Cyber Chain Resilience Consortium

Cyber boost sessie

Wat doe jij tijdens een cyber incident?

INHOUD

Elke dag zijn er nieuwe cyberincidenten in het nieuws die duidelijk maken dat dit voor veel organisaties een steeds groter probleem is. Cyberschaamte is daardoor een bekend fenomeen, er zijn weinig bedrijven die vrijwillig naar voren treden en zeggen "luister, er is wat gebeurd". Niemand wil de zwakste schakel zijn. Cyberweerbaarheid in de keten is daarom een gezamenlijke verantwoordelijkheid.

Als organisaties zijn we natuurlijk steeds afhankelijker van digitale services ongeacht ons businessmodel. Er komt ook steeds strengere wetgeving met betrekking tot het gebruik van data in die digitale services. Denk aan de NIS2** die in de komende jaren effectief gaat worden. En daarbij, je bent nooit 100% cyberveilig, wat je ook doet, het kan jouw bedrijf ook gebeuren. Vroeg of laat word je gehackt.

De schatting is dat maar liefst 1 op de 3 ondernemingen inmiddels te maken hebben gehad met een cyberaanval. Het aantal cyberaanvallen in 2022 is met 38% gestegen vergeleken met die van 2021. De complexiteit van een cyberaanval wordt steeds groter, waardoor het afhandelen van een cyberaanval lastig is en oefening vereist. Bedrijven focussen zich op het voorkomen van cyberincidenten binnen hun eigen organisatie.
En dat is goed!

**zie https://www.digitaltrustcenter.nl/wat-gaat-de-nis2-richtlijn-betekenen-voor-jouw-organisatie

Maar liefst 1 op de 3 ondernemingen hebben inmiddels te maken gehad met een cyberaanval.

Daarnaast is het belangrijk jezelf voor te bereiden voor als je onverhoopt met een cyberaanval te maken krijgt. 100% voorkomen van cyberincidenten is niet mogelijk. En zeker niet nu we steeds afhankelijker worden van (digitale) ketenpartners. Wat doe je als één van je partners slachtoffer is geworden? Het aantal cyberaanvallen gericht op toeleveringsketens is de laatste jaren in opkomst. En, niet alleen het aantal cyberincidenten in de keten, maar ook de impact van deze aanvallen stijgt flink.

In deze whitepaper kijken we vanuit verschillende invalshoeken naar cyberincidenten: vanuit de hacker, het slachtoffer, en vanuit ketenpartners. Zo krijg je een beter beeld van een cyberattack en weet je wat je moet doen om jouw organisatie cyberweerbaarder te maken.

Hacker journey

Veel mensen denken dat hun bedrijf niet geraakt gaat worden, want "ze hebben toch niks bijzonders". En daar zit dus precies een zwakke plek, want iedereen kan het slachtoffer worden van een cyberaanval.

Een cybercrimineel heeft altijd wel een motief om een organisatie binnen te komen met een bepaald belang, en vaak zit dat belang in de keten. Vanuit dat perspectief is het verstandig om je af te vragen hoe de crimineel ongeautoriseerd digitaal bij je binnen zou kunnen komen. En dat is eigenlijk precies de mindset die alle bedrijven, ongeacht of ze klein, MKB, of multinational zijn en in welke sector ze actief zijn, zouden moeten hebben.

Dreiging motieven

Er zijn verschillende dreiging motieven van cybercriminelen waarvan sommigen wel en andere niet voor je bedrijf van toepassing zullen zijn:

Hacktivism: activistische groepen of rebellen, die linken we vaak aan fysieke acties die voor het grote publiek goed zichtbaar zijn zoals de snelwegen blokkeren. Maar ook deze groepen gaan op de digitale wereld over en zoeken nieuwe vormen om hun punt te maken. We hebben al gezien dat bepaalde organisaties zijn platgelegd met een zogenaamde DDoS (Distributed Denial of Service) aanval. Een dergelijke aanval overbelast de website van een bedrijf zo ernstig dat het onbereikbaar is.

Crime: dit is de gangbaarste en grootste dreigingscategorie voor de meeste bedrijven, hier staat het financiële belang dat er te halen valt voorop. Dit soort criminele partijen zijn volwaardige en volwassen organisaties met een HR of recruitment afdeling en een helpdesk. Zo heeft de hackersgroep die zichzelf 'Conti' noemt in enkele jaren een vermogen opgebouwd van € 20 miljard aan gestolen bitcoins. Voor hen is het niet belangrijk of je een grote of een kleine organisatie bent en wat je doet, als er maar geld te halen is.

