PLATFORM VOOR CYBERSECURITY
CPNI.NL

NL
’11

JAARBERICHT 2011
CPNI.NL

Kennis delen is meer dan ooit de core business van CPNI.NL. Zo wordt niet alleen de continuïteit van de afzonderlijke organisaties gewaarborgd, maar ook de BV Nederland beschermd tegen moedwillige en overige incidenten en dreigingen.

CPNI.NL PROGRAMMA

Ministerie van EL&I
subsidieverlener

Annemarie Zielstra
director CPNI.NL

Erik Staffeleu
projectleider CAET

Mike Dell
projectleider Lessons Learned Vitaal

Christiaan Colen
projectondersteuning CPNI.NL

Auke Huistra
projectmanager

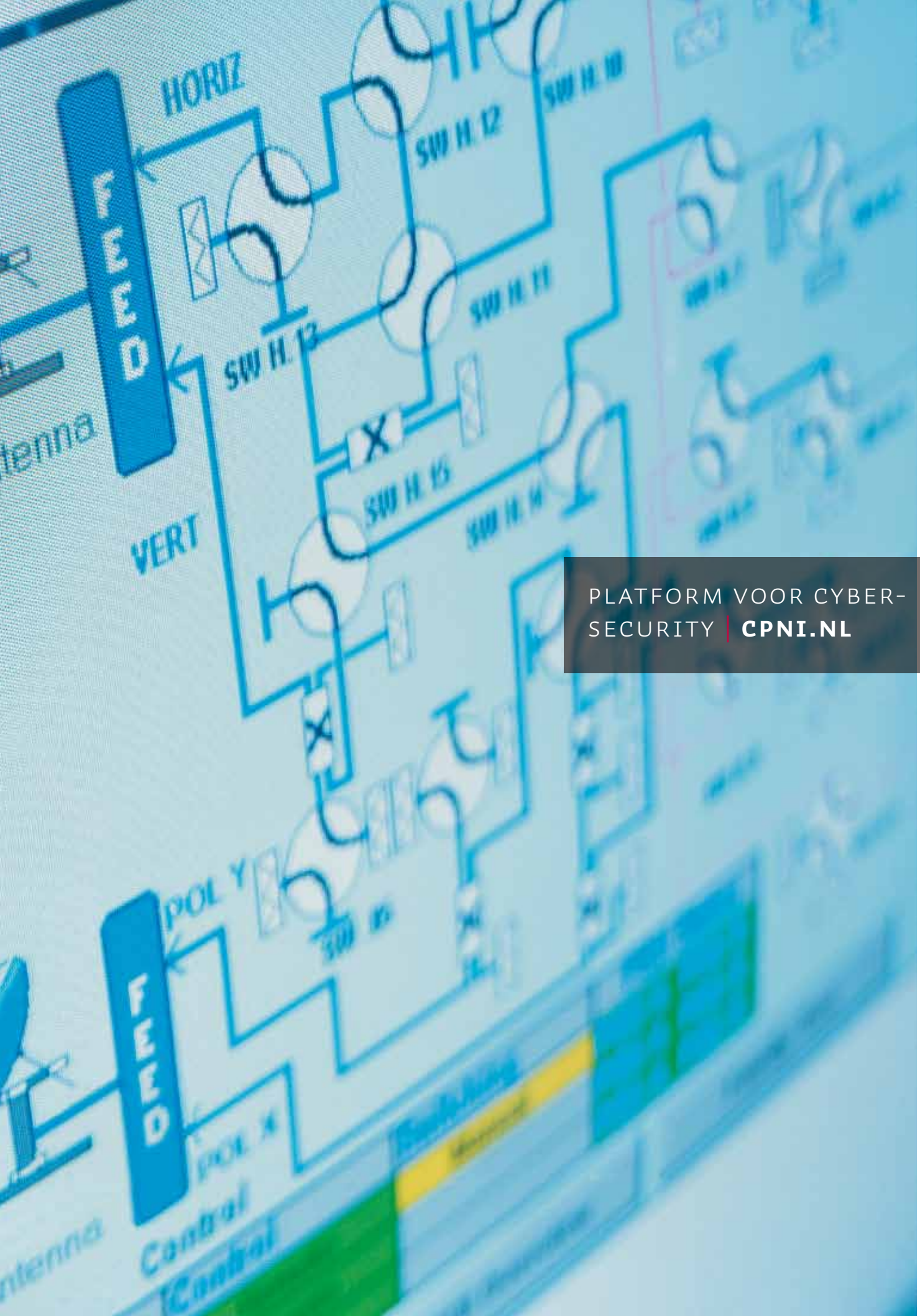
Tjarda Hersman, Allard Kernkamp, Maartje Spoelstra
secretaris ISACs

Marieke Klaver, Eric Luiijf, Maarten Oosterink
expertpool CPNI.NL

Cor Ottens
communicatieadviseur

Uitgave: CPNI.NL | Redactie: Tekstbureau De Nieuwe Koekoek, Utrecht | Fotografie: Marcel Rozenberg Design & Photography, Schiedam | Vormgeving: OSAGE, Utrecht | Druk: Fennema Drukker, Werkendam

april 2012



PLATFORM VOOR CYBER-SECURITY | **CPNI.NL**

SAMEN STERKER: INTERSECTORAAL EN INTERNATIONAAL

CPNI.NL, inclusief het Informatieknooppunt Cybercrime, heeft sinds een jaar een plaats in de TNO-organisatie. Na vijf jaar experimenteren onder het label NICC werken we als CPNI.NL samen met onze vele partners gestaag door aan de verdere verbetering van cybersecurity in de vitale sectoren. De expertise van TNO helpt ons om inhoudelijk te verdiepen.

Kennis delen is meer dan ooit de core business van CPNI.NL. Zo wordt niet alleen de continuïteit van de afzonderlijke organisaties gewaarborgd, maar ook de BV Nederland beschermd tegen moedwillige en overige incidenten en dreigingen. In 2011 hebben meer dan tweehonderd specialisten uit overheid en bedrijfsleven in tientallen ISAC-vergaderingen met elkaar gesproken over potentiële bedreigingen. Zo vonden zij gezamenlijk de meest kansrijke oplossingen. De uitgewisselde informatie is grotendeels zeer vertrouwelijken en daarom niet geschikt voor publicatie in dit jaarbericht. Deelnemers gebruiken de gedeelde kennis in hun eigen organisaties om effectieve maatregelen te nemen.

De aanpak van kennisdeling die CPNI.NL (voorheen NICC) in Nederland al ruim zes jaar toepast, krijgt steeds meer bevestiging. Een recente studie van de toonaangevende National Infrastructure Advisory Council (NIAC) uit de Verenigde Staten heeft de factoren voor succesvolle kennisdeling tussen private en publieke partijen nog eens helder op een rijtje gezet: oog hebben voor elkaars belangen, wederkerigheid als het gaat om uitwisseling van informatie, vrijwilligheid als basis en bovenal kiezen voor die vorm die het meeste vertrouwen biedt. Al die factoren vormen de basis voor succes van het Informatieknooppunt Cybercrime.

In 2011 heeft CPNI.NL definitief de stap naar intersectorale en internationale samenwerking gezet. De ISACs in het Informatieknooppunt weten elkaar steeds beter te vinden. Dat is een grote stap voorwaarts. Ook de scheiding tussen nationaal en internationaal vervaagt. Dat lijkt logisch, want cybersecurity is een 'grenzeloze' aangelegenheid. Toch wil dat nog niet zeggen dat iedereen dan ook direct internationaal kennis deelt. Gelukkig vliegen de sectoren hun activiteiten steeds vaker aan vanuit de internationale dimensie.

Om met een groeiend aantal partijen kennis te kunnen delen, zijn nieuwe stappen nodig. Minister Opstelten heeft in december 2011 aangekondigd dat de ISACs in 2012 aangesloten zullen worden op het kersverse Nationaal Cyber Security Centrum (NCSC). De sectoren energie, ICT/telecom, financieel, drinkwater, keren en beheren oppervlaktewater en transport zullen als eerste worden benaderd. CPNI.NL juicht aansluiting bij het centrum toe.

Op de route naar een betere cybersecurity zal CPNI.NL blijven waken over de consequente toepassing van de essentiële factoren voor succesvolle publiek-private samenwerking: vertrouwen, toegevoegde waarde en wederkerigheid.

VOORWOORD

Annemarie Zielstra | Director CPNI.NL

Als een minister midden in de nacht een persconferentie geeft, dan moet er wel iets heel belangrijks te melden zijn. Minister Donner deed het op 3 september 2011 over de DigiNotar-hack. Het geeft aan dat cybercrime en cybersecurity niet langer meer een louter specialistisch probleem zijn, maar onderwerp van gesprek zijn geworden in de ministerraad en aan de bestuurstafels. Dat is natuurlijk zorgelijk als het gaat om het probleem, maar ook goed nieuws als het gaat om de bestrijding.

Stuxnet, problemen met de OV-chipkaart, DigiNotar, inlogincidenten bij overheden en ga zo maar door. Het zijn onderwerpen die iedere Nederlander voorbij ziet komen in de tv-journaals op primetime. Vijf jaar terug moesten we nog schreeuwen om meer aandacht voor het onderwerp. Nu is de aandacht ons soms zelfs te veel. Cybercrime is zonder meer uitgegroeid tot een maatschappelijk probleem. De schade is zo tastbaar geworden dat het in soundbites neer te zetten is. En voor wie nog twijfelt: journalist van het jaar was in 2011 webjournalist Brenno de Winter, de personificatie van de aandacht voor problemen in onze digitale wereld.

Voor de argeloze tv-kijker mag het een verrassing zijn dat er veel mis kan gaan op het internet, de kenners wisten het allemaal al veel langer. Gelukkig werken we daar in publiek-private samenwerking ook al jaren aan en is er veel bereikt, anders was de maatschappelijke schade nog veel groter geweest. In nagenoeg alle vitale sectoren is informatie-uitwisseling op gang gekomen en wordt publiek-privaat samengewerkt aan goede cybersecurity. Zo zorgen we er voor dat er water uit de kraan komt en elektriciteit uit de stopcontacten. Zo garanderen we dat financiële transacties ongestoord worden uitgevoerd en dat het logistieke hart van onze samenleving, transport via water, lucht, weg en spoor, blijft kloppen.

Want wat had er nog meer in de journaals gezeten als we dat allemaal niet hadden gedaan? Deze 'als-dan'-verhalen hoeven gelukkig niet verteld te worden, maar iedereen in de nationale infrastructuur voor cybersecurity weet wat de inhoud had kunnen zijn. Toch is genoegzaam achterover leunen geen optie. Ieder jaar weer moet een volgende stap gezet worden. Cybercrime is immers een veelkoppig monster: hak je een kop af, dan groeit er vanzelf een nieuwe aan.

'Volgende stappen' zijn er in 2011 volop gezet. Zo is een goede start gemaakt met de samenwerking tussen de sectoren, zoals diverse voorbeelden in dit jaarbericht laten zien. Dat moet ook wel, want de onderlinge afhankelijkheden worden steeds groter. ICT is zo nauw verbonden met fysieke systemen en personen dat er niet meer afzonderlijk gehandeld kan worden op deze drie terreinen. In nagenoeg alle vitale sectoren zijn onbemande installaties die op afstand online bediend worden eerder regel dan uitzondering. De persoonlijke factor in de beveiliging is daarmee veranderd, maar zeker niet minder belangrijk geworden. Integendeel, menselijk handelen is misschien juist wel veel belangrijker dan het ooit is geweest.

Ook de overheid zat niet stil in 2011. De Nationale Cyber Security Raad is geïnstalleerd en op 1 januari 2012 werd het Nationaal Cyber Security Centrum operationeel. Nationaal is dat het sluitstuk van de zoektocht naar een goede aanpak. Maar er moet veel meer gebeuren, want cybersecurity houdt niet op bij de landsgrenzen. Steeds belangrijker worden internationale samenwerkingsverbanden,

het bouwen van (sociale) netwerken, uitwisselen van (vertrouwelijke) informatie in een vertrouwde omgeving en concrete samenwerkingsprojecten. Niet naast elkaar, maar vanuit een gecoördineerde aanpak binnen Europa waar we elkaar verder kunnen versterken en de krachten bundelen.

Daarom hebben enkele Nederlandse organisaties, waaronder CPNI.NL, in 2011 het initiatief ENCS (European Network for Cyber Security) gestart. TNO is een van de consortiumpartners in dit initiatief, dat op Europees niveau wordt omarmd; Alliander is de belangrijkste trekker. Het ENCS wordt een onafhankelijk publiek-privaat samenwerkingsverband op Europees niveau, waarin alle relevante stakeholders voor de bescherming van onze vitale digitale infrastructuren gaan samenwerken. Het ENCS is gebaseerd op vier pijlers die elkaar versterken: Research & Development, Opleiding & Training, Testen en Informatie & Kennisdeling. Onderzoek en het testen van systemen leiden tot de ontwikkeling van effectieve mitigatiestrategieën. Informatie en kennis worden gedeeld en gebruikt om opleiding en training inhoud te geven. Het ENCS zal experts en nationale initiatieven binnen en buiten Europa met elkaar verbinden. De focus zal liggen op Industrial Control Systems en Smart Grids. Daarmee passen de activiteiten prima binnen het initiatief EU-US Working Group on Cyber-Security and Cyber-Crime.

Er gaat trouwens ook buiten cybercrime om van alles mis op security-gebied. Systemen zijn nu eenmaal feilbaar en zullen dat ook altijd blijven. Het is de kunst niet te schieten met hagel maar juist gericht oplossingen te vinden voor specifieke problemen, ofwel security by design. Als we dat in goede publiek-private samenwerking blijven doen, zullen we net als in de afgelopen jaren gestaag meters maken over de hele linie.

INFORMATIEKNOOPPUNT CYBERCRIME

De bedrijven in de Rotterdamse haven en de Managed Service Providers sloten zich in 2011 aan bij het Informatieknooppunt Cybercrime (IKC). Via de nu in totaal tien ISACs in het IKC wisselen de vitale sectoren informatie uit over incidenten, dreigingen, trends en security-maatregelen. Deelnemers worden op de hoogte gehouden van de cybersecurity-ontwikkelingen op nationaal en internationaal niveau.

De uitwisseling van good practices tussen ISACs is goed op gang gekomen. Het nut daarvan is bewezen bij incidenten als DigiNotar en Stuxnet. De voorzitters van de ISACs vinden elkaar steeds vaker op intersectorale onderwerpen, zoals in de gezamenlijke Water-Energy-ISAC. De (vice-) voorzitters van de ISACs hebben in 2011 een lijst met onderwerpen opgesteld die in 2012 intersectoraal worden opgepakt.

