Samen tegen cybercrime, ee

Opsporing en vervolging van cybercrime is nodig, maar niet dé oplossing om veilig digitaal te kunnen werken. Alleen als overheid en bedrijfsleven de handen ineenslaan en informatie over dreigingen uitwisselen, wordt het mogelijk cybercriminelen een stap voor te blijven. In Nederland hebben overheid en bedrijfsleven daarom in 2006 gezamenlijk besloten tot de opzet van een Nationale Infrastructuur ter bestrijding van Cybercrime (NICC). Deze infrastructuur ontstaat alleen als partijen met elkaar samenwerken. Onder het motto 'learning by doing' zijn in 2006 de eerste stappen gezet op weg naar een aanpak tegen cybercrime. Maar kan de aanpak ook succesvol zijn als het gaat om procescontrolesystemen?

Management-summary

De Nationale Infrastructuur ter bestrijding van Cybercrime (NICC) faciliteert de verschillende (vitale) sectoren om de informatiebeveiliging van essentiële functies in de samenleving op orde te krijgen en te houden. Deze aanpak blijkt succesvol voor diverse sectoren, maar diezelfde sectoren constateren ook dat er een blinde vlek is als het gaat om SCADA en andere procescontrolesystemen. Deze systemen besturen en monitoren de fysieke processen in onze samenleving. Dat loopt uiteen van het regelen van eenvoudige gebouwbeheersystemen en automatische vulinstallaties voor melkpakken tot complexe besturingen van onze vitale infrastructuren als gas, elektriciteit, drinkwater, metro, treinen, tunnels en havensystemen. Op 21 mei brengt het NICC vertegenwoordigers van al deze partijen samen in het Process Control Security Event. Tijdens dit evenement wordt onder de titel 'Are you aware?' een aftrap gegeven voor een gezamenlijke aanpak. Dit artikel gaat in op de aanpak van het NICC. Hoe wordt er samengewerkt met private partijen en verschillende kennisfuncties van de overheid? En kan de succesvolle aanpak van de informatiebeveiligingsproblematiek ook uitkomst bieden voor procescontrolesystemen?

SCADA (Supervisory Control and Data Acquisition) en andere procescontrolesystemen *besturen, regelen en monitoren* fysieke processen. Denk hierbij aan gebouwbeheer, het automatisch vullen van melkpakken, het regelen van gas- en elektriciteitstransportnetwerken, het regelen van de metro- en treinenloop en veiligheidssystemen van tunnels. Deze systemen zijn erg kwetsbaar voor allerlei vormen van cybercriminaliteit. Vooral omdat een deel van deze systemen steeds vaker via internet worden bediend. De beveiliging van deze systemen laat in de praktijk om een aantal redenen te wensen over.

De nationale infrastructuur is een krachtenbundeling van alle functies op het gebied van de bestrijding van cybercrime. De inventarisatie van de publieke en particuliere organisaties die deze functies invullen, is in volle gang, zie ook de NICC website (*1). Het NICC doet echter meer dan alleen inventariseren. Het signaleert ook overlappingen en ondersteunt activiteiten die leiden tot het opvullen van witte vlekken. Eén van die witte vlekken blijkt te liggen binnen het Informatieknooppunt Cybercrime: de aandacht voor SCADA dan wel Process Control Security.

Cybercrime is bij uitstek een internationaal verschijnsel. Cybercriminelen opereren vaak vanuit landen waar ze zo min mogelijk last hebben van wetgeving en handhaving. Ze brengen echter schade toe in tientallen andere landen over de hele wereld. Internationale uitwisseling en samenwerking vormen de enige manier om cybercrime effectief *te bestrijden*. Nationale programma's zoals de nationale infrastructuur tegen cybercriminaliteit zijn daarvoor de basis. Het is een instrument om landelijke *regie op de functies te krijgen*. De afzonderlijke functiebeklederds, zowel die uit de private sectoren, als die van de verschillende overheidsdiensten, wisselen informatie uit met hun eigen internationale contacten.

Informatieknooppunt Het Informatieknooppunt Cybercrime is het kloppende hart van de nationale infrastructuur. Hierin wisselen overheid en bedrijfsleven gevoelige informatie uit. De informatie-uitwisseling vindt binnen één sector of sectoroverstijgend plaats. Het informatieknooppunt is opgebouwd volgens het 'bloemblaadjesmodel'. De kern van de bloem bestaat uit kennispartijen van de overheid op het gebied van cybercriminaliteit: AIVD, KLPD, GOVCERT en NICC. Daar omheen zijn overlegorganen van de vitale sectoren

aanpak die werkt

gerangschikt als bloemblaadjes. Binnen elk 'bloemblaadje' wordt informatie gedeeld, bijvoorbeeld over specifieke kwetsbaarheden, incidenten en oplossingen. Via de kern van de bloem kan essentiële informatie worden doorgegeven van het ene bloemblaadje naar het andere, en eventueel aan andere partijen. De sector (het bloemblaadje) die gevoelige informatie aanlevert, bepaalt zelf wat daarvan aan de overige vitale sectoren of andere partijen mag worden bekendgemaakt. Uiteraard onder strikte voorwaarden, en geanonimiseerd. De sector kan zelfs gevoelige onderwerpen bespreken zonder de aanwezigheid van overheidsfunctionarissen.

