HET CYBER SECURITY BELEID VAN DE TOEKOMST

November 2012

BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

ONDERTEKENAARS

Dit beleid wordt ondertekend door:

- Burgerrechtenvereniging Vrijbit
- Dutch Hosting Provider Association
- Free Press Unlimited
- HCC
- Humanistisch Verbond
- Internet Protection Lab
- Ouders Online
- Platform Bescherming Burgerrechten
- Stichting KDVP
- Stichting Meldpunt Misbruik ID-plicht
- Stichting Privacy First
- Vereniging NLUUG
- Vrijschrift / ScriptumLibre
- Mr. A.M. Arnbak, Universiteit van Amsterdam
- Prof.mr. E.J. Dommering, Universiteit van Amsterdam
- Prof.dr. N.A.N.M. van Eijk, Universiteit van Amsterdam
- Rop Gonggrijp
- Dr. P.J.A. de Hert, Universiteit Tilburg
- Dr. J.V.J. van Hoboken, Universiteit van Amsterdam
- Dr. J.H. Hoepman, Radboud Universiteit Nijmegen
- Prof.mr. S. van der Hof, Universiteit Leiden
- Prof.dr.ir. C.T.A.M. de Laat, Universiteit van Amsterdam
- Prof.dr. T. Lange, Technische Universiteit Eindhoven
- Prof.dr. R.A. Lawson, Universiteit Leiden
- Prof.dr. R.E. Leenes, Universiteit Tilburg
- Ing. J.C.G. van de Looy, Madison Gurkha BV
- Dr.ir. E. Poll, Radboud Universiteit Nijmegen
- Drs. R. Rustema, Universiteit van Amsterdam
- Dr. P. Schwabe
- Prof.mr.dr. J.M. Smits, Technische Universiteit Eindhoven
- Prof.dr.ir. H.C.A. van Tilborg, Technische Universiteit Eindhoven

Diginotar, de KPN-hack, Stuxnet: het zijn grote incidenten die Nederland de afgelopen jaren wakker hebben geschud. Nederland wordt steeds afhankelijker van ICT en daarmee worden we ook steeds kwetsbaarder voor aanvallen op onze ICT-systemen. Cybersecurity staat dan ook terecht hoog op de politieke agenda.

Maar als we ons te veel richten op die incidenten, wordt ons cybersecuritybeleid niet meer dan paniekvoetbal: we blussen brand na brand, terwijl het huis verder in de modder zakt. Ondertussen dreigt internetvrijheid, door bijvoorbeeld vergaande vormen van monitoring, in de verdrukking te komen en lopen we het risico om een van de belangrijkste infrastructuren van de 21e eeuw – het internet – te ondermijnen.

Digitale burgerrechtenbeweging Bits of Freedom vindt dat cybersecurity beter verdient. We zijn ervan overtuigd dat we met slimme, gerichte maatregelen onze cybersecurity sterk kunnen verbeteren. Daarom presenteren we in deze notitie vier uitgangspunten en acht maatregelen voor modern cybersecuritybeleid.

UITGANGSPUNTEN
MODERN CYBERSECURITYBELEID

A. CYBERSECURITY IS OOK *PERSONAL SECURITY*

Cybersecurity gaat vaak over het beschermen van vitale infrastructuur, zoals energiecentrales en waterkeringen. Maar cybersecurity gaat ook over een ander belangrijk onderwerp: de bescherming van de meest waardevolle en intieme informatie van burgers en bedrijven. Want als bijvoorbeeld de opgeslagen telefoniegegevens, medische gegevens of locatiegegevens van miljoenen Nederlanders op straat komen te liggen, kan dat een nationale ramp betekenen.

B. CYBERSECURITYBELEID MOET GRONDRECHTEN RESPECTEREN

Cybersecuritymaatregelen die geregeld worden voorgesteld raken al gauw aan grondrechten: zo beperkt een "internetkillswitch" de communicatievrijheid en maakt massale surveillance van internetverkeer ernstige inbreuk op de privacy. Dit is onacceptabel: volgens vaste jurisprudentie van het Europees Hof voor de Rechten van de Mens is de wezenlijke kern van grondrechten onaantastbaar. De noodzaak, proportionaliteit, subsidiariteit en effectiviteit van nieuwe maatregelen moet op dit gebied dus altijd vooraf worden aangetoond. Het logische gevolg hiervan is dat cybersecuritymaatregelen steeds maatwerk vereisen en dus moeten worden toegesneden op het probleem dat opgelost wordt.

