Operational Technology & Industrial Control Systems

Hoe verkleint u het aanvalsoppervlak in industriële netwerken

Orange
Cyberdefense

orange™

Inhoudsopgave

Inleiding

Halverwege de 20e eeuw waren processen in de fabriek en computers op de werkvloer volledig van elkaar geïsoleerd. Productiemachines communiceerden niet met IT-systemen zoals bestel-, inkoop- en productietoepassingen.

Er was geen directe koppeling tussen het ‘Operational Technology’ (OT) netwerk en de daarin aanwezige ‘Industrial Control Systems’ (ICS). Daardoor waren de risico’s op cyberaanvallen zeer beperkt en bestonden ze nagenoeg niet.

Tegenwoordig willen bedrijven hun producten zo snel mogelijk op de markt brengen om de concurrentie voor te blijven. Daarnaast staan de productiekosten vaak onder druk. Daarom worden in toenemende mate IT-toepassingen betrokken bij het operationele proces met als doel het optimaliseren van het productieproces. Hiermee is de ‘Digitale Transformatie’ een feit.

> **De productie industrie is een samenvoeging geworden van OT (het industriële netwerk) en IT (het kantoornetwerk). Het resultaat is een toename van uitdagingen op het gebied van cybersecurity**

Onder invloed van deze digitale transformatie vindt integratie plaats tussen het IT-domein en het OT-domein. En hoewel hier veel voordelen aan verbonden zijn, neemt het op het gebied van

cybersecurity ook wat uitdagingen met zich mee.

Het introduceren van digitalisering op de werkvloer wijzigt het dreigingsrisico van een productiebedrijf als volgt:

- Het OT-netwerk en de Industrial Control Systems, voorheen geïsoleerd, worden nu verbonden met het IT-netwerk. Hierdoor moet worden nagedacht over hoe om te gaan met ondersteuning voor verouderde apparatuur waar geen software updates voor beschikbaar zijn en patchen dus niet mogelijk is
- Er wordt een noodzaak geïntroduceerd voor het uitwisselen van gegevens tussen het IT- en OT-domein. Hoe kan dit op een veilige manier?
- Externe toegang voor leveranciers, partners en fabrikanten heeft veel voordelen, maar vergroot het aanvalsoppervlak.

Peter van der Voort

Solution Architect OT
Orange Cyberdefense

Beveiligingsuitdagingen in OT/ ICS

De digitale transformatie en de integratie van het OT- en IT-domein neemt extra uitdagingen met zich mee op het gebied van cybersecurity.

Maar wat zijn die extra uitdagingen?

- Prioriteiten – De prioriteiten in het OT-domein zijn anders dan die in het IT-domein.
- Kennis – Zoals bij IT-geschoolde mensen kennis ontbreekt over het OT-domein, zo ontbreekt bij mensen in het OT-domein vaak de kennis van cybersecurity.
- Cultuur – Er kan gezegd worden dat, mede door het verschil in prioriteiten en kennisgebied, er een verschil is in cultuur tussen mensen in het OT-domein en mensen in het IT-domein.

Prioriteiten in het OT-domein en het IT-domein

De prioriteiten in het OT-domein en het IT-domein zijn verschillend.

In het algemeen zijn de prioriteiten in het IT-domein als volgt:

1. Vertrouwelijkheid van de gegevens
2. Integriteit van de gegevens
3. Beschikbaarheid van de gegevens

Als we kijken naar OT/ICS hebben we precies het tegenovergestelde:

1. Veiligheid van mens en omgeving
2. Beschikbaarheid van het productieproces
3. Integriteit van het proces (en de data daarin)

Het grootste verschil in prioriteit tussen het OT- en IT-domein is dat in een industrieel netwerk verstoringen niet acceptabel zijn. De vrees dat cybersecurity maatregelen de beschikbaarheid van het operationele proces in gevaar brengen is waarschijnlijk één van de belangrijkste redenen dat weinig organisaties cybersecurity toepassen in het industriële domein. Het resultaat is dat het industriële netwerk vaak een ‘plat’ netwerk is waardoor alle apparatuur vrij met elkaar kan communiceren.

De onderstaande tabel geeft een overzicht van enkele belangrijke verschillen tussen de twee vakgebieden.

	OT	IT
Beschikbaarheid	Kritisch	Belangrijk
Vertrouwelijkheid	Minder belangrijk	Kritisch
Integriteit	Zeer belangrijk	Kritisch
Technologie levenscyclus	15+ jaar	3-5 jaar
Bescherming tegen malware	Slecht (vooral oude systemen)	Normaal
Patching	Alleen tijdens onderhoud	Regelmatig
Protocollen	Eigen OT-protocollen	IP
Cybersecurity awareness	Slecht (wordt langzaam beter)	Goed
Human safety awareness	Kritisch	Slecht
Normen	ISA/IEC 62443	ISO 27000
Toegang op afstand	Onzichtbaar/deel van contract	Gecontroleerd

Cybersecurity kennis

Machine-operators, plantmanagers en procesengineers hebben heel specifieke kennis van proces automatisering en het beschikbaar houden van een specifiek proces. Het komt voor dat de automatisering in een fabriek (meer dan) 30 jaar geleden werd ontworpen, ver voordat cybersecurity iets was om rekening mee te houden.

Het gevolg is dan ook dat mensen die werkzaam zijn in het OT-domein vaak beperkte kennis hebben van cybersecurity. Immers, dit behoort niet tot hun operationele taken en door de jaren heen is hen niet geleerd om cyberdreigingen te herkennen.

Het zou goed zijn wanneer o.a. procesengineers, plantmanagers en machine-operators meer kennis zouden hebben van bijvoorbeeld ‘phising’ en ‘malware’ technieken. Volgens het ‘Data Breach Investigations Report’ (DBIR) uit 2020, opgesteld door Verizon, is 30% van cybersecurity incidenten het gevolg van handelingen van interne mensen. Bijvoorbeeld omdat deze mensen worden betaald om te spioneren, of omdat ze ontevreden zijn en operationele schade willen veroorzaken. Daarnaast zijn cybersecurity incidenten in veel gevallen ook het gevolg van menselijke vergissingen.

Cultuurverschil

Het is verrassend om te merken dat mensen uit het IT- en OT-domein slechts zelden met elkaar in gesprek zijn. Dit is waarschijnlijk historisch gegroeid want op het moment dat Industrial Control Systems werden gebouwd was er geen sprake van cybersecurity. In het algemeen was IT zelfs geen onderwerp van gesprek omdat dit ook nog in de kinderschoenen stond toen ICSs 30 jaar geleden werden ontwikkeld.

Tegenwoordig echter, onder invloed van de digitale transformatie, is er de noodzaak voor organisaties om inzicht te krijgen in data van het productieproces, met als doel om dit te optimaliseren. Doordat hiervoor applicaties moeten worden ingezet die primair ontworpen zijn voor het IT-domein, zijn mensen in het OT-domein bezorgd dat deze applicaties het operationele proces in gevaar brengen.

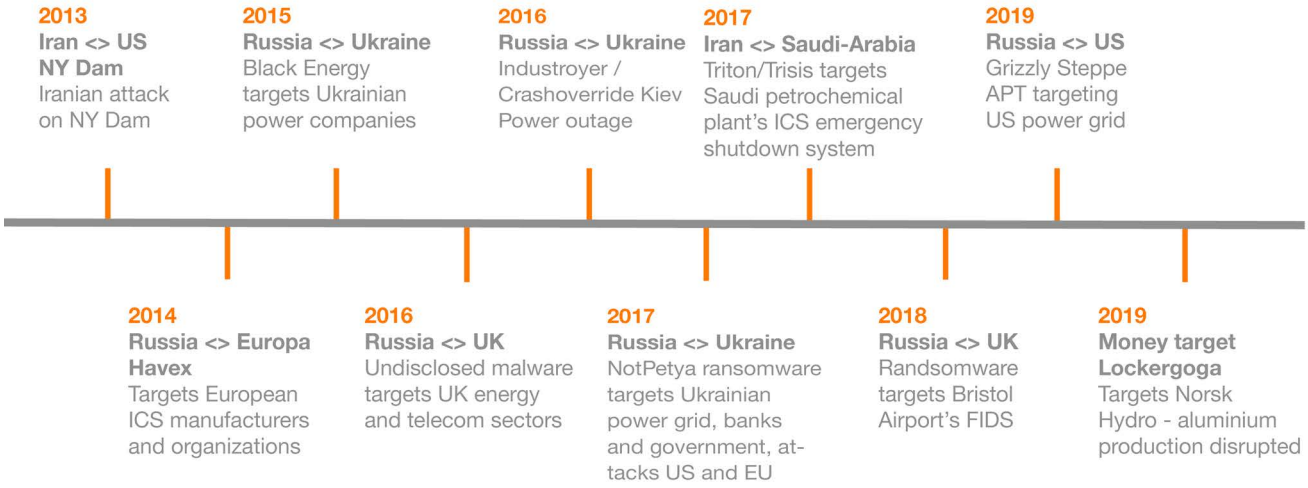
Deze zorg wordt nog versterkt doordat er geen gedeelde verantwoordelijkheid is, en niemand de verantwoordelijkheid wil nemen in het geval er daadwerkelijk een incident optreedt.

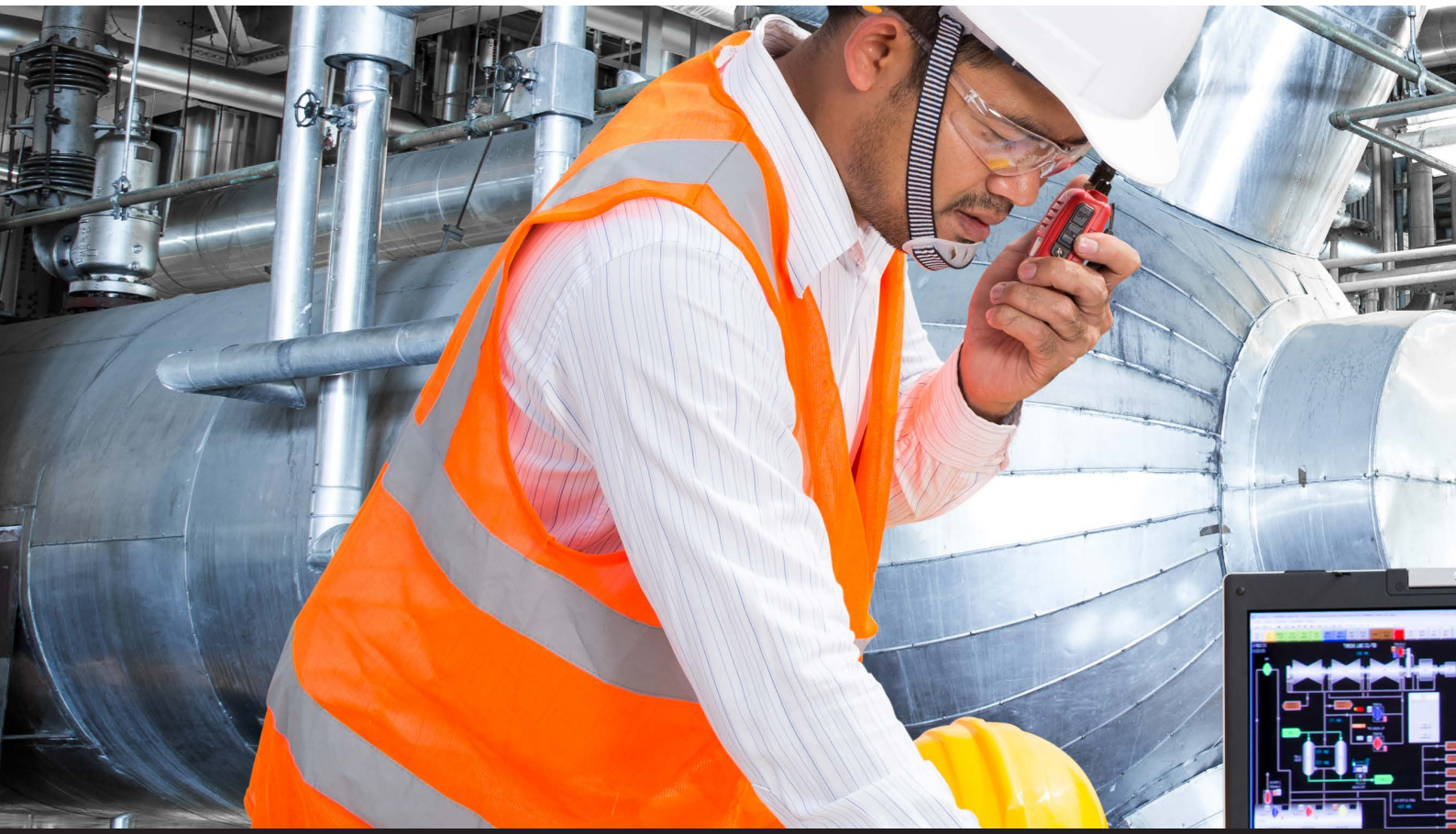
Het grote verschil in belang en in sommige gevallen het gebrek aan begrip voor elkaars domeinen zorgt ervoor dat cybersecurity moeilijk een plaats krijgt in het industriële domein.

OT-cyberaanvallen zijn reëel en groeiend in aantal

Zoals weergegeven in het onderstaande figuur zijn grote aanvallen op industriële bedrijven reëel en leiden ze vaak tot ernstige schade.

In sommige gevallen ontstonden zelfs levensbedreigende situaties.





Verschillende marktonderzoeken komen tot gelijke conclusies. Zoals het Ponemon-rapport opgesteld in maart 2019, het 2020 Verizon Data Breach Investigation Report en andere individuele onderzoeken concluderen samenvattend dat:

90% 90% heeft in de afgelopen twee jaar te maken gehad met minstens één schadeveroorzakende cyberaanval en/of malware.

20% Slechts 20% van de 700+ respondenten in de OT-sector heeft genoeg zichtbaarheid in de assets van hun organisatie.

50% 50% heeft in de afgelopen twee jaar ten minste één cyberaanval meegemaakt wat leidde tot uitval.

55% 5% van de respondenten bracht meer tijd door met het doorlopen van handmatige processen dan reageren op kwetsbaarheden.

De reden voor het toenemend aantal cyberaanvallen is eenvoudig. Het is veel efficiënter en “veiliger” om geld of intellectueel eigendom van multinationals en overheidsinstanties te stelen via cyberaanvallen dan fysieke manipulatie te gebruiken. Het gebrek aan algehele zichtbaarheid in het OT-netwerk geeft de hacker tijd om zijn verkenning in het netwerk maanden vooraf te doen.

Verkleining van het aanvalsoppervlak

Nu de uitdagingen gerelateerd aan cybersecurity in het industriële netwerk bekend zijn kan een begin worden gemaakt met het verkleinen van het aanvalsoppervlak. Hiertoe adviseren wij het gebruik van een raamwerk ter ondersteuning. De praktijk leert dat het gebruik van een raamwerk één van de betere manieren is om te beginnen met een programma voor cybersecurity.

Er zijn verschillende raamwerken beschikbaar, elk met eigen voor- en nadelen. De meest gebruikte in de industriële automatisering zijn IEC 62443 en de NIST 800-82. Maar daarnaast zijn ook de volgende raamwerken noemenswaardig:

- NIS directive
- Mitre Att&ck for ICS
- CIS Critical Security Controls

Wat volgt zijn vijf fundamentele aanbevelingen van Orange Cyberdefense om cybersecurity incidenten in het OT/ICS-netwerk te beperken.

