Procedure

Beveiligingsincidenten

Inhoudsopgave

1 Inleiding

Deze procedure beschrijft hoe te handelen indien er sprake is van een beveiligingsincident waarin er bij één of meerdere marktpartijen sprake is van een beveiligingsincident dat vermoedelijk impact heeft op de informatie-uitwisseling en de ketenprocessen in de sector, de centrale marktfaciliterende systemen of een beveiligingsincident binnen EDSN zelf.

1.1 Referenties

Ref	Titel	Eigenaar	Datum	Versie	Status

1.2 Afkortingen

Afkorting	Omschrijving
BCM	Business Continuity Management

1.3 Versiebeheer

Versie	Status	Wijziging	Auteur	Datum
1.0	Definitief	Initiële definitieve versie	Bart Baars	
1.1	Concept	Actualisatie en migratie naar nieuw template	Bart Baars	30-08-2016
1.2	Ter finale review	Aanpassingen voor sector breed gebruik	Bart Baars, Gerrit Fokkema	20-12-2016
1.3	Ter vaststelling	Enige review aanscherpingen	Bart Baars, Gerrit Fokkema	06-01-2016

2 Doel & definities

2.1 Doel

Het doel van deze procedure is om zeker te stellen dat de gevolgen van optredende beveiliging incidenten worden geminimaliseerd. Tevens beoogt de procedure er voor zorg te dragen dat vergelijkbare incidenten in de toekomst worden voorkomen.

2.2 Scope

Deze procedure is van toepassing op alle NEDU gebaseerde ketenprocessen met de informatieuitwisselingen daarbinnen en EDSN bedrijfsmiddelen waarop het EDSN informatie-beveiligingsbeleid van toepassing is. De procedure is niet van toepassing op situaties die vallen onder Business Continuity Management (BCM, bij grote calamiteiten).

Indien van toepassing kan aansluitend op deze procedure de Procedure Meldplicht Datalekken worden ingeschakeld.

2.3 Doelgroep

Alle NEDU marktpartijen (incl. netbeheerders), EDSN en toeleveranciers, met betrekking tot activiteiten ten aanzien van alle NEDU gebaseerde ketenprocessen en de gegevensuitwisseling daarbinnen alsmede de centrale marktfaciliterende systemen of interne bedrijfsvoering van EDSN.

2.4 Definities

Hieronder staan definities die voor deze procedure van belang zijn.

Term	**Definitie/omschrijving**
Gebeurtenis	Een situatie waarvan na onderzoek vast is komen te staan dat het weinig of geen impact heeft op de ketenprocessen, de organisaties of de beveiliging van bedrijfsmiddelen.
Incident	Een gebeurtenis of serie van gebeurtenissen met (een hoge kans op) impact op de veiligheid van de ketenprocessen, de organisatie of bedrijfsmiddelen.
Zwakheid	Een (softwarematige) tekortkoming in bedrijfsmiddelen of in veiligheidsmaatregelen.
Categorie onbekend	Een gebeurtenis of incident waarvan na onderzoek de categorie niet eenduidig vast te stellen is.
Verantwoordelijke	De persoon (zijnde een natuurlijke persoon, rechtspersoon of ieder ander of een bestuursorgaan) die, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

3 Communicatie

Een goede communicatie is van belang voor het goed en snel oplossen van een incident en de gevolgen ervan. Dat is ook de reden dat er een centrale incidentenprocedure wordt ingevoerd, met een centrale melding. Na de intake van de melding zal er met betrokken partij(en) of marktrollen of alle marktrollen contact worden opgenomen dan wel gecommuniceerd. Hiervoor zal uitsluitend gebruik worden gemaakt van de in de CPR contact groep 'Incidenten Procedure" geregistreerde contacten. Partijen dienen er zorg voor te dragen dat de geregistreerde contacten voldoende goed bereikbaar zijn.
De specifieke communicatie is van geval tot geval verschillend en afhankelijk van de ernst van het incident. De communicatie wordt onderstaand in de procedure beschrijving geduid.

4 Procedure Beveiligingsincidenten

De procedure beveiligingsincidenten bestaat uit de volgende vijf stappen, met daarbinnen meerdere sub-stappen.

1. Registreren van een incident

1.1 Ontvangen melding incident

Het aanmelden van een incident kan gedaan worden door:

- Alle medewerkers van marktpartijen, inclusief netbeheerders;
- Alle medewerkers van EDSN;
- Alle medewerkers van IT leveranciers van EDSN;
- Buitenstaanders.

De EDSN ServiceDesk is op de volgende manieren bereikbaar:
Telefonisch: 0900 - BELEDSN (0900 235 3376)
E-mail: servicedesk@edsn.nl

De Servicedesk geeft aan de melder aan wat er met de melding wordt gedaan en hoe dit op de melder wordt terug gekoppeld.

