Eén publiekprivate geïntegreerde aanpak.
Eén sluitende nationale infrastructuur ter bestrijding van cybercrime.

Process Control Security in het Informatieknooppunt Cybercrime

NICC

Process Control Security in het
Informatieknooppunt Cybercrime
NICC

Mark Frequin
Directeur-generaal Energie en Telecom bij het Ministerie van Economische Zaken

De continuïteit van onze vitale infrastructuren en de veiligheid van vele andere productieprocessen staat of valt met de (informatie)veiligheid van proces-controlesystemen. Uit analyses en incidenten blijkt dat die voor verbetering vatbaar is.
Voordat het risicio voor onze samenleving te groot wordt, moeten we deze veiligheidsproblematiek gezamenlijk oppakken. Ik heb daarover afspraken gemaakt met het CIO Platform Nederland.
Het Informatieknooppunt Cybercrime vormt de schakel tussen de nationale en internationale publiekprivate activiteiten op dit terrein en brengt deze publicatie uit. Hierin wordt duidelijk gemaakt waarom het beveiligingsniveau van productieprocessen op een hoog niveau moet worden gebracht en gehouden.
Het gaat hierbij om de integrale aanpak van zowel de informatiebeveiliging als de organisatorische en fysieke beveiliging om de procescontrolesystemen veilig te houden. Deze awareness is van groot belang en een startpunt voor een gezamenlijke aanpak. Daarom beveel ik u deze publicatie van harte aan.

Opsporing en vervolging van cybercrime? Heel belangrijk, maar niet dé oplossing voor het probleem. Voorkómen is beter!

Inleiding

Opsporing en vervolging van cybercrime? Heel belangrijk, maar niet dé oplossing voor het probleem. Voorkómen is beter! De sectoren die zijn aangesloten op het Informatieknooppunt Cybercrime hebben de (informatie)beveiliging van procescontrolesystemen (PCS), waaronder SCADA, als uitdaging opgepakt. Deze publicatie maakt duidelijk waarom het noodzakelijk is dat organisaties de controle hebben en houden over de beveiliging van de informatie- en communicatietechnologie (ICT) in hun procesbesturingsomgevingen.
Ook wordt duidelijk gemaakt waarom het van belang is om de procescontrolesystemen binnen en buiten de vitale sectoren op het gewenste beveiligingsniveau te krijgen en te houden en waarom een gezamenlijke aanpak van belang is. 'Gezamenlijk' betekent hier de publiekprivate bundeling van de krachten en kennis van de PCS-gebruikers en alle andere betrokkenen, zoals fabrikanten, leveranciers, system integrators, dienstverleners, overheden, opleidingen en kennisinstellingen.

Op de linkerpagina's van deze publicatie vindt u eerst een uitleg over PCS, en vervolgens een bloemlezing van het gebruik van PCS in verschillende sectoren. Deze stukjes geven in een notendop aan wat het belang is van de betrouwbaarheid van PCS voor de Nederlandse samenleving. Het gaat om zaken die u dagelijks persoonlijk raken. Om de betrouwbaarheid ervan te waarborgen, is het nodig dat we samen de informatiebeveiliging van die PCS onder controle brengen en houden. De noodzaak daarvan wordt onderaan de pagina's geïllustreerd met voorbeelden over waargebeurde incidenten en bedreigingen.

Procescontrolesystemen: het hart van veel sectoren

Onder de term PCS verstaan we het totaal aan procescontrolesystemen, waaronder systemen voor Supervisory Control and Data Acquisition (SCADA), procescontrolenetwerken, PLC-systemen en hun fysieke en organisatorische omgevingen. Dit wordt ook vaak procesautomatisering (PA) genoemd.
PCS worden in veel sectoren gebruikt voor de automatische monitoring en besturing van essentiële fysieke processen. Denk hierbij aan onze energie- en drinkwatervoorzieningen (productie, transport en distributie), de waterhuishouding, het railvervoer (bijvoorbeeld wissels en seinen) en tunnelveiligheidsystemen.
PCS vormen het hart van productieprocessen in raffinaderijen, de chemische industrie en de voedingsmiddelen- en medicijnindustrie. Ze worden steeds vaker toegepast in gebouwbeheer- en toegangscontrolesystemen in vitale objecten als telecommunicatieknooppunten en computercentra.
Er zijn verschillen tussen kantoorautomatisering en procesautomatisering als het gaat om de eisen die aan de systemen worden gesteld. Waar het bij kantoorautomatisering vaak gaat om Vertrouwelijkheid en dan pas om Beschikbaarheid en Integriteit, gaat het bij procesautomatisering juist in de eerste plaats om Beschikbaarheid en Integriteit en daarna pas om Vertrouwelijkheid. Daardoor verschilt ook de beveiligingsfocus.

APRIL 2009 Jesse William McGraw (hackersidentiteiten: GhostExodus en PhantomExodizzmo) dringt binnen in een aantal systemen van het W.B. Carrell Memorial Clinic ziekenhuis in Dallas, Texas. Hij krijgt toegang tot het patiëntenregistratiesysteem en de procescontrolesystemen die de verwarming, ventilatie en overige luchtbehandeling regelen.

Samen tegen cybercrime

Private en publieke partijen strijden in de Nationale Infrastructuur ter bestrijding van Cybercrime zij aan zij om het niveau van cybersecurity binnen de vitale sectoren in Nederland op het gewenste niveau te brengen. Het programma Nationale Infrastructuur ter bestrijding van Cybercrime (NICC) speelt daarbij een faciliterende, verbindende en versterkende rol. Door kennis te delen en informatie uit te wisselen, beschikken overheid en bedrijfsleven over voldoende informatie om zelf de goede beslissingen te kunnen nemen.

