HOE KWETSBAAR IS MIJN **INDUSTRIËLE INFRASTRUCTUUR** VOOR **CYBERAANVALLERS?**

Sleutelconcepten voor de beveiliging van industriële controlesystemen

index

1. Inleiding

Industriële automatisering beïnvloedt ons dagelijks leven meer dan we ons voor durven stellen. Procesautomatisering komt voor bij de productie van voeding, drinkwater, gas en elektriciteit, maar ook bij verkeerslichten, sluizen en bruggen. De laatste decennia ondergingen deze systemen een diepgaande verandering. Ging het tot een paar jaar geleden over geïsoleerde, gesloten systemen, dan wordt nu gebruik gemaakt van commerciële basiscomponenten, geïntegreerd met back-end systemen en netwerken, vaak verbonden met het internet en andere bedrijfsnetwerken. Innovatie heeft ervoor gezorgd dat de klassieke regelaars uitgerust werden met een arsenaal aan communicatiemogelijkheden. HMI (Human machine interface) en SCADA (Supervisory Control And Data Acquisition) systemen, FTP en Web servers, behoren ondertussen zowat tot de standaarduitrusting.

Deze evolutie heeft geleid tot een afname in kosten en een hoger gebruiksgemak waarvan controle en beheer op afstand concrete voorbeelden zijn. Terzelfdertijd werden systemen kwetsbaar en netwerken blootgesteld aan aanvallen van buitenaf. Deze systemen maken gebruik van onderdelen en technologieën die verouderd zijn op het vlak van beveiliging. Bovendien wordt bij de ontwikkeling van nieuwe systemen vooral gefocust op de regeling van het systeem of het proces; de beveiliging daarentegen wordt stiefmoederlijk behandeld of zelfs genegeerd. Een aanval kan echter grote fysische, economische en imago schade veroorzaken en zelfs tot ongelukken en rampen leiden. Bij een studie van circa 120 industriële systemen in 2014 werden maar liefst 38.753 kwetsbaarheden aangetroffen. Tijdens datzelfde onderzoek is gebleken dat kritische infrastructuren kwetsbaarheden bevatten die reeds 3 jaar lang publiek bekend waren. Ook in Europa is dit niet onopgemerkt gebleven.

Een aanval kan grote fysische, economische en image schade veroorzaken.

In 2011 bracht ENISA aanbevelingen uit om de beveiliging van deze omgevingen te verhogen, waaronder de nood aan bewustmaking en training rond de beveiliging van industriële systemen. Midden 2016 werd in het Europees parlement gestemd over de NIS (Network and Information Security) richtlijn die de noodzaak van een goede beveiliging van industrie en kritische infrastructuren onderstreept.

De bedrijven maken zich dan ook niet onterecht zorgen over de beveiliging van hun industriële netwerken. Enerzijds is er de vraag naar sterkere garanties en eisen rond de veiligheid bij het beheer en ontwerp van industriële systemen. Anderzijds hebben KMO's een beperkte kennis omtrent de beveiliging van industriële netwerken. Bovendien is er een vraag naar het gebruik van nieuwe technieken zoals mobiele toepassingen en Cloud omgevingen waarvan ook de gevolgen op het vlak van veiligheid slecht ingeschat kunnen worden door de bedrijven.

Deze brochure biedt een overzicht van essentiële informatie voor de uitrol en het onderhoud van industriële controlesystemen, en kwam tot stand door de expertise die werd opgebouwd door vier onderzoeksgroepen in Vlaanderen in het kader van twee technologie transfer projecten gefinancierd door IWT Vlaanderen in de periode 2014-2016.

2. Kenmerken van een industrieel controlesysteem

Tot voor kort waren industriële controlesystemen (ICS) vaak geïsoleerde installaties die bestonden uit gespecialiseerde software en hardware componenten met propriëtaire protocollen. Alsmaar meer maken deze dure componenten plaats voor goedkopere apparaten met gestandaardiseerde protocollen. Controlesystemen worden daarenboven steeds vaker gekoppeld aan het internet, zoals dat voor IT systemen reeds enkele decennia het geval is. ICS systemen hebben echter unieke karakteristieken die verschillen van IT omgevingen. De beveiligingsmaatregelen die ingezet worden bij IT systemen kunnen om die reden niet zomaar overgenomen worden in ICS omgevingen. Bovendien kan de impact van succesvolle aanvallen op ecologisch en economisch vlak heel groot zijn.

Eigenschappen van controlesystemen

PERFORMANTIE

Heel wat ICS systemen zijn tijd-kritisch. Deterministische antwoordtijden zijn vaak cruciaal. Het overschrijden van de aanvaardbare antwoordtijden kan leiden tot uitval met enorme economische schade of zelfs menselijk leed tot gevolg. Noodgevallen moeten binnen heel strikte tijdsintervallen worden afgehandeld en interactie met gebruikers mag geen onvoorspelbare vertragingen veroorzaken.

BESCHIKBAARHEID & INTEGRITEIT

De continue en correcte werking van veel ICS systemen is essentieel. Onverwachte uitval is vaak niet aanvaardbaar of kan een grote financiële of ecologische impact hebben. Zo loopt de rekening snel hoog op bij het uitvallen van nutsvoorzieningen, of kan het wegvallen van stroomvoorziening ernstige ecologische schade veroorzaken of apparatuur in ziekenhuizen buiten werking stellen. In tegenstelling tot IT systemen is het frequent heropstarten van ICS apparatuur na het installeren van updates vaak geen optie. De CIA (Confidentiality – Integrity – Availability) karakteristieken zijn onlosmakelijk verbonden met ICS omgevingen waarbij beschikbaarheid en integriteit de voornaamste belangen zijn. Confidentialiteit is belangrijk in systemen waar gevoelige data wordt verzameld en verwerkt.

LEVENSDUUR VAN ICS COMPONENTEN

Apparatuur in IT omgevingen – servers, laptops, werkstations en tablets – wordt regelmatig vervangen. ICS componenten daarentegen hebben een veel langere levensduur die kan oplopen tot meer dan 20 jaar. Hierdoor zijn industriële controleomgevingen vaak opgebouwd uit verouderde componenten met beperkte opslag- en verwerkingsmogelijkheden. Dit heeft tot gevolg dat oude, vaak kwetsbare versies van besturingssystemen en applicatiesoftware worden uitgevoerd op deze platformen. Effectieve virusscanners kunnen vaak niet uitgevoerd worden op deze componenten. Andere strategieën voor beveiliging zijn noodzakelijk.

