# ‘Aanval afgeslagen’

## Leerevaluatie cyberaanval Hogeschool van Amsterdam en Universiteit van Amsterdam

**6 juli 2021**

# Inhoudsopgave

# 1. Aanleiding, aanpak & context

## 1.1 Aanleiding

Op 15 februari merken de Hogeschool van Amsterdam (hierna: HvA) en Universiteit van Amsterdam (hierna: UvA) dat ze zijn gehackt. De instellingen werken hard in de crisisrespons om de impact van de hack minimaal te houden. De HvA en UvA willen leren van de gebeurtenissen en hebben het COT Instituut voor Veiligheids- en Crisismanagement (hierna: COT) gevraagd te ondersteunen bij het leren. In deze rapportage presenteren wij de uitkomsten van de leerevaluatie waarin ervaringen, dilemma's en leerpunten centraal staan. Anders dan bij een verantwoordingsonderzoek ligt de nadruk niet op de precieze reconstructie van de feiten en het beoordelen op basis van kaders, maar op het in beeld brengen van uitdagingen, dilemma's en leerpunten.

## 1.2 Doel

De HvA en UvA willen leren van de cyberaanval die zij hebben meegemaakt. De situatie is in vergelijking met andere cyberincidenten relatief snel onder controle. Wel vergt dit een grote inzet van velen en de herstelmaatregelen lopen nog. De crisisorganisatie is opgeschaald waarbij de HvA en UvA intensief hebben samengewerkt. In reactie op de cyberaanval heeft een security/IT-respons plaatsgevonden waarbij ook externe cybersecurity-specialisten van Fox-IT zijn ingezet. In de respons zijn verscheidene teams ingezet (o.a. Computer Emergency Response Team (CERT), Centrale Crisisteam (CCT), security teams, crisiscommunicatieteam) en zijn nieuwe teams (kernteams voor impactbepaling en continuïteit) gevormd. De leerevaluatie resulteert in een overkoepelend relaas over wat er is gebeurd (het verhaal), wat er is gedaan en welke leerpunten er zijn. De leerpunten gaan zowel over de procesmatige kant van security/IT als over het crisismanagement en de bredere informatiebeveiliging.

## 1.3 Thema's

In de leerevaluatie gaan wij in op de volgende thema's:

- Informatiebeveiliging & beleid en aanpak algemeen
- Voorbereiding op incidenten (protocol/escalatie/expertise)
- De aanval en aanvallers (op basis van informatie vanuit Fox-IT)
- Signalering en incident respons
- Crisismanagement
- Communicatie
- Informatiemanagement
- Breder stakeholder management
- Situationeel bewustzijn & scenariodenken
- Privacy
- Overgang naar de nafase/fase van herstel

## 1.4 Gevolgde aanpak

Deze evaluatie is uitgevoerd in de periode tussen maart en juni 2021. Het COT is gestart met een analyse van verschillende documenten. Voorbeelden hiervan zijn verslagen van de CCT-vergaderingen, beleidsdocumenten, interne en externe communicatie-uitingen etc. De beschikbaar gestelde documenten zijn met de grootste zorgvuldigheid behandeld en uitsluitend ingezet om de feiten scherp te krijgen en inzicht te krijgen in de beschikbare informatie en in de gemaakte afwegingen.

In totaal hebben wij twaalf individuele gesprekken en twee groepsgesprekken gevoerd met direct en indirect betrokkenen. De opbrengst van de gesprekken is direct verwerkt in een werkdocument van het COT. In de gesprekken is aan de hand van thema's besproken wat, terugkijkend, de belangrijkste lessen zijn, maar ook wat goed is gegaan en belangrijk is om vast te houden. De interviews zijn benut als input voor zes zogenoemde leertafels met de teams die tijdens de periode actief zijn: het CCT, Crisiscommunicatie, Kernteams Bedrijfscontinuïteit en Impact, CERT/Security Operations Center (SOC)/ICT Services (ICTS)/Tech-Team, Prio 1-team en een afsluitende leertafel. Tijdens de leertafels

is besproken waar de deelnemers terugkijkend trots op zijn, wat ze willen vasthouden voor de toekomst en wat leerpunten zijn.

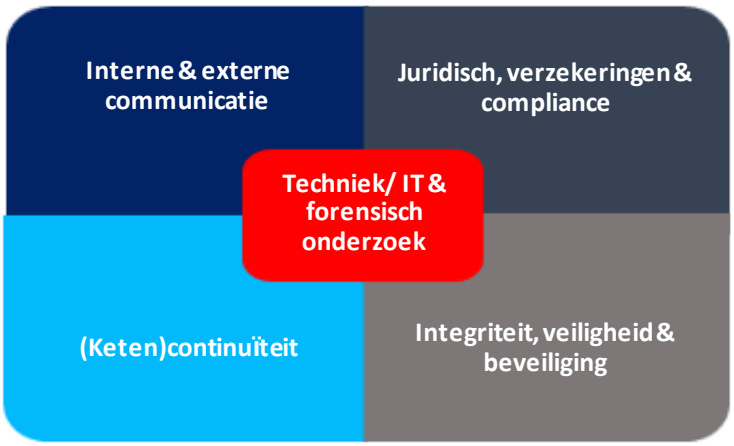
## 1.5 COT-visie op cybercrises: terugkerende uitdagingen

Digitale risico's zijn onverminderd groot en niet fundamenteel veranderd. Dit meldt het Nationaal Cyber Security Centrum (NCSC) in het Cybersecuritybeeld Nederland 2020. In de huidige samenleving blijven cyber gerelateerde incidenten één van de top risico's voor organisaties. Het verlies/de diefstal van informatie en het stilleggen van (de toegang) tot systemen zijn situaties met grote impact. Een cyberincident kan impact hebben op de continuïteit, de veiligheid (bijvoorbeeld bij manipulatie van data) en het vertrouwen in de organisatie (de reputatie). De risico's zijn aanzienlijk.

Informatiebeveiliging en privacy worden daarom als de twee thema's met het hoogste risico ingeschat door hoger onderwijsinstellingen volgens het Risico- en Dreigingsbeeld Hoger Onderwijs 2021. Daarnaast is kennisveiligheid een steeds belangrijker thema. Het profiel van hoger onderwijsinstellingen als grote, open organisaties die veel kennis beheren maakt hen geliefde doelwitten voor cybercriminelen en mogelijk statelijke actoren (spionage). Volgens het SURF Cyberdreigingsbeeld 2020-2021 zijn verkrijging en openbaarmaking van data, identiteitsfraude en verstoring van ICT-voorzieningen de meest voorkomende dreigingen.

Organisaties worden steeds weerbaarder, ook voor cyberdreigingen. Er zijn verdachte activiteiten en kleinere incidenten. Goede beveiliging en preventie dragen bij aan het voorkomen van impactvolle incidenten. Het blijft echter onmogelijk om volledig weerbaar te zijn voor cyberdreigingen. Beroepscriminelen, statelijke actoren, (h)activisten en overige onbekenden – en insiders – vormen een blijvend risico. Een organisatie kan een gericht doelwit zijn van kwaadwillenden maar ook onderdeel worden van een veel breder probleem, omdat een kwetsbaarheid aanwezig is waar veel organisaties mee te maken krijgen. De mogelijkheid om tijdig technische mitigerende maatregelen te treffen hangt in belangrijke mate af van de voorbereiding en de inrichting van de systemen.

Een cyberincident kan een crisis worden als de bestrijding en/of het beperken van de gevolgen onvoldoende lukt en de impact groot is. In de respons op een cybercrisis zijn in ieder geval de volgende componenten in meer of mindere mate van belang afhankelijk van het incident en de impact ervan.




Op basis van eerdere evaluaties en praktijkervaringen zien wij 10 bijzonderheden van een cybercrisis. Dit overzicht benutten wij als referentiekader in deze leerevaluatie.

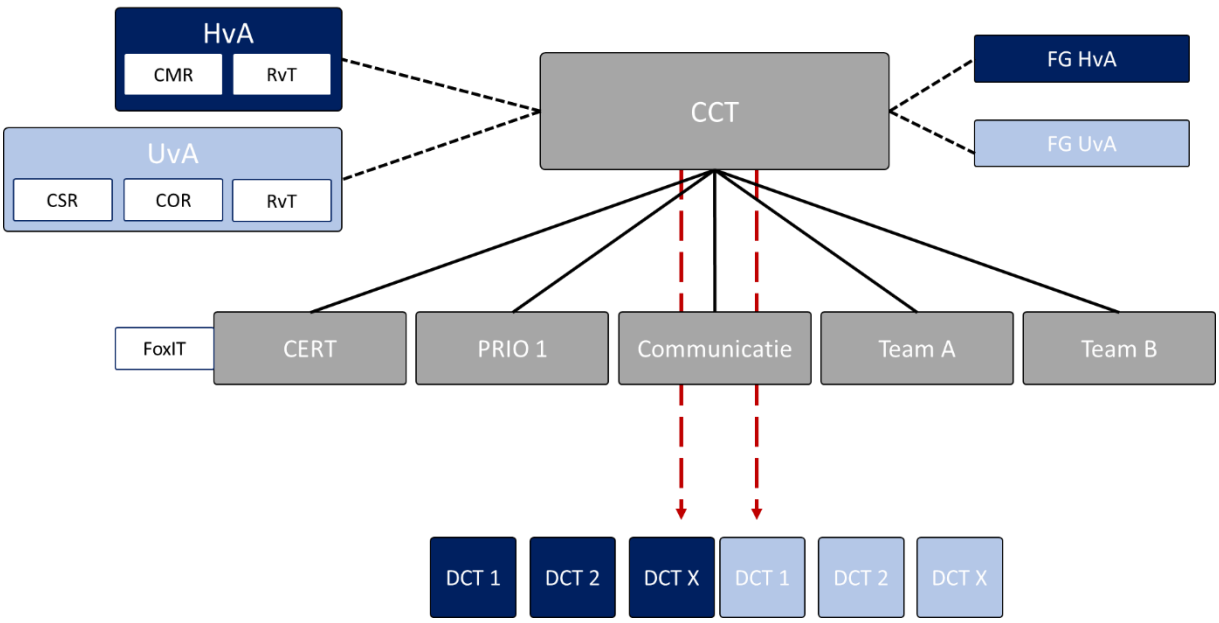
| Regelmatigheden bij een (dreigende) cybercrisis |
|---|
| 1. Van 'onzichtbare' problemen naar merkbare impact: aanvallers of insluipers kunnen al langere tijd in het systeem zitten om te verkennen en omsteeds verder door te dringen |
| 2. Noodzaak van tijdige escalatie: herkennen van het gevaar en het komen tot een eerste diagnose / attributie (Wat gebeurt er? Wat is mogelijke impact? Wie zit erachter? |
| 3. Onderschatting van het probleem en (te) hoge verwachtingen van de (snelheid van) de oplossing |
| 4. Onbekende koppelingen leiden tot onzekerheid: wat kan er gebeuren? Hoe hangen de verschillende systemen samen? Welke processen en applicaties zijn hieraan gekoppeld? Wat gebeurt er als delen uitvallen of uit worden gezet? |
| 5. Verbinden van twee werelden (technisch-bestuurlijk) en het spreken van verschillende 'talen': specifieke IT-terminologie is vaak niet goed bekend bij crisisfunctionarissen |
| 6. Forensische aspecten: het onderzoeken van systemen en applicaties om na te gaan wat er is gebeurd; waar de insluiper/aanvaller is geweest en/of wat is onttrokken, gewijzigd of juist is ingebracht. |
| 7. Internationale dimensie: quamogelijke kwetsbaarheden, aanvallers en/of (deel) van de oplossing |
| 8. Privacy als complicerende factor, vooral als het gaat om een mogelijk datalek en de dynamiek rond melden maar ook mogelijke risico's voor degene wiens data mogelijk in verkeerde handen is gevallen. |
| 9. Het is moeilijk om in te schatten wanneer het 'klaar' en/of 'veilig' is: hoe groot is het restrisico? Wat kan er gebeuren als data is gestolen? |
| 10. Lange duur en intensief herstel van functionaliteiten. Dit geldt ook voor situaties waarbij geen uitval heeft plaatsgevonden. |

Ransomware blijft een veelvoorkomend risico, ook in het onderwijs. De ervaring met de situatie bij de Universiteit Maastricht (eind 2019/begin 2020) heeft geresulteerd in extra aandacht voor cyber in het hoger onderwijs.[1] Naast het risico van gegijzelde data is in toenemende mate ook het risico dat onttrokken data wordt vrijgegeven aanwezig. Dit als extra chantagemiddel. Ook kunnen meerdere kwaadwillenden betrokken zijn: van degene die zorgt voor de eerste toegang (de hacker) tot degene die vervolgens een actie onderneemt gericht op het gijzelen. Het uitgangspunt bij ransomware is veelal om niet te betalen. Tegelijkertijd zijn er terugkerende dilemma's en voorbeelden van situaties met grote impact waarbij het betalen van 'losgeld' alsnog wordt overwogen. HvA/UvA hebben niet te maken gehad met daadwerkelijke gijzeling van data, maar dit was wel onderdeel van de dreiging.

## 1.6 Crisisorganisatie

Gedurende de crisisrespons is gewerkt met een gezamenlijke crisisorganisatie. We lichten deze hier kort toe als achtergrond voor de tijdlijn in hoofdstuk 2. Alle teams en rollen binnen de HvA en UvA zijn vrijwel gelijk. In de eigen organisatie moeten vanzelfsprekend wel eigen acties worden uitgevoerd. Onderstaande afbeelding toont op hoofdlijnen de belangrijkste crisisteams en functionarissen gedurende de crisis.