Insider: criminelen vinden altijd wel wegen om digitaal toegang te krijgen tot een bedrijf. Zo zien we dat de interne medewerker ook weleens de bron kan zijn van een cyberaanval. Het levert veel geld op voor de insider om even een paar dagen toegang te verkopen. Dus je wachtwoord verkopen of een tooltje installeren op je pc van de crimineel waarmee ze toegang hebben tot het bedrijfsnetwerk.

Spionage: een dreigingscategorie waarmee de crimineel vooral op zoek is naar vertrouwelijke data. Denk hierbij aan R&D gegevens of aan gegevens die inzicht geven over de economie. Het stelen van de vertrouwelijke data gebeurt onopgemerkt en vaak door andere landen (statelijke actoren).

Terrorisme en sabotage: deze vorm is vaak meer gericht op publieke organisaties waarmee ontwrichting van de maatschappij bereikt kan worden. Het kan een belang zijn van een statelijke actor om maatschappelijke onrust te creëren waardoor het land zich focust op de interne crisis en minder op externe conflicten.

Iedereen kan cyberslachtoffer worden. We vinden het heel normaal om als organisatie regelmatig brandoefeningen te doen. Hup, iedereen achter z´n bureau vandaan en naar een centraal verzamelpunt, looproutes oefenen en koppen tellen bij het verzamelpunt. Maar, de kans dat er brand ontstaat bij je bedrijf is 1 op 8000. Vergelijk dat met de kans op een cyberaanval en toch zien we dat het oefenen van cyber scenario´s veel minder vaak voorkomt dan brandoefeningen.

We moeten als bedrijven veel meer gaan oefenen, je wordt een keer slachtoffer van een incident, ook als je alle maatregelen op orde hebt. De keten is nu eenmaal kwetsbaar.

Hoe gebeurt zo'n incident dan?

Kleinste foutje kan fataal zijn

- Succesvolle phishing
- Vergeten server te updaten
- Zwak admin wachtwoord
- Onveilige koppeling met leverancier

Non-stop zoeken criminelen naar kwetsbare organisaties

- Tools scannen heel internet op zoek naar zwakheden
- Tools testen alle gelekte accounts op alle servers wereldwijd
- Tools om alle gevonden e-mail adressen te phishen

Er is altijd wel ergens een zwakke plek, een medewerker die op een linkje klikt, een zwak admin wachtwoord of een onveilige koppeling met een leverancier.

Victim journey

Een cyberaanval kan niet altijd worden voorkomen, je kunt wel beter of slechter voorbereid zijn op zo'n incident. Een onderdeel van die voorbereiding is het oefenen van scenario´s en het proactief voorbereiden van draaiboeken met acties in die verschillende scenario's.

Maar, heel veel bedrijven kunnen niet grootschalig oefenen of zijn zich simpelweg nog niet bewust van de risico's. Maar, zoals eerder genoemd, elk onderdeel van de keten is kwetsbaar en niemand wil de zwakste schakel zijn.

Het speelveld is aan het verschuiven naar kleinere organisaties, grote organisaties hebben vaak meer resources om zich beter te beschermen. Het speelveld voor de cybercriminelen is daardoor dus ook steeds groter, wat maakt dat het weerbaar maken van de keten steeds belangrijker wordt voor onze maatschappij.

Niemand komt je redden. Vaak wordt er tijdens een crisis aangenomen dat een externe, specialistische partij de boel wel komt oplossen.

Terugkerende uitdagingen tijdens een cyberincident:

