Houtkopersstraat 6
3334 KD Zwijndrecht (NL)
T +31 (0)78 6100 300
E info@tmx.nl
I www.tmx.nl
KvK 23039023

2018/cn

PRODUCTINFORMATIE

Security maatregelen in TMX-Net Pro Welke maatregelen worden toegepast om data secure uit te wisselen?

Het TMX telecontrol systeem wordt in allerlei toepassingen gebruikt voor het aansturen en monitoren van kritische systemen. Data wordt met TMX-onderstations, andere merken onderstations en met andere IT-systemen uitgewisseld via diverse koppelvlakken. Hoe zit het met de security-maatregelen die in TMX worden toegepast om data secure uit te wisselen?

Security in industriële automatisering

Over het algemeen wordt security door gebruikers als 'lastig' ervaren. In de industriële automatisering is de uptime topprioriteit. Dit in tegenstelling tot de kantoorautomatisering waarbij de veiligheid (security) op nummer 1 staat. We zien bovendien binnen de industriële automatisering veel 'legacy' hardware in het veld. Gebruikers vinden een levensduur van 10 tot 15 jaar voor een telemetrie onderstation heel normaal, terwijl de PC op kantoor iedere 3 tot 5 jaar vervangen wordt. Gelukkig zien wij bij gebruikers een omslag hierin. Men ziet steeds meer het belang in van een veilig systeem en begrijpt dat hiervoor aangepast gedrag en extra (technische) maatregelen noodzakelijk zijn.

Regelmatig installeren van updates een must (FOTA)

TMX brengt voor zowel de TMX-Net Pro hoofdpost software als TMX onderstations regelmatig updates uit. Deze updates bevatten niet alleen nieuwe functionaliteiten en bugfixes maar ook security-patches. Moderne TMX onderstations en dataloggers, zoals de LMX400, LMX800 en TSX100 beschikken over de mogelijkheid om op afstand de software te updaten door middel van FOTA (Firmware Over The Air). TMX adviseert gebruikers dringend om minimaal ieder half jaar te controleren of de onderstations nog over de meest recente firmware versie beschikken en waar nodig deze middels FOTA bij te werken. De TMX-Net Pro hoofdpost beschikt hiervoor over een speciaal FOTA-scherm om dit eenvoudig te kunnen controleren en uitvoeren.

Updaten van TMX-Net Pro

De TMX-Net Pro hoofdpostsoftware wordt dagelijks bijgewerkt voor security zaken. Twee keer in de maand voeren wij na werktijd regulier onderhoud uit aan TMX-Net Pro. Tijdens dit onderhoud voeren wij ook updates uit in verband met security.

Hoe verloopt de communicatie met de onderstations?

TMX onderstations maken vaak gebruik van openbare infrastructuren, zoals de bekende mobiele netwerken (2G/3G/4G). In Nederland worden deze netwerken door bekende providers als KPN, Vodafone en T-Mobile uitgevoerd. TMX maakt hierbij gebruik van een eigen APN (Access Point Name). Deze TMX APN zorgt ervoor dat de verbinding tussen de onderstations en de TMX-Net Pro hoofdpost afgeschermd is van het andere dataverkeer en het internet. Omdat TMX binnen de TMX APN per gebruiker alle

onderstations in een zogeheten ‘subnet’ zet, worden ook de datastromen van onderlinge gebruikers volledig van elkaar gescheiden. De APN is via een VPN (Virtual Private Network) verbonden met de TMX-Net Pro servers in ons datacenter.

TMX kent twee soorten APN’s:

- Managed SIMs:

Dit is de variant die TMX nadrukkelijk adviseert omdat deze, naast de security zaken, ook allerlei voordelen op het gebied van beheer, administratie en kosten heeft. Basis hierbij is een SIM-kaart van KPN. Onze ervaring is dat KPN beschikt over een van de meest betrouwbare en stabiele mobiele netwerken van Nederland van zowel 2G, 3G als 4G. Het dataverkeer verloopt binnen de TMX APN en klant-subnet. Een onderstation kan dus uitsluitend communiceren met de TMX-Net Pro hoofdpost. TMX beschikt over de mogelijkheid om de SIMs te managen en te monitoren. Is een SIM bijvoorbeeld gestolen, dan kan TMX deze na een melding direct blokkeren zodat er niet ingebroken kan worden op het netwerk.

- Unmanaged SIMs:

Bij de unmanaged variant wordt de TMX APN aan een bestaande SIM toegevoegd. Voorwaarde is wel dat de SIM direct bij een van de grote providers (KPN, Vodafone of T-Mobile) is afgenomen. Abonnement en kosten blijven bij de klant. Ook hier loopt het dataverkeer van/naar de TMX-Net Pro hoofdpost via de afgescheiden TMX APN en klant subnet. Deze variant beschikt niet over de mogelijkheid om de SIM te blokkeren na diefstal.

Communicatie met de onderstations – encryptie, autorisatie en whitelisting

Moderne onderstations als de LMX400 en de LMX800 zijn voorzien van extra beveiligingsmechanismen. Dit omdat beveiligingsrichtlijnen als de BIG/BIR/BIWA (voor respectievelijk gemeenten, Rijkswaterstaat en Waterschappen) vereisen dat er bij communicatie van vertrouwelijke informatie over onvertrouwde netwerken, zoals het internet en mobiele netwerken, altijd geschikte encryptie moet worden toegepast. De LMX400 en LMX800 onderstations en TMX-Net Pro hoofdpost loggen bovendien bij elkaar in, zodat ook alleen geautoriseerde onderstations verbinding krijgen. Dit is noodzakelijk om bijvoorbeeld in geval van SIM diefstal te voorkomen dat er ongeautoriseerd ingelogd kan worden op de communicatie interface van de hoofdpost. TMX werkt bovendien hier met zogeheten ‘whitelists’ waardoor berichten van onbekende bronnen worden genegeerd.

De TMX-TWIN koppeling voor het uitwisselen van data

Voor uitwisseling van data met andere systemen beschikt de TMX-Net Pro hoofdpost over de TWIN webservice. Via deze webservice kunnen onder andere registraties, instellingen en setpoints worden uitgewisseld met andere IT-systemen. TWIN kent een uitgebreid autorisatiemodel. De TMX beheerder kan hierbij aangeven welke functionaliteit (registraties, setpoints, instellingen, etc.) er vrijgegeven wordt en voor welke locatie(s) en kanalen dit gebeurt. Bovendien kennen individuele functionaliteiten extra autorisatiemogelijkheden; zo kan de tijdperiode van een registratiereeks bijvoorbeeld worden beperkt. Omdat bij TMX-Net Pro de gegevens over internet

verstuurd worden, is het noodzakelijk om deze af te schermen en te versleutelen. Dit gebeurt via een VPN verbinding.

Meer informatie?

In dit artikel zijn wij ingegaan op slechts een beknopt overzicht van enkele security oplossingen binnen TMX-Net Pro. Wilt u meer informatie? Dan kunt u hiervoor contact opnemen met de afdeling sales van TMX via 078 6100 300 of sales@tmx.nl of met een van onze dealers: Modderkolk Projects & Maintenance (024 648 6400), Van der Arend Installaties (0174 612 570) of Vlaar Techniek (0227 570 260).