1.2 Registratie melding incident

Binnen EDSN worden alle meldingen van incidenten geregistreerd bij de ServiceDesk van EDSN. De medewerker van de ServiceDesk registreert de melding van een (vermoedelijk) beveiligingsincident in het incidentenregistratiesysteem van EDSN.

De EDSN ServiceDesk registreert minimaal de volgende gegevens:

- Naam van de melder;
- Organisatie(onderdeel) van de melder
- Functie van de melder;
- Datum melding;
- Welk proces of systeem de melding betreft;
- Wie heeft waargenomen;
- Datum en tijdstip incident;
- Beschrijving incident.

1.3 Beoordelen melding incident

De EDSN ServiceDesk beoordeelt of er sprake is van een beveiligingsincident. Voor een beveiligingsincident wordt de onderstaande definitie gebruikt:
Een beveiligingsincident is een gebeurtenis of serie van gebeurtenissen met (een hoge kans op) impact op de veiligheid van de ketenprocessen, de organisatie of bedrijfsmiddelen, dus waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie of informatieuitwisseling in de sector of informatieverwerkende systemen in gevaar is of kan komen.

Enkele voorbeelden van beveilingingsincidenten zijn:

- Verliezen van services, functionaliteiten of andere faciliteiten;
- Verlies van een laptop met daarop vertrouwelijke informatie;
- Systeem-, software- of hardware storingen;
- Non-compliancies (niet voldoen aan wetgeving of regelgeving zoals bijvoorbeeld informatie beveiligingsbeleid);
- Inbraak(pogingen) of andere fysieke beschadigingen;
- Ongeautoriseerde toegang tot systemen, software en/of fysieke locaties.

Bij de beoordeling van een incident spelen factoren een rol als welke (keten)processen in welke mate worden verstoord, het belang van die processen, het aantal betrokken marktpartijen, aantal marktrollen of de gehele sector, het belang van en het aantal getroffen systemen en/of dataverzamelingen.

Indien er sprake is van een beveiligingsincident waarbij (vermoedelijk) persoonsgegevens betrokken zijn, wordt de Procedure Meldplicht Datalekken gebruikt. In dat geval wordt er niet verder gegaan met deze procedure. De incidentmelding blijft dan wel open staan tot het incident afdoende is afgehandeld.

2. Classificeren en prioriteren beveiligingsincident (triage)

Alle beveiligingincidenten worden direct na registratie door de ServiceDesk doorgezet naar de Security Administrator.

2.1 Classificeren

De Security Administrator classificeert en categoriseert conform de categorieën uit het meldingsformulier:

- Onbekend;
- Zwakheid;
- Gebeurtenis;
- Incident.

Meldingen geclassificeerd als ‘Onbekend’ verdienen nader onderzoek om toch zo snel als mogelijk de oorzaak te kunnen achterhalen.

Als er meerdere meldingen van dezelfde categorie binnenkomen, zal de Security Administrator de Security Officer inschakelen. De Security Officer zal op basis van classificatie/impact van het bedrijfsmiddel, kans op verspreiding/besmetting binnen de infrastructuur, en de beschikbare resources de prioritering bepalen.

2.2 Impact bepalen

Tevens bepaalt de Security Administrator direct na registratie van het incident in welke impactcategorie deze valt. Deze categorie bepaalt met welke prioriteit het incident wordt afgehandeld en welke vervolgstappen er worden genomen.

Impact: Laag

Bij incidenten met een lage impact bestaan er geen directe nadelige gevolgen voor processen binnen

de sector of EDSN. De afhandeling wordt binnen de afdeling EDSN Beheer belegd. Deze pakt het incident op naast de normale werkzaamheden.

Incidenten met deze impact worden opgepakt en afgehandeld tijdens kantooruren.

Impact: Midden
Het incident heeft enige invloed op de processen binnen de sector en/of EDSN of de informatievoorziening in de sector en/of in het kader van centrale marktfacilitering. Het oplossen van het incident heeft prioriteit. Tenminste eenmaal per werkdag stemmen de direct betrokkenen bij het incident af over de status en de oplosrichting. De Security Administrator of Manager Beheer heeft de leiding over voortgang en afhandeling van het incident.

Incidenten met deze impact worden opgepakt en afgehandeld tijdens kantooruren.

Indien de informatievoorziening in de sector en/of in het kader van de centrale marktfacilitering wordt geraakt, neemt de Security Officer contact op met de Security Officers van de betrokken marktpartijen om vervolgstappen te bepalen. Hiervoor wordt de contactlijst in het CPR gebruikt.