C. CYBERSECURITY VEREIST TRANSPARANTIE

Beleid op het gebied van cybersecurity kan vergaande maatschappelijke gevolgen hebben, onder meer voor grondrechten en voor de werking van het internet. Juist daarom moet dit beleid controleerbaar zijn, zodat dit zo nodig in een vroeg stadium kan worden bijgestuurd. Dit betekent dat transparantie het uitgangspunt moet zijn: het beleid moet onder meer uitgaan van reële en verifieerbare dreigings- en risicoanalyses, die zijn toegesneden op het specifieke risico dat het beleid probeert te adresseren. Die analyses moeten vóóraf maar ook periodiek ná invoering van het beleid worden uitgevoerd.

D. EXTREME MAATREGELEN LEIDEN NIET TOT ABSOLUTE VEILIGHEID

Hoe belangrijk veiligheid in het digitale domein ook is: extreme maatregelen leiden niet tot absolute veiligheid. Veiligheid is per definitie de uitkomst van een kosten-batenafweging. Juist voor cybersecurity geldt bovendien dat kleine partijen tegen relatief lage kosten al grote schade kunnen aanrichten: de ontwikkeling van een geavanceerd virus zoals Dorifel is daarvan een voorbeeld. Risico's kunnen zo veel mogelijk worden voorkomen door vooraf simpele veiligheidsmaatregelen te nemen, door risico's zo veel mogelijk te spreiden en te voorzien in terugvalmechanismen. Maar ook in die omstandigheden zullen we bepaalde cybersecurityrisico's gewoonweg moeten accepteren omdat de kosten om die risico's te voorkomen te hoog zijn (zowel in euro's als in de aantasting van onze individuele vrijheid).

MAATREGELEN
MODERN CYBERSECURITYBELEID

1. **CYBERSECURITYBELEID MOET *PERSONAL SECURITY* CENTRAAL STELLEN**

   De afgelopen jaren heeft de overheid steeds vaker verplicht om gevoelige gegevens van miljoenen burgers op te slaan: vingerafdrukken, kentekens, verkeersgegevens (van telefonie en e-mail), locatiegegevens, etc. Ook wordt de toegang tot dit soort gegevens onvoldoende beperkt. De gegevens van telefonie-abonnees zijn makkelijk toegankelijk voor de politie en worden daardoor bijna drie miljoen keer per jaar opgevraagd. Dit moet anders: met beginselen als dataminimalisatie of decentralisatie kunnen we het volgende datalek voorkomen, simpelweg omdat er niets of niet genoeg te lekken valt. De overheid moet veel minder opslaan: zij zal steeds vooraf moeten aantonen dat de opslag van bepaalde gegevens noodzakelijk is en welk doel dit dient. Indien dit doel niet bereikt wordt, moeten die gegevens bovendien kunnen worden vernietigd. Verder moet de overheid de toegang tot deze gegevens tot het minimum beperken en van *security by design* en *privacy by design* centrale ontwerpbeginselen maken. Onderdeel daarvan is dat de overheid bij de inkoop van producten en diensten moet streven naar een gezonde diversiteit van IT-systemen, om zo kwetsbaarheden te beperken. En die uitgangspunten gelden niet alleen voor de publieke sector: ook de opslag en toegang tot privégegevens door bedrijven moet aan strengere banden worden gelegd en de beveiliging moet beter worden geregeld.

2. **ER MOET WORDEN GEÏNVESTEERD IN KENNIS EN CAPACITEIT OP HET GEBIED VAN CYBERSECURITY, NIET IN NIEUWE BEVOEGDHEDEN**

   De overheid beschikt vaak niet over voldoende kennis en capaciteit om adequaat te reageren op cybersecurityincidenten en de bestaande bevoegdheden effectief te gebruiken. De overheid moet daarom investeren in mensen met de benodigde kennis en huidig personeel bijscholen. Zo zou de overheid meer ambtenaren met een technische achtergrond moeten aantrekken en ervoor moeten zorgen dat opsporingsambtenaren verder worden opgeleid in digitaal rechercheren.

Verder moet de overheid investeren in onderwijsinstellingen op het gebied van cybersecurity, zodat het kennisniveau in Nederland zich verder kan ontwikkelen en voor de toekomst gewaarborgd is. Tot slot moet de overheid investeren in aanvullend wetenschappelijk onderzoek. Pas als er voldoende kennis en capaciteit is om de huidige bevoegdheden goed aan te wenden, is er aanleiding om over nieuwe bevoegdheden te spreken.

