CYBER INTEGRAAL ONDERDEEL VAN ONS HELE OPTREDEN

DEFENSIE CYBER STRATEGIE

Cyber. Voor velen is het een vaag begrip. Voor Defensie is het echter iets om steeds meer rekening mee te houden. Tijdens het symposium van 27 juni in Breda presenteerde minister van Defensie Hans Hillen de cyberstrategie voor de Nederlandse krijgsmacht. De minister noemde cyber naast land, lucht, zee en de ruimte 'het vijfde domein voor militair optreden'. In dit artikel komt eerst de minister van Defensie aan het woord en daarna de commandant van de Task Force Cyber, kolonel ir. Hans Folmer, in de media beter bekend als de 'cyber-kolonel'.

De foto's bij dit artikel zijn afkomstig van het VOV Symposium 'Cyber in de Praktijk' van 9 oktober 2012.

"Cyber security staat nu volop in de aandacht. En terecht, want de digitale dreiging is reëel", zegt de minister in zijn toespraak. "Deze dreiging kan een ICT-afhankelijke samenleving als de onze op tal van manieren ontregelen. Niet alleen in technische zin, maar ook in psychologische zin: denk aan de angst, de paniek en wellicht de toegeeflijkheid jegens de agressor die kan optreden als onze digitale systemen op grote schaal worden gesaboteerd." Hoe de digitale dreiging eruit ziet, is moeilijk in te schatten, weet ook minister Hillen. "Veel is nog onduidelijk over de aard van digitale conflicten. Hoe zullen de cyberwapens van de toekomst er uit zien? Het is nog speculeren." Dat betekent niet dat Defensie op haar handen gaat zitten en kijken wat er komen gaat. "We kunnen het ons niet veroorloven lijdzaam af te wachten en maar te zien wat anderen bedenken. Vrijwel alles wat iemand zich kan verbeelden, zo leert de geschiedenis, zal vroeg of laat ook worden gemaakt."

SPEERPUNTEN

De cyberstrategie van de Nederlandse krijgsmacht bestaat uit zes speerpunten. Opvallend is dat er ook wordt gesproken over offensieve mogelijkheden. Hillen: "Als zwaardmacht moet de krijgsmacht naar mijn overtuiging ook in het digitale domein offensief kunnen optreden. Het uitschakelen van een tegenstander blijft de bijzondere taak van de krijgsmacht. Ook in het digitale domein. Kennis van offensieve methoden en technieken is bovendien noodzakelijk voor het versterken van de digitale weerbaarheid." Een ander belangrijk speerpunt is integrale aanpak. Digitale middelen bieden mogelijkheden in het militaire optreden. In alle domeinen kunnen zij de operatie ondersteunen. Daaruit volgt dat cybercapaciteiten als enabler kunnen fungeren, en standaard in de toolbox van de commandant moeten zitten.

WHITE HAT HACKER

In de cyberstrategie wordt verder het speerpunt 'adaptief en innovatief' aangehaald. "De snelheid waarmee ontwikkelingen in het digitale domein zich voltrekken, stelt zeer hoge eisen aan het aanpassingsvermogen en de innovatieve kracht van Defensie", concludeert minister Hillen. "Zij moet in het digitale domein in staat zijn snel nieuwe technologie in te voeren en korte innovatiecycli te doorlopen." Een bijzondere uitdaging voor Defensie vormt het aantrekken en behouden van gekwalificeerd personeel dat ook kan functioneren in een militaire omgeving. Hillen: "Om de noodzakelijke kennis, kunde en vaardigheden in huis te halen en te behouden wordt specifiek aandacht besteed aan personeelsbeleid en opleidingen. Specifieke loopbaanpatronen voor 'digitale soldaten' zijn daarbij zeker denkbaar." De krijgsmacht stelt zich nadrukkelijk open voor mensen die digitale kennis in huis hebben, maar waar de overheid nog te weinig gebruik van maakt: de 'white hat hacker'-community, oftewel de betrouwbare hackers. "Zij wijzen ons vaak op lekken. Daar moeten we niet boos om worden, maar gebruik van maken, want zo maken we elkaar sterker. Waarom zou een 'white hat hacker' zich niet willen inzetten om te helpen bij de verdediging van zijn eigen land? Zeker als hij daarvoor niet eens door de modder hoeft te kruipen, maar achter zijn computer kan blijven zitten", betoogt de minister van Defensie.

