

Onderstaande tekst geeft de essentie uit een e-mail weer.

Doel van de firewall in een VRI

Aan het VRI systeem wordt een netwerkfirewall systeem toegevoegd die de besturingsunit van de VRI beschermd tegen malware, manipulatie en crashes via de externe netwerkaansluiting. De interne componenten worden allen via het firewall systeem op het besturingsnetwerk (VOR-IN) aangesloten.

Al het verkeer van- en naar de VRI wordt gefilterd en geïnspecteerd door de firewall. Het gedrag is standaard “dicht tenzij functioneel noodzakelijk”. Uitsluitend noodzakelijk verkeer wordt doorgelaten.

Het systeem houdt een activiteiten logboek bij en kan deze logging ook geautomatiseerd op het besturingsnetwerk beschikbaar stellen bijvoorbeeld in de vorm van het syslog protocol.

Het firewall systeem wordt in de VRI systeemkast geplaatst en voldoende fysiek afgeschermd zodat manipulatie van de netwerkbekabeling, het aftappen van in-en uitgaande datastromen, of het wijzigen van de configuratie via een aanwezige console poort niet eenvoudig mogelijk is. Netwerkbekabeling kan bijvoorbeeld weggewerkt worden in kabelgoten en het kan fysiek erg moeilijk gemaakt worden de bekabeling te wijzigen door bijvoorbeeld niet gebruikte aansluitingen uit te schakelen en/of af te doppen. Hiermee wordt dan bij geopende systeemkast ook het interne netwerk achter de firewall beschermd.

Het firewall systeem wordt als een intrinsiek onderdeel van de VRI gezien en vormt het koppelvlak met het besturingsnetwerk. Dit is ook het punt waarop de verantwoordelijkheden gedeeld worden. De VRI leverancier is verantwoordelijk voor het leveren van een cybersecure apparaat en daarmee ook voor de veilige configuratie en periodiek onderhoud van het firewall systeem. De leverancier heeft uiteraard mogelijkheden nodig om het VRI systeem over het netwerk te kunnen onderhouden en gebruiken. Het is niet toegestaan hiervoor een secundaire verbinding, bijvoorbeeld op VPN basis, te gebruiken omdat hiermee een “backdoor” situatie ontstaat ten aanzien van het besturingsnetwerk. De gemeente stelt de nodige voorzieningen beschikbaar om de leverancier het beheer en onderhoud van de installatie te kunnen laten uitvoeren. Gedacht kan dan bijvoorbeeld worden aan een beveiligde telewerkvoorzieningen en toegang tot managementsystemen of bedienposten waarmee het onderhoud uitgevoerd kan worden.

Vertaald in een lijst met functionele eisen voor alleen het te selecteren firewall systeem wordt dit:

1. Industrieel temperatuurbereik
2. Markt conform product dat eenvoudig onderhoudbaar en vervangbaar is.
3. Uitgebreide logging faciliteiten
4. Niet gebruikte functionaliteit moet uit te schakelen zijn. (dus ook niet gebruikte ethernet en console aansluitingen)
5. Detectie en bescherming tegen (D)DOS attacks, flooding, brute forcing etc.

Wij hebben gekeken naar routers met firewall functie. Deze voldoen naar ons idee niet voor toepassing in een VRI.

Zonder de leverancier voor te schrijven welk model firewall hiervoor wel noodzakelijk is, hebben we gekeken naar wat hier zoal voor op de markt te koop is. Er zijn verschillende fabrikanten die industriële firewall producten leveren. Als **voorbeeld** staan hieronder een paar linkjes naar de industriële firewall producten van Hirschmann. Vooral de Eagle-20/30 of Eagle-40 serie zouden we voor onze omgeving geschikt achten. In het pdf document in de hyperlinks staat een vergelijkingstabel van functionaliteiten en daarbij zie je bij de duurdere modellen de opties voor logging en auditing die in onze ogen geschikt zijn. Automatische security updates is ook zo’n functie, die essentieel is. Deze apparaten zijn er in een groot aantal poortvarianten te koop.

https://hirschmann.com/en/Hirschmann_Produkte/Industrial_Ethernet/security-firewall/index.phtml

https://www.belden.com/hubfs/emea/resources/Picture%20Park%20Assets/Download%20Center%20PDFs%20-%20Going%20Live/Industrial%20Network%20Security%20Systems_Original_96107.pdf

https://hirschmann.com/en/Hirschmann_Produkte/Industrial_Ethernet/security-firewall/eagle40-video/index.phtml