3. INTERNETGEBRUIKERS MOETEN ZICHZELF KUNNEN BESCHERMEN

De overheid moet ervoor zorgen dat internetgebruikers (inclusief vele organisaties in de publieke en private sector) zichzelf goed kunnen beschermen tegen digitale risico's. De *tools* en de ondersteuning die internetgebruikers nu voor handen hebben zijn vaak onvoldoende. Tegelijkertijd is een groot aantal incidenten te wijten aan simpele kwetsbaarheden en kunnen die incidenten worden voorkomen door het toepassen van simpele veiligheidsmaatregelen, zoals regelmatige software-updates. Cybersecurity begint dan ook bij voorlichting over die maatregelen, het stimuleren van het gebruik van cybersecurity-technologie, zoals versleutelingssoftware en anonimiseringstechnologie, en de ontwikkeling van veilige software. Dit betekent ook dat de overheid *backdoors* in versleutelingstechnieken niet moet verplichten en de ontwikkeling hiervan niet moet stimuleren.

4. DE OVERHEID MOET ZELF HET GOEDE VOORBEELD GEVEN

Gebrek aan controle of grote afhankelijkheid van derden vormt een aanzienlijk veiligheidsrisico en ondermijnt de geloofwaardigheid van overheidsbeleid op het gebied van cybersecurity. De overheid heeft aanvullende kennis en capaciteit op het gebied van ICT nodig zodat zij de controle over haar eigen infrastructuur kan uitoefenen en de risico's van beleid dat zij voorstelt beter kan inschatten.

5. CYBERSECURITY MOET EEN KERNTAAK VAN DE OVERHEID BLIJVEN

De overheid heeft een belangrijke rol om ervoor te zorgen dat onze informatiemaatschappij veilig is. Juist vanwege de grote maatschappelijke belangen moet de overheid zich daarom terughoudend opstellen bij het steunen van zelfregulering en publiek-private samenwerking en altijd eindverantwoordelijke blijven. Dit betekent dat de overheid alleen de hulp van private partijen mag inroepen als de

overheid (i) de noodzaak daarvan vóóraf heeft aangetoond, (ii) de eisen voor die samenwerking opstelt, (iii) eindverantwoordelijke blijft, (iv) transparant is over deze samenwerking, en (v) – waar grondrechten in het geding zijn – parlementaire controle garandeert.

6. DE UITWISSELING VAN INCIDENTINFORMATIE MOET WORDEN GESTIMULEERD

Voor hun eigen veiligheid en de veiligheid van anderen zijn organisaties in de publieke en private sector mede afhankelijk van incidentinformatie van anderen: aan de hand van bekende dreigingen en kwetsbaarheden kunnen zij hun informatiesystemen beter beveiligen. De overheid moet de uitwisseling van dit soort informatie bevorderen, bijvoorbeeld via platforms voor het uitwisselen van bekende softwaregaten, aanvalspatronen en besmette IP-adressen. Voor zover mogelijk moet dit soort informatie ook publiek worden gedeeld. De uitwisseling van incidentinformatie moet met waarborgen worden omkleed om misbruik van en fouten in de informatie te voorkomen. Ook moet zij zorgen dat kennis over kwetsbaarheden in ICT-technologieën zo snel mogelijk openbaar wordt gemaakt. Ze moet meldingen van ethische hackers stimuleren door het opstellen van richtlijnen voor *responsible disclosure.*

7. ER MOET EEN MELDPLICHT VOOR DATA- EN BEVEILIGINGSLEKKEN KOMEN

Het lekken van persoonsgegevens leidt tot identiteitsfraude en verlies van vertrouwen in informatietechnologie. De overheid en het bedrijfsleven moeten daarom worden verplicht om onbevoegde toegang tot persoonsgegevens te melden aan slachtoffers. Een publiek register voor data- en beveiligingslekken stelt bedrijven en de overheid in staat om te leren van de fouten en dreigingen inzichtelijk te maken.

8. TOEZICHTHOUDERS MOETEN KRACHTIG KUNNEN OPTREDEN

Het College Bescherming Persoonsgegevens (CBP) ziet toe op de bescherming van onze persoonsgegevens. Het Nationaal Cyber Security Centrum (NCSC) gaat over onze weerbaarheid in het digitale domein. Beiden moeten kunnen bepalen of een incident een significant risico voor informatieveiligheid vormt en zo nodig snel en effectief kunnen reageren. Dat betekent dat ze voldoende budget en bevoegdheden moeten krijgen. Daarnaast moet (internationale) coördinatie en samenwerking tussen toezichthouders worden bevorderd.

OVER BITS OF FREEDOM

Bits of Freedom verdedigt de communicatievrijheid en privacy van Nederlandse internetgebruikers. Zij doet dat door constructieve campagnes te voeren en de overheid en het bedrijfsleven te informeren.

Voor een nadere toelichting op dit document zijn wij vanzelfsprekend graag beschikbaar.

Stichting Bits of Freedom
Postbus 10746
1001 ES Amsterdam

Simone Halink
T: 06 46 28 26 93
E: simone.halink@bof.nl