ZWAKSTE SCHAKEL

De Nederlandse defensieorganisatie richt zich volgens de cyberstrategie ook op de beveiliging van de eigen systemen en op nationale en internationale samenwerking. "In het digitale domein treden publieke en private, civiele en militaire en nationale en internationale actoren tegelijkertijd op. Een gezamenlijke aanpak is noodzakelijk", zegt Hans Hillen. Een ander belangrijke taak in het teken van cyber security is weggelegd voor alle defensiemedewerkers. Ondanks alle maatregelen blijkt uit de praktijk dat systemen kwetsbaar zijn door menselijk gedrag. Dat komt vaak door de zwakste schakel: de medewerker. "Elke defensiemedewerker moet zich bewust worden van de risico's die aan het gebruik van digitale middelen verbonden zijn", aldus de minister. Waar de medewerker daarbij aan moet denken is bijvoorbeeld het gebruik van een usbstick. Weet je niet waar die vandaan komt? Gooi die dan in de prullenbak. Open ook geen bijlagen van onduidelijke e-mails. Defensie zal overigens geen afzonderlijk krijgsmachtdeel oprichten voor het optreden in het digitale domein. De operationele cybercapaciteiten zullen in 2014 worden ondergebracht in het Defensie Cyber Commando bij de landstrijdkrachten.

DEFENSIE STRATEGIE VOOR HET OPEREREN IN HET DIGITALE DOMEIN

uit Defensie Cyber Strategie

Het digitale domein is, naast het land, de lucht, de zee en de ruimte, inmiddels het vijfde domein voor militair optreden. Dit domein en de toepassing van digitale middelen als wapen of inlichtingenmiddel zijn onmiskenbaar sterk in ontwikkeling. Digitale middelen zullen in toenemende mate integraal deel uitmaken van het militaire optreden. De afhankelijkheid van digitale middelen leidt daarentegen ook tot kwetsbaarheden die urgente aandacht behoeven. De Nederlandse krijgsmacht trekt hier de noodzakelijke gevolgen uit en wil in het digitale domein de vooraanstaande rol spelen die bij ons land past. Om de inzetbaarheid van de krijgsmacht te waarborgen en haar effectiviteit te verhogen, versterkt Defensie de komende jaren haar digitale weerbaarheid en ontwikkelt zij het vermogen om cyber operations uit te voeren.

Kol Hans Folmer, Commandant van de Task Force Cyber presenteert Defensie Cyber Strategie

Tegen deze achtergrond doe ik u hierbij de Defensiestrategie voor het opereren in het digitale domein toekomen: de Defensie Cyber Strategie. Zij geeft op een voortvarende manier uitwerking aan de in de beleidsbrief 'Defensie na de kredietcrisis' van 8 april 2011 (Kamerstuk 32 733, nr. 1) opgenomen cyberintensivering en aan het defensiedeel in de Nationale Cyber Security Strategie (Kamerstuk 26643, nr. 174). De strategie is aangekondigd in de kabinetsreactie op het advies over 'digitale oorlogvoering' van de Adviesraad voor Internationale Vraagstukken (AIV) en de Commissie van Advies inzake Volkenrechtelijke Vraagstukken (CAVV) (Kamerstuk 33 000-X, nr. 79).
De Defensie Cyber Strategie geeft de komende jaren richting, samenhang en focus aan de integrale aanpak voor de ontwikkeling van het militaire vermogen in het digitale domein. Zij is daardoor van wezenlijk belang voor de toekomstige effectiviteit en relevantie van onze krijgsmacht.

DE MINISTER VAN DEFENSIE drs. J.S.J. Hillen

CYBER INTEGRAAL ONDERDEEL VAN ONS HELE OPTREDEN

INTERVIEW MET KOLONEL IR. HANS FOLMER, COMMANDANT VAN DE TASKFORCE CYBER

"Naast het land, de lucht, de zee en de ruimte, is cyber het inmiddels vijfde domein voor militair optreden", zo vertelde minister Hans Hillen van Defensie eind juni bij de presentatie van de Defensie Cyber Strategie. Directeur Business Development Bastiaan Bakker van Motiv sprak met 'cyber-kolonel' Hans Folmer over de nieuwe cyberstrategie en het 'opereren in het vijfde domein'.

