

TC035

TOEGANG MARKTFACILITERENDE SYSTEMEN

Heeft het issue impact op..?	
Grootverbruik	X
Kleinverbruik	X
Elektriciteit	X
Gas	X
RNB	X
LNB	X
LV	X
MV	X
PV	X
Codes	(zie codepakket IC208-210)
Berichten	
Ketenprocessen	
Privacy	
Is het issue release afhankelijk/onafhankelijk en welke invoeringsdatum heeft het issue.	
Release-afhankelijk	
Release-onafhankelijk	X

Nummer TC035
Datum 29-3-2017
Versie 1.0
Status Vastgesteld

Opsteller(s) Bram van Straalen
 Gerrit Fokkema

Inhoudsopgave

Colofon	3
Versiebeheer	3
Distributie	3
Probleemdefinitie	4
Overwegingen	5
Gekozen oplossing	6
Algemene beveiligingsmaatregelen	6
Toegang ingeschakelde derden.	7
Autorisatiebeheer	9
Impact	9
Invoeringsstrategie	10
Te vervallen issues	10

COLOFON

VERSIEBEHEER

Versie	Status	Wijziging	Auteur	Datum
0.1	Concept	Eerste opzet	Bram van Straalen	9-2-2017
0.2	Concept	N.a.v. eerste opmerkingen en aanscherpingen	Bram van Straalen	10-2-2017
0.3	Concept	N.a.v. review vanuit o.a. EDSN	Bram van Straalen	16-2-2017
0.4	Concept	Ombouw issue naar haakje in de IcEG tot procedure afspraken	Gerrit Fokkema	21-2-2017
0.5	Concept	Wederom gewijzigde opzet met codetekst via IC208	Gerrit Fokkema	23-2-2017
0.6	Ter vaststelling	Kleine aanscherpingen obv review commentaar	Gerrit Fokkema	28-02-2017
0.7	Concept	Verplichting door LV systemen en IP adressen weggehaald	Gerrit Fokkema	07-03-2017
0.8	Concept	Aanscherping formuleringen en herstructurering	Gerrit Fokkema	09-03-2017
0.9	Ter vaststelling	Paar kleine verbeteringen	Gerrit Fokkema	20-03-2017
1.0	Vastgesteld ALV NEDU		Gerrit Fokkema	29-03-2017

DISTRIBUTIE

Gremium	Verstuurd (versie/datum)									
	0.1	0.2	0.3	0.4	0.5	0.6	0.70	0.8	0.9	1.0
	dd-mm-jjjj	dd-mm-jjjj	dd-mm-jjjj	dd-mm-jjjj	dd-mm-jjjj	dd-mm-jjjj	dd-mm-jjjj	dd-mm-jjjj	dd-mm-jjjj	dd-mm-jjjj
TC		10-02-2017	16-02-107		23-02-2017	28-02-2017		10-03-2017		
IC-Klant-WG Dataveiligheid		10-02-2017		22-02-2017	23-02-2017			10-03-2017		
IC-Klant/IC-WG/IC-WG					23-02-2017			10-03-2017		
Taskforce Dataveiligheid							8-03-2017	10-03-2017		
SPC					(23-02-2017)					
ALV NEDU						28-02-2017			20-03-2017	29-03-2017
Allen										