De publiek-private samenwerking in het IKC is in enkele jaren tijd een succesformule gebleken, die internationaal de aandacht trekt. CPNI.NL werkt inmiddels met verschillende partijen in Nederland en Europa (zoals ENISA) samen om het ISAC-model op te schalen naar Europees niveau. Voorbeelden hiervan zijn de European FI-ISAC en de EuroSCSIE. Verderop in dit jaarbericht leest u hier meer over.

Het succes van de ISACs staat of valt met de vertrouwelijkheid van de uitgewisselde informatie. Daardoor is het vaak niet mogelijk om specifieke informatie over onderwerpen te geven die in de overleggen aan bod zijn gekomen. We kunnen daarom slechts een globale indicatie geven van de werkzaamheden en resultaten van de ISACs.

In de ISACs zijn het afgelopen jaar voortdurend incidenten op het gebied van bijvoorbeeld phishing, skimming, bedrijfsspionage, certificaten (bijvoorbeeld DigiNotar), procescontrole-systemen (onder meer Stuxnet) besproken en van duiding voorzien. Het gaat hierbij zowel om incidenten die hebben gespeeld bij de deelnemers van de ISACs als over incidenten die elders in Nederland of internationaal hebben plaatsgevonden. De input is afkomstig uit private en publieke bronnen (GOVCERT.NL, AIVD en Team High Tech Crime van het KLPD). Op basis van de uitgewisselde informatie voeren de betrokken organisaties zelf een risicoanalyse uit en nemen ze maatregelen.

Vanuit het IKC neemt CPNI.NL deel aan andere overleggen, zoals het Cybercrime-overleg (met deelnemers vanuit diverse overheidsorganisaties), de Special Interest Group Informatiebeveiliging (SIG IB) van de Academische Ziekenhuizen en de werkgroep Plant Security van de WIB.

CPNI.NL verzorgt twee keer per jaar input in het overleg van de SIG IB van de Nederlandse universitaire medische centra. In 2011 heeft ook het informatiebeveiligingsoverleg van de algemene ziekenhuizen aangegeven samen te willen werken met CPNI.NL. In 2012 zal CPNI.NL enkele gezamenlijke bijeenkomsten voor deze twee overleggen organiseren. Onderwerpen zijn onder meer management awareness en het voldoen aan de vernieuwde norm NEN 7510. In deze norm speelt naast informatiebeveiliging ook continuïteitsmanagement een belangrijke rol.

DE VOLGENDE ISACS MAKEN ONDERDEEL UIT VAN HET IKC:

ISAC	TYPE ORGANISATIE	AANTAL DEELNEMENDE ORGANISATIES
Airport-ISAC	Bedrijven en overheidsorganisaties die actief zijn op en rond Schiphol	10
Energy-ISAC	Elektriciteits- en gasbedrijven	10
FI-ISAC	Bedrijven uit de financiële sector	15
Haven-ISAC	Bedrijven en overheidsorganisaties die actief zijn in de Rotterdamse Haven	6
MSP-ISAC	Bedrijven die managed ICT-services aanbieden aan organisaties die behoren tot de vitale infrastructuur in Nederland	11
Multinationals-ISAC	Multinationals met AEX-notering en hoofdkantoor in Nederland	11
Nucleair-ISAC	Bedrijven in de nucleaire sector	6
PCS-Vendors-ISAC	Aanbieders van procescontrolesystemen	6
Telecom-ISAC	Aanbieders van openbare telecommunicatienetwerken, openbare telecommunicatiediensten en huurlijnen die deel uit maken van het Nationaal Continuïteitsoverleg Telecommunicatie (NCO-T)	6
Water-ISAC	Drinkwaterbedrijven	11

De ISACs komen één keer per zes tot tien weken fysiek bij elkaar om informatie te delen over incidenten, dreigingen, kwetsbaarheden en good practices. Tussen deze bijeenkomsten zijn er vele bilaterale contacten en wordt informatie gedeeld via digitale kanalen. Hieronder volgt een bloemlezing van de onderwerpen die in 2011 in de ISACs zijn besproken:

- modus operandi (nationale en internationale) incidenten;
- trends in dreigingen zoals botnets en phishing;
- ontwikkelingen op nationaal en internationaal gebied zoals de Nationale Cyber Security Strategie, de Nationale Cyber Security Raad, het Nationaal Cyber Security Centrum, de cybercomponent binnen het Alerterings-systeem Terrorismebestrijding (ATb), Nationale Roadmap voor veilige proces-controlesystemen en het European Network for Cyber Security;

- studies zoals het Nationaal Dreigingsbeeld, het Cybersecurity Beeld en de Kwetsbaarheids-analyse Spionage, het cyberspionage-scenario binnen de Nationale Risicobeoordeling, het onderzoek naar kwalificatie en certificatie van informatiebeveiligers, diverse studies van ENISA en dreigingsanalyses van de sectoren zelf;
- (ICT) business continuïteit;
- kwantificeren van informatiebeveiliging;
- economische impact van cybercrime;
- mobiele devices (onder meer 'Bring Your Own Device');
- sociale media;
- monitoring en logging;
- Process Control Systems (onder meer 'Hoe om te gaan met legacy systemen?' en de Benchmark Security PCS-omgevingen);
- de gevaren van monocultuur binnen een bedrijf;
- elektromagnetische puls en de bescherming daartegen;
- beveiliging van samenwerkingsplatform software;
- security by design;
- control frameworks, risk analysis en IT governance (met overkoepelende normen-kaders);
- information security normeringen per sector en algemeen.

Naar een integrale aanpak

In 2011 zijn ook de eerste stappen gezet om de aanpak te verbreden richting de fysieke en personele kant van security. Verschillende ISACs hebben activiteiten georganiseerd waarbij medewerkers op het gebied van de fysieke en personele security zijn betrokken.

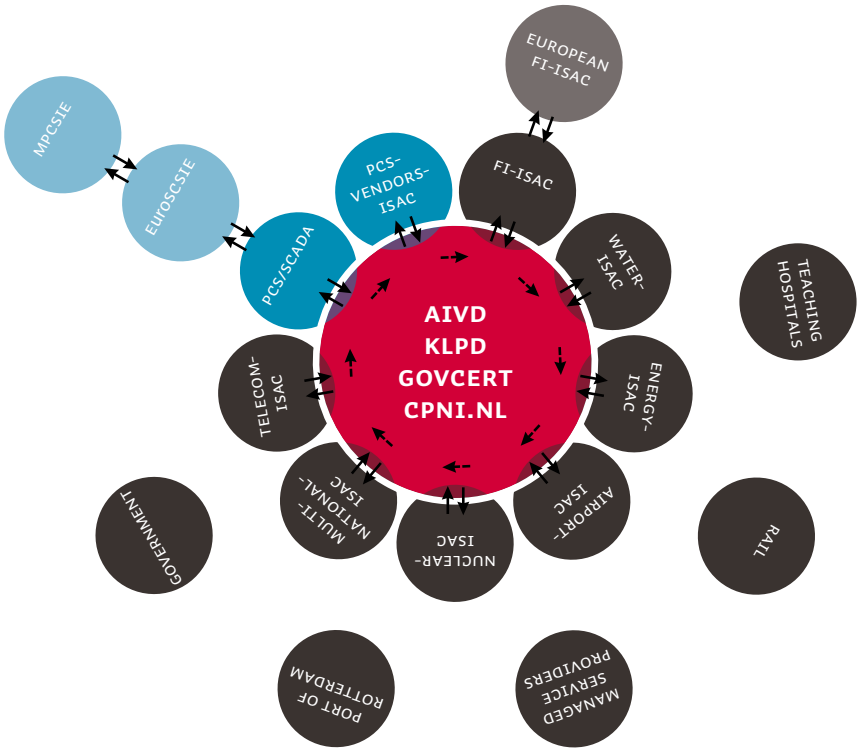
- De Water-ISAC en het Platform Beveiliging en Crisis Management (BCM) hebben in 2011 onder facilitering van de VEWIN en CPNI.NL het initiatief genomen om samen te gaan werken in het Platform Continuïteit Drink-water. De Water-ISAC voorziet in de behoefte van de drinkwaterbedrijven om gezamenlijk kennis en ervaring te delen op het gebied van cybersecurity.
  Het Platform Beveiliging en Crisismanagement (BCM) doet dit op het gebied van (fysieke) beveiliging en crisismanagement. Beide over-leggen opereren op tactisch-operationeel niveau en de onderwerpen die ze behandelen sluiten goed op elkaar aan.
  Met de oprichting van het Platform Continuïteit Drinkwater wil de sector toe naar een integrale security-benadering waarin maatregelen op het vlak van organisatorische, fysieke, logische en ICT-beveiliging met elkaar samenhangen. De drinkwatersector is hiermee een voorloper op het gebied van integrale veiligheid.
- De Nucleair-ISAC heeft in 2011 plannen gemaakt om in 2012 de handen ineen te slaan met het overleg van Plant Security Managers en deels gezamenlijk te vergaderen. Het doel is om ook hier security in het brede integrale perspectief te bespreken. In 2012 wordt deze informatiedeling en integratie tussen verschillende veiligheids- en beveiligings-disciplines geëffectueerd.
- In mei organiseerde de Airport-ISAC in nauwe samenwerking met het platform Beveiliging en Publieke Veiligheid Schiphol (BPVS) het Schiphol Information Security Awareness Symposium (SISAS) voor alle bedrijven en geledingen op Schiphol. Het SISAS werd met negentig deelnemers uit de luchtvaartsector

goed bezocht. Mede door de enthousiaste reacties op het SISAS hebben de Airport-ISAC en het BPVS besloten om hier in 2012 een vervolg aan te geven.

- De Multinationals-ISAC organiseerde in juni een bijeenkomst over het onderwerp economische spionage, waar naast de ISAC-leden ook collega's uit de hoek van fysieke beveiliging en de bescherming van intellectueel eigendom aanwezig waren. Daarbij lag de focus op cyberspionage, een onderwerp dat in diverse dreigingsanalyses (zoals in het recent verschenen Cyber Security Beeld Nederland) hoog scoort. In interactieve sessies zijn modus operandi van incidenten en good practices gedeeld. Dit heeft geleid tot een lijst van tien gouden regels om economische cyberspionage te voorkomen, en als het toch gebeurt vroegtijdig te detecteren en passende opvolging te geven.

Intersectoraal

In 2011 is de intersectorale uitwisseling tussen de ISACs uitgebreid. De Water-ISAC en de Energy-ISAC, die met vergelijkbare ICT-beveiligingsuitdagingen te maken hebben, vergaderen twee keer per jaar gezamenlijk. Onderwerp van gesprek is bijvoorbeeld de beveiliging van procescontrolesystemen die de operationele processen van deze bedrijven aansturen. In het kader van het CAET-traject (zie verderop in dit jaarbericht) zijn verschillende intersectorale workshops gehouden



om de weerbaarheid van de vitale sectoren ten opzichte van grootschalige uitval van elektriciteit en telecommunicatie in kaart te brengen. Vertegenwoordigers van diverse ISACs zijn betrokken geweest bij het opstellen van het cyberspionage-scenario in het kader van de Nationale RisicoBeoordeling (NRB). In diverse ISACs hebben vertegenwoordigers vanuit andere ISACs good practices gedeeld middels presentaties.

De (vice-)voorzitters van alle ISACs hebben gezamenlijk de (intersectorale) agenda voor 2012 vastgesteld.

Internationaal

Internationaal is er veel aandacht voor de wijze waarop in Nederland vitale sectoren en de overheid samenwerken en informatie uitwisselen, de vliegwielfunctie die CPNI.NL hierin vervult, en in het bijzonder de wijze waarop de private sectoren zelf samen initiatieven oppakken om hun eigen weerbaarheid te vergroten. CPNI.NL is in 2011 veel gevraagd om in andere landen de Nederlandse aanpak uit te komen leggen.

Cybersecurity is een internationale aangelegenheid die ook een internationale aanpak en informatie-uitwisseling nodig heeft. Het IKC neemt daarom deel in verschillende Europese initiatieven:

- In de European FI-ISAC delen de financiële sector, de politie en de CERT-gemeenschap informatie over incidenten, dreigingen en kwetsbaarheden die zijn gericht op de financiële sector (financiële malware, botnets, DDoS-aanvallen, phishing). De partijen wisselen modus operandi en good practices uit. De European FI-ISAC komt twee keer per jaar bij elkaar en wordt voorgezeten door de voorzitter van de Nederlandse FI-ISAC.
- In de European SCADA and Control Systems Information Exchange (EuroSCSIE) komen organisaties die gebruik maken van procescontrolesystemen (overheid, wetenschap en met name de energiesector) drie keer per jaar bij elkaar om informatie uit te wisselen en good practices te delen. De deelnemers komen uit verschillende Europese landen en vanuit Europese instituties zoals Joint Research Center en ENISA. CPNI.NL is voorzitter van de EuroSCSIE.
- De voorzitter van de Haven-ISAC en CPNI.NL hebben Nederland vertegenwoordigd bij de validatieworkshop van ENISA 'Cyber Security Aspects in the Maritime Sector' in Brussel. ENISA heeft in 2011 een eerste EU-rapport op het gebied van cybersecurity-uitdagingen in de maritieme sector gepubliceerd. Het rapport geeft een analyse van de digitale kwetsbaarheden en geeft een overzicht van bestaande initiatieven. Op basis hiervan worden aanbevelingen gedaan om cybersecurity in de maritieme sector op een hoger plan te brengen. De werkwijze van CPNI.NL en de dit jaar opgezette Haven-ISAC worden in het rapport nadrukkelijk genoemd als good practice.

ELECTRONIC CRIMES TASKFORCE (ECTF)

Het Korps Landelijke Politiediensten (KLPD), het Landelijk Parket, de banken en CPNI.NL slaan de handen ineen bij het voorkomen en aanpakken van digitale criminaliteit zoals fraude met internetbankieren. De organisaties gaan samenwerken in de Electronic Crimes Taskforce (ECTF), ook wel het 'bankenteam' genoemd. CPNI.NL vervult in deze publiek-private samenwerking een faciliterende rol.

De focus van de ECTF ligt vooral op financiële malware, phishing-aanvallen en andere cybercrime-gerelateerde incidenten die gericht zijn tegen de financiële sector. Tien miljoen via internet bankierende klanten zijn een aantrekkelijk doelwit voor criminelen. De afgelopen jaren is de schade door phishing-aanvallen dan ook fors toegenomen. Volgens de Nederlandse Vereniging van Banken bedroeg de schade als gevolg van fraude met internetbankieren in 2010 maar liefst 9,8 miljoen euro. In 2009 was dit nog 1,9 miljoen euro.