Kolonel Hans Folmer is als Commander Taskforce Cyber verantwoordelijk voor de coördinatie van alle cyber gerelateerde activiteiten binnen Defensie. "En dat behelst zeker niet de opzet van een 'cyberleger'", zo benadrukt Folmer, om meteen maar een misverstand uit de wereld te helpen. "We gaan niet een apart krijgsmachtdeel voor cyber oprichten, want dat zou volledig inefficiënt zijn. Cyber is een onderdeel van het hele spectrum van inzetmogelijkheden en maakt deel uit van land-, lucht- en marineoperaties. Je kunt nooit zuiver en alleen in cyber opereren."

In plaats van een 'cyberleger' komt er een 'cybereenheid' van zo'n tweehonderd man sterk. Deze eenheid wordt ondergebracht bij de landmacht maar is ondersteunend aan alle krijgsmachtonderdelen. Uiteindelijk is het de bedoeling dat 'cyber' de rode draad wordt door alles wat Defensie doet. "Cyber zal bijvoorbeeld deel gaan uitmaken van al onze oefeningen, al onze opleidingen en al onze trainingen", vertelt Folmer. "Iedereen moet zich realiseren dat we kwetsbaar zijn en dat we gevaar lopen."

Bastiaan Bakker: Loopt Nederland een reëel gevaar om te worden aangevallen via cyber?
Hans Folmer: "Er zijn al voorbeelden bekend van landen die zijn aangevallen via cyber. In 2007 bijvoorbeeld zijn er grote DDoS-aanvallen geweest op Estland, nadat ze daar een standbeeld van een Russische krijger hadden verplaatst naar een buitenwijk. Het is altijd onduidelijk gebleven of Rusland achter die aanvallen zat, of dat dit het werk was van sympathisanten. Veel gecoördineerder was de aanval van Rusland op Georgië ten tijde van de oorlog in Zuid-Ossetië in 2008. Tijdens de inval van Rusland in Georgië werden ook de overheidssystemen aangevallen. Dat was heel duidelijk staat tegen staat, al heeft Rusland de aanval op de overheidssystemen nooit toegegeven. En nu op dit moment is er ook een cyberoorlog vanuit Syrië aan de gang. Vanuit Syrië is bijvoorbeeld al een paar keer Reuters gehackt met als doel daar informatie te plaatsen die vervolgens wordt overgenomen door andere netwerken. Ook wij moeten ons realiseren dat we kwetsbaar zijn als we in de toekomst ergens ingrijpen. Als we bijvoorbeeld een humanitaire actie uitvoeren in 'land X' kan het best zijn dat sympathisanten in 'land Y' het daar niet mee eens zijn en Nederland via cyber aanvallen. Daar moeten we ons tegen wapenen. Overigens maakt het voor je reactie wel uit of je door een land of door sympathisanten – en dus burgers – wordt aangevallen; je moet noodzaak en proportionaliteit altijd meenemen in je reactie."

Waarom heeft Defensie een eigen cyberstrategie ontwikkeld, naast de Nationale Cyber Security Strategie (NCSS)?
"De Nationale Cyber Security Strategie geeft de strategie van de 'BV Nederland' weer. Daarin staat ook een paragraaf over Defensie, maar de invulling daarvan moest Defensie nog wel zelf doen. Dat hebben we gedaan in een Defensie Cyber Strategie waarin staat wat Defensie de komende vijf tot tien jaar gaat doen op het gebied van cyber. Echt een blik vooruit waarin we duidelijk aangeven wat onze plannen zijn, waar onze focus ligt en hoe we dat gaan doen.

Ikol Marco Verhagen, dagvoorzitter VOV Symposium 'Cyber in de Praktijk' en tweede man van de Task Force Cyber

Het is belangrijk dat we richting Tweede Kamer en het publiek duidelijk aangeven wat we willen."