Hardware en software overzicht

Een van de belangrijkste stappen om het OT-domein te beveiligen is te weten wat er zich in dat domein bevindt. Een nauwkeurige inventarisatie van (OT) assets zoals hardware inclusief fabrikant en type-nummer alsook software inclusief versie nummer en eventueel patch-level, is de eerste stap naar een hoger niveau van cybersecurity.

Een goede inventarisatie wordt best gemaakt met een geautomatiseerd systeem die op een passieve manier gegevens van alle OT-assets kan verzamelen. Tegelijkertijd moet het systeem een baseline kunnen creëren van verkeersstromen van- en naar de ontdekte assets, inclusief het gebruikte (industriële) protocol. Een dergelijk systeem kan dan, gebaseerd op de baseline, alarmeren wanneer van deze baseline wordt afgeweken. Een afwijking is mogelijk een indicatie van een cyberaanval.

Het is van belang dat de beheerders van het industriële netwerk een goed overzicht hebben van dat industriële netwerk. Voor het maken van een netwerktekening geldt ook hier dat deze best gemaakt wordt met een geautomatiseerd systeem, bij voorkeur hetzelfde systeem dat de inventarisatie van assets doet.

Voor het creëren van een netwerkdiagram en een inventarisatie van OT-assets wordt best gebruik gemaakt van een geautomatiseerd monitoring systeem. Hierbij is het van belang dat het systeem geen impact heeft op het operationele proces.

Hoewel veel fabrikanten claimen een technische oplossing te kunnen bieden, is het belangrijk om te kiezen voor een oplossing die volledige ondersteuning biedt voor industriële protocollen zoals Modbus, Profinet, Ethernet/IP, enz.

Wanneer een duidelijk overzicht is gecreëerd van assets, waar deze zich in het netwerk bevinden en welke verkeersstromen er zijn, kan inzichtelijk worden gemaakt welke verbindingen er zijn tussen verschillende assets en zones. Vervolgens kan worden bepaald of deze verbindingen zijn toegestaan of moeten worden beperkt middels een security policy (op bijvoorbeeld een firewall).

Maak gebruik van een geautomatiseerd systeem dat een volledig beeld geeft van het industriële netwerk, de gebruikte systemen en kan rapporteren op afwijkingen.

Wijzigingsbeheer

Elke wijziging in het industriële netwerk moet worden gemonitord, gedetecteerd en bijgehouden. Het toevoegen van nieuwe appraten of het maken van configuratiewijzigingen, ongeacht of dit per ongeluk of bewust wordt gedaan, kunnen impact hebben op de operationele systemen. In het ergste geval kan een operationeel proces stil komen te liggen.

Zorg er dus voor dat alleen goedgekeurde wijzigingen worden uitgevoerd. Maar zorg er ook voor dat ongeautoriseerde wijzigingen worden gedetecteerd.

Gecentraliseerde logging

Log-informatie van systemen kan een goed beeld geven van de status van het systeem in kwestie, maar ook van het gehele netwerk. Zorg er dus voor dat logging op een centrale plaats wordt verzameld.

De daarop volgende stap is het analyseren van de logs, zodat inzicht wordt gekregen in de ‘health status’ van het netwerk, maar ook zodat eventuele cybersecurity incidenten kunnen worden opgemerkt.

Een goed log-systeem kan log-informatie filteren voordat dit naar bijvoorbeeld een SIEM wordt gestuurd. Immers, het heeft geen zin om elke dag dezelfde meldingen te krijgen over een bekend Windows-XP systeem, het doel is om te kunnen rapporteren op afwijkingen van de normale situatie.

Het is van belang dat het log-systeem kan filteren op specifieke datum- en tijdsintervallen om afwijkingen tijdens een specifieke periode inzichtelijk te maken.

Beheer van kwetsbaarheden

Een grote uitdaging met betrekking tot het vinden van kwetsbaarheden van OT-apparatuur is dat dit soort apparatuur niet actief gescand mag worden omdat het risico op verstoring van het operationele proces te groot is. Daarom moet passieve detectie worden toegepast. Middels passieve detectie kan een inventarisatie worden gemaakt van de actieve componenten in het netwerk, inclusief de gebruikte software versies.

Wanneer een inventarisatie is gemaakt van software versies in het OT-domein kan deze worden vergeleken met een database waarin kwetsbaarheden worden bijgehouden. Het meest bekend hierin is de 'Common Vulnerabilities and Exposures' (CVE) database. De meeste cyberaanvallen met malware zijn gebaseerd op kwetsbaarheden die in de CVE-database zijn geregistreerd. Omdat bedrijven vaak achterlopen met het patchen van kwetsbare systemen maken aanvallers gebruik van de informatie in de CVE-database.

Selecteer een oplossing die op een passieve manier het OT-netwerk kan monitoren, bij voorkeur aangevuld met de mogelijkheid voor actieve monitortechnieken voor die delen van het netwerk waar dit wel mogelijk is.
Houd er rekening mee dat risicoscores geprioriteerd moeten kunnen worden weergegeven zodat eenvoudig een planning kan worden gemaakt om de grootste bedreigingen als eerste te kunnen verhelpen.

Selecteer een monitoring oplossing die niet alleen het netwerk in kaart brengt maar ook automatisch logische zones definieert en de verkeersstromen tussen deze zones (de conduits) in kaart brengt.