Veilig en betrouwbaar betalingsverkeer is van groot belang voor de stabiliteit en integriteit van het financiële stelsel. De samenwerking in de ECTF brengt daarvoor unieke en specifieke kennis, informatie en expertise samen. Dat zorgt voor betere analyses en versterking van de informatiepositie om cybercrime aan te vallen. In de Verenigde Staten en Groot-Brittannië zijn dergelijke 'bankenteams' al succesvol gebleken.

Deelnemers wisselen publiek-private informatie uit om gezamenlijk op te treden tegen cybercriminelen met als resultaat:

- betere analyses en een sterkere informatiepositie;
- voorstellen voor interventies (preventieve of repressieve maatregelen zoals het opwerpen van drempels of barrières);
- concrete (onderzoeks)voorstellen voor een effectieve bestrijding.

CPNI.NL heeft actief meegewerkt aan de totstandkoming van het projectplan en het convenant voor het ECTF. In de uitvoering dragen medewerkers van CPNI.NL bij aan de evaluatie van dit initiatief en het overbrengen van de lessons learned naar de sectoren van het IKC. Verder zoeken zij mogelijke relevante samenwerkingspartners.

Het bankenteam is gehuisvest bij het KLPD. Na een jaar wordt de samenwerking geëvalueerd.

JAN WILLEM SCHOEMAKER | Security Officer en Business Continuity Manager bij het Erasmus MC en voorzitter van de Special Interest Group Informatiebeveiliging (SIG IB) van de Nederlandse universitaire medische centra.

“Eind vorig jaar hebben we een calamiteit gesimuleerd in ons kinderziekenhuis. Dan gaan de ogen wel open!”

CPNI.NL verzorgt twee keer per jaar input in het overleg van de Special Interest Group Informatiebeveiliging (SIG IB) van de Nederlandse universitaire medische centra. In 2011 hebben CPNI.NL, SIG IB en het IB-overleg van de algemene ziekenhuizen afgesproken de samenwerking te versterken. In het voorjaar van 2012 gaat dit bredere samenwerkingsverband van start. Jan Willem Schoemaker: “Je krijgt toegevoegde waarde van andere partijen, want bij de AIVD en het KLPD zit kennis, deskundigheid en ervaring die we goed kunnen gebruiken. En bij landelijke CPNI.NL-overleggen leg je contacten met mensen die je verder kunnen helpen.”

Wat is het belangrijkste thema in de SIG IB?
“We proberen de beschikbaarheid, integriteit en vertrouwelijkheid van informatie te waarborgen voor onze instellingen, de acht UMC’s in Nederland. Elk van hen heeft een of meer vertegenwoordigers in ons overleg. De SIG IB is in 2004 ontstaan naar aanleiding van de NEN 7510 Medische informatica - Informatiebeveiliging in de zorg. Ik was toen net bij het Erasmus MC komen werken, mijn eerste ervaring als security officer in de zorgsector. Om het werkveld te leren kennen zocht ik mijn collega’s op. Zo is het overleg ontstaan.”

Vanwaar nu die uitbreiding naar de algemene ziekenhuizen?
“De Inspectie voor de Gezondheidszorg heeft het toezicht verhoogd en eiste dat ieder ziekenhuis voor eind 2010 een onafhankelijk oordeel over informatiebeveiliging kon overleggen. Dit is aanleiding geweest om de samenwerking uit te breiden en onze kennis combineren. Daarnaast kwam er in het najaar van 2011 een nieuwe versie van de NEN-norm uit.

In de SIG IB vraag ik aan mijn collega’s of ze onderwerpen hebben voor CPNI.NL, dan regelen zij daar een spreker voor. Een voorbeeld is het dreigingenbeeld, en of dat alleen in de zorg speelt of ook bij bijvoorbeeld de banken. Ik ga zelf naar landelijke CPNI.NL-bijeenkomsten. Een van de onderwerpen daar is bijvoorbeeld process control security. Als ziekenhuis hebben wij daar ook mee te maken vanwege onze gebouwinstallaties.”

“Ook vanuit de algemene ziekenhuizen komen nu dergelijke vragen, vandaar dat we het overleg breder hebben getrokken. Je krijgt toegevoegde waarde van andere partijen, want bij de AIVD en het KLPD zit kennis, deskundigheid en ervaring die we goed kunnen gebruiken. En bij landelijke overleggen hoor je meer over hoe het er in andere vitale sectoren aan toe gaat. Daar leg je contacten met mensen die je verder kunnen helpen.”

Is het werkveld veranderd sinds de oprichting van de SIG IB in 2004?
“We behandelen een steeds breder scala aan onderwerpen. In het begin waren de UMC’s qua informatievoorziening nog gesloten bolwerken. Patiënteninformatie bleef grotendeels binnen het ziekenhuis. Dat verandert, er wordt veel meer informatie uitgewisseld. Al die koppelingen zijn een uitdaging voor de informatiebeveiliging. In het proces is de nadruk verschoven van het implementeren van de NEN-norm naar aandacht voor risicoanalyse en managementsystemen: waar loop ik de grootste risico’s en moet ik maatregelen nemen en continu monitoren met behulp van een Information Security Management Systeem (ISMS).”

Aan de muur van Schoemakers kantoor hangen posters van oude en nieuwe veiligheids-campagnes uit het Erasmus MC. De menselijke factor van veiligheid wordt benadrukt met slogans als 'Wie gaat er met uw identiteit op de loop?' en 'Veiligheid ook jouw zorg!'

Het gaat bij het Erasmus MC dus niet meer alleen puur over informatiebeveiliging maar meer over integrale veiligheid, in samenhang met fysieke en personele aspecten?
"We hebben het steeds meer ook over die andere aspecten van veiligheid: hoe ga je om met gevaarlijke stoffen, hoe zit het met de fysieke beveiliging? Een ziekenhuis is semi-openbare instelling. Maar toch moeten we toe naar zonering, plekken achter de paslezer waar alleen medewerkers kunnen komen. Dat is in een ziekenhuis lastig door de combinaties van functies. Als Business Continuity Manager help ik het Erasmus MC goed voorbereid te zijn op calamiteiten, ongeacht aard en oorzaak. Dat kan een stroomstoring zijn maar ook een bezetting of wateroverlast. Alle afdelingen moeten van tevoren weten wat ze dan gaan doen."

En in de SIG IB?
"In de NEN-norm gaat maar één hoofdstuk over continuïteitsbeheer, dus in het SIG IB-overleg gaat het momenteel nog meer over informatiebeveiliging dan over Busines Continuity Management (BCM). Bij het Erasmus MC heb ik in 2004 een statusbepaling gedaan op alle onderwerpen uit de NEN 7510. Continuïteitsbeheer kwam hieruit als een van de prioriteiten naar voren. Een structurele en geïntegreerde aanpak van veiligheid is mijn stokpaardje. Ikzelf verenig de functies van Security Officer en Business Continuity Manager, maar dat is niet in elk UMC zo. Ook daarom gaat het in het overleg toch vooral over informatiebeveiliging."

De zorgsector is het afgelopen jaar onderzocht in het kader van het Capaciteitsadvies Elektriciteit en Telecom/ICT (CAET). Wat is het belang van stroom en telecommunicatie voor de zorg?
"Stroom is van levensbelang. Als een ziekenhuis geen betrouwbare stroomvoorziening heeft, mag er niet worden geopereerd en ook geen intensive care worden gevoerd. Bij calamiteiten merk je wel dat de keten van behandeling leegloopt, dus de druk van de chirurgen die zo snel mogelijk weer willen starten met opereren is hoog. Maar het moet toch eerst veilig zijn. BCM heeft dus consequenties voor de hele bedrijfsvoering."

"Bij telecommunicatie ligt het genuanceerder. De meest dringende kwestie is dat veel handelen in de zorg hangt op communicatie. De arts moet de uiteindelijke beslissing nemen over een behandeling, dus die moet bereikbaar zijn. In het Erasmus MC is de telefonie gedeeltelijk VoIP, dus daarin zijn we al afhankelijker geworden van netwerken dan in 2003, toen we alleen maar vaste lijnen hadden. Daar is dus een noodcentrale voor nodig. Dat werd ons wel ons duidelijk toen de overgang naar de nieuwe telefooncentrale in eerste instantie problemen opleverde en de noodcentrale moest worden ingezet."

Hoe wordt BCM vormgegeven in de zorg?
"Bij het Erasmus MC vinden we dat je BCM integraal moet aanpakken. We hebben de opzet, inhoud en het beheer van de continuïteitsplannen daarom overal op dezelfde manier ingericht. Er zijn uiteraard aparte plannen voor bijvoorbeeld het kinderziekenhuis of de afdeling radiologie, maar wel met onderlinge samenhang.

Als je de organisatie van de instelling herinricht kun je afdelingensplannen ook veel makkelijker verschuiven omdat de structuur hetzelfde is."

"Gelukkig dringt dat besef ook door in andere academische en algemene ziekenhuizen. Daarover wisselen we in losse initiatieven al informatie uit. Ziekenhuizen raken steeds meer van elkaar afhankelijk. Het Elektronisch Patiëntendossier (EPD) stelt strenge eisen aan het veilig beschikbaar stellen en uitwisselen van informatie. Het nieuwe EPD moet dus noodvoorzieningen hebben die dubbel zijn uitgevoerd."

Hoe ver kun je gaan in veiligheid?
"We gaan steeds nadrukkelijker nadenken over wat er allemaal gebeurt in een crisissituatie, maar daar zit wel een grens aan. Neem bijvoorbeeld onze neonatologie-IC, een van de grootste van Nederland. Het liefst wil je daar in geval van nood een exacte kopie van hebben waar je onmiddellijk dezelfde zorg kunt leveren, maar dat is gewoon niet haalbaar. En dan heb je ook nog bezuinigingen in de zorg... De grenzen aan de veiligheid worden heel pijnlijk wanneer het persoonlijk wordt, bijvoorbeeld als jouw kindje op die neonatologie-IC ligt en deze afdeling door een calamiteit wordt getroffen. Ook dan blijven wij verantwoordelijk voor de zorg voor dat kindje. Dat is voor ons een grote uitdaging."

Wat is de truc om ervoor te zorgen dat veiligheid integraal en in samenhang vorm krijgt?
"Risicoanalyse, het gebruik van managementsystemen en integrale veiligheid zijn drie trends in opkomst, niet alleen bij het Erasmus MC maar ook bij andere UMC's. We kijken niet meer alleen naar één onderwerp, maar nemen een aantal onderwerpen met betrekking tot veiligheid bij elkaar. In 2012 starten we hier in het ziekenhuis met een systematiek waarbij elke afdeling ieder maand over een bepaald veiligheidsaspect een vragenlijst invult. Dat kan gaan over informatiebeveiliging, medicatieveiligheid of personele veiligheid. Al die antwoorden komen via de planning- en controlcyclus bij elkaar. Dat levert trends op voor het hele Erasmus MC en maakt een geïntegreerde aanpak van verbeteringen mogelijk. We stemmen maatregelen ook zoveel mogelijk af met de mensen die het werk doen, zodat ze zien wat het oplevert. Wat ook helpt is veel oefenen. Eind vorig jaar hebben we een calamiteit gesimuleerd in ons kinderziekenhuis. Dan gaan de ogen wel open!"

Hoe zit het met de benodigde management awareness?
"Die wisselt nu nog sterk. Voor informatiebeveiliging is dat bewustzijn bij het management wel groeiende. Voor BCM zijn er wat incidenten geweest, zoals een brand in een stroomverdeler in het Erasmus MC in 2006. Het VU MC was door een brand in 2007 langdurig een belangrijk deel van de operatiecapaciteit kwijt. Dat is toen opgelost met noodvoorzieningen in portacabins. Maandenlang draaide het personeel dubbele diensten om het op te lossen, maar op een gegeven moment is de rek er dan helemaal uit. Ook dat verhoogt de awareness bij managers."

Welke rol speelt CPNI.NL nu en in de toekomst in de SIG IB?
"Als we nu groot acuut beveiligingsincident zouden hebben, dan is CPNI daar niet voor ingericht natuurlijk. Maar we kunnen wel veel sneller terecht bij overheidinstanties want daar hebben we nu contacten. CPNI.NL is immers vooral een netwerkorganisatie. Daarom willen

we dat overleg ook versterken. De toegevoegde waarde is tot nu nog te beperkt. We doen wel ons voordeel met de presentaties die ze regelen, maar we willen toch meer gebruik gaan maken van de beschikbare kennis en ervaring over nieuwe ontwikkelingen op beveiligingsgebied. We willen tijdig weten wat de dreiging is, in plaats van dat die ons gewoon overkomt. Vaak is zo'n dreiging immers al in een andere sector begonnen. En als er een andere vitale sector is die bepaalde onderdelen van integrale veiligheid al perfect geregeld heeft, dan kunnen we daar eens een middagje gaan praten en tools en methodes uitwisselen. Het zou mooi zijn als CPNI.NL ook zelf concrete onderwerpen aan zou bieden voor de zorg, zoals ze dat op de landelijke bijeenkomsten doen."

Heeft u nog tips voor het vormgeven van BCM voor zorginstellingen die nog aan het begin van die ontwikkeling staan?
"Het is een beetje een open deur, maar management commitment is wel heel belangrijk. Waar ik voor pleit is een structurele aanpak van BCM want dat is zeker bij grotere zorginstellingen nodig. Wij hebben in 2004 eerst een pilot op een afdeling gedaan. Toen dat goed bleek te gaan is BCM in de hele organisatie ingevoerd."

"In een grote organisatie als het Erasmus MC is men terughoudend in het treffen van noodvoorzieningen. Dat is voor mij ook een leerproces geweest. Ik kwam uit de wereld van de computerbeveiliging, waar computeruitwijk vanzelfsprekend is. Als computer A platligt, schakel je over op computer B en je test die noodvoorziening uit totdat deze werkt. Maar in de zorg heb je te maken met heel gebouw vol verpleegafdelingen. Daar willen ze niet nadenken over de hoeveelheid noodopvang als er nog niets aan de hand is. Dat regelen ze wel onderling als het zo ver is. Daar zijn nog barrières te overwinnen. Wees je daarvan bewust als je met zorgverleners praat en probeer ze ervan te doordringen dat zich ieder moment van de dag een situatie kan voordoen waarin ze meteen moeten handelen. Daar zijn we nog lang niet mee klaar. Het beste werkt dan toch een oefening of een echt incident. Na een simulatie in ons laboratorium zei het hoofd van de afdeling: 'Toch goed dat we dat eens hebben geoefend.' Zoiets hoor ik graag."