PROBLEEMDEFINITIE

Onderdeel	Omschrijving
De ontwikkeling betreft:	Naar aanleiding van een onderzoek van de AP en ACM heeft een gezamenlijke taskforce Dataveiligheid met vertegenwoordiging van netbeheerders, leveranciers en Nedu een Actieplan opgesteld met maatregelen om de bescherming van klantgegevens in de processen waarin gegevensuitwisseling plaatsvindt te borgen. Er zijn daarbij ook maatregelen afgesproken om de toegang tot en het gebruik van de marktfaciliterende systemen (zoals bij EDSN) beter te regelen ter voorkoming van ongeautoriseerde toegang tot de marktfaciliterende systemen.
En raakt:	Alle marktrollen
Als gevolg waarvan:	Onvoldoende duidelijk is wie toegang heeft tot de marktfaciliterende systemen, waarbij m.b.t. de door een marktpartij ingeschakelde derden geldt dat onvoldoende duidelijk is namens welke marktpartij de derde toegang heeft, voor hoelang en of daarbij de relevante beveiligingsmaatregelen en andere toegangseisen worden nageleefd, waardoor mogelijk onrechtmatige toegang kan worden verkregen tot de marktfaciliterende systemen en datalekken in de zin van de Wbp kunnen ontstaan.
Een goede oplossing moet:	De toegang van marktpartijen en van onderaannemers van marktpartijen (zogenaamde “derden”) tot de marktfaciliterende systemen moet aansluiten bij de gezamenlijke uitgangspunten die de sector daarvoor heeft opgesteld in het Actieplan. Deze uitgangspunten zijn: • het treffen van generieke beveiligingsmaatregelen c.q. het treffen van passende organisatorische en technische maatregelen door marktpartijen om rechtmatige toegang te garanderen; • het voeren van een deugdelijk autorisatiebeheer; • de toegang van derden tot de marktfaciliterende systemen vindt uitsluitend plaats namens en onder verantwoordelijkheid en toezicht van de marktpartij die de derde heeft ingeschakeld (‘verantwoordelijke marktpartij’); • de toegang van derden tot de marktfaciliterende via rechtstreekse verbindingen wordt altijd door de verantwoordelijke marktpartij gemeld aan de beheerder van de marktfaciliterende systemen. Het overzicht met derden als hier bedoeld wordt actueel gehouden; toegangsrechten van derden hebben een tijdelijk karakter.
Of deze doelen worden behaald, kan worden gevalideerd door:	Implementatie van de maatregelen bij de marktpartijen. Marktpartijen voldoen aan een aantal vereisten m.b.t.: • Het gebruik van de (centrale) marktfaciliterende systemen; • Het beveiligingsbeleid bij marktpartijen die toegang tot deze (centrale) marktfaciliterende systemen hebben; • Autorisatiebeheer.
Opdrachtgever te realiseren oplossing	NEDU
Probleemeigenaar	TC

OVERWEGINGEN

Naar aanleiding van een onderzoek van de AP en ACM naar de dataveiligheid in het kader van de Wbp heeft een taskforce een Actieplan Dataveiligheid opgesteld om een aantal aanpassingen per sectorrelease 2017 door te voeren in de sector. Het Actieplan kent een breed draagvlak in de sector. Dit issue beschrijft maatregel 3 en 4 uit het Actieplan, die gericht zijn op de toegang en beveiliging van de marktfaciliterende systemen, zoals de netbeheerders die beschikbaar stellen aan de marktpartijen. Het Actieplan richt zich met name op de marktfaciliterende systemen C-AR, CER en TMR. De maatregelen voor toegang en beveiliging richten zich in principe breder op de marktfaciliterende systemen.

Maatregel 3: gecontroleerde toegang voor derde partijen

Verschillende marktpartijen maken gebruik van onderaannemers voor ICT(hosting-) diensten of voor de uitvoering van diverse processen, zoals de werving van nieuwe klanten of verkrijgen van meterstanden. Hiervoor is het soms nodig voor deze onderaannemers om namens en onder verantwoordelijkheid van de marktpartij toegang te hebben tot de marktfaciliterende systemen. De onderaannemers (derden) maken hierbij gebruik van de gebruikersaccounts en systeemaccounts die verstrekt worden door de marktpartij die hen inhuurt en die alleen voor dit doel gebruikt mogen worden. Dit dient tussen de verantwoordelijke marktpartij en de derde contractueel te worden gewaarborgd; de verantwoordelijke marktpartij is daarbij verantwoordelijk om een overeenkomst met de derde af te sluiten (ingeval er sprake is van de verwerking van persoonsgegevens een bewerkersovereenkomst). De maatregel bestaat uit het zeker stellen dat de verantwoordelijke marktpartij voldoende controle heeft en houdt op de toegang tot en het werken met de marktfaciliterende systemen met name door die derden, onder andere door bij voorkeur de systemen van een onderaannemer niet rechtstreeks met de marktfaciliterende systemen te koppelen, maar de toegang tot de marktfaciliterende indien mogelijk alleen via de systemen van de verantwoordelijke marktpartij te laten lopen.

