Blixt
Security. Done.

Operational Technology Security

Een basis aanpak voor de bescherming van zowel IT als OT/Industriële Controle Systemen

Industriële Controle Systemen (ICS) of ook wel Operational Technology (OT) genoemd, is een algemene term die de verschillende typen besturingssystemen omvat die worden gebruikt in industriële productie, inclusief Supervisory, Control and Data-Acquisition (SCADA) systemen; Gedistribueerde controlesystemen (DCZ's) en andere kleinere besturing systeemconfiguraties, zoals programmeerbare logische controllers (PLC's), die vaak te vinden zijn in industriële sectoren en kritische infrastructuren1.

> Vanwege de potentieel catastrofale impact van een cyberincident, hebben leidende beveiligingsbedrijven en CERT's in het verleden voorgesteld om ICS-netwerken op geen enkele manier direct met internet te verbinden.

Door onze aanpak te gebruiken, kan uw organisatie IT en ICS combineren.
Wees je bewust van de verschillen tussen de IT en ICS. ICS-ingenieurs kunnen leren van de IT-beheerprocessen, die vaak overeenkomen met de "IT" in de ICS-omgeving.
Binnen IT is men al jaren gewend naar de 'grote boze buitenwereld" te kijken en zich daartegen te beschermen. Binnen ICS is men daar minder ervaren mee.

Toch zijn de servers en de gebruikte operating systemen hetzelfde. Alleen de applicaties voor de aansturing van de ICS verschillen. Die verschillen zitten vooral in de uit te voeren handelingen/opdrachten en de gebruikte protocollen. Hoewel ook op dat gebied er de laatste jaren steeds meer integratie ontstaat. Seriële koppelingen bestaan alleen nog op oude systemen. IP is normaal geworden. Maar vergis je niet wat er nog aan oude zeer kwetsbare systemen in gebruik is.

[1] In de context van dit document wordt de term ICS gebruikt om het end-to-end systeem te definiëren. Dit omvat servers, netwerkverbindingen, bedieningsconsoles en apparaten zoals een PLC, IED's, robots en andere

ICS-beveiligingsbeheer

In de wereld van industriële controlesystemen (ICS's) is beveiligingsbeheer nog steeds een sterk onderbelicht onderwerp. ICS en kritieke infrastructuren zijn in toenemende mate verbonden met kantoorautomatisering en internet, waardoor deze systemen drastisch grotere veiligheidsrisico's lopen. Het inschatten en beheersen van deze beveiligingsrisico's is meer dan ooit nodig om de continuïteit van productieprocessen te waarborgen en zelfs levensbedreigende incidenten te voorkomen.

De verschillen tussen een ICS en traditionele IT variëren op veel manieren. Om te beginnen is het doel van een ICS compleet anders dan een IT-systeem. Een IT-omgeving is gebouwd om mensen van dienst te zijn die hun dagelijkse taken uitvoeren en automatiseert bedrijfsprocessen zoals facturering, voorraadbeheer, enzovoort. IT omvat de toepassing van computers en telecommunicatieapparatuur voor het opslaan, ophalen, verzenden en manipuleren van gegevens; en automatiseer herhaalde taken zoals het opstellen van rekeningen.

