Starten met IEC 62443

Korte handleiding

www.securitydelta.nl/ipcs

IPCS
INDUSTRIEEL
PLATFORM
CYBER SECURITY

Revisie

datum	naam	revisie
10-apr-2025	Philip Roodzant	Eerste IPCS (HSD) uitgave – 2025Q2
11-apr-2025	Marcel Jutte	QC en contactinformatie geactualiseerd

Voorwoord

Voor het opzetten van een goed beveiligingsbeleid van uw OT omgeving is de IEC 62443 een prima hulpmiddel. Omdat het op het eerste gezicht lastig is te bepalen waar te beginnen in de omvangrijke standaard, hebben de leden van het Industrieel Platform Cyber Security (IPCS) deze korte handleiding voor u geschreven. Deze leden zijn in het dagelijks leven werkzaam als IT/OT cybersecurity specialist of -consultant bij eindgebruikers, systemintegrators en leveranciers (vendoren).

De handleiding bestaat uit een aantal stappen, waarbij wordt geadviseerd deze in de beschreven volgorde[1] uit te voeren. U zult waarschijnlijk al snel zien dat u al best het nodige gedaan hebt om uw OT omgeving te beschermen. Deze handleiding helpt u om hier meer structuur in te brengen om vervolgens de diepte in te gaan.

Let op dat bij wijzigingen elke stap opnieuw doorlopen moet worden zie hiervoor hoofdstuk 8.

[1] De volgorde wijkt iets af van datgene wat in de norm omschreven is, er is gezocht naar een praktische start en zoveel mogelijk aan te sluiten bij datgene wat in veel gevallen al aanwezig is binnen een bedrijf.

1.Asset register

IEC 62443
Normdelen
2-1, 2-4, 3-2

Apparatuur in een netwerk waarvan niemand weet dat die er is, is niet te beschermen. De eerste vraag is dan ook: wat is er allemaal aanwezig in uw netwerk? Een eenvoudige vraag, maar het beantwoorden ervan kost soms de nodige tijd.

Een ‘asset register’ is een overzicht van alle systemen die met uw netwerk verbonden zijn. Dat klinkt niet al te moeilijk, maar is het vaak wel. Er is namelijk veel méér aan een netwerk gekoppeld dan op het eerste gezicht gedacht wordt. Denk daarbij bijvoorbeeld aan:

- PLC’s, DCS en embedded systemen en hun onderdelen
- Safety controllers, SIS
- Remote I/O, frequentie-omvormers, sensoren, barcode scanners, RFID lezers etc.
- SCADA systemen, bedienterminals, HMI’s, monitors
- Switches, routers, gateways, wifi access points, firewalls, etc.
- Printers, beeldschermen, etc.
- Bewakingscamera’s, toegangscontrolesystemen, badge-lezers, etc.
- Gebouwbeheerssystemen

Ervaringen uit de praktijk leren dat organisaties soms meer dan twee keer zoveel systemen aan een netwerk hebben gekoppeld dan bekend is.

Door goed in kaart te brengen welke systemen u in gebruik heeft, kunt u beter bepalen welke systemen u moet beschermen. Met behulp van Excel is al heel eenvoudig een asset register op te stellen. Begin met het opschrijven van het merk, type, software-versie en het IP-adres van het systeem en breidt de lijst uit met voor u belangrijke gegevens (bijvoorbeeld: locatie en eigenaar).

Een volgende stap is om met speciale software een deel van uw assets automatisch te laten inventariseren. Het deel wat nog niet automatisch geïnventariseerd wordt, blijft u bijhouden in uw Excellijst.

Nog een stap verder is het volledig automatiseren van de asset inventarisatie met speciale hard- en software (zie ook hoofdstuk 7) en door te groeien van een asset register naar een CMDB (configuration management database). In een CMDB kunnen ook relaties tussen assets worden vastgelegd.

In de praktijk blijkt vaak dat het asset register snel veroudert, omdat wijzigingen aan een netwerk worden uitgevoerd zonder terugmelding. Daarmee verliest het asset register snel aan waarde, en dat heeft consequenties voor andere processen (zoals back-up- en patch-management) die we hieronder zullen beschrijven. Ook hierom is een automatische asset inventarisatie aan te bevelen.

Voorbeelden van assetregisters zijn te vinden in **Bijlage 1 en 2.**

2. Datastromen

IEC 62443
Normdelen
2-1, 3-2, 3-3

Nadat u weet welke systemen u heeft, is het tijd om te bepalen welke systemen met elkaar communiceren. Deze gegevens legt u vast in een ‘Datastromen register’ of ‘connectivity database’.

Daar kan zoal instaan:

- Wie communiceert er met wie
- Waarom doen ze dit
- Wat voor data wordt er uitgewisseld, en met welke frequentie

Deze informatie is belangrijk om straks een goede risico-inventarisatie op te kunnen stellen. Als bijvoorbeeld systeem A besmet is met malware, en systeem A veel communiceert met systeem B, dan is het zeer aannemelijk dat systeem B ook snel besmet raakt met de malware.

Het datastromen register is een belangrijke bron van informatie dat een actueel overzicht bevat van de verzameling van verschillende soorten één- en twee-richtingen datastromen tussen systemen.

Doel van het register is het valideren en verkrijgen van een overzicht van alle datastromen tussen alle interne systemen én alle datastromen tussen interne- en externe systemen, om vervolgens via de firewall alléén communicatie toe te staan tussen systemen (en netwerken) die met elkaar mogen communiceren.

Nut van het register

Het is belangrijk om te beschikken over een actueel en volledig datastromen register, dit omdat het in veel situaties gebruikt kan worden, denk hierbij aan:

- Inzicht verkrijgen in de werking van netwerken, systemen en applicaties
- Bepalen van de juiste configuratie van netwerk-, systeemcomponenten en applicaties
- Identificeren van legitieme en niet-legitieme verkeersstromen
- Sneller oplossen van storingen en communicatieproblemen
- Belangrijke informatie voor opstellen van het risicoprofiel
- Bepalen van de impact bij het toevoegen van nieuwe netwerk-, systeemcomponenten of applicaties

Wanneer er geen actueel en volledig beeld is van de datastromen, is het onmogelijk om te bepalen of switches, routers, netwerk- en systeemfirewalls op een correcte wijze zijn geconfigureerd en er voldoende beveiligingsmaatregelen zijn getroffen om systemen zo optimaal mogelijk te beschermen.

Wat wordt geregistreerd

In het datastromen register wordt (onder andere) de volgende basisinformatie vastgelegd;

- Bron- en bestemmings- IPv4/IPv6 adres van systemen
- Transport protocol
- TCP/UDP protocol poortnummers
- Gebruikte methode van data-encryptie
- Naam van het systeem (applicatie)
- Welke data wordt uitgewisseld met welke frequentie
- Reden voor communicatie

Het datastromen register vormt dé enige bron waarin is beschreven en bepaald welke systemen (en netwerken), op welke wijze met elkaar mogen communiceren.

Nog een stap verder is het volledig automatiseren van het bijhouden van de datastromen met speciale hard- en software (zie ook hoofdstuk 7).

Voor een voorbeeld van een datastromen register zie **Bijlage 3**.

3. Risico Inventarisatie

IEC 62443
Normdelen
2-1, 3-2

Cybersecurity vraagt om permanente monitoring met name in Industriële automatisering. Bovendien vergt het veilig houden van dergelijke digitale systemen om maatregelen die afwijken van de standaard ICT methodieken. Er dient altijd een afweging gemaakt te worden tussen kosten/investeringen en het managen van risico's in de digitalisering.

De risico's gedurende de lifecycle van een product of installatie zijn continu aan verandering onderhevig. Daarom is het van belang om een continu beeld te hebben van de dreigingen, zwakheden en incidenten en de gekozen maatregelen daarop aan te passen.

Het sturen daarop gebeurt vanuit risicomanagement. Periodiek dient er een risico- inventarisatie gemaakt te worden waarin alle dreigingen en zwakheden van een installatie in beeld worden gebracht.

Door de impact en de kans te kwalificeren kan het risico worden vastgesteld en kunnen de maatregelen worden bepaald. Risico's kunnen betrekking hebben op: mens/milieu, processen, en techniek. Bij het oplossen van incidenten moet een risicoanalyse plaatsvinden op het incident.

Het is van belang dat elke organisatie een overzicht heeft van de risicobereidheid. Dit dient de basis te zijn voor het risicomanagement. Op die manier kan bijvoorbeeld een 3-3 of een 5-5 matrix worden gemaakt. De kleuren van de vlakken geven de bereidheid aan.

Met de reeds verzamelde gegevens is het nu mogelijk om de risico's in kaart te brengen. Een goede methode om mee te beginnen is: RISICO = KANS X IMPACT.