Maatregel 4: standaardiseren accountbeleid

Marktpartijen (en daarmee ook de door hen ingeschakelde derden) met toegang tot de marktfaciliterende systemen moeten passende maatregelen nemen voor de logische toegangsbeveiliging. Uitsluitend bevoegde personen krijgen toegang tot en kunnen gebruik maken van de functionaliteiten van de marktfaciliterende systemen. De bevoegdheid van een persoon moet worden afgeleid van de taak, functie of verantwoordelijkheid van de betreffende persoon.

De marktpartij autoriseert en registreert feitelijke gebruikers/beheerders die toegang hebben tot de marktfaciliterende systemen op basis van een formele procedure, waarvoor een aantal voorschriften wordt opgelegd. Gebruikers- en beheeraccounts mogen niet zijn voorzien van meer rechten dan strikt noodzakelijk is voor het uitvoeren van de noodzakelijke taken. Hiervoor wordt een autorisatiematrix bijgehouden. De netbeheerders (als verantwoordelijken voor de marktfaciliterende systemen) kunnen ad hoc controle verleende toegangsrechten en controle van gebruiksgegevens van de marktfaciliterende systemen uitvoeren.

Verankering

De benodigde aanpassingen in de informatiecode zullen worden meegenomen in het pakket code aanpassingen in IC208 - IC210, die eveneens als gevolg van het actieplan zijn opgesteld. Vooruitlopend op de bekrachtiging van de codeaanpassingen is de bedoeling conform actieplan dat de sector al vanaf 1 april 2017 conform bovengeschetste maatregelen gaat werken. Daartoe is dit issue opgesteld, die een aantal eisen concreter uitwerkt.

GEKOZEN OPLOSSING

In dit issue wordt specifiek ingegaan op het noodzakelijk geachte beveiligings- en autorisatiebeleid voor toegang van marktpartijen en de door hen ingeschakelde derden (hierna te noemen: 'derden') tot de marktfaciliterende systemen en bijhorend berichtenverkeer.

Voor de toepassing van dit issue heeft een door een derde ingeschakelde derde (en eventuele derde partijen daarachter) eveneens te gelden als een derde als in dit document bedoeld, en geldt alles wat in dit document in relatie tot een derde is gesteld op overeenkomstige wijze.

ALGEMENE BEVEILIGINGSMAATREGELEN

Marktpartijen, die gebruik maken van de marktfaciliterende systemen:

- dienen een informatiebeveiligingsbeleid te hanteren conform een algemeen aanvaarde standaard, afgestemd op de specifieke context en beveiligingsrisico's;
- zijn gehouden om passende maatregelen te nemen voor toegangsbeveiliging tot de marktfaciliterende systemen, waaronder begrepen het gebruik van een passend betrouwbaarheidsniveau voor authenticatie;
- dienen te beschikken over een procedure die de omgang met beveiligingsincidenten beschrijft. Beveiligingsincidenten met betrekking tot de marktfaciliterende systemen dienen onverwijld te worden gemeld aan de netbeheerders. Hiertoe kan de recent vastgestelde procedure beveiligingsincidenten¹ worden gebruikt;
- dragen er zorg voor dat de door hen aan de beheerder van de marktfaciliterende systemen door te geven IP-adressen, waarmee toegang kan worden verkregen tot de marktfaciliterende systemen (in het kader van whitelisting²), tot een minimum aantal beperkt blijven. Periodiek en ten minste 1 maal per 2 jaar evalueert de marktpartij alle geregistreerde IP-adressen op noodzaak voor toegang en mogelijkheden voor minimalisatie en borgt de verslaglegging hiervan in de organisatie. De alsnog benodigde adressen zullen worden gemeld aan de beheerder van de marktfaciliterende systemen.

¹ SC003 procedure beveiligingsincidenten, vastgesteld in de ALV vergadering van 18 januari 2017, te vinden op de NEDU sharepoint onder <https://nedunl.sharepoint.com/ActueleProcesdocumentatie/Issueoverzicht>.

² Whitelisting is een techniek om op basis van een ('witte') lijst (met in dit geval IP-adressen) selectief toegang te verlenen (en alle andere te blokkeren).

TOEGANG INGESCHAKELDE DERDEN.