[1] SURFnet: lessen ransomware Universiteit Maastricht




Afbeelding: organogram gezamenlijke crisisorganisatie HvA/UvA

De (security) responsorganisatie ontstaat in reactie op de opgave die voorligt. De voorbereide crisisorganisatie wordt op maat aangepast:

- Op strategisch niveau is het gezamenlijk CCT actief. Zowel de HvA als de UvA hebben in de crisisorganisatie een eigen CCT. Voor de cyberaanval is besloten om, in plaats van parallel naast elkaar te werken, de teams samen te voegen als één actief CCT. Leden van het CCT zijn onder andere, maar niet uitsluitend: Voorzitter CMT HvA (tevens College van Bestuur (CvB)-lid portefeuillehouder Integrale Veiligheid), Voorzitter CMT UvA (tevens CvB-lid portefeuillehouder Integrale Veiligheid), Secretaris van de HvA, Secretaris van de UvA, Chief Information Security Officer (CISO), Directeur ICTS, Woordvoerder HvA en UvA en een plotter. Het CCT beschikt over een aantal adviseurs in de flexibele schil, zoals de Chief Risk and Insurance Manager (CRIM), de Functionaris Gegevensbescherming (FG) van de HvA en de FG van de UvA.
- De HvA en UvA hebben samen een eigen SOC en CERT op tactisch/operationeel niveau. Het SOC is onderdeel van ICTS. Het CERT is een virtuele organisatie en valt onder de CISO.
- Het Prio 1-team valt onder ICTS en komt bijeen op 15 februari jl. Het Prio 1-team van ICTS is aan zet bij verstoringen in de ICT-dienstverlening. Cyberaanvallen worden in het Prio 1-handboek als voorbeeld van een Prio 1-verstoring genoemd.
- Daarnaast stelt het CCT een zogenoemd Team A en Team B in. Deze 'impact' projectteams werken elk vanuit een eigen opdracht scenario's uit voor het 'zwarte scenario' en voor bedrijfscontinuïteit. De teams stellen adviezen en scenario's op als input voor de besluitvorming in het CCT.
- Op facultair- en dienst niveau zijn zowel bij de HvA en de UvA Decentrale Crisisteams (DCT) actief. Faculteiten worden via de Bedrijfsvoeringsoverleg (BVO)/Centraal Bestuurlijk Overleg (CBO)-update geïnformeerd. Een aantal DCT's inventariseren tijdens de crisisrespons, op verzoek van het CCT, welke systemen als kritisch beschouwd worden en welke verdere impact wordt ondervonden.
- Het CCT informeert zowel interne als externe stakeholders, waaronder de beide Raden van Toezicht. Zie voor meer informatie paragraaf 3.9 over breder stakeholdermanagement.

**Informatiebeveiligingsorganisatie** De HvA en UvA hebben een gezamenlijke security organisatie: SOC, CERT en ICTS. De CISO is direct onder het bestuur van de HvA en het bestuur van de UvA gepositioneerd. De CISO is een rol op strategisch en tactisch niveau. De CISO formuleert het informatiebeveiligingsbeleid en helpt bij een juiste vertaling daarvan naar de instelling sonderdelen. Binnen de afdeling ICTS zijn de rollen van Information Security Manager (ISM) en Information Security Officer (ISO) belegd.

Daarnaast is het CERT als ICT-incident responsteam bezig met het voorkomen, detecteren en oplossen van security incidenten. Het CERT heeft een directe escalatielijn met de CISO, de FG en het CvB indien nodig. Het CERT bestaat uit ICT- en securityspecialisten en wordt gecoördineerd door de Information Security Manager. Eerder is een bewuste keuze gemaakt rondom de wijze van monitoring.

## 1.7 Opbouw rapportage

In hoofdstuk 2 beschrijven wij de gebeurtenissen voor zover wij deze hebben kunnen reconstrueren, mede op basis van beschikbare documentatie en interviews. De nadruk ligt hierbij op de besluiten die vanuit de verschillende teams zijn genomen en op de interne en externe communicatie-uitingen. Onze observaties staan centraal in hoofdstuk 3. We gaan hierbij in op de thema's zoals benoemd in paragraaf 1.3. Op basis van de hoofdstukken 2 en 3 komen wij in het laatste hoofdstuk 4 tot onze overkoepelende bevindingen en leerpunten. In de bijlage staat een overzicht van de gebruikte afkortingen en staan de eerder door Fox-IT gegeven aanbevelingen.

# 2. Samenvattend overzicht van gebeurtenissen en acties

In dit hoofdstuk geven wij de belangrijkste gebeurtenissen en ontwikkelingen weer in relatie tot de hack. Dit is een selectie van de vele ontwikkelingen en acties. We beschrijven de gebeurtenissen en belangrijkste activiteiten voor drie domeinen: de technische respons, het crisismanagement en de communicatie.

| Thema | Selectie van belangrijkste gebeurtenissen |
|---|---|
| **Aanval** | **11 februari** Een laptop is met malware gecompromitteerd door een aanvaller en verkrijgt daarbij vele accountgegevens, onder andere een HvA/UvA user credentials.<br><br>**12 februari** Op 12 februari, binnen 24 uur na de aanval op de laptop, worden de eerste verkenningen gedetecteerd op de Citrix omgeving, waarbij buitgemaakte inloggegevens van de laptop zijn misbruikt.<br><br>**13 februari** Een andere aanvaller dringt binnen in de IT-omgeving van de HvA/UvA gebruik makend van het op de laptop verkregen account. |
| **Technische respons** | **15 februari** Het SOC signaleert verdachte bewegingen in het netwerk. Ze zien een *password spraying attack* en netwerk-verkenningsactiviteiten in het HvA/UvA netwerk van vrijdagnacht 12 februari tot en met zondag 14 februari. Het SOC meldt dit intern aan het CERT en neemt in overleg met het CERT eerste maatregelen om het risico te beperken. Om te zien of de aanvaller zich nog in het netwerk bevindt wordt besloten de monitoring uit te breiden. De gesignaleerde activiteiten passen bij ransomware-aanvallen. Het vervolgens opgeschaalde CERT muteert een aantal van de wachtwoorden en blokkeert een aantal gecompromitteerde admin-accounts. Een blokkade wordt ingesteld op de Command and Control server IP-adressen. Externe extra expertise wordt toegevoegd aan de incident respons door Fox-IT in te schakelen. Intern zijn het SOC, het CERT en het Prio 1-team actief.<br><br>**16 februari** Er wordt meer bekend over de situatie. Fox-IT heeft bewegingen van de aanvallers kunnen traceren vanaf zaterdag 13 februari. Het is nog onduidelijk of de aanvallers ransomware hebben geïnstalleerd. De OTA-omgevingen zijn uitgezet om ruis op het netwerk te voorkomen, waardoor detectie van eventuele vervolgbewegingen van de aanvaller sneller gedetecteerd kunnen worden. Geïnfecteerde SAP-servers zijn uitgezet om misbruik te voorkomen, voorzolang nog niet zeker is dat de aanvaller uit het netwerk is verwijderd. Deze 'active defense' heeft geen impact voor de gebruikers.<br><br>**17 februari** In de nacht van 16 op 17 februari wordt gebruik gemaakt van 'live monitoring'. Op één server wordt activiteit waargenomen. Fox-IT meldt dat de aanvaller mogelijk de beschikking heeft over de Active Directory domeindatabase met daarin inloggegevens met beheer- en gebruikersnamen en versleutelde wachtwoorden, maar ook andere gevoelige informatie zoals e-mailadressen, telefoonnummers en andere beschrijvingsvelden van UvA- en HvA-medewerkers en studenten.<br><br>**18 februari** Patiënt-0 is geïdentificeerd, het is de laptop van een gebruiker van de HvA/UvA. De laptop wordt direct vervangen en door Fox-IT forensisch onderzocht.<br><br>**19 februari** Fox-IT meldt dat het aannemelijk is dat de aanvaller de Active Directory domeindatabase heeft gedownload. De aanvaller kan deze gegevens zelf gebruiken om opnieuw aan te vallen of kan de gegevens verkopen. |