Bedreigingen en gevolgen

EXTERNE AANVALLERS

Individuen en criminele groeperingen willen ICS systemen verstoren of platleggen om economische schade toe te brengen aan een organisatie, of om de reputatie van een bedrijf te kelderen. Vandaag zijn terroristische groeperingen en inlichtingendiensten bij overheden eveneens potentiële aanvallers die digitale wapens inzetten voor cyberaanvallen tegen kritische infrastructuur (zoals stroom- en watervoorziening, telecommunicatie-infrastructuur...). Anderzijds heeft industriële spionage tot doel intellectuele eigendom en kennis te verwerven om de concurrentiepositie van een bedrijf te verzwakken.

INTERNE AANVALLERS

Heel wat werknemers komen in nauw contact met ICS apparatuur: operatoren, technici, machinebouwers, onderhoudspersoneel, etc. Bescherming tegen aanvallen van internen is heel moeilijk. Vaak hebben deze laatsten fysieke toegang tot kritische componenten of beschikken ze over heel wat privileges om vanop afstand ernstige schade toe te brengen. Dikwijls bestaan er geen of gebrekkige procedures om bij ontslag heel snel alle rechten van werknemers in te trekken. Internen kunnen ook onopzettelijk malware op ICS apparatuur installeren onder meer via USB sticks.

MALWARE

Virussen en wormen zijn voorbeelden van kwaadaardige software of malware die confidentiële informatie kunnen stelen uit ICS systemen, de werking ervan kunnen verstoren of zelfs het systeem stilleggen. Sommige malware wordt ontwikkeld met als doel specifieke ICS omgevingen te bespioneren of plat te leggen en wordt vaak doelgericht geïnjecteerd in ICS componenten door aanvallers. Andere malware kan onbewust via media stations in ICS apparatuur terechtkomen.

3. Kwetsbaarheden in industriële controlesystemen

In **NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security** classificeert het *National Institute of Standards and Technology (NIST)* de oorzaken van ICS kwetsbaarheden volgens drie categorieën, namelijk (a) zwakke procedures en beleid, (b) kwetsbare platformen, en (c) kwetsbare netwerken. De waarschijnlijkheid dat specifieke kwetsbaarheden worden uitgebuit hangt af van verschillende factoren, zoals de impact van een mogelijke aanval en de waarschijnlijkheid om achteraf aansprakelijk gesteld te worden.

Zwakke procedures en beleid

In tegenstelling tot wat gebeurt in IT omgevingen besteden beheerders van OT infrastructuur vaak heel wat minder aandacht aan beveiliging. Dit komt omdat OT omgevingen traditioneel geïsoleerde systemen waren. Een onaangepast beveiligingsbeleid manifesteert zich in een gebrek aan documentatie over de afzonderlijke ICS componenten en netwerkverbindingen, maar ook in een gebrek aan training van operatoren en de afwezigheid van security audits. Tenslotte ontbreken vaak herstelplannen om bij een succesvolle aanval snel de kritische infrastructuur opnieuw op te

starten. Het koppelen van ICS omgevingen aan netwerken impliceert tevens dat IT en OT beheerders een gezamenlijk beleid inzake beveiliging moeten uitstippelen.

Kwetsbare platformen

Zwaktes in ICS componenten ontstaan zowel bij de ontwikkeling als bij de uitrol en het onderhoud ervan. Kwetsbaarheden ontstaan al tijdens het ontwikkelingsproces door het selecteren van onveilige ICS protocollen en door onveilige implementaties. Buffer overflows zijn een typisch voorbeeld hiervan. Bij installatie is vaak weinig aandacht voor fysische bescherming van apparatuur en documentatie. Andere problemen doen zich voor bij de configuratie en het onderhoud van componenten. In vele gevallen worden default paswoord en debug instellingen ongemoeid gelaten; software patches uitgebracht om beveiligingsproblemen aan te pakken worden erg laat of zelfs niet uitgevoerd. Veelal is bij de uitrol ook weinig aandacht voor de bescherming tegen malware en worden onnodige software services niet uitgeschakeld.

Kwetsbare netwerken

Communicatie infrastructuur is kwetsbaar omwille van verschillende redenen. Heel wat problemen worden veroorzaakt door een naïeve of platte netwerkarchitectuur. Het opdelen van de infrastructuur in zones met een aangepast veiligheidsbeleid reduceert de impact van succesvolle aanvallen. In vele gevallen zijn ook de verschillende netwerkcomponenten fysiek toegankelijk. Netwerkkabels kunnen ingeplugd worden om succesvolle aanvallen te lanceren. Tenslotte verzwakt de netwerkinfrastructuur door een ondoordachte strategie in verband met netwerkauthenticatie en autorisatie. Op onbeveiligde verbindingen kunnen paswoorden gelekt worden, of berichten worden gewijzigd waardoor het ICS systeem in een inconsistente toestand kan terechtkomen.

4. Factoren die leiden tot verhoogd risico

Gestandaardiseerde protocollen en technologieën

Fabrikanten van ICS componenten stellen alsmaar meer de specificaties van hun protocollen **beschikbaar voor het grote publiek** om integraties toe te laten door derde partijen. Bovendien schakelen fabrikanten over op gestandaardiseerde technologieën zoals Windows en UNIX systemen om competitief te blijven. Deze evoluties bieden technologische en economische voordelen. Helaas zijn een groot aantal kwetsbaarheden bij veel gebruikte technologieën gedocumenteerd waardoor de vatbaarheid voor cyberaanvallen stijgt. Toch is het gebruik van standaarden die door experten onder de loep genomen zijn te verkiezen boven eigen ontwikkelde protocollen.

Koppeling van controlesystemen met andere netwerken

Industriële controlesystemen worden steeds vaker gekoppeld aan bedrijfsnetwerken

die op hun beurt met het internet verbonden zijn. Het beveiligingsbeleid is gericht op het beschermen van bedrijfsprocessen en niet op de beveiliging van kritische systemen.

