Ir. Max Kerkers
is manager bij KPMG Cyber & Privacy.

Drs. Pieter de Meijer RE CISSP CISA
is director bij KPMG Cyber & Privacy.

Ir. Ronald Heil
is partner bij KPMG Cyber & Privacy.

Beveiliging van Smart Grids: een onder-geschoven kindje

Met het oog op een groene toekomst hebben energienetwerken slimme oplossingen nodig om vraag en antwoord op elkaar te kunnen afstemmen. Deze Smart Grids bieden fantastische mogelijkheden, maar voorwaarde is wel dat de cyberveiligheidsrisico's ervan voldoende aandacht krijgen. En dat is nu niet altijd het geval. Overheden, netbeheerders, energieproducenten en alle andere betrokkenen moeten daarmee nog meer aan de slag. De technische beveiliging krijgt reeds de nodige aandacht, maar daarmee zijn we er nog niet. In dit artikel gaan we in op de mogelijke oplossingen om cyberrisico's te beperken en schade te voorkomen als een incident zich voordoet.

INLEIDING

De energietransitie vraagt bijzonder veel van het Nederlandse elektriciteitsnetwerk. De toenemende elektrificatie eist steeds meer capaciteit en er moeten (veel) meer aansluitingen komen: voor zonnepanelen, windmolens en allerlei andere lokale energie-initiatieven. Een traditionele aanpak van deze uitdaging – bijvoorbeeld het netwerk blijven uitbreiden – wordt praktisch onbetaalbaar en daarom zijn Smart Grids een goed idee. Dat zijn technologische oplossingen die helpen de vraag naar energie te laten meebewegen met het aanbod, waardoor de extra druk op het netwerk beperkt blijft. Met Smart Grids is het dus mogelijk onze samenleving te vergroenen in het tempo dat ons voor ogen staat.

Een van de belangrijke randvoorwaarden voor een succesvolle implementatie van Smart Grids is dat deze ook goed beveiligd zijn. Het goede nieuws in dit verband is dat netbeheerders vaak (deels) nog in de ontwerpfase zitten van deze slimme netwerken. Gelegenheid genoeg dus om de context te creëren die nodig is om Smart Grids ook veilig te laten functioneren.

Maar helaas is er ook minder goed nieuws: van de mogelijkheden om een goed fundament te leggen voor (cyber)veilige Smart Grids wordt nu maar nauwelijks gebruikgemaakt. In dat fundament moeten risico's worden geïdentificeerd en moeten effectieve maatregelen worden genomen. Daarbij dienen we uit te gaan van de situatie dat het toch misgaat en dat erover nagedacht is hoe de schade zo beperkt mogelijk gehouden kan worden. Dat fundament kan enkel werken zolang het inzicht aanwezig is wie de op Smart Grids aangesloten partijen zijn en zolang kan worden gestuurd op het gezamenlijk beveiligen van Smart Grids.

> Hackers, al dan niet in dienst van vijandige staten of criminele organisaties, maken in toenemende mate de digitale wereld onveilig

Dat dit fundament nog beperkt wordt gelegd, komt mede doordat de beveiliging niet enkel de verantwoordelijkheid is van de netbeheerders: zij hebben aan de gebruikende kant slechts beperkt grip op de mate van beveiliging. Denk aan elektrische auto's met de bijbehorende laadpalen. Of industrieterreinen met eigen energieopwekcapaciteit via zonnepanelen en windturbines. Daarnaast doemen vragen op rondom de stijgende interconnectiviteit en de mogelijkheden voor kwaadwillenden om hier gebruik van te maken. En wat moet er gebeuren om te voorkomen dat deze slimme netwerken straks toch niet zo slim blijken te zijn?

De oplossingen zijn voorhanden, maar alhoewel de oplossingen in de energietransitie meer en meer op de agenda komen, is de complexiteit van het digitaliseren van een bestaand (fysiek) netwerk in een bestaand ecosysteem enorm. In die complexiteit dienen cyberrisico's serieus genomen te worden en structureel te worden aangepakt. Dat vergt politieke wil en sturing gecombineerd met samenwerking in de keten tussen private en publieke partijen.

In dit artikel gaan we in op deze oplossingen om cyberrisico's te identificeren, om ze te voorkomen en om de schade te beperken, mocht zich toch een cyberincident voordoen.

CYBERRISICO'S ZIJN EEN REËLE DREIGING

Dat cyberrisico's niet denkbeeldig zijn, is intussen wel gebleken. De Russische aanvallen op Oekraïense energienetwerken voordat de oorlog in Oekraïne uitbrak, maar zeker ook gedurende de oorlog in 2022 en 2023, en de voortdurende agressie richting (grote) bedrijven met ransomware zijn maar twee voorbeelden. Hackers, al dan niet in dienst van vijandige staten of criminele organisaties, maken in toenemende mate de digitale wereld onveilig. Als het gaat om energienetwerken, kan dat op verschillende fronten nare gevolgen hebben. Hieronder worden vijf fronten als dwarsdoorsnede beschreven.