| | |
|---|---|
| | **23 februari** In een mail-to-all, gericht aan studenten en medewerkers, wordt bericht dat aanvallers (mogelijk) toegang hebben tot versleutelde wachtwoorden. Een plan wordt opgezet voor het proces wachtwoord wijziging. Dit proces bevat communicatieve en technische voorbereidingen die deels al in gang zijn gezet.<br><br>**1 maart** De CISO stelt samen met de betrokken experts een stappenplan met 10 randvoorwaarden op waaraan voldaan moet zijn voordat het sein 'brand meester' gegeven kan worden. De grootste onzekerheid voor het sein 'brand meester' is het analyseren van de servers die nu uit staan. Tot op heden zijn 70.000 wachtwoorden van de 177.000 wachtwoorden gewijzigd.<br><br>**2 maart** Vanaf vandaag worden accounts waarvan het wachtwoord nog niet gewijzigd is, geblokkeerd.<br><br>**3 maart** Het proces 'wachtwoord wijziging' gaat goed, de servicedesk werkt hard maar is niet overbelast. Microsoft doet een melding over een zwakheid in de mailomgeving. Een update is hierdoor vereist. Dit tweede incident staat los van de hack maar heeft wel impact aangezien de prioritering verandert en het de capaciteit van ICTS verkleint.<br><br>**9 maart** Het forensisch onderzoek van Fox-IT loopt nog. Er worden telkens servers vrijgegeven, maar nog niet alle servers zijn onderzocht. Hierdoor schuift het moment van sein 'brand meester' op.<br><br>**10 maart** Het project wachtwoord wijziging is grotendeels afgerond. De CISO adviseert aan het CCT om het sein 'brand meester' te geven en het CCT neemt het advies over.<br><br>**11 maart** De Microsoft Exchange-situatie maakt het komen tot een balans tussen benodigde rust voor zwaar belaste medewerkers en het opstarten van herstelwerkzaamheden lastiger.<br><br>**15 maart – 17 maart** De herstelwerkzaamheden starten. De SAP-omgevingen (HvA/UvA data, personeelsdossiers etc.) en Citrix-servers worden aangezet. Op 16 maart gaan de beheerservers om de werkplek te beheren (zoals Active directory) weer aan. De beheerservers zoals update- en monitoringservers zullen op 17 maart aangezet worden. Een aantal omgevingen is te complex om met interne kennis te herbouwen en worden nader onderzocht ter verificatie of ze daadwerkelijk schoon zijn.<br><br>**19 maart** Er wordt hard gewerkt aan het herstel. Indien besluitvorming nodig is wordt het Bestuurlijk Overleg Gemeenschappelijke Diensten (BOGD) hierover geraadpleegd. |
| **Crisis-management** | **15 februari** Verantwoordelijke leden van beide CvB's worden vroeg in de middag geïnformeerd over de hack. Hierop volgt een gezamenlijk bestuurlijk overleg. In dit overleg besluiten ze dat sprake is van een crisis. Twee CCT-vergaderingen vinden plaats waarin veel aandacht wordt besteed aan beeldvorming en duiding. De gezamenlijke crisisorganisatie is ingericht en een aanvalsplan wordt opgesteld. De FG's en de woordvoerders worden geïnformeerd en de cybercrime-unit van de politie Amsterdam wordt ingelicht. Er wordt nog geen aangifte gedaan, maar relevante gegevens worden door de politie wel gedeeld met Europol en Interpol. |

De CISO en de directeur ICTS leggen het CCT drie mogelijke scenario's als reactie op de aanval voor. Na het bespreken van de scenario's en de bijbehorende risico's besluit het CCT te kiezen voor het scenario 'terugvechten'. Dit houdt in dat direct counteren van de activiteiten van de aanvaller hopelijk leidt tot het terugtrekken van de aanvaller. Besloten wordt om de volgende ochtend het definitieve besluit over het scenario te nemen.

**16 februari** Het besluit om terug te vechten wordt bevestigd. Ook worden enkele aanvullende maatregelen genomen op basis van het advies van de deskundigen en op verzoek van de systeemeigenaar zelf: geïnfecteerde SAP-servers worden uitgezet. De helft van de Exchange servers wordt uitgezet.
De HvA en UvA doen een voorlopige melding bij de Autoriteit Persoonsgegevens (AP).

**17 februari** Interne en externe stakeholders worden telefonisch ingelicht over de aanval. Het communicatieteam stelt een overzicht van stakeholders en contactpersonen op.

**18 februari** Patiënt-0 is geïdentificeerd, het is de laptop van een student. Tijdens het CCT wordt benadrukt dat de gebruiker beschermd moet worden (geen naam bekend maken) en in het CCT wordt afgesproken dat de gebruiker uitleg wordt gegeven over het proces en de afhandeling.

**19 februari** Vanwege het risico dat de aanvallers in accounts kunnen komen van medewerkers en studenten, is het advies om alle wachtwoorden te wijzigen. Het gaat om een zeer groot aantal accounts. Om adequaat te kunnen reageren op alle verzoeken en vragen moet extra capaciteit worden gerealiseerd. Dit kost tijd. Het CCT neemt het besluit dat het verzoek aan de gebruikers om hun wachtwoord te wijzingen uitgesteld wordt tot het moment waarop de randvoorwaarden op orde zijn om dit verantwoord te kunnen doen.

**21 februari** De crisisorganisatie gaat 'fase twee' in. Het bestuur heeft aan de CISO en directeur ICTS verzocht om inzichtelijk te maken wat een 'veilige' situatie is waarop de aanval onder controle is. Vanaf nu wordt toegewerkt naar een sein 'brand meester'. Het CERT en betrokken experts werken dit nader uit. De CISO en de directeur ICTS adviseren het CCT om de wachtwoorden van studenten en medewerkers te laten wijzigen. Het CCT volgt dit advies op en besluit om alle wachtwoorden uiterlijk 8 maart gewijzigd te hebben. De Servicedesk van ICTS wordt opgeschaald om de verhoogde hulpverzoeken te verwerken. Pas als aan deze randvoorwaarde is voldaan, zal gecommuniceerd worden.