Wat wil Defensie met de Defensie Cyber Strategie bereiken?
"Binnen de Defensie Cyber Strategie hebben we zes speerpunten gedefinieerd. Een eerste belangrijk speerpunt is een integrale aanpak van cyber. Cyber is niet iets unieks maar moet een integraal onderdeel zijn van ons hele optreden. Ook moeten we defensieve capaciteiten inrichten om onszelf te beschermen. De NCSS zegt dat iedereen in Nederland zelf verantwoordelijk is voor de beveiliging van de eigen systemen en dat geldt ook voor Defensie. Daarnaast moeten we een inlichtingencapaciteit inrichten zodat we cyber kunnen gebruiken als inlichtingenmiddel. Een volgende stap is het inrichten van een operationele capaciteit; cyber moet in operaties een integraal onderdeel zijn van de 'toolbox' van de commandant. Dat betekent dat een commandant zelf zijn systemen moet kunnen beveiligen en binnen het cyberdomein zelf gevechtsinlichtingen moet kunnen verzamelen en offensief moet kunnen optreden. Een ander speerpunt is dat we snel en adaptief moeten zijn zodat we snel kunnen inspelen op de veranderende digitale wereld en zelf dingen kunnen ontwikkelen. Tot slot zullen we moeten samenwerken met andere partners want we kunnen dit niet alleen. Maar dan moeten we wel eerst leren lopen; nu zijn we allemaal nog aan het kruipen."

Met welke partners gaat u de samenwerking zoeken?
"Dan denk ik aan samenwerking met publieke partners zoals het Nationaal Cyber

De Cyberwarfare arena van KPN door Martijn van der Heide

Bent u een Actor of een Victim door Ikol Rob Tollenaar van DEFCERT

Security Centrum, de KLPD en de AIVD en in internationaal verband de Navo en de Europese Unie en bilateraal met andere landen. Maar we gaan ook nadrukkelijk de samenwerking zoeken met private partners. In andere situatie zijn wij de vragende partij en biedt het bedrijfsleven de oplossing; in cyber hebben wij allemaal hetzelfde probleem en kunnen we dingen gezamenlijk aanpakken."

Wat bedoelt u als u zegt dat we 'allemaal hetzelfde probleem' hebben?
"Binnen de BV Nederland moet iedereen zichzelf beschermen en dat is voor iedereen een uitdaging. Hoe kan ik mij zo goed mogelijk beschermen; hoe kan ik ervoor zorgen dat ik nieuwe dreiging afsla en vrij en veilig kan opereren in het digitale omgeving en met anderen kan communiceren. Natuurlijk heeft Defensie wel een voorsprong als het gaat om het afslaan van een dreiging. Wij mogen inlichtingen verzamelen en als we een mandaat hebben van de regering met de juiste 'rules of engagement', dan mogen we ook opereren in cyberspace net zoals we dat mogen ter land, ter lucht, ter zee en in de ruimte."

En 'opereren in cyberspace' is dan ook daadwerkelijk aanvallen met digitale middelen?
"Dat kan zijn daadwerkelijk zelf aanvallen, maar dat kan ook zijn het beïnvloeden van de digitale systemen van de tegenstander waardoor een systeem bijvoorbeeld een andere functie gaat vervullen of onbruikbaar wordt. Maar het doel kan ook zijn het vergaren van informatie uit de systemen van de tegenstander."

Wat voor soort wapens worden in het domein cyber ingezet?
"Dan moet je denken aan wapens of systemen die zeer gecompliceerd zijn en een zeer specifiek doel hebben. Wij hebben niets aan een virus dat zichzelf ongecontroleerd via internet verspreidt en een half land plat legt. Het moet iets zijn wat alleen het doel bereikt

Cyber Test Range door Marko Lindgren van IVENT

want 'collateral damage' willen we te allen tijde voorkomen. De ontwikkeling van dergelijke wapens is een continu proces. Cyberwapens kun je maar één keer inzetten; als ze eenmaal een keer zijn ingezet, zijn ze onbruikbaar geworden. De tegenstander kan dan zijn eigen kwetsbaarheid opheffen en je eigen wapen kan zelfs tegen jezelf worden gebruikt."