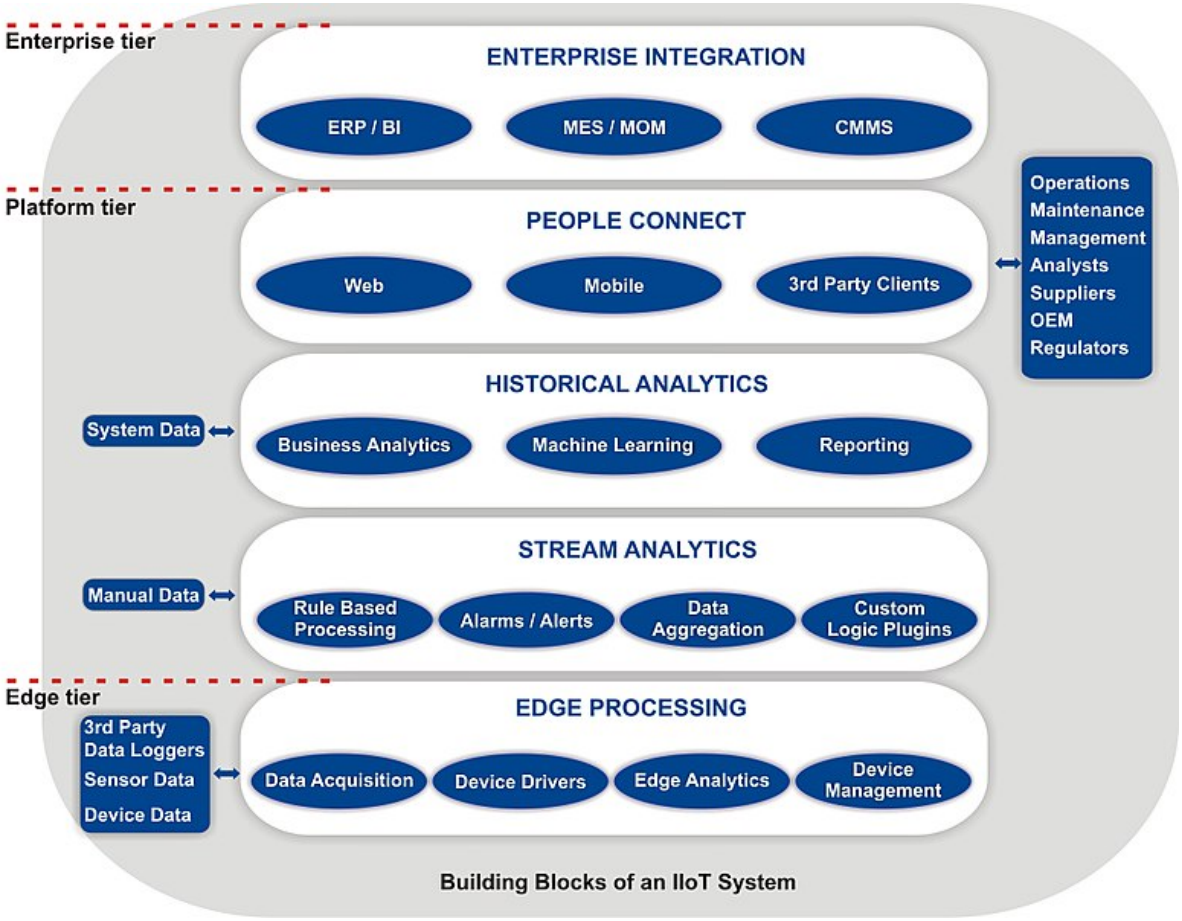
Een ICS is een automatiseringssysteem dat speciaal is ingericht voor het aansturen van industriële processen.

Deze omvatten productieprocessen in een fabriek of ondersteunende diensten zoals waterbeheer, verlichting, roltrappen, liften, opslagcontrole, transport en distributie van chemische producten, olie-, gas-, water- en/of elektriciteitsvoorziening, enzovoort. Door de verschillende aard van de omgevingen waarin IT-systemen en een ICS opereren en het verschillende doel dat ze dienen, is ook de mogelijke impact van incidenten totaal verschillend.

Incidenten in ICS-omgevingen kunnen gecontroleerde processen verstoren of gecontroleerde apparatuur vernietigen, zoals generatoren, pompen, kleppen, centrifuges, enzovoort. Het resultaat zijn catastrofale ongevallen die in extreme omstandigheden kunnen leiden tot letsel of overlijden. Als u bijvoorbeeld op het verkeerde moment een klep in een chemische fabriek opent, kunnen er giftige dampen of vloeistoffen in het milieu terechtkomen. Het verstoren van een regionale energiedistributie kan een onmiddellijk effect op de openbare veiligheid. Zelfs nucleaire rampen kunnen niet worden uitgesloten.

