854/2

Raadgevende Interparlementaire Beneluxraad

10 juli 2014

AANBEVELING

over cybersecurity

(Aangenomen ter plenaire vergadering van 21 juni 2014)

Conseil Interparlementaire Consultatif de Benelux

10 juillet 2014

RECOMMANDATION

concernant la cybersécurité

(Adoptée en séance plénière du 21 juin 2014)

VAST SECRETARIAAT
VAN DE INTERPARLEMENTAIRE BENELUXRAAD
PALEIS DER NATIE — BRUSSEL

SECRETARIAT PERMANENT
DU CONSEIL INTERPARLEMENTAIRE DE BENELUX
PALAIS DE LA NATION — BRUXELLES

De Raad,

gelet op

— de Benelux-conferentie “De bewustmaking van de burger van de risico’s van cybercrime”, gehouden te Luxemburg op 26 april 2013;

— de Benelux-conferentie ‘Cyber security en de vitale infrastructuur.- Aanpak van de Benelux’, op 2 juni 2014 gehouden te Den Haag, met:

• de heer Joris den Bruinen, deputy director, The Hague Security Delta (HSD),

• drs. Leo Freriks, city account manager, Siemens Nederland N.V.,

• de heer Louis Oosterom, manager business development, Bosch,

• de heer Pascal Steichen, Direction du commerce électronique et de la sécurité informatique, Ministère de l’Economie (Luxemburg);

— de Benelux intentieverklaring Cyber Security van 5 april 2011;

— de gezamenlijke mededeling van het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio’s: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace;

— de noodzaak voor de lidstaten om Richtlijn 2013/40/EU van het Europees Parlement en de Raad van 12 augustus 2013 over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad tegen uiterlijk 4 september 2015 te implementeren;

vaststellende dat

— de Beneluxlanden ieder beschikken over een Computer Emergency Response Team (CERT) dat belast is met de behandeling van cyber issues;

Le Conseil,

vu

— la conférence Benelux “La sensibilisation du public aux risques de la cybercriminalité” qui s’est tenue à Luxembourg le 26 avril 2013;

— la conférence ‘Cybersecurity et l’infrastructure vitale’.- Approche du Benelux’, tenue à La Haye, le 2 juin 2014, avec:

• M. Joris den Bruinen, deputy director, The Hague Security Delta (HSD),

• drs. Leo Freriks, city account manager, Siemens Nederland S.A.,

• M. Louis Oosterom, manager business development, Bosch,

• M. Pascal Steichen, Direction du commerce électronique et de la sécurité informatique, Ministère de l’Economie (Luxembourg);

— la déclaration d’intention Benelux du 5 avril 2011 sur la Cybersécurité;

— la communication commune du Parlement européen, du Conseil, du Comité Économique et Social Européen et du Comité des Régions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace;

— la nécessité pour les États membres de transposer pour le 4 septembre 2015 au plus tard la Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d’information et remplaçant la décision-cadre 2005/222/JAI du Conseil;

constatant que

— chaque pays du Benelux est doté d’un Computer Emergency Response Team (CERT) chargé du traitement de cyberdossiers;

— de Beneluxlanden ieder een eigen cyber security strategie hebben ontwikkeld, waarbij veel belang wordt gehecht aan grensoverschrijdende samenwerking;

— de samenwerking tussen de verschillende CERT's plaatsvindt, maar veelal op basis van persoonlijke contacten en informele lijnen;

overwegende dat

— de Europese Unie oproept tot meer samenwerking;

— de Benelux daarin een voortrekkersrol kan spelen, aangezien de landen gezamenlijk over veel kennis beschikken op het terrein van cyber security;

verzoekt de regeringen de volgende concrete stappen te ondernemen:

• de identificatie van een concrete cyber gerelateerde crisis in de vitale infrastructuur die zich recent heeft voorgedaan, dan wel van een concreet risico binnen de vitale infrastructuur zoals de energievoorziening;

• de oprichting van een Benelux-brede werkgroep met experts op het gebied van cyber security en betreffende wetgeving waarbij op regelmatige wijze afstemming plaatsvindt met het Beneluxparlement;

• de identificatie van juridische bottlenecks voor een Benelux-brede aanpak en samenwerking en de formulering van voorstellen voor de oplossing ervan;

• de vaststelling van normering, zowel voor de overheden als voor private partijen, inclusief midden- en kleinbedrijf, om preventie en aanpak van cyber issues te waarborgen. Daarbij dient te worden gewaakt voor teveel normering en het dichtregelen van de problematiek;
• de uitwerking van een sanctiemechanisme voor het niet naleven van deze normering;

• een presentatie van de voorgestelde Beneluxaanpak voor dit concrete geval binnen één jaar,

— chaque pays du Benelux a développé sa propre cyberstratégie en accordant une grande importance à la coopération transfrontalière;

— la coopération entre les différents CERT est réelle mais se fait souvent sur la base de contacts personnels et de lignes informelles;

considérant que

— l'Union européenne appelle à davantage de coopération;

— le Benelux peut jouer à cet égard un rôle de précurseur puisque les pays possèdent, ensemble, une large connaissance dans le domaine de la cybersécurité;

demande aux gouvernements d'entreprendre les démarches concrètes ci-après:

• l'identification d'une récente crise concrète liée à l'informatique au niveau de l'infrastructure vitale ou d'un risque concret dans le cadre de l'infrastructure vitale, comme l'approvisionnement en énergie;

• la constitution à l'échelle du Benelux d'un groupe de travail réunissant des experts dans le domaine de la cybersécurité et de la législation en la matière avec la mise en place d'une coordination régulière avec le Parlement Benelux;

• l'identification des entraves juridiques à une approche et une coopération à l'échelle du Benelux et la formulation de proposition pour y remédier;

• la définition de normes à la fois pour les instances publiques et privées, en ce compris les petites et moyennes entreprises, pour garantir la prévention et l'approche dans les cyberdossiers. Il convient à cet égard de se garder d'un excès de normes et d'une sur-régulation;
• l'élaboration d'un mécanisme pour sanctionner le non-respect de ces normes;

• la présentation dans un an de l'approche Benelux proposée pour ce cas concret, par exemple

bijvoorbeeld tijdens de internationale cyber security conferentie van 2015 in Den Haag.

• de integratie van een Benelux-brede aanpak in de omzetting van richtlijn 2013/40/EU van het Europees Parlement en de Raad van 12 augustus 2013 over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad.

à l'occasion de la conférence internationale sur la cybersécurité qui se tiendra à La Haye en 2015.

• l'intégration d'une approche à l'échelle du Benelux dans la transposition de la Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil.