Hoe uw verouderde machines cyberveilig connecteren

12 oktober 2021, 02:00

Annanda Rath
Christophe Michiels
Tatiana Galibus

Sirris lanceerde onlangs haar cybersecurity-dienst voor de maakindustrie. Nu we bedrijven beginnen aan te schrijven via onze gratis intake of individuele coaching, krijgen we steeds meer vragen rond connectiviteit. Voor fabrikanten lijkt dit een complexe materie, maar met een aantal gestructureerde tips valt het eenvoudig op te lossen.

Er bestaat geen pasklare oplossing om legacy apparatuur cyberveilig te maken en, zoals gekend, is de ketting maar zo sterk als de zwakste schakel. Net daarom is het belangrijk meerdere *lagen* op te bouwen om verouderde systemen te versterken en zo het *risico* op problemen met de cyberveiligheid te *beperken*.

Mogelijke strategieën en maatregelen

- De eerste belangrijke strategie die moet worden overwogen bestaat erin te **voorkomen dat uw apparatuur verouderd raakt**, of op zijn minst te trachten dit proces te vertragen. Dit kan door alle wijzigingen en updates die aan de machine worden uitgevoerd, te documenteren. Bevat de machine een pc-gebaseerd besturingssysteem, dan moet u ervoor zorgen dat alle (veiligheids)patches worden toegepast. Dit geldt ook voor DCS- of PLC-apparatuur. U kan dit opnemen in het onderhoudscontract tussen u en uw leverancier/integrator. Als een bepaald onderdeel na verloop van tijd niet meer softwarematig te patchen is, overweeg dan een upgrade naar nieuwe hardware. Dit impliceert een constante monitoring en voortdurende investeringen. Maar gezien de kosten die moderne cyberaanvallen mogelijk met zich meebrengen, kan dit een goede investering zijn.

- Een tweede strategie bestaat erin **een overzicht bij te houden van al uw geconnecteerde assets**, met inbegrip van dcs -of plc-systemen in de machines. U kunt immers niet beschermen wat u niet kent. Een inventaris is dus essentieel. Het is belangrijk om deze up-to-date te houden, hoe lastig dit ook is! Gekende kwetsbaarheden veranderen na verloop van tijd; u moet dan ook regelmatig uw apparatuur op kwetsbaarheden scannen. Maak een visuele voorstelling van dit overzicht, zodat u kunt zien welke versterkende maatregelen effect hebben op welk deel van uw productie of op welke machines. Dit vergemakkelijkt het plannen en ontwerpen van uw infrastructuur.

- De absolute minimale maatregel die moet worden genomen, is het **scheiden van uw IT-kantoorapparatuur en uw OT-productieapparatuur**. Bijvoorbeeld, door een afzonderlijke

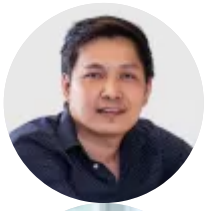
industriële firewall tussen beide te plaatsen. Nog beter is een verdere scheiding tussen de verschillende afdelingen, lijnen of machines. Uiteraard moeten de firewalls zelf beheerd en up-to-date worden gehouden door patches toe te passen wanneer deze door de fabrikant worden verstrekt. Afhankelijk van de grootte van uw installatie wordt het ook als een goede praktijk beschouwd om toestellen van verschillende leveranciers te gebruiken.

- Een niet-intrusieve manier om een systeem te monitoren, is het **monitoren van het netwerkverkeer** van of naar een machine. Deze praktijk wordt virtueel patchen genoemd. U installeert een apparaat tussen de machine en de rest van het netwerk. Wanneer het detecteert dat een gekende kwetsbaarheid wordt misbruikt, blokkeert het verder netwerkverkeer en brengt het de beheerder op de hoogte van het voorval.

- Soms wordt nog **oude software** gebruikt om bestanden voor een bepaald type machine te genereren (bijv. CNC). Dat dit soort software alleen op Win98 of WinXP draait, is lang geen uitzondering. In deze gevallen is het aangewezen om het oude OS en de software in een virtuele machine op een moderne pc te laten draaien. Dit lost niet alle mogelijke problemen op, maar verkleint wel aanzienlijk het aanvalsgebied.

De tips die we u in deze blog meegeven, zijn slechts een greep uit de vele mogelijke manieren om uw legacy OT-infrastructuur te versterken. In onze masterclass 'Cyberveiligheid voor maakbedrijven' gaan we dieper op deze materie in, met praktijkvoorbeelden en een praktisch stappenplan voor het beveiligen van uw geconnecteerde machines. Schrijf u nu in en woon de masterclass bij op 8 november 2021!

Auteurs



Annanda Rath



Christophe Michiels



Tatiana Galibus