Terwijl ICS-omgevingen potentieel hebben voor rampzalige incidenten met een veel bredere impact, lag de focus altijd meer op veiligheid dan op beveiliging. Dit was te wijten aan ICS-controlesystemen ooit standalone of gekoppeld aan gesloten systemen. De urgentie voor beveiliging was er simpelweg niet, zoals in IT-omgevingen waar alle assets zijn verbonden via kwetsbare interne of externe netwerken.

Helaas is de urgentie voor het beveiligen van een ICS dramatisch veranderd omdat er veranderingen in connectiviteit van ICS-netwerken hebben plaatsgevonden. Vanwege de grootschalige en grote gevolgen van nadelige evenementen over nationale veiligheid, vitaliteit van de economie en volksgezondheid en veiligheid, het beschermen en beveiligen van ICS en omgevingen moeten een prioriteit zijn voor betrokken bedrijven en industrieën.



Figuur 1:"IT-OT Integratie

Ontwikkelingen in ICS vergroten beveiligingsrisico's

Bedrijven zijn altijd op zoek naar manieren om kosten te besparen en de productiviteit te verbeteren. Afhankelijk van de geografische spreiding van ICS-eindpunten, kan het onderhouden van speciale ICS-netwerken erg kostbaar zijn. Daarom hebben veel bedrijven hun IT- en ICS-netwerken geïntegreerd en een aanzienlijke kostenbesparing gerealiseerd. Tegelijkertijd stelden ze ICS in staat om rechtstreeks te communiceren met kantoorautomatiseringstools, zoals geografische informatiesystemen, verwerking van factureringsinformatie en Enterprise resource management-tools voor activabeheerdoeleinden. Dit is een groot voordeel voor medewerkers in de controlekamer, bedrijfsprocessen, factureringsautomatisering en rapportagemogelijkheden.

Toen ICS's werden geïntroduceerd, waren ze ontworpen om één specifieke functie uit te voeren, of om een bepaald productieproces aan te sturen. Door ICS-informatie echter

rechtstreeks terug te voeren naar de bedrijfsprocessen nam de bedrijfswaarde van deze systemen enorm toe. Dus de ICS-waarde is gewijzigd.

Het verbinden van ICS- en IT-netwerken zorgt nu automatisch voor een indirecte verbinding tussen het Internet en de ICS-omgeving. Nu zijn ICS plotseling kwetsbaar voor internet gerelateerde bedreigingen. Net zoals de IT-omgeving al jaren is. Dit is een gegeven dat bedrijven zich niet altijd realiseren.

In vergelijking met de snel veranderende wereld van IT, zijn veranderingen in de ICS-wereld extreem traag. Een levenscyclus van drie tot vijf jaar voor IT-systemen is min of meer de baseline. Industriële componenten zijn ontwikkeld om jarenlang ongestoord te functioneren. Met een levenscyclus van ICS-besturingssystemen die 15 tot 20 jaar of langer meegaan. Wanneer een ICS-component wordt gecompromitteerd, kan een heel productieproces worden stopgezet, of erger.

Het risico neemt ook nog eens toe wanneer het onderhoud van het ICS wordt uitgesteld of achterwege gelaten, inclusief het onderhoud aan geïnstalleerde software en besturingssystemen, en het ontbreken van de noodzakelijk security patches. Ook de vervanging van niet langer ondersteunde software wordt zo lang mogelijk uitgesteld. Denk hierbij aan Windows- en Linux Operating systems die al lang niet meer ondersteunt worden en waar dus geen beveiligingslekken meer in opgelost worden.

Afhankelijk van de branche kan een cyberaanval op een ICS catastrofale gevolgen hebben voor het toekomstige bestaan van een bedrijf en/of de directe omgeving. Zelfs verlies van mensenlevens kan niet uitgesloten worden. Zonder het juiste beveiligingsniveau te implementeren, is een cyberincident onvermijdelijk omdat niet-gepatchte systemen extreem kwetsbaar zijn, waardoor ze een gemakkelijk doelwit zijn.

De dreiging van ICS-cyberaanvallen

Vanwege de potentieel catastrofale impact van een cyberincident, hebben toonaangevende beveiligingsbedrijven en Computer Emergency Response Teams (CERT's) geadviseerd ICS-netwerken volkomen gescheiden te houden van het internet.

