

B

jaargang 14 - 2014

#2

MATIEBEVEILIGING

WEERBAARHEID

De sterkte van wachtwoorden en hun tekortkomingen

ISO27001 herzien

COLUMN: het recept voor privacyvriendelijk innoveren

Nationale Cyber Security Strategie 2

Op 28 oktober 2013 werd de tweede Nationale Cyber Security Strategie (NCSS 2) uitgebracht, tweeëneenhalf jaar na de eerste. De strategische focus verschuift van publiek-private samenwerking naar publiek-private participatie en strategische samenwerking. De nieuwe strategie beoogt dat Nederland qua volwassenheidsniveau op Cyber Securitygebied van bewust naar bekwaam gaat. Wat zijn de nieuwe doelstellingen en actielijnen van de NCSS 2 en wat betekent dat voor u en uw organisatie?

VERSLAG NATIONALE CYBER SECURITY STRATEGIE 2

Van bewust naar bekwaam



Nederland internationaal gidsland met onder andere cyberdiplomatie

Bij de start van de campagne Alert Online presenteerde minister Opstelten van Veiligheid en Justitie op 28 oktober jongstleden de tweede Nationale Cyber Security Strategie, de NCSS 2 [1]. Na het uitbrengen van de eerste NCSS tweeëneenhalf jaar geleden zijn grote stappen gezet. Daarentegen is het duidelijk dat de urgentie van aandacht voor en aanpak van Cyber Security alleen maar groter geworden is [2]. Grote incidenten als de DigiNotar-affaire, de KPN hack en de denial-of-service aanvallen op Nederlandse banken, KLM en de overheid hebben dit duidelijk gemaakt.

De nieuwe nationale strategie gaat uit van de visie dat Nederland samen met haar internationale partners inzet op een veilig digitaal domein, waarin de kansen die digitalisering onze samenleving biedt volop worden benut, dreigingen het hoofd worden geboden en fundamentele rechten en waarden worden beschermd. Nederland heeft drie ambities die invulling moeten geven aan deze visie: (1) onze samenleving weet op een veilige manier optimaal gebruik te maken van de voordelen en kansen die cyberspace ons biedt, (2) Nederland loopt voorop op het gebied van security-by-design en privacy-by-design en (3) Nederland vormt met internationale partners een vooruitstrevende coalitie voor het beschermen van fundamentele rechten en

waarden in het digitale domein, of te wel cyberspace. Voor een dergelijk brede benadering van cyberspace is het nodig om nationaal en internationaal de juiste balans te zoeken tussen veiligheid, vrijheid en de economische voordelen van cyberspace. De eerste Nationale Cyber Security Strategie uit begin 2011 had tot doel om te komen tot bewustwording over het cyberberrisico. Deze strategie beoogt een nieuw volwassenheidsniveau qua Cyber Security te bereiken: die van bekwaam. Dat kan natuurlijk alleen in samenwerking met burgers, private partijen en de overheden waarbij kennisontwikkeling en -toepassing, transparantie en (zelf)regulering een grote rol spelen. Van burgers (consumenten) wordt gevraagd om minimaal een basisoniveau aan cyberhygiëne te betrachten, een

Auteur: Eric Luijck is principal consultant Cyber Operations & Critical (Information) Infrastructure Protection bij TNO.

Eric is bereikbaar via eric.luijck@tno.nl.

eigen verantwoordelijkheid te nemen en een zekere bekwaamheid te ontwikkelen in het veilig gebruik van cybermiddelen en -diensten. Denk aan het gebruik van sterke wachtwoorden en het privé houden daarvan, het regelmatig updaten van de eigen computersystemen en het zorgvuldig beschermen van privégegevens. De overheid verwacht dat private partijen aanspreekbaar zijn op hun verantwoordelijkheid voor veilig cybergebruik. Ze hebben een zorgplicht richting burgers, andere bedrijven en overheden. Van leveranciers wordt verwacht dat zij inzetten op security-by-design en privacy-by-design. Leveranciers, systeemintegratoren en dienstenleveranciers zouden hun producten en diensten veilig 'uit de doos' moeten leveren. Dat betekent bijvoorbeeld dat standaardwachtwoorden uit den boze zijn, dat bij een initiële installatie een sterke beveiligingssituatie wordt afgedwongen en dat dienstenleveranciers zich minimaal houden aan 'good cyber security practices'. De rijksoverheid is van plan dit gedrag sterk te stimuleren.

