De verenigde Nederlandse hackerspaces en organisaties
Postbus 503
2501 HJ Den Haag

Woordvoorder: Dhr. K.F.J. (Koen) Martens – 06-24707813

Aan: de leden van de commissie Binnenlandse Zaken van de Tweede Kamer der Staten-Generaal

Betreft: brandbrief van nationale hackergemeenschap inzake ICT-beveiliging overheid

Den Haag, 15 september 2011

Zeer geachte leden van de vaste Tweede Kamercommissie BiZa,

De Nederlandse hackergemeenschap, vertegenwoordigd door de ondergetekende organisaties, maakt zich zorgen over de beveiliging van ICT-systemen van de Nederlandse overheid. Keer op keer zien wij hoe basale beveiligingsprincipes niet worden toegepast binnen bestaande en nieuwe ICT-systemen.

Recente voorbeelden zijn de kwestie rond Diginotar en de SSL-certificaten, de OV-chipkaart, het elektronisch patiëntendossier (EPD) en nog vele andere systemen en omgevingen. Wij hebben een omvangrijke lijst van voorbeelden van overheidssystemen die persoonsgegevens bevatten of persoonsgegevens vragen aan burgers waar de beveiliging niet op orde is.

Dit zijn geen ingewikkelde hacks, maar fouten die mensen zonder opleiding kunnen misbruiken. Daarvoor is standaard programmatuur op internet voorhanden. Het gaat om elementaire beveiligingsprincipes die structureel niet worden toegepast en een blind vertrouwen in techniek, gestoeld op onvoldoende begrip van de risico's. Audits en certificeringen zijn papieren tijgers. Er wordt onvoldoende gekeken naar de systemen zelf en blind vertrouwd op verklaringen van bijvoorbeeld de ontwikkelaars.

Er wordt niet voldoende getoetst of de beloftes van ICT-bedrijven ingehuurd door de overheid realistisch zijn en worden nagekomen. Adequate bescherming van databanken met persoonsgegevens is onvoldoende gewaarborgd. Er wordt niet nagedacht over mogelijk misbruik van nieuwe systemen. Tegelijk worden aan de overheid gelieerde instanties zoals het College Bescherming Persoonsgegevens (CBP) en GOVCERT in onvoldoende mate betrokken bij ICT-trajecten.

De hackergemeenschap voelt zich geroepen deze zaken aan de kaak te stellen. Echter, er heerst op dit moment een klimaat waarin de boodschapper wordt gestraft en de betreffende departementen en bedrijven niet tot verantwoording worden geroepen. Wij zijn daarom terughoudend in het delen van informatie over deze beveiligingslekken.

Wij maken ons zorgen over het feit dat de beveiligingslekken dermate elementair zijn, dat het vrijwel zeker is dat mensen met kwade bedoelingen zich hiervan bewust zijn en deze fouten kunnen uitbuiten. Zoals de recente kwestie met de Iraanse overheid heeft laten zien.

Wij roepen derhalve op om de kwestie Diginotar niet als incident te zien, maar als een symptoom van een gebrek aan controle op de veiligheid van ICT-systemen bij de overheid. Het is tijd dat de leden van de Tweede Kamer, zij die het volk vertegenwoordigen en geacht worden het volk te behoeden voor dit soort vergissingen, zich realiseren dat er sprake is van een structureel probleem.

De Nederlandse hackergemeenschap beschikt over de kennis en kunde met betrekking tot bovengenoemde zaken, en deelt deze graag met de volksvertegenwoordigers.

Hoogachtend,

Koen Martens
Namens de verenigde Nederlandse hackerspaces en organisaties:

Stichting Hack42 te Arnhem
Stichting ACKspace te Heerlen
Stichting TkkrLab te Enschede
Stichting Bitlair te Amersfoort
Stichting Revelation Space te 's-Gravenhage
Stichting Randomdata te Utrecht
Stichting Frack te Leeuwarden
Stichting Sk1llz te Almere

Stichting eth0
2600nl.net
Stichting HXX