MIJLPALEN

3 JANUARI
CPNI.NL start bij TNO | Soesterberg

27 JANUARI
Lancering CPNI.NL tijdens NICC-winterborrel bij TNO | Soesterberg

22 FEBRUARI
Presentatie Nationale Cyber Security Strategie | Den Haag

14 MAART
Kick-off ECTF en ondertekening convenant | Den Haag

25 MAART
Final workshop NEISAS project | Londen

11 APRIL
Start projectfase Cyber-TEC

11 APRIL
Rapport kwalificatie en certificatie informatiebeveiligers

20-21 APRIL
European FI-ISAC | Rome

11 MEI
Smart Grid Conferentie Alliander | Bussum

17 MEI
Schiphol Information Security Awareness Symposium | Schiphol

CAPACITEITSADVIES ELEKTRICITEIT EN TELECOM/ICT (CAET)

Hoe weerbaar zijn de vitale sectoren tegen grootschalige uitval van elektriciteit en telecom/ICT? Het vorige kabinet is onder de titel Capaciteitsadvies Elektriciteit en Telecom/ICT (CAET) een traject gestart om die vraag te beantwoorden. In opdracht van de ministeries van Economische Zaken, Landbouw en Innovatie en Veiligheid en Justitie voert CPNI.NL dit onderzoek uit.

CAET geeft inzicht in de weerbaarheid van vitale sectoren tegen ernstige verstoringen in de elektriciteit- en telecommunicatiesector. Het geeft ook aan op welke plaatsen die weerbaarheid groter zou moeten zijn. Door de onderzoeken in de sectoren is er een bewustwordingsproces op gang gekomen. Vitale sectoren realiseren zich hoe afhankelijk ze zijn van elektriciteit en telecommunicatie, denken na over de reeds genomen maatregelen en gaan in discussie over mogelijke aanvullende maatregelen. Het feit dat de witte vlekken gedurende het proces inzichtelijk zijn geworden, heeft al direct geleid tot activiteiten van de sectoren zelf.

Het CAET-traject heeft veel losgemaakt in de onderzochte sectoren. Er zijn diverse discussies ontstaan binnen de bedrijven, tussen bedrijven en leveranciers, binnen de sectoren en tussen de sectoren. Deze discussies hebben een beweging in gang gezet die een grote meerwaarde is van dit traject. Uiteindelijk zijn het immers de bedrijven zelf die de maatregelen moeten treffen om zorg te dragen voor de continuïteit van hun dienstverlening.

De sectoren elektriciteit en telecommunicatie hebben een actieve rol gespeeld door deel te nemen aan de workshops van alle vitale sectoren. Het doel van deze workshops was om het inzicht in de onderlinge afhankelijkheden te vergroten en samen na te denken over maatregelen om de weerbaarheid te vergroten. CAET heeft er zo toe geleid dat de contacten tussen de vitale sectoren enerzijds en telecommunicatie en elektriciteit als toeleverende sectoren anderzijds zijn verstevigd.

In samenspraak met het verantwoordelijke vakdepartement en vertegenwoordigers uit de sector heeft CPNI.NL het bereik van het sectorale onderzoek vastgesteld. In totaal zijn de afgelopen jaren twaalf sectoren doorgelicht. In de tabel op de volgende pagina vindt u deze sectoren en de bestudeerde vitale onderdelen.

De onderzoekers hebben de bevindingen uit interviews, desk research, bijeenkomsten en workshops opgenomen in de sectorale rapportages. Deze rapportages zijn besproken in bijeenkomsten met vertegenwoordigers van de sectoren en de vakdepartementen. Ook dit leidde tot zinvolle discussies en aanscherping van de rapportages.

	VITALE SECTOR	VAKDEPARTEMENT	VITALE PRODUCTEN OF DIENSTEN
FASE 1	Telecom	EL&I	Vast, mobiel en internet
	Elektriciteit	EL&I	Transport, distributie en handhaven energiebalans
	Financiën	FIN	Betalings- en effectenverkeer
	Gas	EL&I	Winning, behandeling, transport en distributie
FASE 2	Drinkwater	I&M	Winning, zuivering en distributie van drinkwater; crisiscoördinatie
	Keren en beheren oppervlaktewater	I&M	Openen en sluiten van vitale keringen en het draaien van vitale gemalen
	Olie	EL&I	Raffinage, opslag, distributie en transport
	Openbare Orde en Veiligheid	V&J	· Handhaving openbare orde (handhaving politie) · Handhaving openbare veiligheid (respons brandweer) · Handhaving openbare veiligheid (noodhulp politie en GHOR) · Ambulancezorg (noodhulp politie)
	Openbaar Bestuur	BuZa V&J BZK	· Diplomatieke communicatie · Informatieverstrekking overheid (media en publieksvoorlichting in crisistijd) · Besluitvorming openbaar bestuur (functioneren van de nationale en regionale crisisbesluitvorming) · Vier basisregistraties GBA, NHR, BAG, BRK
FASE 3	Gezondheidszorg	VWS	Spoedeisende zorg, essentiële medische producten en sera en vaccins
	Rechtsorde	V&J	Rechtspleging, rechtshandhaving en detentie (rechtspraak, OM en DJI)
	Transport	I&M	Mainport Schiphol, Mainport Rotterdam, Hoofd-wegen- en Hoofdvaarwegennet (Rijksinfrastructuur)
	Voedsel *	EL&I	Voedselvoorziening en –veiligheid
	Chemische en Nucleaire Industrie *	I&M EL&I	Vervoer, opslag en productie/ verwerking van chemische en nucleaire stoffen

* Voor de sectoren Voedsel en Chemie/Nucleair is een notitie opgesteld in plaats van een rapportage.

Duidelijk is dat er verschillen tussen de sectoren bestaan in bewustzijn van de afhankelijkheid van elektriciteit en telecommunicatie en ook in genomen maatregelen:

- om de kans op een gebeurtenis te verminderen;
- om de impact van een gebeurtenis te verminderen;
- om de respons op een gebeurtenis zo goed mogelijk te laten zijn.

Zo beschikt bijvoorbeeld een gedeelte van de sector elektriciteit over een eigen telecommunicatienetwerk dat bij uitval van het openbare netwerk kan worden gebruikt. Andere sectoren zoeken het in het maken van goede afspraken met de leveranciers van telecommunicatiediensten.

De sectoren en vakdepartementen werken de aanbevelingen verder uit en beoordelen welke aanvullende maatregelen wenselijk en haalbaar zijn. Zij doen dit op basis van een afgewogen risicoanalyse, waarin ze de bevindingen van de CAET-rapporten gebruiken. In het voorjaar van 2012 wordt een afsluitende bijeenkomst georganiseerd om de bevindingen en aanbevelingen te delen, bijvoorbeeld:

- het bevorderen van management awareness op de continuïteit van de kritische processen en vooral de afhankelijkheid van elektriciteit en telecommunicatie;
- het verder definiëren van kritische processen in de vitale sectoren;
- het positioneren van continuïteitsmanagement in de organisatie;
- het bevorderen van integrale veiligheid en continuïteitsmanagement;
- het maken van duidelijke afspraken met partijen aan wie onderhoud en beheer van ondersteunende systemen zijn uitbesteed;
- het stimuleren van informatie-uitwisseling tussen vitale sectoren.

De intersectorale samenwerking heeft geleid tot meer inzicht in elkaars afhankelijkheden, meer en betere risicoanalyses, en passende maatregelen en afspraken.

LESSONS LEARNED VITAAL

Inzicht in incidenten helpt bij de realisatie van een meer robuuste infrastructuur. Het CPNI.NL-project Lessons Learned Vitaal maakt deze inzichten breed en sectoroverstijgend toegankelijk via de CPNI.NL-site. Niet alleen op het gebied van cybercrime, maar ook als het gaat om fysieke en personele veiligheid.

De aanleiding voor de start van het project 'Lessons Learned Vitaal' in 2011 waren cascade-uitvalincidenten en near misses in de vitale sectoren. Voorbeelden daarvan zijn de grootschalige Europese energie-blackout in november 2006 en soortgelijke kleinere incidenten op lokaal niveau. Het project bouwt voort op een door TNO onderhouden incidentendatabase die al is gebruikt in enkele Nederlandse en Europese projecten, waaronder CAET en de NRB. Het project wordt in fases uitgevoerd.

In fase 1 is een verkenning uitgevoerd naar te ontsluiten gegevensbronnen, de wijze waarop de analyse wordt uitgevoerd en hoe de resultaten kunnen worden gerapporteerd. In de tweede fase wordt momenteel informatie ontsloten en een prototype ontwikkeld. Daarbij zijn Nederlandse hogescholen en universiteiten betrokken. In eerste instantie gaat het om het ontsluiten van incidenten vanuit open bronnen, maar het eindproduct moet het ook mogelijk maken om vertrouwelijke incidenten in een besloten omgeving met elkaar te delen.

Aan de incidenten worden ervaringsgegevens over impact op andere (vitale) sectoren en duur van uitval toegevoegd. Tevens wordt vastgelegd wat de oorzaak van het incident was en op welke wijze het voorkomen had kunnen worden. Op deze wijze creëert het project een uitgebreide en actuele bron van informatie. Om de kwaliteit te garanderen wordt de informatie in een controleslag getoetst en kunnen gebruikers van het informatiesysteem dit nog verder verrijken door feedback te geven op het incident. Naast de basisinformatie over een incident kan een uitgebreidere analyse worden toegevoegd. De beschikbare informatie is eenvoudig en aantrekkelijk te raadplegen.

KWALIFICATIE EN CERTIFICATIE VAN INFORMATIEBEVEILIGERS

Door de grote verscheidenheid aan opleidingen, certificaten en titels op het gebied van informatiebeveiliging is het moeilijk te bepalen of informatiebeveiligers voldoende competenties in huis hebben. Daarom kreeg CPNI.NL de vraag vanuit verschillende ISACs, het Platform voor Informatiebeveiliging (PvIB) en de Commissie Informatiebeveiliging van VNO-NCW om een onderzoek te ondersteunen naar de wenselijkheid en haalbaarheid van een Nederlands kwalificatie- en certificatiestelsel voor informatiebeveiligers.

Uit het onderzoek blijkt dat een uniform kwalificatie- en certificatiestelsel voor informatiebeveiligers nuttig en haalbaar is. Het doel daarvan is te komen tot een herkenbaar en erkend niveau van vakbekwaamheid dat toepasbaar is in alle sectoren van de samenleving, inclusief de overheid. Uniforme kwalificatie en certificatie zijn vooral zinvol (en misschien zelfs noodzakelijk) voor informatierisicomanagers op strategisch en tactisch niveau, ICT-beveiligers op strategisch, tactisch en operationeel niveau en relatief grootschalige specialistische beroepen op het gebied van informatierisicomanagement en ICT-beveiliging. Sommige van deze beroepen, zoals IT-auditor en digitaal forensisch onderzoeker, werken al met kwalificatie en certificatie.

Om een goede afstemming met de beroepspraktijk te krijgen ligt de trekkersrol bij voorkeur bij de beroepsorganisaties. Het meest voor de hand ligt het Platform voor Informatiebeveiliging (PvIB), eventueel samen met de andere beroepsorganisaties. De certificatie-instantie is bij voorkeur een onafhankelijke organisatie die daarvoor door de beroepsorganisaties is opgezet of aangewezen.

Het is nog geen uitgemaakte zaak wie het beheer van het kwalificatie- en certificatiestelsel op zich kan nemen. Bovendien is er nog geen goed financieel plaatje voor het kwalificatie- en certificatiestelsel.

Het onderzoek is gedeeld met en getoetst door de ISACs. Het eindresultaat is openbaar gemaakt aan VNO-NCW, het kwartiermakersteam van het Nationaal Cyber Security Centrum, de InfoSecurity-vakbeurs, vakbladen, het CIO-platform en CIO's van de overheid.

MIJLPALEN

15 JUNI
Afronding CAET fase 2 en start fase 3

24 JUNI
Economical Espionage Event van de Multinationals-ISAC

27 JUNI
EuroSCSIE-bijeenkomst | Heraklion

30 JUNI
Benelux-top over Cyber Security; installatie Cyber Security Raad | Den Haag

20 JULI
Kick-off Haven-ISAC

18 AUGUSTUS
CEO-diner Cyber-TEC | Den Haag

26 AUGUSTUS
Start Managed Service Providers-ISAC

MIKE VISSCHER | Consultant Information Security bij Luchtverkeersleiding Nederland (LVNL) en sinds 2010 voorzitter van de Airport-ISAC.

SCHIPHOL INFORMATION SECURITY AWARENESS SYMPOSIUM

De Airport-ISAC organiseerde op 17 mei 2010 het eerste Schiphol Information Security Awareness Symposium (SISAS). Dit symposium had als doel het verhogen van de security awareness van de negentig deelnemers, die werkzaam zijn bij bedrijven op en rond Schiphol.

Jan de Boer van CapGemini, gaf een presentatie over social engineering. Arno Reuser van het ministerie van Defensie benadrukte het belang van training, omdat beveiligingsmaatregelen vaak te ingewikkeld zijn om effectief toe te passen. Jos Weyers van Tennet liet zien dat veel sloten makkelijk te kraken zijn met tools die gewoon te koop zijn op internet. Wim Holthuis van Luchtverkeersleiding Nederland legde de best practices van de LNVL uit: koppeling van fysieke beveiliging en internetbeveiliging door middel van een security management systeem, waarvoor dan wel de hele keten moet samenwerken. Kees Jans, CIO van de Schiphol Group, benadrukte het belang van informatiebeveiliging en een integrale aanpak daarvan.

Op www.cpni.nl/events/schiphol-information-security-awareness vindt u een kort verslag van het SISAS.

“Mensen triggeren voor korte tijd is niet moeilijk. Het vasthouden en continu verbeteren van het bewustzijnsniveau is het lastigst”

De deelnemers aan de Airport-ISAC zijn Information Security vertegenwoordigers van bedrijven die een directe en belangrijke relatie hebben met de hoofdactiviteiten op en rond Schiphol. Samen kwamen ze tot de conclusie dat informatiebeveiliging en fysieke beveiliging niet van elkaar te scheiden zijn. Dus organiseerden ze een symposium voor alle partijen die met de beveiliging in en rond Schiphol te maken hebben.

Vanwaar een symposium voor een bredere doelgroep dan alleen ISAC-leden?
“In de ISAC groei je samen naar een bepaald bewustzijn over information security toe. We onderhouden contacten met het Platform Beveiliging en Publieke Veiligheid Schiphol. Ook daar wordt steeds meer onderkend dat fysieke beveiliging een link heeft met informatiebeveiliging, want informatie ligt in gebouwen. Die twee werelden groeien naar elkaar toe. Dan is het goed om overleg te plegen over wat voldoende fysieke beveiliging inhoudt. Bij beide ga je immers uit van dreigingen, risico’s en de maatregelen die je kunt nemen. Het leek ons een goed idee om iets te organiseren voor andere partijen die werkzaam zijn op Schiphol maar niet aangesloten bij de Airport-ISAC. Ook zij spelen een rol in de beveiliging van het Schipholproces.”

