Vervlecht cybersecurity in reguliere beheerprocessen

Zit cyberdefense wel in de haarvaten van de ontwerp-, bouw-, storings- en onderhoudsprocessen van onze vitale infrastructuur?

Als manager technische automatisering bij een Nederlandse vitale infrastructuur wil je dat cybersecurity daadwerkelijk een plek krijgt in de dagelijkse gang van zaken. Hoe zorg je hiervoor en bereik je met de activiteiten die je hiertoe onderneemt dat je 'in control' bent?

Highlights

- Cybersecurity moet een plek krijgen in de beheersingsprocessen van onze vitale infrastructuur.
- Reken de werklast en additionele diensten van cybersecurity door en reserveer daar een budget voor. Gebruik aanwezige tools en aanpakken om zicht te krijgen op de hoeveelheid werk.
- Investeer in een verbeterprogramma om cyberverdediging procedureel ingebed - en operationeel ingepland - te krijgen.
- De maintenance engineers van 'control and instrumentation' moeten de Getting Things Done (GTD) aanpak aanleren. Deze werkt ook voor het bestaande, niet security georiënteerde, werk.

Hoe leg je het managementteam uit hoeveel extra inzet er dagelijks gestoken moet worden in cyberverdediging? Hoe organiseer je dit nieuwe werk? Alle zaken die ons werk gemakkelijker moeten maken, zoals mobiele apparatuur, cloudoplossingen of remote control, brengen securityrisico's met zich mee. Om de professional in de frontlinie te ondersteunen bij de verdediging van kritische infrastructuur bieden wij hieronder handvatten die in operationele plannen en checklists gebruikt kunnen worden.

In 2009 nam de aandacht voor cybersecurity in vitale sectoren enorm toe door de ontdekking van het Stuxnet-virus dat ontwikkeld was om Iraanse ultracentrifuges te saboteren die gebruikt worden voor het nucleaire programma. Nucleaire installaties zijn vitale infrastructuur en door deze ontdekking nam de ontwikkeling van het cybersecurityvakgebied een sprong, naast de aandacht die er traditioneel al was voor de fysieke veiligheid (safety).

Met cybersecurity is de scope uitgebreid voor de beveiliging van de vitale infrastructuur, waarbij er gelukkig nog niet zo veel grootschalige incidenten zijn voorgevallen. De veiligheidscultuur rondom fysieke veiligheid van vitale infrastructuur lijkt er nog niet te zijn voor cybersecurity. Wanneer een fatale vliegramp heeft plaatsgevonden, worden bijvoorbeeld alle haarscheurtjes in de ophangingbouten van 747-vliegtuigen geïnspecteerd en waar nodig vervangen. Een ander voorbeeld is de tomeloze aandacht voor het voorkomen van graafschade aan de infrastructuur in de Nederlandse bodem. Hiervoor is een heel stelsel van beheersmaatregelen ingevoerd, terwijl graafschade nog steeds in de top-10 staat van de storingen aan de elektriciteits- en gasnetten. Er is veel cybersecurity gerelateerd werk afgekomen op mensen die een rol hebben in het beschikbaar houden van onze vitale infrastructuur. In dit artikel wordt ingegaan op hoe zij hier mee om kunnen gaan.

Stel je bent verantwoordelijk voor de technische automatisering van een bepaalde vitale infrastructuur, zoals energiecentrales, spoorinfrastructuur, landingsbanen, rijwegsignalering, bruggen, water- en energiedistributienetten en je hebt sinds een jaar of vijf stappen gezet om cybersecurity onder de knie te krijgen. Dan breekt onvermijdelijk de fase aan dat je uit je 'fleet protection programma' komt waarin de dijken verhoogd zijn, de dijkgraaf aangesteld is en de grote inhaalslag gemaakt is. In securitytermen heet het dan dat je het eerste baseline securityniveau hebt gerealiseerd. Wetende dat het cybersecuritydomein zich in een hoog tempo ontwikkelt, en realiserende dat verdediging van infrastructuur vaak veel meer kost dan wat cyberaanvallers

hoeven te investeren, ga je twijfelen of je het verdedigingsprogramma wel kan afsluiten of dat je tot een permanentere organisatievorm moet komen waarin je heel adaptief je verdediging kan inrichten.

