NEDU

BEVEILIGINGSBELEID

INFORMATIE UITWISSELINGSPROCESSEN

Titel	Beveiligingsbeleid Informatie Uitwisselingsprocessen
Versie	1.0
Status	Vastgesteld door de ALV NEDU
Datum	7 maart 2018
Auteurs	Aad Dekker, Marcel Kerkhof, Anne Spoelstra, Tore ter Horst

Versielog

Versie	Datum	Auteur	Opmerking
0.1	01-05-2017	Aad Dekker, Anne Spoelstra	Eerste opzet.
0.2	21-06-2017	Aad Dekker, Anne Spoelstra, Marcel Kerkhof	Opmerkingen verwerkt.
0.3	25-07-2017	Aad Dekker, Anne Spoelstra, Marcel Kerkhof	Opmerkingen verwerkt.
0.31	16-08-2017	Gerrit Fokkema	Enige aanscherpingen
0.32	22-09-2017	Marcel Kerkhof	Toevoeging risicoanalyse en BIV
0.4	24-10-2017	Gerrit Fokkema	Enige aanscherping n.a.v. finale review SC
0.5	27-10-2017	Gerrit Fokkema	Nagekomen review opmerkingen SC verwerkt
0.6	22-01-2018	Luisella ten Pierik Marcel Kerkhof Tore ter Horst	Rationalisatie en verduidelijking van scope
0.61	25-01-2018	Tore ter Horst	Aangepaste versie t.b.v. afstemming alle SC-leden
0.62	05-02-2018	Tore ter Horst	Feedback van alle SC-leden verwerkt
0.7	09-02-2018	Tore ter Horst	Consensus SC-leden
1.0	07-03-2018	Gerrit Fokkema	Vastgesteld door de ALV op 7 maart 2018

Inhoudsopgave

1 INLEIDING

Onvoldoende informatiebeveiliging op de informatie uitwisselingsprocessen tussen de NEDU leden kan leiden tot onacceptabele risico's bij de uitvoering van de ketenprocessen. Incidenten en inbreuken op deze informatie uitwisselingsprocessen kunnen leiden tot grote financiële consequenties en imago schade in de hele sector. De leden van de NEDU hebben voor de eigen bedrijfsvoering belang bij een adequaat niveau van informatiebeveiliging, maar dit geldt evenzeer voor externe stakeholders, zoals klanten en toezichthoudende instanties. De noodzaak om systematisch aandacht te besteden aan de beveiliging van de informatievoorziening is dan ook groot.

Onder informatiebeveiliging verstaat NEDU:

> ***Alle (management) activiteiten ter waarborging van de beschikbaarheid, vertrouwelijkheid en integriteit van de informatie uitwisselingsprocessen, zoals gedefinieerd binnen de NEDU.***

De vereniging NEDU besteedt aandacht aan informatiebeveiliging om de volgende redenen:

1. De NEDU is een vereniging van alle (erkende) rollen in de Nederlandse energiemarkt, met veel verschillende leden. NEDU definieert de werking van ketenprocessen met informatieuitwisseling tussen de ketenpartijen. Voorbereid zijn op compromitteren van de informatievoorziening is daarbij noodzakelijk.
2. Informatiebeveiliging op maat: meer dan voorheen gebaseerd op sector requirements, die in lijn zijn met de risico-inschatting van de leden binnen de NEDU.
3. Informatiebeveiliging wordt nogal eens gezien als een beperkende factor, terwijl adequate security requirements in de design fase juist kunnen bijdragen aan plezieriger werken, voldoen aan wetgeving en een snelle delivery maar ook dure aanpassingen achteraf voorkomen.
4. Datakwaliteit en informatiebeveiliging gaan hand in hand. Effectief beschermde informatieuitwisseling en bijhorende systemen vergroten de datakwaliteit en reduceren de inspanning die de sector moet verrichten op het gebied van beheer.