Het Informatieknooppunt Cybercrime is het kloppende hart van de NICC. De vitale sectoren nemen hieraan deel. Zij hebben informatieveiligheid van PCS geïdentificeerd als een sectoroverstijgend thema.
De informatieveiligheid van PCS loopt achter bij die van de normale kantoorautomatisering (KA). Ongewenste beïnvloeding van PCS is een toenemende dreiging. Samen resulteert dit in een risico dat niet meer genegeerd mag en kan worden. PCS besturen fysieke processen. Ongewenste beïnvloeding daarvan kan leiden tot ernstige verstoring van vitale infrastructuur, wat ernstige gevolgen heeft voor onze economie, het milieu en de levens van mensen en dieren. Daarom moeten bedrijfsleven (als gebruiker en leverancier), overheid (als gebruiker, toezichthouder en katalysator), onderwijs en onderzoek de aanpak van dit risico samen voortvarend oppakken.

Veilig ondergronds

Dagelijks vervoeren GVB in Amsterdam en RET in Rotterdam ieder enkele honderdduizenden reizigers per metro naar hun plaats van bestemming. Dat vereist betrouwbare PCS voor het energiebeheer, de tractiespanning en het instellen van veilige rijwegen door middel van seinen en wissels. PCS worden ook gebruikt voor het bewaken van de veiligheid van de reizigers in de ondergrondse stations. Denk aan de brandveiligheid en sluitsystemen bij indringend water.
Beide vervoerbedrijven bestuderen de volledige automatisering van de metro's, waardoor geen bestuurder meer nodig is. In Amsterdam is het plan hiermee in 2014 op de Oostlijn te starten. In 2019 moeten alle metro's zonder bestuurder rijden. Daarvoor moet wel eerst (informatie)beveiliging van de PCS die dit allemaal besturen en bewaken goed geborgd zijn.

JANUARI 2008 Een jonge hacker weet de tramwissels in het Poolse Łódź te manipuleren met een gemodificeerde afstandsbediening. Vier trams ontsporen, er vallen twaalf gewonden.

Wat is het risico?

Veel ingrediënten verhogen samen de kwetsbaarheid van PCS. We zetten ze op een rijtje in vier categorieën.

Risicofactoren van de PCS-technologie

De (informatie)beveiliging van PCS loopt vaak sterk achter bij die van de kantoorautomatisering. De redenen hiervoor zijn zowel van beleidsmatige, organisatorische en technologische als economische aard. In veel organisaties zijn er grote cultuurverschillen tussen de procesautomatisering en de kantoorautomatisering.

Procesautomatisering is van oudsher gericht op een hoge graad van beschikbaarheid, betrouwbaarheid, efficiency en veiligheid. De wijziging van PCS-technologie gaat sluipend. Vroeger werd speciale PCS-hardware met leverancier-specifieke programmatuur en hardware gebruikt, die moeilijk beïnvloedbaar was van buitenaf. Dit wordt echter steeds vaker vervangen door COTS-computersystemen (Commercial-Off-The-Shelf) met open besturingssystemen zoals Windows of Linux, een Internetprotocolsuite en toepassings-programmatuur (soms zelfs open source SCADA-software).

De afschrijfperioden van PCS zijn voor de niet-Windows-systemen lang in vergelijking met die voor kantoorauto-matisering. PCS hebben dus een lange economische levens-duur in vergelijking met de snelle technische ontwikkelingen van ICT en zijn dus lange tijd in gebruik. Het is vaak lastig om extra veiligheidsmaatregelen toe te voegen.

Het personele risico

Traditioneel is de procesautomatiseerder niet opgeleid in (informatie)beveiliging. Hij is zich er dan ook niet of nauwelijks van bewust dat er een taak is bijgekomen.

Als het procesautomatiseringsmanagement al beveiligingsbewust is, vindt het nauwelijks een luisterend oor bij het hogere management omdat wijzigingen veel geld kunnen kosten.

De ICT-afdelingen zien procesautomatisering eerder als een verzameling sensoren, pompen, motoren en kleppen, en niet als te beveiligen informatietechnologie.

Wanneer procesautomatiseerders en ICT-ers proberen samen te werken, blijkt er een groot cultuurverschil te bestaan tussen de procesbesturing en -controle ('vierentwintig uur per dag, zeven dagen per week') enerzijds en de ICT-aanpak bij de kantoorautomatisering ('even herstarten tijdens de lunchpauze') anderzijds.

Risicofactoren van de PCS-omgeving

De procesautomatiseringsomgeving wordt steeds opener. Door marktontwikkelingen zijn organisaties soms verplicht gegevens uit hun PCS via het internet aan derden te leveren. Ook is het handig dat storingsmedewerkers van thuis uit de PCS kunnen benaderen. En leveranciers van turnkey-systemen willen op afstand wijzigingen kunnen doorvoeren.

Betrouwbaar drinkwater

PCS zijn onmisbaar geworden bij de winning, zuivering en distributie van ons drinkwater. Deze processen zijn daardoor sterk verbeterd. Met de komst van PCS is het bijvoorbeeld mogelijk geworden verbruiksprognoses te gebruiken bij het aansturen van het productieproces. Er kan daardoor veel gelijkmatiger geproduceerd worden, wat de efficiëntie en de productkwaliteit sterk ten goede komt. De gegevens over het productieproces zijn ook veel sneller beschikbaar. Waterleidingbedrijven kunnen daar dus sneller, in de meeste gevallen zelfs automatisch, op reageren. De continuïteit van de waterlevering en de waterkwaliteit zijn door PCS goed geborgd.

Het belang van betrouwbare PCS is dus duidelijk. Vaak zullen de waterleidingbedrijven bij uitval van de PCS terug kunnen vallen op de oude methoden van water leveren. Maar dat is zeker niet eenvoudig en het heeft grote gevolgen voor de effectiviteit, efficiency en organisatie.

FEBRUARI 2008

Een PCS storing in het pompstation te Epe leidt tot het ongecontroleerd oplopen van de druk in het drinkwaterleidingstelsel. Leidingen breken op zeven plaatsen. In Epe, Oene en Zuuk valt de drinkwatervoorziening enkele uren uit.

PCS-ontwerpers, PCS-leveranciers en systeemintegratoren zijn meer gericht op het ontwikkelen van nieuwe mogelijkheden dan op het ontwikkelen van inherent veiliger systemen. Dit wordt mede veroorzaakt door de vraag van de klant. Overigens is daar al wel een kentering te zien, zowel aan de vraag- als de aanbodzijde.

