Volledige reactie van de Unie van Waterschappen

Herkent u de gesignaleerde problemen?
Het gebeurt inderdaad dat de duur van beveiligingsupdates beperkt is, terwijl apparatuur langer meegaat. Hier worden maatregelen voor genomen. Onder andere worden er goede afspraken met leveranciers gemaakt: zorgen dat de beveiliging van de software up to date blijft en dat, zodra er een update is, die kan worden geïnstalleerd. Daarnaast zijn er mogelijkheden om apparatuur te 'hardenen' en te isoleren. Dan zet je overbodige functies op de apparatuur uit, zoals verhinderen dat verbinding met internet gemaakt kan worden. En wordt het domein van waaruit de procesautomatisering wordt beheerd, ingericht met nodige specifieke beveiligingsmechanismen. Meer in het algemeen vind beveiliging bij de waterschappen gelaagd en meervoudig plaats.
[Het gaat hier om procesautomatisering, en om computers die speciaal ontworpen zijn om machines en processen te beheersen. Zogenoemde PLC's (programmable logic controller).]

Moeten we (burgers) ons zorgen maken?
Beveiliging 'is zo sterk als de zwakste schakel'. Dit betekent dat in aanleg alles een risico voor de veiligheid kan vormen. PLC's die niet meer ondersteund worden met beveiligingsupdates, kunnen een informatiebeveiligingsrisico inhouden. Naast PLC's geldt dit voor alle bedrijfsobjecten in de informatievoorziening. Maar dat risico maken we zo klein mogelijk. De waterschappen hebben al honderden jaren de taak Nederland veilig en schoon te houden (tegen overstroming en vervuiling van het water) en zijn daar goed in. Als het gaat om Informatieveiligheid nemen de waterschappen de risico's dan ook uiterst serieus en investeren zij fors in het herkennen van en adequaat reageren op cyberdreigingen.

Wat doet u ertegen?
Waterschappen werken risico gebaseerd aan de beveiliging en continuïteit van de bedrijfsobjecten om de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening te kunnen waarborgen. Door een combinatie van maatregelen (van organisatorische en technische aard) worden risico's van

informatieveiligheid tot een aanvaardbaar minimum teruggebracht en regelmatig getoetst op robuustheid. De normen uit de Baseline Informatiebeveiliging Waterschappen (BIWA, afgeleid van de internationaal erkende ISO-27001-beveiligingsnorm) definiëren het minimum- cq het basis-beveiligingsniveau. [We kunnen niet tot in details treden over veiligheidsmaatregelen, dan zou het niet veilig meer zijn…]