Onveilige connecties

Dikwijls wordt toegang tot het ICS systeem vanop afstand voorzien om opvolging en onderhoud te ondersteunen. De hierbij horende paswoordtechnologie is niet zelden onderhevig aan aanvallen van de meest uiteenlopende soort. Bij social engineering aanvallen wordt een werknemer overtuigd om zijn paswoord vrij te geven aan een derde die zich voordoet als een medewerker die dit paswoord nodig heeft. In heel wat situaties worden bovendien zwakke paswoorden gebruikt of default paswoorden niet veranderd.

Publieke informatie

Er wordt vaak nonchalant omgegaan met gegevens over de architectuur en de componenten van ICS omgevingen. Deze worden te vaak beschikbaar gesteld aan werknemers, integratoren en verkopers van ICS componenten. In sommige gevallen zijn deze gegevens zelfs publiek beschikbaar. Deze informatie geeft hackers strategische voordelen bij het plannen en uitvoeren van een cyberaanval.

5. Enkele recente incidenten

Recente cyberincidenten leren ons dat niet zelden maandenlange voorbereiding de eigenlijke aanval voorafgaan. Dikwijls keren dezelfde twee fasen terug. Tijdens de voorbereidingsfase wordt kennis ingewonnen over de opbouw van de ICS omgeving. Op basis daarvan kan malware ontwikkeld worden die vervolgens tijdens de eigenlijke uitvoering van de aanval wordt ingezet.

De STUXNET worm

De STUXNET worm (2010) is een software programma dat zich heeft verspreid op tienduizenden platformen. De worm brengt enkel schade toe aan specifieke Siemens S7-PLCs die via Profibus DP communiceren met frequentieomvormers van twee fabrikanten. Analyse van het virus toont aan dat een specifieke configuratie in het toerental van centrifuges het virus activeert. Deze configuratie is alleen aanwezig op de site voor de verrijking van uranium in het Iraanse Natanz.
Het virus maakt gebruik van zwaktes in PLCs, beveiligingslekken in Windows platformen en onvoorzichtige werknemers. STUXNET neemt controle over de centrifuges om ze op een te hoog en te snel fluctuerend toerental te laten werken waardoor ze

ernstig worden beschadigd.
Een belangrijk detail hierbij is dat dit controlesysteem niet gekoppeld is aan andere netwerken. Het virus werd via een USB stick binnengebracht in de opwerkingsfabriek. In dat geval spreekt men van een *airgap* die overbrugd moet worden.

Sabotage in Duitse staaloven

Deze aanval (2014) wordt beschreven door het Bundesambt für Sicherheid in der Informationstechnik (BSI). De overheidsdienst rapporteert dat hackers met zeer geavanceerde capaciteiten gebruik maakten van social engineering aanvallen op werknemers om toegang te krijgen tot de controlesystemen van de staalfabriek. Vervolgens werd het systeem gemanipuleerd zodat een hoogoven niet meer op een gecontroleerde manier kon worden uitgeschakeld.

Onderbreken van de energievoorziening in Oekraïne

Verschillende energieleveranciers in Oekraïne zijn in de eindejaarsperiode 2015-2016 het doelwit geweest van hackers. De aanval had een stroomonderbreking tot gevolg in een gebied groter dan Vlaanderen. Naast het onderbreken van de stroom werden de werkstations van operatoren gesaboteerd om de herstelprocedure te vertragen. Bovendien werden de telefooncentrales buiten werking gesteld zodat inwoners van de getroffen gebieden geen hulplijn konden bereiken.

6. Strategieën voor beveiliging van industriële controlesystemen

Beveiliging vereist een integrale aanpak. Vaak wordt daarvoor verwezen naar het concept *defense-in-depth*. In tegenstelling tot de dikwijls gebruikte perimeter beveiliging, is het belangrijk om de veiligheid te verhogen op verschillende niveaus. Het eerste onderdeel van deze integrale aanpak richt zich op het component niveau. Er wordt een overzicht gegeven van de technische aspecten die belangrijk zijn om de beveiliging van de onderdelen in het industrieel systeem zelf te beveiligen, en dit zowel op sensor/machine niveau als op het controle niveau. Het tweede deel focust op het ontwerp van een veilige netwerk infrastructuur en de bescherming van de communicatie over dit netwerk.

Component beveiliging

Het sensor/machine niveau omvat standaard low-level industriële componenten zoals industriële regelaars en eenvoudige sensoren waarvan de mogelijkheden om deze te beschermen beperkt zijn.

De componenten op het supervisie niveau (HMI, Historian, databases, programmeer PCs) maken vooral gebruik van standaard besturingssystemen zoals Windows of Linux die toegankelijker zijn voor de gebruiker. In dat geval kunnen beveiligingscomponenten toegevoegd worden. Verschillende praktijken uit de IT beveiliging, zoals *system hardening*, *antivirus*, *whitelisting* en *patching* (of updates) komen dan ook in aanmerking. Jammer genoeg kunnen niet al deze technieken zomaar overgenomen worden. Zo kunnen automatische updates een herstart van het OS veroorzaken en het achterliggend industrieel proces in de war sturen. Anderzijds kan het gebruik van USB sticks en andere transport media de veiligheid van het netwerk ondermijnen. Virussen bereiken dan het industrieel netwerk zonder last te hebben van firewalls of andere gelijkaardige maatregelen. Bij *system hardening* wordt het platform dichtgetimmerd. Voorbeelden zijn het verwijderen van onnodige toepassingen en het afsluiten van ongebruikte poorten.

Beveiliging van communicatie en netwerkinfrastructuur

Een veilig netwerk is opgebouwd uit verschillende veiligheidszones (bv. sensor/machine zone, controle zone en het bedrijfsnetwerk) en de communicatie tussen deze zones wordt streng gecontroleerd. De meest kritische zones worden het strengst bewaakt en toegang ertoe wordt beschermd door verschillende mechanismen waarvan er een aantal in de volgende sectie worden besproken.

Het gebruik van veiligheidszones is een belangrijke techniek voor het verbeteren van de veiligheid van industriële netwerken.

