Kiezen voor de veilige weg

Cybersecurity in Verkeer & Vervoer

CGI

Experience the commitment®

We worden steeds afhankelijker van IT en digitalisatie. Niet alleen voor ons gemak, maar ook voor onze veiligheid. In de sectoren Transport, Logistiek, Post & Pakket- en Personenvervoer is dat niet anders. De onderlinge verbondenheid, de samenwerking van diverse organisaties en de innovaties waarmee de sector bezig is, maken de afhankelijkheid van Informatie Technologie en Operationele Technologie (IT en OT) groot. Helaas neemt onze kwetsbaarheid daarmee ook toe.

Wat een cyberaanval kan aanrichten, zagen we bijvoorbeeld in 2017. Het ransomware-virus Wannacry trof 230.000 computers in 150 landen. Beursgenoteerde bedrijven blijken maar moeizaam te herstellen van deze aanval. En Wannacry staat niet op zich. Wat zijn bijvoorbeeld de gevolgen als hackers de bediening van waterkeringen overnemen? Of als halverwege de avondspits plotseling alle verkeerslichten op groen gaan? Cyberdreiging is een van de grote thema's van deze tijd. In deze brochure gaan we graag met u in op de broodnodige bescherming van uw missiekritische systemen.

Digitalisering in de sectoren Transport, Logistiek, Post & Pakket- en Personenvervoer

De onderlinge verbondenheid van computersystemen van burgers, bedrijven en overheidsinstellingen levert een schat aan informatie op en biedt organisaties unieke kansen om nieuwe markten te exploiteren. Dit wordt inmiddels alom erkend, zo tonen CGI's Client Global Insights van de laatste twee jaar aan (zie tekstinzet). Ook binnen de sectoren Transport, Logistiek, Post & Pakket- en Personenvervoer zien we nieuwe businessmodellen ontstaan rondom digitalisering. Drie ontwikkelingen die de sector raken springen eruit:

1. **Data analytics en artificial intelligence**
   Onze klanten in de sector Verkeer en Vervoer evalueren allemaal de mogelijkheden van data-analyse. Hun aandacht gaat uit naar technologieën zoals data analytics en artificial intelligence. Dankzij data-analyse kan onderhoud aan apparatuur op het gunstigste moment worden uitgevoerd. Ook kunnen we er rijgedrag mee voorspellen en beïnvloeden. Cruciaal is dan wel de beschikbaarheid, integriteit en vertrouwelijkheid van data. Hoe borg je die betrouwbaarheid?

2. **Privacy en data governance**
   In mei 2018 wordt de Algemene Verordening Gegevensbescherming (AVG) van kracht. Organisaties moeten precies weten over welke privacygevoelige gegevens zij beschikken en waar die zijn opgeslagen. Ook moeten ze inzage geven wanneer daarom gevraagd wordt. Dit vereist een herdefiniëring van data governance. Hoe zorg je voor adequate classificatie en beheer van gegevens? Op welke wijze ga je inzage geven? En hoe werkt de verantwoordingsplicht wanneer organisaties met elkaar samenwerken in een ecosysteem?

3. **Samenwerken in de keten**
   Organisaties opereren steeds meer in ecosystemen. Dit stelt bijzondere eisen aan de beveiliging van de hele samenwerkingsketen, want ook security is maar zo sterk als de zwakste schakel. Op dit moment worden verschillende methodieken beproefd op hun vermogen grip te geven op de ketenbeveiliging. Denk aan blockchain, maar ook aan traditionele vormen, zoals audits bij toeleveranciers. Hoe beveilig je je eigen IT-omgeving als ketenpartners ook toegang tot je data moeten hebben?

In de 1.300 klantgesprekken die we in het kader van de Client Global Insights wereldwijd hebben gevoerd met leiders uit het bedrijfsleven en de overheid, komt cybercrime veelvuldig aan bod. Het groeiende risico van cybercrime heeft voor hen de hoogste prioriteit na de digitale transformatie. Meer weten? Ga dan naar www.cginederland.nl/global-insights.