	Kans Laag	Kans Middel	Kans Hoog
Impact Laag	Risico Zeer Laag	Risico Laag	Risico Middel
Impact Middel	Risico Laag	Risico Middel	Risico Hoog
Impact Hoog	Risico Middel	Risico Hoog	Risico Zeer Hoog

Figuur 1, voorbeeld van een risicomatrix

De risicokleuren bepalen de risicoacceptatie, en zal per bedrijf/situatie bepaald moeten worden.

De impact kan zich o.a. uiten in: verlies van mensenlevens, geld, milieu-, imagoschade en verlies van product.

Er zijn verschillende impactcategorieën; elk bedrijf zal moeten bepalen welke voor haar relevant zijn.

De bepaling van de KANS kan bijvoorbeeld volgen uit:

ZEER ONWAARSCHIJNLIJK	ONWAARSCHIJNLIJK	MOGELIJK	KANSRIJK
Nog nooit voorgekomen	Is in de branche/bedrijfstak wel eens voorgekomen	Is in het bedrijf wel eens voorgekomen	Het situatie doet zich verschillende keren per jaar voor

De bepaling van de IMPACT kan bijvoorbeeld volgen uit:

Categorie	Hoog	Middel	Laag
Verwonding	Dood, verminking	Ziekenhuisopname	Eerste hulp/BHV
Financieel verlies	Miljoenen €	€ 100.000's	€ 1000's
Milieuschade	Permanent	Langdurig	Tijdelijk / lokaal
Onderbreking van productie	Weken	Dagen	Uren
Aantasting imago	Permanent	Langdurig	Tijdelijk

Door op een simpele manier te beginnen, voorkomt u vast te lopen in allerlei details. Als u deze basis gereed heeft, kunt u eventueel overgaan tot een verdiepingsslag voor de systemen waarbij het risico zeer hoog is.

Bepalen van de maatregelen

Nadat alle risico's geclassificeerd zijn kunnen de maatregelen bepaald worden die de impact en/of kans verkleinen. We kennen een aantal strategieën om risico's te mitigeren: Verkleinen, Voorkomen en Verleggen. Is mitigatie niet mogelijk of wenselijk dan zal het risico geaccepteerd moeten worden.

Een voorbeeld zou kunnen zijn:

Cyber Risico	Kans	Impact	Risico	Maatregel	Kans na toepassen maatregelen	Impact na toepassing maatregel	Risico
Ongeoorloofde toegang op systemen	2	3	6	- Toepassen 2 factor authenticatie - Toepassen tokens	1	3	3

Nadat de maatregelen zijn uitgevoerd vindt er een nieuwe risicoclassificatie plaats. Is het risico nog steeds te hoog, dan moeten verdere maatregelen getroffen worden.

Op deze manier vindt elke jaar een nieuwe beoordeling plaats van de dreigingen en de risico's, en wordt vastgelegd of de genomen maatregelen nog het gewenste effect bereiken.

Bijvoorbeeld, een 'Zeer hoog' risico heeft de waarde 9, een 'Zeer laag' risico de waarde 1.

Waardeketen

Maatregelen kunnen worden genomen op het vlak van kans- en/of impactbeperking.

Het is wel van belang dat de gehele waardenketen van het bouwen, inbedrijfstellen, en de operationele fase van een industriële installatie wordt meegenomen in de analyse, van toeleverancier, opdrachtnemer en opdrachtgever.

4. Back-up Management

IEC 62443
Normdelen
2-1, 2-4, 3-3,

Hoe goed een netwerk ook beveiligd is, er is altijd een kans dat malware toch zijn slag kan slaan. Een recent Nederlands voorbeeld is de ransomware op de universiteit van Maastricht, die alle bestanden (en de back-up!) onleesbaar maakte. Ook ‘wipers’, malware die de harde schijf formatteert, kunnen leiden tot massaal dataverlies.

Om bij een catastrofe, zoals brand of malware, in staat te zijn de systemen te herstellen, is het belangrijk om goede back-ups te hebben.

3-2-1 Back-up strategie

Voor het maken van back-ups is ‘3-2-1’ back-up strategie een goed uitgangspunt. Een 3-2-1 back-up strategie betekent dat u ten minste **3** kopieën van uw gegevens heeft, waarvan **2** bewaard lokaal op verschillende opslagmedia en ten minste **1** exemplaar off-site. Deze laatste kan bijvoorbeeld bij een cloud-provider worden opgeslagen, of (op tape of disk) bij iemand thuis.

Op deze manier is er een grote kans dat er een betrouwbare back-up beschikbaar is vanaf waaraf de getroffen systemen hersteld kunnen worden.

Herstelmethode

Bepaal per systeem (zie: asset register) of een back-up noodzakelijk/zinvol en mogelijk is. Kleinere (embedded) apparaten hebben vaak geen back-up mogelijkheid.

Als het sneller is om bij een calamiteit het systeem opnieuw in te richten, zorg er dan voor dat alle benodigde software, installatie-handleidingen, en eventuele licenties, beschikbaar zijn. Let er op dat voor het activeren van licenties vaak internet-connectiviteit nodig is, en die kan op kritieke momenten misschien niet (volledig) beschikbaar zijn, omdat de benodigde infrastructuur misschien zelf ook getroffen is door de malware.

Aantal

Als een back-up noodzakelijk geacht wordt, bepaal dan hoe vaak er een back-up gemaakt moet worden, hoeveel versies er bewaard moeten worden en hoelang deze bewaard moeten blijven. Kan er volstaan worden met een aantal incrementele (gedeeltelijke) back-ups, gevolgd door bijvoorbeeld een wekelijkse full back-up; of moet er dagelijks een volledige back-up gemaakt worden? Dat hangt af van de frequentie waarmee bestanden wijzigen. Wijzigt er niets, dan is een dagelijkse back-up natuurlijk niet nodig.

Het kan ook zijn dat een maandelijkse back-up volstaat, bijvoorbeeld bij applicatie-servers waarbij nauwelijks wijzigingen op de server plaatsvinden.

Back-ups moeten ook gemaakt worden nadat op een apparaat een nieuwe softwareversie of een patch is geïnstalleerd.

Restore

Kijk ook naar de tijd die nodig is om een back-up terug te zetten (restoren). Als er een grote calamiteit optreedt, kan het zijn dat er meerdere systemen teruggezet moeten worden.

Denk er van tevoren over na welke systemen als eerste weer beschikbaar moeten zijn. Houd hier rekening mee als je gaat restoren. Een restore duurt langer als er meerdere systemen tegelijkertijd teruggezet moeten worden. Door dit slim te plannen, kunnen belangrijke systemen eerder weer beschikbaar gemaakt worden.