Het gebruik van deze veiligheidszones is een belangrijke techniek voor het verbeteren van de veiligheid van industriële netwerken. Gezien de beperkte mogelijkheden om de componenten op sensor/machine niveau te beveiligen en door het gebruik van onveilige communicatieprotocollen, zijn er andere mechanismen nodig om deze componenten adequaat te beschermen. Een goede netwerkinfrastructuur laat bovendien ook toe om toegangscontrole en authenticatie op netwerk niveau te implementeren. De gevaren ten gevolge van onveilige protocollen worden op die manier geminimaliseerd en beperkt tot een afgebakende zone. Authenticatie zorgt er voor dat enkel toegelaten gebruikers of componenten communiceren met componenten in een andere veiligheidszone. Communicatie in transit doorheen andere segmenten wordt versleuteld en enkel omgezet naar het onveilig protocol in de zone waar de component zich bevindt en waarmee gecommuniceerd wordt. Hoewel het concept van veiligheidszones eenvoudig is, is de correcte implementatie ervan geen triviale aangelegenheid.

7. Enkele software technologieën van nabij toegelicht

Firewalls

Firewalls zijn de digitale toegangspoorten voor *in- en uitgaand verkeer*. Een firewall zorgt ervoor dat toestellen of personen niet zonder toestemming toegang krijgen tot een netwerk van *buitenaf*. Firewalls zijn ofwel hardware componenten op het netwerk ofwel software componenten toegevoegd aan een besturingssysteem. Hardware firewalls, zoals Telenet en Proximus modems in thuisomgevingen, voorkomen dat onbevoegden toegang krijgen tot het thuisnetwerk en de hiermee verbonden toestellen. Software firewalls voorkomen dat eender wie op het netwerk toegang krijgt tot de bestanden die zich op de computer bevinden.

Een firewall zal standaard alle inkomende verkeer tegenhouden. Een firewall moet bijgevolg geconfigureerd worden om toegang mogelijk te maken tot interne diensten. Eenvoudige firewalls werken met twee types parameters, namelijk IP adressen en poorten. Zo kan een firewall regel ingesteld worden om een lokale website op een gegeven IP adres en poort toegankelijk te maken voor externen.

Firewall regels kunnen ook omgekeerd gebruikt worden. Ze leggen beperkingen op

aan uitgaand verkeer. Op die manier kunnen bijvoorbeeld BitTorrent Trackers van het lokale netwerk geweerd worden.

NextGeneration firewalls onderscheiden zich vooral in het aantal parameters dat in de firewall regels kan toegevoegd worden. Zo kunnen specifieke domeinnamen van websites geblokkeerd of net toegelaten worden. Daarnaast worden geavanceerde firewalls vaak uitgerust met een antivirus systeem.

Antivirus software

Een eenvoudige firewall houdt geen malware tegen. Een firewall zal immers de inhoud van het toegelaten verkeer (zoals e-mails of gegevens op USB sticks) niet nakijken. Antivirus software analyseert de gegevens die in een systeem worden binnengebracht, of de programma's die op een platform worden uitgevoerd. Hierbij worden de gegevens of programma's vergeleken met een lijst van gekende malware. Onder kwaadaardige software vallen virussen, wormen, ransomware, cryptoware, adware, spyware, trojan horses, etc. Antivirus programma's draaien doorgaans op het besturingssysteem en worden vandaag de dag dikwijls meegeleverd met het besturingssysteem (zoals *Windows Defender* vanaf Windows 8).

Een antivirus programma kan alle bestanden inspecteren, met bijzondere aandacht voor de bestanden die worden opgestart of die het systeem binnenkomen via email, download of USB stick. De antivirus software neemt een snapshot of signatuur van elk bestand en vergelijkt dit dan met een database van gekende malware.

Dagelijks worden honderden nieuwe types malware ontdekt. Het updaten en bijwerken van de antivirus software is daarom zeer belangrijk, al gebeurt dit normaal gezien automatisch. Antivirus beveiliging komt voor in veel varianten. Zo zullen sommige programma's zich inwerken in de browser om kwaadaardige websites op te sporen en bestaan er programma's om specifiek *crypto malware* te detecteren.

Over virusscanners bestaan heel wat misopvattingen.

Vandaar, de noodzaak om hier een aantal eigenschappen toe te lichten. Waterdichte antivirussoftware bestaat niet. Geen enkele virusscanner slaagt er in gloednieuwe malware te detecteren zonder deze eerst uit te voeren. Ook het naast elkaar gebruiken van meerdere antivirusprogramma's heeft weinig zin, daar dit leidt tot een gevoelige vertraging van de computer. De eerder naïef verwachte voordelen wegen niet op tegen de nadelen.

Uiteindelijk is waakzaamheid van de gebruiker belangrijker dan eender welke antivirussoftware.

Uiteindelijk is waakzaamheid van de gebruiker belangrijker dan eender welke antivirussoftware. Bij twijfel over mogelijke virussen op een bestand, kunnen websites geraadpleegd worden, zoals o.a. **www.virustotal.com**. Hier kunnen verdachte bestanden opgeladen en geanalyseerd worden door meer dan veertig verschillende antivirusprogramma's.

Intrusion Detection Systemen (IDS)

Intrusion Detection Systemen (IDS) vertonen veel gelijkenissen met antivirus programma's en firewall software. Meestal werken deze op basis van databases met signaturen en ontvangen geregeld updates.

Een IDS ontvangt echter niet het echte verkeer maar voert zijn analyses uit op een kopie van alle inkomend en uitgaand verkeer. De analyses vertonen sterke gelijkenissen met de analyses van antivirus software. Normaliter worden deze analyses uitgevoerd op een aparte machine en wordt het verkeer voor het gehele netwerksegment geanalyseerd. Een IDS systeem kan ook verdachte patronen en pakketten detecteren en op basis daarvan inschatten of hackers een computernetwerk binnendringen.

Aan de hand van analyses worden rapporten en aanbevelingen gegenereerd, en kunnen alarmen afgaan. IDS systemen zullen in dat geval SMS of e-mail berichten versturen naar vooraf ingestelde ontvangers bij detectie van verdachte patronen binnen een netwerk.

Intrusion Prevention Systemen (IPS)

Intrusion Prevention Systemen (IPS) worden in tegenstelling tot IDS wél *in de flow* van het verkeer geplaatst. Een IPS kan dus op basis van de detectie het verkeer tegenhouden alvorens het afgeleverd wordt. Aanvallen en virussen kunnen dus res-

pectievelijk voorkomen en tegengehouden worden in tegenstelling tot een IDS. Een belangrijk nadeel is echter dat alle verkeer wordt vertraagd. Afhankelijk van het IPS systeem, de hoeveelheid data en het type verkeer kan dit zelfs zeer aanzienlijk zijn. Verder werkt een IPS dus gelijkaardig aan een IDS.

