SC008

Beveiliging e-mail verkeer tussen marktpartijen met TLS

Het issue heeft impact op:	
Grootverbruik	X
Kleinverbruik	X
Elektriciteit	X
Gas	X
LNB	X
RNB	X
LV	X
MV	X
PV	X
EDSN	X
Codes	
Berichten	
Ketenprocessen	
Is het issue release afhankelijk/onafhankelijk	
Release-afhankelijk	
Release-onafhankelijk	X, uiterlijk 07-02-2019 ingevoerd

Nummer SC008
Datum 07-11-2018
Versie 1.0
Status Vastgesteld

Opsteller(s) NEDU Security Commissie

Inhoudsopgave

Colofon

Versiebeheer

Versie	Status	Wijziging	Auteur	Datum
0.1	Concept	Eerste opzet, gebaseerd op brief van de SC met dito strekking aan IC-Klant	Security Commissie/Gerrit Fokkema	11-10-2018
0.2	Ter vaststelling	Aanscherpingen n.a.v. review door SC en TC leden	Gerrit Fokkema	23-10-2018
0.3	Ter vaststelling	Enige redactionele verbeteringen	Gerrit Fokkema	24-10-2018
0.4	Ter vaststelling	Enige redactionele verbeteringen	Eline Spauwen	24-10-2018
0.5	Ter vaststelling	N.a.v. finale bespreking in de SC en reacties vanuit de IC-Klant	Gerrit Fokkema	30-10-2018
1.0	Vastgesteld	Na vaststelling in de ALV van 7 november 2018	Gerrit Fokkema	15-11-2018

Distributie

Gremium	Verstuurd (versie/datum)									
	0.1	0.2	0.3	0.4	0.5	1.0				
Security Commissie	11-10-2018	23-10-2018	24-10-2018	24-10-2018	30-10--2018	15-11-2018				
Technische Commissie	11-10-2018	23-10-2018			30-10--2018					
Sectorplanningscommissie		24-10-2018								
ALV NEDU					30-10--2018					
Allen						15-11-2018				

Referenties

Ref	Titel	Eigenaar	Datum	Versie	Status
1	TC039 Veilige kanalen	NEDU - TC	15-01-2018	0.6	Ter vaststelling
2	TC038 Jaarlijkse update cipersuites	Nedu-TC	23-05-2018	3.0	Vastgesteld, in invoering
3	TC024 Overgang op TLS1.2	NEDU - TC	01-04-2015	2.0	Vastgesteld en ingevoerd
4	TC023 Beveiligde verbindingen	NEDU - TC	24-04-2013	1.0	Vastgesteld en ingevoerd

1 Probleemdefinitie

Onderdeel	Omschrijving
Het probleem / de ontwikkeling / de wet- of regelgeving betreft:	Via ‘gewone’ e-mail verkeer worden in de sector ad-hoc gegevens uitgewisseld tussen partijen. Deze gegevens betreffen vaak ook persoonsgegevens. In het kader van dataveiligheid heeft op verzoek van de IC-Klant de Technische Commissie samen met de Security Commissie een advies opgesteld in TC039 om deze gegevens beveiligd uit te wisselen. De bedoeling was een dergelijke oplossing snel te implementeren, maar dat laat blijkbaar nog wel even op zich wachten.
En raakt:	Alle partijen in de sector.
Als gevolg waarvan:	Persoonsgegevens onvoldoende veilig worden uitgewisseld.
Een goede oplossing moet:	Snel leiden tot een betere beveiliging van de ad-hoc uitwisseling van persoonsgegevens via e-mail berichtenverkeer tussen marktpartijen. Let wel het betreft een snelle reparatie, maar biedt niet de inTC039 beoogde robuust veilige oplossing
Of deze doelen worden behaald, kan worden gevalideerd door:	Door navraag te doen of de marktpartijen e-mailberichten primair met TLS versturen.
Opdrachtgever te realiseren oplossing	ALV NEDU.
Probleemeigenaar	Alle NEDU leden, alle partijen actief in de sector.

2 Introductie

Naar aanleiding van de acties in het kader van Dataveiligheid heeft de IC-Klant aan de Technische Commissie vragen gesteld over de ad-hoc uitwisseling van persoonsgevoelige gegevens in de sector. Als antwoord hierop is issue TC039 opgesteld door de Technische- en Security Commissie, met daarin een analyse van mogelijke oplossingen en een aantal concrete voorstellen. Het was de bedoeling om al voor de zomer van 2018 de daarin beoogde oplossing van een 'berichtenbox' te implementeren. Echter, die implementatie lijkt vooralsnog uit te blijven, waardoor de ad-hoc gegevensuitwisseling nog steeds via het reguliere e-mail wordt gedaan. Daarmee worden persoonsgevoelige gegevens naar oordeel van de Security Commissie onvoldoende beveiligd uitgewisseld. Dit issue beoogt met een snelle verbetering de beveiliging sterk te verbeteren, maar leidt niet tot een robuust veilige oplossing.