Verschillende marktpartijen maken gebruik van derden voor de uitvoering van diverse processen, zoals in outsourcing van ICT diensten of voor de werving van nieuwe klanten of verkrijgen van meterstanden. Hiervoor is het soms nodig deze derden namens en onder verantwoordelijkheid de marktpartij toegang te verlenen tot de marktfaciliterende systemen. Deze derden maken hierbij gebruik van de gebruikersaccounts en systeem-accounts die verstrekt worden door en onder verantwoordelijkheid van de marktpartij die hen inhuurt, en die alleen voor dit doel gebruikt mogen worden.

- Een marktpartij, als gebruiker van de marktfaciliterende systemen, die gebruik maakt van een derde:
 - is verantwoordelijk voor de toegang van die derde tot de marktfaciliterende systemen en de acties die de derde op deze systemen uitvoert;
 - houdt toezicht op de toegang van die derde tot de marktfaciliterende systemen en de acties die de derde op de marktfaciliterende systemen uitvoert;
 - draagt er zorg voor dat een door hem ingeschakelde derde niet rechtstreeks toegang krijgt tot de marktfaciliterende systemen, tenzij dat niet anders kan gelet op de feitelijke situatie. Het gebruik van de (functionaliteit van de) marktfaciliterende systemen door een ingeschakelde derde dient derhalve te lopen via een door de verantwoordelijke marktpartij (gebruikt en) gecontroleerd ICT-systeem en alleen bij wijze van uitzondering mag dat anders worden ingevuld.
 - meldt, indien nodig is dat een derde via een rechtstreekse verbinding toegang krijgt tot de marktfaciliterende systemen, het/de daartoe benodigde IP adres(sen) voor whitelisting aan de beheerder van de marktfaciliterende systemen waarbij tevens opgave zal worden gedaan van minimaal de volgende gegevens:
 - juridische tenaamstelling derde en KvK-nummer;
 - naam contactpersoon derde + contactgegevens;
 - taak of rol derde;
 - duur van het aan derde verleende toegangsrecht (max. 2 jaar).
 - dient beëindiging of opschorting van de overeenkomst met de derde zo snel mogelijk maar in ieder geval binnen een week te melden aan de beheerder van de marktfaciliterende systemen, die vervolgens het/de bijhorende IP adres(sen) zal verwijderen uit de whitelist;
 - is gehouden om contractueel te borgen dat een ingeschakelde derde zelfstandig voldoet aan alle verplichtingen die gelden voor toegang tot van de marktfaciliterende systemen, waaronder in ieder geval begrepen de verplichtingen zoals die voortvloeien uit onderhavig issue, de Informatiecode Elektriciteit en Gas en de Wet bescherming persoonsgegevens;
 - regelt eventueel benodigde B2B (webservices) toegang van de bewerker tot de marktfaciliterende systemen als volgt:

- i. hoofdregel; de marktpartij en de derde maken een beveiligde koppeling tussen hun systemen t.b.v. de toegang via het ICT Netwerk van de marktpartij tot webservices van de marktfaciliterende systemen. Via deze koppeling kan m.b.v. het systeem-account van de marktpartij t.b.v. de uitvoering van de werkzaamheden van onderaannemer toegang verkregen worden tot de marktfaciliterende systemen;
 - ii. de marktpartij monitort actief het gebruik van de bewerker van de marktfaciliterende systemen;
 - iii. de marktpartij zorgt voor een passende beveiliging van de verbinding met en de systemen van de derde en legt hierover afspraken contractueel vast;
 - iv. de marktpartij zorgt bij beëindiging van de dienstverlening door c.q. het contract met de derde zo snel mogelijk maar in ieder geval binnen een week na de beëindiging voor ontkoppeling van de systemen van de marktpartij met de systemen van de derde.
- regelt eventueel benodigde toegang tot webapplicaties (gebruiker die inlogt via internet) van de derde tot de marktfaciliterende systemen als volgt:
 - i. hoofdregel: de marktpartij en de derde maken een beveiligde koppeling tussen hun systemen t.b.v. de toegang via het ICT Netwerk van de marktpartij tot de webapplicaties van de marktfaciliterende systemen. Via deze koppeling kan m.b.v. een door de beheerder van de marktpartij aangemaakte gebruikersaccount toegang verleend worden tot webapplicaties van de marktfaciliterende systemen ;
 - ii. het registreren en beheren van feitelijk gebruikers van de derde vindt plaats volgens de onderstaande vereisten voor autorisatiebeheer;
 - iii. de gebruikersaccounts van medewerkers van een derde zijn als zodanig herkenbaar.
- De beheerder van de marktfaciliterende systemen houdt een registratie bij van de toegelaten IP-adressen. Een bij de beheerder van de marktfaciliterende systemen onbekende derde zal geen toegang worden verleend tot de marktfaciliterende systemen. Met een bij de beheerder van de marktfaciliterende systemen onbekend IP adres van een bekende derde kan evenmin toegang worden verkregen tot de marktfaciliterende systemen. De door een marktpartij opgegeven IP-adressen van derden zullen: i.) op verzoek van de verantwoordelijke marktpartij, ii.) na het verstrijken van de looptijd van het gebruiksrecht van de derde (zoals opgegeven door de marktpartij, max. 2 jaar) dan wel iii.) na verloop van 2 jaar na registratie, worden verwijderd uit de whitelist van de marktfaciliterende systemen tenzij de verantwoordelijke marktpartij tijdig (uiterlijk 14 dagen voor afloop van de lopende gebruikstermijn) aan de beheerder van de marktfaciliterende systemen laat weten dat het gebruik van een bepaald IP adres door een derde nog langer gewenst is onder opgave van voor welke duur dat heeft te gelden (max. 2 jaar).

AUTORISATIEBEHEER

Marktpartijen (en daarmee de door hen ingeschakelde derden) met toegang tot de marktfaciliterende systemen, moeten passende maatregelen voor de logische toegangsbeveiliging treffen. Uitsluitend bevoegde personen krijgen toegang tot en kunnen gebruik maken van de functionaliteiten van de marktfaciliterende systemen. De bevoegdheid van een persoon moet worden afgeleid van de taak, functie of verantwoordelijkheid van de betreffende persoon.

- Een marktpartij, die gebruik maakt van de marktfaciliterende systemen:
 - is gehouden om toegangsgerechtigden tot c.q. de feitelijk gebruikers van (de functionaliteiten van) de marktfaciliterende systemen te autoriseren en te registreren op basis van een formele procedure. Deze formele procedure voorziet tenminste in het volgende:
 - i. het verlenen en intrekken van toegangsrechten tot de functionaliteiten van de marktfaciliterende systemen vindt plaats op basis van de uit te voeren functie/taken, waarbij niet meer rechten worden toegekend dan strikt noodzakelijk voor het uitvoeren van deze functie/taken;
 - ii. het toegangsaccount van een toegangsgerechtigde is herleidbaar tot een identificeerbaar natuurlijk persoon;
 - iii. een toegangsaccount mag enkel en alleen door een geautoriseerd persoon worden gebruikt;
 - iv. het intrekken van autorisaties bij wijziging van functies/taken vindt uiterlijk 5 dagen na de wijziging plaats.
 - zorgt minstens ieder kwartaal voor controle en schoning van de verleende toegangsrechten;
 - heeft ten alle tijden een compleet en actueel overzicht van de gebruikers van de marktfaciliterende systemen (binnen en buiten de organisatie) en bijbehorende autorisaties;
 - heeft schriftelijke afspraken gemaakt met medewerkers (zowel intern als extern) over het inzien van de informatie in marktfaciliterende systemen. Bijvoorbeeld een geheimhoudingsverklaring.
- De verantwoordelijken voor de marktfaciliterende systemen zijn bevoegd om de naleving van de verplichtingen met betrekking tot het autorisatiebeheer bij een marktpartij te (laten) controleren en voorts om de verleende toegangsrechten tot de marktfaciliterende systemen te (laten) controleren.

IMPACT

De impact op de IcEG wordt opgenomen in de codevoorstellen voor IC208-IC201.

INVOERINGSSTRATEGIE

	Release onafhankelijk	Release afhankelijk
Na vaststelling ALV NEDU	Per 1 april 2017	
Sectorrelease 2017		
Specifieke datum		

TE VERVALLEN ISSUES

Nvt