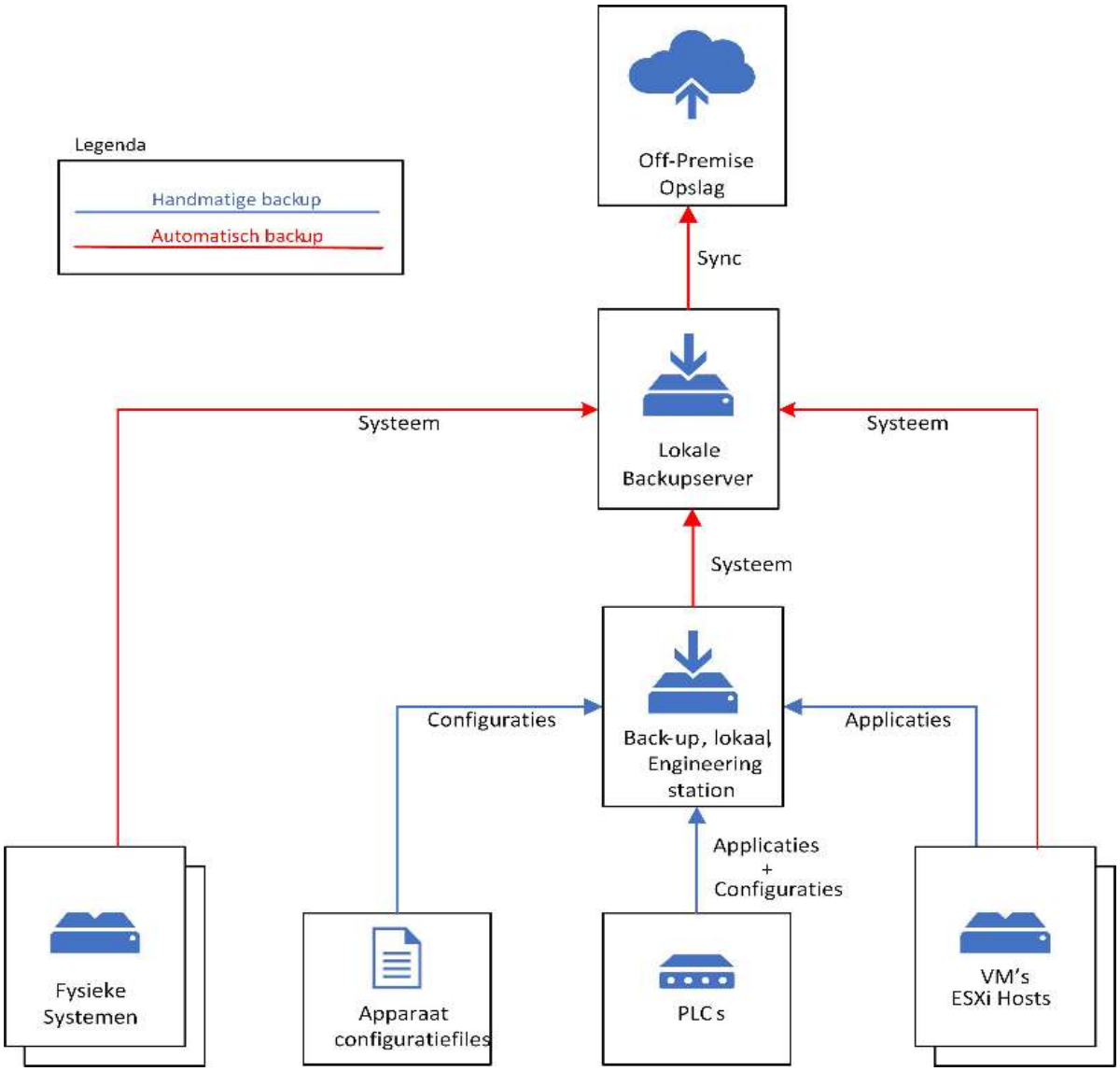
Oefenen en Testen

De restore van back-ups moet ook regelmatig geoefend en getest worden. Zo komen onvolkomenheden in de procedures aan het licht. Ook problemen met de media (disk, tape, cd-rom, etc.) worden zo zichtbaar, u zult de eerste niet zijn die erachter komt dat op de back-up media helemaal geen data staat, of dat de media niet meer te lezen zijn. Door de restore te testen weet u ook hoeveel tijd dit kost.

Back-up types

Er wordt onderscheid gemaakt tussen verschillende soorten back-ups:

- **Applicatie back-up**: van de gerealiseerde applicatie, bijvoorbeeld de PLC of de SCADA software. Meestal kan hier gebruik gemaakt worden van de mogelijkheden van de applicaties zelf. Bijvoorbeeld, de back-up van een Siemens PLC wordt gemaakt met de ontwikkelomgeving die ook voor het programmeren van de PLC wordt gebruikt.
- **Configuratie back-up**: in het geval van SCADA betreft dat bijvoorbeeld de back-up van de configuratie-bestanden per computer waarin is vastgelegd wat de rol van een specifieke computer in de configuratie wordt. Een configuratieback-up kan ook de instellingen bevatten van het besturingssysteem zoals bijvoorbeeld de voorgeschreven instelling van de datum/tijd notatie.
- **Software back-up**: van de softwarepakketten die op de systemen geïnstalleerd zijn, bijvoorbeeld installatiebestanden van de besturingssystemen, ontwikkelomgevingen, licenties, softwarebibliotheken, en PLC programmeersoftware.
- **Systeem back-up**: het besturingssysteem zelf, evenals alle configuraties, licenties, geïnstalleerde applicaties, gebruikersgegevens en databases. Dit betreft dus zowel virtuele machines als fysieke machines.



Figuur 2, Back-up architectuur

Bij voorkeur wordt van een back-up een hash vastgesteld. Hiermee kan altijd de authenticiteit worden vastgesteld: als er ook maar één bit wijzigt in een bestand, zal de hash anders zijn.

Configuratie back-up

De configuratie back-up kan bestaan uit een installatiehandleiding waarin staat beschreven hoe een systeem moet worden ingericht om zijn rol binnen de configuratie te vervullen. Dit is handig wanneer veel identieke systemen in de configuratie aanwezig zijn die alleen in identificatie en netwerkadres van elkaar verschillen.

Door in deze situatie één systeem back-up te maken, vergezeld van een configuratie back-up waarin staat beschreven wat de aan te passen parameters zijn, wordt het beheren van de back-up eenvoudiger. Voor welke systemen deze werkwijze geldt zal ook gedocumenteerd moeten worden.

5. Patch Management

Normdelen
2-1, 2-3, 2-4, 3-3

Software is nooit 100% goed. Zolang software wordt gemaakt, zitten er fouten in. Programmeerfouten, ontwerpfouten, architecturale fouten, etc. kunnen zorgen dat software niet werkt zoals bedoeld. Het is natuurlijk mogelijk om fouten te corrigeren, er komt dan een nieuwe versie van de software uit. Die kan de eindgebruiker na vrijgave door systeemleverancier en verificatie dan installeren.

Niet alle softwarefouten zijn ook direct cybersecurityproblemen. Een bekend voorbeeld is software die niet weet dat eens in de 4 jaar er een 29e februari is. Dat zorgt misschien wel voor een probleem bij de gebruiker, maar is geen cybersecurityprobleem en vormt geen cyber gevaar.

Sommige softwarefouten zijn wél gevaarlijk, omdat hackers en malware dankzij die fouten toegang kunnen krijgen tot een apparaat en/of een netwerk, de apparatuur misbruiken, er malware op kunnen installeren, etc. Dit heet een ‘kwetsbaarheid’ (Engels: ‘vulnerability’). Deze kunnen de software, en/of het systeem waar het deel van uitmaakt, beletten te functioneren zoals bedoeld is. Ook kan de veiligheid, beschikbaarheid, performance, etc. beïnvloed worden.

Als leveranciers dit weten, zullen ze een nieuwe versie van de software genereren. Het is daarom belangrijk dat nieuwe versies van software zo snel mogelijk geïnstalleerd worden. De nieuwe versie(s) dichten de ‘achterdeurtjes’ die hackers en malware kunnen misbruiken. Het installeren van de nieuwste versies van software om softwarefouten of lekken te herstellen heet: ‘patchen’.

Het uitvoeren van de installatie van de patch, het ‘patchen’ dus, moet de eindgebruiker uiteraard zelf doen. De IEC 62443-2 houdt zich niet bezig met hóe een patch precies geïnstalleerd moet worden. Dit is een technisch aspect, dat voor elke leveranciers anders is.

Patch management volgens IEC 62443

De IEC 62443-2 houdt zich niet bezig met hóe een patch precies geïnstalleerd moet worden. Dit is een technisch aspect, dat voor elke leveranciers anders is. Wél houdt de standaard zich bezig met ‘patch **management**’. Dit is het werkproces dat een organisatie moet inrichten om risico’s met betrekking tot kwetsbaarheden in systemen en / of programma’s tot een acceptabel niveau te reduceren.

Patch management beschrijft dit proces voor alle systemen en programmatuur en definieert hierbij de volgende stappen:

- Requirements: welke software en welke systemen
- Frequentie: hoe vaak wordt er gepatcht (wekelijks, maandelijks, etc.)
- Plan van aanpak: coördinatie met productie, patch moment
- Test proces: is zeker dat installatie van een patch geen problemen oplevert
- Systeem / asset eigenaar / beheerder: wie doet wat en wanneer

- Afstemming met system Integrator/leverancier: zijn de patches vrijgegeven door de leverancier
- Integriteitscontrole van de te installeren patches

Patch management moet altijd worden gedaan met een risico-gestuurde benadering. Als het verlagen van het risico minder kostbaar is dan het patchen van het probleem, zou er kunnen worden gekeken naar mitigerende maatregelen.

Rapportcijfer

De ene kwetsbaarheid is de andere niet. Sommige zijn vrij onschuldig, andere zijn zéér gevaarlijk. Om dit te kunnen kwantificeren krijgt elke kwetsbaarheid een rapportcijfer in het bereik 0.0 t/m 10.0 (in stappen van 0.1), waarbij geldt: hoe hoger het cijfer, des te gevaarlijker. Dit zegt dus iets over het risico dat men loopt met zo'n kwetsbaarheid, mits er geen aanvullende beschermende maatregelen getroffen zijn.

De vakterm voor 'rapportcijfer' is: 'CVSS Score' (Common Vulnerability Scoring System). Dit is een wereldwijd geaccepteerde methodiek. Voor sommige doeleinden is het nuttiger om een kwalitatieve beschrijving van de waarde te hebben. Deze is als volgt vastgelegd:

0,0	Geen
0.1 – 3.9	Laag
4.0 – 6.9	Middel
7.0 – 8.9	Hoog
9.0 – 10.0	Kritiek

Hoewel de CVSS-score een nuttig hulpmiddel is voor het beoordelen van de ernst van een kwetsbaarheid, moet de score in veel situaties worden genuanceerd en gecombineerd met andere factoren zoals o.a. locatie van de kwetsbaarheid, reeds getroffen mitigerende maatregelen (zoals netwerksegmentering en firewalls) en risicoprioritering voor een volledige en nauwkeuriger beveiligingsevaluatie. Met andere woorden, een hoge CVSS vereist snelle evaluatie, eventuele patching van de kwetsbaarheid kan afhankelijk van de omstandigheden een lagere prioriteit hebben.

Wát gaan we patchen?