1. Een black-out. Delen van de samenleving komen zonder stroom, warmte of andere energievorm te zitten. Het effect kan ontwrichting zijn.
2. Fysieke gevolgschade. Delen van de infrastructuur kunnen worden vernietigd of men verstoort doelgericht de energielevering op vitale plaatsen, bijvoorbeeld ziekenhuizen. Dit kan leiden tot doden of gewonden.
3. Technische verstoringen. Meer op de techniek gerichte verstoringen zoals het verschuiven van netfrequenties, waardoor digitale klokken niet meer gelijklopen. Met name oudere apparaten gaan daardoor stuk en dat kan leiden tot (hoge) kosten, inefficiënties, oponthoud en ander ongemak.

4. Financiële schade. Verminderde beschikbaarheid van energie, zoals door black-outs en verstoringen, kunnen leiden tot hogere energieprijzen. Huishoudens houden daardoor minder geld over om aan andere zaken uit te geven en kunnen hierdoor in de financiële problemen komen. Zeker in het licht van de huidige geopolitieke situatie is dit niet ondenkbaar.
5. Privacyschendingen. Omdat Smart Grids zeer fijnmazig zijn, met meerdere aansluitingen tot in de woonomgeving van consumenten, kan de via die netwerken uitgewisselde informatie privacygevoelig zijn. Bijvoorbeeld het feit of bewoners thuis zijn of niet, kan tot schade (inbraak) leiden.

Enkele kenmerken van Smart Grids maken dit type netwerk bovendien nog gevoeliger voor cyberrisico's dan andere netwerken. Het gaat met name om de genoemde fijnmazigheid. Het aantal contactpunten neemt toe, net zoals het aantal verbindingen en de omvang van de interactie tussen al die onderdelen: het zogeheten aanvalsoppervlak wordt al met al een stuk groter. Het identificeren van relevante dreigingen, maar zeker ook van de kwetsbaarheden in de eigen organisatie en infrastructuur, moet dan ook onderdeel zijn van de implementatie van Smart Grids.

De vraag hoe die kwetsbaarheden te beheersen, te verminderen dan wel uit te sluiten zijn, moet al bij het ontwerp van Smart Grids een focuspunt zijn. Preventieve maatregelen zullen centraal staan, aangevuld met de juiste maatregelen om bedreigingen te detecteren en acties die de schade van aanvallen kunnen beperken.

PREVENTIEVE MAATREGELEN OM DE KANS OP EEN CYBERINCIDENT TE VERKLEINEN

Qua preventie is de belangrijkste oplossing het voorzien in veilige standaarden voor het opzetten van Smart Grids. Dergelijke standaarden ontbreken nu. Bijna elke partij kiest voor een andere benadering van de beveiliging en dat levert reeksen kwetsbaarheden op. Wij pleiten voor samenwerking tussen de grote marktpartijen – gestimuleerd door de overheid – om zo'n veilige standaard te ontwikkelen. Vervolgens zou die verplicht moeten worden toegepast door de hele industrie.

Van belang daarbij is dat het gaat om een 'ecosysteem' van stakeholders in de energieketen. De standaarden dienen niet enkel voor de netbeheerders van toepassing te zijn; de complexiteit in dit speelveld is te groot en het beveiligingsvraagstuk wordt niet opgelost door enkel meer van de netbeheerders te verlangen. Daar komt nog eens bij dat de afgelopen jaren duidelijk is geworden dat de energietransitie flinke financiële investeringen heeft gevergd en zal blijven vergen van de netbeheerders. Het wordt tijd dat de beveiligingslast door meer schouders wordt gedragen.

In aansluiting hierop is een grotere sturende rol van de overheid een tweede belangrijke oplossing voor de cyberrisico's van Smart Grids. De huidige Europese richtlijn (de NIS Directive) voor de beveiliging van kritieke infrastructuur is in Nederland geïmplementeerd met de Wet beveiliging netwerk- en informatiesystemen (Wbni). Van beide moet echter gezegd worden dat de naleving niet optimaal is (op zijn minst) en dat de controle op die naleving onvoldoende is. Veel organisaties beschouwen dergelijke wet- en regelgeving vanuit een complianceperspectief: doen omdat het moet en niet vanuit een intrinsieke motivatie. En zolang de 'stok' onvoldoende wordt gehanteerd, is de noodzaak om te bewegen matig. Het toezicht is tot op heden nog beperkt, mede doordat dit toezicht per sector georganiseerd is en doordat toezichthouders te maken hebben met schaarse capaciteit voor het uitvoeren van controles en toezicht.