1. **Tijdige escalatie** - wanneer is het een crisis? Is er echt iets aan de hand of valt het mee? Wanneer ga je offline? Wanneer ben je gehackt? Wie heeft het mandaat? Is dat de CISO of ga je eerst de leverancier bellen? En wat gebeurt er dan? Dit zijn allemaal vragen die tijdens een crisis naar voren komen en onder tijdsdruk beantwoord moeten worden. Het duurt vaak te lang voor er geëscaleerd wordt en dus ben je als bedrijf te lang kwetsbaar.
2. **Impact** - de cyberindustrie is constant in beweging en er zijn continu nieuwe dreigingen. Maar wat is de impact van die dreigingen? We focussen vaak vooral op het technische incident, maar kijken naar de werkelijke crisis is een nog grotere uitdaging: je kunt niet meer leveren, de media komt op je af, en je wordt verantwoordelijk gehouden.
3. **Onderschatting van het probleem** - niemand komt je redden. Vaak wordt er tijdens een crisis aangenomen dat een externe, specialistische partij de boel wel komt oplossen. “We bellen even iemand en dan komt het goed”. Maar, die partijen focussen eerst vooral op forensisch onderzoek, je kunt dan als bedrijf niet gewoon functioneren alsof er niets aan de hand is.
4. **Onbekende koppelingen leiden tot onzekerheid** - wie maakt er allemaal gebruik van de systemen van dat bedrijf? Er zijn vaak vele koppelingen die je niet kent. Zeker in de supply chain, als een stukje software ergens een issue heeft, dan weet je niet op welke andere systemen dit invloed heeft.
5. **Taalbarrière** - bij een incident krijg je forensische partijen, leveranciers, IT’ers, en mensen van verschillende afdelingen in het bedrijf samen in een crisisteam. En, die praten een andere taal. Zowel een productiedirecteur als een salesmanager moeten snappen wat er aan de hand is en wat de impact van de situatie is. Daar kan de CISO een belangrijke rol spelen, de brug slaan tussen techniek en business.
6. **Forensische aspecten** - eigenlijk kan bijna geen enkel bedrijf dit zelf doen. In een crisissituatie heb je daar echt gespecialiseerde partijen voor nodig die ervaring hebben met forensisch onderzoek.
7. **Internationale dimensie** - vaak draait een software overal in de wereld, dus het is bijna altijd een crisis met internationale impact. Het is dus niet alleen jouw bedrijf of alleen in Nederland, het is meestal veel wijder verspreid.
8. **Wanneer is het veilig?** - er heerst vaak de mindset van; we betalen en dan is het opgelost. Maar je kunt bijna nooit met zekerheid zeggen dat de hackers niet heel veel data van je server hebben gehaald of iets hebben achtergelaten in je systemen en het later nog een keer gaan gebruiken. Daarom is de grootste zorg voor directies dat het vaak lastig is om echt zeker te weten dat het weer veilig is. Meestal is daar wel een paar weken forensisch onderzoek voor nodig.

Afwegingen tijdens een cyberincident:

- Moet je wel of niet betalen?
- Moet je contact leggen met de hackers en onderhandelen?
- Moet je een nieuwe omgeving bouwen? Het probleem negeren, alles uitzetten en opnieuw beginnen?

En, buiten deze dilemma's is een bijkomende uitdaging ook: hoe leg je je keuze uit? Dit heeft de Universiteit van Maastricht bijvoorbeeld handig gedaan. Zij kozen ervoor om wel te betalen, ze vonden het een te grote impact op alles waar ze voor staan en wilden het risico om alle data te verliezen niet nemen. Er was te weinig capaciteit om te herstellen en een te groot gat tussen baten en lasten. Maar, zij konden die keuze ook goed beredeneren door als onderwijsinstelling hun ***lessons learned*** wijd te delen en iedereen hiervan te laten leren.

Ondanks het voorgaande voorbeeld, over het algemeen is het advies bij een incident om NIET te betalen, tenzij:

- Er gevaar is voor personen (bijv. chantage, veiligheid)
- Er sprake is van grote maatschappelijke schade/ontwrichting
- Er langdurige discontinuïteit is met zeer grote gevolgen voor de dienstverlening
- Er een disproportionele groot gat is tussen gevraagde ransom en kosten voor alternatieven

"Iedere organisatie is interessant voor cybercriminelen, alleen wordt dit nog onvoldoende beseft door organisaties"

Kelvin Rorive – CCRC

Maar om tot een dergelijke conclusie te komen, heb je wel bepaalde inzichten nodig:

- Inzicht in de aanvallers/aanval: hoe gevaarlijk is het? Wat kan er nog meer gebeuren? Data?
- Inzicht in de 'betrouwbaarheid'
- Inzicht in aanwezigheid van eventuele alternatieven
- Inzicht in afhankelijkheden van derden
- Inzicht in mogelijkheden voor herstel (inclusief duur & kosten)

En als je besluit te betalen, zijn er natuurlijk ook randvoorwaarden:

- Technisch kunnen betalen - betalingen gebeuren vaak met bitcoins of andere crypto, weet je hoe dit proces in z'n werk gaat?
- Goede governance en het consulteren van de juiste stakeholders
- Communicatief goed voorbereid zijn: wat wel en niet te zeggen? Ga je proberen dit uit de media te houden of stap je proactief naar buiten?
- Correcte melding datalek - weet je wat je wettelijke verplichtingen zijn?