Patchen kennen we allemaal van Windows PC's, elke tweede dinsdag van de maand. Maar PC's zijn niet de enige apparaten waar software op geïnstalleerd is. Het asset register geeft inzicht in welke apparatuur er in gebruik is. De volgende stap is dan om per (type) apparaat vast te leggen:

- Welke patches zijn beschikbaar?
- Is de patch noodzakelijk voor de eigen apparatuur?
- Is de patch getest op juiste werking, en afwezigheid van neveneffecten?
- Is de patch geautoriseerd om te mogen installeren?
- Is de patch effectief?
- Waar is de patch (al) geïnstalleerd?

Om te weten of er patches beschikbaar zijn, is contact met de leverancier van de apparatuur nodig. Sommige leveranciers zijn heel actief in het informeren van klanten, anderen zijn er vrij zwijgzaam

over. Daarnaast zijn er publieke websites, zoals bijvoorbeeld van ICS-CERT (US) en VDE (Duitsland) die veel informatie geven.

Mitigerende maatregelen

In sommige gevallen zal er geen mogelijkheid zijn om patches uit te rollen voor bepaalde kwetsbaarheden, systemen of programma's.

Redenen hiervoor kunnen (onder andere) zijn:

- Dat software na installatie van de patch niet meer (goed) werkt.
- Dat een leverancier een patch (nog) niet goedkeurt voor installatie, omdat de juiste werking van het product niet gegarandeerd kan worden.
- Dat de productie niet kan worden onderbroken om de patch te installeren.
- Dat de fabrikant van de software niet meer bestaat.
- Dat de fabrikant zijn product niet meer ondersteunt.

In dat geval kan een verlaging van de risico's worden gezocht in mitigerende maatregelen. Hierbij kan gedacht worden aan:

- Het segmenteren van het netwerk.
- Het isoleren van een kwetsbaar segment of component.
- Het vervangen van de betreffende component.
- Firewalls met 'virtual patching' mogelijkheden, etc.

In het algemeen zijn dit maatregelen die niet 1-2-3 te implementeren zijn.

Planning

Een heel belangrijk onderdeel van het patch management is: *wanneer* gaan we installeren? Dit is omdat de installatie van een patch vaak eist dat software moet stoppen, een systeem moet herstarten, etc. Gedurende deze tijd kan de software / het systeem dus niet zijn taak uitvoeren, en dit kan consequenties hebben voor de machine, productielijn, procesinstallatie, etc. In de meeste bedrijven is het installeren van patches dus niet mogelijk zolang de productie loopt.

Het moment waarop patches wél geïnstalleerd kunnen worden, zal dus vaak liggen tijdens geplande stilstand en onderhoud. Soms kan dit in een weekend, soms alleen eenmaal per jaar (tussen Kerst/Nieuwjaar bijvoorbeeld), of soms zelfs alleen tijdens een vijfjaarlijkse productiestop.

Een goede coördinatie met de productieplanning is dus gewenst. Aangezien de beschikbare tijd voor installatie van alle patches vaak kort is, is het verstandig om:

- Alle benodigde documentatie, bestanden, media (USB sticks, cd-roms etc.) te verzamelen.
- Op voorhand al zoveel mogelijk te testen of een patch goed werkt. Het komt namelijk wel eens voor dat een patch een (onbedoeld) neveneffect heeft op software, of dat configuratiewijzigingen in andere software nodig zijn. Hiervoor is dus een testopstelling nodig.

Er rekening mee te houden dat een ‘roll back’ van een patch nodig is, als een patch niet werkt. Hiervoor zijn dus wel oude software-versies nodig. Hou in de gaten dat een roll back bij sommige leveranciers of apparatuur niet mogelijk is.

Afhankelijk van de hoeveelheid te installeren patches en de beschikbare tijd kan het voorkomen dat niet alle patches te installeren zijn. In zo’n geval moet op voorhand een selectie gemaakt worden: welke wel en welke niet? De CVSS score kan hierbij eventueel helpen (kwetsbaarheden met het hoogste risico eerst). Maar ook kan gedacht worden aan het eerst patchen van de meest kritieke productiesystemen. De IEC 62443-2-3 zegt hier niets over, wat & hoe kunt u zelf bepalen.

Automatisch patchen

Voor consumenten-apparatuur gelden andere methodes van installeren van patches dan voor industriële apparatuur. Bijvoorbeeld, elke 2e dinsdag van de maand installeren Windows PC’s de nieuwste patches van Microsoft automatisch. Dat is goed voor consumenten-apparatuur, omdat de meeste gebruikers anders helemaal niet zouden patchen. Maar, zoals u ongetwijfeld zelf wel zult hebben ervaren, de PC wil dan ook altijd herstarten, en dan is vaak op een zeer ongewenst moment.

Voor industriële systemen zijn automatische installatie van patches en de onvoorspelbare herstart van apparatuur nooit gewenst. Schakel dit uit!

Lifecycle

Patchen is geen eenmalige actie. Het is een proces, dat zich met een bepaalde regelmaat moet gaan herhalen. De IEC 62443-2-3 helpt u bij het inrichten van dit zeer belangrijke proces. Het ‘bijblijven’ met de laatste stand van software is een van de meest effectieve maatregelen om veel malware buiten de deur te houden!

6. Netwerksegmentering, zones en conduits

Normdeel
2-1, 2-4, 3-2

Om de digitale weerbaarheid van een organisatie te borgen is het van belang om IT- en OT-netwerken van elkaar te scheiden. Aanvullend daarop dienen binnen de OT-omgeving zelf aanvullende maatregelen te worden genomen om eventuele digitale incidenten te isoleren en daarmee de continuïteit van dienstverlening te borgen.

De IEC 62443 gebruikt een zonemodel dat vorm is gegeven rondom ‘zones’ en ‘conduits’. Dit zonemodel scheidt het OT-netwerk van het IT-netwerk en brengt verdere, risico gebaseerde segmentering aan op basis van functionaliteit van de assets in het OT-netwerk. Echter, een te ver doorgevoerde segmentering kan leiden tot vertragingen in de communicatie. Begin simpel!

Zo adviseert de IEC 62443 om de volgende assetcategorieën van elkaar te scheiden in aparte zones:

- Safety systemen
- Kritieke control systemen
- Niet-kritieke control systemen
- Wireless systemen
- Remote access systemen
- Overige systemen

Apparaten die in dezelfde zone zijn ingedeeld, mogen elkaar vertrouwen. Per zone moet een security-niveau (1.4) worden bepaald in relatie tot de belangrijkheid van de betreffende zone. Afhankelijk van het beoogde security-niveau dient de scheiding logisch dan wel fysiek te zijn.

De communicatieverbindingen tussen de verschillende zones worden gevormd door ‘conduits’ (de letterlijke vertaling hiervan is: kabelgoot, maar in deze context gaat het om een datastroom). Een zone kan verschillende conduits hebben naar andere zones. Bijlage 4 geeft een voorbeeld van een indeling in zones en conduits.

Deze conduits dienen te voldoen aan dezelfde securityvereisten als de zone met het hoogste securityniveau van de zones waartussen verbinding wordt gemaakt.

Met een goede netwerksegmentering neemt de digitale weerbaarheid van een installatie toe. Immers, incidenten kunnen niet meer op eenvoudige wijze escaleren naar andere delen van het netwerk en blijven beperkt tot de zone waarin een dreiging zich manifesteert.

7. Monitoren van netwerkverkeer

IEC 62443
Normdeel
2-3, 3-2, 3-3

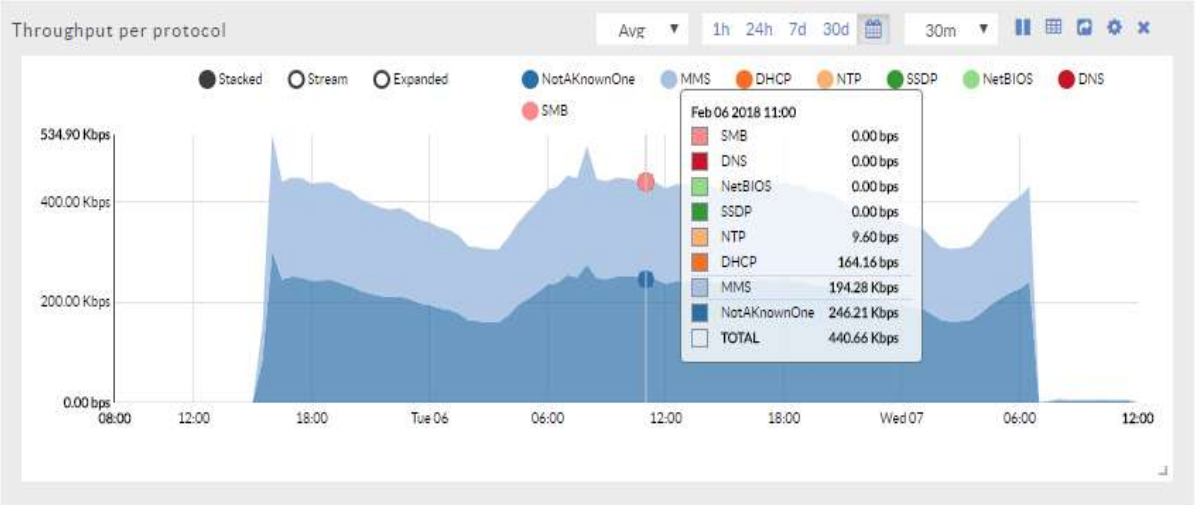
Monitoring van netwerkverkeer in een OT omgeving is nog niet zo gebruikelijk als in een IT omgeving. Tools in gebruik op het IT netwerk worden dan ook niet geaccepteerd in OT omgevingen, om het risico op productie onderbrekingen tot een minimum te beperken.