Externe (criminele) risicofactoren

Aan de dreigingzijde constateren we een toenemende belangstelling voor en kennis over PCS/SCADA in hackerskringen. Externe koppelingen van PCS-netwerken met de buitenwereld gepaard aan een lage weerstand van PCS-protocollen voor incorrecte communicatieberichten verhogen de kans op een PCS-verstoring door een Trojan of een hacker aanzienlijk.

Overigens kunnen besmettingen zowel bewust als onbewust een PCS-infrastructuur binnen dringen. In beide gevallen kan de schade aanzienlijk zijn.

Continu druk op gas

Gasunie voorziet heel Nederland en delen van Noordwest-Europa van aardgas. Een verstoring van de gasvoorziening heeft direct maatschappelijke gevolgen. Gasunie wil verstoringen zoveel mogelijk voorkomen, en als dat niet lukt de gevolgen daarvan beperken. Daarom is flexibiliteit in het leidingnet ingebouwd.
De PCS die het gastransport aansturen, zijn dubbel uitgevoerd. De omschakeling wordt geregeld getest. Om fouten te voorkomen, worden wijzigingen aan de systemen zorgvuldig gecontroleerd en getest. De netwerkomgeving van de PCS is afgescheiden van de kantooromgevingen. Ook de robuustheid tegen ongewenste toegang door personen en kwaadaardige software wordt periodiek getest. Goed getrainde en risicobewuste medewerkers zorgen ervoor dat Gasunie zijn gastransporttaken hoogwaardig en betrouwbaar kan uitvoeren. Het moet goed gaan, ook als het onverhoopt fout gaat.

NOVEMBER 2001

Een deel van Zeeland krijgt gas met een zeer hoog percentage stikstof geleverd. Oorzaak: één van de PCS van het Delta-gasmengstation in Borssele werkt fout door het installeren van verkeerde PCS-software. Zo'n 26.000 huishoudens zitten tot drie dagen in de kou en kunnen niet koken. De huis-aan-huis-heraansluiting op de gasvoorziening vereist een grootschalige inzet van politie, brandweer en gasstoringsmedewerkers uit het hele land.

Vinger aan de pols

Hoe veilig of onveilig gaan we om met de (informatie)beveiliging van PCS? Die vraag stelde de Nederlandse drinkwatersector zichzelf in 2007. Een quickscan-benchmark toonde sectorbreed een aantal zwakke punten aan. Ook kwamen opvallende verschillen in beveiligingsniveaus tussen de verschillende drinkwaterbedrijven aan het licht.
De drinkwatersector heeft good practices ontwikkeld om de zwakke punten aan te pakken. Om ook bedrijven buiten Nederland te helpen en zinvolle feedback terug te krijgen, zijn deze good practices in het Engels vertaald en internationaal beschikbaar gesteld. Aan vertalingen in het Italiaans, Frans en Japans wordt door derden gewerkt.
De energiesector heeft dezelfde benchmark-aanpak gebruikt. Ook daar zijn sectorbreed verbeterpunten gevonden. Een vergelijking tussen beide sectoren laat interessante overeenkomsten en verschillen zien. Vrijwel alle bedrijven in beide sectoren gebruiken de Code voor Informatiebeveiliging (ISO/IEC 27002:2005) voor hun kantoorautomatisering.
De meeste bedrijven uit beide sectoren passen deze Code ook toe als beveiligingsleidraad voor hun procesautomatisering.
De grootste verschillen tussen beide sectoren zitten in de beleidsmatige hoek, bijvoorbeeld het wel of niet hebben van specifiek beleid voor de PCS-omgeving.

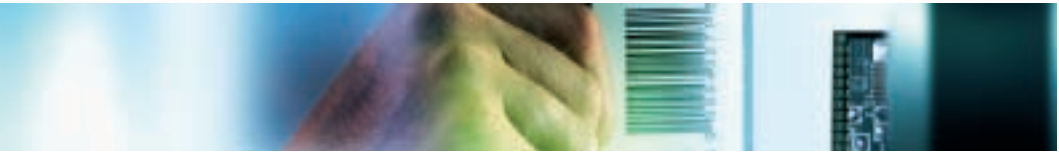
Droge voeten

Veel Nederlanders leven meters beneden de zeespiegel of het rivierniveau. Toch slapen we rustig. We vertrouwen op onze waterschappen die de dijken, pompen, sluizen, stuwen en andere waterwerken onderhouden. Het beheer van de waterpeilen in polders en de watergangen, 24 uur per dag en het hele jaar door, wordt steeds meer geregeld met PCS. Het meten van de peilen en de aansturing van pompen en stuwen gebeurt vaak op afstand, soms via GSM/GPRS of zelfs via het internet.
Ook de grote zeekeringen, bijvoorbeeld de Oosterschelde- en Maeslandtkeringen en de zeesluiscomplexen, houden onze voeten en infrastructuur droog. Rijkswaterstaat beheert ze met PCS. Bij dreigende situaties, gebaseerd op wind- en tijverwachtingen, sluiten de zeekeringen volautomatisch.

MAART 2000 Als gevolg van een menselijke bedienfout gaat de verkeerde sluisdeur open in de zeesluizen bij Delfzijl. Door de sterke stroming zijn de sluisdeuren daarna niet meer te sluiten. Kanalen lopen leeg, arken en boten tot in de stad Groningen aan toe komen enkele dagen droog te liggen en de beroepsvaart ligt dagenlang stil.

Zorgpunten voor beide sectoren zijn onder andere het gebrek aan borging van de PCS-informatiebeveiliging door audits (de Wet op de jaarrekening stelt die zelfs verplicht) en de wijze waarop toegang voor onderhoudstechnici van derde partijen tot de PCS-omgeving is geregeld.

De benchmark heeft zijn waarde in de praktijk bewezen. Hij heeft een aantal collectieve aandachtspunten geïdentificeerd en individuele bedrijven gewezen op punten waar ze tekortschieten. Daarmee is tevens een agenda gezet voor de Water-ISAC en de Energy-ISAC in het Informatieknooppunt Cybercrime.