De ambitie van de informatiebeveiliging is een passende mate van informatieveiligheid, die wordt bepaald op basis van beschikbaarheid, integriteit en vertrouwelijkheid classificatie (BIV[1]) van de informatie uitwisselingsprocessen

Informatiebeveiliging werkt vanuit zowel een preventieve als responsieve aanpak. Het gaat om treffen van preventieve maatregelen en het voortijdig signaleren van bedreigingen voor de informatie uitwisselingsprocessen binnen de NEDU en het adequaat opvangen van de gevolgen van inbreuken op de informatie uitwisselingsprocessen. De leden van de NEDU treffen die set van preventieve en correctieve maatregelen, die een adequate graad van bescherming voor de informatie uitwisselingsprocessen garanderen.

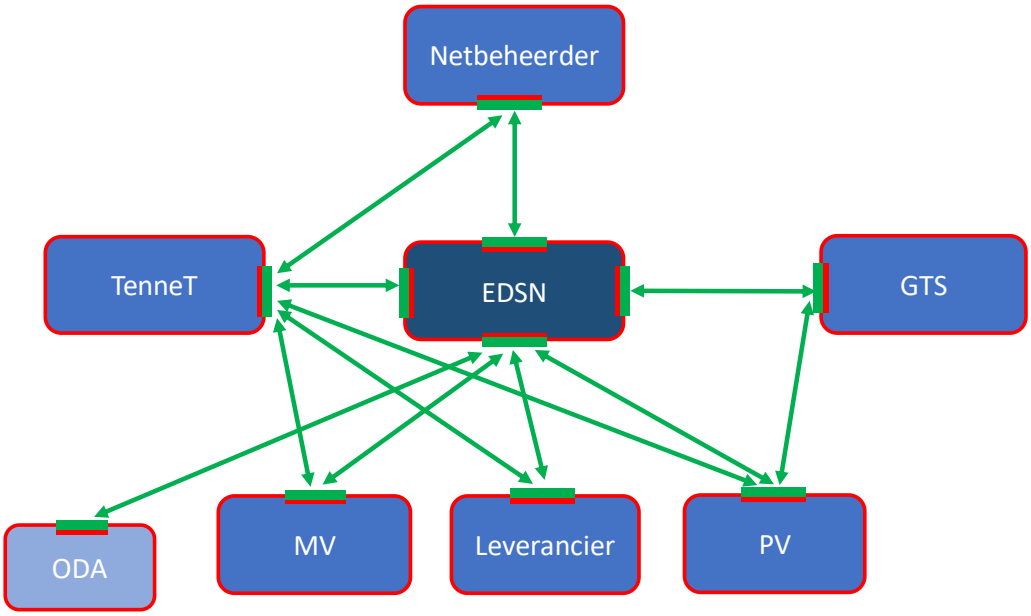
Dit document werkt het security beleid ten behoeve van de informatie uitwisselingsprocessen nader uit in de vorm van:

- Beschrijving van de scope van het informatiebeveiligingsbeleid;
- Governance die hier bij hoort;
- Principes die hierop van toepassing zijn.

[1] *Beschikbaarheid: Informatie is tijdig aanwezig om te gebruiken zodra dat nodig is.*
Integriteit: Informatie is over tijd controleerbaar authentiek en onveranderd.
Vertrouwelijkheid: Informatie is uitsluitend vindbaar, benaderbaar en toegankelijk voor daartoe aangewezen personen.

2 SCOPE

Het informatiebeveiligingsbeleid is van toepassing op alle informatie uitwisselingsprocessen zoals gedefinieerd binnen de NEDU. Binnen het gebied van het uitwisselen van keteninformatie (en de bijbehorende processen) conformeert iedere partij, die een bijdrage levert aan deze informatievoorziening, zich aan het beleid. Iedere partij draagt daarbij zelf de verantwoordelijkheid dat er invulling wordt gegeven aan het beleid voor het deel dat onder zijn verantwoordelijkheid valt. In het onderstaande figuur[2] is de scope schematisch weergegeven. De groene markeringen geven weer waarop de scope betrekking heeft. In hoofdstuk 4 wordt dit door middel van de principes nader geconcretiseerd.



Het beleid kan daarbij invloed hebben op zowel (proces)technisch als business/organisatorisch vlak. Denk hierbij aan communicatieprotocollen en –kanalen en de invulling van adequaat Identity en Access Management ten behoeve van de communicatie.