3 Overwegingen

- De Security Commissie hecht er aan haar zorg uit te spreken over het uitblijven van een veilige oplossing en roept op de onveilige ad-hoc gegevensuitwisseling via e-mail verkeer zo snel mogelijk te vervangen door een robuust veilige oplossing conform TC039;
- Mochten er in de huidige situatie, waarin persoonsgegevens via onbeveiligd e-mail verkeer worden uitgewisseld, onverhoopt problemen ontstaan dan is moeilijk uitlegbaar dat in de sector geen afspraken zijn gemaakt om de onveilige uitwisseling van persoonsgegevens beter te beveiligen;
- Als noodmaatregel stelt de Security Commissie voor per direct of zo snel als maar mogelijk is het e-mail verkeer, dat voor genoemd doel wordt gebruikt, te beveiligen met TLS verbindingen. Dit is weliswaar geen sluitende, afdwingbare beveiliging, zoals in TC039 aangegeven, maar een grote verbetering op de huidige onbeveiligde uitwisseling. Ook al ondersteunen beide partijen TLS, geeft dit nog geen betrouwbare opzet van de verbinding. SMTP is een client-server protocol zonder wederzijdse authenticatie;
- Alle betrokken marktpartijen zullen zelf moeten zorgen voor e-mail verkeer via met TLS beveiligde verbindingen. Het is niet afdwingbaar voor tegenpartijen;
- Vele partijen hebben al TLS beveiliging op de verbindingen van hun e-mail verkeer ingevoerd;
- Binnen de sector zijn standaarden afgesproken over het gebruik van TLS beveiligde verbindingen (zie TC023 en TC024).
  Het is bij beveiliging van het e-mail verkeer niet vereist om PKI-Overheidscertificaten voor de beveiliging te gebruiken, andere geschikte certificaten van gerenommeerde (voldoende betrouwbare) certificaat autoriteiten (CA's) kunnen worden gebruikt. Verder is de eis voor versie 1.2 voor TLS niet hard en kan een lagere versie worden gebruikt. Wel is aan te bevelen om de beveiliging van het e-mail verkeer zo veilig mogelijk in te richten;
- Gezien het feit dat via het e-mail verkeer de partijen met meer dan alleen de marktpartijen onderling moeten kunnen communiceren, zijn de eisen van TC038 om de voor de verbinding gebruikte ciphersuites sterk in te perken niet aan de orde. Wel wordt sterk aangeraden de veiligste ciphersuites te hanteren en deze bovenaan de lijst te zetten voor onderhandeling in het tot stand brengen van een verbinding en af te dwingen dat van hoog naar laag wordt onderhandeld;

- Het eenvoudigst is zogenaamde opportunistische TLS(zie *link*) in te stellen.
  Nadeel van opportunistische TLS is dat er nog steeds makkelijk een 'man-in-the-middle downgrade' kan worden uitgevoerd. Een malafide actor kan aangeven dat hij/zij geen van de TLS versies ondersteunt en toch graag cleartext wil communiceren. Dit blijft een nadeel van client-server protocollen zonder wederzijdse authenticatie;
- Op basis van de artikelen van o.a. de Autoriteit Persoonsgegevens is een aantal alternatieven naar voren gekomen:
  1. StartTLS: https://nl.wikipedia.org/wiki/STARTTLS;
  2. StartTLS + DANE: https://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions.
     Relevante artikelen:
     - https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/beveiliging-van-persoonsgegevens;
     - https://www.forumstandaardisatie.nl/standaard/starttls-en-dane;
     - https://www.sidn.nl/a/veilig-internet/veilige-e-mail-coalitie-van-start;
     - https://www.ncsc.nl/actueel/factsheets/factsheet-beveilig-verbindingen-van-mailservers.html.
- Het advies is StartTLS (zonder DANE) te implementeren. Dit is op veel servers al standaard aanwezig en gemakkelijk te implementeren;
- Via de website https://www.internet.nl/ kan men eenvoudig controleren hoe goed de e-mailservers beveiligd zijn. Dit kan gebruikt worden zowel voor controle van de eigen servers als voor die van tegenpartijen.

4 Gekozen oplossing

Uiterlijk 3 maanden na vaststelling door de ALV voeren alle partijen TLS beveiliging in op de e-mailverbindingen waarmee de ad-hoc communicatie tussen partijen in de sector wordt uitgevoerd. Hierdoor wordt bij dit e-mailverkeer primair geprobeerd via een TLS beveiligde verbinding de e-mail te versturen (een ieder ondersteunt **opportunistische TLS**, om te voorkomen dat we moeten gaan verplichten dat er altijd TLS gebruikt **moet** worden bij communicatie tussen marktpartijen). Als de wederpartij geen TLS ondersteuning biedt, wordt de e-mail zonder TLS verstuurd. Daarom is het wel zaak dat alle partijen TLS beveiliging op hun e-mail verbindingen instellen.

5 Invoeringsstrategie

	Release onafhankelijk	**Release afhankelijk**
Na vaststelling ALV NEDU	Uiterlijk 3 maanden na vaststelling, 07-02-2019	

	Release onafhankelijk	Release afhankelijk
Sectorrelease		
Specifieke datum		

6 Te vervallen issues

Geen.