Merk op dat zowel IDS als IPS nooit volwaardige alternatieven zijn voor antivirus software op computers. Zo is HTTPS of VPN verkeer versleuteld tussen twee eindpunten. Dit impliceert dat het niet onderworpen kan worden aan onderzoek door systemen die tussen deze eindpunten worden geïnstalleerd. Hierbij komt dat niet enkel versleuteld maar ook gefragmenteerd verkeer dikwijls aan de aandacht zal ontsnappen van IDS en IPS. Bij teveel verkeer op het netwerk zullen beide systemen namelijk slechts selectief pakketten analyseren.

Merk ten slotte op dat IDS, IPS en Firewall vaak in één adem worden genoemd. De meeste hardware IPS/IDS systemen zijn tegelijk ook firewalls.

Virtual Private Network (VPN)

Gebruikers moeten soms op afstand toegang verkrijgen tot diensten op private netwerken zoals IT omgevingen of productiesites. Zo is het handig dat een hersteller op afstand toegang kan krijgen tot de productiesite om taken uit te voeren. Een VPN verbinding zorgt ervoor dat apparaten in een extern netwerk kunnen aangesproken worden alsof ze zich in het lokale netwerk bevinden. Daarnaast biedt VPN verhoogde privacy en veiligheid ten opzichte van een normale verbinding. Deze eigenschappen worden bereikt door *tunneling* en *encryptie*. Tunneling houdt in dat een bericht in een ander bericht verpakt wordt. Het pad waarover het ingepakte bericht reist, heet de tunnel. Encryptie zorgt voor authenticatie en confidentialiteit.

VPN wordt vaak gebruikt in twee gevallen:

TOEGANG OP AFSTAND

Er wordt een verbinding opgezet tussen het werkstation van een gebruiker en een extern netwerk (zoals het IT netwerk of het productie netwerk). Een VPN cliënt op het werkstation zet de VPN verbinding op met het extern netwerk. De cliënt staat in voor het inpakken en encrypteren van berichten. De VPN cliënt connecteert met een VPN server in het externe netwerk. De VPN gateway is verantwoordelijk voor het controleren dat alleen gemachtigde gebruikers toegang tot het externe netwerk kunnen verkrijgen.

VERBINDING TUSSEN TWEE SITES

Er wordt een verbinding gelegd tussen twee netwerken. Aan beide netwerken is een gateway opgesteld die toegang reguleert. De VPN verbinding is in dit geval volledig transparant voor de gebruiker.

Er bestaan twee grote implementaties voor VPN:

- **IPsec** bestaat uit een verzameling van protocollen die een veilige VPN tunnel realiseren op IP-niveau. Het is gestandaardiseerd door het Internet Engineering Task Force.
- **OpenVPN** is een open-source project dat onderliggend gebruik maakt van TLS om VPN-functionaliteit aan te bieden.

Intermezzo:
Bouwstenen voor veilige communicatie

Confidentialiteit, integriteit en authenticiteit zijn belangrijke veiligheidsvereisten bij communicatie tussen verschillende platformen (werkstations, machines, servers…). In wat volgt worden de bouwstenen toegelicht om deze vereisten te realiseren.

Confidentialiteit en integriteit bij communicatie impliceren dat de inhoud van berichten die worden verzonden tussen twee partijen niet kan achterhaald noch onopgemerkt aangepast kan worden door derden. Symmetrische encryptiesystemen kunnen deze eigenschappen realiseren. Ze gaan ervan uit dat de communicerende partijen over een gedeelde geheime sleutel beschikken, die typisch gedurende een sessie wordt gebruikt. Deze sleutel wordt gebruikt door de zender om de boodschap te encrypteren en door de ontvanger om de boodschap opnieuw te decrypteren. Veel gebruikte symmetrische encryptiealgoritmes zijn AES en 3DES. Sommige encryptiesystemen realiseren enkel confidentialiteit, en worden gecombineerd met Message Authentication Codes (MACs) om de integriteit te garanderen. Een prototype voorbeeld is HMAC dat onderliggend gebruik maakt van SHA1, SHA2 of RIPEMD-160.

Confidentialiteit, integriteit en authenticiteit zijn belangrijke veiligheidsvereisten bij communicatie tussen verschillende platformen.

Authenticated Key Agreement protocollen maken het mogelijk om een geauthentiseerde sessiesleutel af te spreken tussen twee partijen. Na afloop van het protocol delen de beide partijen een sessiesleutel en kennen ze de identiteit van de andere partij met wie ze de sleutel delen. Ze zijn een cruciaal onderdeel van systemen voor veilige communicatie. Om een sessiesleutel af te spreken zijn twee strategieën mogelijk:

PRE-SHARED KEY (PSK)

PSK gaat ervan uit dat beide partijen reeds een symmetrische sleutel delen, die gedurende een langere termijn wordt opgeslagen en gebruikt. Op basis van deze gedeelde sleutel kan een sessiesleutel afgesproken worden. De lange termijn geheime sleutel wordt op voorhand geconstrueerd en uitgewisseld, wat een negatieve impact heeft op het beheer en de schaalbaarheid.

ASYMMETRISCHE ENCRYPTIE SYSTEMEN

Asymmetrische encryptie systemen werken de nadelen weg van PSK, en zijn gebaseerd op sleutelparen. Een sleutelpaar bestaat uit een private en een publieke sleutel, en elke partij die haar identiteit wil bewijzen aan andere partijen moet over een dergelijk uniek sleutelpaar beschikken. Bij Authenticated Key Agreement worden de publieke sleutels uitgewisseld om uiteindelijk met behulp van de private sleutel elkaars identiteit te bewijzen, en een gedeelte symmetrische sessiesleutel tot stand te brengen. Asymmetrische encryptie systemen worden frequent gecombineerd met Public Key Infrastructure (PKI). PKI zorgt ervoor dat publieke sleutels kunnen vertrouwd worden door partijen die willen communiceren met de eigenaar van de corresponderende private sleutel. Certificaten zorgen in deze context dat de publieke sleutel bewijsbaar gebonden wordt aan een individu, machine of organisatie. De Certificate Authority (CA) stelt zich hiervoor garant, en is ook meteen de partij die certificaten – vaak tegen betaling – uitreikt aan eigenaars van private sleutels. Deze eigenaars kunnen het certificaat vervolgens doorgeven aan andere partijen waarmee ze willen communiceren.