Bijna alle bedrijven hebben dit advies lang gevolgd en dus waren aanvallen op een ICS bijna niet mogelijk.

Het gebrek aan externe verbindingen dwong aanvallers om alternatieve aanvalsmethoden te zoeken, zoals fysieke inbraak in het pand, of door malware te verspreiden via draagbare media, verspreid onder onoplettende werknemers.

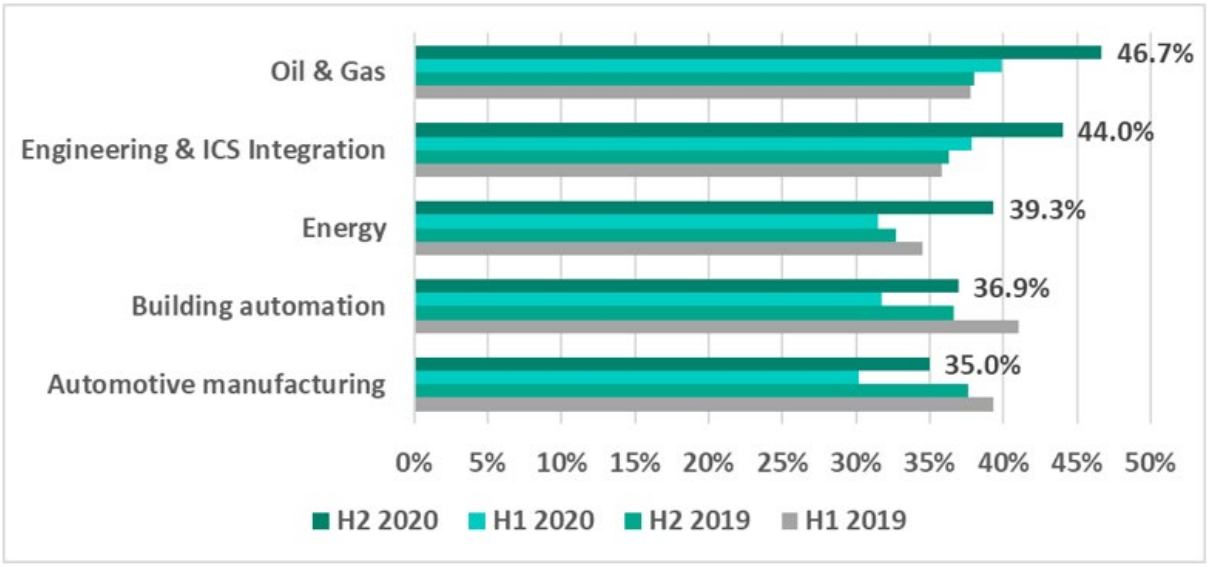
Hoewel we het alweer over 2012 hebben, 9 jaar geleden, was Stuxnet de ultieme wake-up call voor met name de energiesector. De aanvalsmethodiek zelf kan echter overal toegepast worden. Stuxnet is geschreven om een heel specifiek type procesbesturingssysteem aan te vallen van een bepaalde leverancier. Het was gericht tegen de Iraanse nucleaire sector. Stuxnet werd via draagbare media overgebracht.

Hoewel het niet duidelijk is wie het virus heeft gemaakt, is de broncode van de aanval is vrijgegeven via internet, dus het kan en kan worden gebruikt, herschreven en ingezet door iedereen die er zin in heeft. Stuxnet was de eerste van vele ICS-virussen die volgden.

Een terugblik op 2020

In 2020 heeft de industriële gemeenschap verbazingwekkende prestaties geleverd om de beschaving te laten draaien onder extreem uitdagende omstandigheden met de wereldwijde pandemie. Infrastructuuraanbieders hielden belangrijke diensten en goederen beschikbaar, waaronder elektriciteit, gefabriceerde goederen, water, olie en gas, mijnbouw, chemie, spoorwegen en transport.

Als gevolg van deze inspanningen hebben organisaties hun manier van zakendoen verschoven naar een steeds meer verbonden industriële omgeving. Dit is een trend die al vele jaren bestaat, hoewel veel organisaties nog steeds dachten dat ze sterk gesegmenteerde of zelfs air-gapped ICS-netwerken hadden.