Continue overslag

In de Nederlandse havens worden goederen overgeslagen vanuit zeeschepen naar de wal en andersom. De integratie van PCS met back-office ICT speelt hierin een steeds grotere rol. Bij de Europese Container Terminal (ECT) in Rotterdam worden zeecontainers vierentwintig uur per dag, zeven dagen per week volautomatisch met kranen uit het schip gelicht. Computergestuurde, zelfstandig over de terminal rijdende wagens (Automated Guided Vehicles ofwel AGV's) brengen de containers naar hun opslaglocatie en laden ze op trein-wagons of trailers voor direct transport.
PCS geven de AGV's de opdracht om naar de opslag- of behandellocatie te rijden. Ze bewaken de positie en status van de wagens en regelen de voorrang van de ene AGV op een andere. PCS zorgen voor een snelle overslag van de zee-containers, zodat een zeeschip uiterlijk binnen 24 uur de Rotterdamse haven weer kan verlaten.

MEI 2004 Het PCS-netwerk van het Australische RailCorp wordt getroffen door de Sasser-worm. In de ruime omgeving van Sydney valt een dag later 80% van de treinen uit doordat het veiligheidssysteem onbetrouwbaar is. 50.000 passagiers lopen ernstige vertragingen op.

Inzicht in incidenten

Het veiligheidsrisico, ofwel de combinatie van kwetsbaarheid, dreiging en potentieel effect, zorgt ervoor dat het onderwerp (informatie)beveiliging van PCS nationaal en internationaal steeds vaker op de agenda van beleidsmakers terecht komt. Terecht vragen zij naar de urgentie en omvang van het probleem. Dat is niet eenvoudig te beantwoorden.
Om inzicht te krijgen in het risico voor de Nederlandse samenleving, hebben TNO en KEMA in opdracht van het ministerie van Economische Zaken in 2006 de PCS-(informatie)beveiligingsproblematiek in kaart gebracht. Treden beveiligingsincidenten op en, zo ja, wat was hun (potentiële) impact? Openbare bronnen laten eigenlijk alleen PCS-(informatie)beveiligingsproblemen zien in de Verenigde Staten en Australië. Openbaarmaking van incidenten komt daar vaak voort uit een wettelijke verplichting tot melden of door openbare rechtbankverslagen.
Niet-openbare bronnen laten echter zien dat PCS-(informatie)-beveiligingsincidenten ook in Europa en in Nederland plaats-vinden. Soms halen ze de pers, vaak vermomd als 'technische storing' of 'problemen met een nog onbekende oorzaak'. De meeste PCS-incidenten blijven binnenshuis. Bij gebrek aan formele rapportagelijnen zijn ze vaak ook niet zichtbaar voor het topmanagement.

Binnen de sectoroverleggen van het Informatieknooppunt Cybercrime delen publieke en private partijen vertrouwelijke informatie over dergelijke incidenten. Desondanks is de aard en omvang van ongewenste PCS-beïnvloeding in Nederland, net als in andere landen, nog onduidelijk. Om landelijk inzicht te krijgen en te leren van incidenten bij anderen, is vanuit het Informatieknooppunt Cybercrime als proef een PCS-incidentenregistratie gestart. GOVCERT.NL heeft de hosting van deze incidentendatabase op zich genomen. Organisaties kunnen vrijwillig deelnemen aan de proef. Alleen deelnemers krijgen volledige toegang tot de informatie.

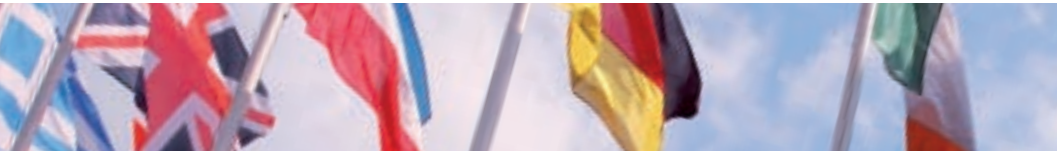
Veilig achter slot en grendel

De Dienst Justitiële Inrichtingen (DJI) zorgt namens de minister van Justitie voor de uitvoer van straffen en vrijheidsbenemende maatregelen. De DJI heeft 19.000 medewerkers in de meer dan honderd vestigingen van gevangenissen en huizen van bewaring, forensische psychiatrische centra en detentie- en uitzetcentra verspreid over heel Nederland. Jaarlijks zijn daar zo'n 80.000 personen voor korte of langere tijd ondergebracht. Dagelijks verwerkt de DJI bovendien een stroom van bezoekers. PCS bewaken en regelen continu de veiligheid van die ruim honderdduizend personen. Gebouwbeheer-, veiligheids- en beveiligingssystemen zorgen ervoor dat DJI-medewerkers veilig kunnen werken en dat gedetineerden veilig en beveiligd ingesloten blijven. Geïntegreerde PCS regelen de brandveiligheid, noodstroomvoorzieningen, airconditioning, camera's, slagbomen en op afstand bedienbare sloten. De Schipholbrand toonde aan hoe belangrijk deze systemen zijn voor het waarborgen van de veiligheid van ingeslotenen en DJI-medewerkers.

MEI 2009 Een storing in het veiligheidssysteem van gevangenis De Geerhorst in Sittard leidt tot commotie. Het lijkt alsof er een persoon op het dak van de gevangenis zit. Een kordon van een helikopter en politiewagens wordt om de gevangenis geplaatst, maar na onderzoek blijkt dat alle gevangenen nog aanwezig zijn.

