Hoog tijd voor een deltaplan cybersecurity

D66

Het belang van ICT neemt elk jaar toe. Er is bijna geen aspect van ons leven meer te bedenken waar digitalisering géén rol speelt. Met dit toegenomen belang van ICT neemt ook het belang van cyberveiligheid toe. Ons dagelijks leven, onze economie, zelfs onze samenleving is ervan afhankelijk. Cyberveiligheid is dus van cruciaal belang voor onze toekomst. Toch blijft de aandacht voor cyberveiligheid, bij de overheid, maar óók bij bedrijven, ver achter.

Cyberveiligheid is van groot belang voor elk aspect van ons leven. Zonder een veilig internet kunnen we niet internetbankieren, kunnen we geen gevoelige informatie delen met vrienden, familie, artsen en de overheid en kunnen we niet veilig informatie opzoeken. Het is zelfs mogelijk om via cyberaanvallen onderdelen van onze vitale infrastructuur (energie, water, communicatie) plat te leggen. Zo werden in Oekraïne en Brazilië elektriciteitscentrales plat gelegd met grote gevolgen voor de fysieke veiligheid van mensen – denk aan ziekenhuizen en ouderen die zorg nodig hebben. Maar er zijn ook voorbeelden van waterzuiveringsinstallaties die gesaboteerd zijn. Ook in Nederland ligt onze vitale infrastructuur constant onder vuur van cyberaanvallen.

Het afgelopen half jaar hebben we in de Verenigde Staten gezien dat cyberveiligheid ook belangrijk is voor onze democratie. Russische hacks op de Democratische Partij leidden tot beïnvloeding van de campagne. Ook bij de verkiezingen in Nederland, Frankrijk en Duitsland dit jaar is dergelijke Russische inmenging in het democratisch proces mogelijk. Daar moeten we niet naïef over zijn.

Nu al kost Cybercriminaliteit Nederland jaarlijks zo'n 12 miljard euro.[1] Met name onze innovatieve bedrijven zijn een populair doelwit voor economische spionage. Het kan gaan om cyberaanvallen die de productie van bedrijven onderbreken of om aanvallen waarbij intellectueel eigendom het doelwit is. Maar we zien ook steeds meer virussen die data versleutelen waardoor mensen en bedrijven schade oplopen.

Daarom wil D66 dat het volgende kabinet een deltaplan cyberveiligheid start. Hiervoor maakt D66 jaarlijks 125 miljoen euro beschikbaar. Dat deltaplan moet bestaan uit de volgende elementen:

1) 50 miljoen voor een Topinstituut voor cyberveiligheid

D66 investeert 1 miljard euro in onderzoek en innovatie. Daarvan wil D66 50 miljoen euro steken in een nieuw instituut voor cyberveiligheid. Onderzoekers kunnen op dit instituut, samen met bedrijven en overheden, baanbrekend onderzoek doen op het gebied van cyberveiligheid. De inzichten uit dit instituut kunnen leiden tot een wereldwijd leidende industrie; cyberveiligheid is immers een wereldwijd probleem.

1https://www2.deloitte.com/nl/nl/pages/over-deloitte/articles/cybercriminaliteit-kost-nederlandse-organisaties-10-miljard-euro-per-jaar.html,
http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

2) 50 miljoen voor Defensie Cyber Commando

De oorlog van vandaag en morgen wordt steeds meer gevoerd op het digitale slagveld. Al een aantal jaar waarschuwen onze inlichtingendiensten, de MIVD en de AIVD, voor cyberaanvallen vanuit Rusland en China. Ook is er sprake van toenemende dreiging van digitale spionage tegen Defensie, defensietoeleveranciers, bondgenootschappelijke netwerken en producenten van militair-relevante producten. D66 wil dat Defensie over voldoende slagkracht beschikt voor deze digitale strijd. Daarom investeren we substantieel in cyberwarfare capaciteiten. Ook verbeteren we onze inlichtingenpositie.

3) 25 miljoen voor meer cyberrechercheurs en kennis bij politieagenten

Nederlanders doen zelden aangifte van cybercriminaliteit. Dit komt omdat de politie onvoldoende kennis en middelen heeft om cybercriminaliteit effectief aan te pakken. Politieagenten die aangiftes opnemen moeten meer kennis hebben van ICT en de politie moet meer geld krijgen om meer cyberrechercheurs aan te nemen en op te leiden. Ook moet de hackwet aangepast worden. Deze wet houdt veelgebruikte apparaten zoals telefoons en tablets onveilig voor hacks door criminelen.

4) Garantie op slechte software

Als consument heeft u recht op een goed product. In de wet staat dat een product deugdelijk moet zijn. Dit moet niet alleen voor de hardware gelden, maar ook voor de software. Is de software onveilig en weigert het bedrijf het te beveiligen, dan moet je als consument het product terug kunnen brengen. Net als bij een stoel waar de poot na een week vanaf valt. Steeds meer bedrijven zijn tegenwoordig softwareontwikkelaar en daarom moeten zij zich bewust zijn van de verantwoordelijkheid die hoort bij het leveren van software.

Natuurlijk is software nooit 100% veilig. Maar niet genoeg aandacht besteden aan de kwaliteit van software of het niet tijdig updaten van software is een vorm van nalatigheid. Net zoals het nalatig is om niet over de brandveiligheid van producten na te denken. De Amerikaanse toezichthouder FTC heeft bijvoorbeeld het Taiwanese bedrijf D-link aangeklaagd omdat het bedrijf producten zou verkopen met softwarefouten die al decennia lang bekend zijn en makkelijk te voorkomen zijn.

5) ICT doorlichten en inkoop en aanbesteding aanscherpen

Bijna elke week is er wel weer een schandaal over een onveilig ICT-systeem van de overheid. Van de software waarmee stemmen geteld worden tot de belastingdienst en van het kadaster tot gemeentewebsites. D66 wil alle vitale overheidssystemen doorlichten op cyberveiligheid en indien nodig vervangen.

Ook moet de inkoop en aanbesteding van software aangescherpt worden. De Commissie Elias schatte dat er jaarlijks zo'n 1 tot 5 miljard wordt verspild aan de aanbesteding van software systemen. Toch gaat de overheid nog steeds in zee met partijen die keer op keer broddelwerk leveren. Voortaan moet één minister verantwoordelijk zijn voor alle ICT-projecten van de Rijksoverheid, krijgt het Bureau ICT-Toetsing écht tanden en leveranciers die slechte software aanleveren worden voortaan uitgesloten.

6) Nationaal cybertestcentrum

D66 wil een testcentrum om de weerbaarheid van water-, energie-, telecom- en zorgvoorzieningen tegen cyberaanvallen te verbeteren. Door de toenemende cyberaanvallen op onze vitale infrastructuur is een dergelijke testcentrum van groot belang. De eerste stappen naar een dergelijk testcentrum zijn al genomen door The Hague Security Delta en TNO. Dit testcentrum kan bovendien nieuwe bedrijven en werkgelegenheid aantrekken.