Artikel Binnenlands Bestuur: Waterschappen worstelen met beveiligingsupdates sluizen

(8 december 2017)

Achtergrondinformatie

In het artikel wordt ingegaan op de security aspecten van de toepassing van PLC's in sluizen, gemalen en andere objecten. Er kan niet genoeg aandacht worden besteed aan een onderwerp als cyber security, aangezien wij allen regelmatig verhalen horen of berichten lezen over de veiligheid van kritische infrastructuur. Binnen de bedrijfsvoering van TMX vormt cyber security een zeer belangrijk onderdeel. Inhoudelijk wil TMX ingaan op een aantal aspecten uit dit artikel.

- Legacy hardware is een groot probleem in de industriële automatisering. Er wordt doorgaans een afschrijvingstermijn van 25 tot 30 jaar gehanteerd op elektrische installaties. Wij adviseren hardware (onderstations) niet te rekenen tot elektrische installaties. Het is beter om voor onderstations een economische afschrijvingstermijn van 10 jaar te hanteren. Moderne onderstations zijn eigenlijk computers. Dit advies heeft ook te maken met de verdergaande ontwikkeling van nieuwe communicatietechnieken en de ontwikkeling op het gebied van cyber security, waardoor een periode langer dan 10 jaar niet reëel is. Ter vergelijking: IT-afdelingen schrijven computers af in een periode van drie tot maximaal vijf jaar.
  Bovendien spelen ook andere ontwikkelingen, zoals telecom, een rol. Een klein voorbeeld is de verdere ontwikkeling van 2G, 3G naar 4G en verder.

- TMX software wordt voor een lange termijn ondersteund. De beperking is vaak de hardware mogelijkheden. Hierbij kan gedacht worden aan de technische levensduur van componenten, de beperkte processorkracht naar huidige maatstaven en toenemende security risico's.

- De veiligheid van telemetriesystemen is op te splitsen in drie aandachtsgebieden: de hoofdpost, de verbindingen en de onderstations. Voor al deze gebieden biedt TMX oplossingen. Zo wordt de communicatie tussen de webbrowser van de gebruiker en de TMX-Net Pro servers standaard versleuteld middels een SSL-certificaat (net als bij bijvoorbeeld elektronisch bankieren) en kan alle datacommunicatie worden afgeschermd van het overige dataverkeer middels VPN en/of APN. Standaard is op deze wijze de communicatie veilig afgeschermd.

- TMX benadrukt actief bij haar klanten om regelmatig te patchen. Softwareonderhoud is en blijft noodzakelijk om de kwaliteit en security te waarborgen, zowel bij de TMX hoofdpost als ook de TMX onderstations. Firmware is op afstand te updaten (FOTA) voor alle moderne TMX onderstations en dataloggers.

- TMX wordt met enige regelmaat ge-audit door partijen als FoxIT, in opdracht van TMX gebruikers. TMX heeft zich ten doel gesteld klanten bewust te maken, dat softwareonderhoud net zo belangrijk is als technisch onderhoud. In 2018 komt TMX met een software assurance voor onderstations, zodat updates gedurende de duur van de software assurance gegarandeerd zijn en waarmee men dus verzekerd is van de laatste security updates in de software.

- TMX neemt actief deel aan security onderzoeken van de TU Delft en TNO om kennis in te winnen en om op te hoogte te blijven van de laatste ontwikkelingen. TMX is partner binnen HSD (The Hague Security Delta). HSD heeft als doel de innovatie op het gebied van veiligheid en economische ontwikkeling te bevorderen door de samenwerking tussen bedrijven, overheid en kennisinstellingen.