Invulling geven aan de AVG valt niet binnen de scope van de security commissie. Eventuele security maatregelen als gevolg van de AVG worden in de issuecommissies bepaald in afstemming met de Security Commissie.

[2] Situatie na invoering van C-ARM en Nexus

3 GOVERNANCE

Het informatiebeveiligingsbeleid wordt opgesteld door de Security Commissie. De leden van de Security Commissie zorgen ervoor dat het beleid is afgestemd met de eigen organisatie. Na akkoord van de Security Commissie wordt het beleid via de voorzitter van de Security Commissie ter bekrachtiging voorgelegd aan de Algemene Leden Vergadering.

Ten minste jaarlijks of indien omstandigheden daar aanleiding toegeven worden het informatiebeveiligingsbeleid door de security commissie en de daarop gebaseerde principes & richtlijnen geëvalueerd. Indien aanpassingen nodig zijn dan wordt het voorgaande proces gevolgd. Voorbeelden van externe ontwikkelingen zijn veranderende wetgeving, nieuwe richtlijnen vanuit best practices, incidenten en verandering in het dreigingsbeeld.

Om 'security by design' goed te beleggen zoekt de security commissie aansluiting bij de issue commissies, zodat de security aspecten al bij het uitwerken van business oplossing worden meegenomen.

Bij het opstellen van advies vanuit de Security Commissie wordt zoveel mogelijk rekening gehouden met lopende initiatieven. Samenwerking zal daar waar relevant worden gezocht met andere commissies binnen de NEDU.

De issue commissies zijn verantwoordelijk voor het uitvoeren van risico analyses. De security commissie levert ondersteuning bij de risico analyses op het gebied van security risico's. Op basis van de vastgestelde risico's stelt de security commissie maatregelen voor die het risico kunnen mitigeren. Het al dan niet doorvoeren van maatregelen valt onder de verantwoordelijkheid van de issue commissie.

4 PRINCIPES

Security principes zijn de basis van de uiteindelijk te implementeren maatregelen (in nog te benoemen document). De principes geven richting aan alle verdere acties op het gebied van security, zoals richtlijnen, processen en techniek.

De principes beschrijven wat beoogd wordt, de leden bepalen zelf hoe hier concreet invulling aan te geven, richtlijnen geven hierbij handvatten. De concrete invulling is de verantwoordelijkheid van de individuele leden. Vanuit de Security Commissie is dus geen actief toezicht op de verschillende individuele leden.

Het beveiligingsbeleid voor informatie uitwisselingsprocessen wordt gestoeld op een aantal basisprincipes:

Ref-ID	Omschrijving	Toelichting
SP-01	Risico gebaseerd	Aanvullende maatregelen worden getroffen op basis van een proces voor risico analyse. Periodiek en op basis van veranderende omstandigheden.
SP-02	Minimale rechten	Alleen noodzakelijke rechten worden toegekend
SP-03	Proportionaliteit	Maatregelen zijn proportioneel tot hun doel
SP-04	Defense in depth	Vertrouw niet op enkelvoudige security oplossingen
SP-05	Bescherming aan de bron	Plaats bescherming zo dicht mogelijk bij het te beschermen object
SP-06	Beveiliging vanaf ontwerp (security by design)	Bouw beveiliging in vanaf het ontwerp
SP-07	Eenvoud van ontwerp	Kies voor een simpele oplossing
SP-08	Open ontwerp	Ontwerpen zijn bestand tegen openbaarheid
SP-09	Gelijke sterkte	Gelijkwaardige schakels in de security keten moeten even sterk zijn
SP-10	Scheiding van diensten	Scheid componenten met verschillende security profielen van elkaar. De data in een informatieuitwisseling dient van gelijkwaardig niveau te zijn.
SP-11	Gemeenschappelijk mechanisme	Gebruik zoveel mogelijk één standaard mechanisme
SP-12	Altijd voldoende security	Implementeer nu wat er nu mogelijk is, en blijf up-to-date
SP-13	Security is aantoonbaar en traceerbaar	Security maatregelen zullen niet altijd afdoende werken maar aangetoond kan worden dat maatregelen aanwezig zijn.

Deze basis principes zijn verder uitgewerkt in het document “Security principes en richtlijnen”.