlandse overheid heeft vijf scholieren die in 2004 de sites regering.nl, kabinet.nl, nederland.nl en overheid.nl platlegden, verantwoordelijk gesteld voor de geleden schade. De vijf zijn 'verbijsterd' over de hoogte van de schadeclaim: vijf ton. De overheid moest het gebruikte verkeer vergoeden, nieuwe beveiligingsmaatregelen treffen en extra hardware aanschaffen.



Samen tegen cybercrime

18

Al deze afgeronde en lopende projecten, onderzoeken en experimenten leveren nu al veel waardevolle kennis op over de aard en omvang van cybercrime-dreiging en de beveiliging daar tegen.

Het NICC gebruikt deze informatie, en vragen uit de markt, als input voor verdergaande samenwerking en nieuwe activiteiten.

De eerste resultaten zijn dankzij inspanningen van publieke en private partners al binnen: het Informatieknooppunt groeit, phishing-sites worden aangepakt, het midden- en kleinbedrijf is alert, waarschuwingssystemen voor scholen en gemeenten zijn in de maak.

De Nationale Infrastructuur is nooit af!

Het NICC blijft in 2007 en 2008 samen met alle mogelijke betrokken partners energiek verder bouwen aan een veilige digitale samenleving. Het NICC zet sterk in op tegenhouden en stoppen van cybercriminaliteit en zal het informatieknooppunt een extra impuls geven. Dat zijn belangrijke eerste stappen. Echt succes ontstaat vooral door samen te zoeken naar de volgende stappen om de Nationale Infrastructuur te versterken.



NICC-programma

20

Albert van Wijk (OM)

Opdrachtnemer NPC

Edwin Mac Gillavry (NVB)

projectleider

Annemarie Zielstra (ICTU)

programmamanager

Jan Wester (ministerie van EZ)

programmavid

Cor Ottens

communicatieadviseur

Auke Huistra

projectleider informatieknooppunt

Monique Bonoo

secretaresse

NICC

p/a ICTU

Bezoekadres

Wilhelmina van Pruisenweg 104
2595 AN Den Haag

Postadres

Postbus 84011
2508 AA Den Haag

T 070 888 79 46

nicc@ictu.nl

www.samentegencybercrime.nl