Internationaal probleem

Internationaal begint het steeds meer door te dringen dat de (informatie)beveiliging van PCS sterk achterloopt bij die van de kantoorautomatisering, en dat er een toenemend risico is. In de Verenigde Staten vinden hierover hoorzittingen plaats in het Congres. De GAO, de Amerikaanse Rekenkamer, stelt kritische rapporten op. Het Department of Homeland Security heeft R&D-programma's opgestart ter verbetering van de PCS-beveiliging. Internationaal wordt ook gewerkt aan het documenteren van Good Practices en de ontwikkeling van nieuwe standaarden voor (informatie)beveiliging van PCS.
De kern hierbij is dat de uitdagingen gezamenlijk aangepakt worden door de overheid (als gebruiker, wetgever voor speciale sectoren en toezichthouder), PCS-gebruikers, fabrikanten, system integrators, leveranciers en kennis-, opleidings- en onderzoeksinstituten.
Nederland heeft de keuze: stilzitten en afwachten tot standaarden en technische verbeteringen uitontwikkeld zijn, of proactief in internationale samenhang de problemen aanpakken. De deelnemende partijen in de Nationale Infrastructuur ter bestrijding van Cybercrime kiezen voor de laatste strategie. Zij ontwikkelen initiatieven op nationaal niveau maar stemmen deze internationaal af. Het NICC neemt actief deel aan de European SCADA and Control Systems Information Exchange (EuroSCSIE) en de Meridian Process Control Security Information Exchange (MPCSIE). Een internationale groep van PCS-afnemers heeft zich verenigd in de werkgroep Plant Security van de WIB (International Instrument Users' Association) om te werken aan het verhogen van het niveau van PCS-security in hun organisaties.



Knop om, licht uit

In Nederland kunnen we op de stroomvoorziening vertrouwen. We realiseren ons niet dat de elektriciteitsvoorziening een complex proces is, opgebouwd uit generatie (kern-, kolen-, gas- en waterkrachtcentrales, windparken, zoncentrales), schakel- en transformatiestations en transmissielijnen. De begrenzing van deze gedistribueerde hoogspanningsmachine loopt van de Noordkaap via Engeland en het Iberisch schiereiland via Marokko, Italië, Griekenland en de Oost-Europese landen tot aan de Baltische staten. Op termijn wordt dit uitgebreid tot aan Vladiwostok en komt er een gesloten ring rond de Middellandse Zee. Het proces werkt, ondanks dat het bestaat uit vele componenten die beheerd worden door een groot aantal organisaties met vaak tegengestelde commerciële belangen.
PCS bewaken, besturen en controleren de elektriciteitsgeneratie. Door de omwentelingssnelheid van de generatoren te regelen, wordt de generatie in balans gebracht met de elektriciteit die wordt afgenomen (load). PCS bewaken ook het voltage en de frequentie in het netwerk, de vermogensoverdracht via transmissielijnen en transformatoren, het reactief vermogen en nog veel meer. Bij te grote afwijkingen wordt automatisch de load van grote bedrijven afgeschakeld. Is dat niet voldoende om het systeem in balans te houden, dan gaat ook bij de burgers het licht uit.

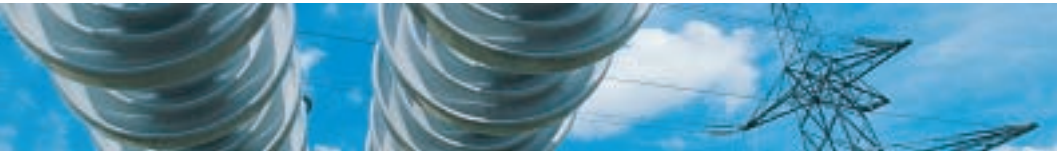
JANUARI 2003 Het PCS-netwerk van de nucleaire centrale Davis-Besse van First Energy in Ohio wordt geïnfecteerd met de SQL Slammer-worm. De worm dringt via een inbelverbinding het PCS-netwerk binnen en infecteert het weergavesysteem voor de beveiligingsparameters. Dit systeem is vijf uur lang niet bruikbaar. Ook de centrale procescomputer is zes uur uit de lucht. De nucleaire centrale is gelukkig in onderhoud.

Fabrikanten en leveranciers

De fabrikanten van PCS en de leveranciers van PCS-diensten (van ontwerp en applicatieontwikkeling tot turnkey-project-ontwikkeling en onderhoud) spelen een grote rol in het beveiligen van PCS. Zij zorgen niet alleen voor beveiligingsmogelijkheden in de programmatuur. Met adviezen en door hun werkwijze kunnen zij de PCS-beveiliging bij hun klanten op een hoger plan tillen. Zij kunnen bijvoorbeeld in hun offertes 'hardening' van het onderliggende besturingssysteem aanbieden. Of vanuit de aanbodzijde proactief afspraken maken over het informatieveilig werken door hun onderhoudspersoneel.

In Amerika hebben gebruikers en aanbieders van PCS gezamenlijk een Cyber Security Procurement Language for Control Systems (CSPL) opgesteld. Deze catalogus met beveiligingseisen voor PCS is een eerste stap in de ontwikkeling van een professionele, gezamenlijke aanpak van (informatie)beveiliging van PCS. In verschillende landen, waaronder Nederland, wordt momenteel gewerkt aan verspreiding en waar nodig verbetering van deze CSPL.

De werkgroep Plant Security van de WIB is bezig met het opstellen van een ideale standaard voor het Process Control Domain. Shell is één van de voortrekkers en heeft zelf al het initiatief genomen tot het opstellen van Process Control Domain Security Requirements for Vendors. Hiermee wordt aansluiting gezocht bij de ontwikkeling van de SP-99 standaard voor PCS. Dat opent de mogelijkheid tot certificering van PCS als het gaat om informatiebeveiliging.



Bagage naar Timbuktu

De bagageafhandelingsystemen op Amsterdam Airport Schiphol verwerken dagelijks tussen de 130.000 en 160.000 stuks bagage. Deze hoogwaardige systemen zorgen ervoor dat uw bagage tegelijk met u aankomt in Timbuktu en voorkomen dat bagage van passagiers op weg naar andere werelddelen in Timbuktu eindigt.
Vanuit de centrale regiekamer houden regisseurs van de luchthaven en KLM het bagageproces vierentwintig uur per dag, zeven dagen per week nauwlettend in de gaten. Dat doen ze via een SCADA IM-pakket (Installation Management) dat specifiek is toegerust op het proces van bagageafhandeling. Als een systeem of parameter afwijkt, kan een regisseur via IM meteen ingrijpen. Een voorbeeld is het vollopen van een sorteerband, het eindpunt in het bagagesysteem waar de bagage van een vlucht wordt uitgesorteerd. Als bagage hier niet op tijd vanaf wordt gehaald, wordt de band te vol. Bij een bepaalde vullingsgraad slaat het IM alarm en grijpt de regisseur in.

