Cybersecuritybeeld Nederland

Om ongestoord te kunnen functioneren, moeten we onze samenleving zo goed als mogelijk beschermen tegen digitale dreiging. Ondanks de inspanningen om de weerbaarheid te verhogen, is er sprake van scheefgroei met de toenemende dreiging. Die scheefgroei vergroot het risico op ontwrichting van onze samenleving. Denk hierbij aan de bankensector, het openbaar vervoer of drinkwater. Dat blijkt uit het jaarlijkse Cybersecuritybeeld Nederland (CSBN) van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), dat in samenwerking met het Nationaal Cybersecurity Centrum (NCSC) is opgesteld.

Het is niet zozeer de vraag of bedrijven worden aangevallen, maar wanneer. Datzelfde geldt voor de overheid, kennisinstellingen en andere organisaties. De basismaatregelen op orde hebben helpt, maar deze zijn nog lang niet overal goed doorgevoerd. Er wordt nog te weinig gewerkt met multifactor authenticatie en het maken en testen van back-ups.

Cyberaanvallen door andere landen: het nieuwe normaal

Cyberaanvallen door buitenlandse inlichtingen- en veiligheidsdiensten zijn niet meer zeldzaam te noemen. Landen gebruiken de digitale ruimte om geopolitieke voordelen te behalen. Vanuit Rusland zijn meerdere EU-lidstaten succesvol geraakt door cyberaanvallen en China heeft op grote schaal en langdurig politieke doelwitten in Europa en Noord-Amerika aangevallen. Maar ook cybercriminelen zijn onverminderd in staat grote digitale schade aan te richten. Criminelen hebben primair een financiële drijfveer, maar een aanval kan zoveel impact hebben dat de nationale veiligheid geraakt wordt. Ook kunnen staten cybercriminelen inhuren, gedogen of onder druk zetten om cyberaanvallen uit te voeren. Dat er banden zijn tussen staten en cybercriminelen bleek onlangs nog, toen cybercriminelen gelieerd aan Rusland nadat de oorlog in Oekraïne uitbrak, waarschuwden tegenstanders van Rusland aan te willen vallen.

Ransomware, zero-days en de cloud

Aanvallen met gijzelsoftware worden steeds vaker ingezet met dubbele of zelfs drievoudige afpersing. Hierdoor wordt niet alleen de primair getroffen organisatie afgeperst maar ook de klanten, partners of leveranciers daarvan. Het NCSC ziet verder een toename van het aantal zero-day kwetsbaarheden. Misbruik daarvan kan grootschalige impact hebben als de kwetsbaarheid in veelgebruikte software of hardware zit. Ook misbruik van de cloud komt in toenemende mate voor. Clouddiensten zijn de afgelopen jaren cruciaal onderdeel geworden van bedrijfsprocessen. Uitval of verstoring kan grootschalige gevolgen hebben voor Nederlandse organisaties en sectoren.

Polarisatie en internationale conflicten: voedingsbodem voor hacktivisten

De directe dreiging die richting Nederland uitgaat van hackerscollectieven is klein. Er kan echter wel een afgeleide dreiging bestaan als acties van hacktivisten verkeerd worden geïnterpreteerd en landen die zij

aanvallen overgaan tot een tegenreactie.

Fundament voor Cyberstrategie

Het CSBN levert ieder jaar input voor beleidsvorming op nationaal niveau. Dit keer vormt het CSBN het fundament voor de nieuwe Nederlandse Cyberstrategie die in het najaar van 2022 verschijnt. Daarom zijn naast de analyse op belang, dreiging en weerbaarheid, ook zes strategische thema's toegevoegd; thema's die nu en de komende vier tot zes jaar relevant zijn voor de digitale veiligheid van Nederland. Dat zijn:

- Beperkingen in digitale autonomie beperken ook digitale weerbaarheid
- Risicomanagement staat nog in kinderschoenen
- Marktdynamiek compliceert beheersing van digitale risico's
- Risico's als keerzijde van gedigitaliseerde samenleving
- Digitale ruimte speelveld voor regionale en mondiale dominantie
- Cyberaanvallen eenvoudig schaalbaar, verdediging daartegen minder

Infographic CSBN 2022

Het CSBN 2022 geeft inzicht in de strategische thema's die nu en de komende vier tot zes jaar relevant zijn voor de digitale veiligheid van Nederland.

- **Beperkingen in digitale autonomie beperken ook digitale weerbaarheid**
  Nederland heeft beperkte keuzemogelijkheden om de richting te bepalen van verdere digitalisering – en daarmee van digitale weerbaarheid.

- **Risicomanagement staat nog in kinderschoenen**
  Digitale risico's hebben nog geen structurele plaats in het bredere risicomanagement binnen en tussen organisaties, sectoren en landen. Risico's zijn vaak niet in beeld, basismaatregelen niet getroffen.
- **Marktdynamiek compliceert beheersing van digitale risico's**
  Op digitale markten komen vraag en aanbod naar digitale diensten, hardware, software en netwerken samen. Hier is digitale veiligheid meestal niet leidend. Dit compliceert de beheersing van risico's.
- **Risico's als keerzijde van gedigitaliseerde samenleving**
  De Nederlandse samenleving is in hoge mate gedigitaliseerd; COVID-19 heeft dit proces verder versneld. Die afhankelijkheid van digitale processen maakt ons ook kwetsbaar voor uitval en activiteiten van kwaadwillenden.
- **Digitale ruimte speelveld voor regionale en mondiale dominantie**
  Staten gebruiken de digitale ruimte structureel én intensief voor de behartiging van hun geopolitieke belangen. Cyberaanvallen, bijvoorbeeld voor het vergaren van inlichtingen, zijn het 'nieuwe normaal'.
- **Cyberaanvallen eenvoudig schaalbaar, verdediging daartegen minder**
  Zware cybercriminaliteit is schaalbaar geworden en maakt daardoor meer slachtoffers, meerschade en is lucratiever dan ooit. Het schaalbaar maken en houden van de weerbaarheidsketen is een grote uitdaging.

Scheefgroei dreiging en weerbaarheid vergroot risico op ontwrichting
Om als maatschappij ongestoord te kunnen functioneren is weerbaarheid van de samenleving tegen digitale dreiging cruciaal. Die weerbaarheid blijft achter bij de omvangrijke belangen en de ontwikkelende dreiging.