Doelstellingen

De rijksoverheid faciliteert daarnaast uitwisseling van informatie over dreigingen en actuele incidenten. Ze zet ook de kaders uit voor nationaal beleid en internationale samenwerking. De eigen cyber security capaciteiten van de overheid - het Nationaal Cyber Security Centrum (NCSC), de politie en bij Defensie - worden daarom versterkt. De genoemde visie en ambities vertalen zich in vijf meerjarige doelstellingen:

1. **Nederland is weerbaar tegen cyberaanvallen en beschermt zijn vitale belangen in het cyberdomein,**
2. **Nederland pakt cybercriminaliteit aan,**
3. **Nederland investeert in veilige en privacybeschermende ICT-producten en -diensten,**
4. **Nederland bouwt coalities voor vrijheid, veiligheid en vrede in het cyberdomein,**
5. **Nederland beschikt over voldoende cyber securitykennis en -kunde en investeert in ICT-innovatie om onze cyber securitydoelstellingen te behalen.**

Deze vijf doelstellingen zijn uitgewerkt in een actieprogramma 2014-2016 met 37 acties/actielijnen. Nieuw ten opzichte van het vorige actieprogramma is dat de 37 acties zoveel mogelijk SMART (Specifiek, Meetbaar, Acceptabel, Realistisch en Tijdgebonden) gemaakt zijn: de acties zijn specifiek, de verantwoordelijke actiehouders zijn aangewezen en er wordt een tijdsverwachting uitgesproken. Ook is aandacht besteedt aan de governance. Jaarlijks zal over de voortgang van het actieplan worden gerapporteerd aan de Tweede Kamer. Ten opzichte van de eerste NCSS wordt hiermee een grote stap vooruit gezet omdat de voortgang of het eventueel achterblijven van de acties op transparante wijze inzichtelijk worden en bijsturing kan plaatsvinden. De acties, die direct van belang zijn voor de lezers van dit blad en hun organisaties, waaronder leveranciers van (beveiligings)producten en -diensten, zijn:

1. **Een nadere aanscherping van welke ICT-afhankelijke systemen, diensten en processen vitaal zijn, een weerbaarheidverhogend programma en publiek-private**

oefeningen.

2. **Het verbeteren en ontwikkelen van cyber security standaarden en good practices voor alle organisaties en het ontwikkelen van minimum veiligheidseisen voor vitale ICT-processen.**
3. **Het stimuleren van security-by-design en privacy-by-design doordat de overheid daarvoor eisen gaat opnemen in haar aanbestedingsprojecten.**
4. **Een onderzoek naar een gescheiden, veilig ICT-netwerk voor publieke en private vitale processen.**
5. **Versterking van sectorale toezichthouders door het opnemen van cyber security eisen in de regelgeving.**
6. **Het intake- en registratieproces van aangiften cybercriminaliteit bij de politie wordt versterkt.**
7. **Het instellen van een publiek-private Task Force Cyber Security Onderwijs die zich onder andere gaat richten op certificering van professionals en het verder ontwikkelen van lesmodules.**
8. **De aankondiging van nieuwe tenders 2014-2015 ter waarde van 6 miljoen euro voor cyber securityonderzoek en de mogelijkheid voor het bedrijfsleven van een cyber security 'scientist on the job'.**

Andere actiepunten betreffen onder andere cyberdiplomatie, de versterking van internationale samenwerking en versnelling van de ambities van Defensie op het gebied van cybercapaciteiten. Voor leveranciers van ICT-producten en -diensten en systeemintegratoren biedt de NCSS 2 kansen. Het bewust ontwikkelen en leveren van cyberveilige en privacybeschermende producten en -diensten kan u binnenkort een marktoversprong geven. Voor organisaties in vitale sectoren is er daarentegen het risico dat toezichthouders minimum beveiligingseisen gaan verplichten als zelfregulering op het cyber security gebied niet werkt.

Conclusie

Met de nieuwe Nationale Cyber Security Strategie geeft de Nederlandse overheid zowel nationaal als internationaal het signaal af dat de borging van fundamentele rechten en waarden in cyberspace en cyber security hoog op de agenda staan, maar ook dat Nederland de economische kansen die cyberspace biedt wil grijpen.

Dit artikel is eerder verschenen in Beveiliging.

Referenties

- [1] Nationale Cyber Security Strategie 2 - van bewust naar bekwaam, Ministerie van Veiligheid en Justitie, oktober 2013, <http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2013/10/28/nationale-cyber-security-strategie-2.html>
- [2] cyber securitybeeld Nederland 3, Ministerie van Veiligheid en Justitie, juli 2013, <http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2013/07/03/Cyber-Securitybeeld-nederland.html>