APRIL 2008 Een softwarefout in het bagageafhandelingssysteem van de nieuwe Heathrow Terminal 5 leidt tot een wekenlang durende chaos in de kofferverwerking. Meer dan 28.000 koffers worden verkeerd gesorteerd. British Airways laat meer dan vier honderd vluchten vervallen. Met extra vrachtvluchten worden grote stapels koffers naar andere Europese vliegvelden in Europa gebracht om via hun bagagesystemen op de juiste plaats van bestemming te komen. De geschatte schade: 50 miljoen dollar.

De uitdaging

In een Round Table hebben CIO's van grote ondernemingen en overheidsorganisaties samen met de Directeur-generaal Energie en Telecom het PCS-risico besproken. De conclusie: geen enkele partij in het veld is nog in staat geheel zelf de PCS-(informatie)veiligheid te borgen. De PA-omgevingen zijn complex en door een toenemende graad van automatisering in de PCS nemen afhankelijkheden toe. De dreigingen zijn divers en zeer veranderlijk. De grenzen van organisaties worden steeds diffuser, waarbij steeds meer werkzaamheden worden uitbesteed aan turnkey-partijen, outsourcing-partners, PCS-leveranciers en andere ingehuurde partijen. Alleen door een gezamenlijke aanpak van alle betrokkenen kan een voldoende niveau van (informatie)veiligheid van PCS in Nederland bereikt en ook in de toekomst geborgd worden. De deelnemers aan de Round Table hebben zich er aan gecommitteerd om te komen tot een nationale aanpak om de (informatie)beveiliging van PCS in Nederland op het juiste peil te brengen en te houden. Enkele partijen in de Nationale Infrastructuur voor de Bestrijding van Cybercrime hebben deze handschoen opgepakt en hebben het initiatief genomen om te komen tot een 'Nationale Roadmap to secure Process Control Systems'. Daarin wordt uitgewerkt welke fysieke, personele en ICT-maatregelen moeten worden getroffen om PCS veilig te houden. Actieve deelnemers zijn onder meer de WIB, verschillende sectoren uit het Informatieknooppunt Cybercrime, leveranciers, kennisinstellingen, universiteiten, het CIO Platform Nederland en de overheid.

Meer met melk

Bij een gezond glas melk denk je niet automatisch aan PCS. Maar in moderne stallen zijn het niet de boer en de boerin zelf maar PCS die de gezondheid van koeien bewaken, het automatisch melken regelen en ervoor zorgen dat de melk veilig op de juiste temperatuur wordt bewaard.
In de melkfabriek wordt het verwerkingsproces van de rauwe melk tot een brede diversiteit aan melkproducten bestuurd en bewaakt door PCS. Zo wordt de kwaliteit van de verschillende eindproducten geborgd.
Aan het einde van het verwerkingsproces zorgen PCS voor het afvullen van de pakken melk, karnemelk, vla, room, pappen, yoghurt, eventueel gemengd met toeslagstoffen en versneden vruchten. De volgende stap is het automatisch stapelen van de eindproducten op pallets.

2005 Een hacker weet het gebouwbeheersysteem van een computercentrum in een grote Europese bankinstelling binnen te dringen. Hij of zij manipuleert de instellingen van de airconditioning waardoor alle servers door oververhitting uitvallen.

Naar een Nationale Roadmap

De eerste stappen naar een Nationale Roadmap to secure Process Control Systems zijn gezet. De inspirerende voorbeelden uit de Verenigde Staten zijn zeer bruikbaar voor de Nederlandse situatie. Daar heeft men bijvoorbeeld ervaren dat in de afzonderlijke sectorale roadmaps slechts accentverschillen te zien zijn. Daarom is in Nederland gekozen voor een sectoroverstijgende aanpak: één Nationale Roadmap.
De menselijke factor vormt daarbij een belangrijke rol. In de Roadmap wordt gestreefd naar een balans tussen de organisatorische en technische aspecten enerzijds en de menselijke gedragslijn anderzijds. De beveiligingsmaatregelen kunnen zowel fysieke, personele, organisatorische als ook ICT-maatregelen zijn.
De aanzet voor de Roadmap werd gegeven tijdens het derde Proces Control Security Event 'Control IT!' van het NICC, in een workshop waarbij alle partijen aanwezig waren. De visie is besproken, de doelstellingen zijn bepaald.
Uitgangspunt van de Roadmap is een gezamenlijke visie die voorlopig als volgt is gedefinieerd:

'Binnen tien jaar zijn beschermingslagen van PCS die kritische processen aansturen, ontworpen en geïmplementeerd en worden ze onderhouden. Dit in overeenstemming met het geïdentificeerde risico. Doelstelling daarbij is om geen verlies van kritische functies te hebben tijdens en na een cyber-incident.'

De Roadmap focust op veilig PCS-gebruik tijdens de gehele PCS-levenscyclus. Fabrikanten, leveranciers, dienstverleners, overheid, opleidingen, kennisinstellingen en internationale dwarsverbanden ondersteunen dit. In nauwe samenwerking hebben deze partijen de visie uitgewerkt tot de volgende doelstellingen.

1. Beveiliging zit bij de mensen in de genen.
2. Meten en bepalen van de stand en het niveau van security.
3. Ontwikkelen en integreren van beschermende maatregelen.
4. Detecteren van 'intrusion' en implementeren van responsstrategieën.
5. Permanente aandacht voor verbetering van de beveiliging.
6. 'Secure-by-design'.

Deze doelstellingen worden in de Roadmap op strategisch en tactisch niveau actiegericht uitgewerkt in mijlpalen op korte termijn, quick-wins (0-1 jaar), middellange termijn (tot 3 jaar) en lange termijn (tot 10 jaar). Taken, rollen en verantwoordelijkheden worden SMART (specifiek, meetbaar, acceptabel, realistisch, tijdgebonden) belegd.

