De verkiezingsprogramma's doorgelicht

Op woensdag 17 maart mogen alle Nederlanders van achttien jaar en ouder weer naar de stembus voor de Tweede Kamerverkiezingen. In aanloop naar de verkiezingen hebben politieke partijen hun verkiezingsprogramma's gepubliceerd waarin ze hun plannen voor Nederland in de periode van 2021 - 2025 kenbaar maken.

Security.NL[1] heeft de verkiezingsprogramma's van alle politieke partijen in de Tweede Kamer doorgelicht en geeft in een reeks van vier achtergrondartikelen een overzicht van de onderwerpen: cybersecurity, privacy, Big Tech en digitalisering. Zo kunnen lezers in één oogopslag zien wat de partijen voor plannen op deze gebieden hebben en wat de overeenkomsten en verschillen zijn.

Omdat u als cyberburgemeester meer dan gemiddeld betrokken bent bij het verder brengen van het onderwerp Cyberveiligheid, delen we de verzamelde informatie door Security.NL met u zodat u in een oogopslag ziet waar de partijen op inzetten. Het gaat om zaken als de bescherming van data en systemen en de aanpak van cybercrime, maar ook de rol die de partijen voor de inlichtingendiensten zien weggelegd.

De onderstaande punten komen direct uit de partijprogramma's. In bepaalde gevallen is er voor de duidelijkheid gekozen om punten samen te vatten.

50Plus (programma)

- Meer geld en middelen voor internetpolitie die fraude en oplichting opspoort.
- Strengere straffen voor internetmisdaden.
- Politie gaat gratis weerbaarheidstrainingen aan ouderen en kwetsbare mensen geven.

Christendemocratisch Appèl (CDA) (programma)

- Nederland moet zich beter voorbereiden en oefenen op een massieve verstoring van het digitale domein door een technische storing of cyberaanval.
- Meerjarig cybersecurityprogramma onder leiding van een aparte Nationale Cybersecurity Coördinator.
- Versterken van inlichtingen en veiligheidsdiensten om Nederland tegen de groeiende digitale dreiging te beschermen
- Creëren van Cyberhub waar het Defensie Cyber commando en het Nationale Cybersecurity Centrum deel van uit maken.
- Waar nodig wordt de Wet op de inlichtingen- en veiligheidsdiensten aangepast om de effectiviteit van de diensten te vergroten.
- Bij Defensie kennis over alle vormen van digitale oorlogsvoering versterken.

[1] Een Community die actuele informatie wil delen over informatiebeveiliging, privacy en cybersecurity via een website en waar je anoniem reacties kunt posten of een forumtopic kunt starten.

ChristenUnie (programma)

- Bestrijding van kinderporno door specialistische teams van cyberrechercheurs.
- Stimuleren van startups op het gebied van cybersecurity.
- Startups en scale-ups krijgen rol in adviseren van overheden op het gebied van cybersecurity.
- Investeren in cyberkennis en -middelen van Defensie.
- Voorlichting over digiveiligheid op scholen en aan ouders.
- Steun van diplomatieke route om tot internationale normen voor het cyberdomein te komen.
- Kinderen bewust en veilig leren omgaan met internet en sociale media.

Democraten 66 (D66) (programma)

- Fors meer investeringen in onderzoek op het gebied van cybersecurity.
- Versterken van vaardigheden en slagkracht van toezichthouders op het gebied van cybersecurity.
- Extra geld voor politie en het OM voor aanpak cybercriminaliteit.
- Jaarlijks cyberafhankelijkheidsbeeld dat laat zien van welke partijen, digitale processen en diensten het functioneren van vitale processen in de Nederlandse samenleving afhankelijk is.
- NCSC mag beveiligingsinformatie van niet-vitale sectoren ook delen met Computer Emergency Response Teams.
- Procedure voor supersnelrecht om online content zo snel mogelijk - eventueel tijdelijk - van het internet te verwijderen.
- Investeren in cybercapaciteiten van Defensie. Kennis hierover bij de Nederlandse krijgsmacht kan zowel in EU- als NAVO-verband worden ingezet.
- Beschermen van vrije toegang tot informatie op Internet. Niet toestaan dat andere landen in de fundamenten van het internet ingrijpen.

Forum voor Democratie (FvD) (programma)

- Overheid mag geen gebruikmaken van Huawei en andere riskante Chinese apparatuur.
- Intrekken van de Sleepwet.
- Verplichting tot privacy en security by design.

GroenLinks (programma)

- Politie krijgt meer capaciteit en kennis om cybercrime en zaken als oplichting en kinderporno via internet op te sporen.
- Nederland zet zich in op het het tegengaan van cyberwar.
- Nederland streeft naar strikte internationale afspraken over inzet van cyberaanvallen.
- Technologie en apparatuur voor cybersurveillance gaan onder het wapenexportbeleid vallen.

- Bij terreurbestrijding ligt de nadruk op het verzamelen van inlichtingen uit menselijke bronnen en gerichte digitale surveillance in plaats van massasurveillance.
- De inlichtingen- en veiligheidsdiensten zetten hun bevoegdheden gericht in en publiceren jaarlijks het aantal geplaatste taps.
- De Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) krijgt de mogelijkheid om samen te werken met andere toezichthouders in betrouwbare Europese landen.