Impact: Hoog
Processen binnen de energiemarkt of binnen EDSN worden ernstig beïnvloed of verstoord door het incident. Oplossen van het incident heeft prioriteit boven de normale werkzaamheden. Betrokkenen bij het incident verzamelen zich (zo veel als mogelijk[1]) in een aparte ruimte. Vanuit deze ruimte wordt het incident opgelost.

Incidenten met deze impact worden direct opgepakt en ook afgehandeld buiten kantooruren.

De EDSN Security Officer zorgt ervoor dat de betreffende contacten (zoals de Security Officers), zoals geregistreerd in de contactgroep incidentenprocedure van het CPR van alle relevante marktpartijen op de hoogte gebracht van het incident. Hiervoor wordt gebruikt gemaakt van de contactlijst, zoals opgenomen in het CPR. Dagelijks of zo veel meer als nodig is, wordt er een update gegeven. Met de direct betrokken marktpartijen wordt de afhandelingsstrategie bepaald.

Daarnaast stelt de EDSN Security Officer het MT van EDSN op de hoogte van het incident en verstrekt hen minimaal dagelijks een update.

Impact: Catastrofaal
Dit betreft een BCM crisissituatie. BCM en BCM situaties behoren niet tot de scope van dit document.

3. Incident toewijzing en opvolging

De bewijslast wordt direct als zij is verkregen veiliggesteld voor (forensisch) onderzoek om zo snel mogelijk tot een oordeel te kunnen komen en ter ondersteuning van verdere (juridische) acties.

Alle betrokken marktpartijen, medewerkers van betrokken partijen, toeleveranciers, extern personeel e.d. zijn verplicht mee te werken aan het onderzoek en alle relevante informatie op

[1] Om de snelheid van werken en pragmatiek hoog te houden zullen indien nodig diverse communicatie middelen (zoals een vast CoCa-nummer) worden ingezet tussen de betrokkenen.

verzoek beschikbaar te stellen. De EDSN Security Officer zal, voor zover mogelijk, additionele informatie van kundig en specifiek technisch specialisten opvragen om de organisatie te ondersteunen bij het zo snel als mogelijk (her)opstarten van de operationele werkzaamheden en/of het initiëren van de contingency plannen mogelijk te maken.

De Security Officer zal de beveiligingsactiviteiten zoals beschreven in van toepassing zijnde werkinstructies plus alle in zijn ogen relevante activiteiten uitvoeren om de operationele ketenprocessen en/of berichtuitwisseling en/of werkzaamheden en/of de reguliere dienstverlening van EDSN zo snel als mogelijk weer te herstarten.
De Security Officer is verantwoordelijk voor het verlenen van autorisaties op 'verdachte' systemen en/of informatie en dient een formeel akkoord te geven voordat een informatiesysteem en/of infrastructuur weer 'normaal' ingezet kan worden voor de regulierereketenprocessen en EDSN activiteiten en dienstverlening.

Marktpartijen worden conform gemaakte afspraken in stap 2 (paragraaf 2.2) aangehaakt. Voor verdere communicatie, zowel binnen de energiemarkt als daarbuiten, wordt aangehaakt bij het (nog te ontwikkelen) NEDU crisiscommunicatieplan. Geen van de betrokken partijen zal zonder overleg op basis van het crisiscommunicatieplan, op eigen initiatief contact zoeken met de pers[2].

4. Afsluiting incident

Zodra de impact onder controle is gebracht en alle correctieve acties zijn doorgevoerd zal het incident worden afgesloten. De Security Officer stelt over het beveiligingsincident een volledig rapport op. Dit rapport bevat de volgende onderwerpen:

- Samenvatting van het incident;
- Oorzaak van het incident;
- Analyse van de gebeurtenissen en impactanalyse;
- Welke acties er genomen zijn;
- Voorstellen eventuele verbeterpunten;
- Effectiviteit van huidige procedures en werkinstructies;
- Afsluiting van incident;
- Eventuele vervolgacties.

Het rapport wordt onverwijld ter beschikking gesteld aan de manager Beheer en alle bij het incident betrokkenen partijen en Security Officers. Tevens wordt het rapport centraal gearchiveerd.

De Security Officer sluit het beveiligingsincident daarna formeel af en informeert relevante interne en externe partijen over de sluiting. Daarnaast stelt de Security Officer correctieve maatregelen op en organiseert de implementatie van deze maatregelen.

5. Rapportage

Maandelijks stelt de Security Officer een beveiligingsincidenten rapportage op. Hierin zijn alle open en afgesloten beveiligingsincidenten met impact op de sector opgenomen. Het rapport stelt hij ter beschikking aan de NEDU Security Commissie en de manager Beheer van EDSN. Tevens wordt het rapport centraal gearchiveerd.

[2] In het communicatieplan zal ook worden opgenomen welk gedrag partijen richting pers zullen volgen mochten ze door de pers worden benaderd aangaande het incident.