Figuur 2: Percentage ICS computers waar malicious objecten op werden geblokkeerd in de genoemde industrieën[2]

Het risico voor ICS komt niet voort uit een convergentie van IT en OT, maar uit een convergentie van een steeds meer ICS-bewust en capabel dreigingslandschap met de digitale transformatie en hyperconnectiviteit van de industriële gemeenschap. Het ICS Cybersecurity Year in Review-rapport van 2020[3], dat nu zijn vierde jaar ingaat, legt vast hoe een deel van de gemeenschap presteert en vordert, en welke verbeterpunten nodig zijn om veilige en betrouwbare operaties te blijven bieden.

Belangrijkste bevindingen

- **90%** van de serviceopdrachten omvatte een bevinding rond gebrek aan zichtbaarheid in OT-netwerken.

[2] Bron: https://www.kaspersky.com/about/press-releases/2021_threats-against-industrial-control-systems-on-the-rise-in-h2-2020
[3] Bron: https://www.dragos.com/blog/industry-news/2020-ics-cybersecurity-year-in-review/

- Er werden **vier nieuwe dreigingsgroepen** ontdekt met de beoordeelde motivatie om zich op ICS/OT te richten, goed voor een **toename van 36%** in bekende groepen.
- Het **misbruiken van geldige accounts** was de nummer één techniek die werd gebruikt door benoemde bedreigingen.
- **54%** van de serviceopdrachten omvatte een bevinding over gedeelde referenties in OT-systemen.
- **88%** van de serviceopdrachten bevatte een bevinding over onjuiste netwerksegmentatie.
- **43%** van de ICS-kwetsbaarheidsadviezen bevatte fouten die het moeilijk zouden maken om prioriteit te geven aan oplossingen.
- **64%** van de adviezen die geen patch hadden, hadden ook geen praktisch mitigatieadvies van de leverancier.
- **61%** van de adviezen met een patch had geen alternatief mitigatieadvies van de leverancier, behalve het aanbrengen van de patch, wat in veel industriële organisaties moeilijk of aanzienlijk vertraagd kan zijn.

ICS-bedreigingslandschap

De dreigingsactiviteit van ICS blijft toenemen, zowel wat betreft het aantal verschillende groepen dat we volgen als de sectoren en regio's waarop ze zich richten. Dragos-analisten ontdekten vier verschillende nieuwe ICS-activiteitengroepen die voornamelijk gericht zijn op energie en productie, bekend als KAMACITE, STIBNITE, TALONITE en VANADINITE.

In de loop van 2020 werd ook waargenomen dat de 11 activiteitengroepen die vóór 2020 waren geïdentificeerd, hun gerichtheid op nieuwe sectoren en regio's uitbreidden en hun gedrag aanpasten, waarbij velen probeerden de verschuiving naar werken op afstand te benutten om toegang te krijgen tot industriële netwerken.

Inmiddels heeft Ransomware zijn weg gevonden naar ICS. Met de toename van bedreigingen, werd er ook vooruitgang geboekt bij het in staat stellen van IT-beveiligingsteams om OT-netwerken, bedreigingen en potentiële effecten beter te begrijpen met de release van het MITRE ATT&CK voor ICS-framework.

ICS-kwetsbaarheden

Dragos analyseerde in 2020 703 ICS/OT-kwetsbaarheden, een stijging van 23% ten opzichte van het voorgaande jaar. Het aantal adviezen met fouten (43%) zette een stijgende lijn door, wat zorgwekkend is en problemen geeft met triage. De frequentie van uitgebrachte adviezen zonder patch en zonder alternatief mitigatieadvies bleef relatief consistent met hun bevindingen in 2019.

Lessen getrokken uit de frontlinies

Nu de bedreigingen toenemen, zien we nog steeds dat een meerderheid van de organisaties, worstelen met de zichtbaarheid van OT-netwerken en daarmee het vermogen om abnormale activiteit te detecteren. Er zijn nog steeds problemen met de juiste netwerksegmentatie. In feite is er op beide gebieden een toename in vergelijking met 2019. Er is enige verbetering in de IT/OT-samenwerking, waarbij een groter deel van de organisaties een Incident Response Plan heeft.

