Algemene Inlichtingen- en
Veiligheidsdienst
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Beleid omgang onbekende kwetsbaarheden

In dit beleid wordt het afwegingskader vastgelegd voor het al dan niet melden van onbekende kwetsbaarheden. Dit beleid betreft alle onbekende kwetsbaarheden waar de Nederlandse inlichtingendiensten AIVD en MIVD op stuiten of over beschikken.

Wat is een onbekende kwetsbaarheid?

Een onbekende kwetsbaarheid is een kwetsbaarheid in een geautomatiseerd werk die kan worden gebruikt om dat geautomatiseerde werk binnen te dringen én waarvan het aannemelijk is of verondersteld kan worden dat die niet bekend bij de producent of leverancier.[1]

Uitgangspunt is 'melden, tenzij…'

In het kader van beveiligingsbevordering melden de diensten onbekende kwetsbaarheden waarop zij stuiten of waarover zij beschikken. In het belang van nationale veiligheid kan er echter voor worden gekozen om de zwakke plekken (tijdelijk) niet te melden, omdat de diensten deze onbekende kwetsbaarheid moeten gebruiken om de dreiging van een kwaadwillende actor te onderzoeken. Het niet melden dient dan het belang van de nationale veiligheid.[2]

Bij iedere onbekende kwetsbaarheid wordt een afweging gemaakt van het belang van het (tijdelijk) niet melden van de kwetsbaarheid in het kader van nationale veiligheid en het belang dat door melden kan worden behartigd.

Wettelijke bepalingen en operationele overwegingen

De wettelijke beperkingen van het melden van een kwetsbaarheid vloeien voort uit de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017). Dit zijn: geheimhouding van actueel kennisniveau, bronbescherming en afschermen van de modus operandi van de diensten (artikel 23 van de Wiv 2017). Indien er wettelijke beperkingen bestaan, wegen deze zeer zwaar in de belangenafweging.

Naast wettelijke beperkingen kunnen er ook operationele bezwaren gelden. Bijvoorbeeld wanneer het aan een belangendrager bekend stellen van een kwetsbaarheid een lopende operatie van de diensten kan schaden, bij de inzet van de onbekende kwetsbaarheid in het kader van een gewapend conflict of als de kennis van een kwetsbaarheid onder voorwaarde van geheimhouding met de Nederlandse overheid is gedeeld.

Afweging

Aan de hand van het afwegingskader wordt gekeken naar de wettelijke bepalingen, operationele overwegingen en belangen die door het melden kunnen worden behartigd.[3] Dit afwegingskader is niet absoluut. De antwoorden op de vragen worden per casus gewogen. Ook wordt er periodiek (in ieder geval jaarlijks) gekeken of de niet gemelde kwetsbaarheid alsnog kan worden gemeld.

De afweging wordt gemaakt door de Commissie Melden Kwetsbaarheden, die onder leiding staat van de directeur-generaal (dg) van de AIVD en de directeur MIVD. De dg AIVD en directeur MIVD informeren de betrokken minister over hun besluit.

Afwegingskader

Om een goede afweging te kunnen maken, wordt per kwetsbaarheid gekeken naar een aantal factoren.

- Risico: hierbij wordt gekeken naar het risico van de kwetsbaarheid voor de Nederlandse samenleving indien de kwetsbaarheid niet wordt gemeld. Dit risico hangt onder andere af van het soort product waar de kwetsbaarheid in zit en waarvoor en hoe wijdverspreid dit product wordt gebruikt. Naarmate het product waar de onbekende kwetsbaarheid in zit meer verspreid is of van groter belang is voor de nationale veiligheid dan wel vitale infrastructuur, zal logischerwijs de ruimte om niet te melden kleiner worden. Daarnaast wordt gekeken naar het risico dat kwaadwillenden de kwetsbaarheid ontdekken en gebruiken met kwade bedoelingen en welke schade dit mogelijk teweegbrengt.
- Wettelijke beperkingen: bekeken zal worden of er sprake is van wettelijke beperkingen uit de Wiv 2017 voor het melden van de kwetsbaarheid. Wettelijke beperkingen zijn: geheimhouding van actueel kennisniveau, bronbescherming en afschermen van de modus operandi van de diensten.
- Noodzaak: bekeken wordt hoe groot de toegevoegde waarde is van het gebruiken van de onbekende kwetsbaarheid voor het onderkennen van dreigingen en of er geen ander lichter middel beschikbaar is die dezelfde gewenste informatie kan opleveren (subsidiariteit).
- Geheimhouding: er wordt nagegaan of de onbekende kwetsbaarheid onder voorwaarde van geheimhouding is gedeeld. Het schenden van zo'n voorwaarde leidt tot het risico dat met deze of vergelijkbare partijen geen zaken meer kunnen worden gedaan, dat risico's voor de nationale veiligheid oplevert.

---

[1] Artikel 126fa Wetboek van Strafvordering zoals voorgesteld in kader CCIII.
[2] Conform Kamerbrief over kwetsbaarheden in hardware en software, 8 november 2016, kenmerk 2008352.
[3] Deze vragen zijn gebaseerd op criteria die in de VS worden gehanteerd bij de afweging een kwetsbaarheid al dan niet te melden, het zogenaamde 'Vulnerabilities Equities Policy and Process for the United States Government, November 15, 2017', beschikbaar via www.whitehouse.gov