Hacked! Samen oefenen

Om te beginnen met oefenen met je ketenpartners is een eenvoudig voorbeeld vaak voldoende. Gebruik wel een scenario wat makkelijk te vertalen is naar je eigen organisatie. In deze whitepaper, beschrijven we een simpel oefenscenario, gebruikt tijdens één van onze Cyber boost sessies. In deze boost sessie spelen de deelnemers dat ze eigenaar zijn van een grote winkel die de volledige boekhouding en administratie heeft uitbesteed aan een online dienstverlener. Doel van dit scenario was de deelnemers van de sessie te laten ervaren wat ketenafhankelijkheid betekent en hoe je moet reageren wanneer het fout gaat in de keten.

De deelnemers werkten samen in kleine groepjes om gezamenlijk te discussiëren over de situatie die was ontstaan en hoe daar het beste op te reageren om de crisis te beslechten.

Ronde 1
Met beperkte info toch in actie komen

'Je merkt bij zo'n oefening de dynamiek van verschillende achtergronden, verschillende persoonlijkheden, en verschillende ideeën'

In de eerste ronde werden bepaalde feitjes bekend gemaakt die duidelijk maakten dat er echt iets aan de hand was met de online dienstverlener, maar er was nog geen enkele clue over wat nu echt het probleem was. Dit gebeurt natuurlijk in de praktijk ook vaak en wat doe je dan? Wachten of ga je toch actief wat zaken voorbereiden?

Welke acties ga je NU ondernemen als directie van een getroffen bedrijf?
Hieronder enkele acties die werden genoemd door de deelnemers van de workshop:

1. **We moeten weten wat er aan de hand is** - leverancier blijven proberen te bereiken
2. **Waar zit het grootste risico?** Wie zijn de kritische partners in de keten en hoe moeten we daarmee omgaan?
3. **Intern crisis team opzetten** en regelmatig overleg over vervolgstappen
4. **Isoleren** - omgeving isoleren en productie laten doorlopen, ruimte om verder onderzoek te doen
5. **Hulp zoeken** van externe partij

Reflectie:
Net zoals bij een echt incident, merk je bij zo'n oefening de dynamiek van verschillende achtergronden, verschillende persoonlijkheden, en verschillende ideeën. Sommige mensen trekken gelijk conclusies, anderen zijn meer afwachtend. En dat gebeurt dus ook bij een echte crisis. Daar moet je als bestuurder orde in krijgen. Er is op dit moment nog zo weinig informatie, je kunt eigenlijk alleen jezelf voorbereiden op een mogelijke crisis. Begin met jezelf organiseren, zet een crisisteam op en betrek de juiste mensen erbij. Check eventuele externe partijen die zouden kunnen helpen.

Ben je proactief of reactief? Als je bijvoorbeeld al eerder over een soortgelijk scenario hebt nagedacht, dan heb je waarschijnlijk een plan. Een besluit over wel of niet offline gaan kun je op dit moment (waarbij nog maar zo weinig informatie bekend is) alleen nemen als je hier al eerder over hebt nagedacht. Heb je hier daarentegen nog niet eerder over nagedacht en werk je info gestuurd dan blijf je eindeloos zoeken naar meer informatie en die is er simpelweg niet.

Overzicht van acties die werden besproken in de teams:

- Info inwinnen
- Organisatie informeren
- Is het Twitter bericht legit?
- Medewerkers op de hoogte brengen
- Onderzoek (laten) doen naar lekken
- Bevestiging of het echt een hack is
- In kaart brengen van ervaren problemen
- Incident response plan pakken
- Crisisteam bijeen roepen
- Impact bepalen
- Communicatie over bereikbaarheid
- Intern: back-ups, status & isolatie
- Informeren IT team, escaleren forensisch team, identificeren probleem

'Training maakt je kundig in besluitvorming met een minimale hoeveelheid aan informatie'

Eric-Jan de Roode – CCRC

Ronde 2
Er is invloed op de keten

Op dit moment werd meer duidelijk over de crisis en realiseerden de deelnemers zich dat de keten ineens ook een belangrijke rol ging spelen in de afhandeling van de cyberattack. In deze ronde, hadden de deelnemers 15 minuten de tijd om te kijken of bovengenoemde acties nog wel passend waren. Ook bespraken ze welke vragen ze aan hun leverancier wilden stellen tijdens de volgende Q&A die was opgezet door de leverancier. De tijdsdruk tijdens zo´n oefening is lastig, maar dat gebeurt natuurlijk tijdens een echt incident ook.