Gezien het belang van Smart Grids voor onze groene toekomst is dat een onwenselijke situatie: een strakkere regie vanuit de overheid is noodzakelijk. Bijkomend voordeel is de recent uitgevaardigde opvolger van de NIS Directive: de NIS2.

De NIS Directive (NIS staat voor: Network & Information Systems) is Europese regelgeving die erop gericht is de cyberveiligheid en weerbaarheid van kritieke systemen in Europa te vergroten. Het is aan de Europese lidstaten om de Directive te vertalen in nationale wetgeving. In Nederland is dat gedaan in de vorm van de Wbni, waarbij het toezicht is belegd bij de Rijksinspectie Digitale Infrastructuur (RDI), voorheen bekend als het Agentschap Telecom. De NIS2 Directive is de opvolger van de NIS Directive en is begin 2023 van kracht geworden. De uitwerking van NIS2 voor Nederland zal later in 2023 haar beslag krijgen; de deadline voor de lidstaten is oktober 2024. Organisaties die onder de regelgeving vallen, moeten uiterlijk januari 2025 voldoen aan de gestelde eisen. De energiesector in brede zin is onder de NIS Directive al aangemerkt als 'kritieke infrastructuur' en dit wordt met NIS2 nog verder uitgebreid richting het onderliggende ecosysteem.

Alhoewel de inhoud en insteek grotendeels overeenkomen met die van de huidige NIS Directive, is het te verwachten dat NIS2 minder vrijblijvend zal zijn en ook op technisch vlak meer 'voorschrijvend'. De boetes die met de toegenomen handhaving gepaard gaan zijn, althans op papier, niet misselijk. Ze kunnen maar liefst oplopen tot 10 miljoen euro of 2 procent van de wereldwijde omzet. Dat de energiesector zelf als 'kritiek' wordt beschouwd vanuit de regelgeving, zal geen verrassing mogen zijn. Immers, zonder energievoorziening zullen heel veel essentiële diensten in een land direct tot stilstand komen.

De verwachting is dat ook de ondersteunende en toeleverende bedrijven van de energiesector in grotere mate te maken gaan krijgen met de NIS2-vereisten. Het zal nog wel wat voeten in de aarde hebben om de handhaving in Nederland vorm te geven en de nodige ervaring en capaciteit te verzamelen.

Een derde preventieve maatregel om aanvallen op (toekomstige) slimme netwerken te voorkomen is het certificeren van de netwerkapparaten die consumenten gebruiken. Met een degelijk en uniform certificeringssysteem kan de consument ervan verzekerd zijn dat er geen malware in de apparatuur zit en dat die niet van buitenaf te misbruiken is.

Cyberrisico's moeten een plaats krijgen in de plan- en ontwerpfase van Smart Grids

SCHADE BEPERKEN NA EEN INCIDENT

In aanvulling op preventieve maatregelen zal de toepassing van Smart Grids ook beter beveiligd zijn als overheden, netbeheerders, energieproducenten, bedrijven en consumenten actie ondernemen om de schade te beperken, mochten zich onverhoopt incidenten voordoen. Het gaat dan ten eerste om het aanleggen van meer buffercapaciteit, bijvoorbeeld met industriële accu's met significante capaciteit (denk aan een leveringscapaciteit van 100 megawatt). Een van de belangrijkste voordelen van het gebruik van Smart Grids is weliswaar dat het dan juist niet nodig is de capaciteit van netwerken enorm uit te breiden, maar met het oog op de veiligheid is het ook niet aan te bevelen alle speelruimte qua uitwijkmogelijkheden weg te nemen. Door de aanwezigheid van buffercapaciteit wordt de impact van een cyberincident beperkt doordat de energievoorziening langer kan blijven doorgaan.

Een breder cyberrisicomanagement – waar de aanleg van buffers deel van kan uitmaken – moet daarnaast organisaties en consumenten ervan verzekeren dat de gevolgen van incidenten binnen de perken zullen blijven. Cyberrisicomanagement zorgt voor het gestructureerd in kaart brengen van dreigingen en kwetsbaarheden, wat leidt tot een beeld van relevante risico's.

Voor ieder risico moet dan worden nagedacht welke maatregelen (preventief, detectief, repressief of correctief) effectief nodig zijn om het risico tegen te gaan.