**23 februari** In een mail-to-all, gericht aan studenten en medewerkers, wordt bericht dat aanvallers (mogelijk) toegang hebben tot versleutelde wachtwoorden. Een plan wordt opgezet voor het proces wachtwoord wijziging. Dit proces bevat communicatieve en technische voorbereidingen die deels al in gang zijn gezet.

**25 februari** Het CCT stemt in met het advies om de ongewijzigde wachtwoorden evenredig te laten vervallen over een aantal dagen (3, 4, 5 maart). Zo moeten kwetsbaarheden worden beperkt.

**1 maart** Het CCT neemt de memo van kernteam A over en besluit HvA/UvA-data tot 8 maart offline te houden.

| | |
|---|---|
| | **5 maart** Het kunnen geven van het sein 'brand meester' loopt vertraging op in verband met de Microsoft Exchange kwetsbaarheid. Dit incident staat los van de hack. Het sein kan pas op zijn vroegst 9 maart afgegeven worden.<br><br>**9 maart** Het CCT stemt in met versnelde mail-migratie naar de Cloud. Dit vanwege de kwetsbaarheid in Microsoft Exchange.<br><br>**10 maart** Het CCT besluit om het sein 'brand meester' te geven. Op dit moment is aan één randvoorwaarde niet volledig voldaan. De overgebleven punten worden als aanvaardbaar risico ingeschat. Communicatie over het sein 'brand meester' vindt plaats via een persbericht. Vanaf het moment van sein 'brand meester' gaat de crisisorganisatie een nieuwe fase in, 'fase 3': de nafase.<br><br>**11 maart** De HvA en UvA doen aangifte bij de politie.<br><br>**12 maart** Het CCT begint met de afschaling. Het vergaderritme is nu drie keer per week. Kernteam B schaalt af en gaat in 'slaapstand'. De HvA en de UvA maken de definitieve melding van het incident bij de AP.<br><br>**19 maart** Het agendapunt 'technische ontwikkelingen' verdwijnt van de agenda van het CCT omdat de werkzaamheden inmiddels vallen onder de reguliere taken van ICT. |
| **Communicatie** | **15 februari** De woordvoerders zijn betrokken bij het CCT. Het advies is om nog niet te communiceren over de situatie.<br><br>**16 februari** Het crisiscommunicatieteam is geactiveerd. Nadere interne communicatie vindt plaats, onder meer voor het CBO- en BVO-overleg. De Raad van Toezicht (RvT)-voorzitters worden ingelicht. Het communicatieteam adviseert om pas breder te communiceren wanneer er meer duidelijkheid is. Het communicatieteam stelt daarnaast de volgende communicatiestrategie voor: het zorgen voor een balans tussen informeren en meenemen in de ernst van de hack en het behouden van rust en begrip. Deze strategie wordt overgenomen door het CCT.<br><br>**17 februari** De HvA en UvA communiceren conform strategie intern en extern over het feit dat een cyberaanval heeft plaatsgevonden. Beide instellingen communiceren dit via sociale media en op de websites. Verscheidene media berichten over de aanval.<br><br>**18 februari** Beide instellingen geven via sociale media en op de websites een korte update van de situatie waarin wordt benadrukt dat zeer beperkt hinder is van de aanval en dat alle systemen online en operationeel zijn.<br><br>**22 februari** Het communicatieteam stelt een bericht op voor alle medewerkers en studenten. In dit bericht staat een update van de situatie. Het bericht wordt op de website geplaatst. Hierin bedanken de CvB's iedereen voor de inzet en de hulp. Ook geven zij aan waar medewerkers en studenten updates kunnen volgen en vragen zij hen om de eigen mailbox in de gaten te houden.<br><br>**23 februari** Het e-mailbericht met het verzoek aan alle studenten en medewerkers om zijn/haar wachtwoord te wijzigen wordt verstuurd. Het bericht bevat een toelichting op het proces. Het attendeert gebruikers dat wanneer ze hetzelfde wachtwoord voor andere accounts gebruiken, het noodzakelijk is deze |

wachtwoorden ook te veranderen. Daarnaast verwijst het bericht de gebruikers die vragen hebben naar de Frequently Asked Questions (FAQ's) of de servicedesk ICT.

**25 februari** Uit de omgevingsanalyse blijkt dat het zowel in de reguliere media als op sociale media rustig is. Alle stakeholders zijn benaderd. Er wordt niet meer dagelijks gecommuniceerd.

**5 maart** De voorgestelde communicatieboodschap over het sein 'brand meester' wordt goedgekeurd door het CCT. In de landelijke media en op social media zijn nauwelijks nieuwe berichten over de aanval.

**10 maart** De HvA en UvA brengen naar buiten dat de cyberaanval is afgeslagen. Media en andere instanties reageren op het sein 'brand meester'. HvA/UvA ontvangen meerdere complimenten. De boodschap is dat de aanval is afgeslagen en dat het niet tot een gijzeling van data of tot een losgeldeis is gekomen.

# 3. Overkoepelend beeld & observaties per thema

In dit hoofdstuk beschrijven wij de observaties per thema. Waar relevant verwijzen we naar planvorming en eventuele afspraken. Eerder hebben we de tijdlijn op hoofdlijnen beschreven. Bij de observaties is het soms nodig aanvullende feiten op te nemen ter verduidelijking. We sluiten ieder thema af met een overzicht van leerpunten. Dit kunnen zowel punten zijn die goed zijn gegaan en moeten worden vastgehouden als punten waar versterking mogelijk is.

## 3.1 Overkoepelend beeld

In de toelichting per thema komen tal van aspecten aan de orde. Voordat we de thema's toelichten, geven we in deze paragraaf ons overkoepelend beeld. De observaties in de thema's zijn hier een verdere uitwerking van.

| Overkoepelend beeld |
|---|
| - De aanvallers zijn binnengekomen nadat malware gedownload wordt op een laptop een student. Er zijn gegevens gestolen op de laptop door een aanvaller en een andere aanvaller is daarmee binnengekomen en heeft steeds meer rechten verzameld.<br>- De impact van de aanval is relatief beperkt gebleven op onderwijs en onderzoek maar vergt een grote inspanning, ook in de nafase. Het gaat om een zeer risicovolle situatie waarvan de gevolgen veel ernstiger hadden kunnen zijn.<br>- De HvA en UvA zijn voortdurend bezig met het verbeteren van informatiebeveiliging. Naar aanleiding van de cyberaanval bij de Universiteit Maastricht zijn extra maatregelen getroffen en is aanvullende expertise aangenomen. Niet alle maatregelen zijn al geïmplementeerd op het moment van de aanval, en er zijn deels bekende en onbekende restrisico's.<br>- Er is sprake van breed gedeelde trots over de aanpak, maar ook realisme over het risico.<br>- Het is gelukt om de impact van de cyberaanval tot een minimum te beperken zowel in continuïteit als in vertrouwen.<br>- Er is door velen hard gewerkt om dit voor elkaar te krijgen. Veel mensen in de organisatie hebben bijgedragen, het commitment is groot. Tussen sleutelfunctionarissen zit onderling vertrouwen.<br>- De interne samenwerking is – enkele knelpunten daargelaten – effectief. Hierbij is op integrale wijze gewerkt (technisch, continuïteit, communicatie, juridisch, e.a.). Er is flexibel gereageerd op de opgave die voorligt.<br>- Vanwege beperkt zicht op een aantal zaken en beperkte uitwerking in draaiboeken moet veel worden geïmproviseerd. Dit is krachtig gebeurd vanuit ervaring en expertise.<br>- De kwetsbaarheid in Microsoft Exchange vraagt aanvullende inzet. Dit staat los van de hack, maar geeft extra druk en belasting.<br>- Specialisten zijn niet verrast dat een dergelijke aanval zich voor kan doen. Er waren en blijven kwetsbaarheden als het gaat om preventie en mitigatie, ondanks alle inspanningen. Respondenten benadrukken het belang van een paradigmashift naar cyberweerbaarheid. |

