Overpeinzingen over beveiligingsautomatisering voor IoT- en OT-omgevingen

"Je kan niet beveiligen wat je niet weet" Asset Management "Visibility is key"

Onze visie

Automatisering is niets nieuws
Automatisering wordt soms gezien als een concept van de 21e eeuw. Zeker in de context van kunstmatige intelligentie of machine learning hebben automatisering of automaten tot onze verbeelding gesproken als iets dat de toekomst voor ons in petto heeft, en dat iets moet worden vereerd of gevreesd. In werkelijkheid bestaat automatisering, of de poging om processen automatisch te maken, al sinds Henry Ford voor het eerst de lopende band populair maakte, en waarschijnlijk dateert zelfs van vóór de industriële revolutie zelf. Sinds het ontstaan van de mensheid is de mens continue bezig geweest met het automatiseren van de processen om zo het leven steeds aangenamer te maken.

Een van de aspecten van automatisering die soms onze collectieve verbeelding prikkelt - zowel in termen van angst als hoop - is het concept van machines die met andere machines praten. Dergelijke communicatie, misschien in strijd met de populaire verbeelding, bestaat al decennia. Energiebedrijven, farmaceutica, chemische fabrikanten, olie- en gasraffinaderijen, kerncentrales, - al deze sectoren, gezamenlijk aangeduid als 'kritieke en industriële infrastructuur', vertrouwen op 'Operational Technology'-netwerken die bestaan uit sensoren, PLC's, DCU's , HMI's en technische werkstations die met elkaar communiceren. Machines praten met machines om processen te automatiseren - en dat is op zich niet per se een slechte zaak.

Beveiligingsautomatisering - vooral in OT- en IoT-omgevingen - is relatief nieuw
De uitdaging is dat veel, zo niet al deze 'OT'- of, in toenemende mate' IoT'-apparaten, niet kunnen worden gemonitord door de huidige monitoringsystemen, en het is dus ingewikkelder om ze te monitoren op bedreigingen of een actuele inventaris bij te houden dan voor traditionele IT-endpoints. Automatisering is nodig om voor elk apparaat type inventaris op te halen en zoveel mogelijk informatie over dat apparaat te krijgen. In een industrieel controlesysteem of elke omgeving waar verstoring niet alleen kan leiden tot winstderving, maar zelfs tot grote veiligheids- of milieu-incidenten, moeten de activa worden bewaakt met zo min mogelijk verstoring.

"Er zijn miljoenen IoT en OT devices waarbij security bij design niet is meegenomen" deze devices zijn kwetsbaar en vormen een potentiële risico.

Als je beveiliging serieus moet nemen, dan heb je automatisering nodig. Het handhaven van een hoge standaard van IoT/OT-veiligheid en beveiliging is onmogelijk zonder automatisering.

Denk bijvoorbeeld na over het proces van device (CMDB) inventarisatie. Allereerst is het van cruciaal belang dat uw device inventaris continu up-to-date is wanneer nieuwe devices het netwerk binnenkomen of verlaten. U zou een melding moeten krijgen van de devices die gekoppeld en ontkoppeld worden aan uw netwerk. Denk aan de schade die een willekeurige laptop die zich ongemerkt op het OT-netwerk aansluit zou kunnen aanrichten - dit device introduceert een portaal waarmee malware en aanvallers verlammende schade kunnen toebrengen aan de OT-omgeving, of erger nog, aan de mensen die daar werken. Helaas zien we dit scenario vrij vaak, waarin werknemers of externe contractanten nieuwe devices in de OT-omgeving brengen - tegen het beleid in, maar al te vaak blijven deze niet-geautoriseerde devices onopgemerkt. U moet deze device detectie automatiseren omdat handmatige inventarisatie te vatbaar is voor menselijke fouten, te traag en eerlijk gezegd te log.