Wat was het doel van het eerste Schiphol Information Security Awareness Symposium (SISAS, zie kader)?
“In de Airport-ISAC is ons doel information security management naar een hoger plan te tillen. Maar je hebt altijd te maken met andere bedrijven op Schiphol, die ook schakels in die keten vormen. Als daar iets gebeurt, kan dat doorwerken op het operationele proces van Schiphol. De afhandeling van het vliegverkeer mag daardoor niet verstoord worden, dus met onze beperkte club binnen de ISAC wilden wij ons bewustzijn over de risico’s en dreigingen, en de overlap tussen fysieke en informatiebeveiliging, delen met andere betrokken partijen.”

Hoe is het programma tot stand gekomen?
“We hebben alle ISAC-deelnemers gevraagd waar hun partners behoefte aan hebben. Zij kwamen met voorstellen voor presentaties. Ook CPNI.NL dacht als gelijkwaardige partner met ons mee over interessante sprekers en wat die zouden moeten vertellen. Wat er uit die wisselwerking kwam is in de ISAC afgestemd, zodat we een volwassen programma konden samenstellen. Het was wel makkelijk dat CPNI.NL de meeste sprekers al kenden van andere presentaties, dus zij hebben de meeste mensen ook benaderd.”

Het lijkt vanzelfsprekend dat security awareness, zowel fysiek als virtueel, op het netvlies staat van iedereen die werkt op en rond Schiphol. Wat hadden de deelnemers aan het SISAS nog te leren?
“Juist zo’n specialisme kan leiden tot beroepsblindheid. Je focust alleen op je eigen werk en zorgt dat je dat goed op orde hebt. Maar als je geen oog hebt voor de security-aspecten buiten je eigen aandachtsgebied, kun je toch iets over het hoofd zien. Een gebouw en systemen kun je heel goed beveiligen. Maar soms werken bedrijven met een externe partner die via een internetverbinding de systemen onderhoudt. Als je niet weet hoe goed ze dat beheren, zet je mogelijk de poort open naar je bedrijfsinformatie. Je kunt nog zo goed je fysieke schil op orde hebben en alles afschermen met firewalls en wacht-

woorden, maar als je niet op dat soort dingen let is er toch nog een weg naar binnen."

Hebben de sprekers hun publiek een beetje wakker kunnen schudden?
"Anno Reuser van het ministerie van Defensie kwam net terug uit Amerika met een laptop vol informatie over internet security en open source intelligence. Als die losbrandt word je overvallen door stortvloed aan opmerkelijke feiten en security-voorvallen! Dat was een goede start. Zelf vond ik Jos Weyers' verhaal over het openbreken van sloten een eyeopener. Hij is lid van The Open Organisation Of Lockpickers (TOOOL). Hij demonstreerde diverse methoden om sloten te forceren. Met een blanco sleutel die hij slechts twee keer bij moest vijlen had hij een duur slot in no time open. Dan besef je pas dat een slot als enige beveiliging van de computerkast in de serverruimte makkelijk te doorbreken is, en ook dat je dat onopgemerkt kunt doen. Dus moet je de toegang tot die ruimte eerst beperken. Andere sprekers gingen meer in op het management van security: hoe hebben we dingen geregeld, hoe zou het kunnen, hoe goed doe je het ten opzichte van anderen?"

Hoe hebben de deelnemers aan het SISAS de dag ervaren?
"Mijn indruk is dat het programma zeer goed ontvangen is, en ook uit de enquête bleek dat men erg enthousiast was. Het publiek was natuurlijk heel divers. Voor de ISAC-leden zelf was het informatief. We hadden verder al onze eigen contactpersonen uitgenodigd die met security bezig zijn, en daarnaast andere relevante bedrijven en organisaties uit de Schipholsector een algemene uitnodiging gestuurd. Daar zaten ook deelnemers tussen die vrij hoog in de organisatie zitten, zoals CIO's en managers beveiliging. Voor wie alleen de eigen organisatie kent was het symposium een eyeopener. Het is moeilijk te zien of daar al wat door gaat bewegen. Ik hoop dat ze van het SISAS in ieder geval één nieuw idee meenemen, bijvoorbeeld betere sloten installeren. Ikzelf heb dat in ieder geval meteen teruggekoppeld naar degene die bij LVNL voor fysieke beveiliging verantwoordelijk is. Regelmatig praat ik met onze beveiligers, dus zo verspreidt zo'n praatje zich wel verder. Hopelijk doen de andere deelnemers dat ook."

Komt er een vervolg?
"We gaan kijken of we in 2012 een tweede symposium kunnen organiseren. De mensen zijn wakker geschud, dus hebben we in het ISAC besproken op welke onderwerpen we dieper in zouden kunnen gaan. Het programma is nog niet definitief maar mogelijke onderwerpen zijn het Nieuwe Werken, social media en natuurlijk security awareness. Het programma zal, net als de vorige keer, zowel informatief als praktisch van aard zijn."

Op welke plek in een bedrijf kun je het beste beginnen met het verbeteren van Security Awareness?
"Bij degene die security coördineert. Dat is sterk afhankelijk van de organisatie. Bij LVNL hebben we daar in mijn persoon een aparte functionaris voor. In kleinere organisaties is security soms de neventaak van een directeur of manager. Daar moet je dus bovenaan beginnen, al is het wel belangrijk dat het bewustzijn 'landt' bij de mensen op de werkvloer. Alle informatie gaat immers door hun handen. Kijk, mensen voor korte tijd triggeren is niet moeilijk. Het vasthouden en continu verbeteren van het bewust-

zijnsniveau is het lastigst. Dat betekent een cultuurverandering. En dan heb je soms meer aan een bevlogen directeur die met de vuist op tafel slaat en middelen vrijmaakt, dan aan een speciaal daarvoor aangestelde functionaris die een roepende in woestijn is."

"Om directeuren en managers te triggeren is helaas vaak eerst een incident nodig. Het afgelopen jaar, met incidenten als DigiNotar, heeft wel geholpen om het bewustzijn van de risico's te vergroten. Omdat je aansprekende voorbeelden kunt aanhalen wordt het steeds makkelijker om je punt duidelijk te maken."

Kunt u een blik in de toekomst van de information security werpen?
"Ik denk dat er over tien jaar heel wat veranderd is want de ontwikkelingen in het technologie- en ict-landschap gaan snel. Hopelijk krijgen we steeds meer security by design, dus beveiliging die al is ingebouwd vanaf het eerste ontwerp van een systeem. Die tendens is er nu al. Ik zie informatiebeveiliging en fysieke beveiliging naar elkaar toegroeien. Maar het zal toch altijd wel een kat-en-muisspel blijven tussen degene die de beveiligingsmaatregelen implementeert en degene die ze probeert te omzeilen. Dat is koorddansen, want de beveiligingsmaatregelen moeten wel in verhouding tot het nut staan. Overal dikke stalen deuren tussen plaatsen werkt ook niet. Voor de jeugd is chatten en van alles op internet zetten vanzelfsprekend. Ze willen de bedrijfsmail op hun smartphone ontvangen. Als je dat niet toestaat gaan ze er omheen werken, met alle gevolgen van dien, dus kun je dat beter op een veilige manier mogelijk maken. Op die manier houd je als bedrijf de controle. Je ziet gelukkig dat de overheid steeds meer voorlichting geeft over veilig gebruik van het internet, want cybercrime is een lucratieve business waarin honderden miljoenen worden verdiend. Ik zou er voor willen pleiten om die voorlichting al in opleidingen mee te nemen, want jongeren zijn zich niet bewust van de gevaren van hun openheid in bijvoorbeeld social media. Als je daar op school al aandacht aan besteedt, zijn mensen zich daar al meer bewust van zodra ze het werkproces in gaan."

Welke cybersecurity-onderwerpen zijn in 2012 voor Schiphol het belangrijkst?
"Dan heb je het over mobile devices, bedrijfsspionage en de impact op de Schipholsector, business continuity en de link met de ICT Response Board van het NSCS."

Heeft u nog tips voor collega's?
"Probeer te denken als een hacker. Ik lees zelf veel over hun manier van werken. Het gaat niet eens om technische hoogstandjes. Met een combinatie van fysiek en social engineering kom je vaak al een heel eind binnen. Zoek eens op termen als 'password' of 'vertrouwelijk' in je eigen systeem en kijk wat er boven water komt. En wat is er op het internet allemaal over jezelf te vinden? Social engineering kan heel ver gaan. Goed beschouwd zijn wij security officers zelf een interessant doelwit. Wij hebben inzicht in hoe de beveiliging in elkaar steekt, informatie die voor een hacker zeer interessant is. Als je je dat realiseert, profileer je jezelf dan nog steeds openlijk als security professional op bijvoorbeeld LinkedIn?"

NATIONALE ROADMAP VOOR VEILIGE PROCESCONTROLESYSTEMEN

De Nationale Roadmap voor veilige procescontrolesystemen is in 2011 gestart om het bewustzijn over de noodzaak tot het beter beveiligen van dit soort systemen op een hoger niveau te brengen. Daarvoor zijn het afgelopen jaar diverse activiteiten ontplooid op het gebied van kennis- en nieuwsvoorziening, opleiding en training. Verder heeft CPNI.NL actief gewerkt aan kennisoverdracht en het opbouwen en onderhouden van netwerken.

Mede ondersteund door de inspanningen van CPNI.NL en door de actuele dreiging van Stuxnet staat de security van procescontrolesystemen (PCS) nu stevig op de agenda van bedrijven en de overheid.

Op de website van CPNI.NL ontsluit de nieuwsdatabase informatie uit openbare bronnen over ontwikkelingen op het gebied van PCS. Deze informatie wordt ook actief gedeeld via het Twitter-account '@PCS_Roadmap_NL'. In de LinkedIn-groep 'PCS Roadmap NL' (een subgroep van 'Samen tegen Cybercrime') wordt het laatste nieuws gedeeld en gediscussieerd.

In het kader van de Roadmap heeft CPNI.NL in 2011 sterk geïnvesteerd in het geven van presentaties en het faciliteren van discussies in diverse gremia. We geven hier enkele voorbeelden.

- Presentatie van onderwerpen uit de Roadmap in de Energy-ISAC, Water-ISAC, Nucleair-ISAC, Airport-ISAC, Multinationals-ISAC en PCS-Vendors-ISAC, en in de werkgroep Plant Security van de WIB.
- Workshop over process control security voor de Schiphol Group, in samenwerking met GOVCERT.NL.
- Presentaties op bijeenkomsten van:
  - VNO/NCW - MKB Nederland
  - Deloitte-conferentie over process control security
  - Norman/Actemium-seminars
  - Infosecurity.NL
  - Energy/Utilities Summits in Amsterdam
  - NISSF 2011 in Israël
- Bijeenkomsten van de Meridian Process Control Security Information Exchange, EuroSCSIE, ERNCIP en de Europese Commissie.
- Workshops over IT en process control security tijdens de World Institute Nuclear Security (WINS) in april in Wenen, en voor de werkgroep Technische Automatisering UNETI-VNI bij DAF in Eindhoven begin december.

In oktober nam een selectie van veertig Nederlanders uit diverse vitale sectoren, overheden en hun toeleveranciers deel aan de Advanced SCADA Security Red Team | Blue Team Training in Idaho Falls. Deze training werd georganiseerd door het Amerikaanse Department of Homeland Security en Idaho National Laboratories in samenwerking met CPNI.NL. Alle deelnemers hebben de week als zeer nuttig en inspirerend ervaren. Dit heeft geleid tot diverse

vervolgactiviteiten in de bedrijven waar de deelnemers werkzaam zijn.

In 2011 heeft CPNI.NL in nauwe samenwerking met gebruikers en leveranciers van PCS (waaronder veel leden van ISACs) een aanzet gemaakt voor het schrijven van whitepapers volgens een vaste manier van werken. Specialisten uit het netwerk van CPNI.NL leveren input middels workshops; in twee review-rondes wordt het concept van de whitepaper verder aangescherpt. De whitepapers 'Beveiliging van legacy proces-controlesystemen' en 'ICS Threat Landscape' zijn zo goed als af. De volgende whitepapers zullen gaan over het omgaan met removable media zoals usb-sticks, en over het integreren van informatiebeveiliging in acceptatietests (Factory Acceptance Test en Site Acceptance Test).

Daarnaast hebben medewerkers van CPNI.NL meegeschreven aan de Process Control Domain Security Good Practices voor Vendors van de WIB en de position paper Essential Regulatory Requirements and Recommendations for Data Handling, Data Safety, and Consumer Protection die is geschreven door de Task Force Smart Grids Expert Group 2 en aangeboden aan de Europese Commissie.

EU REFERENCE NETWORK FOR CRITICAL INFRASTRUCTURE PROTECTION (ERNCIP)

CPNI.NL zal de komende vier jaar coördinator zijn van de themagroep Industrial Control Systems (ICS) en Smart Grids in het EU-project European Reference Network for Critical Infrastructure Protection (ERNCIP).

ERNCIP wil komen tot standaardisatie en certificatie van security-oplossingen door de krachten op het gebied van research & development te bundelen en gezamenlijke testprotocollen op te stellen. Het wordt een Europees netwerk waarbinnen concrete werkgroepen worden ingericht op de thema's Industrial Control Systems (ICS) en Smart Grids. De themagroep ICS en Smart Grids zal jaarlijks aanbevelingen doen aan de Europese Commissie.

NATIONAL AND EUROPEAN INFORMATION SHARING AND ALERTING SYSTEM (NEISAS)

Het NEISAS-project (National and European Information Sharing and Alerting System) heeft in 2010 de functionele eisen op papier gezet voor een digitaal informatie-uitwisselingsplatform voor ISACs en Information Exchanges. Het prototype is in het eerste kwartaal van 2011 gepresenteerd.

NEISAS is een door de Europese Commissie gesponsord project dat publieke en private stakeholders bij elkaar brengt die door middel van informatie-uitwisseling het thema Critical Information Protection (CIP) aanpakken. Partners in NEISAS zijn Booz & Co., de Italiaanse overheid, ENEA, CPNI.NL (voorheen NICC), LanditD, Symantec en het Britse Ministerie van Binnenlandse Zaken. Centraal in dit project stond de behoefte om digitaal informatie uit te wisselen via een betrouwbaar platform.

CPNI.NL heeft kennis over vertrouwelijke informatie-uitwisseling ingebracht die is opgebouwd in de ISACs en het programma NICC. Andere landen hebben hun eigen methodes; NEISAS zorgt ervoor dat tussen al die verschillende modellen informatie uitgewisseld kan worden.