Kwetsbaarheden voor het Verkeer en Vervoersdomein

Cyberaanvallen beperkten zich niet langer tot administratieve processen. Ook industriële en operationele processen kunnen tegenwoordig worden getroffen. De geautomatiseerde kranen in de havens, vliegtuigen, treinen: ze blijken allemaal kwetsbaar. De beveiligingsincidenten die zich de afgelopen jaren hebben voorgedaan, wijzen op drie ontwikkelingen die overheid en bedrijfsleven aan het denken zetten:

1. **Convergentie van Informatie Technologie en Operationele Technologie**
   De werelden van IT (kantoorautomatisering en administratieve processen) en OT (aansturing van onder meer luchtvaart, verkeersinformatiesystemen en waterkeringen) lopen steeds meer in elkaar over. Veel organisaties zijn afhankelijk van die koppeling tussen IT en OT, maar onderkennen de gevolgen onvoldoende. Een NotPetya-malware-aanval had onlangs grote gevolgen voor de operationele processen van APM Terminals, Mars en MERCK & Co. Anders dan gedacht bleken onveilige omgevingen toch gekoppeld. Dit leidde tot systeemuitval en hoge kosten voor wekenlang herstelwerk.

2. **Complexiteit rondom het beheer assets**
   OT-assets dateren vaak uit de jaren ’80 en ’90. Zij zijn niet gemaakt voor interconnectieve operaties en daarmee onveilig by design. Gekoppeld aan een IT-omgeving met verbindingen naar de buitenwereld staan in feite alle deuren open. Veel organisaties hebben weinig zicht op de omvang en status van al hun assets in de operationele omgeving en zien dus ook de gevaren niet. Vaak zijn ze aangewezen op reactief beheer in plaats van proactieve monitoring. Terwijl juist tijdige detectie een eerste vereiste is voor adequaat ingrijpen.

3. **Beperkte beveiliging Internet of Things**
   Ook de sectoren Transport, Logistiek, Post & Pakket- en Personenvervoer bewegen richting Internet of Things (IoT). Steeds meer apparatuur is ontworpen om autonoom beslissingen te nemen. Denk bijvoorbeeld aan in-vehicle apparatuur, monitornetwerken en weg- en walkantapparatuur. Via IoT worden sensorgegevens verzameld en geanalyseerd voor predictive maintenance op het spoor, bij waterkeringen en bruggen. Planning van post- en logistieke ketens verloopt door gebruik van sensordata. Helaas is de beveiliging van IoT-apparatuur nog niet op orde. Zo zijn sensoren kwetsbaar voor aanvallen om een botnet te creëren voor spyware, klikfraude of denial-of-service- aanvallen.

Waarom CGI?

CGI helpt organisaties in de sector Transport, Logistiek, Post & Pakket- en Personenvervoer slimmer te bewegen. We danken onze diepgaande domeinkennis aan onze lange historie in deze sector. Onze sectordeskundigen trekken samen op met onze cybersecurity-experts. Safety en security vormen daardoor een integraal onderdeel van ons Move Smarter gedachtengoed.

Met verstand van context en processen brengen wij de risico’s voor organisaties sneller in kaart. Monitoring richten we in op basis van zeer specifieke use cases. Wij kennen de impact van incidenten op de omgevingen van onze klanten in het Verkeer en Vervoerdomein als geen ander; we maken ze immers van dichtbij mee op het moment dat ze zich aandienen. Wij kijken naar het gehele ecosysteem waarin klanten opereren, omdat aanvallen zelfs kunnen lopen via vertrouwde leveranciers. We kunnen zo nodig de operationele beveiligings-activiteiten overnemen en monitoren, zodat onze experts kunnen optreden zodra zich een incident openbaart. Op die manier voorkomen we dataverlies of diefstal en borgen we de bedrijfs-kritische processen. Daarnaast voorkomen we dat de veiligheid van burgers of medewerkers in het geding komt.