Er zijn ook honderden andere manieren waarop device wijzigingen onopgemerkt kunnen blijven en uw omgeving in gevaar kunnen brengen, vooral nu digitalisering en Industrie 4.0-initiatieven een verhoogde internetverbinding in OT-omgevingen introduceren. Automatisering is van cruciaal belang om te begrijpen hoe devices communiceren in deze complexe omgevingen, om device veranderingen zoals wijzigingen in firmware/versies te begrijpen en om ervoor te zorgen dat u proactief kwetsbaarheden aanpakt die van invloed zijn op uw "kroonjuweel". Als bijvoorbeeld wordt ontdekt dat een device kwetsbaar is omdat er een patch ontbreekt, moet de eigenaar van het device weten welke patch ontbreekt en moet hij kunnen bepalen welke devices welke patches nodig hebben en in welke volgorde.

De volgende belangrijke stap bij het automatiseren van de beveiliging van geautomatiseerde processen is niet alleen om deze device en device details te ontdekken, maar ook om veranderingen in hun gedrag te volgen - zoals veranderingen in internetconnectiviteit, programmeerwijzigingen in PLC's (die nog zorgwekkender zijn als ze plaatsvinden). op abnormale tijden, zoals buiten kantooruren), ongewoon PLC-gedrag (zoals een PLC die meer uitlezingen heeft dan vroeger) of protocolovertredingen die wijzen op pogingen om het protocol te misbruiken.

Door deze gedragsveranderingen te detecteren, kunt u bedreigingen sneller en nauwkeuriger vinden, zodat u de tegenstander kunt stoppen voordat ze een materiële impact op uw bedrijf hebben. En hoewel je theoretisch genoeg mensen zou kunnen inhuren om handmatig de inventaris van devices, firmwarewijzigingen en beveiligingslogboeken te controleren, zou dit soort geavanceerde analyse niet praktisch zijn in termen van tijd.

Hoewel het concept van beveiligingsautomatisering in OT- en IoT-omgevingen nieuw is, is het nu al een noodzaak

De waarde van automatisering gaat echter verder dan inventaris van activa en detectie van bedreigingen. Denk aan het enorme aantal aanvalsvectoren in de moderne onderneming. Als je kijkt naar slechts 300 apparaten die alleen met elkaar kunnen worden gemanipuleerd, resulteert dat in meer dan 90.000 mogelijke bedreigingsvectoren - en dat is voor een kleine omgeving. Als een mens al deze bedreigingsvectoren handmatig zou aanpakken, zelfs als het maar één minuut per potentiële aanvalsvector zou kosten, zouden ze het grootste deel van een jaar nodig hebben.

Hoewel automatisering een oneindig potentieel heeft, is de waarde ervan op het gebied van asset-discovery, kwetsbaarheidsbeheer en detectie van bedreigingen alleen van onschatbare waarde voor de hedendaagse organisaties. Dit effectief doen met alleen mankracht is onmogelijk in de complexe omgevingen van vandaag.

Als u meer automatisering in uw IoT & OT-beveiligingsomgeving probeert op te nemen, kan IoT / OT-bewuste beveiligingstechnologie helpen. Neem rechtstreeks contact met ons op om hoe u de detectie van bedreigingen, het beheer van kwetsbaarheden en de detectie van activa in uw omgeving het beste kunt automatiseren.

intergrid

“ONAFHANKELIJKE SERVICE INTEGRATOR VOOR ORGANISATIES MET COMPLEXE EN KRITISCHE INFRASTRUCTUREN”

Als service integrator levert Intergrid diensten op het gebied van IT, OT, IoT, Security, Infrastructuur en Strategische vraagstukken. De kracht van Intergrid kenmerkt zich door haar onafhankelijkheid, expertise en professionaliteit.

“Intergrid wil bijdragen aan het vertrouwen in de maatschappij en helpen bij het oplossen van belangrijke courante uitdagingen.”

Dat is onze missie en daarmee dé toetssteen voor de dingen die we doen of willen gaan doen én voor het bepalen of iets een succes is.

Voor Intergrid zijn waarden bepalend voor wie we zijn. Het gaat er niet alleen om wat we doen, maar vooral ook hoe we het doen.

Wij maken samen met onze klanten, partners en medewerkers het verschil vanuit onze Betrokkenheid, Professionaliteit, Integriteit en Onafhankelijkheid

https://intergrid.nl - info@intergrid.nl - +31 653322040

“If you wait for perfect conditions, you will never get anything done”