Hieronder eerst een willekeurige opsomming van wat er bijvoorbeeld allemaal aan nieuw werk op je af komt als verantwoordelijke voor de technische automatisering:

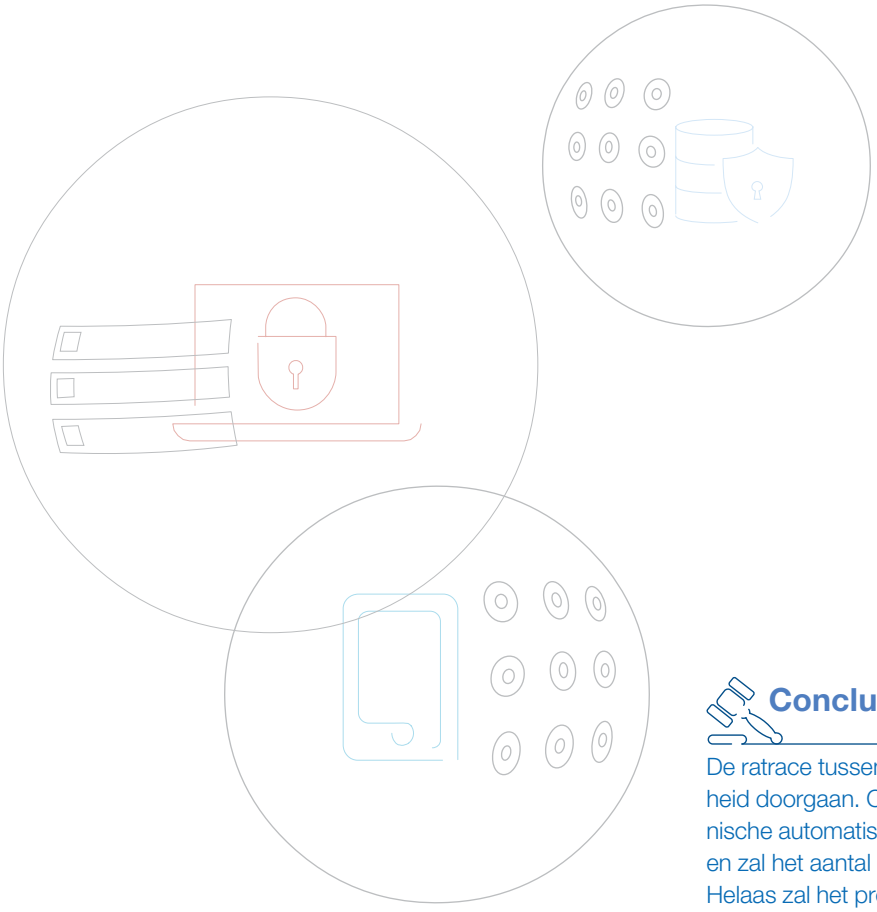
- Bij aanschaf van nieuwe assets veel nadrukkelijker kijken naar de securityaspecten.
- Oefenen hoe je de assets verdedigt bij een cyberaanval.
- Malware beschermingsdiensten inrichten en bewaken.
- Waar mogelijk penetratietesten uitvoeren.
- Indien verantwoord mogelijk, patchmanagement operationaliseren.
- Historie van afwijkend netwerkverkeer analyseren.
- De securitycontrols nalopen op deugdelijke werking.
- Remote access professioneel ondersteunen inclusief controls en procedures voor werken op afstand in je controlsystemen.
- Externe engineers die on-site komen aanspreken op gebruik van USB-sticks en verbindingen die ze maken vanaf hun laptop naar de procesautomatiseringssystemen.

Een deel van de taken zijn niet door eigen medewerkers uit te voeren, maar kunnen het beste door anderen worden gedaan. Zij moeten in dat geval rapporteren hoe de zaken ervoor staan. Het komt neer op cyberdefensedoelen stellen, het cybersecuritywerk gedaan krijgen, evalueren hoe het loopt, continu bijleren, samenwerken met andere medewerkers en overzicht houden.