## 3.2 Informatiebeveiliging & beleid en aanpak algemeen

**Informatiebeveiliging** Informatiebeveiliging is een beleidsverantwoordelijkheid van het bestuur van de HvA en het bestuur van de UvA. Beide instellingen hebben een eigen informatiebeveiligingsbeleid en hun eigen instellingsstrategie, de CISO werkt voor beide instellingen. Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening te garanderen.

Binnen de organisaties wordt informatiebeveiliging bewust breed geïnterpreteerd. Zo zien de HvA en UvA een belangrijke relatie en een gedeeltelijke overlap met andere beleidsterreinen, namelijk privacy, safety, security (fysieke beveiliging) en personeelsbeleid. Het doel van het informatiebeveiligingsbeleid is het bieden van een kader, het stellen van normen, het nemen van verantwoordelijkheid en voldoen aan compliance.

**Security principes** Daarnaast hebben de HvA/UvA een aantal security principes genoemd in hun beleid. Deze principes vormen de algemene regels en richtlijnen voor het gebruiken van de inzet van de architectuur van de informatievoorziening van de organisatie. De security principes zijn als volgt:

1. Informatiebeveiliging is proportioneel met de risico's
2. Beveiligen is standaard vanaf het ontwerp – *security-by-design and security-by-default*
3. Gelaagde verdediging – *layered defense*
4. Alleen toegang na expliciete toestemming
5. Veilige hardware en software
6. Traceerbare gegevensverwerking
7. Informatie is geclassificeerd
8. Op kwetsbaarheden wordt gescand en op aanvallen wordt gemonitord

**Lessons learned Universiteit Maastricht** De HvA en UvA hebben met belangstelling gekeken naar de evaluatie en aanbevelingen die vanuit de ransomware-aanval bij de Universiteit Maastricht zijn opgesteld. Gekeken is of de aanbevelingen toepasbaar zijn op de eigen instellingen. Zo is vanaf de dag van de aanval op de Universiteit Maastricht per direct gecontroleerd of back-ups voldoende zijn afgeschermd. Daarnaast is een aanvullend leerpunt het inrichten van een eigen SOC. Het SOC van de HvA/UvA is in de tweede helft van 2020 actief geworden. Om te voorkomen dat aanvallers over veel data kunnen beschikken is een ander leerpunt om in de in uitvoering zijnde netwerksegmentatie versneld verder te implementeren. De HvA/UvA hebben dit opgenomen in het verbeterplan informatiebeveiliging en een aantal punten zijn geheel of gedeeltelijk opgepakt.

**Verbeterplan informatiebeveiliging** In het ICTS verbeterplan informatiebeveiliging 2020 – 2022 zijn preventieve, detectieve, responsieve en organisatorische maatregelen benoemd. Uit de leertafels en interviews komen vanuit meerdere respondenten signalen naar voren dat een deel van de aanbevelingen voor Maastricht zijn opgenomen in het verbeterplan informatiebeveiliging. Een groot deel van deze aanbevelingen besteedt veel aandacht aan de technische security maatregelen op informatiebeveiliging. Uit de interviews en leertafels blijkt dat minder aandacht is besteed aan de governance en cultuur - thema's die terugkwamen in de aanbevelingen vanuit Universiteit Maastricht. Meerdere mensen geven aan dat vertraging in de uitvoering van het verbeterplan informatiebeveiliging zit. Zo heeft de cyberaanval plaatsgevonden in een onderdeel van een netwerk dat nog niet in zones is opgedeeld. Het is logisch dat een verbeterplan een continu doorlopend proces is, maar het is van belang dat gewerkt wordt met een prioritering in uitvoering. De verantwoordelijkheid voor de maatregelen/verbeterpunten ligt bij verschillende organisatieonderdelen, waardoor niet duidelijk is of de risicoafweging voor het wel of niet uitvoeren van projecten en actiepunten integraal wordt gemaakt.

| | |
|---|---|
| **Leerpunten** | - Benoem eigenaren voor actiepunten waarbij de verantwoordelijkheid nog niet goed belegd is. Dit eigenaarschap zorgt ervoor dat iemand verantwoordelijk is voor zijn/haar lopende deelprojecten/maatregelen.<br>- Voer een integrale risicoafweging uit voor projecten/actiepunten die nog niet zijn uitgevoerd, zodat duidelijk wordt welke projecten/actiepunten een hoge prioriteit hebben en pas waar nodig de planning aan.<br>- Voeg leerpunten uit deze evaluatie toe aan al bestaande verbeterplannen, zodat een eenduidig overzicht aanwezig is van te nemen maatregelen en acties. |
| **Vasthouden** | - Blijf actief leren van incidenten en crises bij anderen (zoals is gedaan n.a.v. de situatie in Maastricht).<br>- Blijf werken met leidende principes en draag zorg voor dat deze breed bekend en doorleefd zijn. Ga in dialoog na of de betrokken professionals hiermee uit de voeten kunnen.<br>- Blijft actief aandacht besteden aan een samenhangend programma voor informatiebeveiliging. |

## 3.3 Voorbereiding op incidenten

In paragraaf 3.2 is de verschillende planvorming beschreven. Een draaiboek voor een grotere aanval met rolverdeling SOC, CERT en Prio 1-team is niet aanwezig. Hier kunnen deels andere plannen voor gebruikt worden. Wel geven respondenten aan dat het behulpzaam kan zijn als het scenario 'grotere aanval' een eigen draaiboek krijgt, zodat de rolverdeling helder is. Bij dit type cyberincidenten is de rolverdeling tussen de technische teams nu niet altijd duidelijk. De organisatie heeft veel ervaring met IT-storingen en met kleinere cyberaanvallen. Er is een responsorganisatie en -procedure voor Prio 1-situaties. In die gevallen is ICTS in de lead.

