Rathenau Instituut

Extra maatregelen nodig tegen cyberdreigingen

Bericht aan het Parlement

Het rapport 'Een nooit gelopen race' van het Rathenau Instituut laat zien dat de huidige maatregelen van overheid en bedrijfsleven tegen cyberdreigingen niet volstaan. In de strijd tegen de steeds professionelere methoden van statelijke actoren, cybercriminelen en andere kwaadwillende hackers zijn extra maatregelen nodig. De Rijksoverheid en bedrijven met hoogwaardige technologie zijn structureel doelwit van digitale spionage. Daarnaast lopen het MKB en de burger steeds grotere risico's. Cyberdreigingen ondergraven het concurrentievermogen van het Nederlandse bedrijfsleven en het vertrouwen in de digitale samenleving. Versterking van cybersecurity moet dan ook meer prioriteit krijgen. Zo moet de overheid als grote inkoper van beveiligingsproducten een voorbeeldrol vervullen als 'launching customer', en meer investeren in expertiseontwikkeling en capaciteitsuitbreiding.

Toenemende afhankelijkheid van ICT

Nederland hoort tot een van de meest gedigitaliseerde landen ter wereld. Het maatschappelijke en economische verkeer is in hoge mate afhankelijk van een goede ICT-infrastructuur. Nederland vormt daarmee een aantrekkelijk doelwit voor statelijke actoren en cybercriminelen.

Belangrijkste cyberdreigingen

Buitenlandse inlichtingendiensten verzamelen op grote schaal politieke, militaire

en technologische informatie. Daarnaast worden cybercriminelen professioneler, de gebruikte methoden geavanceerder en hun verdienmodel winstgevender. Consumenten en mkb-bedrijven worden steeds vaker slachtoffer van cybercriminaliteit.

Weerbaarheid onvoldoende op orde
Burger, bedrijfsleven en overheid zijn onvoldoende weerbaar tegen cyberdreigingen. Basale beveiligingsmaatregelen, zoals software-updates, sterke wachtwoorden of back-ups van belangrijke bestanden, worden vaak niet genomen. Door gebrekkig inzicht in risico's en de mogelijkheden om daar iets aan te doen, wordt vaak gekozen voor goedkope oplossingen. Ook binnen de vitale sectoren is de cyberweerbaarheid niet altijd op orde. Dit is des te verontrustender omdat cyberdreigingen de komende jaren alleen maar verder zullen toenemen.

Internet of Things versterkt kwetsbaarheid
De opkomst van het Internet of Things versterkt de kwetsbaarheid voor cyberaanvallen. De beveiliging van 'slimme' apparaten, zoals slimme poppen of webcams, is vaak niet op orde, waardoor ze kunnen worden gehackt en ingezet voor grootschalige DDoS-aanvallen. Op dit moment ontbreken de economische prikkels voor fabrikanten om de beveiliging van ICT-apparaten substantieel te verbeteren. Dat is een vorm van 'marktfalen'.

Continue wedloop tussen aanvallers en verdedigers
ICT is inherent onveilig. Software en hardware bevatten onvermijdelijk allerlei kwetsbaarheden. Aanvallers zijn voortdurend op zoek naar nieuwe kwetsbaarheden en nieuwe aanvalsmethoden, waartegen verdedigers zich steeds opnieuw moeten wapenen. Door de snelle technologische ontwikkelingen is sprake van een continue wedloop tussen aanvallers en verdedigers. Informatiebeveiliging is dan ook nooit af, maar vergt voortdurend aandacht en investeringen.

Cyberveiligheid biedt ook kansen
De Nederlandse kennisinstellingen en cybersecuritysector beschikken over veel expertise op het gebied van ICT-beveiliging. Die kennis kan worden benut om de aantrekkelijkheid van Nederland te vergroten als vestigingsplaats voor ICT-bedrijvigheid. Beveiligingsmaatregelen bieden ook nieuwe kansen voor de cybersecuritysector.

Aanbevelingen
Het rapport 'Een nooit gelopen race' doet de volgende aanbevelingen aan de overheid en het bedrijfsleven ter versterking van de weerbaarheid tegen cyberdreigingen:

- Besteed binnen het onderwijs en in voorlichtingscampagnes meer aandacht aan digitale vaardigheden, maar overvraag de burger niet.
- Investeer in een onafhankelijk kennis- en adviescentrum voor mkb-bedrijven.
- Spreek vitale sectoren sterker aan op hun verantwoordelijkheid voor een veilige bedrijfsvoering, bijvoorbeeld door een jaarlijkse hacktest in te voeren.
- Geef als overheid het goede voorbeeld als 'launching customer' en stuur binnen de overheid sterker aan op adequate beveiligingsmaatregelen.
- Maak als overheid meer werk van vervolging van cybercrime.
- Leg 'open' beveiligingsnormen in wetgeving vast voor slimme apparaten en laat toezichthouders op basis hiervan actief optreden tegen onveilige ICT-producten.
- Zie toe op naleving van zorgplichten voor veilige producten door ICT-leveranciers, en ga na of de zorgplichten en aansprakelijkheidswetgeving hiervoor aanpassing behoeven.
- Investeer in cybersecurity-opleidingen.
- Investeer in voldoende expertise en capaciteit binnen de overheid, betrokken toezichthouders en de AIVD.

Monitor 'checks and balances' verruimde bevoegdheden diensten

De Tweede Kamer heeft onlangs ingestemd met de wetsvoorstellen Computercriminaliteit III en modernisering Wiv, die de bevoegdheden van opsporingsdiensten en inlichtingen- en veiligheidsdiensten moeten verruimen. Deze wetsvoorstellen hebben veel discussie losgemaakt. De discussie spitst zich vooral toe op het toezicht op het gebruik dat de diensten maken van hun (ruimere) bevoegdheden en de waarborgen voor de rechtspositie van de burger. Het verdient aanbeveling te monitoren of in de in de wetsvoorstellen opgenomen 'checks and balances' in de praktijk afdoende zijn.

Achtergrond

Onderzoek naar de kansen en risico's van de digitale samenleving vormt een van de speerpunten van het werk van het Rathenau Instituut. Het instituut deed dit onderzoek naar ontwikkelingen in cyberdreigingen en cyberweerbaarheid op verzoek van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en de Algemene Inlichtingen- en Veiligheidsdienst (AIVD). Er is literatuuronderzoek verricht en er zijn 36 interviews gehouden. De bevindingen hiervan zijn besproken tijdens twee workshops met deskundigen en betrokken maatschappelijke partijen.