ECP Deelnemersspecial

Cyberweerbaarheid;
wat je moet weten, wat je moet doen

Op donderdag 30 mei organiseerde ECP in samenwerking met het ministerie van Economische Zaken en Klimaat en de Online Trust Coalitie de ECP Deelnemersspecial 'Cyberweerbaarheid; wat je moet weten, wat je moet doen' in Nieuwspoort, Den Haag.

Welkom en introductie

Arie van Bellen heet namens ECP de aanwezigen welkom. Cyberveiligheid is een bouwwerk, met tal van afspraken, beleid, politiek, technici en experts. ECP host met trots een aantal samenwerkingsverbanden die aan onze cyberweerbaarheid werken, waaronder de Online Trust Coalitie.

Dagvoorzitter Kees Verhoeven -- Kernteamlid Online Trust Coalitie -- schetst de opbouw van de middag: we gaan van cybersecurity mondiaal, naar Europa (wetgeving), Nederland (rol van de Tweede Kamer en bewindspersonen), naar de vraag hoe verantwoordelijken in organisaties sturing aan cyberweerbaarheid kunnen geven en daarmee voldoen aan de komende wetgeving in het digitale domein.

Cyberweerbaarheid: internationaal perspectief

Jochem de Groot -- Oprichter Humanative - gaat in op de omvang en aard van de cybersecurity dreiging en op de tegenmaatregelen.

Cyberweerbaarheid is belangrijker dan ooit: vorige week, half mei, werd door intensieve samenwerking van 14 diensten over de hele wereld het grootste ransomwarenetwerk ooit opgerold. Nederland speelde niet alleen een belangrijke rol bij het oprollen, maar was ook een belangrijke criminele speler: 33 servers stonden in Nederland. Bovendien kwamen recent twee grote hacks in het nieuws, bij Christies en Ticketmaster, waarbij de gegevens van miljoenen klanten zijn buitgemaakt. Tenslotte staan we aan de vooravond van een nieuw kabinet, waarbij de kandidaat-premier de hoogste verantwoordelijke voor cyberveiligheid in Nederland was.

De economische schade door cyberaanvallen en daarmee het belang van cyberweerbaarheid loopt in de vele miljarden. Bij het versterken van cyberweerbaarheid is het belangrijk onderscheid te maken tussen de doelen van verschillende actoren in dit domein: niet alleen criminelen, maar ook natiestaten (nationale belangen) en hacktivisten (om allerlei ideële doelstellingen te bereiken) bedreigen cyberveiligheid. Niet alleen geldelijk gewin maar ook beïnvloeding en ontwrichting van samenlevingen of regelrechte offensieve militaire doeleinden kunnen een motief vormen. Nederland speelt met de VS een belangrijke rol op al deze vlakken: we zijn digitaal sterk verbonden en daarmee kwetsbaar, maar hebben ook een goede informatiepositie en kennis rond weerbaarheid. En criminelen maken graag gebruik van onze betrouwbare en snelle verbindingen.

De rol en mogelijke impact van AI (deepfakes, desinformatie) groeit snel en dat geeft het vraagstuk cyberweerbaarheid een heel nieuwe dimensie.

Globale dynamiek rond cybersecurity

Een raamwerk om de dynamiek te duiden biedt "Digital empires: the global battle to regulate technology" van Prof. Anu Bradford -- zij schetst hoe er drie globale machtsblokken zijn ontstaan, die proberen landen in hun model te trekken: de VS - vrije markt, EU - waarden en China - staatsgedreven. De EU markt is groot en welvarend waardoor Europese wetten druk uitoefenen op de andere blokken om aan die wetten te voldoen.

De rol van techpartijen in cyberweerbaarheid is veranderd: denk aan de recente rol van Microsoft, AWS en Google bij het beschermen van de digitale infrastructuur in de Oekraïne tegen aanvallen uit Rusland. Lokke Moerel bepleitte naar aanleiding daarvan dat het niveau van cyberweerbaarheid niet door commerciële dienstverleners zou moeten worden bepaald, maar dat dat niveau de basis zou moet vormen voor cyberweerbaarheid van de hele samenleving.

Europese wetgeving in het digitale domein

Arnoud Engelfriet -- Chief Knowledge Officer ICTRecht --constateert dat er 112 wetten gerelateerd aan het digitale domein op ons af komen. Het is een actieve poging van Europa om de samenleving te herijken: Europese kernwaarden te verankeren in het digitale domein. Wat hebben we nodig om waardig en inclusief te zijn.