Integratie met een Next Generation Firewall van een dergelijke monitoring oplossing is een voordeel omdat er dan geautomatiseerd een security policy kan worden gedefinieerd, gebaseerd op de gedetecteerde verkeersstromen. Uiteraard beslist de OT-afdeling of deze policy wordt geïmplementeerd.

Network zones & segmentation

Netwerksegmentatie wordt bereikt door het opdelen van het netwerk in zones. Binnen die zones worden systemen met gelijke operationele functie en gelijk risico profiel gegroepeerd. Verschillende zones hebben dan verschillende risico profielen.

Met behulp van 'conduits' worden gecontroleerde communicatiepaden tussen zones gecreëerd.
Deze paden worden beveiligd met behulp van Next Generation Firewalls.

In de praktijk wordt duidelijk dat organisaties zijn begonnen met het segmenteren van het industriële netwerk door het plaatsen van firewalls. Echter, de toegepaste policy op deze firewalls is vaak nog gericht op het doorlaten van al het verkeer en blokkeert slechts malware.

Security Lifecycle

Eén van de meest prominente en bekende concepten in cybersecurity is de 'Security Lifecycle'. Bij Orange Cyberdefense gebruiken we de security lifecycle samen met het 'Security Maturity Model' om het huidige niveau van cybersecurity van onze klanten vast te stellen. Het maturity model wordt ook gebruikt als leidraad om onze klanten naar een hoger niveau van cybersecurity te brengen.

Hoewel een dergelijk maturity model onbereikbaar kan lijken en vooral haalbaar is voor volwassen organisaties, wijst de praktijk anders uit. Het model beschrijft verschillende onderwerpen waarmee alle organisaties het niveau van cybersecurity kunnen verhogen.

Het security lifecycle model van Orange Cyberdefense is weergegeven in onderstaande figuur.

Anticipate **Identify** **Protect** **Detect** **Respond**

Anticipate

Onder de pijler 'Anticiperen' valt alles wat te maken heeft met het continu monitoren van- en reageren op (mogelijke) cyberdreigingen in het industriële netwerk.

Uitdagingen

Om te kunnen anticiperen op cyberdreigingen krijgen organisaties te maken met verschillende uitdagingen en stellen zich onder andere de volgende vragen:

- Is onze organisatie een doelwit voor cybercriminelen?
- Hoe moeten we een 'Cyber Response Plan' creëren?
- Welk beveiligingsraamwerk moeten we gebruiken?
- Hoe kunnen we de cybersecurity vaardigheden van het OT-personeel vergroten?

Orange Cyberdefense oplossingen

Naar aanleiding van bovenstaande vragen kan Orange Cyberdefense ondersteuning bieden en wel als volgt.

- Er kan worden gesteld dat elke (industriële) organisatie een mogelijk doelwit is voor cybercriminelen. Met behulp van assessments kan Orange Cyberdefense helpen om kwetsbaarheden zichtbaar te maken. Hierbij wordt niet alleen gekeken naar cyberdreigingen van buitenaf, maar ook naar dreigingen van binnenuit of naar dreigingen veroorzaakt door vertrouwde derde partijen. Gebaseerd op de uitkomst van een dergelijk assessment kunnen beslissingsmakers een gefundeerde beslissing nemen.

- Het creëren van een cyber responseplan is een basisvereiste voor het kunnen reageren op cybersecurity incidenten. Maar ook kan het een grote rol spelen bij het voorkomen daarvan. Hierbij is het belangrijk om zowel medewerkers uit het OT-domein als medewerkers uit het IT-domein te betrekken zodat eenieder weet wat van hem/ haar verwacht wordt in geval van een cybersecurity incident.
- De keuze voor een raamwerk voor cybersecurity is afhankelijk van wat de doelstellingen van een organisatie zijn op het gebied van cybersecurity. Wanneer wordt gestreefd naar een cybersecurity certificering dan is de IEC 62443 wellicht goed geschikt. Wanneer vooral pragmatisch cybersecurity naar een hoger niveau moet worden gebracht dan is de NIST 800-82 een goede keuze. En misschien is een combinatie van verschillende raamwerken wat het best past. Uiteraard zijn er nog meer overwegingen voor de keuze van het juiste raamwerk. Aan de hand van een assessment kan Orange Cyberdefense een onderbouwd advies doen en organisaties begeleiden bij zowel de keuze voor- als de implementatie van een raamwerk.
- Op het gebied van cybersecurity vaardigheden voor OT-personeel kan Orange Cyberdefense een training verzorgen waarbij de deelnemers bekend worden gemaakt met cybersecurity dreigingen zoals malware en phishing technieken.

Identify

De pijler 'identificeren' is de tweede fase en één van de belangrijkste pijlers binnen de OT-security lifecycle omdat deze te maken heeft met het inventariseren van de bestaande situatie.

Uitdagingen

De specifieke uitdagingen waar een organisatie mee te maken krijgt wanneer een inventarisatie van de bestaande situatie moet worden gemaakt zijn onder andere:

- Wat is de zichtbaarheid van het OT/ ICS netwerk?
- Hoe lopen verkeersstromen, welke communicatie bestaat er tussen de OT-assets en eventueel met de buitenwereld?
- Hoe kwetsbaar zijn de OT-assets voor cybersecurity dreigingen?
- Welke communicatiepaden bestaan van- en naar de meest kritieke operationele processen?
- Hoe kan het huidige cybersecurity niveau van het OT-domein worden bepaald?
- Wat is de impact op de bedrijfsvoering wanneer een cybersecurity incident optreedt in het OT-domein?