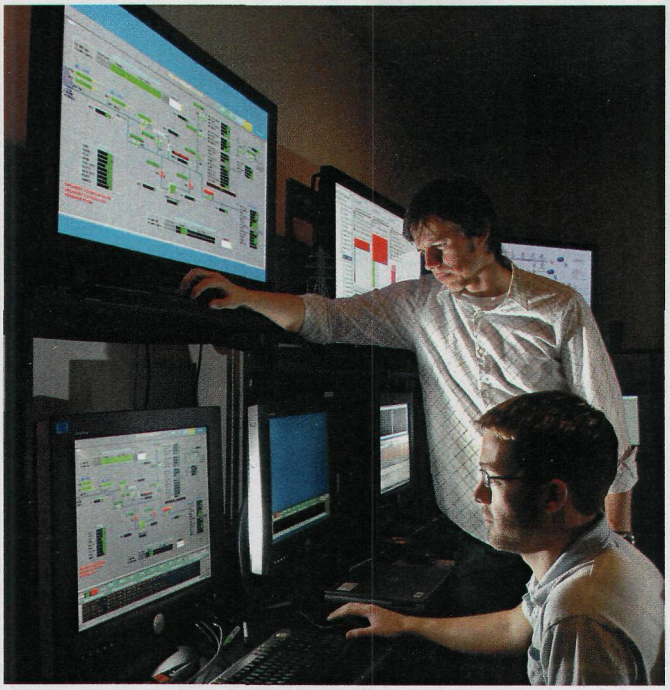
Het Informatieknooppunt groeit gestaag. Verschillende sectoren zijn al een tijd bij het knooppunt aangesloten. Daar heeft de informatie-uitwisseling zijn waarde bewezen, is onderling vertrouwen opgebouwd en worden zelfstandig nieuwe initiatieven ontplooid. Andere sectoren zijn net aangesloten of zijn bezig met de voorbereidingen daarvoor. In oktober 2006 sloot de bancaire sector zich als eerste aan op het Informatieknooppunt. In april 2007 volgden de waterleidingbedrijven. In september sloot de energiesector zich aan en ook Schiphol was eind vorig jaar volledig operationeel. Het spoor, multinationals, de havensector, de telecommunicatiesector zijn begin 2008 gestart met de eerste overleggen.

Als er thema's zijn die van een zodanig groot belang zijn voor meer sectoren, is het ook mogelijk om samenwerking over de sectoren heen op dat specifieke thema te organiseren. In dat geval wordt er een specifiek bloemblaadje voor dat thema ingericht.

SCADA Vrijwel alle eerder genoemde sectoren hebben de behoefte geuit aan het uitwisselen van kennis en informatie op het gebied van informatiebeveiliging voor SCADA en procesautomatisering. Daarom is SCADA het eerste thematische overleg in oprichting. Deelnemers uit bijna alle (vitale) sectoren bespreken daar de veiligheid van SCADA en procesautomatisering. Dit omvat het gezamenlijk verkrijgen van inzicht in dreigingen, risicofactoren en kwetsbaarheden en het delen van Good Practices. Een echt bloemblaadje kan dat overleg nooit worden. De groep geïnteresseerden is immers veel groter dan de beperkte hoeveelheid partijen in één sector (bijvoorbeeld banken). Daarom kiest het NICC voor een aanpak waarbij alle betrokken tweemaal per jaar op een besloten congres worden samengebracht. Op 21 mei staat het eerste evenement op het programma.

In de kern gaat het om hoogwaardige kennisuitwisseling. Op die manier ontstaat een gedeeld nationaal beeld waarmee iedereen zijn voordeel kan doen. Daarnaast zorgt het NICC er ook voor dat er informatie wordt uitgewisseld met overheidsorganisaties en SCADA-grootgebruikers uit andere Europese landen. Op SCADA gebied gebeurt dit door het NICC onder andere in het European SCADA and Control Systems Information Exchange (EuroSCSIE) overleg. Samen met het Verenigd Koninkrijk (CPNI) en Zweden (SEMA) is Nederland één van de grondleggers en voortrekkers van dit Europese overleg. GOVCERT op zijn beurt wisselt actuele dreigings- en kwetsbaarheedeninformatie uit binnen de vertrouwde kringen van de internationale computer emergency response teams en onderzoekt de actuele mate van dreiging voor de SCADA-systemen.