Aanpak op korte termijn

Op de korte termijn worden bekende kwetsbaarheden en snel identificeerbare dreigingen op een hoog niveau aangepakt. Het werk omvat het identificeren van de belangrijkste activa van de organisatie en het identificeren van de belangrijkste security risico's. Voer Quick-wins door. Maatregelen die gemakkelijk en snel zijn geïmplementeerd, met een korte doorlooptijd en relatief lage kosten.

Algemene beveiligingschecklists, zoals SANS ICS Top 20, kunnen je helpen bij het identificeren van de belangrijkste maatregelen.

Kortom, de korte termijn aanpak is een vorm van symptoombestrijding.

Sommige beveiligingsrisico's kunnen zijn gemitigeerd of verminderd, maar uw ICS-beveiliging en risico's zijn nog steeds niet onder controle. Wat ontbreekt er is een structurele, op risico's gebaseerde benadering van beveiligingsbeheer. Dit is het doel om te bereiken in de aanpak op lange termijn.

Beide benaderingen kunnen gelijktijdig worden gestart en uitgevoerd, maar de korte termijn De resultaten van de aanpak moeten worden gedocumenteerd en gebruikt als input voor de lange termijn aanpak.

Lange termijn aanpak

Het doel van de activiteiten in de lange termijn benadering is het verhogen van de efficiëntie van de implementatie van beveiligingscontroles en bescherming van organisatiedoelen door het opzetten van een ICS-programma voor beveiligingsbeheer. Een beveiligingsbeheerprogramma kan in een deel worden verdeeld in een organisatorisch ICS-beveiligingsbeheer en een risicobeheergedeelte.

In het governance-gedeelte van het programma, dat de eerste fase is van de lange termijn aanpak, is de doelstelling is het definiëren van een organisatie brede ICS-beveiligingsorganisatie, een ICS-security framework en een ICS-beveiliging strategie die past bij de doelen en doelstellingen van de organisatie.

Het security framework zal bestaan uit beleid, verklaringen, richtlijnen en processen die nodig zijn om de gedefinieerde beveiligingsstrategie te handhaven en te ondersteunen.

Het belangrijkste proces dat moet worden opgezet, is het risico-beheerproces, dat uiteindelijk zou moeten zijn geïmplementeerd in alle afdelingen van de organisatie die betrokken zijn bij IT- en ICS-functionaliteit en processen.

Risicomanagement moet onderdeel zijn van de dagelijkse bedrijfsvoering, in plaats van ad hoc-activiteiten.

Opgemerkt moet worden dat hoewel ICS en IT op zich heel verschillend zijn, als we kijken naar het doel ze dienen en, tot op zekere hoogte, het soort omgevingen waarin ze bestaan; het proces van het beheersen van risico's waarmee ze allebei worden geconfronteerd, goed vergelijkbaar en gelijkelijk toepasbaar is.

Als uw organisatie al een IT-risico heeft managementproces en/of organisatie, is het raadzaam gebruik te maken van de beschikbare kennis, en combineren IT- en ICS-risicobeheer. Uiteindelijk hebben beide hetzelfde doel te bereiken: ervoor zorgen dat

organisatiedoelen en doelstellingen op een veilige en verantwoorde manier kunnen worden bereikt.

De volgende lijst toont de activiteiten die op een geordende manier moeten worden ingezet, en kunnen als leidraad worden gebruikt om de einddoelen te bereiken.
Het is aan elke organisatie om haar IT/ICS security vorm te geven in een programma naar zijn behoeften en voorkeuren.