Orange Cyberdefense oplossingen

Als geen ander realiseren wij ons dat beveiliging begint met het identificeren van actieve apparatuur, het vaststellen van kwetsbaarheden en daarmee het creëren van zichtbaarheid.

Om dit te bewerkstelligen kunnen we een 'Asset Discovery & Vulnerability' (ADV) onderzoek uitvoeren waarbij door middel van passief monitoren het industriële netwerk in kaart wordt gebracht. Hierbij is het niet nodig om gebruik te maken van 'agents' of actieve scan-technieken.

Door op een passieve manier te luisteren naar netwerkverkeer garanderen we dat er geen enkele impact is op het operationele proces.

Zaken die worden geïnventariseerd zijn onder andere:

- OT-asset type, fabrikant, serienummer en software versie
- Cybersecurity kwetsbaarheden in geïnventariseerde software
- Netwerk layout, zowel fysiek als logisch
- Verkeersstromen en communicatiepaden
- Gebruikte industriële protocollen

Het in kaart brengen van de communicatiepaden van- en naar de operationele processen is uitermate belangrijk om een inventarisatie te kunnen maken van de impact die een eventueel cybersecurity incident heeft op de bedrijfsvoering.

Protect

De derde pijler van de security lifecycle is ‘beveiligen’. Nadat in de tweede fase een inventarisatie is gemaakt van componenten in het OT-domein, inclusief mogelijke kwetsbaarheden, kan nu worden bepaald welke mate van beveiliging moet worden toegepast.

Uitdagingen

Eén van de grootste uitdagingen bij het beveiligen van het OT-domein ligt in het feit dat apparatuur en processen in dit domein niet zijn ontworpen voor cybersecurity. Zaken die hierdoor overwogen moeten worden:

- Hoe kan worden voorkomen dat malware zich kan verspreiden door het hele OT-domein?
- Hoe kunnen systemen zoals ‘Human Machine Interfaces’ (HMIs) worden beveiligd wanneer deze gebruik maken van een operating systeem waarvoor geen beveiligingsupdates meer worden uitgebracht (zoals Windows XP)?
- Hoe kan optimaal gebruik worden gemaakt van bijvoorbeeld bestaande firewalls, door deze te integreren met OT-security systemen?

Orange Cyberdefense oplossingen

Hoewel de uitdagingen bij het beveiligen van een industrieel netwerk groot zijn, zijn er toch methoden om het cybersecurity niveau te verhogen zónder het vervangen van OT-apparatuur. Hieronder worden twee suggesties gedaan waarmee begonnen kan worden zonder dat er invloed is op het operationele proces.

- Segmentatie, ofwel het aanbrengen van zones in het OT-netwerk is de eerste stap om de mogelijke verspreiding van malware te voorkomen. Vaak is een industrieel netwerk niet gesegmenteerd waardoor malware vrij spel heeft en zich ongehinderd kan verspreiden, met als mogelijk gevolg dat alle productieprocessen stil komen te liggen. Door middel van segmentatie kan weliswaar niet worden voorkomen dat malware binnen komt, maar de verspreiding ervan kan worden gestopt door het binnen een zone in quarantaine te zetten. Segmentatie wordt aangebracht met behulp van Next Generation Firewalls die industriële protocollen begrijpen. Hiermee worden communicatiepaden – de ‘conduits’ – tussen verschillende zones gecontroleerd en kan beveiligingsbeleid worden afgedwongen.

Segmentatie, ofwel het aanbrengen van zones in het OT-netwerk is de eerste stap om de mogelijke verspreiding van malware te voorkomen.

- Het beveiligen OT-assets zoals PLCs, RTUs en HMIs is een uitdaging op zichzelf. Vaak is het niet mogelijk om anti-malware software te installeren en in sommige gevallen is het zelfs niet toegestaan door de leverancier omdat dit de beschikbaarheid van het OT-asset in gevaar zou kunnen brengen. Vanwege deze beperking raden we aan om zo veel mogelijk verkeersstromen via een Next Generation Firewall te laten lopen. Zelfs wanneer deze verkeersstromen binnen een zone blijven is het mogelijk, door de firewall in ‘transparante modus’ te configureren, de verkeersstromen te controleren en malware te detecteren. Hierdoor kan snel worden ingegrepen wanneer dat nodig is.

Detect

Nadat het industriële netwerk is beveiligd is het van belang dat eventuele cyberaanvallen worden gedetecteerd. Daarnaast moet het mogelijk zijn om te detecteren dat configuratiewijzigingen worden doorgevoerd en/ of parameters worden aangepast, zodanig dat deze buiten een veilige waarde vallen. Dit laatste biedt beveiliging tegen cybercriminelen, maar ook tegen het door een operator per vergissing instellen van een onjuiste waarde.

Uitdagingen

Het detecteren van cyberaanvallen is niet altijd even gemakkelijk. Immers, aanvallers zullen er alles aan doen om in eerste instantie onopgemerkt te blijven. En wanneer malware detectie is gebaseerd op 'signatures' dan zijn veel anti-malware oplossingen vaak te laat met detectie.

