REGISTRATIESYSTEEM VOOR CCI-MATERIAAL

De heer ing. Leo Keijzer, CDC / IVENT

De heer ing. Leo Keijzer is projectleider en werkzaam bij CDC / IVENT (Informatie Voorziening En Technologie). Een zeer kritische rapport van de Algemene Rekenkamer over het beheer van CCI-materiaal binnen Defensie heeft de ontwikkeling van een CCI-beheertool in een stroomversnelling gebracht. De heer Keijzer is belast met de Defensiebrede implementatie van het *Controlled Cryptographic Item Registratie Systeem* (CCIRS). Dit CCIRS is in zijn huidige vorm nog geen *Electronic Key Management System* (EKMS). In dit artikel wordt de weerbarstige implementatie van een CCIRS binnen Defensie geschetst.

UITROL CCIRS

De 'Uitrol CCIRS' is in juli 2008 gestart met het doel de registratie van CCI-middelen onder te brengen in een geautomatiseerd systeem en de gegevens op de defensienetwerken Mulan (kantooromgeving) en TITAAN *(out of area)* beschikbaar te stellen. Dominante randvoorwaarden bij de 'uitrol CIIRS' zijn beheer door IVENT en beschikbaarheid op de departementaal vertrouwelijke werkplekken Mulan en TITAAN Zwart.

PAPIEREN REGISTRATIE

Defensie gebruikt voor de uitvoering van haar taken ICT-middelen die van crypto worden voorzien of gelden als een CCI. Deze cryptomiddelen dienen conform de aanwijzingen van het Nationaal Bureau Verbindingsbeveiliging (VBV-reeks) en NAVO (AMSG-reeks) op een veilige, gecontroleerde wijze te worden gedistribueerd en beheerd. Het betreft het aanmaken en uitgeven van cryptosleutels en codeboeken, het werken met en beheren van CCI-artikelen en het uitgeven van documenten met een crypto of CCI-merking. Tot de invoer van CCIRS was het gehele proces nagenoeg handmatig en op basis van papier opgezet.

EINDE VAN HET ROC

De oude methode van werken hield in dat van elke verplaatsing van CCI-apparatuur, van de ene cryptobeheerder naar de andere, een papieren *Report Of Crypto* (ROC) moest worden gemaakt. Onder een ROC stonden twee handtekeningen: een van de zender en een van de ontvanger. Deze papieren moesten bewaard worden en kopieën verzonden naar de DEFDA, die op haar beurt ook weer moest archiveren.
CCIRS maakt het produceren van papieren ROC's overbodig. De applicatie doet dit digitaal. De gegevens zijn direct zichtbaar voor de verzender, ontvanger en DEFDA, waardoor ook sneller inzicht ontstaat in welke bewegingen van CCI-middelen er zijn. Er ontstaat een digitaal archief waarin makkelijk na te gaan is welke weg een bepaald CCI-middel door Defensie heeft afgelegd.

DE TOEKOMST: 2015

Oktober 2015, de migratie van data uit de tijdelijke registratiesystemen voor gevoelig materieel naar het ERP-systeem is zonder problemen verlopen. Het begrip ERP staat voor *Enterprise Resource Planning*. De hoge kwaliteit van de te verwerken data heeft een positieve invloed gehad op het verloop van deze migratie. Het succes van de migratie is het gevolg van jaren van grote inspanning door elke gebruiker van de tijdelijke CCIRS systemen. Een periode waarin is benadrukt dat discipline in het bijhouden van registraties van groot belang is, heeft zijn vruchten afgeworpen. Men is er altijd van op de hoogte welke apparatuur zich waar bevindt. Vooral de crypto-organisatie profiteert hiervan. Uitwisseling van apparatuur tussen de verschillende eenheden, dwars door Defensie heen, verloopt soepel.

Jaarlijkse tellingen vergen slechts een beperkte inspanning en de tellingen worden ook daadwerkelijk uitgevoerd. Controles op de tellingen worden *on-line* verwerkt door de centrale organisatie DEFDA (Defensie Distributie Autoriteit voor Crypto).
Het spreekt vanzelf dat de controles door de ADD (Audit Dienst Defensie) en de Algemene Rekenkamer positieve rapporten opleveren. De crypto-organisatie is een voorbeeld voor NATO-partners, want juist bij *out of area* optreden bewijst de goede beheersing van de cryptoregistratie zijn dienst. Dit merken de samenwerkende partners doordat hun vragen snel en adequaat beantwoord worden.

In de Tweede Kamer maakt men zich geen zorgen meer over de kwaliteit van het beheer van gevoelig materieel. Tot zover een schets van de toekomst.