Het gepresenteerde prototype is een technisch platform gebaseerd op het traffic light protocol en waarborgt de vertrouwelijkheid van informatie-uitwisseling. Degene die de informatie inbrengt, houdt controle erover. Hij of zij bepaalt of de informatie alleen gelezen mag worden of bijvoorbeeld ook gedownload, hoe lang de informatie zichtbaar is en wie er toegang toe krijgt.

Eén van de pilots van het NEISAS-platform draaide in Nederland. Daaruit bleek dat een tool pas werkt als er eerst vanuit persoonlijk contact vertrouwen is opgebouwd. Op basis van de ervaringen uit de pilot zal besproken worden of het platform verder wordt ontwikkeld.

Meer informatie vindt u op www.neisas.eu.

EU-US WORKING GROUP ON CYBER-SECURITY AND CYBER-CRIME

Het doel van de EU-US Working Group on Cyber-Security and Cyber-Crime (EU-US WG) is het gezamenlijk aanpakken van nieuwe bedreigingen voor de wereldwijde netwerken waar de veiligheid en welvarendheid van vrije samenlevingen steeds meer afhankelijk van zijn.

De EU-US WG is opgericht naar aanleiding van de EU-US-top op 20 november 2010 in Lissabon. De werkgroep gaat diverse producten opleveren:

- briefings en rapporten over onderwerpen als botnets en smart grids;
- een strategie en actieplan om met de private sectoren samen te werken;
- algemene principes voor een stabiel en toegankelijk internet.

Diverse Expert-Sub Groups (ESG's) ontwikkelen een strategic framework voor publiek-private samenwerking. De nadruk ligt op meetbare resultaten bij de bestrijding van botnets, het uitwisselen van informatie met de industrie (bijvoorbeeld het snel informeren van bedrijven bij zich ontwikkelende dreigingen) en industrial control systems security (inclusief industriële controlesystemen en smart grids). CPNI.NL maakt deel uit van de ESG Publiek-Private Samenwerking, die zich richt op ICS en Smart Grids. In deze ESG zijn principes voor internationale samenwerking opgesteld. De samenwerking gaat zich vooral richten op C-level awareness, opleiding en training, informatie delen, bewustwording, incident response en testmogelijkheden. Er ligt een roadmap voor 2012 om de samenwerking daadwerkelijk op gang te brengen.

MIJLPALEN

1 SEPTEMBER
(Vice)voorzittersoverleg ISACs

8-9 SEPTEMBER
CRITIS 2011 | Luzern

22 SEPTEMBER
Presentatie over cybersecurity tijdens NOREA IT-auditorsdag 2011 | Amstelveen

28 SEPTEMBER
Presentatie tijdens ENISA workshop 'Cyber Security Aspects in the Maritime Sector' | Brussel

29 SEPTEMBER
Nazomerborrel CPNI.NL | Overveen

4 OKTOBER
(Vice)voorzittersoverleg ISACs

10-14 OKTOBER
Red Team /Blue Team training INL | Idaho Falls

24-27 OKTOBER
NAVO-bijeenkomst 2011 IRCSG Seminar | Lissabon

25-26 OKTOBER
Meridian 2011 | Qatar

Henk Geveke | Algemeen directeur Integrale Veiligheid bij TNO.

“Ik weet niet of integrale security al een frequent issue is in de Nederlandse bestuurskamers, maar dat zou het wel moeten zijn”

Sinds een jaar heeft CPNI.NL inclusief het Informatieknooppunt Cybercrime onderdak gevonden bij TNO Integrale Veiligheid. Henk Geveke heeft daar geen moment spijt van gehad. “Voor cybersecurity heb je ook kennis, onderzoek en innovatie nodig. Die driehoek tussen de overheid, het bedrijfsleven en de kennisinfrastructuur moet je creëren. Door het Informatieknooppunt Cybercrime (IKC) in te bedden in onze kennisomgeving is een goede wisselwerking ontstaan.”

Wat houdt integrale veiligheid precies in?
“Wij proberen daarmee aan te geven dat veiligheid veel dimensies kent: een nationale én een internationale, een objectieve en een subjectieve, een fysieke en een digitale, een interne en een externe, een militaire en een civiele. Dat noopt tot een samenhangende visie en aanpak. TNO Integrale Veiligheid richt zich op onderzoek en innovatie voor alle partijen die voor veiligheid zorgen: defensie, justitie, hulpdiensten als de brandweer en politie, en regionale en lokale overheden. We pakken veiligheid integraal aan omdat ontwikkelingen bij defensie ook nuttig kunnen zijn voor bijvoorbeeld de brandweer. Ook voor cybersecurity is bij uitstek een integrale en multidisciplinaire aanpak nodig. Het is niet alleen een ict-vraagstuk maar gaat ook over personele beveiliging en fysieke security. Het probleem reikt van het stelen van identiteiten of het platleggen van het internet tot het voeren van oorlog, dus zo breed pakken wij het onderwerp ook aan.”

Bij de komst van CPNI.NL naar TNO zei u: ‘TNO is trots dat het de eer krijgt om het Informatieknooppunt Cybercrime een permanente plaats in de Nederlandse samenleving te mogen geven.’ Is die trots er nog steeds?
“Die is alleen maar toegenomen. Afgelopen jaar is cybersecurity een hot issue geworden doordat de nodige incidenten aandacht hebben gegenereerd. De legitimiteit van CPNI.NL zie ik dus alleen maar bevestigd, want publieke en private partijen moeten samen oplossingen vinden. CPNI.NL is gericht op de eindgebruikers, en die hebben praktische oplossingen heel hard nodig.”

“Ik ben er ook trots op dat TNO erbij betrokken is omdat je voor cybersecurity kennis, onderzoek en innovatie nodig hebt. Die driehoek tussen de overheid, het bedrijfsleven en de kennisinfrastructuur moet je zien te creëren. Door het Informatieknooppunt Cybercrime (IKC) in te bedden in onze kennisomgeving zie ik een goede wisselwerking ontstaan.”

Is die samenwerking zo uitgepakt als u had verwacht?
“Zelfs beter dan ik had verwacht. Het is heel nuttig dat dit publiek-private platform bij ons is ingebed. TNO heeft veel relevante onderzoeksprogramma’s, bijvoorbeeld op het gebied van kritische infrastructuren, informatiebeveiliging en het toekomstig gebruik van internet. Daar komen analyses en oplossingen uit die kunnen worden gebruikt in de ISACs. Omgekeerd is het ideaal dat de praktijkmensen uit de ISACs nu bij TNO zo makkelijk in contact komen met toegepaste wetenschappers die bekend zijn met het veld en praktische oplossingen kunnen verzinnen voor hun problemen. Omdat we bij elkaar in huis zitten, ontstaan er vanzelf nieuwe netwerken: mensen vinden elkaar sneller.”

De slogan van TNO is ‘Innovation for life’. Daar spreekt een groot vertrouwen uit in technische oplossingen. In het netwerk van CPNI.NL hoor je vaak dat techniek juist niet de oplossing voor cybersecurity is: de mens is vaak de zwakste schakel…
“TNO is ooit opgericht voor toegepast natuurwetenschappelijk onderzoek. Maar in de praktijk is de organisatorische en gedragswetenschappelijke component in ons onderzoek steeds belangrijker geworden. We hebben niet voor niets zo’n vijfhonderd gedragswetenschappers in huis. Technologie alleen is niet de oplossing, net zo min als organisatieverbetering op zichzelf. Innovaties ontstaan juist in de combinatie van mens en technologie. Onze missie is het verbinden van mensen en kennis om innovaties te realiseren die de concurrentiekracht van Nederland en het welzijn van de samenleving duurzaam versterken. Geen gadgets dus, maar structurele oplossingen. Wij doen dat op verschillende terreinen, zoals bouw, transport en mobiliteit, voeding en gezondheidszorg, industriële productie en energie. Op al deze terreinen speelt het vraagstuk van cybersecurity. Ik denk dat onze missie en die van CPNI.NL in elkaars verlengde liggen. CPNI.NL focust op de vandaag opkomende praktische vragen en oplossingen, wij op de vraagstukken van morgen en overmorgen. We vullen elkaar aan.”

TNO is een wetenschappelijk instituut, CPNI.NL is een zeer praktisch initiatief gericht op direct resultaat. Past dat wel bij elkaar?
“De drive van Annemarie Zielstra en haar collega’s is natuurlijk heel hit-and-run, en die dynamiek is ook echt nodig voor CPNI.NL! Daar zal vast wel eens een TNO-onderzoeker vreemd van opgekeken hebben, ja. Maar het is belangrijk dat we ieder doen waar we sterk in zijn, want bij onderzoek kan je anders ook wel eens té hard gaan.”

Hoe staat het met samenwerking op het gebied van digitale, fysieke en personele veiligheid? Wat is daar van terecht gekomen?
“Dat is groeiende. In de ISACs heeft verbreding naar andere vormen van security al wel plaatsgevonden. Een voorbeeld is het Schiphol Information Security Awareness Symposium van de Airport-ISAC. Maar we zijn nog lang niet klaar. Ik vermoed dat na DigiNotar de volgende crisis weleens zou kunnen plaatsvinden in de procescontrole, en dan kom je vanzelf tegen dat je cybersecurity moet inbedden in fysieke en personele security. Je wilt niet weten hoe snel een kwaadwillende in een beveiligde serverruimte kan komen… Op dat vlak zijn we er nog niet. In die verbreding spelen TNO, CPNI.NL en de ISACs een aanjagende rol. Elke security officer zal je vertellen dat security awareness een aandachtspunt is. Enerzijds moeten medewerkers hun usb-stick niet laten slingeren, maar anderzijds moet er ook bewustzijn op CEO-niveau komen. Ik weet niet of integrale security al een frequent issue is in de Nederlandse bestuurskamers, maar dat zou het wel moeten zijn. Op het niveau van ‘cybersecurity voor dummy’s’ zul je de risico’s moeten blijven herhalen. We moeten permanent aandacht vragen voor awareness.”

Wat vinden bedrijven en overheden ervan dat CPNI.NL bij TNO onderdak heeft gevonden?
“Dat is heel goed gevallen. TNO is bij wet opgericht met de opdracht om iets te betekenen voor de samenleving én het bedrijfsleven, dus wij zijn inherent publiek-privaat. We werken met

een groot deel van het Nederlandse bedrijfsleven en met vele internationale bedrijven samen. We dragen via research & development bij aan het versterken van hun prestaties. TNO was dus heel logisch als landingsplek voor CPNI.NL en zo hebben alle betrokken partijen dat ook ervaren. Waar anders in Nederland heb je zo'n plek waar publiek, privaat en kennis bij elkaar komen? Die potentie kan nog wel verder groeien. Het net gestarte European Network for Cyber Security richt zich op SCADA en smart grids in de energiesector, maar ook voor de andere sectoren zou je de internationale ambitie moeten hebben om iets dergelijks over alle sectoren heen te maken."

Wat vindt u ervan dat het Informatieknooppunt Cybercrime aangehaakt gaat worden aan het Nationaal Cyber Security Centrum (NCSC)?
"Dat lijkt me noodzakelijk. Ik zie het NCSC als dé plek waar allerlei activiteiten op het gebied van cybersecurity op elkaar afgestemd gaan worden. De activiteiten van de ISACs moeten goed aansluiten bij wat anderen doen en er mag geen overlap ontstaan. Maar met een succesformule moet je ook voorzichtig zijn! Vooral als je niet alleen een publiek-private samenwerking hebt maar ook een kennis- en innovatiekant, is het alleen maar verstandig om het IKC door ervaren mensen te laten uitvoeren die ook bij de publieke en private partijen bewezen hebben succesvol te zijn. Zorg dat je die driehoek op een goede manier blijft verbinden. TNO is het programma CPNI.NL begonnen met als doel de ICT-security te koppelen aan andere vormen van security en kennis en kunde op het gebied van informatiemaatschappij. De problemen zitten immers vaak op de grensvlakken. Je kunt dat niet los zien van het goed beheren van het IKC. Zorg dus dat die kenniscomponent blijft ingebed, en dan vormt TNO graag het platform daarvoor. We hebben met het ministerie van EL&I, de subsidiegever, afgesproken dat we er in 2012 de tijd voor nemen om die goede verbinding met het NSCS tot stand te brengen."

Waar moet CPNI.NL volgens u in 2012 de grootste stap zetten?
"Om te beginnen dus die stap naar het NCSC toe. De eerste grote opgave is daar een goede, logische verbinding neer te leggen en de ambities van de ministers Opstelten, Verhagen en Hillen waar te maken. Natuurlijk zou ik het een eer vinden wanneer TNO het IKC voor het NCSC mag blijven coördineren. De andere opdracht voor 2012 is de ISACs op internationaal niveau te brengen. Het onderwerp cybersecurity is grensoverschrijdend, maar ik weet niet of de netwerken dat ook al voldoende zijn. Deze ambitie is ook afhankelijk van wat de overheden in EU-verband doen. Als de internationale ambitie van het NCSC wordt waargemaakt, dan moet CPNI diezelfde vertakkingen krijgen en contacten leggen met ISAC-achtige initiatieven in andere landen. Brussel zou zoiets als een CPNI.EU moeten herbergen."

Welke bijdrage gaat TNO leveren om dat te bewerkstelligen?
"Onderzoeksnetwerken zijn internationaal. Wetenschappers weten elkaar over de hele wereld te vinden. De EU kent grote onderzoeksprogramma's die ook relevant zijn voor cybersecurity. De consortia die op de tenders van deze programma's inschrijven hebben meestal een publiek-private samenstelling. TNO zit in de top-3 van consortia die daar gebruik van maken. Dat internationale netwerk en de resultaten van

al dat onderzoek kunnen wij inbrengen, net als onze contacten in bijvoorbeeld de EARTO (European Association of Research and Technology Organisations) die diverse andere domeinen bestrijkt. Zelf vertegenwoordig ik TNO binnen de EOS (European Organisation for Security) die cybersecurity hoog op de agenda heeft staan. Maar cybersecurity speelt op alle maatschappelijke terreinen. Mijn zes collega-directeuren bij TNO, verantwoordelijk voor Mobiliteit, Informatiemaatschappij, Industriële Innovatie, Energie, Gebouwde Omgeving en Gezond Leven, hebben ook allemaal hun eigen internationale contacten. Wij dragen onze netwerken en de kennis die daar in zit graag bij."