Een basis voor de aanpak van de SCADA-beveiligingsproblematiek in NICC-verband is gelegd in de drinkwatersector. In 2007 heeft een onderzoek plaatsgevonden naar de mate van informatiebeveiliging van SCADA en procescontrolesystemen binnen die sector. Om te komen tot een brede, evenwichtige aanpak van de SCADA-beveiliging in de gehele sector, is voor ▸



de drinkwatersector een verzameling van 39 Good Practices voor het (top)management en het technisch systeem- en beveiligingsmanagement opgesteld (*2). Deze Good Practices worden inmiddels ook internationaal opgepakt. In navolging hierop is begin 2008 een dergelijk onderzoek in de energiesector gestart.

Agenda Op basis van het eerdere TNO-KEMA rapport (*3), internationale signalen en de voorbeeldaanpak door de drinkwatersector, heeft de Nederlandse overheid samen met het bedrijfsleven en betrokken organisaties besloten de SCADA-beveiligingsproblematiek breder op te pakken en onder de aandacht te brengen. Op 21 mei zal tijdens het 'Process Control Security Event', als onderdeel van 'Het Instrument 2008', een eerste stap worden gezet. De genodigden zijn afkomstig van verschillende managementniveaus: van board room tot aan de automatiseringsmanager moet immers aandacht worden besteed aan de SCADA-problematiek. Dit event wordt samen met het CIO Platform Nederland, TU Delft, het WIB en de Federatie voor technologiebranches (FHI) georganiseerd.
De titel van het event 'Are you aware?' geeft aan dat een goede aanpak alleen mogelijk is als iedereen zich bewust is van de gevaren. De nadruk zal op 21 mei daarom liggen op kennisdeling op inhoud over het onderwerp process control security en het uitbouwen van het kennisnetwerk. Het gewenste resultaat is een structureel thematisch bovensectoraal overleg op het gebied van process control security. Daarnaast moet het event ervoor zorgen dat het onderwerp blijvend op de bestuurlijke en politieke agenda terechtkomt.

Inbreng Het Process Control Security Event wordt ingevuld met sterke inbreng van de sectoren. Christian Gresser zal het probleem met een live-hack concreet maken. Er wordt dus niet abstract gedebateerd over een mogelijk probleem, maar zichtbaar en concreet naar de cybercrimedreiging gekeken. Eric Byres uit de Verenigde Staten zal ingaan op de verborgen gebreken in proces controlesystemen. Hij zal voorbeelden van praktijkincidenten geven. In interactieve sessies wordt thematisch doorgesproken over de mogelijke knelpunten. Daarbij wordt naar alle mogelijke aspecten gekeken. Van soft- en hardware naar organisatorische problemen. De knelpunten vormen het aangrijpingspunt voor uit te zetten acties. In kleiner verband zal daar na het event over doorgepraat worden.
In november krijgt deze dag een vervolg in de vorm van een tweede event. Dezelfde groep wordt dan weer uitgenodigd en bespreekt de resultaten van de uitgezette acties. Op die manier moet het eerste thematische bloemblaadje van het Informatieknooppunt Cybercrime zijn beslag krijgen. Bij alle andere bloemblaadjes is gebleken dat het succes moet groeien. Eerst moet er onderling vertrouwen zijn en pas daarna wordt er waardevolle informatie uitgewisseld. Dat zal bij dit onderwerp op dezelfde wijze gaan gebeuren. Overheid en bedrijfsleven investeren in deze samenwerking via het NICC. Alles vanuit de overtuiging dat een sluitende aanpak alleen mogelijk is als alle relevante partijen goed met elkaar samenwerken. Op die manier zal 'Samen tegen cybercrime' ook tot succes leiden als het gaat om de beveiliging van procescontrolesystemen.

Samenwerking Het NICC faciliteert samenwerking. Het luistert naar de markt en handelt vraaggestuurd. Het totale programma draait in nauwe samenwerking met partijen die concrete en werkbare initiatieven aandragen. Daarom is het NICC dynamisch en flexibel. Wat gisteren noodzakelijk was is morgen achterhaald. Geen lange aanlooptijden en ingewikkelde structuren, niet eindeloos overleggen. Gewoon beginnen, aldoende leren en waar nodig bijstellen. Tot nu toe heeft dat goed gewerkt. Het Process Control Security Event op 21 mei is hopelijk de start van een uitbreiding van dat succes naar SCADA- en procescontroleomgevingen.

■ Annemarie Zielstra, Manou Ali en Eric Luiijf
Redactie@beveiliging.nl

Referenties
1) Website: www.samentegencybercrime.nl
2) Eric Luiijf MSc, SCADA Security Good Practices for the Drinking Water Sector, report TNO DV 2008-C096, March 2008.
3) Ir. H.A.M. Luiijf en Ir. R. Lassche, SCADA (on)veiligheid: een rol voor de overheid?, TNO-KEMA rapport, april 2006.