Partij van de Arbeid (PvdA) (programma)

- Meer capaciteit voor bestrijding cybercrime.
- Meer en betere rechercheurs die cybercrime aanpakken.
- Beschermen tegen cyberaanvallen en industriële spionage.

Partij voor de Dieren (PvdD) (programma)

- Overheid zet zich in voor het realiseren van cybereisen aan Internet of Things-apparaten.
- Zorgen voor een robuuste taskforce die spionage opspoort en tegengaat.
- De AIVD is zeer terughoudend met het delen van gegevens van burgers met buitenlandse veiligheidsdiensten.
- De Sleepwet wordt ingetrokken en er komt een nieuwe privacy-vriendelijke Wet op de inlichtingen- en veiligheidsdiensten (Wiv).
- Opsporingsinstanties mogen niet rondsnuffelen in computers zonder dat daar een zwaarwichtige, door de rechter getoetste reden voor is. Er komen strengere normen voor het aftappen van telefoons. Het communicatiegeheim wordt beschermd en gerespecteerd.
- Overheid gaat structureel investeren in softwareprojecten om de digitale infrastructuur beter te beveiligen.

Partij voor de Vrijheid (PVV) (programma)

- Extra geld voor bestrijding geavanceerde cybercrime en digitale dreiging buitenlandse mogendheden.
- Een "Cybercrime-offensief".
- Politie moet digitale vormen van criminaliteit serieuzer gaan aanpakken en de daders moeten voor de rechter komen.

Staatkundig Gereformeerde Partij (SGP) (programma)

- Ondernemers ondersteunen bij het werken aan meer cyberveiligheid.
- Versterken van inzet en capaciteit van het Digital Trust Centre.
- Overheid en bedrijfsleven maken afspraken over de cyberveiligheid van kritieke infrastructuur.
- Hogere veiligheidsstandaarden voor de kritieke delen van de digitale processen.
- Frequent en grootschalig testen van de beveiliging van de kritieke infrastructuur.
- Onderzoek naar digitale kwetsbaarheid van bevoorrading van supermarkten.

- Uitbreiden van aantal cyberreservisten bij Defensie.
- Meer budget voor het Defensie Cybercommando en de MIVD.
- Nationaal rapporteur voor internetcriminaliteit.
- Laagdrempelige voorzieningen voor burgers om internetcriminaliteit en internetpesten te beëindigen.
- Netneutraliteit mag internetfiltering niet onmogelijk maken.
- Overheid maakt afspraken met bedrijfsleven om kwetsbare groepen te beschermen tegen cybercrime.
- Meer politie- en recherchecapaciteit voor digitale vormen van fraude.
- Een bevel tot verwijderen van content of decryptie moet mogelijk worden.
- Investeringen in goede beveiliging en betere ICT-systemen bruggen, sluizen en spoorwissels.

Socialistische Partij (SP) (programma)

- Meer mensen en middelen voor de aanpak van digitale criminaliteit.

Volkspartij voor Vrijheid en Democratie (VVD) (programma)

- Investeringen in het Defensie Cybercommando en de inlichtingendiensten.
- Versterken van de Nationale Politie met extra cyberexperts.
- Meer vrijwilligers met cyberexpertise bij de Nationale Politie, Justitie, Defensie en de veiligheidsdiensten.
- Betere arbeidsvoorwaarden voor cyberexperts om bij Nationale Politie, Justitie, Defensie en de veiligheidsdiensten te werken.
- Versterking van samenwerking tussen overheid en bedrijfsleven om vitale infrastructuur te beschermen tegen cyberaanvallen.
- Overheid moet samen met de beheerders van de vitale infrastructuur de minimale beveiligingsstandaarden verhogen.
- Diensten zoals het Nationaal Cyber Security Centrum, het Defensie Cyber Security Centrum en de inlichtingendiensten versterken om de digitale slagkracht en weerbaarheid te vergroten.
- De overheid versterkt het toezicht op de digitale veiligheid van vitale bedrijven.
- Samen met NAVO-bondgenoten in het geval van cyberaanvallen "terughacken".

DENK (programma)

- In het verkiezingsprogramma van DENK wordt er niet over cybersecurity gesproken.

Conclusie

Nagenoeg alle partijen die in hun programma iets zeggen over cybersecurity willen dat er meer geld wordt uitgetrokken voor de bestrijding van cybercrime. Ook pleiten meerdere partijen voor het investeren in kennis over cybersecurity, zowel bij overheid als burgers. Een

ander terugkerend punt is de samenwerking tussen overheid en bedrijfsleven op het gebied van cybersecurity.

Het investeren in de inlichtingendiensten is ook in meerdere programma's terug te vinden. Toch zijn er ook verschillen als het om de diensten gaat. Zo wil het CDA de Wet op de inlichtingen- en veiligheidsdiensten aanpassen om de effectiviteit van de diensten te vergroten, terwijl het FvD de wet juist wil intrekken. Opvallende punten in de programma's zijn het decryptiebevel van de SGP en het 'samen terughacken' zoals de VVD voorstelt.

Opvallend is dat de aandacht voor preventie en digitale weerbaarheid vanuit de lokale overheid wat onderbelicht lijkt. Daar is uw rol als ‘oliemannetje/olievrouwtje cruciaal.