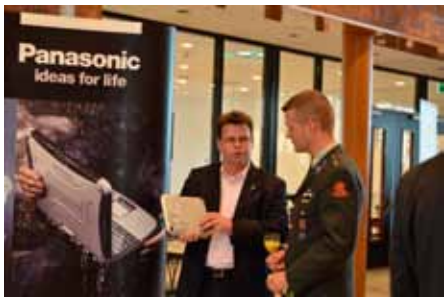
Maar dan heeft Defensie naast militairen ook behoefte aan ontwikkelaars die continu wapens ontwikkelen!
"Klopt. Voor de ontwikkeling van wapens hebben we al mensen in huis en we gaan zeker nog mensen binnenhalen. Maar de mensen die we binnenhalen moeten ook defensief kunnen optreden en inlichten kunnen verzamelen. We hebben dus niet alleen ontwikkelaars nodig, maar ook adviseurs, mensen die nadenken over de doctrine, mensen die resultaten analyseren, trainers, mensen die oefeningen leiden... We focussen iedere keer op die hackers, maar dat is maar een relatief kleine groep!"

Welke stappen worden nu gezet om de zes speerpunten uit de Defensie Cyber Strategie te realiseren?
"We staan aan het begin van een ontwikkeling. Minister Hillen heeft nu net de strategie gepresenteerd en mijn programma bestaat sinds januari van dit jaar. We beginnen nu met de defensieve en inlichtingencapaciteit en we denken na over de defensieve capaciteit. Eind 2013, begin 2014 moet het

Defensive and Offensive use of Malware door Christiaan Beek van McAfee

DefCERT (Defensie Computer Emergency Response Team, red.) volledig operationeel zijn en in staat zijn om 24x7 alle systemen te monitoren. DefCERT kijkt aan de buitenkant welke dreigingen op ons afkomen en adviseert de beheerder van de netwerken – die feitelijk verantwoordelijk is voor de beveiliging – hoe de kwetsbaarheid voor de dreiging kan worden opgeheven. We hebben nu al een DefCERT maar de capaciteit van dit team zijn we nu verder aan het uitbreiden. Eind 2013, begin 2014 moet eveneens het Defensie Cyber Expertise Centrum operationeel zijn. Deze eenheid gaat zich bezighouden met de kennisontwikkeling op het gebied van cyber – door middel van bijvoorbeeld research en het onderhouden van een cyberlaboratorium waar we kunnen testen en oefenen – en het uitdragen van die kennis. Een jaar later hebben we de offensieve capaciteit ontwikkeld en zullen we het Defensie Cyber Commando operationeel stellen als onderdeel van de landmacht en daarin zit dan de operationele capaciteit en het Defensie Cyber Expertise Centrum. Dan heb je het domein zowel defensief, inlichtingen en offensief operationeel afgedekt."

Bent u niet bang dat de cyberstrategie gaat lijden onder de forse bezuinigingen die ook op Defensie worden doorgevoerd?
"Als we kijken naar de begroting voor 2012 en verder, dan zien we dat we bijna een miljard euro bezuinigen maar dat er wel extra geld is vrijgemaakt voor cyber. Als er verder druk op het budget komt, weet ik niet wat de gevolgen zijn voor het cyberbudget. Maar ik verwacht eigenlijk niet dat het cyberbudget echt onder druk komt te staan. De aandacht is er, de urgentie is er. Door het neerzetten van een strategie hebben we ook aangegeven welke prioriteit we er aan geven. Cyber is een van de belangrijkste intensiveringen van onze regering."



Foto's met dank aan kap b.d. A.J.J. Buitendam en kap b.d. H.T.J. Meijers

DEFENSIE CYBER STRATEGIE

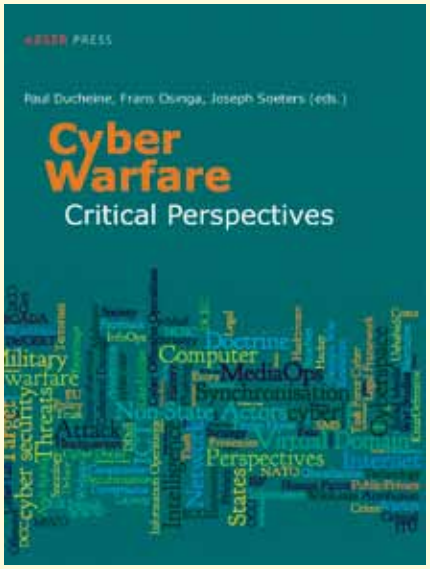
De Defensie Cyber Strategie geeft de komende jaren richting, samenhang en focus aan de ontwikkeling van het militaire vermogen in het digitale domein. In de strategie worden zes speerpunten genoemd. Dat zijn:
- de totstandkoming van een integrale aanpak;
- de versterking van de digitale weerbaarheid van Defensie;
- de ontwikkeling van het militaire vermogen om cyber operations uit te voeren;
- de versterking van de inlichtingenpositie in het digitale domein;
- de versterking van de kennispositie en van het innovatieve vermogen van Defensie in het digitale domein en
- de intensivering van de samenwerking in nationaal en internationaal verband.