Europa neemt een decennium de tijd voor de transitie die is gestart in 2021 met The Digital Decade policy programme 2030. Er zijn acht thema's te onderscheiden in de 112 wetten die op ons afkomen dit decennium:

1. **Mensgericht en inclusief:** de wetgeving gaat om zaken die fundamenteel zijn voor onze samenleving: dat inwoners zonder controle van bovenaf of vooraf door overheid of bedrijfsleven, kunnen kiezen. De wetten willen voorkomen dat de economische waarde van (de data van) een persoon bepaalt welke informatie en mogelijkheden iemand krijgt. De wetgeving geeft inwoners van Europa de mogelijkheid de rechten die de wet hen geeft te claimen, door leveranciers financieel aansprakelijk kunnen stellen rond deze thema's.
2. **E-Identiteit**: de wetten rond e-identiteit voorkomen dat bedrijven (en overheden) bepalen wie (rechtsgeldig) kan handelen in het Europese digitale domein. Wetgeving rond digitale bezittingen voorkomen dat bedrijven bepalen wat een digitaal eigendom is en wat de waarde daarvan is. Er worden eisen gesteld aan de vertrouwelijkheid van digitale communicatie door wetten over digitale encryptie.
3. **Inhoud en expressie.** De wetten gaan over moderatie, politieke advertenties, illegale inhoud en pluriformiteit. Doel is dat beeldvorming voor inwoners in de EU zone niet gedomineerd gaat worden door specifieke politieke en economische belangen.
4. **Infrastructuur en toegang**: zijn wetten die gaan over onze netwerken en digitale infrastructuur. Doel is brede toegankelijkheid tot de netwerken en netneutraliteit: dat overheden en bedrijven controle hebben over de informatie.

5. **Digitale economie en markten**: een deel van de wetten gaat over digitale marktwerking, zakelijke transparantie, digitale handel en content. Duurzaamheid is een belangrijk onderwerp van deze wetten.
6. **Data en privacy**: veiligheid en beschikbaarheid van data is een belangrijk thema. Het gaat over vrij verkeer van data (wat mag de EU uit), eigenaarschap en toegang tot data (apparaten die autonoom gaan beslissen, biometrie). Deze wetten hebben sterke overlap met privacy.
7. **Cybersecurity en weerbaarheid**: weerbaarheid is onderwerp van een aantal meer sectorspecifieke wetten (NIS2, CRA) en meer generieke zoals de Cybersecurity Act en digitale weerbaarheid (denk aan DORA, Cyber Solidarity Act, CER directive).
8. **Digitale soevereiniteit**: een aantal wetten hebben invloed op soevereiniteit van de Europese economie: over grip op digitale hardware (chips), grip op big tech in de AI ACT, DSA, DMA, grip data via Data Act en GDPR.

Arnout benadrukt dat een wet een grof instrument is: het heeft last van "bijwerkingen". Iedere wet heeft immers een eigen kader met eigen doelen, begrippen en procedures, met eigen toezichthouders. Inconsistentie en overlap is bijna inherent aan wetgeving. Iedere wet probeert zelf een wiel uit te vinden, dat andere misschien wetten geheel of ten dele ook al hebben uitgevonden.

De 112 wetten die betrekking hebben op het digitale domein leiden ongetwijfeld aan die bijwerkingen. De Europese Commissie heeft geprobeerd om dat te ondervangen door iedere wet te voorzien van een kader: het doel dat de wet probeert te bereiken.

Strategic compliance

Organisaties kunnen daarmee "strategic compliance" nastreven: ze kunnen misschien niet aan de letter van al die wetten voldoen, maar wel aantonen dat ze in control zijn en bijdragen aan de doelstellingen van die wetten. Veel van de wetten vragen bedrijven te doen, wat ze toch al willen of zouden moeten doen: zorg dragen voor eigen continuïteit, informatieveiligheid, cybersecurity, privacy en controle over die processen. Omdat we op die thema's behoorlijk achter zijn gaan lopen, zullen de wetten voor veel organisaties een inhaalslag betekenen.

Overhandiging wetgevingsoverzicht

Tom Vreeburg, lid van het Kernteam van de Online Trust Coalitie overhandigt het wetgevingsoverzicht dat ICTRecht in opdracht van de OTC heeft ontwikkeld aan Roman Volf, die vanuit het Ministerie van Economische Zaken en Klimaat mede aan de wieg heeft gestaan van de OTC. Het overzicht gaat in op 19 Europese wetten, die grote impact hebben op het digitale domein. Het biedt de stand van zaken, het soort wet, de doelgroep, de impact, het toezicht en geeft raakvlakken aan met andere reguleringen. De komende tijd zal de OTC met ICTRecht maandelijks het overzicht bijwerken, vanwege de snelle ontwikkelingen.

Roman benadrukt hoe welkom zo'n overzicht is, voor het ministerie en voor alle partijen die zich voor willen bereiden op de komst van de wetten of anderen daarbij adviseren.

