Inbreng KPN Rondetafelgesprek Digitale Weerbaarheid

6 september 2022

KPN is een toonaangevende leverancier van telecommunicatie en IT diensten en marktleider in Nederland. Met onze vaste en mobiele netwerken voor telefonie, data en televisie bedienen we klanten in binnen- en buitenland. KPN richt zich op zowel particuliere klanten als zakelijke gebruikers, van klein tot groot. Wij zetten alles op alles om iedereen in Nederland te verbinden met een duurzame toekomst. Met passie werken we aan veilige, betrouwbare en toekomstbestendige netwerken en diensten, zodat mensen en apparaten altijd en overal met elkaar verbonden kunnen zijn.

Digitale weerbaarheid is een fundamentele voorwaarde om in business te blijven in een samenleving met voortdurende cyberaanvallen. We delen daarom graag een aantal inzichten en onze visie op cybersecurity met de Tweede Kamer.

Chefsache

We leven in een wereld waarin digitale dreigingen aan de orde van de dag zijn en alleen maar toenemen. Bij KPN is security daarom *chefsache*. Dit betekent dat security op alle niveaus van ons bedrijf verankerd is. ‘Security first’ heet dat bij ons. Dit komt onder andere tot uiting in het feit dat Security een standaard onderdeel is van onze innovatie trajecten (Security-by-design). Verder besteedt het inwerkprogramma van nieuwe medewerkers hier veel aandacht aan.

Cybersecurity van fundamenteel belang voor de organisatie

Om maximale veiligheid te kunnen bieden, hanteert KPN een Cybersecurity Framework (NIST). NIST onderscheidt vijf hoofdfuncties: identify, detect, protect, respond en recover. Dit gaat verder dan de omgang met incidenten. Het draagt immers bij aan de weerbaarheid van de gehele organisatie.

- **Identify** betreft het overzicht houden op alle productiemiddelen die nodig zijn voor onze dienstverlening en voor onze interne automatisering. Denk aan netwerken, systemen, applicaties, databases en technische gebouwen.
- **Protect** krijgt vorm door risicoanalyses te doen op al onze productiemiddelen en maatregelen te nemen om de risico’s terug te brengen.
- **Detect** omvat het monitoren van onze bedrijfsmiddelen in ons Security Operations Center op security incidenten, het uitvoeren van technische testen (pentesten) op onze bedrijfsmiddelen en het oplossen van de kwetsbaarheden die daarbij worden gevonden.
- **Respond** Zodra er sprake is van een incident of bedreiging komt ons Computer Emergency Response Team (CERT) in actie. Het CERT staat 24 uur per dag klaar. Bij een melding van een hack of systeemzwakte, maken de CERT-experts een aanval snel onschadelijk door gaten in de beveiliging te dichten. Ook onderzoekt CERT hoe hackers zijn binnengekomen. KPN CERT werkt nationaal en internationaal intensief samen met een groot aantal CERT-teams van andere bedrijven en overheden.
- **Recover** betreft het nemen van correctieve maatregelen na een incident, problem en change management, maar ook in de update van onze security policy vanuit incidenten of wet- en regelgeving vanuit de overheid.

Samenwerking tijdens een cyberincident
KPN hecht groot belang aan de continuïteit van dienstverlening. Samenwerking is in dat kader cruciaal. Dit betreft niet enkel de samenwerking met de overheid, maar ook de samenwerking tussen bedrijven onderling. KPN voelt hiervoor een verantwoordelijkheid.

Vindt er een cyberincident plaats dat meerdere partijen raakt, dan maken we gebruik van diverse afspraken over samenwerking en aansluiting op de crisisstructuur van de overheid. Hierbij zijn het Departementaal Crisiscentrum (DCC) van het ministerie van EZK, het Nationaal Crisiscentrum en de Veiligheidsregio betrokken.

Daarnaast speelt het Nationaal Cyber Security Center (NCSC) een centrale rol in het verzamelen van cyber security dreigingen en het informeren van vitale sectoren over dreigingsinformatie (threat intel). Ook informeert en adviseert het NCSC andere centrale partijen en branche organisaties. Iedere partij zal met deze informatie de eigen cybersecurity risico's moeten aanpakken. De Nationaal Coördinator Terrorismebestrijding en Veiligheid onderhoudt daarnaast het Nationaal Crisis Plan Digitaal en daarbij wordt de Commissie Vitaal waar de vitale sectoren in deelnemen (waaronder KPN) betrokken.

Om de samenwerking tussen bedrijven te bevorderen is KPN onderdeel van de Circle of Trust. Met deze groep vooraanstaande bedrijven in Nederland delen we inzichten, ervaringen en geïdentificeerde cyberdreigingen. Uiteraard wordt deze informatie ook weer met het NCSC gedeeld.

Tot slot concretiseert KPN het belang van samenwerking door actief te participeren in een aantal samenwerkingsverbanden en door nieuwe proposities te ontwikkelen. Denk aan de samenwerking met de Anti-DDoss-coalitie en de het Anti Abuse netwerk die bijdragen aan een veiliger internet. Met Elastic Interconnect hebben KPN en NL-IX een propositie ontwikkeld waarmee end-to-end veiligheid voor organisaties wordt gecreëerd.

Het belang van oefenen
Nederland is weerbaarder wanneer er adequaat wordt gehandeld tijdens een grote crisis. Deze crisis kan ontstaan door een hack of storing die bijvoorbeeld de overheid of vitale infrastructuren raakt. De evaluatie van de grootschalige publiek-private oefening Isidoor III laat zien dat regelmatig oefenen om grote crises het hoofd te bieden van groot belang is.

Het is van belang dat overheden zoals het NCSC, NCTV, opsporingsorganisaties, ministeries e.d. oefenen op crises. Niet alleen met zichzelf en elkaar, maar juist ook met niet-overheidsorganisaties, in het bijzonder vitale sectoren zoals banken, telecom, water en energie. Het is daarom van groot belang dat er voortdurend en in wisselende samenstellingen wordt geoefend in groot en klein verband.

Voortvarendheid in Europese wetgeving op het gebied van hard- en software
De Europese RED (Radio Equipment Directive) en CRA (Cyber Resilience Act) regelgeving zijn in ontwikkeling. Deze gaan helpen om security eisen op te leggen, snel verbeteringen door te voeren en aansprakelijkheid bij nalatigheid toe te passen bij software en hardware leveranciers. Wat we als organisatie inkopen moet veilig zijn, maar daar zijn nu nog te weinig wettelijke waarborgen voor. We verwachten een positieve bijdrage aan veilige hard- software als gevolg van de invoering van voorgenoemde wetgeving. Het is daarom van belang dat dit wetgevingsproces voortvarend en zorgvuldig verloopt. Uiteraard leveren wij graag een actieve bijdrage aan dit proces.