A bigger bang for the Buck door Willem Groenendaal van Logica

BRONNEN:

- Defensie Cyber Strategie
- Defensiekrant juni 2012
- Woordvoerder van het Ministerie van Defensie
- Motiv, Magazine Motivator
- Ferry Waterkamp, Freelance journalist, E-mail: ferry@fw-forwords.com
- VOV Symposium 'Cyber in de praktijk'

CYBER WARFARE: CRITICAL PERSPECTIVES



Editors: Associate Prof. Paul Ducheine, Prof. Frans Osinga, Prof. Joseph Soeters, Nederlandse Defensie Academie, Breda, The Netherlands

Abstract
Next to sea, land, air and space, 'cyberspace' appears to be the fifth operational domain for the military. This manmade and virtual sphere brings along opportunities and threats. In this book, academics of the Netherlands Defense Academy as well as specialists and military professionals from other institutions analyze developments in cyber security. The authors use various fields of expertise, enabling them to apply a truly multi-disciplinary approach.

Cyber threats affect states' vital interests. By consequence, responses are required that need to come from public authorities as well as organizations on the market and in civil society. Additionally, this is not a national state's affair; cyber threats are an international concern.

This collection of essays questions the premises and scenarios on which policy responses are based. Are these scenarios describing real or imaginary threats? A number of contributions specifically deal with this issue.

This volume also covers the process of 'securitization', the legal aspects of cyber operations, the use of social media in military operations as well as an economic analysis of the costs of cyber dangers. Furthermore, the authors analyze organizational responses to cyber threats. Resilience is the central term in this respect, both at the individual and the organizational level of military HQs and strategic network management. An analysis based on operations research and game theory illustrates the vulnerabilities of digital networks. No matter how dangerous cyber threats may look at face value, one should not overdramatize the dangers, as the last chapters seem to imply.

In all contributions, the authors have attempted to combine academic theory with practical views and suggestions. This makes this book valuable not only for people from academic life, but particularly also for people who struggle with the intricacies and worries of cyber threats in their everyday (professional) life.

Kol Paul Ducheine betrokken bij de discussie tijdens het Symposium 'Cyber in de Praktijk'.

Colonel Paul Ducheine is associate professor of cyber operations at the Netherlands Defense Academy and a lecturer in military law at the University of Amsterdam. Air-Commodore Frans Osinga is professor of military operational art and sciences at the Netherlands Defense Academy.
Joseph Soeters is professor of management and organization studies at the Netherlands Defense Academy and at Tilburg University
Publisher: T.M.C. ASSER PRESS
Date published: 2012
Details
Pages: 319 pp. Hardbound
ISBN: 978-90-6704-341-0
Language: English
Price (€) : 25.00

GARANTIES AMERIKAANSE CLOUDDIENSTEN FLINTERDUN

De garanties die Amerikaanse clouddiensten bieden ten aanzien van de bescherming van Europese persoonsgegevens zijn nogal dun, stelt het College Bescherming Persoonsgegevens (CBP).
Overheden en bedrijven die gegevens laten verwerken door in de VS gebaseerde clouddiensten, zoals die van bijvoorbeeld Google, Dropbox of Microsoft, moeten zich realiseren dat de garanties die dergelijke bedrijven bieden ten aanzien van de bescherming van persoonsgegevens flinterdun zijn. Organisaties blijven zelf verantwoordelijk voor de gegevens.

ZELFCERTIFICERING

Het College Bescherming Persoonsgegevens onderzocht de garanties - met name de Safe Harbor-verklaring die Amerikaanse bedrijven afgeven - op verzoek van SURFmarket, dienstverlener voor honderdduizenden medewerkers en studenten in het Nederlandse hoger onderwijs. De Safe Harbor-regeling is een afspraak tussen de VS en de EU, die stelt dat Amerikaanse bedrijven alleen Europese persoonsgegevens mogen verwerken en opslaan als ze een Safe Harbor-certificaat hebben. Die vorm van zelfcertificering garandeert volgens het CBP niet dat de verwerking van de gegevens in de VS zelf voldoet aan Europese richtlijnen. Evenmin is Safe Harbor (waaraan een paar duizend Amerikaanse bedrijven zeggen te voldoen) een garantie voor afdoende gegevensbeveiliging.

