6 AANBEVELINGEN

Dit onderzoek laat zien dat kwetsbaarheden in software leiden tot onveiligheid voor organisaties die software gebruiken, en voor hen die van deze organisaties afhankelijk zijn. De kloof groeit tussen digitale afhankelijkheid en de dreigingsomvang enerzijds, en de weerbaarheid van de samenleving daartegen anderzijds. Snel en fundamenteel ingrijpen is nodig om te voorkomen dat de maatschappij ontwricht raakt. Daarom doet de Onderzoeksraad voor Veiligheid aanbevelingen. De eerste aanbeveling is erop gericht om op korte termijn de responscapaciteit te vergroten. De erna volgende aanbevelingen hebben als doel om op de langere termijn het publieke en private stelsel te versterken en prikkels te introduceren zodat er een systeem ontstaat waarbinnen fabrikanten en afnemers voortdurend werken aan het veiliger maken van software.

Aan het Nederlandse kabinet en aan organisaties in Nederland die software gebruiken:[227]

1. Zorg er op korte termijn voor dat alle potentiële slachtoffers van cyberaanvallen snel en doeltreffend - gevraagd en ongevraagd - worden gewaarschuwd, zodat zij maatregelen kunnen treffen voor hun digitale veiligheid . Breng daartoe private en publieke responscapaciteit samen en zorg daarbij voor voldoende mandaat en wettelijke waarborgen.

Toelichting: Het gaat hierbij in ieder geval om informatie over welke systemen van welke organisaties kwetsbaar zijn en risico lopen om aangevallen te worden (zogenoemde 'slachtofferinformatie'). Momenteel staat de juridische interpretatie van de AVG (IP-adressen als persoonsgegeven) en de Wbni (mandaat van het NCSC beperkt tot Rijk en vitaal) het NCSC in de weg om alle slachtoffers waar zij informatie over krijgen te waarschuwen en om zelf proactief deze informatie te verzamelen ('scannen').

Aan de Eurocommissaris voor Interne Markt en de Eurocommissaris voor een Europa dat klaar is voor het digitale tijdperk:

2. Zorg dat uw initiatieven om te komen tot wetgeving voor veiligere software leiden tot een Europese verordening die de verantwoordelijkheid van fabrikanten vastlegt en afnemers inzicht geeft in hoe fabrikanten die verantwoordelijkheid invullen. Leg vast dat fabrikanten aansprakelijk zijn voor de gevolgen van softwarekwetsbaarheden.

Toelichting: Essentiële elementen van deze verordening zijn onder andere – maar niet uitsluitend - verplichte deelname aan *bug bounty* programma's, richtlijnen voor onafhankelijke audits, het melden van kwetsbaarheden, traceerbaarheid, *recalls*, en het delen van lessen uit cyberaanvallen. Ervaringen met wet- en regelgeving als de AVG/GDPR bewezen dat Europese regulering in het digitale domein haalbaar en effectief is.

227 Uit praktische overwegingen schrijft de Onderzoeksraad de overheid in zijn rol als afnemer aan via de staatssecretaris van Binnenlandse Zaken, het Interprovinciaal Overleg, de Vereniging van Nederlandse Gemeenten en de Unie van Waterschappen. De andere organisaties, waaronder zorg, onderwijs, vitale aanbieders en het overige bedrijfsleven schrijft de Raad aan via de bij de SER betrokken ondernemersorganisaties VNO-NCW, MKB-Nederland en LTO Nederland.

Aan fabrikanten van software gezamenlijk:[228]

3. Ontwikkel met andere fabrikanten good practices om software veiliger te maken. Neem in de overeenkomsten met uw afnemers op dat u zich hieraan committeert.
4. Waarschuw en help al uw afnemers zo snel en doeltreffend mogelijk wanneer kwetsbaarheden in software gesignaleerd worden. Schep de randvoorwaarden die noodzakelijk zijn om uw afnemers te kunnen waarschuwen.

Toelichting: De verantwoordelijkheid en mogelijkheden om software veiliger te maken en om afnemers te waarschuwen ligt in de eerste plaats bij fabrikanten zelf.

Aan de minister van Binnenlandse Zaken en Koninkrijksrelaties en de minister van Economische Zaken en Klimaat (ten behoeve van alle organisaties en consumenten in Nederland): [229]

5. Bevorder dat Nederlandse organisaties en consumenten gezamenlijk veiligheidseisen formuleren en afdwingen bij softwarefabrikanten. Zorg dat de overheid daarbij een voortrekkersrol speelt. Ga uit van het principe: collectieve samenwerking waar mogelijk; branche-specifiek waar noodzakelijk.

Toelichting: Het is noodzakelijk dat afnemers hun krachten bundelen zodat zij hun positie richting fabrikanten versterken en schaarse cybersecurity-expertise gezamenlijk zo doelmatig en effectief mogelijk inzetten, zoals een aantal Nederlandse banken nu al doet.

Aan het Nederlandse kabinet:

6. Creëer naar analogie van de Comptabiliteitswet een wettelijke basis voor de beheersing van digitale veiligheid door de overheid.
7. Verplicht alle organisaties om op eenduidige wijze verantwoording af te leggen over de wijze waarop zij digitale veiligheidsrisico's beheersen.[230]

Toelichting: De wijze waarop overheden en bedrijven de risico's die gepaard gaan met digitalisering beheersen en zich daarover verantwoorden is vooralsnog vrijblijvend. Versnippering van verantwoordelijkheden staat een slagvaardig optreden in de weg. Essentieel is dat er een sluitend stelsel komt dat organisaties helpt om de digitale veiligheid op systematische en doelmatige wijze te beheersen. Mogelijke elementen zijn een eenduidig mandaat voor CISO's bij de overheid, toezicht dat is belegd bij de minister die het aangaat en voor alle organisaties verplichte verantwoording over de beheersing van digitale veiligheidsrisico's, via jaarverslagen en onder controleverklaring van de accountant.

228 Deze aanbeveling is gericht aan alle fabrikanten van software. Uit praktische overwegingen schrijft de Onderzoeksraad de fabrikanten aan die betrokken waren bij de voorvallen die dit onderzoek beschrijft, de gemeenschappen van de betrokken open source-projecten en de (leden van de) brancheorganisatie Business Software Alliance.

229 Zie voetnoot 224. Vanwege de relevantie van veilige software voor eindgebruikers (inclusief consumenten) dient ook de Consumentenbond hierbij te worden betrokken. En de Kamer van Koophandel voor ondersteuning aan organisaties.

230 Het ligt in de rede om aan te sluiten bij bestaande structuren en verplichtingen in de Comptabiliteitswet 2016 (van toepassing op overheden), Burgerlijk Wetboek (niet-beursgenoteerde rechtspersonen), nadere voorschriften controle- en overige standaarden (NV COS) vanuit de NBA en geharmoniseerde wetgeving voor naamloze vennootschappen vanuit de EU.