8. Ontwerp van een veilige netwerk architectuur

Tijdens de ontwerpfase van een moderne industriële installatie wordt nagedacht over de netwerkarchitectuur, d.w.z. dat ICS componenten worden met elkaar verbonden via netwerken. Deze verbindingen, al dan niet ethernet gebaseerd, zijn noodzakelijk voor de correcte werking van de installatie en kunnen niet vermeden worden. Bij een naïeve benadering worden alle componenten eenvoudig verbonden met behulp van switches, wat leidt tot een plat netwerk. Voor de ontwikkelaar en de operator van de installatie is dit zeer intuïtief, maar vanuit het perspectief van beveiliging suboptimaal. Bij een plat netwerk is elk geconnecteerd toestel binnen het netwerk zichtbaar en rechtstreeks aanspreekbaar. Verkeer van potentiële interne aanvallers kan zich hierdoor vrij doorheen het netwerk bewegen zonder enige vorm van controle. Andere strategieën dringen zich op tijdens de ontwerpfase met het oog op verhoogde beveiliging.

Het **zones & conduits model** beschreven door de IEC 62443 standaard vertrekt van het idee dat een netwerk moet opgedeeld worden in verschillende zones. Een zone is een groep van logische of fysieke componenten met gelijkaardige beveiligingsvereisten. De grenzen van een zone worden duidelijk afgebakend zodat geen twijfel kan bestaan of een component al dan niet tot een bepaalde zone behoort. Zones worden gekoppeld via *conduits*. Dit zijn de communicatiepaden tussen zones. Op deze paden worden technologieën voor beveiliging ingezet.

Een eenvoudige toepassing van dit model is de opsplitsing in twee zones, namelijk het kantoornetwerk en de regelaars (of het eigenlijke controlesysteem). Beide zones worden gekoppeld via één of meerdere conduits. Binnen elke conduit kunnen beveiligingstechnologieën worden ingezet. Zo kunnen beperkingen gelegd worden op het verkeer dat een zone kan binnengaan of verlaten. De verbinding met het internet verloopt via een conduit vanuit het kantoornetwerk, eveneens voorzien van de geschikte beveiligingstechnieken. Een meer geavanceerde maar veel gebruikte architectuur voegt een bijkomende *demilitarized zone* (DMZ) toe tussen het kantoornetwerk en de regelaars. In die zone worden toestellen of diensten geplaatst die door de beide andere worden aangesproken zoals loggingservers en programmeercomputers. Uiteraard kan men elke zone verder opdelen in kleinere zones, en zo bijvoorbeeld machines van elkaar scheiden.

Logische opdeling in zones op basis van benodigde beveiliging is aangewezen.

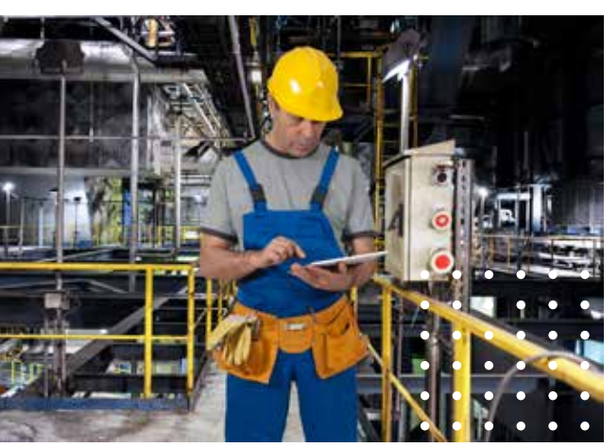
Het opdelen in zones kan gebeuren op basis van de fysieke locatie van componenten. Dit is intuïtief voor beheerders en operatoren, maar is niet steeds de optimale strategie vanuit het perspectief van beveiliging. Logische opdeling in zones op basis van de benodigde beveiliging is meer aangewezen. Segmentatie via VLANs is een veelgebruikte techniek om de logische opdeling praktisch te realiseren. Segmentatie is een strategie die oorspronkelijk werd ingezet om de prestaties van het controlenetwerk aanvaardbaar te houden in complexere omgevingen, maar wordt tegenwoordig gehanteerd om zones te creëren waartussen de monitoring en beveiliging kan gebeuren.

Binnen een zone worden de acties vastgelegd die kunnen uitgevoerd worden door toestellen en gebruikers. Een goede strategie verleent slechts die minimale rechten die nodig zijn voor de correcte werking van de installatie. Men spreekt in deze context van *Principle of Least Privilege*. Hoewel de impact van aanvallen door het invoeren van zones kan verzacht worden kunnen aanvallers en malware nog steeds zones binnendringen. Daarom is het belangrijk om permanente monitoring te voorzien door het inzetten van IDS en IPS systemen.

9. Oprukkende trends

Mobiele platformen

Over het algemeen worden standaard industriële componenten zoals HMIs gebruikt om productieprocessen te monitoren en aan te sturen. Mobiele platformen kunnen echter een interessante toevoeging zijn aan ICS omgevingen. Hedendaagse mobiele platformen zijn heel krachtig en hebben de mogelijkheid om data van verschillende bronnen te verwerken en op een aantrekkelijke manier weer te geven. Door hun rijke mogelijkheden aan draadloze communicatie en mobiliteit kunnen ze gebruikt worden om on-demand specifieke gegevens van het productieproces op te vragen en, indien nodig, acties te ondernemen zoals het inroosteren van onderhoud, bestellen van nieuwe onderdelen of het ingeven van rapporten.



Het introduceren van mobiele toepassingen in industriële netwerken is echter niet zonder risico. Veel industriële componenten zijn gevoelig voor onverwacht netwerkverkeer en de meeste industriële protocollen implementeren geen enkele vorm van authenticatie. De openheid en flexibiliteit van mobiele toestellen introduceren bijgevolg extra risico's. Hierdoor is het van cruciaal belang om technieken zoals beheer van mobiele toestellen en toegangscontrole tot het netwerk in te zetten om deze risico's te beheersen.