De uitdagingen waarmee organisaties op dit gebied mee te maken krijgen zijn onder andere:

- Hoe kan op een passieve manier detectie van cyberaanvallen plaatsvinden.
- Hoe kan op een passieve manier worden gedetecteerd of parameters binnen een vooraf ingesteld bereik vallen.
- Is het mogelijk om afwijkingen van 'normaal gedrag' te detecteren en hierover te alarmeren.
- Kunnen cybersecurity incidenten en afwijkingen van normaal gedrag gecentraliseerd weergegeven worden.

Orange Cyberdefense oplossingen

Er zijn verschillende oplossingen te noemen om bovengenoemde uitdagingen te adresseren. Het is echter van belang dat geen wildgroei ontstaat aan verschillende apparatuur waardoor de complexiteit van het netwerk onevenredig toeneemt. Vanuit dit oogpunt kunnen we de onderstaande aanbevelingen doen.

- Het creëren van een baseline van normaal gedrag kan worden gedaan met dezelfde apparatuur dat wordt gebruikt voor het maken van een inventarisatie. Op een passieve manier wordt 'geluisterd' naar het verkeer op het netwerk. Afhankelijk van de complexiteit van het netwerk kan al na 2 weken een goed beeld worden geschetst van normale verkeerspatronen. Met behulp van 'Artificial Intelligence' (AI) en 'Machine Learning' (ML) kunnen afwijkingen in verkeerspatronen, bijvoorbeeld onder invloed van cyberaanvallen, snel worden opgemerkt.
- Door het luisteren naar het netwerkverkeer, gecombineerd met 'Deep Packet Inspection' (DPI) worden waardes van parameters uit de verkeersstromen gedestilleerd. Deze waardes worden over langere periode vastgelegd waardoor ook hier eenvoudig kan worden gerapporteerd over eventuele afwijkingen. Bovendien is het mogelijk om een bereik in te stellen waarbinnen specifieke waarden zich mogen bevinden en kan gealarmeerd worden wanneer een waarde buiten dit bereik valt.
- Het toepassen van een gedistribueerde oplossing maakt het mogelijk om op verschillende locaties, op verschillende punten in het netwerk te monitoren en de resultaten centraal weer te geven. Deze centralisatie is extra van belang om incidenten in verschillende delen van het netwerk te kunnen correleren. Hierdoor kan aan elk incident een realistische risico-score worden toegekend waardoor een geprioriteerd overzicht kan worden gegeven van verschillende gebeurtenissen in het netwerk.

> **Het is van belang dat er geen wildgroei ontstaat aan verschillende apparatuur, waardoor de complexiteit van het netwerk onevenredig toeneemt.**

Bij het kiezen van een oplossing is het van belang dat deze voldoet aan de eisen en wensen van de organisatie, ook waar het gaat om implementatie mogelijkheden. Zo kan er worden gekozen voor een 'on-premise' oplossing waarbij apparatuur in het eigen datacenter wordt geïnstalleerd, of er kan worden gekozen voor een installatie in de cloud.

Vanzelfsprekend moet de gekozen oplossing kunnen integreren met bestaande ticket systemen, een SIEM, en/ of een Next Generation Firewall.

Respond

De laatste pijler van het security lifecycle model heeft betrekking op het reageren op gebeurtenissen in het netwerk. Ook hierbij zijn een aantal uitdagingen te identificeren.

Uitdagingen

In veel gevallen is er een overvloed aan meldingen vanuit het netwerk. Niet zelden moeten deze meldingen stuk voor stuk worden bekeken en geclassificeerd, bij voorkeur in 'real time', 24 uur per dag, 7 dagen per week en 365 dagen per jaar. En vervolgens moet de juiste actie worden ondernomen. Hierbij komen we vaak de onderstaande uitdagingen tegen.

- De meeste organisaties zijn reactief waar het aankomt op reageren op gebeurtenissen in het OT-domein, zeker daar waar het cybersecurity betreft.
- Door gebrek aan een solide 'Cyber Response Plan' wordt ingeval van een cybersecurity incident vaak gefocust op het beperken van de schade.
- Het verkrijgen en behouden van mensen die voldoende zijn gekwalificeerd op het gebied van cybersecurity, met name in combinatie met het OT-domein, is lastig.

Orange Cyberdefense oplossingen

De uitdagingen in deze laatste fase van het lifecycle model zijn niet volledig op te lossen door de inzet van techniek. Hoewel de techniek uiteraard ondersteuning kan bieden moet een groot gedeelte worden ingevuld met de inzet van mensen.

- Een passend monitoring systeem kan real-time alarmeren op bijvoorbeeld afwijkingen in verkeerspatronen. Vervolgens is het wel noodzakelijk dat een medewerker actie onderneemt en de melding valideert en classificeert.
- Om het mogelijk te maken om meldingen juist te classificeren is het van belang dat er een Cyber Response Plan bestaat. Het opzetten hiervan kan lastig en tijdrovend zijn maar zal van onschatbare waarde blijken in geval van een cybersecurity incident.
- Het vinden en behouden van mensen met de juiste kwalificaties blijft een uitdaging voor vrijwel elk bedrijf. Op dit punt kunnen wij een helpende hand bieden door middel van onze Cyber SOC diensten.

