Gedragscode Responsible Disclosure

1 Reikwijdte

- Deze Gedragscode Responsible Disclosure richt zich op een procedure voor het melden van vermoedelijke beveiligingsproblemen en het verantwoord openbaar maken daarvan (hierna: "**Responsible Disclosure**");
- Deze Gedragscode Responsible Disclosure is van toepassing op zowel PZEM als de melder van een beveiligingsprobleem of kwetsbaarheid;
- Hetgeen afgesproken in deze code laat wettelijke verplichtingen onverlet.

2 Definities

- Een melding betreft het door een melder aan PZEM melden van een vermoedelijk beveiligingsprobleem op een verantwoorde wijze;
- De melder is de persoon of instantie die een melding doet;
- PZEM produceert, verhandelt en levert energie aan MZM en GZM;
- Een beveiligingsprobleem of kwetsbaarheid is een (vermoedelijke) zwakte in of inbreuk op de beveiliging van de infrastructuur of ICT-systeem van het bedrijf;
- Op verantwoorde wijze melden houdt in dat de melder het beveiligingsprobleem of kwetsbaarheid meldt via het proces zoals dat door PZEM wordt gehanteerd.

3 Aanleiding

PZEM neemt veiligheid uiterst serieus. Voor PZEM staat het vertrouwen in dienstverlening bovenaan. PZEM heeft een eigen verantwoordelijkheid om beveiliging op een passende wijze te waarborgen. PZEM werkt daarnaast gezamenlijk met andere bedrijven in de energiesector aan het vergroten van de beveiliging. PZEM is voor de continuïteit van dienstverlening afhankelijk van complexe ICT-systemen. De privacy van gebruikers en klanten van PZEM is van groot belang, net als de vertrouwelijkheid van communicatie en informatie. Daarom moet voorkomen worden dat onbevoegden toegang krijgen tot de infrastructuur van PZEM of de gegevens van gebruikers en klanten. Om dit te voorkomen investeert PZEM veel in de veiligheid van de infrastructuur. Daarnaast controleert PZEM voortdurend op onregelmatigheden, zoals inbraakpogingen.

Incidenten kunnen diverse oorzaken hebben, zoals menselijke fouten, externe factoren als stroomuitval of kwetsbaarheden in een ICT-systeem. In sommige gevallen worden kwetsbaarheden voortijdig opgemerkt door derden. Met een responsible-disclosure-procedure wil PZEM het makkelijker maken voor derden om vermoedelijke beveiligingsproblemen te melden. Hiermee hoopt PZEM problemen sneller te herstellen en te voorkomen dat informatie in de verkeerde handen valt.

Er kan verschil ontstaan in de wijze van opvolging van meldingen. Zo is een bekende kwetsbaarheid, waarvoor al een beveiligingsupdate bestaat eenvoudiger te dichten dan een nieuwe kwetsbaarheid die voor het eerst aan het licht komt. Ervaring met responsible-disclosure-programma's van internationale ICT-bedrijven leert dat het verhelpen van sommige nieuw ontdekte kwetsbaarheden van enkele maanden tot meer dan een jaar kan duren. De snelheid waarmee een kwetsbaarheid kan worden verholpen, kan dus sterk verschillen.

4 Responsible-disclosure-procedure

De intentie van deze procedure is het ervoor zorgen dat het voor derden helder is hoe zij op een verantwoorde wijze kwetsbaarheden in de beveiliging van de infrastructuur en ICT-systemen van PZEM kunnen rapporteren. Met het onderschrijven van deze gedragscode hanteert PZEM de volgende uitgangspunten en procesafspraken voor responsible disclosure:

4.1 De uitgangspunten

- PZEM zorgt voor een voor derden duidelijke proces en eigen meldpunt om beveiligingsproblemen en kwetsbaarheden te rapporteren. PZEM zorgt voor een bekendmaking van dit proces, bijvoorbeeld door het te plaatsen op de corporate website, eventueel met uitleg en randvoorwaarden;

- PZEM zorgt ervoor dat de procesafspraken op relevante plekken in de organisatie bekend zijn en worden nageleefd;

- De melder van een kwetsbaarheid en PZEM spreken af op welke termijn duidelijkheid geboden zal worden over de wijze waarop de kwetsbaarheid verholpen kan worden;

- De melder van een kwetsbaarheid en PZEM spreken af of en op welke wijze er publiciteit wordt gezocht;

- De persoonsgegevens van een melder worden zorgvuldig behandeld en gewist zodra de melding afgerond is. Hierbij worden de AVG-regels in acht genomen. Er wordt vooraf aan de melder toestemming gevraagd, wanneer zijn persoonsgegevens gedeeld zullen worden met derde partijen.

4.2 De procesafspraken voor een melding

- PZEM zorgt ervoor dat een kwetsbaarheid op een toegankelijke manier gemeld kan worden. Op de website pzem.nl staan de stappen uitgelegd;

- De melder zelf moet duidelijk benoemen wat het onderwerp is en de melding moet vergezeld gaan met bewijsmateriaal ten behoeve van de handelingsperspectief voor PZEM;

- De melding mag anoniem worden gedaan;

- PZEM informeert de melder over de termijn waarop de kwetsbaarheid verholpen zal zijn en maakt afspraken met de melder hoe eventueel de publiciteit wordt gezocht. PZEM houdt hier rekening met de AVG-belangen van de melder.

4.3 Het aangiftebeleid

- PZEM zal niet tot aangifte overgaan indien de melder geen misbruik heeft gemaakt van de gevonden kwetsbaarheid en niet voortijdig de publiciteit is gezocht;

- Als blijkt dat voor of na de melding door de melder misbruik is gemaakt, kunnen de procesafspraken voor responsible disclosure niet worden gevolgd en kan PZEM ervoor kiezen toch aangifte doen;

- Onder misbruik van de kwetsbaarheid valt onder meer het bemachtigen van gegevens (anders dan nodig is om kwetsbaarheid aan te tonen), manipulatie van informatie, wijziging van de netwerkconfiguratie en het kennis nemen dan wel openbaar maken van (vertrouwelijke) gegevens;

- PZEM hoeft de procesafspraken voor responsible disclosure niet te volgen als blijkt dat de aanvaller zich middels social engineering naar binnen heeft gepraat of wanneer het een denial-of-service-aanval betreft.

5 Wijze van bekendmaking

PZEM heeft de beschikbare informatie die samenhangt met deze Gedragscode Responsible Disclosure in begrijpelijke bewoordingen en in toegankelijke vorm op één pagina op de corporate website van het bedrijf geplaatst. Op de corporate website van het bedrijf is aangegeven dat het bedrijf de Gedragscode Responsible Disclosure hanteert. De gedragscode is ook te vinden op de corporate website van het bedrijf.

6 Slotbepalingen

Wijzigingen in deze code komen tot stand op initiatief van PZEM en worden gepubliceerd op pzem.nl - op de reguliere webpagina voor het meldpunt beveiligingslekken.