Verslag dialoog: Security

De digitalisering van onze samenleving gaat steeds verder en sneller. Maar hoe zorg je ervoor dat je met al dat digitaliseren de menselijke maat niet uit het oog verliest? Ook KPN staat, als ICT-speler en enige échte groene verbinder van en voor Nederland, midden in die samenleving. Voor verschillende maatschappelijke thema's, nemen we onze verantwoordelijkheid. Thema's die in het hart van ons bedrijf zitten en waarbij ICT een belangrijke driver is om Nederland, samen met anderen, écht verder kunnen brengen. Ieders mening, ervaring en expertise zijn voor ons bijzonder waardevol en leveren mooie inzichten op. Een goede dialoog met onze stakeholders is daarom essentieel.

Dit is het verslag van de dialoog rondom het thema Security

De samenleving digitaliseert waardoor we steeds meer zelfredzaam (moeten) worden. Dit stelt ons in staat om makkelijk en snel veel zaken online vanuit huis te regelen. Deze ontwikkeling brengt ook risico's met zich mee als het gaat om onze digitale veiligheid. Een veelbesproken onderwerp in de samenleving waar ook de media regelmatig over berichten. Het is lastig voor mensen om de ontwikkelingen bij te houden en in te schatten wat de gevaren zijn. Toch gaat die digitalisering door en alsmaar sneller. Wat zijn de belangrijkste risico's die mensen lopen en welke mogelijkheden kunnen we bedenken om hen digitaal weerbaar te maken?

Deelname van vertegenwoordiger van de volgende organisaties

HSD
Fox-IT
Cyberveilig Nederland
Deloitte
ABN AMRO
Northwave
Havenbedrijf Rotterdam

Vertegenwoordiging namens KPN

Jaya Baloo	-	KPN
Martijn Hakstege	-	KPN
Femke Wolthuis	-	moderator
Sjoerd Tiesma	-	KPN (notulist)

Go digital, stay human: computers nemen steeds meer menselijke beslissingen. Hoe human mogen zij worden? Mensen krijgen steeds meer technologie in hun leven. Van koelkast tot smart city. Dat zijn steeds meer attack factors, dus dat maakt kwetsbaar. De maand oktober staat in het teken van digitale bewustwording. Alert Online is een campagne van de overheid om burgers te vragen voorzichtig te zijn. Deze campagne loopt sinds 2012. Onderzoek wijst uit dat 50% wel eens een slechte ervaring heeft, zoals hacken, ransom, etc. Maar van die 50% neemt maar 50% maatregelen (beveiliging, wachtwoorden veranderen, etc). Er zijn twee richtingen om de burgers te leren beter met technologie om te laten gaan: awareness en behaviour.

De stelling: Awareness (alleen) werkt niet.

Een aanpak alleen gericht op awareness is onvoldoende. Awareness is zeker belangrijk op boardroom niveau, waar inzicht in risico's nodig is en die afgewogen moeten worden tegen de kosten van beveiliging. Als het gaat om menselijk gedrag, dan is een bredere aanpak gericht op gedragsverandering verstandig.

De jaarlijkse nationale Alert Online campagne slaagt er onvoldoende in om het bewustzijn bij een breder publiek te creëren. Het jaarlijkse onderzoek laat dit jaar zien dat het bewustzijn nauwelijks toeneemt. Ook niet nadat iemand slachtoffer werd van bijvoorbeeld cybercrime.

Een multidisciplinaire aanpak - bijvoorbeeld met inzet van psychologen in dit werkveld - ligt voor de hand. Een psycholoog weet veel over het gedrag van mensen. Zij kunnen organisaties inzicht geven hoe men het gedrag kan veranderen/beïnvloeden en hoe je mensen kunt leren veilig om te gaan met technologie. Awareness is een eerste stap in het proces, maar je moet toewerken naar een verandering in cultuur. En kun je dan het gewenste gedrag verwachten of moet je technologie inzetten om bepaald gedrag 'af te dwingen'?

Verwachten we niet teveel van de eindgebruiker?

Tegenwoordig hebben mensen al snel minstens 40 verschillende accounts met 40 verschillende wachtwoorden voor allerlei diensten die zij afnemen. Bovendien wordt snel doorgeklikt als het gaat over veiligheidsinformatie – zoals algemene voorwaarden - omdat men zo snel mogelijk gebruik wilt maken van het product of de dienst. Er is een onbalans ontstaan tussen individu en aanbieder. Teveel verantwoordelijkheid wordt bij de eindgebruiker gelegd. Een deel van deze verantwoordelijkheid moet helemaal niet bij de eindgebruiker liggen, maar bij de producent. Hoewel de adoptie van nieuwe technologieën langer duurt bij ouderen dan bij jongeren, gaan ouderen wel voorzichtiger om met de gevaren en voorwaarden die eraan verbonden zijn. De nieuwe generatie kijkt er nauwelijks of vaak helemaal niet naar om. Dit is ook een reden dat het bedrijfsleven een deel van deze verantwoordelijkheid moet dragen, omdat men er simpelweg niet mee om kan gaan.

Hoe werk je toe naar een verandering in de cultuur?

Elke generatie is nu - tot op zekere hoogte - verplicht om bepaalde technologie te omarmen. Alleen het adoptieproces is heel verschillend. Er is sprake van een generatiekloof. Ouderen hebben, in tegenstelling tot kinderen, veel meer moeite om nieuwe technologie te omarmen. De leercurve is simpelweg langer. Verschillende generaties moeten daarom op verschillende manieren worden benaderd.

Onderwijs

Om in de basis een verandering door te voeren in gedrag, is onderwijs essentieel. Veilig omgaan met technologie moet een vast onderdeel zijn van het curriculum; al vanaf de basisschool. Het is goed om naast de kansen ook de risico's te laten zien. Kinderen leren dan dat iets wat leuk is en bijvoorbeeld gratis, ook gevaren kent. Zoals het betalen met je persoonlijke gegevens. Digitalisering moet beter verweven worden in het volledige onderwijssysteem. Het moet een vast onderdeel worden van het basis, voortgezet en hoger beroepsonderwijs.

Bedrijfsleven

Ook bedrijven spelen een belangrijke rol in het leren veilig om te gaan met technologie. Bijvoorbeeld cursussen of basistrainingen voor medewerkers invoeren voordat er gebruik gemaakt mag worden van hardware en/of software. Bedrijven kunnen hand-in-hand met de overheid werken aan een veiligere technologische omgeving. Ook kunnen bedrijfsleven en overheid gezamenlijk beter optrekken in de strijd tegen cybercriminaliteit en -spionage. Er zou meer kennis over incidenten kunnen worden uitgewisseld zodat het de veiligheid van heel Nederland ten goede komen.

Tot slot

De technologische industrie heeft zelf een rol en verantwoordelijkheid als het gaat om het leveren van veilige hard- en software. Hard- en software zou aan minimale veiligheidseisen moeten voldoen voordat het mag worden verkocht. Het ontwikkelen van standaarden en keurmerken gaat daarbij helpen. En de overheid kan de mogelijkheden van wetgeving en softwareaansprakelijkheid verder uitwerken. Dit betreft overigens een internationale uitdaging, omdat veel hard- en software niet uit Nederland komt.