Vaak hebben deze IT tools een actieve benadering van de assets op het OT netwerk, iets wat door de oudere apparatuur (legacy) niet ondersteund is. Ook kan het netwerk niet berekend zijn op zulke (extra) verkeersstromen.

Passieve detectie

Om verstoring van productieprocessen te voorkomen zijn er voor OT omgevingen tools ontwikkeld die op een passieve manier het netwerk inzichtelijk kunnen maken. Deze tools gebruiken een SPAN port (of: netwerk TAP) om het netwerkverkeer naar de monitoring tool te leiden. Zo'n tool luistert alleen maar (is 'passief').

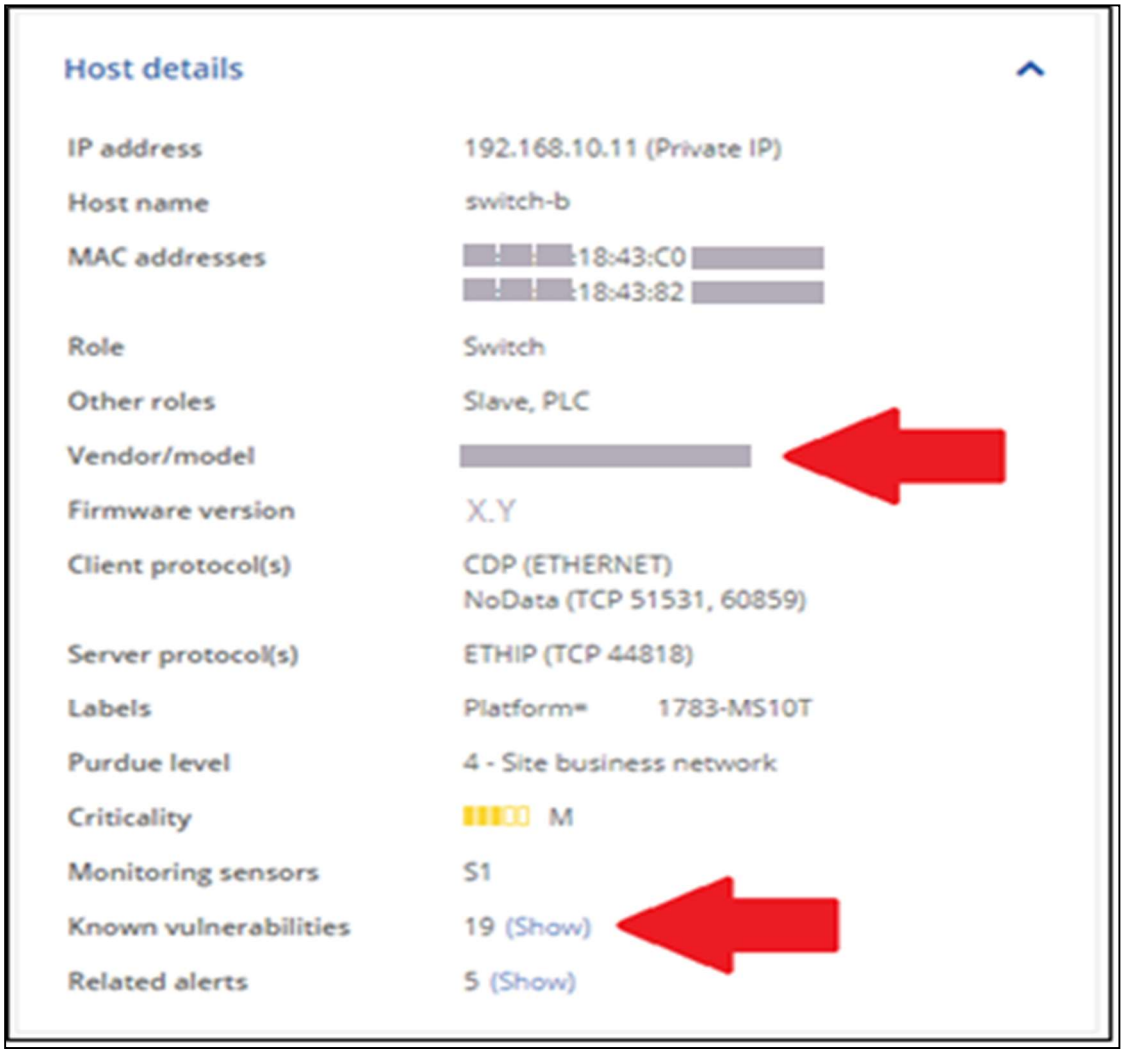
Bij deze tools speelt het herkennen van de in gebruik zijnde OT protocollen een zeer belangrijke rol. Het gaat er daarbij niet om de hoeveelheid protocollen die herkend kunnen worden, maar wel hoeveel informatie er uit het protocol gehaald kan worden. Met deze 'Deep Packet Inspection' technieken voor industriële protocollen (zoals Modbus, ProfiNet, BACNet, IEC10x, MMS, etc.) kan heel veel interessante informatie uit netwerkberichten gehaald worden.



Figuur 3, voorbeeld van netwerkmonitoring tool

Sommige protocollen versturen veel nuttige informatie, andere protocollen helemaal geen, en weer andere protocollen alleen op bepaalde momenten. Het Ethernet MAC adres is meestal makkelijk te achterhalen, maar daarnaast zijn ook de leverancier, productidentificatie, en de actuele software

versie(s) een belangrijk gegeven. De context is dus belangrijk, helemaal als naast beheer van het asset register ook detectie van kwetsbaarheden belangrijk is (voor patch-management).



Figuur 4, een asset met zijn leverancier, firmware, versie en gedetecteerde kwetsbaarheden

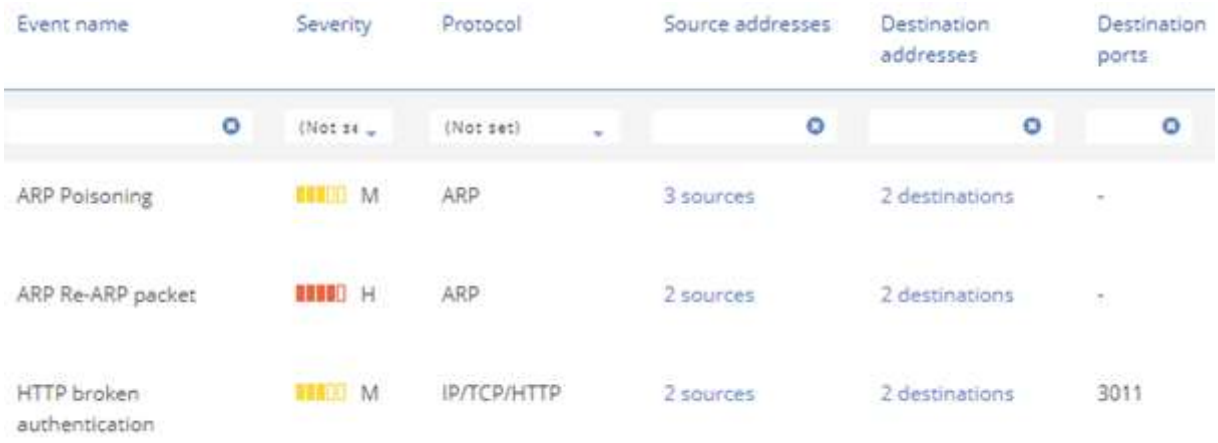
Naast passieve tools bestaan ook actieve tools. Deze sturen wél netwerkberichten, bijvoorbeeld om een asset zijn softwareversie op te vragen. Het is dan van belang dat als een asset op een passieve manier ontdekt is, men ook weet welk protocol het asset spreekt. Men kan dan door middel van dit protocol meer informatie verkrijgen door het asset op een actieve manier te benaderen, zonder een risico te vormen voor de productie processen.

IDS (Intrusion Detection System)

Door op een passieve manier de assets en verkeerstromen in kaart te brengen weten IDS tools na een leerperiode wat normaal gedrag is in een OT omgeving. Er is nu een baseline gevormd. De assets zijn bekend, de communicatie is bekend en de gebruikelijke proceswaarden zijn bekend.