BEVEILIGING

Ook standaarden als SAS 70, de in Nederland gangbare ISAE 3402 en SSAE 16, die gaan over extern toezicht op de beveiliging, bieden niet de garantie dat de beveiliging zelf aan alle eisen voldoet. Daarnaast is het nog de vraag of zogeheten 'sub-bewerkers' (partijen die door de cloudleverancier worden ingeschakeld om bijvoorbeeld opslag of beheer te verzorgen) eveneens aan de Safe Harbor-regels voldoet en hoe die garantie wordt gecommuniceerd.

MELDPLICHT

Ten slotte merkt het CBP ook nog op dat de door de regering gewenste meldplicht voor datalekken in het geval van clouddiensten alleen is te realiseren als de verantwoordelijke daarover heldere afspraken maakt met de 'bewerker' (de cloudleverancier) en eventuele sub-bewerkers. De organisatie die gegevens bij clouddiensten onderbrengt blijft te allen tijde zelf verantwoordelijk voor het naleven van de Wet bescherming persoonsgegevens, stelt het CBP.

BRONNEN:

- http://www.binnenlandsbestuur.nl/digitaal-besturen/
- de heer Freek Blankena

ATOS VOLTOOIT BEHEER KRITISCHE IT-SYSTEMEN OLYMPISCHE SPELEN LONDEN 2012

Dit artikel is een vervolg op cyber-veilige Spelen in 2012 in Interom 2011-1.

Honderden business technology-specialisten leveren topprestatie tijdens meest interactieve Spelen ooit.

Londen - 13 augustus 2012 - Atos - wereldwijd IT-partner van de Olympische Spelen - en het Organiserend Comité van de Olympische en Paralympische Spelen in Londen (LOCOG) hebben bekendgemaakt dat de levering van de IT-infrastructuur van het wereldwijde sportevenement succesvol is verlopen. Deze kernsystemen maakten het mogelijk dat meer dan 8 miljoen toeschouwers in de stadions en ruim 4 miljard mensen wereldwijd getuige waren van de Olympische Spelen Londen 2012. Londen 2012 gaat de geschiedenis in als één van de meest interactieve Olympische Spelen ooit. Meer mensen dan ooit tevoren bekeken de wedstrijden via verschillende apparaten. Aan de basis van het succesvolle beheer van de IT-systemen van de Spelen staan de business technology-specialisten van Atos, die een individuele topprestatie hebben geleverd door de wedstrijdresultaten in minder dan 0,3 seconden wereldwijd aan de media beschikbaar te stellen. Dat is 30 keer sneller dan de winnende tijd die is neergezet tijdens de finale van de 100 meter sprint heren.

"Met de ondersteuning van Atos waren we in staat een antwoord te geven op de behoefte van toeschouwers de Spelen realtime te volgen via verschillende kanalen. Het team van business technology-specialisten is er in geslaagd de belangrijkste componenten van de end-to-end IT-systemen te ontwerpen, bouwen en beheren en ervoor te zorgen dat de wedstrijdresultaten door meer mensen dan ooit gelezen en bekeken konden worden", benadrukt Jacques Rogge, Voorzitter van het Internationale Olympische Comité (IOC). "Atos is het brein achter het management van de IT-systemen van de Olympische Spelen en heeft consistent op tijd en binnen budget geleverd. Ik zie er naar uit om tijdens de Olympische Winterspelen in Sochi 2014 en de Olympische Zomerspelen in Rio 2016 opnieuw met Atos - sinds jaren onze wereldwijde IT-partner - samen te werken."