Na de 15 minuten vergaderen kwam de groep met de volgende vragen voor de leverancier:

1. Welke data is precies in bezit van de crimineel? Alles of een gedeelte?
2. Wat is jullie plan van aanpak? Welke externe partij helpt jullie erbij? Hoe zit het met jullie back-up?
3. Wat is jullie advies? En het advies van de externe partij?
4. Wie is onze contactpersoon en wanneer spreken we elkaar weer voor een volgende update?

Reflectie:

In deze ronde zaten twee punten die als red flag zouden moeten gelden voor het opgezette crisisteam:

- Slechts twee uur nadat het forensisch onderzoek is begonnen, werd er al gemeld dat er geen toegang was tot netwerken van klanten. Maar, kan dat zo snel gezegd worden? Hier moet je je twijfels over hebben.
- Dat ze proactief een call opzetten voor al hun klanten betekent dat het incident openbaar is. Dit betekent dat jouw klanten ook weten wat er aan de hand is en je dus vragen gaat krijgen. Daar moet je op voorbereid zijn en een communicatieplan voor maken.

En, samenvattend heb je als bedrijf nu drie problemen:

1. Een herstel-probleem
2. Een continuïteitsprobleem
3. Een AVG-probleem

Bij een incident heb je informatie nodig van de keten om je eigen crisis goed te kunnen managen, en dat moet je ook afdwingen bij jouw leverancier.

Overzicht van andere punten die besproken werden in de teams:

- Communicatieplan
- ***Status so far***
- Vervolg acties
- Mogelijke consequenties in eigen systeem
- Waarom is er zo lang gewacht met inschakelen van een externe partij?

Je bent in zo´n geval 100% afhankelijk van de keuzes die gemaakt worden door de leverancier. En dat is geen goed gevoel.

Ronde 3
Hoe gaat dit aflopen?

In de laatste ronde werd duidelijk dat de cybercrisis onbeheersbaar groot werd. De deelnemers werd gevraagd na te denken over hoe dit zou aflopen.

Mogelijke scenario's hoe deze crisis zou aflopen volgens de groep:

1. Er wordt betaald en alles komt terug
2. De data komt niet terug
3. Punten 1 of 2, maar de eigen omgeving is ook besmet en je bent nog meer dingen kwijt

Verder, werden de volgende stappen gedefinieerd:

1. Crisiscommunicatie: we zijn verantwoordelijk voor onze klanten en moeten nu crisiscommunicatie gaan opzetten naar onze klanten en de buitenwereld.
2. Bedrijfscontinuïteit gewaarborgd - is er een verzekering?
3. Data herstel? We gaan ervan uit dat we de data niet meer terugkrijgen en het uitgangspunt is dat we niet betalen. Is er ergens een back-up? Kunnen we een back-up maken van al onze data die we nog veilig kunnen stellen?

Reflectie:
Je bent in zo´n geval 100% afhankelijk van de keuzes die gemaakt worden door de leverancier. En dat is geen goed gevoel. Logischerwijs wil je maatregelen treffen om minder afhankelijk te zijn, zoals regelmatig eigen back-ups maken etc.

Maar, wat heb je in het eerste uur (het zogenoemde “gouden uur”) gedaan om erger te voorkomen? Denk bijvoorbeeld aan simpele acties zoals bepaalde dingen uitprinten voor je offline gaat.

Het vertrouwen in deze leverancier is waarschijnlijk weg en dus neig je op zoek te gaan naar een andere leverancier. Daarom is het zo belangrijk dat ook die kleine leveranciers samen met hun ketenpartners oefenen, ze moeten weten hoe ze hun klanten kunnen bijstaan en zo die wantrouwende eerste reactie kunnen voorkomen.

Door in het gouden uur van een aanval direct concrete stappen te nemen, kan de schade flink beperkt worden.

