FACTSHEET **VEILIGHEID**

Zeven maatregelen die de veiligheid van Data Safe House garanderen

Om de energietransitie te realiseren, hebben netbeheerders inzicht nodig in de toekomstplannen van de industrie. Die verduurzamingsplannen zijn echter vertrouwelijk. In Data Safe House worden deze plannen veilig opgeslagen en van daaruit gedeeld met partijen die daartoe zijn geautoriseerd. Om de informatie vertrouwelijk te houden, hanteren we een aantal strikte veiligheidsmaatregelen.



1 CISO

Data Safe House heeft een Chief Information Security Officer in dienst: Wil van Egdom. Met zijn jarenlange ervaring heeft hij een uitgebreide risicoanalyse uitgevoerd, om te onderzoeken welke risico's er specifiek voor Data Safe House zijn. Op basis van deze aandachtspunten zijn specifieke veiligheidsmaatregelen genomen voor Data Safe House.

Als CISO blijft hij de veiligheid van onze data en processen monitoren.

2 Best practice om veilig te blijven: ISO 27001

Data Safe House zal over de gehele keten ISO 27001 gecertificeerd zijn. Onze cloudprovider en het IT-platform zijn dat al. De organisatie zelf zit in het proces. In oktober is de certificering formeel afgerond. Onze medewerkers worden daarom nu al in trainingen bewust gemaakt van de informatiebeveiliging.

Met ISO 27001 als erkende norm voor informatie-beveiliging blijven we ook in de toekomst veilig, omdat het werkt volgens een *Plan, Do, Check, Act* cyclus. Veiligheidsmaatregelen zijn inmiddels gepland (*Plan*) en ingevoerd (*Do*). Nu wordt regelmatig *gecheckt* of de beveiliging nog voldoende is, of dat risico's zijn gewijzigd. Als dat zo is, dan is *Actie* vereist om de maatregelen aan te passen. Deze cyclus zorgt dat Data Safe House voortdurend is aangepast aan nieuwe risico's.

3 Audit door onafhankelijke partij

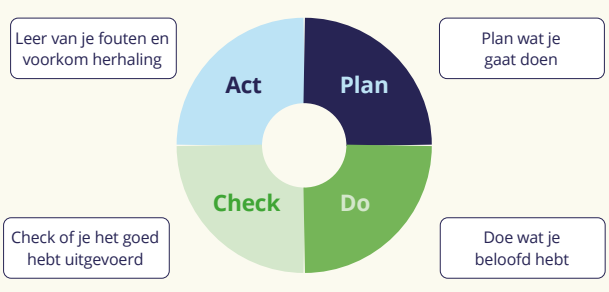
Zowel de techniek als de administratieve processen worden periodiek door een onafhankelijke partij ge-audit om te toetsen of we nog voldoen aan de ISO27001 normen. Ook laten we periodiek een penetratietest van het IT-platform uitvoeren.

4 Beveiliging dataserver

De Data Safe House oplossing is een *three-tier* implementatie. Dat wil zeggen dat de webserver (1), database (2) en de applicatieserver (3) van elkaar gescheiden zijn. Een hacker kan dus niet via de website toegang krijgen tot de gegevens van de deelnemers of tot hun verduurzamingsplannen.

Zelfs als iemand erin slaagt toegang te krijgen tot de database, dan kan hij nog niet bij de data, omdat die allemaal versleuteld opgeslagen zijn. Ook tijdens het verzenden is alle communicatie tussen de verschillende servers versleuteld, zowel op het publieke internet als binnen het datacenter. Alle denkbare maatregelen zijn genomen om afluisteren op de lijn onmogelijk te maken.

PDCA cyclus



Stap voor stap een veilig aanmeldproces



5 Identificatie en toegangscontrole

Iedere gebruiker krijgt toegang op persoonsniveau via tweefactor authenticatie.

6 Autorisatieprofielen op basis van need-to-know

Data Safe House werkt met autorisatieprofielen. Voor elk profiel is nauwkeurig vastgelegd tot welke data deze toegang geeft op een need-to-know basis.

Bedrijven hebben alleen toegang tot hun eigen data en alleen de Data Safe House manager kan alle data inzien van het eigen industriecluster. Andere Data Safe House medewerkers hebben geen toegang tot de data. Data-aanvragers, zoals netbeheerders hebben alleen toegang tot data in het cluster waar zij opereren en voor de energiedrager waarvoor zij de infrastructuur beheren.

Toegang is echter nog geen toepassing. Voor het toepassen van data voor een bepaalde analyse of studie moeten partijen vooraf een specifieke data-aanvraag doen. Binnen de Data Board bespreken de deelnemers de data-aanvraag. Als de aanvrager de data mag gebruiken, dan is dat voor een bepaalde termijn voor het specifieke doel van de aanvraag.

Autorisatie is gebaseerd op het principe van **need-to-know**, alleen toegang tot wat nodig is

Passende autorisatieprofielen worden **beheerd** door de **Data Safe House manager**

Toegekende autorisaties worden **periodiek opnieuw beoordeeld** en waar nodig aangepast

Aan ieder **persoon** (e-mailadres) wordt een autorisatieprofiel toegekend met registratie van een **termijn**

7 Afsprakenstelsel

Bovenop alle technische maatregelen om de vertrouwelijkheid te borgen, heeft Data Safe House Algemene Voorwaarden opgesteld. Met de ondertekening verplichten deelnemende bedrijven zich onder andere dat ze de data vertrouwelijk behandelen en alleen gebruiken voor het doel dat vooraf is afgesproken. Alleen industriepartijen, netbeheerders en netwerkpartijen die deze Algemene Voorwaarden ondertekenen, mogen deelnemen aan Data Safe House.

Vertrouwen: dé succesfactor voor de energietransitie

Het vertrouwen van de industrie dat Data Safe House een veilige omgeving is om verduurzamingsplannen te delen, en het vertrouwen van netbeheerders dat de data correct en volledig is, zijn cruciaal voor het slagen van de energietransitie. Met de 7 bovengenoemde maatregelen hebben we de vertrouwelijkheid zoveel mogelijk geborgd.

Heeft deze factsheet je vertrouwen gegeven dat we veilig omgaan met jullie verduurzamingsplannen? Sluit je dan aan bij Data Safe House. Want hoe meer bedrijven meedoen, hoe sneller netbeheerders kunnen bouwen aan de nieuwe energie-infrastructuur. Zo gaan we samen sneller door de energietransitie!

Doe ook mee en deel je verduurzamingsplannen in Data Safe House!