Cloud omgevingen

Steeds meer parameters worden gemeten in productieomgevingen. Voorbeelden zijn temperatuur, vochtigheid, start- en stoptijden van taken, en trillingen. Sommige parameters zijn enkel relevant binnen het productieproces en worden gebruikt voor de directe aansturing van de machine. Andere daarentegen zijn dan weer nuttiger voor processen buiten de productieomgeving, of zelfs buiten de organisatie. Zo kunnen parameters uit de productieomgeving nuttige informatie verschaffen voor de planningssoftware (of MES systemen). Het doorsturen van productiegegevens naar cloud systemen verhoogt de toegankelijkheid van deze gegevens voor werknemers zonder dat ze hiervoor toegang moeten hebben tot het interne bedrijfsnetwerk. Bepaalde gegevens kunnen eveneens doorgestuurd worden naar de machinebouwer, die op zijn beurt deze gegevens kan benutten voor het uitvoeren van herstellingen, het voorspellen van onderhoud aan de machine of het wegwerken van knelpunten bij de ontwikkeling van toekomstige machines. Tenslotte kunnen deze parameters benut worden door statistici of gouvernementele organisaties.

Cloud omgevingen zijn technologische bouwblokken die deze tendens kunnen faciliteren. Hierbij wordt vaak een onderscheid gemaakt tussen *private cloud systemen* – waarbij gegevens binnen het bedrijf worden opgeslagen en/of verwerkt – en *publieke cloud systemen* – waarbij gegevens worden opgeslagen/verwerkt bij derde partijen die over de nodige digitale opslagcapaciteit beschikken. Bij *hybride cloud systemen* worden beide strategieën gecombineerd. Diverse belangen kunnen de keuze voor een specifieke set-up beïnvloeden. Zo worden erg gevoelige bedrijfsgegevens vaak lokaal opgeslagen en verwerkt. Anderzijds is de betrouwbaarheid en beschikbaarheid van de data vaak hoger bij opslag op servers van derde partijen die door middel van *Service Level Agreements* (SLAs) garanties bieden omtrent deze eigenschappen.

10. Aanbevelingen voor herstel bij cyberincidenten

Hoewel een doordachte netwerkarchitectuur samen met het inzetten van gepaste beveiligingstechnologieën het risico op succesvolle aanvallen beperken en de impact kunnen verzachten, zijn aanvallen niet uitgesloten. Om efficiënt te reageren op cyberincidenten zijn herstelprocedures noodzakelijk. Merk op dat heel wat overheden *cyber emergency response teams (CERTs)* oprichten om bedrijven te ondersteunen bij cyberincidenten. In België is meer info te vinden op **www.cert.be**. CERT coördineert en geeft advies voor herstel in geval van ernstige cyberincidenten, en biedt ondersteuning aan bedrijven om cyberincidenten te voorkomen.

Disaster Recovery Plan (DRP)

Een plan voor herstel in geval van rampen moet deel uitmaken van elke ICS omgeving. Er moeten procedures uitgeschreven worden die in werking treden in geval van cyberincidenten en waarin verantwoordelijkheden worden toegekend aan verschillende individuen en teams binnen de organisatie. Verder is het belangrijk om steeds te beschikken over een volledig logisch netwerkdiagram en een lijst van individuen die toegang hebben tot delen van de ICS omgeving.

Incident Response

Het is heel belangrijk cyberaanvallen zo vroeg mogelijk te detecteren. Verschillende symptomen kunnen immers een cyberincident aankondigen zoals gebruikers die niet langer kunnen inloggen, waarschuwingen van antivirus en IDS systemen en onverwachte configuratie wijzigingen of uitval van componenten. Gedocumenteerde herstelplannen versnellen de herstelprocedures en kunnen de ecologische of economische schade beperken.

11. Gevallenstudies

Heel wat praktische experimenten werden uitgevoerd door de partners in technologie transfer projecten. Hieronder worden een drietal gevalsstudies geschetst, en beknopte generieke besluiten geformuleerd. Voor meer gedetailleerde informatie kan u de projectpartners contacteren.

PLC Security

Heel wat PLC ontwikkelaars leveren specifieke tools voor PLC programmatie. Sommige fabrikanten gebruiken zelf ontwikkelde software, zoals Siemens met Step7 / TIA Portal. Anderen vallen terug op een derde partij zoals PC WORX bij Phoenix Contact. Nog anderen bouwen dan weer modules bovenop een gekend platform. Zo biedt Beckhoff TwinCat aan bovenop Microsoft Visual Studio.

PLCs hebben een aantal gemeenschappelijke kenmerken. Typisch worden communicatieprotocollen zoals ModBus of Profinet ondersteund. Bovendien ontbreekt authenticatie en autorisatie op de meeste PLCs met uitzondering van enkele recente types. Dit houdt in dat iedereen met behulp van de meegeleverde PLC software tools en toegang tot het netwerk waarin de PLC staat opgesteld de PLC kan herprogrammeren om het gedrag ervan te veranderen.

Bij Phoenix PLCs, meer specifiek de ILC-serie, zijn na het programmeren de projectgegevens vrij toegankelijk via een publieke FTP sessie naar de PLC. Bijgevolg kan de PLC eenvoudig met PC WORX software geherprogrammeerd worden. Netwerksegmentatie is bijgevolg de belangrijkste strategie om toegang tot de PLCs beter af te schermen.

Industrial Network Discovery Protocols

Heel wat industriële componenten ondersteunen automatische detectie op het netwerk. Dit betekent dat via het uitsturen van *broadcast discovery pakketten* het hele netwerk geadresseerd kan worden. De industriële componenten reageren op deze pakketten, en laten weten op welke manier ze kunnen aangesproken worden. Dit is handig voor ingenieurs die HMI en PLC systemen wensen te programmeren, en niet op de hoogte zijn van de structuur van het netwerk en de protocollen. Automatische detectie wordt echter ook ondersteund op diverse andere industriële apparaten waarvan het nut minder duidelijk is. Switches, routers en vele Windows systemen reageren eveneens op deze broadcast pakketten.

Een typisch voorbeeld is het Profinet Discovery Protocol (Profinet-DCP) dat is ingebouwd in de TIA Portal tool van Siemens. Dit protocol vertoont een aantal eigenschappen die belangrijk zijn met het oog op beveiliging:

1

Profinet-DCP moet men situeren op MAC niveau binnen het OSI-model. Dit heeft tot gevolg dat routers en firewalls automatisch deze pakketten tegenhouden.