Conclusie

Aanvallen kunnen niet altijd worden voorkomen. Je hebt wel invloed op de mate van impact door goed voorbereid te zijn:

- Die voorbereiding kun je beter met je ketenpartners samen doen i.p.v. ieder voor zich. In dit geval geldt zeker het principe 1 + 1 = 3.
- Cyberoefeningen met verschillende ketenpartners zijn een goede manier om zwakke plekken bloot te leggen en beter voorbereid te zijn op verschillende scenario’s.

Door met de hele keten bewust te zijn van de gevaren én samen voorbereidingen te treffen voor mogelijke incidenten, zorgen korte en geoefende lijntjes met ketenpartners voor snel en collectief handelen bij een cyberaanval in de keten. Een passende opvolging bij een cyberaanval kan de impact van een aanval behoorlijk verkleinen. Door verschillende scenario’s te oefenen, kunnen deze opvolgingen al deels worden voorbereid.

De unanieme conclusie van de Cyber boost sessie was dat cyberaanvallen aanzienlijke impact en kosten met zich meebrengen, maar met de juiste oefening kun je deze drastisch verminderen en jouw organisatie beter beschermen. Want, als je geen mogelijke scenario´s hebt voorbereid met bijbehorend stappenplan, dan is de beslissing om wel of niet offline te gaan tijdens een incident eigenlijk niet te maken. Je hebt namelijk nooit genoeg informatie over wat er aan de hand is. Het regelmatig oefenen, samen met anderen, en het opzetten van duidelijke communicatiekanalen om zo in het gouden uur van een aanval direct concrete stappen te nemen, kan de schade flink beperken.

Lessons Learned:

- Incidenten kunnen niet worden voorkomen, maar je kunt wel verschillende scenario's oefenen een paar keer jaar. Het feit dat je hier als organisatie mee bezig bent is al zo waardevol.
- Je wilt voorkomen dat er een schuldvraag komt te liggen om zo communicatie te bevorderen.
- In een crisisteam moet je niet alleen technische mensen hebben, maar juist ook mensen die de business vertegenwoordigen, maar ook disciplines zoals communicatie en servicedesk. Er is grote behoefte aan iemand die de brug kan slaan tussen techniek en business.
- Cyberoefenen moet niet alleen voor de security afdeling zijn, juist directeuren die geen IT verantwoordelijkheden hebben, zouden mee moeten doen in oefeningen.
- Maak vooraf een ***stakeholder map***: wie moet je benaderen voor wat en hoe ga je deze mensen benaderen tijdens een incident?
- Denk na over welke back-ups je wanneer maakt.
- Welke scenario's heb je voor je verschillende systemen? Bedenk van tevoren hoe lang je zonder een bepaald systeem kunt, voordat het echt een probleem wordt.
- Houd tijdens de voorbereiding van incidenten ook rekening met een scenario dat niets het meer doet. Het is bijvoorbeeld heel goed als je een draaiboek en contactenlijst hebt, maar als die op een sharepoint of in een email staan waar je niet bij kunt, heb je daar nog steeds niets aan.

CCRC partners

NFIR IT FORENSICS & INCIDENT RESPONSE

Microsoft

FME POWERED BY DUTCH TECHNOLOGY

ECP Platform voor de InformatieSamenleving

Nationaal Cyber Security Centrum Ministerie van Veiligheid en Justitie

COT Instituut voor Veiligheids- en Crisismanagement

digital trust center.

CIO PLATFORM NEDERLAND

Over CCRC

Het Cyber Chain Resilience Consortium (CCRC) helpt bedrijven bij het uitvoeren van cyberoefeningen in de keten en maakt daarmee organisaties, en dus ook Nederland, meer cyberweerbaar. Als partner van CCRC ben je onderdeel van een platform met voornamelijk (security)vertegenwoordigers van Nederlandse bedrijven die cyberoefeningen willen uitvoeren met hun ketenpartijen.

Ben jij klaar om te oefenen?

Organisaties binnen diverse sectoren van verschillende omvang kunnen deelnemen, want een cyberaanval kan alle organisaties treffen, groot of klein. Samen met de andere deelnemers oefen, deel je kennis en leer je samenwerken in de keten. Heb je interesse? Lees meer op www.ccrc.nl of stuur een mail naar contact@ccrc.nl. We nemen dan snel contact met je op.

Cyber Chain Resilience Consortium