Wat staat er nog op uw verlanglijstje?
"De sturing vanuit TNO, de overheid en het bedrijfsleven op CPNI.NL kan nog wat beter. De overheid en het bedrijfsleven hebben er nog meer belang bij dat de driehoek van overheid-kennisinfrastructuur-bedrijfsleven goed samenwerkt dan wij als TNO! Per slot van rekening zijn het publieke middelen die effectief en efficiënt moeten worden ingezet. Ik zou graag zien dat de uitwisseling tussen wetenschap en praktijk veel meer tot uitdrukking komt. Overigens heeft TNO daar zelf ook een uitdrukkelijke rol in. Onze onderzoeken en die van universiteiten en andere kennisinstellingen zouden vaker en structureler bij de preventie op en bestrijding van inbreuken op de digitale veiligheid gebruikt kunnen worden. Dus niet alleen als antwoord op een specifieke vraag. Ik hoop dat dit een gezamenijke ambitie is, en dat dit de leidraad kan vormen voor de toekomstige sturingsrelatie en het leggen van de noodzakelijke verbinding naar het Nationale Cyber Security Centrum."

EUROPEAN NETWORK VOOR CYBER SECURITY (ENCS)

Of het nou gaat om gas, elektriciteit, water of geldstromen: de beveiliging van maatschappelijk essentiële sectoren kan niet meer alleen nationaal worden geregeld. Het verdwijnen van de grenzen vergroot de dreiging én de impact van uitval. Het European Network voor Cyber Security (ENCS) brengt publieke en private partijen op Europees niveau bij elkaar om samen te werken aan de beveiliging van vitale infrastructuren.

ENCS is een gezamenlijk initiatief van Alliander en TNO | CPNI.NL. Overige consortiumpartners zijn KPN, KEMA, Radboud Universiteit Nijmegen en de gemeente Den Haag. ENCS moet zo snel mogelijk leiden tot een doorlopende, geconcentreerde internationale campagne om de Europese vitale infrastructuren zo weerbaar mogelijk te maken tegen alle typen bedreigingen. Het gaat daarbij om het zo veel mogelijk voorkómen van menselijke en technische fouten, en beveiliging tegen kwaadwilligen zoals terroristen of afpersers. ENCS wordt gedragen door vier pijlers:

- informatie- en kennisdeling;
- educatie en training;
- testen;
- research & development.

Naast kennisuitwisseling gaat het vooral ook om samenwerking op het operationele vlak, bijvoorbeeld door het aanbieden van research- en testfaciliteiten voor open source cybersecurity en privacy enhancing technologies.

ENCS start officieel in 2012, maar het voorwerk is al in 2011 verricht. Het initiatief is in augustus 2011 gepresenteerd aan de CEO's van grote bedrijven, kenniscentra en organisaties. Half december is het business plan opgeleverd en gepresenteerd. Op basis hiervan hebben de CEO's de beslissing genomen om door te gaan. Momenteel worden publieke en private partijen in heel Europa benaderd om zich aan te sluiten.

SMART GRIDS OP DE AGENDA

Goede informatiebeveiliging is een absolute voorwaarde voor het toepassen van slimme energienetwerken ofwel smart grids. Daarom is in 2011 in Europees verband door DG INFSO de Expert Group on the security and resilience of communication networks and information systems for Smart Grids gestart die de dreigingen, het risico en beveiligings-oplossingen voor smart grids in kaart gaat brengen. Vanuit Nederland nemen vertegen-woordigers van CPNI.NL, TNO en Alliander deel aan deze expertgroep.

De inzet van slimme energienetwerken moet een grote bijdrage gaan leveren aan de 20-20-20-doelstellingen van de EU. Volgens deze doelstelling is in 2020 het volgende bereikt:

- meer dan 20% reductie van broeikasgassenuitstoot ten opzichte van 1990;
- meer dan 20% van de energie uit duurzame bronnen;
- meer dan 20% vermindering van energie-gebruik door een hogere energie-efficiëntie.

Om het energieverbruik te optimaliseren wordt extra ICT toegevoegd aan bestaande energie-netwerken die 'meedenkt' met de energie-afnemer. Het huidige energienetwerk wordt een smart grid. Zo'n slim energienetwerk zorgt ervoor dat elektrische auto's alleen opladen in de daluren en wasmachines met het netwerk onderhandelen wanneer ze zo goedkoop moge-lijk kunnen wassen. Ook kan door smart grids bijvoorbeeld de restwarmte van warmtekracht-installaties van bedrijven ingezet worden voor de energievoorziening in de buurt.

De ontwikkeling van smart grids brengt echter ook risicofactoren met zich mee. De informatie over het energieverbruik van particulieren kan leiden tot problemen op het gebied van privacy en veiligheid. De verzamelde gegevens kunnen misbruikt worden omdat er bijvoorbeeld uit blijkt wanneer iemand niet thuis is. Ook onbevoegde beïnvloeding van energienetwerken door criminelen, activisten en vreemde mogendheden moet zoveel mogelijk worden ingeperkt.

Bij smart grids zijn veel partijen betrokken, zoals producenten van 'slim' witgoed, burgers, kleine energieopwekkers ('prosumers'), windmolen- en zonne-energieparken, producenten van trans-formatoren en andere regelsystemen, bulk-energieopwekkers en distributie- en transmissie-bedrijven. Het is dus een gezamenlijke uitdaging van al deze partijen om het smart grid robuust en veilig te maken.

Om inzicht te krijgen in deze uitdaging, is in 2011 in Europees verband een expertgroep gestart om de belangrijkste smart grid-elementen, moge-lijke dreigingen, risicofactoren en de mogelijke aanpak daarvan in kaart te brengen. Alliander, TNO en CPNI.NL leveren een actieve bijdrage in deze expertgroep. De bevindingen vanuit de expertgroep worden medio 2012 opgeleverd aan de Europese Commissie.

World Economic Forum: Partnership for Cyber Resilience

De workshop van het World Economic Forum in november 2011 in Londen had als thema Risk and Responsibility in a Hyperconnected World. Aan de workshop gingen sessies vooraf in de Verenigde Staten en China om zoveel mogelijk invalshoeken te verzamelen vanuit de industrie, de kenniscentra en de publieke sector.

CPNI.NL nam deel aan de workshop en bracht ervaringen in op het gebied van publiek-private samenwerking en informatie-uitwisseling. Uit de workshop kwamen veel vragen naar voren over de (on)mogelijkheid om binnen de huidige bestuurlijke paradigma's decentrale systemen als het internet te managen. Dit leidde tot het idee van een collectief bestuursmodel van betrouwbare publiek-private netwerken.
Ook op CEO-niveau werd collectieve actie op de korte termijn besproken, bijvoorbeeld het implementeren van 'gouden regels', een executive toolkit of risk management waarmee acute cyberdreigingen kunnen worden aangepakt. Een dergelijk CEO-netwerk zou de bewustwording en het onderlinge vertrouwen onder CEO's bevorderen die nodig zijn voor informatie-uitwisseling en langetermijnoplossingen gericht op bijvoorbeeld preventie. Een belangrijk onderwerp is het ontbreken van C-level awareness, een van de aandachtspunten die in 2011 in alle onderzoeksrapporten naar voren kwam.

De diverse ontstane concepten worden verder uitgewerkt in een Partnership for Cyber Resilience, dat op het World Economic Forum in 2012 zal worden gepresenteerd.

MIJLPALEN

3 NOVEMBER
Voorbereiding World Economic Forum 2012 | Londen

8-9 NOVEMBER
Energy and Utility Cyber Security Summit | Amsterdam

14 NOVEMBER
SMi The European Smart Grid Cyber Security and Privacy conference | Amsterdam

22-23 NOVEMBER
EuroSCSIE bijeenkomst | Finland

29-30 NOVEMBER
Kick-off ERNCIP | Ispra

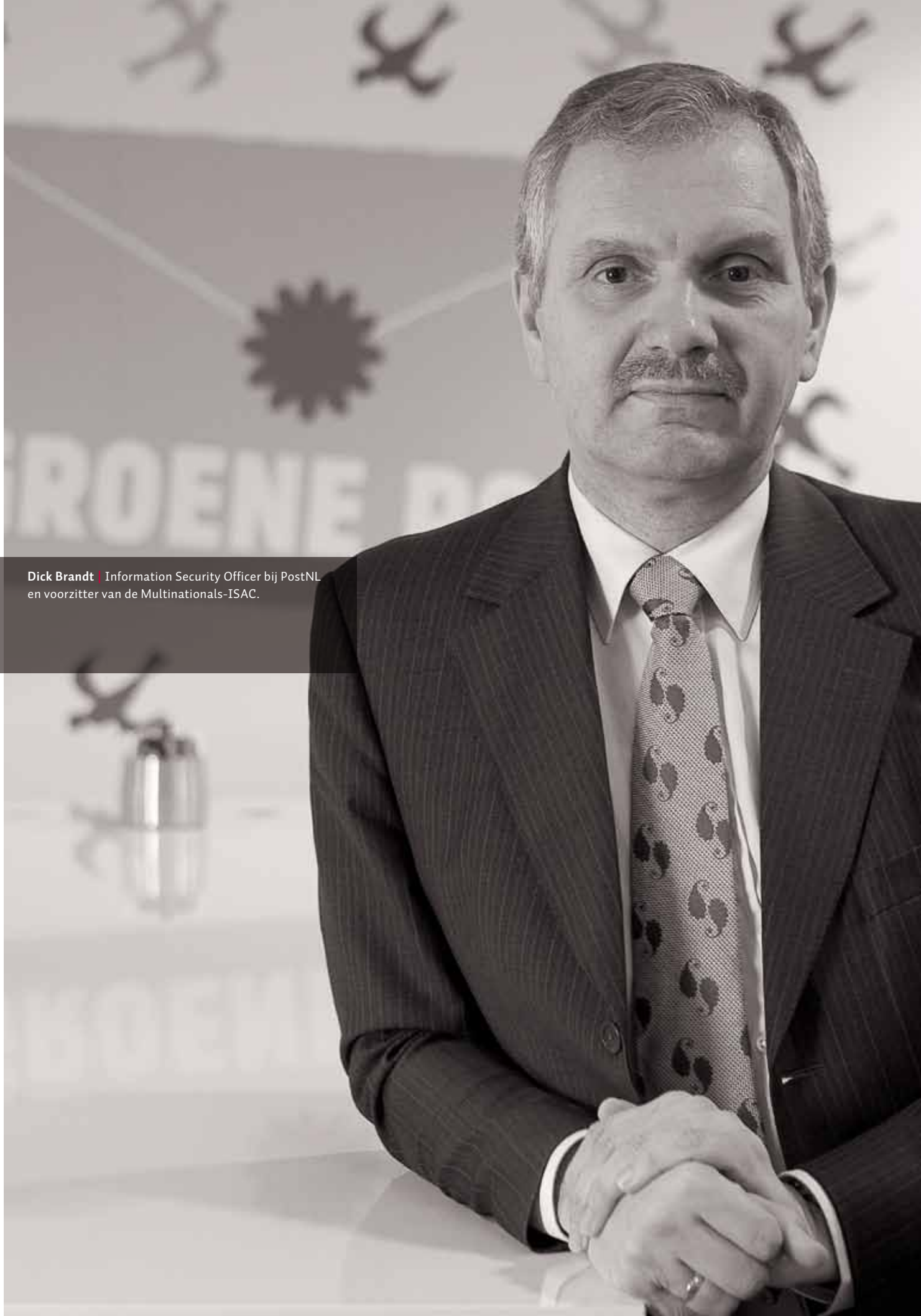
7-8 DECEMBER
European FI-ISAC | Estland

14 DECEMBER
Presentatie Cyber-TEC Business Plan | start ENCS

16 DECEMBER
Afronding CAET fase 3: rechtsorde, gezondheidszorg, transport, chemie / nucleair en voedsel

20 DECEMBER:
Eerste EU-rapport ENISA over Maritieme Cyber Security

21 DECEMBER
Start ERNCIP, Thematic Area ICS and Smart Grids



Dick Brandt | Information Security Officer bij PostNL en voorzitter van de Multinationals-ISAC.

“Zodra iemand geld kan verdienen aan jouw informatie, heb je een probleem”

Economische spionage is een belangrijk maar ongrijpbaar onderwerp voor grote bedrijven. Op 24 juni 2011 hield de Multinationals-ISAC daarom een Economical Espionage Event, gehost door de AIVD. Het event was slechts toegankelijk voor de ISAC-leden en een select aantal genodigden (juristen, fysieke security) uit hun organisaties. Dit om het onderlinge vertrouwen te waarborgen en het onderwerp zo integraal mogelijk te benaderen. Dick Brandt: “Een belangrijk resultaat is het besef dat anderen ook last hebben van economische spionage, en dat je van hen kennis kan krijgen over hoe je het aanpakt.”

Wat verstaat u onder economische spionage?
“Alle activiteiten die door derden ondernomen worden om economisch voordeel te halen uit de kennis die binnen een bedrijf of land aanwezig is.”

Waarom is dit onderwerp zo belangrijk voor de samenleving?
“In Engeland verscheen een tijd terug een rapport met harde cijfers over de schade aan intellectueel eigendom ten gevolge van economische spionage. Het ging om miljarden. Het rapport sloeg in als een bom, want het maakte duidelijk dat het beschermen van intellectueel eigendom belangrijk is. Multinationals, en vooral bedrijven die zelf veel aan research doen, geven veel geld uit aan patenten en octrooien. Vaak beschermen ze een onderzoek ook al voordat er een patentaanvraag ligt. Dat zouden ze niet doen als het niet belangrijk was.”

“Binnen de ISAC hebben we geen harde cijfers hoe groot de schade door economische spionage voor Nederland is, maar we weten uit eigen ervaring dat het gebeurt. Zodra er iemand geld kan verdienen aan jouw informatie, heb je een probleem. Dat is slecht voor onze samenleving. Als ons intellectueel eigendom in het buitenland terecht komt en dus niet geëxploiteerd kan worden door de bedrijven die het ontwikkelen, investeren die straks geen geld meer in research & development. Dan raakt Nederland uiteindelijk achterop. En dat terwijl we toch voor een groot deel een kennismaatschappij zijn.”

Waar bestaat de spionagedreiging uit voor de BV Nederland?
“Sommige buitenlanden zien het beschermen van belangen iets anders dan Nederland. De inlichtingendiensten van de meeste andere overheden hebben economische spionage dan ook keihard in hun missie staan. Dan heb ik het niet alleen over schurkenstaten of ontwikkelingslanden. Ook grote landen als China en diverse westerse mogendheden achten het beschermen van hun economische belangen als een taak van de inlichtingendienst. ”

“Wij zijn in Nederland altijd roomser dan de paus, dus de wet op de Inlichtingen- en veiligheidsdiensten staat in Nederland alleen contraspionage en terrorismebestrijding toe. De AIVD kan bedrijven alleen beschermen tegen spionage van anderen, en wijzen op de risico’s.”