"In onze hoedanigheid van leidende systeemintegrator, projectmanager en operations manager voor kritische IT-systemen was Atos verantwoordelijk voor belangrijke IT-systemen van de Olympische Spelen. Ik ben er zeer trots op te kunnen zeggen dat ons team erin geslaagd is het beheer van alle IT-systemen geruisloos te laten verlopen. Dat hebben zij gedaan op een wijze die al onze verwachtingen overtreft", vertelt Thierry Breton, bestuursvoorzitter en CEO van Atos. "De manier waarop mensen tijdens deze Spelen met elkaar in verbinding stonden via hun tv, mobiele apparatuur, social media en internet maken Londen 2012 tot de meest interactieve Spelen aller tijden. We zijn trots op de rol die we hebben gespeeld tijdens het evenement dat een enorm succes is geworden voor het IOC, LOCOG en de voltallige olympische familie."

NIEUWE STANDAARD VOOR DE TOEKOMST

Het team van Atos werkte achter de schermen intensief samen met LOCOG en de overige technologiepartners om een vlekkeloze ontsluiting van informatie tijdens de Spelen te waarborgen. Het was het meest omvangrijke en meest geavanceerde sportgerelateerde IT-project ooit, waarbij het team een aantal nieuwe benchmarks voor toekomstige Spelen heeft vastgesteld:

- levering van IT-systemen die meer dan 250.000 accreditaties voor de olympische familie hebben verwerkt en geactiveerd;
- ondersteuning van 35 wedstrijdlocaties op basis van een volledige IT-infrastructuur om ervoor te zorgen dat wedstrijden volgens schema konden plaatsvinden;
- verwerking en ontsluiting van 30 procent meer wedstrijdresultaten dan tijdens voorgaande Spelen aan media en persagentschappen wereldwijd;
- distributie van real-time wedstrijdresultaten en data van alle 26 olympische sporten aan internationale omroeporganisaties. Deze informatie is verspreid via het Commentator Information System (CIS) van Atos;
- het verspreiden van wedstrijdresultaten, wedstrijdschema's en informatie over weersomstandigheden, transport en andere relevante gegevens aan alle 14.700 atleten - ontsloten via het Info+-systeem van Atos;
- het vanaf de openingsceremonie mogelijk maken van de dagelijkse publicatie van 900 Engelstalige artikelen door de olympische nieuwsdienst

Tijdens de Olympische Spelen in Londen 2012 was het e-mailverkeer tijdens kritische IT-processen voor het eerst tot nul gereduceerd. In plaats hiervan paste het technologische team instrumenten toe om informatie over de belangrijkste processen effectief te beheren en te delen.

VLEKKELOOS VERLOOP OLYMPISCHE SPELEN

"Eén van de grootste uitdagingen tijdens Londen 2012 is de ontsluiting van enorme volumes data die zijn ontsloten via de IT-systemen van de Spelen aan miljarden toeschouwers over de hele wereld - via verschillende kanalen en in real-time", aldus Jean-Benoît Gauthier, directeur technologie van het Internationale Olympische Comité. "Atos - de wereldwijde IT-partner van de Olympische en Paralympische Spelen - heeft een doorslaggevende rol gespeeld bij de bouw en het beheer van een uiterst complex IT-systeem dat aan de basis stond van een succesvol verloop van de Spelen."

"De ontwikkeling van de technologie voor de Spelen vroeg van het organiserend comité en al onze partners om als één team met elkaar samen te werken met als doel een ongelooflijk complexe technologische oplossing te leveren. Atos was ongetwijfeld één van de belangrijkste spelers binnen dit zeer succesvolle team", aldus Gerry Pennell, CIO van LOCOG.

"De Olympische Spelen zijn een complexe mix van technologie, IT-processen en mensen. We stonden tijdens Londen 2012 voor de uitdaging een IT-oplossing te ontwikkelen die het mogelijk maakt elk denkbaar moment van sportieve prestaties vast te leggen en internationale media te ondersteunen hiervan rechtstreeks via televisie en internet verslag te doen", zegt Patrick Adiba, CEO Major Events & Olympic Games van Atos.

Londen 2012 waren de eerste Olympische Spelen in de geschiedenis waarbij sprake was van live streaming van elke minuut van de wedstrijden. Het was bovendien voor de eerste keer dat tijdens de Olympische Zomerspelen alle 26 olympische sporen toegevoegd waren aan CIS. Een geoptimaliseerd en uitgebreid Remote CIS-systeem zorgde er ook voor dat de snelheid waarmee data door Atos werden ontsloten verslaggevers in staat stelden rechtstreeks vanuit hun eigen land commentaar te leveren, zonder de noodzaak ter plekke in het stadion aanwezig te zijn.