OPINIERUBRIEK OVER DE IDEALE ENERGIEVOORZIENING. FEEDBACK EN REACTIES ZIJN WELKOM OP TWITTER: @netbeheerNL

tekst: Margot Derksen

‘De virtuele **voordeur** van de energiesector moet beter op slot”

PROF.DR. ROB DE WIJK
OPRICHTER EN NON-EXECUTIVE DIRECTEUR VAN HET DEN HAAG CENTRUM VOOR STRATEGISCHE STUDIES (HCCS)



Rob de Wijk geniet ook bekendheid als professor Internationale Betrekkingen aan de Universiteit van Leiden, voorzitter van de Denktank Nationale Veiligheid en schrijver van een wekelijkse een column in Trouw.

‘Een hoogspanningsmast opblazen is effectiever”

Het internet was eigenlijk helemaal niet bedoeld voor het aansturen van apparaten. *The Internet of Things*, waarbij niet alleen mensen maar ook dingen (systemen/apparaten) met elkaar verbonden zijn en data genereren, maakt het ook allemaal een stuk complexer. Hoe meer apparaten je aan het internet hangt, hoe groter en hoe kwetsbaarder het systeem wordt. Daardoor nemen de veiligheidsrisico’s toe. Dat speelt ook bij energiesystemen.
In Nederland is de urgentie nog steeds vrij laag om bepaalde vitale sectoren beter te beveiligen. Media, burgers en overheid hebben er relatief weinig aandacht voor, maar je ziet wél een toenemende angst voor inbreuk op hun privacy door de digitalisering. Hoewel iedereen vrijwillig privé-gegevens op social media plaatst, ontstaat er wantrouwen jegens de overheid en bedrijven: wat doen zij met al mijn persoonlijke gegevens? Ik denk dit een sociaal-maatschappelijk probleem betreft. Het gaat om vertrouwen in de overheid, in bedrijven, in autoriteiten.

Natuurlijk moet je de systemen optimaal beveiligen. Daar doen organisaties zoals the European Network for Cyber Security (ENCS) hun best voor. Maar honderd procent veiligheid bestaat niet, nergens. Er is altijd een reële kans dat ingebroken wordt op systemen. Daar moet je gewoon rekening mee houden. *It’s all in the game*. In de Verenigde Staten werden in 2014 rond de tachtig cyberincidenten op het energienet geteld. In Nederland zijn de cijfers volgens mij niet openbaar, maar hier zijn natuurlijk ook incidenten.

Cyberaanvallen op cruciale energie-infrastructuur komen relatief weinig voor en het effect van de aanvallen is eerlijk gezegd gering. Het is lastig om het energienet via een cyberaanval helemaal plat te leggen, daarvoor is de infrastructuur te complex. Als je echt grote schade wilt veroorzaken, dan kun je beter zoeken naar andere zwakheden. Blaas iets op in het net, zoals een hoogspanningsmast of een elektriciteitshuisje. Dat is effectiever en het duurt langer voor de schade is hersteld. Ook is het spectaculairder en zichtbaarder, waardoor de daders makkelijker de verantwoordelijkheid voor hun daad kunnen claimen. Een cyberaanval op het energienet kan door iedereen worden opgeëist.

Het echte probleem van de digitalisering is naar mijn mening niet de vergrote kans op cyberaanvallen, maar het toenemende wantrouwen jegens de overheid en grote instanties. De wereld wordt complexer, mensen begrijpen er minder van en daardoor groeit de angst voor Big Brother.

DESINTERESSE BEMOEILIJKT FINANCIERING

We hebben afgelopen maart gezien wat er gebeurt als de stroomvoorziening plat ligt. Dan is het hele maatschappelijke leven ontwricht. Door de digitalisering van het net ontstaan nieuwe gevaren. De beveiliging van de stroomvoorziening tegen de gevaren van cyberaanvallen moet meer aandacht krijgen. Het publiek en de overheid nemen de gevaren van cybercriminaliteit nog niet heel erg serieus. Dat komt wellicht omdat we onvoldoende bekend zijn met het aantal cyberaanvallen; gedupeerde bedrijven zijn niet echt happig om ermee naar buiten te treden vanwege de negatieve publiciteit. Maar er zijn wel degelijk incidenten. Energiebedrijven realiseren zich heel goed dat er iets moet gebeuren. Maar mede door de beperkte interesse van de overheid en burgers is de financiering van de cybersecurity van de energievoorziening nog een probleem. Ik denk dat een opslag op de huidige stroomprijs de oplossing kan zijn om de voordeur en de meest opzichtige achterdeur beter te beveiligen. De kosten daarvan zijn voor Europa als geheel jaarlijks ongeveer drie miljard euro. Voor een Nederlands huishouden betekent dat een bijdrage van ongeveer drie euro per jaar.

‘Leg een opslag op de stroomprijs om cybersecurity te bekostigen’

JAAP SCHEKKERMAN
DIRECTEUR GLOBAL CYBER SECURITY CGI



SAMEN OPTREKKEN MET ANDERE VITALE SECTOREN

Samenwerking tussen vitale sectoren bij het voorkomen van en voorbereiden op incidenten is belangrijk. De kwetsbaarheden zitten vaak in de afhankelijkheden tussen sectoren. Bovendien kunnen sectoren van elkaar leren hoe je de beveiliging kunt verbeteren. Wij zijn vooral gericht op ondersteuning van netbeheerders. De opkomst van slimme meters en smart grids maakt elektriciteitsnetten kwetsbaarder voor aanvallen op afstand. Door de koppeling van digitale netwerken aan elektriciteitsnetwerken worden meters en onderstations ook digitaal toegankelijk. Hackers zoeken naar een slecht bewaakte ingang. Het is dus zaak om ze goed af te sluiten en te bewaken. Het gaat erom maatregelen te nemen die de risico’s acceptabel maken. Bij het inschatten van risico’s weegt vooral de mogelijke impact van aanvallen zwaar. We weten niet precies wat de kans is op een cyberaanval in de toekomst, maar de schade van sabotage aan het elektriciteitsnetwerk kan enorm zijn. Aan de andere kant hoeven cybersecurity-maatregelen niet kostbaar te zijn, als je ze op tijd neemt. In de energiesector worden nu grote investeringen gedaan om te digitaliseren. Het is dus het juiste moment om de beveiliging aan te pakken.

‘Dit is het juiste moment om de beveiliging aan te pakken’

MAARTEN HOEVE
TECHNICAL TEAM MANAGER EUROPEAN NETWORK FOR CYBER SECURITY (ENCS)