Een IDS kan nu veranderingen op deze baseline detecteren. Dit kunnen bijvoorbeeld nieuwe assets zijn die op het netwerk verschijnen, nieuwe protocollen of communicatiepatronen, download van nieuwe applicatiesoftware, maar ook afwijkingen in proceswaarden die niet gezien zijn tijdens het bepalen van de baseline. Deze informatie zal beoordeeld en verwerkt moeten worden, dit is arbeidsintensief werk. Dit werk kan deels in een later stadium ook door een SIEM of SOC verwerkt worden.

Voorbeelden van afwijkingen van de baseline kunnen zijn: het veranderen van de temperatuur waarbij de waarden afwijken van de range die we in de baseline hebben gezien / geleerd, protocol functiecodes die niet overeenstemmen, of rechtstreekse verbindingen of pogingen daartoe vanuit de OT omgeving naar Internet.



Event name	Severity	Protocol	Source addresses	Destination addresses	Destination ports
	(Not se	(Not set)			
ARP Poisoning	M	ARP	3 sources	2 destinations	-
ARP Re-ARP packet	H	ARP	2 sources	2 destinations	-
HTTP broken authentication	M	IP/TCP/HTTP	2 sources	2 destinations	3011

Figuur 5, door een IDS gedetecteerde protocolafwijkingen

Dit kunnen allemaal triggers zijn waarop een IDS actie kan ondernemen. Te denken valt bijvoorbeeld aan een alert via email te versturen (via een SMTP integratie), een alert naar een SIEM oplossing, of een trigger naar een firewall (die een bepaalde policy klaar heeft staan, die geactiveerd wordt waarop de firewall een actie onderneemt).

Dit laatste zien we meer en meer bij firewalls tussen de IT en OT omgeving, waarbij bijvoorbeeld een asset in de IT omgeving afgesloten wordt en geen data meer kan sturen vanuit deze IT omgeving naar de OT omgeving.

8. PDCA (Plan, Do, Check, Act)

Normdeel
2-1

Als u bovenstaande stappen heeft doorlopen, heeft u een goede start gemaakt met het beveiligen van uw OT omgeving. Helaas kunt u nu niet achterover gaan leunen maar is het belangrijk om het geheel up-to-date te houden. Daarvoor kunt u de PDCA (Plan-Do-Check-Act) cyclus gebruiken, voor een continue verbetering van processen.

Continue verbetering van processen binnen een IEC 62443 implementatie

Organisaties die bezig zijn met implementatie van de IEC 62443 kunnen niet volstaan met een eenmalige implementatie. Een organisatie verandert, omgevingsfactoren veranderen en het is belangrijk dat een bedrijf kijkt of de diverse onderdelen, genoemd in voorgaande hoofdstukken 1-7 nog altijd voldoen, of dat deze wellicht bijgesteld dienen te worden. Op deze manier zorgt een organisatie ervoor dat ze op het gewenste niveau blijft, of groeit.

Een veel gebruikte methode die gehanteerd wordt om continu te verbeteren is de PDCA-methodiek ook wel (naar de bedenker) de Deming Cirkel, of kwaliteitscirkel genoemd.

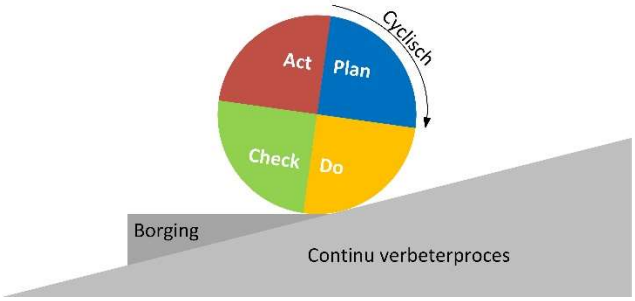
PDCA staat voor:

Plan: Maak een plan

Do: Voer het uit

Check: Controleer resultaat

Act: Stuur bij, indien resultaat nog niet behaald.



Figuur 6, PDCA cyclus

Deze kwaliteitscirkel kan steeds herhaald worden, net zo lang tot dat het gewenste resultaat is bereikt. Veel organisaties zijn sterk in het maken van P plannen, het D uitvoeren, maar C controleren of het werkt krijgt vaak minder aandacht. Hierdoor vindt er onvoldoende A actie plaats met het bijsturen.

De PDCA methodiek is dus goed te gebruiken om structureel verbetering aan te brengen in een organisatie, ongeacht of dit nu op strategisch, tactisch of operationeel niveau is, of een normelementen uit de IEC 62443. Verbeteren doe je dus in het algemeen daar waar fouten of onvolkomenheden worden ontdekt of gesignaleerd in je proces.

Wanneer men dit wil oppakken moet men starten met het zoeken van de oorzaak, op basis daarvan een passend plan maken wat vervolgens gevolgd gaat worden met de PDCA-cirkel. Het is van

belang om direct betrokkenen actief mee te nemen bij het zoeken naar de oorzaak en het maken van het plan. Op deze wijze wordt commitment met het plan bereikt en verhoogt het de kans van slagen.

Het is te adviseren om in het plan duidelijke mijlpalen te plaatsen: wanneer wat bereikt moet zijn, wie het uitvoert, wanneer de check/evaluatie plaats vindt, en hoe vastgesteld worden of het resultaat is bereikt, en als niet of er bijsturing nodig is.

Een voorbeeld

Een organisatie merkt dat zij keer op keer verstoringen heeft op het netwerk. Het plan zou kunnen zijn:

Do: Activeer metingen binnen het netwerk om te bekijken waar de verstoringen vandaan komen

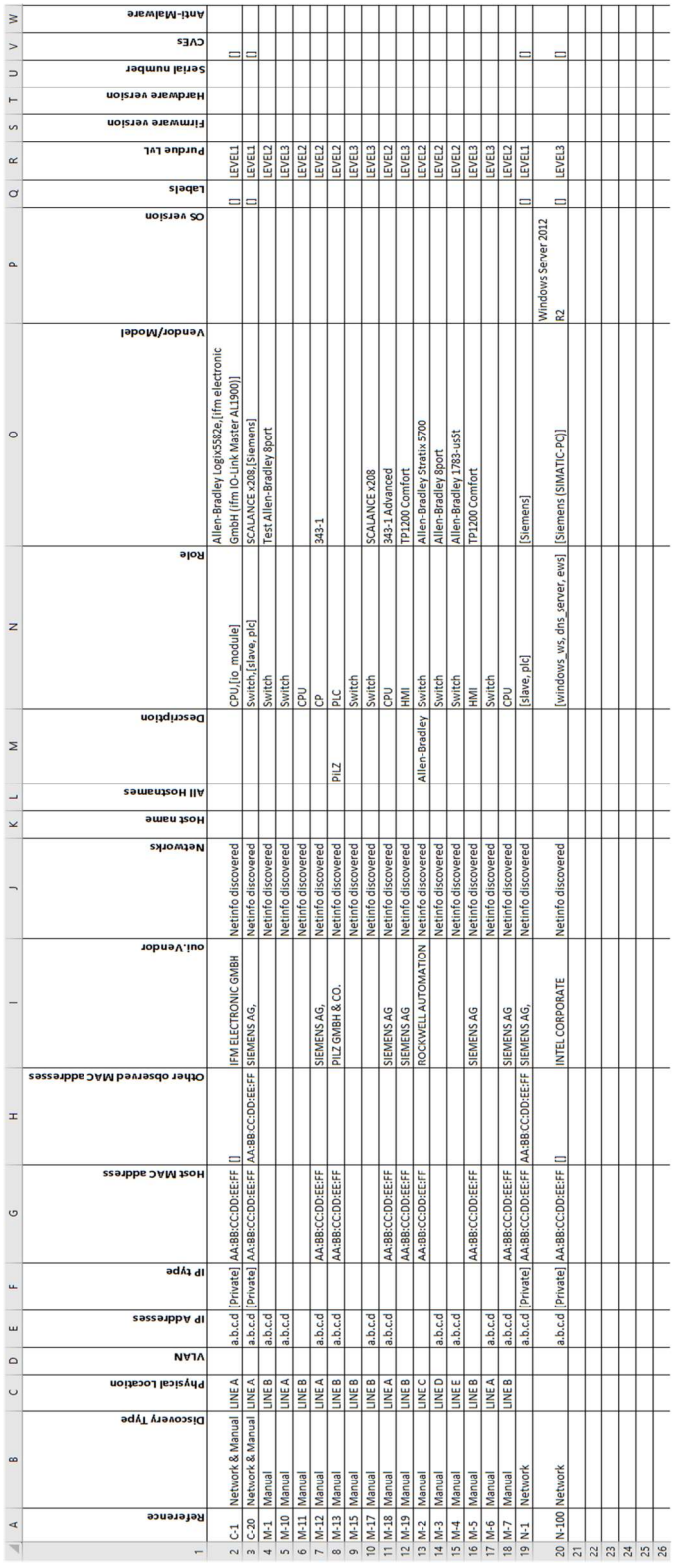
Check: Meet het resultaat gedurende een relevante periode

Act: Neem passende maatregelen op basis van de bevindingen

NB: Wanneer dit nog niet het gewenste resultaat leidt dan zou het opnieuw onderzoeken van het netwerk door het activeren van metingen tot de mogelijkheden behoren.