Cybergestuurd kraken

In onze havens en op andere plaatsen in Nederland staan grote petrochemische complexen met krakers en vele kilometers transportleidingen. Krakers verwerken bij hoge temperatuur en druk grondstoffen als nafta, butaan, etheen en andere olieproducten. Lange koolstofketens worden gebroken, zodat lichtere fracties na destillatie uit de kraker stromen: (poly)ethyleen en andere aromaten die in nabije fabrieken gebruikt worden voor de productie van complexe koolstofchemische producten.
PCS zijn de oren en ogen van de procesoperators in de (petro)-chemische industrie. Veilig werken staat voorop. Vanuit centrale controlekamers worden alle procesparameters bewaakt en zo nodig bijgeregeld, zodat de tussen- en eindproducten van de juiste kwaliteit zijn. Het proces is fail-safe ontworpen. Dat voorkomt echter niet dat er soms grote vlammen boven de affakkelkolom verschijnen en onaangename geuren ontsnappen als de controle over het proces uit de hand loopt. Onbevoegde beïnvloeding van de bestuurde processen moet te allen tijde voorkomen worden. Toch is bekend dat hackers zijn doorgedrongen tot de PCS die dergelijke petrochemische installaties besturen.

MEI 2008 Na zijn ontslag manipuleert Mario Azar, een PCS-software manager bij Pacific Energy Resources, van 8 mei tot 29 juni 2008 de instellingen van het lekdetectiesysteem van oliepijpleidingen tussen olieplatformen en de kust.

In de loop der jaren hebben bedrijven en overheid al de nodige activiteiten uitgevoerd en maatregelen genomen om de veiligheid van PCS op een hoger plan te tillen. Deze worden zoveel mogelijk geïntegreerd in de Roadmap. Denk hierbij aan bijvoorbeeld de organisatie van Red/Blue team trainingen (in samenwerking met het Amerikaanse Department of Homeland Security), internationale samenwerking, het invoeren en aanpassen van de Cyber Security Procurement Language, het opstellen van 'Process Control Domain Security Requirements for Vendors', ontwikkeling van standaarden, de PCS-incidentenregistratie en (inter)nationale Process Control Security Events.

Helder afvalwater

Gemeenten en Waterschappen zijn verantwoordelijk voor het transporteren en zuiveren van ons afvalwater. Daar worden ruim 100.000 kilometer riolering en 368 rioolwaterzuiverings-installaties voor gebruikt. De zuiveringscapaciteit van één enkele installatie kan oplopen tot één miljoen inwoners. Dit continue proces is in hoge mate geautomatiseerd. Door steeds complexere processtappen en regelingen, bediening op afstand en outsourcing wordt de afhankelijkheid van de betrouwbaarheid van PCS alleen maar groter. Als de afval-waterketen hapert, heeft dat ernstige gevolgen voor het milieu en de volksgezondheid.

NOVEMBER 2007

In Nokia, Finland wordt een verbinding tussen een afvalwaterleiding en een drinkwaterleiding opengezet om de afvalwaterleiding door te spoelen. Door drukverschil komt afvalwater terecht in het drinkwater (backflow). 12.500 inwoners krijgen last van maag- en darmklachten. Honderden mensen worden in het ziekenhuis opgenomen, drie patiënten overlijden als gevolg van het besmette drinkwater. Het weer veilig krijgen van het drinkwatersysteem duurt enkele maanden.

Samen aan de bak

De voorbeelden in deze publicatie tonen glashelder aan waarom het borgen van de beschikbaarheid en betrouwbaarheid van vele vitale en essentiële producten en diensten van belang is. Niet alleen voor onze samenleving als geheel, maar ook voor de individuele burgers. Tevens wordt aangetoond dat geen enkele partij deze uitdaging alleen kan oppakken en tot een succesvol einde kan brengen. Samenwerking is nodig!

Zicht op bruggen

Rijkswaterstaat beheert rijkswegen en rijksvaarwegen. Steeds meer bruggen, sluizen en tunnels worden met PCS op afstand bediend. Problemen in en uitval van die bediening leiden tot grote files, stremming, veel oponthoud, onveilige situaties, overlast elders en soms schade voor het milieu. Wat te denken als bijvoorbeeld een brug onverwacht in de spits openstaat, zoals gebeurde bij de brug in de A4 bij Leiderdorp?
Weggebruikers vertonen ook onverwacht gedrag: ze negeren een stoplicht of slagboom. Als dat mis gaat en er auto's van de brug vallen, is het voorpaginanieuws. Het veilig openen en sluiten van een brug met zicht op de actuele situatie is dus cruciaal voor Rijkswaterstaat. PCS helpen bij de doorstroming en veiligheid.

DECEMBER 2006

Sinds de opening in december 2006 is de Dublin Port-tunnel ruim twintig keer urenlang gesloten geweest ten gevolge van SCADA-storingen. De tunnel zorgt ervoor dat vrachtverkeer tussen de haven en de omliggende snelwegen het centrum en woonwijken kan vermijden. Uitval van de tunnel resulteert iedere keer in een grote verkeerschaos en veel milieuoverlast.