Wat zijn hulpmiddelen om je operationele plannen op te baseren? Een goed voorbeeld is een praktische securityrichtlijn die de Noorse overheid heeft opgesteld voor de daar rijkelijk aanwezige olie en gasindustrie genaamd OLF104, die in 16 eenvoudig geformuleerde vragen een goed richtsnoer biedt[1]. Een ander voorbeeld is van het Amerikaanse Departement of Homeland Security die een complete ‘security assesment tool’ heeft ontwikkeld dat helpt met het omzetten van risico’s naar te nemen securitymaatregelen[2]. Ook heeft zij een specifieke training opgezet voor de beveiliging van controlesystemen waarin wordt gesimuleerd dat een echt fysiek proces verdedigd moet worden door de helft van de deelnemers, terwijl de andere helft aanvalt. Een laatste voorbeeld komt van de Duitse overheid die bedrijven in vitale sectoren verplicht heeft om de technische automatisering ook op te nemen in het Information Security Management System (ISMS), zodat reguliere periodieke cybersecurity-activiteiten geagendeerd staan en daarmee op tijd worden uitgevoerd (zoals bijvoorbeeld audits). Het zijn allemaal voorbeelden om het uitvoeren van cybersecurity-werk inzichtelijk te krijgen, te weten hoe je er voor staat, te bepalen welke zaken intern (IT-afdeling) of extern uitbesteed kunnen worden en welke zaken in bestaande operationele procedures en werkwijzen ingebed moeten worden. Een voorbeeld is de Management of Change (MoC) aanpak voor wijzigingen in een plant of fysieke processen. Daarin komt meestal het security-aspect nog niet voor (wel vaak het IT-aspect), maar zou dat wel moeten krijgen om vervolgens consequent uit te voeren worden bij alle wijzigingen.
De operationele verbeteraanpak is doorgaans gebaseerd op een Plan-Do-Check-Act (PDCA) cyclus. De operationele onderhoudsaanpak is vaak gebaseerd op urgent en niet urgent te plannen onderhoudsorders. Het is verstandig deze bestaande aanpakken ook te gebruiken voor cybersecurity gerelateerd werk en dus gepland onderhoud toe te voegen voor het uitvoeren van controles van logfiles, het bekijken van virusscannerstatistieken en het uitvoeren van systeempatches. Als er een grotere revisie van een installatie of verandering (change) in het proces doorgevoerd gaat worden, dan moeten ook de grote securityverbeteringen worden doorgevoerd en dus met voldoende prioriteit mee worden gepland. Daarnaast moet tijd worden gereserveerd voor zaken die vallen onder de brede categorie ‘samenwerken en afstemmen’. Denk hierbij aan regulier overleg met de leveranciers om (beleids)wijzigingen aan beide zijden te bespreken op impact en verantwoordelijkheden, de huidige stand van zaken door te nemen en terug te kijken op uitgevoerde veranderingen (changes). Ook kan worden gedacht aan de afstemmingsoverleggen met de interne IT-afdeling waarin de securitystandaard op de agenda moet komen.

Wat het meest lastige is om mee om te gaan, is de constante stroom aan nieuwe securitykwetsbaarheden. Deze zijn niet te veronachtzamen, maar zijn heel divers in impact, aanpak en doorlooptijd. Die kunnen net als sommige andere typen van onderhoud worden getypeerd als ‘urgent’. Alleen komen deze urgente onderhoudsorders meestal niet uit de controlroom van een fabriek of van de wacht van een centrale, maar vanuit de securitydijkbewaking (van bijvoorbeeld het security operating center of het computer emergency response team van een van de leveranciers). Dan is het zaak deze te bespreken met de supervisor en er een urgente order van te maken.
Een ander belangrijk aspect betreft het stimuleren van securitybewustzijn. Dit omvat zowel voorbeeldgedrag, regelmatige speciale bewustzijnverhogende acties uitvoeren, maar zeker ook anderen erop aanspreken als er onveilig gewerkt wordt. Alleen beveiligde bestandsuitwisseling of geen bestandsuitwisseling moet net zo gangbaar worden als de leuning gebruiken bij traplopen. En regelmatig oefenen hoe te handelen bij een cyberaanval. Dit is vergelijkbaar met een reguliere crisismanagementoefening maar dan met een speciale focus (scenario) op het onzichtbare gevaar van cybercriminaliteit.

[1]https://www.norskoljeoggass.no/en/Publica/Guidelines/Integrated-operations/104-Recommended-guidelines-for-information-security-baseline-requirements-for-process-control-safety-and-support-ICT-systems/.
[2]https://ics-cert.us-cert.gov/Assessments.



Conclusie

De ratrace tussen cyberverdediging en -aanval blijft in alle hevigheid doorgaan. Op termijn zullen productleveranciers van technische automatisering ‘security by design’ onder de knie hebben en zal het aantal doorsnee kwetsbaarheden significant afnemen. Helaas zal het probleem daarmee niet afnemen maar verschuiven naar geavanceerdere kwetsbaarheden. Het is zaak om op basis van een risicogebaseerde benadering cyberdefense in te bedden in het reguliere securitymanagement van uw organisatie.

Over de auteurs

Christiaan van Essen BBA is consultant bij Capgemini. Christiaan voert hoofdzakelijk opdrachten uit in de publieke markt en is expert of het gebied van veiligheidsmanagement. Milé Buurmeijer is senior ICT architect bij Capgemini en heeft ruime ervaring in het beschermen van kritische infrastructuur bij toenemende digitalisering van de primaire processen. Roger Wannee is principal consultant bij Capgemini en als zodanig actief op het gebied van openbare orde en veiligheid. Specifiek richt hij zich op vraagstukken op het vlak van cybersecurity, crisisbeheersing, beleidsrealisatie en bedrijfsvoering.

Voor meer informatie kunt u contact opnemen met de auteurs via:
christiaan.van.essen@capgemini.com,
mile.buurmeijer@capgemini.com en roger.wannee@capgemini.com