**OnePager OSDD**

Cyber Innovation Hub Defensie, Kor Gerritsma - 31 januari 2022

**Context**

Het beveiligen van netwerken is een belangrijk aandachtspunt binnen Cyber. Het verkrijgen van toegang tot netwerken door het onderscheppen of modificeren van het netwerkverkeer zijn de basis voor veel security breeches.

Een van de problemen met het beveiligen van netwerken is te herleiden naar de inrichting van het huidige IP gebaseerde netwerkverkeer. Dit is bi-directioneel (2 richtingen verkeer) omdat er in het protocol gegarandeerde aflevering wordt gevraagd. In lekenwoorden: de zendende partij vraagt om een ontvangstbevestiging van verstuurde data. Zonder ontvangstbevestiging wordt het verzonden pakketje nogmaals verzonden. Door deze opzet is het nodig dat het verzendend netwerk ook een ingang voor het ontvangen van pakketjes heeft.

Voor het beveiligen van netwerken bestaan diverse apparaten of software, zoals Firewalls, Intruder Detection Systems, Intruder Prevention Systems en datadiodes. Allemaal hebben ze specifieke functionaliteit die de netwerk veiligheid verhogen.

**Datadiodes**

Een datadiode is een apparaat waarmee fysiek uni-directioneel (eenrichting) netwerkverkeer wordt afgedwongen. Hiermee ontstaat een aanvullende laag van veiligheid, omdat de diode afdwingt dat verkeer alleen van netwerk A naar netwerk B kan stromen en fysiek natuurkundig onmogelijk terug, waardoor netwerk A in dit geval is beschermd.

**Toepassing van datadiodes**

Omdat een datadiode uni-directioneel verkeer afdwingt is deze toepasbaar in specifieke usecases. Veelal worden datadiodes toegepast in usecases waarbij het onwenselijk is dat er netwerkverkeer terugstroomt van of naar een netwerk.

Dit is bijvoorbeeld het geval in situaties waarin ‘air-gapping’ wenselijk is. Air-gapped betekent dat het netwerk of apparaat afgezonderd van het Internet of andere netwerken moet functioneren. Door datadiodes in dergelijke netwerken te integreren kan er op veilige wijze (uni-directioneel) worden gecommuniceerd en wordt het risico vermeden dat onwenselijk verkeer terug of uitzonder dat het netwerk kan worden aangetast.

**Usecases**

Datadiodes zijn goed toepasbaar in air-gapped HGI-netwerken, waarbij wel de behoefte is om berichten te verzenden naar andere netwerken zonder dat het deze netwerken kunnen reageren. Hiermee wordt de integriteit van het verzendende netwerk maximaal geborgd zonder dat er wordt ingeboet op de capaciteit om gegevens te verspreiden.

Datadiodes zijn ook goed toepasbaar in IOT en PLC (industrie netwerken), waarbij het device om veiligheidsredenen niet mag worden benaderd, maar waar wel behoefte is aan het monitoren of het uitlezen ervan. Dit is bijvoorbeeld de situatie in de kritische infrastructuur (energienetwerken, waterzuiveringsinstallaties, sluizen, etc.).

**Behoefte**

Binnen Defensie is behoefte aan datadiodes in het HGI domein, maar ook in domeinen die zich meer gedragen als een IoT / PLC netwerk.

Voor de HGI netwerken wordt in de behoefte voorzien door NBV geaccrediteerde datadiodes. Deze datadiodes zijn echter relatief kostbaar en worden in lage volumes afgenomen.

Voor het IoT, PLC of operationele domein is behoefte aan robuuste datadiodes die in hoge volumes worden ingezet en potentieel ook verloren mogen gaan. Hierdoor is de businesscase op basis van geaccrediteerde diodes op een hoog volume inzet in het IoT/ PCL of operationele domein niet te maken.

Dit betekent: er is behoefte aan een goedkopere maar toch veilige en robuuste datadiode.

Om in deze behoefte te voorzien is de OSDD ontwikkeld.

**De OSDD**

De OSDD is een mid-tier, low-cost, open source datadiode gericht op gebruik bij publieke en private partijen in Nederland. De OSDD bestaat uit een Hardware apparaat, de fysieke diode, en een software suite waarin aanvullende functionaliteit kan worden geprogrammeerd voor specifieke usecases.

De OSDD demonstrator is ontwikkeld in een samenwerking tussen het Ministerie van Defensie, the Hague Security Delta en Technolotion.

**Accreditatie**

Op de OSDD is door het NBV in een eerste beoordeling aangegeven dat op basis van het huidige ontwerp een beveiliging waarde van Dep-V haalbaar moet zijn.

**Stand van zaken**

Momenteel is er een demonstrator van zowel de fysieke diode als ook de software stack beschikbaar en wordt er geëxperimenteerd voor de doorontwikkeling van beide. Voor de fysieke diode loopt een experiment met het toepassen van verbeterd ontwerp, verder beveiligde chips en het fysiek verkleinen van het doosje. Aan de software wordt momenteel geëxperimenteerd met industrieprotocollen, het verhogen van de doorvoersnelheden en het inzetten van diodes in een dual un-directioneel ontwerp.

De OSDD heeft inmiddels een field test in een hoogspanningsstation van Enexis succesvol doorstaan. Enexis is een actieve partner geworden en heeft uitgesproken bij te willen dragen in de doorontwikkeling van de OSDD en deze ook af te willen nemen zodra de diode in productie gaat (in hoge volumes).

Met een aantal Nederlandse bedrijven wordt onderzocht of er een gezamenlijke (open) innovatie community kan worden opgezet om de datadiode verder te ontwikkelen en marktrijp te maken. Het gaat daarbij om zowel de hardware als software doorontwikkeling.

De opensource ontwikkel community zijn we met bedrijfsleven aan het vormgeven. Als Defensie en CIH willen wij daarbij betrokken blijven en ook een actieve bijdrage leveren. Een investering vanuit Defensie/Rijksoverheid zal dat proces versnellen.