PROCEDURES EN ORGANISATIE

Het navolgen van de VBV en AMSG aanwijzingen kan slechts wanneer de samenwerking op het gebied van cryptobeheer adequaat is ingericht en bovendien goed verloopt. Er zijn diverse organisaties en medewerkers betrokken bij het cryptobeheerproces. Alle handelingen moeten op elkaar zijn afgestemd. Dit is vastgelegd in procedures, maar met procedures alleen komt men er niet. In de hoofden van de mensen moet het ook goed zitten. Men moet altijd blijven meedenken en handelen op basis van procedures, maar ook op basis van het eigen gezonde 'boerenverstand'. Procedures zijn er tenslotte alleen maar om te kunnen voldoen aan regelgeving. Deze regelgeving is ontworpen met een bepaalde filosofie. Gebaseerd op het feit in de crypto-organisatie wordt gewerkt met uiterst gevoelig materiaal en dat dit materiaal niet in verkeerde handen mag vallen. Dit materiaal wordt voornamelijk gebruikt door militairen in het veld, geen specialisten op het gebied van cryptoapparatuur. De regelgeving moet ook voor hen duidelijk zijn en erop gericht dat men in het veld snel moet kunnen handelen zonder eerst omslachtige procedures uit te voeren.

Samenwerking geldt niet alleen binnen de crypto-organisatie, maar loopt door heel Defensie heen. Van de operationele militair tot de cryptobeheerder, de *comsec officer*, tot de Beveiligingsautoriteit (BA).
Hier is in het kort geschetst in welke organisatorische omgeving de cryptobeheerders moeten opereren. Dit is de achtergrond voor het project dat het registreren van gevoelig materieel, in het bijzonder CCI-middelen, mogelijk moet maken.

FOCUS AFGHANISTAN

Het CLAS is sinds 1 februari 2006 verantwoordelijk voor het beheer van de nationale cryptomiddelen in Afghanistan. CLAS is aan zet om daar orde op zaken te stellen en het CLAS heeft daartoe de 'Taskforce Cryptobeheer Afghanistan' geformeerd. In uitzendgebieden is het bijhouden van waar de cryptomiddelen zich bevinden een extra weerbarstige klus. Er is tijdsdruk en de operatie heeft voorrang. Dit heeft er in het verleden toe geleid dat apparatuur is verstrekt en uitgeleend, zonder goed te administreren wie wat heeft overgedragen. Met als gevolg dat niet altijd bekend is welke cryptoapparatuur zich waar bevindt. En dat is in feite een onveilige situatie. Orde op zaken stellen is één, maar orde houden is mogelijk nog een lastigere taak. Discipline is een van de belangrijkste aspecten van beheer.
Naast de discipline moet de infrastructuur goed geregeld zijn. Dit is gelukt, echter met een bètaversie van CCIRS, die nog niet volledig in beheer was bij IVENT. CCIRS is een jaar lang 'in de lucht gehouden' door de gebruikersorganisatie zelf. Door gemotiveerd personeel is dit ook inderdaad adequaat uitgevoerd.
De 'Taskforce Cryptobeheer Afghanistan' heeft in januari 2009 de *out of area* inventarisatie in Afghanistan afgerond. Aansluitend is 2009 benut om CCIRS te vullen met de data van de CCI-apparatuur van alle OPCO's, de Bestuursstaf, de DMO en het CDC. Dat is voor een groot deel afgerond.

OPLEIDINGEN

De gebruikers en beheerders van de applicatie zijn opgeleid door OTCMan / School Verbindingsdienst in Ede. De opleiding cryptobeheerder is aangepast, zodat de nieuwe cryptobeheerders leren werken met CCIRS.
Daarnaast is de applicatie CCIRS door IVENT herschreven. Het CLAS had zelf de applicatie ontwikkeld en overgedragen aan IVENT. IVENT heeft het beheer van CCIRS overgenomen en CCIRS geschikt gemaakt voor gebruik op Mulan (kantooromgeving) en TITAAN Zwart *(out of area)*.
In 2010 wordt een nieuwe release van CCIRS beschikbaar gesteld. Er komt een instructiemodule via On-Demand. Dit is een interactieve manier om te leren werken met een applicatie. Deze manier is al te zien in bijvoorbeeld PeopleSoft.

BARCODESCANNERS

Een bijkomend voordeel van het gebruik van digitale opslag van gegevens is, dat gewerkt kan gaan worden met barcodescanners. CCI-apparaten hoeven straks niet meer gedemonteerd te worden uit de plek waar ze bevestigd zijn. Een barcodesticker met daarop de essentiële gegevens kan met een barcodescanner gelezen worden en de data zijn daarna snel zichtbaar in CCIRS. Het tellen en overdragen van apparatuur wordt hiermee vergemakkelijkt.
In 2010 worden ook de barcodescanners ingezet. Dit vereist een behoorlijke operatie aan de kant van de crypto-organisatie. Alle CCI-middelen moeten worden voorzien van een barcodesticker en daarna direct gescand. Ook de applicatie CCIRS zelf wordt geschikt gemaakt om te kunnen werken met barcodescanners.