Weten wat er kan gebeuren is daarvoor een eerste vereiste en met het oog daarop zal gebruikgemaakt worden van scenario-ontwikkeling. Vervolgens is de vraag wat de doelstellingen zijn: hoelang mag een black-out duren voordat de schade onoverkomelijk is, aan welke systemen moet prioriteit worden gegeven bij het herstel, welke partijen krijgen voorrang? Op die doelstellingen zullen de draaiboeken worden geschreven. Oefeningen, liefst grootschalig en op basis van aanvalssimulaties, moeten vervolgens uitwijzen of dit risicomanagement goed geïmplementeerd is.

OVERZICHT KRIJGEN IN HET HELE SPEELVELD

Een van de grootste uitdagingen in dit verband is de landelijke coördinatie. Het is al lastig genoeg om overzicht te krijgen van alle bij het Smart Grid aangesloten punten, want grootverbruikers aangesloten op het Smart Grid hebben een meldplicht, maar particuliere initiatieven kunnen erop aansluiten zonder enige vorm van meldplicht. De verzameling van de netbeheerders, grootverbruikers en particulieren in combinatie met moderne Internet of Things- en Smart Grid-functionaliteit op hetzelfde net maakt het beveiligingsvraagstuk complex. En dan moet ook nog eens per punt (organisaties, bedrijven, laadpunten, zonneparken et cetera) duidelijk zijn welke beheersmaatregelen ten aanzien van de veiligheid daar genomen zijn. Een extra batterij op wijkniveau, aanvullende energieproductie bij een ziekenhuis, het kan allemaal van invloed zijn op het risicomanagement dat op landelijk niveau moet worden ingesteld. Maar de verantwoordelijkheid voor die lokale en regionale maatregelen ligt telkens op decentraal niveau. In onze visie moeten de netbeheerders hierin een grotere rol gaan spelen. In de digitalisering van de infrastructuur van netbeheerders, bijvoorbeeld daar waar het gaat om de onderstations, krijgt de beveiliging de laatste jaren reeds de nodige aandacht. De complexiteit en de onduidelijkheid in de ‘governance’ zijn groter op het terrein van private Smart Grids (bijvoorbeeld op een bedrijventerrein) en binnen ontwikkelingen in ‘smart cities’, waar burgers en overheid samen dienen te werken.

SAMENWERKING TUSSEN ALLE PARTIJEN IS ONONTBEERLIJK

Zo zijn ook de cyberrisico’s van Smart Grids een reden om te voorkomen dat de Nederlandse energievoorziening versnippert. Een onmogelijke opgave is dat niet, maar dan is het wel zaak dat alle betrokkenen snel het pad van de samenwerking kiezen. Dat zal een verregaande en intensieve samenwerking moeten zijn, met veiligheid hoog op de agenda. In de IT komt het vaker voor dat projecten alleen lijken te draaien om functionaliteit, maar rond de bouw en implementatie van Smart Grids kan Nederland zich dat niet veroorloven. Deze slimme netwerken zijn in potentie een prachtige oplossing voor een van de grootste uitdagingen van de energietransitie. Maar het zal onmogelijk blijken die belofte waar te maken als cruciale randvoorwaarden zoals compliance, risico’s en veiligheid onvoldoende worden behandeld.

Daarom is het nú het moment, in de plan- en ontwerpfase van Smart Grids, om de cyberrisico’s van deze slimme netwerken integraal mee te nemen in die plannen en ontwerpen. Zoals we hiervoor beschreven, zijn het met name standaardisering, certificering en een grotere sturende rol voor de overheid die dat mogelijk moeten maken, tezamen met inzicht in wie de aangesloten partijen op de Smart Grids zijn en met gestructureerd cyberrisicomanagement. De netbeheerders maken hierin de nodige stappen. Nu is het zaak om deze stappen ook te nemen in de Smart Grid-ontwikkelingen buiten de infrastructuur van de netbeheerder.

Over de auteurs

Ir. Max Kerkers is manager in het Cyber Assessments-team van KPMG Cyber & Privacy, waar hij klanten helpt met het verkrijgen van inzichten in de beveiliging van hun OT-omgevingen. Hij adviseert hen hoe ze deze veelal kritische omgevingen op een praktische manier beter kunnen beschermen tegen cyberdreigingen.

Drs. Pieter de Meijer RE CISSP CISA is director bij KPMG Cyber & Privacy en heeft ruime ervaring op het gebied van informatiebeveiliging en compliance. Hij heeft diverse organisaties geadviseerd over het structureel verbeteren van hun vermogen om hun informatie te beveiligen.

Ir. Ronald Heil is partner bij KPMG Cyber & Privacy en is gespecialiseerd in de veilige transformatie van IT- en OT-omgevingen, en specifiek de beveiliging van OT-omgevingen. Daarnaast heeft hij een rol bij KPMG als wereldwijde leider voor risk advisory in het energiedomein.