En voor de Multinationals-ISAC?
“Voor ons is het een belangrijk thema. Het maakt wel verschil in welke landen je als bedrijf opereert, en of je al dan niet bedreigend bent voor een nationale industrie elders. Met de Urenco-affaire is economische spionage in de openbaarheid getreden. Maar er zijn veel meer gevallen van buitenlandse spionage geweest die niet aan grote klok worden gehangen. Ook de AIVD besteedt aandacht aan het bewust maken

van bedrijven, onder andere met het rapport Kwetsbaarheidsanalyse Spionage (KWAS).”

Hoe ontstond het idee voor het Economical Espionage Event?
“Eigenlijk wilden we eerst een open event organiseren over dit thema, waar we ook andere ISACs voor zouden uitnodigen. Maar al discussiërend bleek er een behoefte om eerst onderling gevoelige informatie uit te wisselen onder code rood van het stoplichtmodel, het hoogste niveau van vertrouwelijkheid. Om in de diepte te kunnen investeren moesten we de groep dus wat beperkter houden. Uiteindelijk werd het een man of twintig: de deelnemers aan de ISAC mochten elk drie andere mensen uit hun bedrijf meenemen. Een te groot event zou onvermijdelijk ook oppervlakkiger worden. Persoonlijke ontmoetingen zijn zeker voor dit soort onderwerpen belangrijk, want je praat er niet makkelijk over. Je moet er immers op kunnen vertrouwen dat je gesprekspartners zich ook aan code rood houden.”

Hoe hebben jullie dit event aangepakt?
“Inhoudelijk hebben we het programma opgesteld samen met de AIVD. Het lag voor de hand om het ook op hun beschermde locatie te houden. Iemand van de AIVD legde uit wat er plaatsvond op het gebied van economische spionage en welke partijen daarbij betrokken zijn. De resultaten uit de KWAS-rapportage lagen daaraan ten grondslag. We hebben verder wat praktijkcases behandeld in discussiegroepjes: hoe voorkom je spionage, hoe spoor je het op en wat doe je ertegen?”

Lukte het om ook in dit grotere verband vertrouwelijke informatie uit te wisselen?
“We hadden vooraf wat twijfels of het zou lukken om dat onderlinge vertrouwen uit het ISAC-overleg over te brengen op een grotere groep. Door de setting, en omdat we code rood nadrukkelijk hebben benoemd, is dat heel goed gelukt. Normaal zijn we als security officers redelijk open in de ISAC, maar dit was de eerste keer dat er directeuren security bij zaten, en juristen die de intellectual property rights in hun portefeuille hebben. Ze stonden wel even te kijken dat ze bij de deur al hun elektronische apparaten en USB-sticks moesten inleveren! Iedereen was heel enthousiast, ondanks het feit dat ze de hele middag zonder telefoon zaten. Ze kregen alleen een boekje waarin ze hun conclusies mochten opschrijven en zaken die eventueel op hun bedrijf van toepassing waren. Het ging immers vooral om luisteren en praten. Er is zeker ook bedrijfsgevoelige informatie uitgewisseld. En daar is dus geen verslag van gemaakt.”

Kunt u ondanks de vertrouwelijkheid toch wat vertellen over de resultaten van het event?
“Een belangrijk resultaat is het besef dat anderen ook last hebben van economische spionage, en dat je van hen kennis kan krijgen over hoe je het aanpakt. Daarnaast zijn er uit de werksessies tien redelijk basale gouden regels voortgekomen. Ze zijn niet ingewikkeld maar geven wel precies aan waar het om gaat.”

“Het begint met bewustwording en het bepalen waar je kwetsbare assets zitten. Verder gaat het over het managen van risico’s, het nemen van beschermende maatregelen en die doorlopend monitoren. Informeer de ondernemingsraad als

er iets mis is en zorg voor een draaiboek. Zet je lessons learned op papier. Wees je bewust van blinde vlekken: je denkt vaak wel dat je applicaties veilig zijn, maar om dat zeker te weten moet je toch een derde partij inhuren om ze te testen."

Zijn de gouden regels ook interessant voor anderen?
"CPNI wil het onderwerp economische spionage sowieso breder oppakken met de andere ISACs, want we hebben geconstateerd dat het een veel breder probleem is. Als Multinationals-ISAC hebben we toegezegd dat we de gouden regels willen delen met de andere ISACs."

Heeft u zelf nog een gouden tip voor collega's?
"Dan haal ik graag de tiende en belangrijkste gouden regel aan: informatie zal altijd lekken, dus plan daarop en bereid je voor. Beperk de schade door van tevoren te bedenken wat je gaat doen, want als het al lekt heb je daar geen tijd meer voor."

PARTNERS CPNI.NL IN DE (INTER) NATIONALE INFRASTRUCTUUR

A
- ABB BV
- ABN Amro Bank
- Academisch Medisch Centrum
- Academisch Ziekenhuis Maastricht
- Achmea
- Accent Telecom
- Accenture
- Actemium
- Aegon
- AFM
- Agentschap Telecom
- Ahold / Albert Heijn
- AID (Algemene Inspectie Dienst)
- Air Cargo Nederland (ANC)
- Aircraft Fuel Supply BV
- AIVD
- AkzoNobel
- Alares
- Alliander
- American Water Works Association USA
- Amsterdam Airport Schiphol
- AMS-IX
- ANSSI, France
- Applied Control Solutions USA
- ASIS International
- ATOS Consulting
- Australian Government

B
- Bank Nederlandse Gemeenten
- Barclays London UK
- BBNed
- Belastingdienst
- Beveiliging en Publieke Veiligheid Schiphol
- Bex Communicatie
- Binck Bank
- BMKiss Europe
- Booz & Compagny
- Bovenregionale Recherche Noord- en Oost Nederland
- BP Nederland BV
- Brabant Water
- BT Nederland NV
- Bundesamt fur Sicherheit in der Informationstechnik, Germany
- Bundesministerium des Innern, Germany

C
- C-4 Security
- CabinetOffice, UK
- CAIW
- Capgemini
- Cargonaut
- CBP
- Centre for the Protection of National Infrastructure (CPNI), UK
- Centric IT Solutions
- CERN, Switzerland
- CERT-FI, Finland
- CERT Hungary
- Chatham House, UK
- CIO Platform Nederland
- City University London, UK
- Clingendael
- Connexxion
- Consumentenautoriteit
- Consumentenbond
- CP-ICT
- Currence
- Cyber Security UK
- CyberSecurity Malaysia
- Cycris

D
- DAF Truck NV
- David Lacey Consulting UK
- De Kinderconsument
- De Nederlandsche Bank
- Delft TopTech
- Deloitte
- DELTA
- DELTA Netwerkbedrijf
- Delta Lloyd
- Deltalinqs
- Department of Homeland Security USA
- Digibewust
- Douane/Belastingdienst
- Dow Benelux BV
- Dow Chemical USA
- Dröge en Van Drimmelen
- DSM
- Duinwaterbedrijf Zuid-Holland
- Dusecon
- Dutch Hosting and Provider Association
- Duthler Associates

E
- E.ON Benelux NV
- Ebay/Marktplaats
- ECP-EPN Platform voor de InformatieSamenleving
- ECT
- Edridge Fotografie
- Egemin
- Electrabel
- Elster, Germany
- Emerson
- ENEA, Italy
- Eneco
- Energiened
- Enexis
- ENISA, Greece
- Enrichment Technology
- EOS, Belgium
- EPZ
- EQUENS
- Erasmus Medisch Centrum
- Erasmus Universiteit Rotterdam
- Esri Nederland
- Essent
- European Commission
- European Security Advisors
- Evides

F
- Faber organisatievernieuwing
- F. van Lanschot Bankiers NV
- Federal Bureau of Investigation USA
- Federal Department of Finance USA
- Fennema Drukkers
- FHI
- FIOD-ECD
- Fleishman
- Fortis Bank
- Fortum, Finland
- FOX-IT
- Friesland Bank NV
- Fugro

G
- Gasunie
- GBO. Overheid
- GDF Suez Group
- Gemeente Den Haag
- Getronics PinkRoccade

- Global Cyber Security Center, Italy
- Google
- GVB

H
- Haagse Hogeschool
- HBD Total Security
- HCSS The Hague Centre for Strategic Studies
- Heineken
- Het Expertise Centrum (HEC)
- HIMA
- Hochschule Luzern
- Hogeschool Utrecht
- Holland Casino
- Honeywell
- HP
- HTM

I
- IBM
- ICT Media BV
- ICT Recht
- ICT Regie
- ICT-Office
- Idaho National Laboratory, USA
- IDC, Italy
- Infocomm Development Authority of Singapore
- Information Security Forum UK
- ING-Postbank
- Inspectie voor de gezondheidszorg
- Inspectie voor Werk & Inkomen
- Intermark IT, Spain
- Internet Watch Foundation, UK
- Invensys
- IOActive
- ISOC
- ISP Connect
- ISSX
- IT-sec

J
- JPCERT, Japan
- Johns Hopkins University Washington, USA
- Joint Research Centre EU

K
- Kahuna
- Kaspersky
- KEMA
- Kennisnet/ICT op school
- KLM
- KLPD
- Koninklijke Marechaussee
- KPN
- KPMG
- KTH Electrical Engineering, Sweden

L
- Laborelec
- Leaseweb BV
- Liander
- Liandon
- Lucht Verkeersleiding Nederland (LVNL)
- LUMC (Leids Universitair Medisch Centrum)

M
- M+W Group
- Mactwin
- Madison Gurkha
- Marcel Rozenberg Photography Design
- McAfee
- Melani, Switzerland
- Meldpunt Kinderporno
- Meldpunt Discriminatie Internet
- Metropolitan Water District of Southern California, USA
- Microsoft
- Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
- Ministerie van Economische Zaken, Landbouw & Innovatie
- Ministerie van Veiligheid &Justitie
- Ministerie van Infrastructuur & Milieu
- Ministerie van Defensie (incl MIVD)
- Ministry of Home Affairs, Singapore
- MKB-Nederland
- Motion Picture Associates
- MSB Swedish Civil Contingencies Agency

N
- Nationaal Cyber Security Centrum
- National Cyber Security Directorate, Canada
- National IT and Telecom Agency Denmark
- NBC Universal
- NCTV
- Nedap
- Nederland BreedbandLand
- Nederland Digitaal in Verbinding
- Nederlands Politie Instituut
- Nederlandse Thuiswinkel Organisatie
- Nederlandse Vereniging van Banken
- NFI
- NICTIZ
- NIDV Defensie & Veiligheid
- NISA Israel
- NISC Japan
- NLKabel
- NLnetLabs
- Noordelijke Hogeschool Leeuwarden – Lectoraat Cybersafety
- Norman
- NS
- Nuon
- NXP

O
- Oake Communications
- Oasen
- OBT/TDS printmaildata
- Océ
- Office of Cyber Security - Cabinet Office UK
- Office of Cyber Security and Critical Infrastructure Coordination NY USA
- Online
- Onsight Solutions
- Open Universiteit
- Openbaar Ministerie
- Optimeamise
- OPTA
- Österreichisches Institut für Internationale Politik (OIIP)
- Osage

- P
  - Philips
  - Platform voor Informatiebeveiliging (PvIB)
  - Politie
  - Politieacademie
  - Port of Rotterdam (Gemeentelijk Havenbedrijf Rotterdam)
  - PostNL
  - Programma Aanpak Cybercrime (Politie)
  - Programma Cybercrime (OM)
  - Programma Veiligheid begint bij Voorkomen (Justitie)
  - ProRail
  - PWC Consulting
  - PWN Waterleidingbedrijf Noord-Holland
- Q
  - QinetiQ
  - Q-CERT, Qatar
- R
  - Raad voor de Rechtspraak
  - Rabobank Nederland
  - Radboud Universiteit NijmegenRSA
  - RET
  - RIVM
  - Rijkswaterstaat
- S
  - S21Sec
  - Santa Clara Valley Water District, USA
  - SAP
  - Secrétariat Général de la Défense et de la Sécurité Nationale France
  - Security Matters
  - Schiphol Group
  - Schiphol Telematics
  - School of Computing & Information Systems University of Tasmania
  - Secretariat general for national defence France
  - SERN
  - Shell
  - Shell/NAM
  - SIDN
  - Siemens
  - Source Fire
  - SOVI (Strategisch Overleg Vitale Infrastructuur)
  - SNBReact
  - SNS Bank NV
  - SRI International USA
  - Stedin
  - Stichting BREIN
  - Stichting Kennisnet ICT op school
  - Stichting M
  - Stichting Magenta
  - Stichting Mijn Kind Online
  - Stork BV
  - Surfnet.nl
  - SwissGrid
  - Symantec
  - Syntens
- T
  - T-Mobile
  - Tappan
  - Tekstbureau De Nieuwe Koekoek
  - Tele2
  - TenneT
  - Thales, France
  - TNO
  - Total
  - Translink Systems
  - Triodos Bank
  - Tshukudu Technology College (TSTC)
  - TU Delft
- U
  - UK Payments
  - UMC St.Radboud Nijmegen
  - Uneto-VNI
  - Unilever
  - Universitair Medisch Centrum Utrecht
  - Universitair Medisch Centrum Twente
  - Universitair Medisch Centrum Groningen
  - Universiteit van Amsterdam
  - Universiteit Twente
  - Universiteit van Maastricht
  - Universiteit van Tilburg
  - UPC
  - Urenco Nederland BV
  - US Department of Homeland Security
- V
  - Vattenfall Sweden
  - Vereniging van Nederlandse Gemeenten (VNG)
  - VEWIN
  - Veiligheidsberaad
  - Veiligheidsmonitor bureau
  - Veolia Transport
  - Verbund Austria
  - Verdonck Klooster & Associates (VKA)
  - Verizon Business
  - VIAG
  - Vitens
  - VMWare
  - VNO-NCW
  - Vodafone
  - Vopak
  - VU Amsterdam
  - VU Medisch Centrum (VUmc)
- W
  - Warner Bross
  - Water Supply (Network) Department Singapore
  - Waterbedrijf Groningen
  - Waterleidingsmaatschappij Drenthe (WMD)
  - Waterleidingsmaatschappij Limburg (WML)
  - Waterfall
  - Waternet
  - Wave Systems
  - WCK-GRC
  - Wetenschappelijk Bureau OM
  - WIB
  - Wien Energie, Wien
  - Wintershall Noordzee BV
  - Witteveen & Bos
  - WODC
- X
  - XS4ALL
- Y
  - Yokogawa
- Z
  - Zeehavenpolitie/Port Security
  - Zeelandnet
  - Ziggo

CPNI.NL | TNO
Postadres
Postbus 96864
2509 JG Den Haag

Bezoekadres
Oude Waalsdorperweg 63
2597 AK Den Haag

T 088 866 38 61
E info@cpni.nl
I www.cpni.nl