Samenwerking tussen politiek en bedrijfsleven rond ICT

Bestuurders en Cyberweerbaarheid

De tweede helft van de middag gaat in op de vraag wat bestuurders en bedrijven moeten doen om te anticiperen op de golf aan wetgeving in het digitale domein. *Rudrani Djwalapersad* - Partner EY en *Michiel Steltman* - Kernteamlid Online Trust Coalitie betogen dat door de komende wetgeving veiligheid en continuïteit van de informatievoorziening op dezelfde manier gaat worden behandeld als de financiële gezondheid. Bij de verantwoording over de gezondheid van een organisatie moeten bestuurders niet alleen een jaarrekening en een balans kunnen lezen, maar ook weten waar het bedrijf staat wat de veiligheid en continuïteit en wendbaarheid van de informatievoorziening betreft.

De instrumenten voor bestuurders om verantwoording af te leggen over het financiële domein zijn vanzelfsprekend en bestuurders hebben de kennis om daarvoor verantwoordelijkheid te nemen. In het digitale domein zijn deze instrumenten in ontwikkeling en veel bestuurders moeten bijscholen: de NOREA werkt al een aantal jaar met tal van bedrijven en een brede groep accountantsorganisaties aan het NOREA Reporting Initiative. Daar zijn succesvolle pilots mee afgerond. Het NRI helpt bestuurders om sturing te geven aan informatievoorziening.

Holistisch Framework Wetgeving

Rudrani werkt met auditors van andere kantoren en experts binnen de OTC aan een gedeelde interpretatie van de wetten die op ons afkomen: het holistisch data framework. De werkgroep is ervan overtuigd dat er een groot belang zit aan die samenwerking: bedrijven kunnen niet meer aan iedere letter van de wetten kunnen voldoen. Het is van groot maatschappelijk belang dat auditors en toezichthouders binnen en buiten de organisatie en bestuurders en andere belanghebbenden een zelfde definitie hanteren van begrippen. Daarmee wordt de doelmatigheid van maatregelen versterkt en kunnen bedrijven desinvesteringen voorkomen. Auditors kunnen zich richten op waar het echt om gaat in plaats van veel tijd kwijt te raken aan interpretatie van regelgeving: het implementeren van maatregelen.

Compliant zijn betekent voor een bedrijf niet primair een boete voorkomen, maar een aantoonbaar veilig en vitaal bedrijf worden: dat de ICT gerelateerde risico's beheerst, en daardoor scherp aan de wind kan varen bij innovatie en het versterken van de concurrentiepositie. Het voorkomt dat bij kleine veranderingen in de strategie of bij het grijpen van kansen kostbare tijd en geld verloren gaat aan het ad-hoc compliant maken van de wijzigingen. De werkgroep wil met het holistisch data framework bedrijven een handreiking bieden om deze stappen te zetten.

Vijf Stappen voor Cyberweerbaarheid

Michiel Steltman gaat in op de vijf stappen die een organisatie moet zetten:

1. **Kennis van zaken** - een bestuurder moet zorgen voor elementaire basiskennis, zodat deze de taal spreekt van de mensen aan wie wordt gedelegeerd. Welke KPI's geef je mee aan je CIO, hoe stuur je bij, evalueer je risico's, informeer je je over cyberweerbaarheid.
2. **Richt uniforme ''digital control'' in**: zoals bestuurders controle houden over hun financiën, zullen ze dat ook voor cyberveiligheid moeten doen. De CIO krijgt taakstellingen evenals de organisatieonderdelen, er worden budgetten toegewezen, er is een systeem dat controle en uitvoering faciliteert, de organisatieonderdelen en de leveranciers van cloud en ICT diensten rapporteren over weerbaarheid.
3. **Doe een grondige risico inventarisatie**: wat zijn de risico's die de strategische doelen en continuïteit van de organisatie bedreigen? De organisatie zelf en de partijen en mensen die afhankelijk zijn van de organisatie, moeten worden beschermd.
4. **Maatregelen nemen** om incidenten te voorkomen en de impact te verminderen.
5. **Laat dit geheel periodiek (jaarlijks) beoordelen**: klopt het wat je doet, is het effectief? Zorg voor heldere rapportages door de interne toezichthouders, maar ook door onafhankelijke derden te betrekken. Zorg dat de rapportages en de onderzoeken daarvoor zoveel mogelijk plaatsvinden volgens breed geaccepteerde standaarden: voorkom dat je je eigen vragen en lijstjes moet verzinnen. Dat maakt dat onderzoeken herbruikbaar zijn voor verschillende doeleinden en rapportages geschikt zijn voor intern, maar ook voor klanten, afnemers, toezichthouders.