Bijlage 1

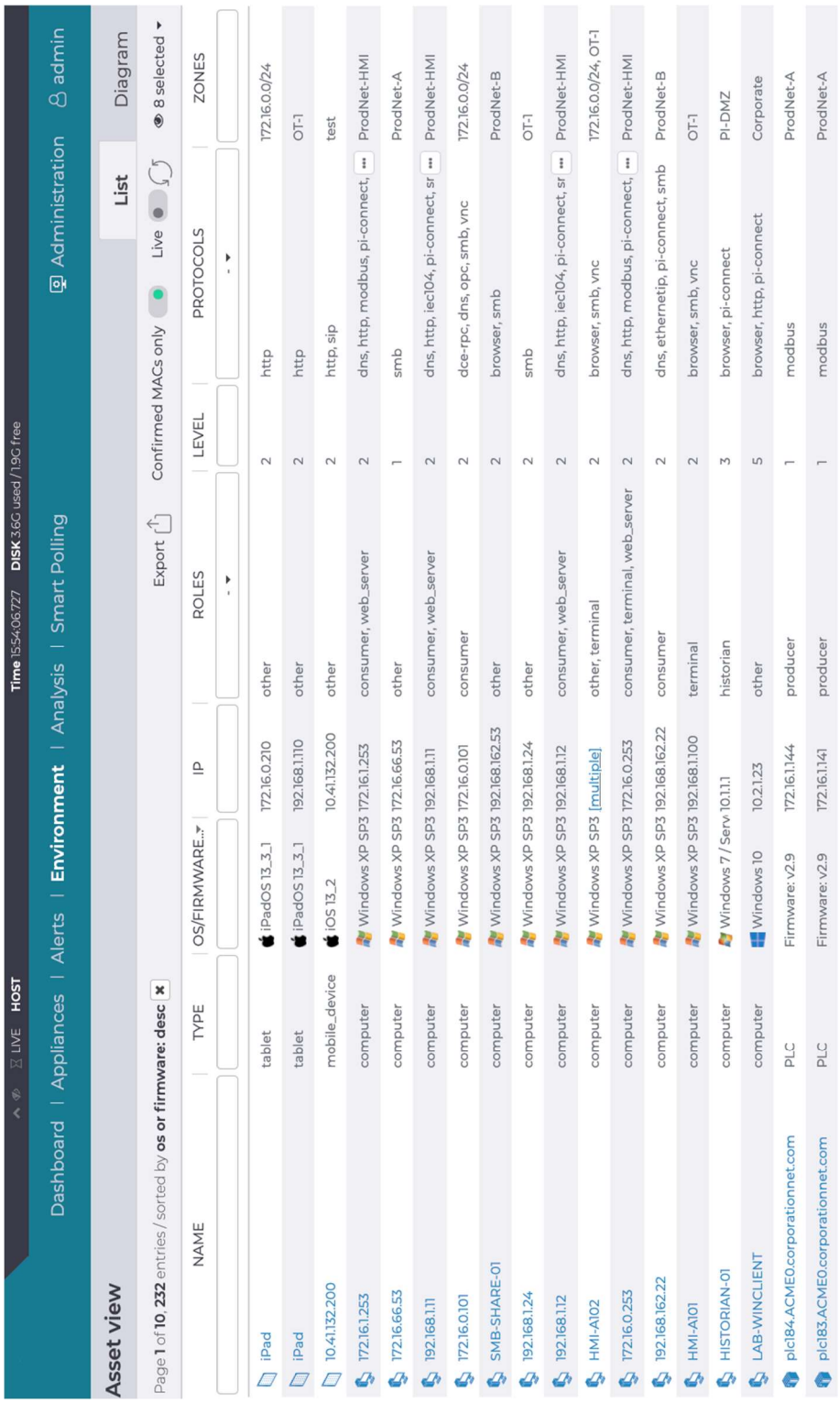
Voorbeeld 1 van een Asset register



Reference	Discovery Type	Physical Location	VLAN	IP Addresses	IP type	Host MAC address	Other observed MAC addresses	oui.Vendor	Networks	Host name	All Hostnames	Description	Role	Vendor/Model	OS version	Labels	Purdue Lvl	Firmware version	Hardware version	Serial number	CVEs	Anti-Malware
C-1	Network & Manual	LINE A		a.b.c.d	[Private]	AA:BB:CC:DD:EE:FF	[]	IFM ELECTRONIC GMBH	Netinfo discovered			CPU,[io_module]		Allen-Bradley Logix5582e,[ifm electronic GmbH (ifm IO-Link Master AL1900)]		[]	LEVEL1				[]	
C-20	Network & Manual	LINE A		a.b.c.d	[Private]	AA:BB:CC:DD:EE:FF	AA:BB:CC:DD:EE:FF	SIEMENS AG,	Netinfo discovered			Switch,[slave, plc]		SCALANCE x208,[Siemens]		[]	LEVEL1				[]	
M-1	Manual	LINE B		a.b.c.d					Netinfo discovered			Switch		Test Allen-Bradley 8port			LEVEL2					
M-10	Manual	LINE A		a.b.c.d					Netinfo discovered			Switch					LEVEL3					
M-11	Manual	LINE B							Netinfo discovered			CPU					LEVEL2					
M-12	Manual	LINE A		a.b.c.d		AA:BB:CC:DD:EE:FF		SIEMENS AG,	Netinfo discovered			CP		343-1			LEVEL2					
M-13	Manual	LINE B		a.b.c.d		AA:BB:CC:DD:EE:FF		PILZ GMBH & CO.	Netinfo discovered		PILZ	PLC					LEVEL2					
M-15	Manual	LINE B							Netinfo discovered			Switch					LEVEL3					
M-17	Manual	LINE B		a.b.c.d					Netinfo discovered			Switch		SCALANCE x208			LEVEL3					
M-18	Manual	LINE A		a.b.c.d		AA:BB:CC:DD:EE:FF		SIEMENS AG	Netinfo discovered			CPU		343-1 Advanced			LEVEL2					
M-19	Manual	LINE B				AA:BB:CC:DD:EE:FF		SIEMENS AG	Netinfo discovered			HMI		TP1200 Comfort			LEVEL3					
M-2	Manual	LINE C				AA:BB:CC:DD:EE:FF		ROCKWELL AUTOMATION	Netinfo discovered		Allen-Bradley	Switch		Allen-Bradley Stratix 5700			LEVEL2					
M-3	Manual	LINE D		a.b.c.d					Netinfo discovered			Switch		Allen-Bradley 8port			LEVEL2					
M-4	Manual	LINE E		a.b.c.d					Netinfo discovered			Switch		Allen-Bradley 1783-us5t			LEVEL2					
M-5	Manual	LINE B				AA:BB:CC:DD:EE:FF		SIEMENS AG	Netinfo discovered			HMI		TP1200 Comfort			LEVEL3					
M-6	Manual	LINE A		a.b.c.d					Netinfo discovered			Switch					LEVEL3					
M-7	Manual	LINE B		a.b.c.d		AA:BB:CC:DD:EE:FF		SIEMENS AG	Netinfo discovered			CPU					LEVEL2					
N-1	Network			a.b.c.d	[Private]	AA:BB:CC:DD:EE:FF	AA:BB:CC:DD:EE:FF	SIEMENS AG,	Netinfo discovered			[slave, plc]		[Siemens]		[]	LEVEL1				[]	
N-100	Network			a.b.c.d	[Private]	AA:BB:CC:DD:EE:FF	[]	INTEL CORPORATE	Netinfo discovered			[windows_vs, dns_server, ews]		[Siemens (SIMATIC-PC)]	Windows Server 2012 R2	[]	LEVEL3				[]	

Bijlage 2

Voorbeeld 2 van een Asset register



Bijlage 3

Een voorbeeld van een datastromen register

Datastromen register

Productie

Bron									Bestemming								
Systeem	Datastroom	Zone	Level (0-5)	Interface	Host IP adres	VLAN	Protocol	TCP/UDP poort	Systeem	Datastroom	Zone	Level (0-5)	VLAN	Interface	Host IP adres	Protocol	TCP/UDP poort	Omschrijving
< voorbeeld >																		
HMI23	*Uitgaand -->*			*E0*	*172.16.181.4*	*3*	*HTTP*	*TCP/random*	*WEB01*	*--> Inkomend*			*6*	*Eth0.6*	*145.10.2.5*	*HTTP*	*TCP/80*	*Webverkeer van HMI23 naar WEB01*
	Inkomend <--			*E0*	*172.16.181.4*	*3*	*HTTP*	*TCP/random*		*<-- Uitgaand*			*6*	*Eth0.6*	*145.10.2.5*	*HTTP*	*TCP/80*	*Retourdata van WEB01 naar HMI23*
	Uitgaand -->									Uitgaand -->								
	Inkomend <--									Inkomend <--								