1. Definieer een bedrijfsstrategie
2. Zet een beveiligingsorganisatie op die verantwoordelijk is voor het beveiligingsbeheer, en de creatie en implementatie van het securitymanagementprogramma.
3. Kies een bestaand beveiligingsraamwerk dat past bij de belangen van uw organisatie of creëer uw eigen (beleids-)kader.
4. Zet een risicobeheerproces op dat van nature herhaalbaar is en moet worden gevolgd in een stapsgewijs proces.
5. Stem de beveiligingsbeheerfasen af op bestaande beheerprocessen.
6. Als er geen formeel beheerproces bestaat, gebruik dan het proces zoals dat beschreven wordt in het gekozen security managementsysteem zoals ISO 27001/ISO 27005.
7. Identificeer en classificeer gerelateerde bedrijfsdoelen, betrokken activa en bepaal de risicobereidheid.
8. Identificeer kwetsbaarheden en impact van incidenten op activa.
9. Overweeg mitigerende maatregelen op basis van processen, mensen en technologie en classificeer de impact van mitigerende maatregelen op risico's.
10. Realiseer je dat er soms maatregelen moeten worden genomen op basis van wettelijke verplichtingen - denk waar mogelijk over overdraagbare risico's, mitigeerbare risico's, acceptabele risico's of vermijdbare risico's.
11. Voer een gap-analyse uit om de kloof tussen ideale situatie en de huidige situatie vast te stellen.
12. Prioriteer de te nemen maatregelen op basis van impact (oplossend vermogen) en kosten en benoem verantwoordelijke eigenaren.

Maak de eerdergenoemde roadmap en start implementatie projecten.

Beveiligingsstatistieken

Als iets meetbaars niet wordt gemeten, wordt het veel moeilijker om het te verbeteren. Dit is de reden waarom beveiligingsstatistieken vanaf het begin bij de ontwikkeling moeten worden gedefinieerd en geïmplementeerd in uw beveiligingsbeheersysteem. De resultaten van metingen geven informatie die helpen bepalen waar de focus voor verbetering moet liggen. Dit geldt natuurlijk ook voor verbeteren van

IT- en ICS-beveiliging. Een rapport met beveiligingsstatistieken moet informatie bevatten over de gebieden van mensen, processen en technologie.

Het uiteindelijke doel van beveiligingsstatistieken is tweeledig:

Beveiligingsstatistieken geven de managementinformatie over beveiliging. Ze helpen demonstreren naleving door IT/ICS-beheer.

Meetresultaten rechtvaardigen het budget voor informatiebeveiliging en helpen bij het onderbouwen van budgetten voor nieuwe investeringen.

Een meting met een langere tijdspanne (maandelijks/kwartaal/jaarlijks) geeft een veel betere weergave van de werkelijkheid. De implementatie van een raamwerk voor veiligheidsstatistieken, als volgende stap, zal helpen om de nodige zichtbaarheid te krijgen van de staat van IT- en ICS-beveiliging. Met meetbare gegevens, kunnen vragen als de volgende worden beantwoord:

- Met welke informatiebeveiligingsrisico's lopen we?
- Is uw beveiligingshouding het afgelopen jaar verbeterd?
- Wat zijn de meest urgente veiligheidsproblemen die we moeten aanpakken?
- Welke investeringen in informatiebeveiliging leveren de beste waarde op?
- Hebben investeringen in beveiliging vruchten afgeworpen?
- Op welk onderdeel van beveiliging moet u zich volgend jaar concentreren?
- Hoe vergelijk ik met mijn branchegenoten?

Meer weten?

Neem dan vrijblijvend contact op met Blixt Security Solutions

Over de auteur

Hans Baars is onafhankelijk cybersecurityconsultant, heeft 23 jaar ervaring in IT- en OT/ICS informatiebeveiliging. Voordat Hans als onafhankelijk adviseur bij HPE kwam werken, bekleedde hij verschillende functies binnen de Nationale Politie o.a. op het gebied IT auditing en als adviseur integrale veiligheid. Na zijn overstap naar het bedrijfsleven werkte hij als (Cyber) Security adviseur voor o.a. Enexis, DNV-GL, HPE, en Omnetric (Siemens) met een belangrijke focus op Industriële Controle Systemen.

Blixt Security. Done.

Hans is IT-auditor en is CISA, CISSP en CISM gecertificeerd. Hij is te bereiken op j.h.baars@blixt.nl