**Crisisoefeningen** Crises worden structureel beoefend binnen de HvA en UvA. Jaarlijks trainen en oefenen centrale en decentrale crisisteams met verschillende scenario's. Niet alle scenario's zijn cyber gerelateerd, maar dit toont wel een mate van ervaring binnen de organisaties. Daarnaast hebben de crisisteams van de HvA en UvA in de afgelopen tijd ervaring opgedaan door de coronapandemie.

In het verleden hebben de teams meegedaan aan de OZON-oefening. Dit is een grootschalige cyberoefening voor het hoger onderwijs, waarbij het functioneren van de keten is getest en de effectiviteit van de interne communicatie is getoetst.[2] De aanbevelingen uit 2018 zijn in gezamenlijkheid opgepakt. In de tabel hebben we de belangrijkste verbeterpunten samengevat:

| Verbeterpunten vanuit de OZON 2018 oefening |
|---|
| - Verbeter de kennisoverdracht van technische security teams naar het tactische en strategische niveau.<br>- Zorg voor basis-cybersecuritykennis op tactisch en strategisch niveau om de communicatie en het begrip van tactisch en strategisch niveau richting operationeel niveau te verbeteren en onderhoudt deze kennis op alle fronten (inhoud-crisiscontext-communicatie).<br>- Verzamel best practices voor crisismanagement in het geval van cybercrises.<br>- Zorg voor genoeg technische security kennis en vaardigheden op operationeel niveau om een cybercrisis het hoofd te kunnen bieden.<br>- Maak afspraken over rolverdeling en kennisdeling binnen de sector tijdens een crisis.<br>- Bekrachtiging van het niveau waarop de crisisorganisatie actief is naar stakeholders (bijvoorbeeld een duidelijke start CCT en het markeren begin en einde 'crisis').<br>- Verklein de fysieke afstand tussen verschillende betrokkenen.<br>- Ontwikkel een scenariokaart 'cyber' dat handvatten biedt. |

De verbeterpunten zijn grotendeels doorgevoerd en deze voorbereidingen zijn ook benut tijdens de aanval. De kennisoverdracht van security teams naar het tactische en strategische niveau is verbeterd door de teams via de BOB-methode te laten vergaderen. Specifiek tijdens deze crisis is ingezet om de technische taal te simplificeren zodat ook het strategische niveau de situatie goed begreep. De basis-cybersecuritykennis op tactisch en strategisch niveau is tijdens de aanval ingeregeld door zowel de directeur ICTS als de CISO deel te laten nemen aan de CCT-vergaderingen. Op operationeel niveau (SOC/CERT) is voldoende technische kennis aanwezig. Het ontwikkelen van de cyber-scenariokaart, waar onder meer best practices in komen te staan, is stil komen te liggen en nog niet verder opgepakt.

**Assetmanagement** Een belangrijk knelpunt tijdens het incident is assetmanagement. Binnen zowel de HvA als UvA is geen volledig overzicht van de verschillende assets en prioriteiten. Tijdens de aanval is geen goed zicht op en overzicht van de assets. Dat zorgt ervoor dat de responsorganisatie 'dubbelblind' is, doordat niet bekend is welke assets geraakt kunnen worden en welke processen/applicaties hieraan gekoppeld zijn. Dit is tijdens de aanval zo goed mogelijk inzichtelijk gemaakt. De CISO geeft aan dat in het assetmanagement-proces informatie ontbreekt over de aanwezigheid van systemen, hun eigenschappen en het eigenaarschap, waardoor tijdens de uitvoering van de crisisrespons kostbare tijd verloren is gegaan met het uitzoeken van deze informatie. Aanvullend komt het (technisch security) crisisteam meerdere malen voor verrassingen te staan omdat

[2] Het COT is betrokken bij de observatie van de oefening en het opstellen van de aanbevelingen.

nieuwe (onbekende) systemen worden gevonden, als ook systemen met verouderde software en onbekende accounts.

Fox-IT geeft aan dat één van de grootste voordelen van goed assetmanagement is dat tijdens een grootschalig incident inzage is in welke systemen in een netwerk aanwezig zijn. Dit overzicht kan dienen als checklist waarmee bijgehouden kan worden welk systeem wel of nog niet is onderzocht, kwetsbaar is of op welk systeem mitigatiemaatregelen zijn toegepast. Zonder die inzichten kan het significant langer duren een incident onder controle te krijgen.

**Multifactor-authenticatie (MFA)** De CISO geeft aan dat de initiële toegang van de aanvallers is verkregen via een ontvreemde gebruikersnaam en wachtwoord. Het huidige aanvalsscenario is niet succesvol als de instellingen MFA ingesteld hebben. MFA vereist dat de gebruiker, naast gebruikersnaam/wachtwoord, tevens beschikt over de additionele factor zoals een (software) token of biometrisch id. Dit maakt het voor aanvallers vele malen moeilijker misbruik te maken van een gecompromitteerd account. Uit input van sleutelfunctionarissen volgt dat de kans op succes door *password spraying*, waarmee meerdere accounts zijn gekraakt, eveneens kleiner is bij het gebruik van sterkere unieke wachtwoorden. *Password spraying* is een techniek waarlangs met eenvoudige of voor de hand liggende wachtwoorden achter het wachtwoord van een of meerdere accounts te komen is. Een goed wachtwoordbeleid voorziet in passende vereisten voor authenticatie.

**Capaciteit** Een aandachtspunt is de capaciteit van de security teams: het CERT en het SOC zijn slagvaardige en compacte teams. Een moeilijkheid is het tijdig kunnen afwisselen. Het is belangrijk om deze groep te vergroten met het oog op de toename van de digitalisering van het onderwijs. Eerder is een bewuste keuze gemaakt in de inzet rondom monitoring. Uit de leertafels en interviews zijn signalen naar boven gekomen dat de security organisatie overvraagd wordt. Dit is ook het geval tijdens de respons op de aanval. In het Prio 1-overleg van 25 februari spreekt men hier zorgen over uit. Hoewel de afdelingshoofden is gevraagd om te gaan werken in meerdere shifts tijdens de respons, is dit in de praktijk niet gelukt omdat alle capaciteit en expertise tegelijkertijd nodig is.

| | |
|---|---|
| **Leerpunten** | - Leg de rolverdeling voor SOC/CERT/Prio 1 vast voor het scenario 'grotere aanval'.<br>- Actualiseer de draaiboeken op de breedte van integrale veiligheid.<br>- Beoordeel met de security teams of de gemaakte keuze rondom monitoring nog passend is in het licht van het huidige risicolandschap.<br>- Zorg voor een dekkend assetmanagement dat centraal benaderbaar is. Maak een overzicht van de verschillende assets en prioriteer deze op basis van de doelstellingen van de organisatie en de rol van de assets daarin. Van belang hierbij is ook inzicht in de processen die hieraan gekoppeld zijn.<br>- Herijk het bedrijfscontinuïteitsplan (BCP) wanneer uit assetmanagement blijkt dat assets in het BCP missen.<br>- Voer MFA in op alle diensten voor alle gebruikers conform het autorisatiebeleid.<br>- Organiseer werksessies voor de verschillende security en ICTS teams om de onderlinge communicatie en rolverdeling te bespreken en vast te leggen.<br>- Houd oog voor het welzijn van medewerkers en ga regelmatig het gesprek aan of ze hulp nodig hebben, aangezien de capaciteit beperkt is. |
| **Vasthouden** | - Blijf investeren in monitoring en detectie en de andere ingezette maatregelen.<br>- Blijf (cyber)crisissituaties beoefenen met elkaar. Zorg dat de leerpunten uit die oefening belegd worden binnen de organisatie.<br>- De benodigde capacitaire inspanning bij een langdurige respons en hersteloperatie is groot. Blijf bewust van dit inzicht, zowel de voorbereiding als voor het inrichten van de respons. |