Safety and Control

Bron									Bestemming								
Systeem	Datastroom	Zone	Level (0-5)	Interface	Host IP adres	VLAN	Protocol	TCP/UDP poort	Systeem	Datastroom	Zone	Level (0-5)	VLAN	Interface	Host IP adres	Protocol	TCP/UDP poort	Omschrijving

Remote Access

Bron									Bestemming								
Systeem	Datastroom	Zone	Level (0-5)	Interface	Host IP adres	VLAN	Protocol	TCP/UDP poort	Systeem	Datastroom	Zone	Level (0-5)	VLAN	Interface	Host IP adres	Protocol	TCP/UDP poort	Omschrijving

Netwerk- en Systeembeheer

Bron									Bestemming								
Systeem	Datastroom	Zone	Level (0-5)	Interface	Host IP adres	VLAN	Protocol	TCP/UDP poort	Systeem	Datastroom	Zone	Level (0-5)	VLAN	Interface	Host IP adres	Protocol	TCP/UDP poort	Omschrijving

Principes

De volgende principes worden gehanteerd voor het opstellen en gebruik van het register:

Het datastromen register betreft een zo volledig mogelijke inventarisatie van alle datastromen die aanwezig zijn in een netwerk-infrastructuur.
Het register is de enige bron die wordt gebruikt voor het configureren van de volgende logisch en/of fysieke componenten:
Principe en uitgangpunt is dat een firewall, ACL of applicatie per definitie uitgaat van een volledig gesloten configuratie waarbij geen enkele datastroom kan worden ontvangen of verzonden.
Op basis van explicite configuratie kan een Firewall, ACL of applicatie zo worden geconfigureerd dat data stromen tot stand kunnen worden gebracht.
Een systeem of applicatie configuratie mag alleen informatie bevatten die vermeld is in de communicatie matrix.
Elk (computer)systeem, applicatie en/of database (Service) moet beschikken over een actuele communicatimatrix waarin voor elke communicatiestroom minimaal het volgende staat vermeld:
- configuatie van een OS gebaseerde Host Based Firewall van een (computer) systeem
- configuatie van een netwerkfirewall of Access Control List (ACL)
- configuratie van een applicatie configuratie

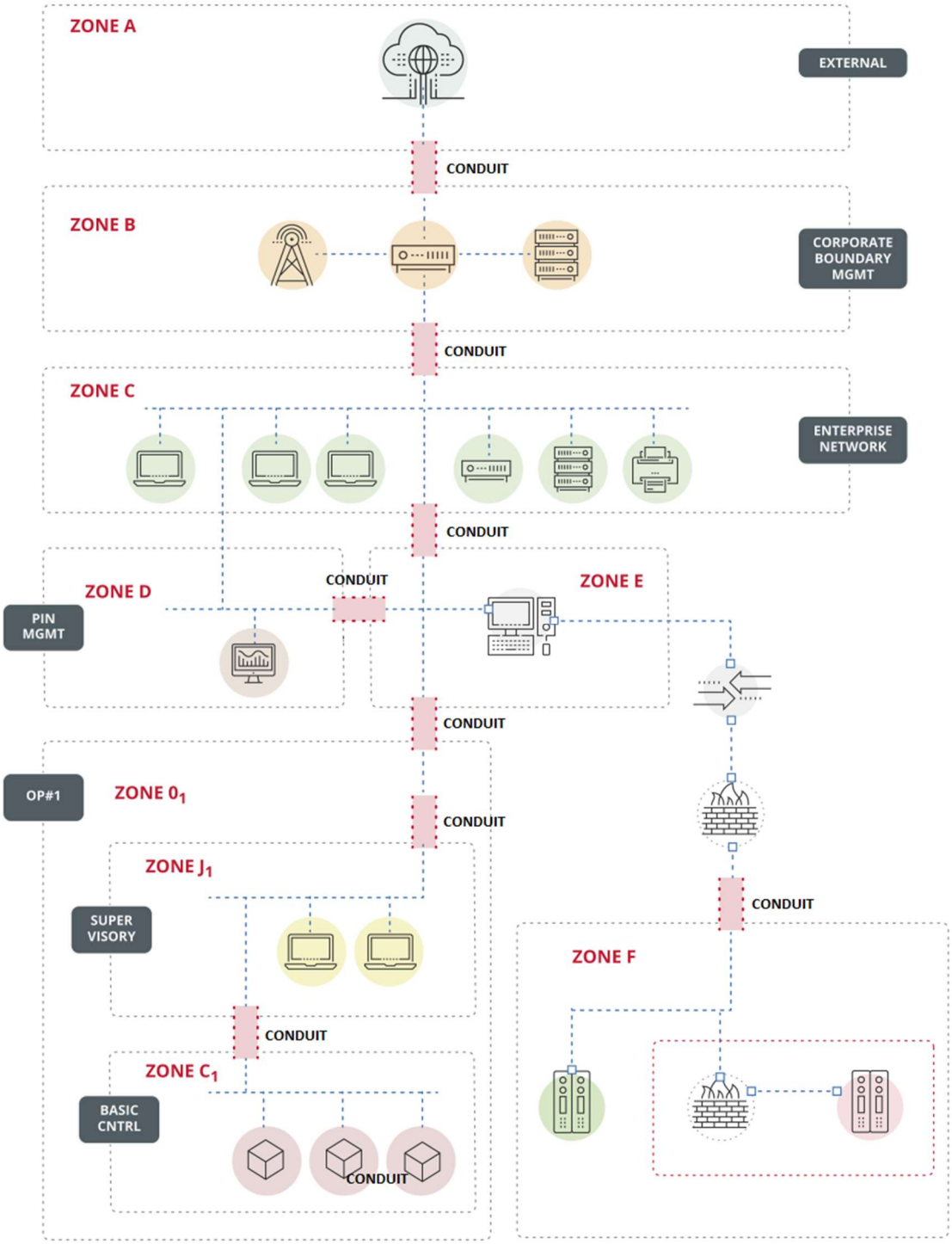
Details

De volgende basis informatie wordt in het datastromen register opgenomen:

- Systeem: *naam van het verzendende of ontvangende systeem* / applicatie
- Datastroom: unidirectionele communicatie richting van de datastroom (gezien vanuit de initiatiefnemer) (bijv. Inkomend of uitgaand)
- Zone: 'naam' van de zone
- Level: numerieke waarde (0-5)
- Interface: 'naam' van fysieke/logische (sub-) interface (bijv. < naam > of < interface-naam nummer.subinterface nummer >)
- VLAN ID: numerieke waarde (1-4094) van logische netwerksegment waar systeem of applicatie in is opgenomen
- Host IP adres: IPv4/v6 adres van systeem of applicatie
- Protocol: Proprietary-, Transport-, applicatie protocol (bijv. Modbus, CANbus, Profibus/Profinet, BACnet, Serial, TCP, UDP, ICMP, HTTP(S), SFTP, SCP, SSH, SNMP, Syslog, etc.)
- TCP/UDP poort: Transport- of applicatie protocol poort(en) (bijv. 21, 22, 53, 80, 123, 443, 636, 3389, 8080, etc.)
- Omschrijving: korte omschrijving van datastroom en motivatie waarom deze noodzakelijk is

Bijlage 4

Een voorbeeld van de indeling van een netwerk in zones, met daartussen de conduits (bron: INCIBE CERT).



Afkortingen

CERT	Computer Emergency Response Team
CMDB	Configuration Management DataBase
CVSS	Common Vulnerability Scoring System
DCS	Distributed Control System
ICS	Industrial Control System
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IPCS	Industrieel Platform Cyber Security
IT	Information Technology
MAC	Media Access Control
OT	Operational Technology
PDCA	Plan-Do-Check-Act
PLC	Programmable Logic Controller
RFID	Radio-Frequency IDentification
SCADA	Supervisory Control And Data Acquisition
SIEM	Security Incident and Event Monitoring
SIS	Safety Instrumented System
SMTP	Simple Mail Transfer Protocol
SOC	Security Operations Centre
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VDE	Verband der Elektrotechnik Elektronik und Informationstechnik

Deze publicatie kunt u opvragen via ipcs@securitydelta.nl

Meer info over IPCS via https://securitydelta.nl/ipcs

Dit document is opgesteld door de volgende leden van het Industrieel Platform Cyber Security:

Eric ten Bos, Markwin Romijn, Ron Perrier, Eric van Aken, Michael Theuerzeit, Stefan Rutten, Johan Assies, Philip Roodzant, Vincent Schijven, Johan den Hartog, Rob Hulsebos.

Met dank aan de overige leden van de 'IPCS werkgroep IEC 62443' voor het reviewen van dit document.

Security Delta (HSD)
Wilhelmina van Pruisenweg 104
2595 AN The Hague
070 204 41 80

info@securitydelta.nl
www.securitydelta.nl