Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

> Retouradres Postbus 20011 2500 EA Den Haag

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Directie Cyber Security

Turfmarkt 147
2511 DP Den Haag
Postbus 20011
2500 EA Den Haag
www.nctv.nl

Ons kenmerk
2110384

Uw kenmerk
2017Z08332

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.

Datum 22 augustus 2017
Onderwerp Antwoorden Kamervragen over het bericht dat malware mogelijk energiebedrijven kan platleggen

Hierbij bied ik u, mede namens de minister van Economische Zaken, de antwoorden aan op de vragen van het lid Kuiken (PvdA) over het bericht dat malware mogelijk energiebedrijven kan platleggen (ingezonden op 15 juni).

De Staatssecretaris van Veiligheid en Justitie,

K.H.D.M. Dijkhoff

Antwoorden van de staatssecretaris van Veiligheid en Justitie en de minister van Economische Zaken op schriftelijke vragen van het lid Kuiken (PvdA)) over het bericht dat malware mogelijk energiebedrijven kan platleggen (ingezonden 15 juni 2017, 2017Z08332)

Directie Cyber Security

Datum
22 augustus 2017

Ons kenmerk
2110384

Vraag 1
Kent u het bericht "IT-beveiliger ESET ontdekt Industroyer, de gevaarlijkste malware gericht op industriële systemen sinds Stuxnet"? 1)

Antwoord op vraag 1
Ja.

Vraag 2
Deelt u de door IT-beveiliger ESET gebezigde stelling dat de malware Win32/Industroyer mogelijk ook schade aan zou kunnen richten aan Nederlandse energiebedrijven of die zelfs stil zou kunnen leggen? Zo ja, waarom? Zo nee, waarom niet?

Vraag 3
Is het waar dat Nederlandse energiebedrijven dezelfde of soortgelijke apparatuur en industriële communicatieprotocollen gebruiken als het Oekraïense bedrijf dat vatbaar is gebleken voor deze malware? Zo ja, welke conclusie trekt u hieruit?

Antwoord op vraag 2 en vraag 3
In de Nederlandse energiesector wordt veelal gebruik gemaakt van apparatuur en communicatieprotocollen gelijk aan, dan wel vergelijkbaar met, de apparatuur en protocollen waar de malware Industroyer zich op richt. Dit is inherent aan standaardisering en interoperabiliteit. Het is niet uit te sluiten dat de malware ingezet zou kunnen worden tegen systemen van Nederlandse energiebedrijven. Om schade aan te kunnen richten met de malware dient een aanvaller van buitenaf toegang tot het netwerk van het doelwit te verkrijgen. Pas daarna kan de malware worden ingezet om te communiceren met industriële controlesystemen. Het is qua weerbaarheid dan ook zaak dat partijen er zorg voor dragen dat een aanvaller van buitenaf niet binnendringt op het netwerk om deze aanvalstechniek in te zetten. Dit vraagt niet om een andere inzet dan bij de bescherming tegen andere aanvallen. Het is aan de partijen zelf om maatregelen te nemen die de kans op misbruik beperken of wegnemen, zoals het installeren van software-updates om kwetsbaarheden weg te nemen, en om maatregelen te nemen die de impact van misbruik kunnen beperken, zoals het implementeren van detectie- en monitoringoplossingen om aanwezigheid van (bekende vormen van) malware te kunnen herkennen. Het managen van cybersecurityrisico's is voor de energiebedrijven een continu proces. Uiteraard ligt de verantwoordelijkheid voor informatiebeveiliging primair bij de partijen zelf.

Vraag 4
Deelt u de mening dat, in het geval er sprake is van vitale infrastructuur zoals energiebedrijven, ook de rijksoverheid een verantwoordelijkheid heeft ten aanzien van de bescherming daarvan? Zo ja, hoe wordt daar in dit concrete geval inhoud aan gegeven? Zo nee, waarom niet?

Antwoord op vraag 4
Overheid en vitale organisaties werken in Nederland samen aan de bescherming van de vitale infrastructuur. De rol van de overheid wordt in generieke zin onder andere ingevuld door middel van wet- en regelgeving. Het Nationaal Cyber Security Centrum (NCSC) van het Ministerie van Veiligheid en Justitie heeft tot taak vitale aanbieders over dreigingen en incidenten te informeren en adviseren en daarbij zo nodig ook anderszins bijstand te verlenen, teneinde maatschappelijke ontwrichting die daarvan mogelijkerwijs het gevolg is te voorkomen en beperken.

Transport en distributie van elektriciteit en gas zijn aangemerkt als vitale processen. Op grond van de Elektriciteitswet 1998 en de Gaswet hebben de netbeheerders de verantwoordelijkheid zorg te dragen voor een veilig en efficiënt transport van energie. ICT beveiliging maakt daar intrinsiek onderdeel van uit. De netbeheerder dient datgene te doen dat binnen zijn (juridische) mogelijkheden ligt om de integriteit van zijn netwerk te beschermen. Op een goede taakuitoefening door de netbeheerders ziet de toezichthouder ACM toe. Energiebedrijven onderhouden contact met relevante overheidsdiensten en partner organisaties om de security controls aan te passen aan nieuwe threat intelligence.

Voorts zij nog gewezen op de Europese Netwerk- en informatiebeveiligingsrichtlijn en de implementatiewetgeving die hiervoor in voorbereiding is, die onder meer voorziet in de verplichting van vitale aanbieders in de energiesector om passende beveiligingsmaatregelen te nemen met betrekking tot hun netwerk- en informatiesystemen, en toezicht op de naleving daarvan. Het implementatiewetsvoorstel is op 16 juni jl. in consultatie gebracht.

Vraag 5
Biedt ESET zelf concrete (commerciële) oplossingen voor de bescherming tegen de in het bericht genoemde malware? Is die ook bruikbaar voor Nederlandse energiebedrijven? Zijn er ook andere bedrijven die diensten aanbieden om deze bedreigingen tegen te gaan?

Antwoord op vraag 5
Ja, ESET biedt als leverancier oplossingen aan voor bescherming van systemen. In algemene zin geldt dat meerdere digitale beveiligingsbedrijven commerciële toepassingen aanbieden. Het is aan partijen zelf of en op welke wijze zij hiervan in het kader van de beveiliging van hun systemen gebruik maken.

Wat het concrete incident in Oekraïne betreft merk ik overigens nog op dat ESET hiervan actief melding heeft gemaakt bij het NCSC en partijen in de energiesector. De relevante Nederlandse partijen waren dan ook tijdig op de hoogte van het rapport van ESET. Het NCSC blijft de situatie monitoren met het oog op het waar nodig tijdig kunnen informeren en adviseren van genoemde partijen.

1) https://www.eset.com/nl/over/newsroom/nl-news-categories-parent/industroyer-grootste-bedreiging-voor-industriele-controlesystemen-sinds-stuxnet/