CGI: geïntegreerd cybersecurity-portfolio

Het doel is een veilige en weerbare omgeving waarin IT, OT, reëel en virtueel door elkaar lopen. De weg daarheen is complex en vereist een cultuuromslag: iedereen in de organisatie zal zijn gedrag moeten aanpassen. Alleen een holistische aanpak, met aandacht voor mensen, processen, technologie en domeinkennis, leidt tot betere weerbaarheid. Zo’n geïntegreerde aanpak is wat CGI zijn klanten biedt. We hebben een zeer uitgebreid portfolio cybersecuritydiensten. Met de kennis van de sectoren waarin CGI al decennia actief is, bieden we cybersecurity-oplossingen, volledig afgestemd op onze klanten in het Verkeer en Vervoer.

CGI Cybersecurity-portfolio

Ons cybersecurityportfolio omvat diensten waarmee we onze klanten ondersteunen op drie terreinen:

Assess

Met Assess helpen we onze klanten bij de inventarisatie om van daaruit samen te werken aan verbetering van informatiebeveiligingsprocessen. Met risicoanalyses en topologyscans brengen we netwerken en zwakke schakels in kaart, ook bij ecosysteempartners, om te zorgen dat de hele keten betrouwbaarder wordt. Denk hierbij aan:

- beveiligings- en risicoassessments bij een post- en pakkettenorganisatie om te bepalen welke cybersecurityrisico's er spelen en welke maatregelen zijn getroffen;
- implementatie van een cybersecuritystrategie bij een luchtvaartmaatschappij.

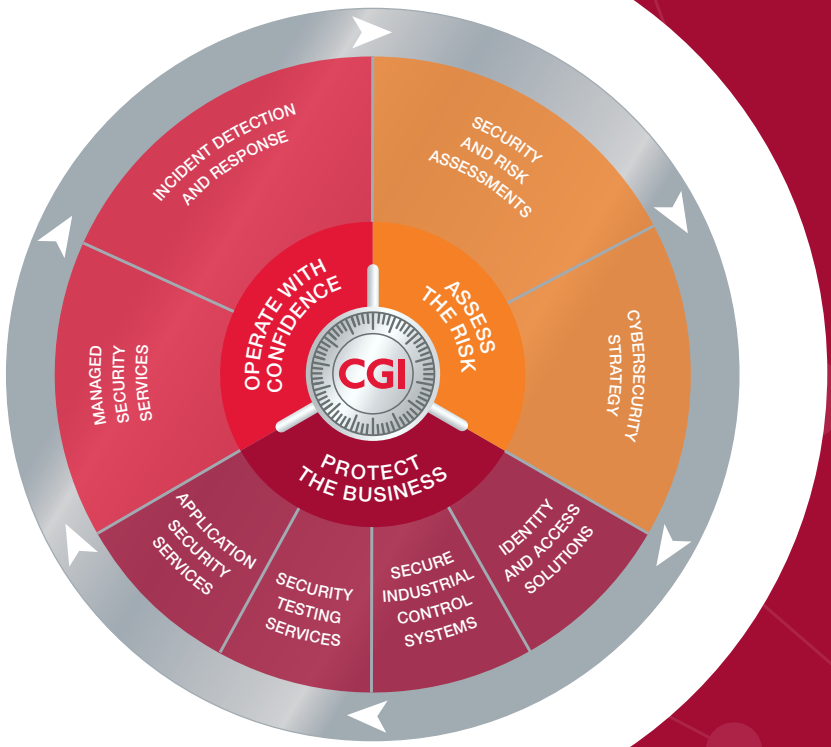
Protect

Protect bouwt voort op de Assess-inventarisatie en houdt in dat we concrete ondersteuning bieden bij de beveiliging van netwerken en omgevingen. Zo richten we onder meer het beheer in en integreren we beveiliging in ontwikkelprocessen. Te denken valt bijvoorbeeld aan:

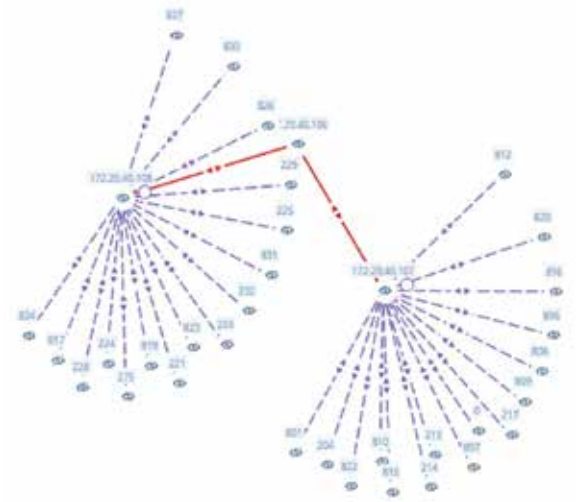
- identiteits- en toegangsbeheer om te zorgen dat applicaties en systemen bediend worden door geauthentiseerde en geautoriseerde personen;
- beveiliging van Industrial Control Systems voor verkeersmanagementsystemen, waterkeringen en sluizen;
- beveiligingstestservices om vast te stellen in hoeverre netwerken daadwerkelijk ontoegankelijk zijn voor kwaadwillende gebruikers.

Operate

Operate wil zeggen dat we ook hulp bieden bij het uitvoeren van de beveiligingsprocessen. Vanuit onze Security Operations Centers (SOC's) controleren we 24/7 alle processen op mogelijke dreigingen. Doen zich ondanks de beschermende maatregelen toch incidenten voor, dan hebben we incidentresponscapaciteit beschikbaar om direct in te grijpen. CGI's Managed Security Services kan die zorg geheel of gedeeltelijk van u overnemen. Zo informeren wij onze klanten bijvoorbeeld proactief wanneer wij informatie over hen aantreffen op het Darkweb. Recent was een klant van ons hierdoor in staat om een dreigend risico af te wenden en aanvullende monitoring in te stellen.



CGI cybersecurity-portfolio en de sectoren Transport, Logistiek, Post & Pakket- en Personenvervoer



Cybersecurity-uitdagingen inzichtelijk maken

De problemen die we nog kennen uit de begintijd van de personal computer vertonen grote gelijkenis met die van de systemen in het OT- en IoT-domein. Security is geen ingebed concept, patchmanagementprocessen zijn niet ingericht en asset- en configuratiemanagement zijn slechts beperkt op orde. Wij helpen u de risico's van de huidige IT-, OT- en IoT-omgeving in kaart te brengen. De methodiek die we daarvoor kiezen is altijd afgestemd op de eisen en wensen van de klant. Met de OT-topologyscan verzorgen we bijvoorbeeld een non-intrusive scan van de OT-omgeving, die we op een heldere manier visualiseren.

Architectuur definiëren en systemen inrichten

Aan de hand van de verworven inzichten bespreken we of geïdentificeerde koppelingen logisch en verwacht zijn en welke risico's we zien in de architectuur. Vervolgens definiëren we een referentie-architectuur, als basis voor de beveiliging, en richten we het configuratie-managementproces in. Verdere optimalisatie bereiken we door segmentering, hardening en intrusion detection en prevention. We maken gebruik van publieke standaarden zoals ITIL, NIST, ISO en SANS. Onze specialisten hebben veel domein- en sectorkennis die ze dag in, dag uit inzetten om het beveiligingsniveau van onze klanten te verhogen.