Bijlagen

Standaarden en Good Practices

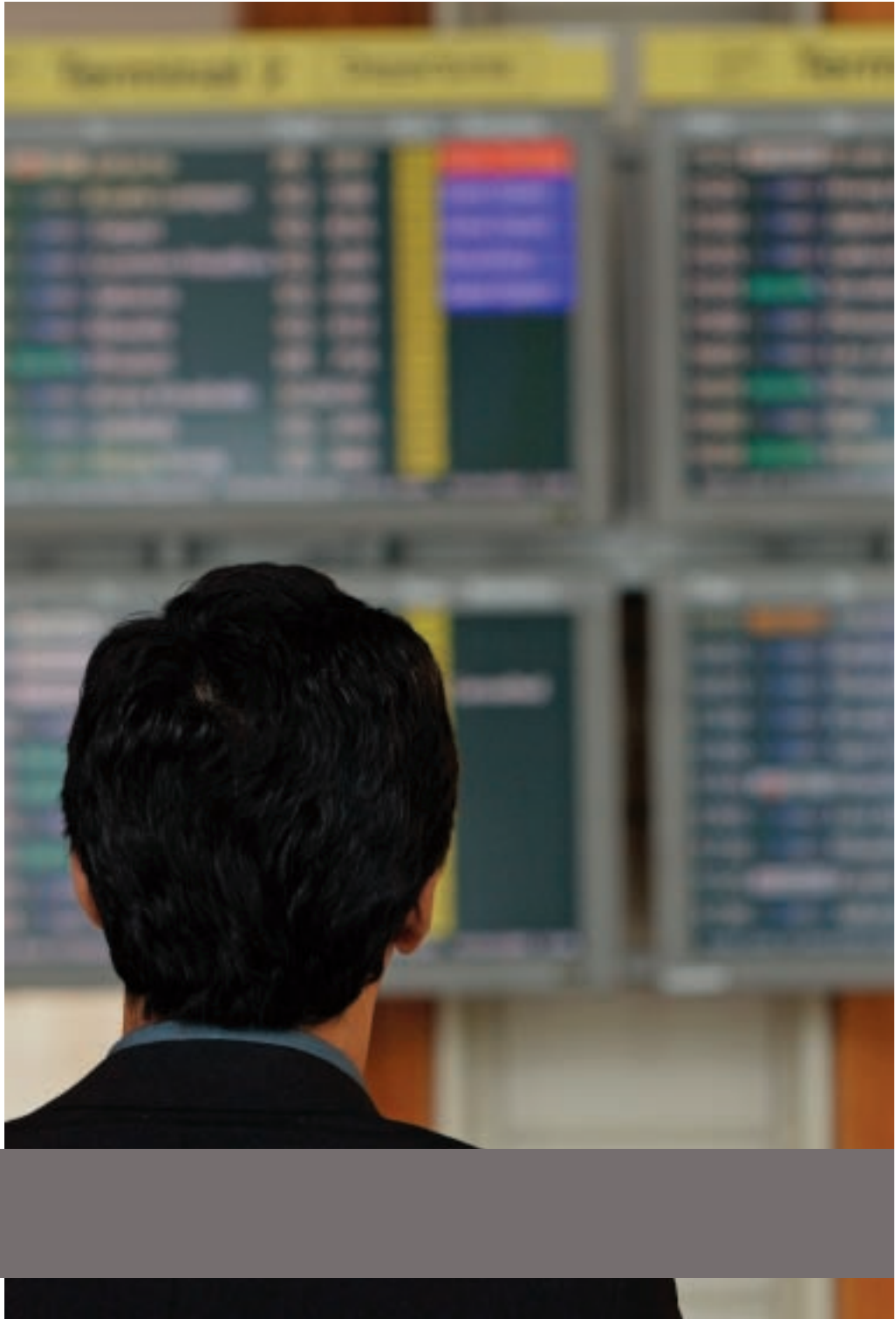
- SCADA Good Practices for the Dutch Drinking Water sector, TNO DV 2008 C096, March 2008.
- Een verzameling SCADA Good Practices, waaronder een firewall guide, door het Centre for the Protection of National Infrastructure (CPNI), http://www.cpni.gov.uk/Products/guidelines.aspx
- 21 steps to improve the security of SCADA networks, http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf
- ISO/IEC 27001:2005, Information Technology – Security Techniques - Information Security Management Systems – requirements.
- ISO/IEC 27002:2005, Information Technology – Code of Practice for Information Security Management.
- NIST Special Publication SP 800-53 - Appendix I: security controls for Industrial Control Systems.
- NIST Special Publication SP 800-82 (draft) Guide to Industrial Control Systems (ICS) Security.
- Cyber Security Procurement Language for Control Systems (INL).
- Establishing an Industrial Automation and Control Systems Security Program, ANSI/ISA-99.02.01-2009 (draft IEC 62443-2-1).
- Operating an Industrial Automation and Control Systems Security Program, ANSI/ISA-99.02.02-2009 (draft IEC 62443-3-1).

Achtergrondinformatie

- H.A.M. Luiijf en R. Lassche, SCADA (on)veiligheid, een rol voor de overheid?, TNO/KEMA rapport, april 2006.
- Control Systems Security Program, DHS and US-CERT, http://www.us-cert.gov/control_systems met onder andere de Cyber Security Procurement Language for Control Systems.
- US Guide to inspections of computerised systems in the food processing industry, USFDA, http://www.fda.gov/ora/inspect_ref/igs/foodcomp.html

Onderzoek en ontwikkeling

- European Workshop on Industrial Computer Systems Reliability, Safety and Security, http://www.ewics.org
- Crutial – Critical Utility Infrastructure Resilience, http://crutial.cesiricerca.it
- IRRIIS – Integrated Risk Reduction of Information-based Infrastructure Systems, http://www.irriis.org
- GRID – Cyber kwetsbaarheid elektriciteitsnetwerken, http://grid.jrc.it



Programma

Annemarie Zielstra (ICTU)
programmamanager

Auke Huistra
projectleider Informatieknooppunt

Eric Luiijf
expertpool NICC (SCADA/PCS)

Het programma NICC is een ICTU-programma. De opdrachtgever is het ministerie van Economische Zaken. Het motto van ICTU is: overheden helpen beter te presteren met ICT. ICTU bundelt kennis en kunde op het gebied van ICT en overheid. Voor en met overheidsorganisaties voert ICTU diverse projecten uit. Zo wordt beleid omgezet in concrete projecten voor de overheid. Meer informatie? Kijk op www.ictu.nl.

Colofon

Uitgave
NICC
Eric Luiijf (expertpool NICC)

Redactie
Tekstbureau De Nieuwe Koekoek, Utrecht

Met tekstbijdragen van
Brabant Water / Gasunie / Luchthaven Schiphol /
Rijkswaterstaat / Shell / Waternet / Witteveen & Bos

Met medwerking van
Paul Bloemen, Gasunie / Jules Vos, Shell /
Martin Visser, Waternet

Ontwerp
OSAGE / communicatie en ontwerp, Utrecht

Fotografie
Marcel Rozenberg, Schiedam

Druk
OBT / TDS printmaildata, Schiedam

november 2009

NICC | ICTU

Bezoekadres
Wilhelmina van Pruisenweg 104
2595 AN Den Haag

Postadres
Postbus 84011
2508 AA Den Haag

T 070 888 79 46
nicc@ictu.nl

www.samentegencybercrime.nl

samen tegen cybercrime
NICC