2

Profinet-DCP discovery duurt gemiddeld 2 seconden ongeacht de grootte van het netwerk. De toestellen die reageren variëren van PLCs, HMIs, IO eilanden, drives, switches en routers tot Windows PCs uitgerust met TIA Portal. Niet enkel Siemens toestellen maar ook PLCs van andere fabrikanten die Profinet ondersteunen reageren op deze pakketten.

3

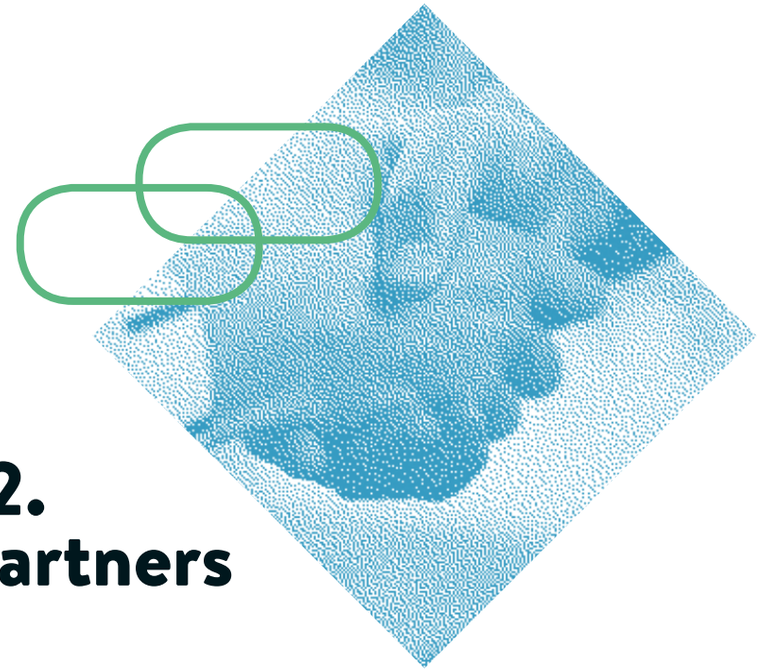
Naast detectie ondersteunt het Profinet-DCP protocol ook de aanpassing van instellingen zoals IP-adresgegevens en de naam van het toestel. Deze aanpassingen kunnen ook uitgevoerd worden bij switches en routers, waardoor deze buiten werking kunnen gesteld worden en derhalve het netwerk kunnen ontregelen.

Netwerksegmentatie verkleint hier ook de impact van discovery tools die ingezet worden door kwaadwilligen. Industriële firewalls kunnen geconfigureerd worden om Profinet verkeer tussen zones te reguleren.

Netwerk Segmentatie met VLAN technologie

Veel bedrijven zijn door geleidelijke uitbereiding van hun netwerk geëvolueerd van een klein beheersbaar netwerk naar een complex netwerk met beperkte of zonder segmentatie. VLAN technologie kan de overgang faciliteren van een plat naar een gesegmenteerd netwerk. Een opdeling van segmenten biedt naast betere bescherming tegen aanvallen ook andere voordelen. Zo hebben praktische gevalstudies aangetoond dat het totale aantal netwerkpakketten kan dalen in concrete omgevingen met 90% waardoor heel wat bandbreedte vrijkomt. Een opdeling in segmenten verhoogt bijgevolg ook de prestaties in het netwerk.

Een opdeling in segmenten verhoogt ook de prestaties in het netwerk.



12. Partners

E&A - Energie & Automatisering

De onderzoeksgroep Energie & Automatisering is één van de 14 onderzoeksgroepen van de faculteit industriële ingenieurswetenschappen van de KU Leuven Technologiecampus Gent. De groep maakt deel uit van de departement ESAT via de technologiecluster Elektrotechniek.
Het onderzoek kadert in de domeinen elektrische energietechniek en industriële automatisering. Binnen de groep wordt via verschillende onderzoeksprojecten expertise opgebouwd rond autonome hybride energiesystemen, industriële datacommunicatie en beveiliging, PV metrologie, industriële energiemetingen en lichte elektrische mobiliteit.

–

Website: www.kuleuven.be/eena
Contact: Jan Cappelle, Bart Huyck, Hendrik Derre

–

MSEC-DistriNet – Mobile & Secure

MSEC focust op de ontwikkeling van complexe software systemen en toepassingen met sterke vereisten inzake beveiliging en privacy. Enerzijds faciliteert MSEC de ontwikkeling van omgevingen met mobiele componenten (zoals smartkaart techno-

logie, smartphone en tablet platformen, en ingebedde systemen). Anderzijds ligt de klemtoon op het ontwerp en de evaluatie van Industriële Controle Systemen (ICS) en SCADA omgevingen. Het onderzoek leidt tot ondersteuning voor zowel ontwerpers als beheerders van gekoppelde productieomgevingen. De MSEC onderzoeksgroep maakt deel uit van iMinds-DistriNet.

–

Website: https://iiw.kuleuven.be/onderzoek/msec/
Contact: Vincent Naessens, Vincent Raes, Jan Vossaert, Laurens Lemaire

–

XiaK – eXpertisecentrum Industriële Automatisering Kortrijk

XiaK-UGent combineert uitgebreide kennis aan expertise binnen de belangrijkste domeinen van de industriële automatisering. Het Industrial Security Center is uitgerust met enkele typische modellen van automatiseringsnetwerken waar demonstraties en testen kunnen plaatsvinden in een veilige en gecontroleerde omgeving. Binnen deze gesimuleerde omgeving kunnen gerichte aanvallen uitgewerkt en toegepast worden op een breed gamma van automatiseringscomponenten, netwerkconfiguraties en industriële controle systemen. Op die manier worden kwetsbaarheden van oude en nieuwe technologieën blootgelegd. Leveranciers vinden hier ook een ideale omgeving om nieuwe componenten, features of patches uit te proberen.

–

Website: http://www.xiak.be/security.php
Contact: Tijl Deneut, Johannes Cottyn

–

Deze brochure werd samengesteld in het kader van de tetra projecten *Industriële Security* (140354) en *Verboten - Veilig beheer en ontwerp van industriële netwerken* (140318) met steun van het Agentschap Innoveren & Ondernemen en de deelnemende bedrijven in de gebruikersgroepen.

Correcties en taalsuggesties: Erik Van Achter | Vormgeving: Marieke Van Raes