Integrale Security Monitoring

Om beveiliging van industriële systemen te combineren we de diensten Industrial Control Systems Security en Managed Security Services. Ook de ontwikkelingen rondom Intelligent Transport Systems en Mobility as a Service (MaaS) vragen om zo'n aanpak. In CGI's Security Operations Centers zijn de cybersecuritydiensten voor het IT- en het OT-domein geïntegreerd. Zo hebben we een totaalbeeld van eventuele bedreigingen en mogelijke verbindingen tussen verschillende bedreigingen. Niet-geautoriseerde opdrachten vanuit de kantooromgeving naar de OT-omgeving worden gedetecteerd en indien noodzakelijk geblokkeerd. Tooling signaleert de installatie en verspreiding van malware van of naar het OT-domein. Daarnaast hebben we de mogelijkheid om cyberdreigingen van elkaar te isoleren en de kans op verdere infectie te verkleinen. Op die manier borgen we niet alleen de beschikbaarheid en integriteit, maar ook de vertrouwelijkheid.

Bewezen expertise:

- Everest Group (2016) positioneert CGI in het Major Contender-kwadrant – Service Provider Landscape with PEAK Matrix™ Assessment 2015 voor IT Security Services.
- Uitgeroepen tot marktleider voor cybersecuritydiensten op het gebied van OT en IT in het Ovum-rapport: 'Ovum Decision Matrix: Het selecteren van een IT/OT-integratiepartner, 2014-15'.
- Samen met Oxford Economics hebben we een studie rondom 'Cyber Value' uitgevoerd. Hieruit blijkt dat de beurskoers van organisaties zich moeizaam herstelt na een cyberaanval.

Wat we doen voor klanten

- CGI ontwikkelt en beheert missiekritische systemen op het gebied van weg- en spoorverkeer en scheep- en luchtvaart. Voor een van onze klanten hebben wij de aanwezige missiekritische systemen geïnventariseerd. Op basis van de resultaten bepaalden we in welke volgorde de systemen werden aangesloten op het Security Operations Center (SOC) van de klant. De technische aansluiting van de geselecteerde systemen op het SOC viel onder onze verantwoordelijkheid, waarna het SOC de securitymonitoring op gevoelige objecten zelfstandig in uitvoering nam. Voor de OT- omgeving bereiden we nu de implementatie van CGI-tooling voor die de OT-topologie in kaart brengt. Dit doen we out-of-band om verstoring in deze kritieke omgevingen te voorkomen.
- Bij een organisatie in de sector Post & Pakket en Logistiek inventariseren we het systeem-landschap en de risico's die hierin op het gebied van cybersecurity spelen. Inmiddels hebben wij een goed beeld van de infrastructuur en starten we met de bouw van beveiligings-maatregelen. Die behelst onder meer de implementatie van Secure Software Development Lifecycle ter bescherming van nieuw ontwikkelde applicaties. Bescherming van de operationele omgeving borgen we met identiteits- en accessmanagement. Dankzij incident-, respons- en secure-operationsplanning kunnen we incidenten detecteren en adequaat actie ondernemen. Met onze kennis van de klantprocessen kunnen we altijd de meest effectieve beveiliging in richten.

Meer Informatie

Wilt u meer weten over cybersecurity van CGI, neem dan contact op met uw accountmanager of met CGI via:
T: +31 (0)88 564 0000
E: cybersecurity.nl@cgi.com
www.cginederland.nl/cybersecurity

Over CGI

Als vier na grootste zakelijk en IT-dienstverlener ter wereld is CGI wereldwijd actief. Lokaal gaan we sterke partnerships aan met onze klanten, waarbij we altijd kunnen putten uit de bijna eindeloos aanwezige technologische knowhow binnen ons bedrijf. Onze focus op Digital Transformation, IT Modernization, Cybersecurity en Advanced Analytics helpt onze opdrachtgevers hun dienstverlening verder af te stemmen op de klantwensen. We weten kosten te besparen, de business flexibeler te maken en de IT-omgeving voor te bereiden op de toekomst. En we doen dat met de toewijding en zorgvuldigheid van een businesspartner die niet anders gewend is dan te werken met de missiekritische systemen van zijn opdrachtgevers.

CGI

www.cginederland.nl