



Manifest Digiveiligheid

Nederland is een ICT land geworden. In ons onderwijs, in de culturele sector en in de economie maken miljoenen mensen dagelijks gebruik van de mogelijkheden die de vooruitgang op dit gebied heeft te bieden. Om de kansen die de digitalisering biedt optimaal te benutten kan de overheid beter presteren dan het nu doet. Zeker ook als het gaat om de veiligheid. Het is in ons nationale en internationaal belang om goed zorg te dragen voor de bescherming van internet als vitale infrastructuur. Om die taak beter uit te voeren hebben wij de volgende aanbevelingen ter verbetering van de 'digiveiligheid':

SP 

ICT & informatiebereikbaarheid

Internet bepaalt steeds meer de informatievoorziening in de wereld. Google wordt door 80 procent van de Nederlandse internetgebruikers gebruikt. Het aanbod van informatie wordt door het commerciële bedrijf Google gestuurd. De bereikbaarheid van onafhankelijke en kritische informatie op het net dient beter te worden gewaarborgd en daar kan de Nederlandse overheid een steentje aan bijdragen:

- Het is wenselijk dat Nederland steun geeft aan het project Quaero, een Europese zoekmachine.
- Nederland 1, 2 en 3 zijn gratis publieksvoorzieningen, dat hoort ook zo op het internet te zijn. Terugkijken en digitale zenders via internet van de publieke omroep moeten in alle gevallen gratis blijven. Internetsendingen moeten tot de kerntaken gaan behoren.

ICT & overheid

Een digitale overheid is belangrijk voor kostenbesparing, efficiëntie en verbetering van dienstverlening. De vele programma's voor een digitale overheid hebben niet kunnen voorkomen dat incidenten het nieuws overheersen. De overheid heeft te weinig kennis van zaken, te weinig gevoel van urgentie en laat met het slingeren van USB sticks zien dat ook bij de mensen zelf het besef van veilig automatiseren nog niet helemaal is doorgedrongen. Daardoor is het niet vreemd dat mensen wantrouwend staan tegenover initiatieven als DigiD en PIP. Er moet duidelijkheid komen over wie wat mag weten bij de overheidsdiensten en welke gegevens aan elkaar gekoppeld mogen worden.

- Daar waar digitaal met de burgers wordt gecommuniceerd moet er een excellente beveiliging zijn, verplichte encryptie en goede gedragslijnen.
- Er moet een bewustwordingsprogramma komen met een strategische aanpak van het wegwerken van kennisachterstanden over ICT bij de overheid, maar ook bij politie en justitie. Ook het management moet ervan doordrongen zijn dat leiding geven zonder basiskennis van ICT niet meer kan in deze tijd.
- Burgers moeten Persoonlijke Internet Pagina's kunnen weigeren. In dat geval moet ook de verzamelde informatie niet beschikbaar zijn in een toegankelijke database. Alternatieven zijn ook van belang in geval van uitval van de primaire systemen.
- Overheid en bedrijven zijn verplicht te melden wanneer privé-gegevens mogelijk gestolen kunnen zijn.

ICT & bedrijfsleven

De ambitie om een kenniseconomie te zijn verplicht ons een forse impuls te geven aan IT-ontwikkeling. Niet alleen voor grote bedrijven, vooral ook kleine ondernemers.

- Softwarepatentering is voor het MKB funest. Daarom moet er geen softwarepatentering komen.
- Daar waar mogelijk moet de overheid overgaan op Open Source en Open Standaard software.
- SIDN dient onder de Opta te vallen voor beter toezicht op uitgifte van domeinnamen
- Evalueer de effectiviteit van subsidies en financiering van ICT projecten. Werk aan een themagerichte aanpak met meer samenhang.

ICT & Criminaliteit

Criminaliteit met computers neemt steeds meer toe. De 'klassieke' criminaliteit digitaliseert deels, maar er ontstaan ook nieuwe vormen. Op internet is fraude, identiteitsdiefstal, hacking, spam, kinderporno-handel en illegaal uploaden aan de orde van de dag. Nederland is één van de landen die op het gebied van cybercrime in één adem genoemd wordt met Albanië en Rusland. Niet iets om trots op te zijn.

- In een High Tech Crime Center - liefst onder één dak - en met een gezamenlijke verantwoordelijkheid, regie en coördinatie moeten toezichthouders, politie, justitie, bedrijfsleven informatie uitwisselen en samenwerken bij de aanpak van hoogtechnologisch criminaliteit. Dit voorkomt overlap, een ieder voor zich mentaliteit en uitsluitend reactief handelen.
- Geef hogere prioriteit aan voor opsporing, vervolging en aanpak van kinderporno, ook in internationaal verband.
- Meer blauw op de digitale snelweg, met een proactief optreden.
- Één landelijk loket voor aangifte.
- Wijs gebruikers op de gevaren van Internet en hun verantwoordelijkheid voor het beveiligen van de computer. In het softwarepakket van een nieuwe computer behoort standaard een beveiligingsprogramma te zitten.

ICT & rechthebbers

Auteursrechten zijn door de komst van IT onder druk komen te staan. Het huidige systeem kraakt in zijn voegen. De roep om meer wetgeving is begrijpelijk maar niet wenselijk. Rechthebbers en hun organisaties zijn eerst aan zet om in te spelen op de nieuwe ontwikkelingen, ondersteund door de huidige wetgeving.

- Uploaden van auteursrechtelijk materiaal zonder toestemming van de maker is illegaal. Hier moet veel beter gehandhaafd worden door politie en justitie. Onwenselijk zijn de activiteiten van Brein die als particuliere organisatie recht probeert te halen omdat de overheid te laks is.
- Heffingen op geluids- en beeld dragers behoren in Europees verband te worden afgesproken. Onderzocht moet worden of het mogelijk is deze heffing te laten vervallen en om te zetten in een generieke heffing. In dat geval zou betalen op het net verleden tijd moeten zijn.

ICT & privé

Internetverslaving, webcamafpersingen, webcamsex, laster en digitaal pesten komen steeds vaker in het nieuws. De aanwezigheid van jeugd op het net geeft ook de overheid een speciale verantwoordelijkheid.

- Aangifte tegen laster moet mogelijk zijn en grond voor het uit de lucht halen van een site.
- Pesten is ook op internet onacceptabel. Besteed hier aandacht aan in het onderwijs, maar ook via de bureau's jeugdzorg.
- Wijs vooral jongeren via het onderwijs erop dat internet een levenslang geheugen heeft.
- Hulpverleningsdiensten als de kinderchat en SOS hulpdienst moeten ook in staat worden gesteld hun hulpverlening op het net 24 uur per dag live te kunnen onderhouden.
- Scholen en ouders moeten informatie en ondersteuning krijgen bij opvoedingsvragen rond het internet.
- Exploitanten en beheerders van digitale diensten dienen de privacy van internetgebruikers te respecteren. Voorafgaande aan het afsluiten van overeenkomsten met hun klanten of abonnees horen zij melding te maken van de wijze waarop de betreffende dienst gebruik maakt van hun persoonlijke en financiële gegevens en hoe die gegevens worden beschermd tegen misbruik.