Security Operations Center

Het continu monitoren van gebeurtenissen in het OT-domein, het classificeren van deze gebeurtenissen en het reageren op incidenten kan tijdrovend en ingewikkeld zijn. Op dit vlak kunnen wij ondersteuning bieden met ons Security Operations Center (SOC) waar specialisten op het gebied van industriële netwerken de meest tijdrovende taken van u kunnen overnemen.

Doordat het SOC niet alleen kijkt naar het OT-domein maar ook naar het IT-domein, is het mogelijk om de juiste correlatie toe te passen en daarmee de juiste prioritering aan gebeurtenissen mee te geven.

Een aantal veel voorkomende gebeurtenissen zijn:

- Nieuwe OT-assets worden aangesloten en beginnen te communiceren.
- Communicatiestromen vanuit het OT-domein naar internet.
- Afwijkingen van een baseline.

Afhankelijk van de gebeurtenis kunnen we adviseren over het opstellen van beveiligingsbeleid en dit eventueel implementeren op firewalls.

Middels vastgelegde procedures zorgen we ervoor dat duidelijk is wat u van ons kunt verwachten en op welke manieren we u kunnen ondersteunen.

Samenvattend

In dit whitepaper zijn diverse onderwerpen besproken die een organisatie kunnen helpen bij het beperken van het cybersecurity risico in het OT-domein. Hierbij is een onderscheid gemaakt tussen risico's van buitenaf en risico's van binnenuit, bijvoorbeeld door een ontevreden werknemer of een vergissing van goedbedoelende proces operator.

Samengevat zijn de meest noemenswaardige zaken uit dit paper als volgt.

- Het integreren van het OT-domein en het IT-domein neemt een cybersecurity risico met zich mee, vooral voor het OT-domein waarin het vaak lastig is om oudere apparatuur te beveiligen. Het is daarom van het grootste belang om te anticiperen op mogelijke cybersecurity incidenten waarbij een specifiek raamwerk gekozen kan worden ter ondersteuning. De samenwerking tussen werknemers uit het OT- en het IT-domein wordt belangrijker om adequaat te kunnen reageren op cybersecurity incidenten, waarbij het voor alle partijen duidelijk moet zijn wat de verantwoordelijkheden zijn.
- Cybersecurity begint met het creëren van zichtbaarheid. Met name van de OT-assets, de gebruikte protocollen in het industriële netwerk, de verkeersstromen tussen verschillende OT- en IT-assets en de zones waarin deze assets zich bevinden. Deze informatie, gecombineerd met het in kaart brengen van kwetsbaarheden van de OT-assets geven een duidelijk beeld van het huidige niveau van cybersecurity. Daarnaast kan een geprioriteerd overzicht worden gemaakt van acties die op de korte, middellange en langer termijn moeten worden ondernomen om de beschikbaarheid van het operationele proces te kunnen blijven garanderen.
- Pas segmentatie toe in het industriële netwerk door het creëren van zones met behulp van Next Generation Firewalls. Op deze manier kunnen kwetsbare systemen worden gegroepeerd in een zone waardoor de firewall specifiek beveiligingsbeleid kan toepassen. De apparatuur die gebruikt wordt voor het inventariseren van verkeersstromen kan worden geïntegreerd met de firewall zodat beveiligingsbeleid eventueel geautomatiseerd kan worden toegepast.
- Door het creëren van een baseline van verkeerspatronen kan snel worden gerapporteerd over afwijkingen. Dit is een bewezen manier voor het detecteren van malware, maar ook voor het signaleren van te grote afwijkingen van parameters. Door afwijkingen centraal te verzamelen in bijvoorbeeld een SIEM kan een correlatie worden gemaakt met cybersecurity incidenten in het IT-domein waardoor integraal inzicht ontstaat.
- Zorg voor een Cyber Response Plan voor het snel en juist kunnen reageren op cybersecurity incidenten zodat operationele processen zo snel mogelijk weer beschikbaar kunnen zijn.
- Ter ondersteuning van organisaties op het gebied van cybersecurity in het OT-domein kan het Security Operations Center van Orange Cyberdefense specifieke diensten leveren waarbij specialisten zowel het OT-domein als het IT-domein monitoren.

Contact informatie

OT/ICS specialist

Heeft u vragen over OT/ICS of ontvangt u graag meer informatie over dit onderwerp?

Neem contact met ons op via info@nl.orangecyberdefense.com of +31(0)88 123 4200.

Waarom Orange Cyberdefense

Orange Cyberdefense is de deskundige cybersecurity-businessunit van de Orange Group en biedt organisaties over de hele wereld managed security, managed threat detection & response-services. Als dé beveiligingsprovider van Europa streven we naar een veiligere digitale samenleving.

Wij zijn een bedreigingsonderzoeks- en inlichtingengestuurde beveiligingsprovider die ongeëvenaarde toegang biedt tot huidige en opkomende bedreigingen.

Orange Cyberdefense heeft een trackrecord van meer dan 25 jaar op het gebied van informatiebeveiliging, meer dan 250 onderzoekers en analisten, 16 SOC's, 10 CyberSOC's en 4 CERT's verspreid over de hele wereld en ondersteuning voor verkoop en services in 160 landen. We zijn er trots op dat we wereldwijde bescherming kunnen bieden met lokale expertise en onze klanten kunnen ondersteunen gedurende de gehele levenscyclus van bedreigingen.

Orange Cyberdefense

orange™