TOT BESLUIT

Het project CCIRS is in de kern eenvoudig: het uitrollen van een *server-client applicatie* en het 'vullen' van deze applicatie met productgegevens.
Toch duurt dit project straks ruim twee jaar, terwijl in eerste instantie elf maanden voldoende leek te zijn. De doorlooptijd is ruim twee keer zo lang gebleken. Met uitloop op de initiële planning wordt bij de start van een project veelal onvoldoende rekening gehouden. De projectplanning is in de regel te optimistisch.
In een grote organisatie als Defensie zijn de taken zo verspreid belegd, dat men vaak geen idee heeft wat het belang is van de eindgebruiker. Zeker als deze taken ook nog eens voor een deel belegd zijn bij een dienstenorganisatie zoals het CDC en dus op afstand staan van de operationele praktijk. Ook al wordt binnen het CDC gestreefd naar het verkleinen van de afstand tot de klant, de onderliggende processen zijn hier niet primair op ingericht.

Het managen van een project als dit lijkt dus eenvoudig, er spelen echter zoveel partijen mee, dat juist dit aspect een aanvankelijk eenvoudig project toch uiteindelijk een ingewikkeld project maakt. Elke partij heeft eigen regels en procedures, en die procedures zijn niet altijd op elkaar afgestemd.

Als projectmanager ben ik dan ook elke keer weer blij wanneer vanuit de SG wordt aangekondigd dat we minder bureaucratie moeten nastreven.

VAN CCIRS NAAR EKMS

Aanleiding

In de komende jaren zijn onder invloed van de technische ontwikkelingen een aantal veranderingen te verwachten. Cryptoproducerende landen leveren hun cryptosleutelmateriaal voor nieuwe systemen nagenoeg alleen nog maar digitaal aan en papieren sleutels verdwijnen versneld. Daarnaast zorgen de technische ontwikkelingen er voor dat de hoeveelheid ICT-middelen die zullen werken met sleutelmateriaal exponentieel toeneemt.

Huidige situatie

Crypto bestaat voor een groot gedeelte nog uit papieren ponsbandjes. Deze worden handmatig door de cryptobeheerders verwerkt, met een grote papierstroom voor beheer. Dit wordt sinds 2009 in de (tijdelijk) geïmproviseerde database van CCIRS gedaan. Op centraal niveau (JCG DEFDA) bevindt zich de centrale database.
Ook het beheer van de ondersteunende hardware gebeurt merendeels handmatig. Hierdoor is geen accuraat en actueel overzicht beschikbaar. Daarnaast bestaan er veel (fabrikant eigen) subsystemen met een (fabrikant) eigen beheer en management.
Sturing en planning op centraal niveau kunnen niet adequaat en accuraat plaatsvinden omdat inzicht ontbreekt in de kwantiteit en de kwaliteit van de crypto en controlled crypto middelen. Daarbij komt dat we, mede door de dynamnische omstandigheden, het beheer en distributie slecht uitvoeren. De beperkte cryptodistributiecapaciteit van het NBV is risicovol. CCIRS verlicht de administratieve last, maar lost niet alle knelpunten op. Wanneer (vanaf 2012) de productie en distributie van papieren ponsbanden stopt, neemt het belang van een andersoortige cryptodistributiecapaciteit toe.

Toekomstige situatie

In de toekomst moet door het moderniseren van de cryptodistributie de ontvangst en reproductie van sleutels en sleutelmateriaal digitaal mogelijk zijn. De verspreiding, installatie en vernietiging van sleutels en sleutelmateriaal *(on line, off line, over the air)* moet mogelijk worden. Het beheer dient zo te zijn, dat de distributie en registratie van sleutels en sleutelmateriaal en CCI-artikelen inclusief de overdrachtverantwoordingen geautomatiseerd mogelijk worden. Daarbij moeten ook de cryptodocumenten en reeksen (incl. NATO, EU en andere landen) geregistreerd en beheerd kunnen worden. Ook de behoefte aan informatie van de J6 DOPS, DMO, DEFDA en van de diverse beheerders moet ingevuld worden. Voor de ondersteuning van (Informatie Operaties) expeditionaire operaties en voor de bescherming van de informatie moet Defensie daarvoor over een adequaat EKMS beschikken dat op alle niveaus van rubricering kan functioneren. Deze EKMS-functionaliteit moet wereldwijd kunnen worden ingezet en dient klokrond beschikbaar te zijn.
EKMS moet passen in de bedrijfsbrede ERP gedachte en moet aansluiting vinden of opgenomen worden in SPEER.