



Critical Supplier Dependency Sheet

Waar je van afhangt, en hoe lang je zonder kunt

Versie 1.0 · NIS2 · IEC 62443 · AI

Een cyberincident hoeft je netwerk niet binnen te komen om je operatie stil te leggen. **Je firewall doet het, je back-ups zijn goed, en je productie ligt er toch uit.**

Dit blad maakt die afhankelijkheid concreet, per leverancier, in uren en in namen.

Waarvoor dit blad is

Eén blad per kritieke leverancier. Aan het eind staat er een besluit op papier: hoe lang je zonder hen kunt, wat je gaat doen, wie dat draagt en wanneer je het nakijkt.

Hoe je het invult

- **Splits het soort afhankelijkheid uit.** Een licentieserver die stopt is iets anders dan een engineer die niet kan komen, en ze vragen om andere maatregelen.
- **Vul de tolerabele onderbreking als eerste in.** Zolang dat veld leeg is, is elke terugval goed genoeg en gebeurt er niets.
- **Vergeet documentatie en kennis niet.** Die twee worden bijna nooit als leveranciersrisico geteld en zijn het lastigst op te lossen. Een onderdeel leg je op voorraad, kennis niet.
- **Een terugval die niet geoefend is, is een aanname.** Zet erbij wanneer hij voor het laatst echt gedaan is.

Leverancier naam, en wie daar jouw aanspreekpunt is	
Soort afhankelijkheid support / licentieserver / onderdelen / datastroom / documentatie / kennis	
Wat je van hen nodig hebt concreet, niet "ondersteuning"	
Wat er bij jou stilvalt welk proces, en na hoeveel tijd	
Tolerabele onderbreking uren of dagen, en waar dat getal vandaan komt	
Terugval wat doe je zonder hen, en is dat een keer gedaan	
Besluit accepteren / terugval regelen / tweede bron / contract aanpassen	
Eigenaar naam, niet inkoop als afdeling	
Bewijs	

contract, test van de terugval, of vastgelegde afspraak	
Review datum, en wat maakt dat je eerder kijkt	

Zo vul je de lijst in

- Zet een vinkje als het echt geregeld is **en** je het kunt laten zien: een contract, een verslag, een afspraak op papier.
- Nog niet geregeld? Geen vinkje. Dat is geen schande, dat is je startpunt.
- Geldt een regel hier niet? Streep hem door. Hij telt dan ook niet mee in je maximum.
- Achter elke regel staat hoeveel punten hij waard is. Niet elke regel weegt even zwaar.
- Tel aan het eind op wat je hebt. Onder de lijst staat wat dat getal betekent.

NIS2 en de Cyberbeveiligingswet

- | | |
|--|------|
| ☐ Deze leverancier staat in het ketenoverzicht met de andere kritieke partijen. (art. 21 lid 2) | 2 pt |
| ☐ De afhankelijkheid staat in de risicoanalyse, niet alleen in het contract. (art. 21) | 2 pt |
| ☐ Er is getoetst of uitval bij hen bij jou meldingsplichtig zou zijn. (art. 23) | 2 pt |
| ☐ Afspraken over melden bij een incident aan hún kant staan op papier. | 1 pt |
| ☐ Het bestuur kent de vijf leveranciers zonder wie het stilvalt. (art. 20) | 2 pt |

Continuïteit

- | | |
|--|------|
| ☐ De tolerabele onderbreking komt uit een analyse en niet uit een gevoel. (ISO 22301) | 3 pt |
| ☐ De terugval is minstens één keer echt uitgevoerd, met datum. | 3 pt |
| ☐ Er is een scenario voor als zij er langer uit liggen dan jouw termijn. | 2 pt |
| ☐ De contactgegevens werken ook als jouw eigen systemen plat liggen. | 2 pt |
| ☐ Er is een tweede bron overwogen, ook als die duurder is. | 1 pt |

Als het OT of AI raakt

- | | |
|--|------|
| ☐ Toegang op afstand van deze leverancier loopt via een conduit met een eigen doelniveau. (IEC 62443-3-2) | 2 pt |
| ☐ Hun toegang is op naam, tijdelijk, en achteraf te herleiden. (IEC 62443-2-4) | 2 pt |
| ☐ Als zij een AI-functie leveren, staat die in jouw AI-inventaris. (ISO/IEC 42001) | 1 pt |
| ☐ Bij een model van een derde is vastgelegd wat er gebeurt als zij het vervangen. | 1 pt |

Generiek, wat een CISO hoe dan ook nakijkt

- | | |
|---|------|
| ☐ Het contract benoemt beschikbaarheid en herstel, niet alleen levering. | 2 pt |
| ☐ De documentatie die zij beheren staat ook bij jou, actueel. | 1 pt |
| ☐ Er is meer dan één persoon bij jou die weet hoe dit systeem werkt. | 2 pt |
| ☐ De exit is beschreven: wat krijg je mee als je stopt. | 1 pt |
| ☐ Deze afhankelijkheid komt terug in de crisisoefening. | 1 pt |
| ☐ De reviewdatum staat in iemands agenda. | 1 pt |

Wat je uitkomst betekent

Tel je punten op. Alles samen is 34. Deze leverancier staat er dan zo voor:

0 – 16 pu	Deze leverancier kan je stilleggen zonder dat iemand dat ziet aankomen. Begin bij de tolerabele onderbreking en de terugval; de rest volgt daaruit.
17 – 26 pu	Je weet waar je van afhangt, maar bij een incident moet je het nog uitzoeken. Zorg dat de terugval een keer echt is gedaan en dat de contactgegevens werken als je eigen systemen plat liggen.
27 – 34 pu	Deze afhankelijkheid is beheerst en uit te leggen aan je bestuur, een toezichthouder of je verzekeraar. Zet de reviewdatum in een agenda; dit verloopt stilletjes als de leverancier verandert.

Regels doorgestreept? Haal die van het maximum af. De grenzen liggen op de helft en op vier vijfde van wat overblijft.

Vijf fouten die dit blad moet voorkomen

- **Leveranciersrisico als één ding.** Zes soorten, zes maatregelen. Op één hoop leidt tot één generieke afspraak die niets oplost.
- **Geen tolerabele onderbreking.** Zonder dat getal is elke terugval goed genoeg en is er geen aanleiding om iets te regelen.
- **Een terugval op papier.** Nooit uitgevoerd betekent onbekend, niet aanwezig.
- **Alleen naar de grote namen kijken.** De partij die stilvalt is vaak klein en levert één ding dat je nergens anders krijgt.
- **Invullen zonder besluit.** Kies er één van de vier, met een naam en een datum erbij.

NIS2 noemt beveiliging van de toeleveringsketen als onderdeel van de maatregelen en schrijft geen methode voor; de richtlijn geldt niet voor elke organisatie. ISO 22301 gaat over bedrijfscontinuïteit en is geen verplichting onder NIS2. Dit blad is een hulpmiddel en geen norm. Meer op cyberbusters.com/nl/blog.