## 3.4 De aanval en aanvallers

**De aanval op de laptop** Fox-IT heeft sporen aangetroffen waaruit blijkt dat op 11 februari 2021 de laptop slachtoffer is van malware, specifiek een "*trojan horse*". Dit stuk malware is de start van het verdere compromitteren van de laptop. De aangetroffen malware richt zich op diverse zaken, waaronder het verkrijgen van inloggegevens en andere informatie.

**De aanval op de HvA/UvA** Uit het onderzoek van Fox-IT en het CERT blijkt dat op 12 februari, binnen 24 uur na de aanval op de laptop, de eerste verkenningen zijn gedetecteerd op de Citrix omgeving, waarbij buitgemaakte inloggegevens van de laptop zijn misbruikt.

Na deze initiële tests begint kort na middernacht op zaterdag 13 februari de daadwerkelijke aanval. Binnen enkele minuten wordt contact gezocht met een *Command and Control server*, waarvandaan verschillende bestanden worden gedownload. Uit analyse van een achtergebleven bestand wordt duidelijk dat daarmee nieuwe kwaadaardige code in het geheugen geladen wordt. De aanval op de laptop en de aanval op het HvA/UvA netwerk is door twee verschillende actoren uitgevoerd.

In drieënhalf uur tijd vinden er verschillende verkennende handelingen plaats voordat de eerste *password spraying attack* begint. Deze aanval is een van de meest in het oog springende indicatoren van de kwaadaardige activiteiten. Deze eerste *password spraying attack* wordt een kleine twee uur later opgevolgd door een tweede aanval, ditmaal vanaf een andere Citrix server. Na deze aanvallen is het de aanvaller gelukt gebruik te maken van ten minste 1 beheeraccount om vanuit Citrix toegang te krijgen tot onder andere de Scripting server.

Uit het onderzoek van het CERT en Fox-IT blijkt dat de aanvaller zich via verschillende routes door het IT-landschap verspreidt. Fox-IT identificeert de omvang van het incident. Daarbij constateren ze dat ten minste 11 gebruikersaccounts, waarvan 10 beheeraccounts, 62 systemen en alle 3 de domeinen (*hva.nl, uva.nl* en *foret.nl)* in de infrastructuur van de instelling zijn gecompromitteerd.

Op basis van de logs van Azure ATP heeft het SOC tevens geconstateerd dat in ten minste twee gevallen met Windows Management Instrumentation (WMI) is gepoogd om op afstand code uit te voeren. Er is succesvol misbruik gemaakt van WMI.

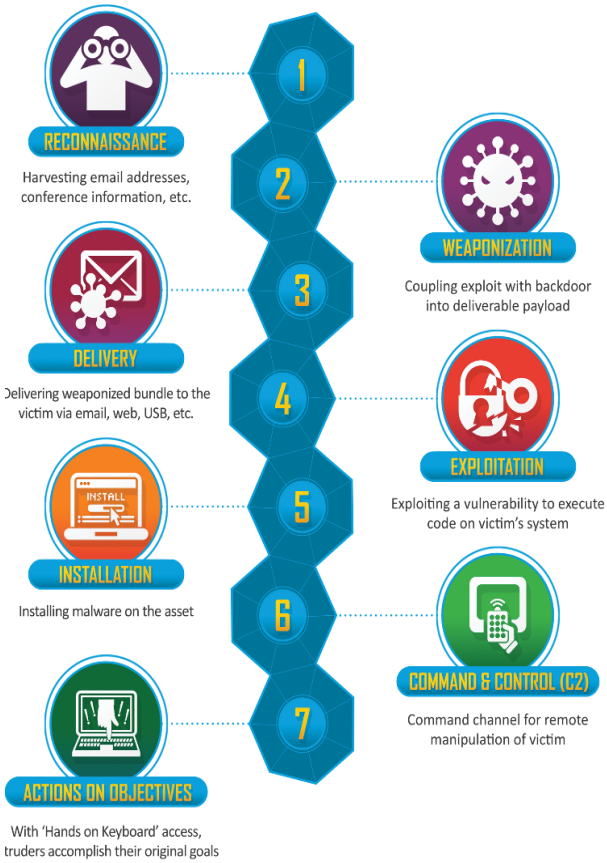
Fox-IT geeft aan dat de aanvaller op ten minste drie manieren toegang heeft weten te bemachtigen tot gebruikersgegevens. De aanvaller heeft een kopie gemaakt van de Active Directory-domeindatabase. Deze database bevat o.a. inloggegevens zoals gebruikersnamen en wachtwoord-hashes, e-mailadressen en telefoonnummers.

Het SOC van de HvA en UvA signaleert de aanval op maandagochtend 15 februari. Uit het technische onderzoek blijkt dat de aanval op de HvA/UvA waarschijnlijk uitgevoerd is door een andere actor dan de actor die de laptop heeft gecompromitteerd. Er is vooralsnog geen bewijs dat deze twee actoren aan elkaar te linken zijn.

**Cyber kill chain** Bij een cyberaanval wordt gesproken van een zogenaamde *cyber kill chain* van zeven stappen (zie afbeelding).[3] De CISO heeft het voor het CCT teruggebracht naar vier stappen: verkennen, eerste vorm van binnendringen, persistence en aanval. De eerste drie stappen zijn door de aanvallers uitgevoerd op het moment dat de aanvallers door het SOC worden gedetecteerd. De laatste stap 'de aanval' (in het plaatje stap 7) heeft niet plaatsgevonden. De uitleg van de *cyber kill chain* door de CISO is een goed voorbeeld van de verkleinde afstand tussen technische en strategische wereld.

[3] Ontwikkeld door Lockheed Martin. C2 = Command & Control: het daadwerkelijk toegang hebben en kunnen 'controleren'.

**Scenario's** De technische en bestuurlijke scenario's zijn terugvechten, systemen offline/afsluiten of zelf een nieuwe omgeving creëren. Bij de keuze voor het scenario is ook de strategie op de besturing (impact en bedrijfscontinuïteit) en de communicatie (stakeholdermanagement en community) onderdeel van gesprek en meegewogen. Deze drie scenario's zijn uitgewerkt en besloten is om terug te vechten. De andere twee scenario's zijn besproken, maar de inschatting is dat er nog steeds grote risico's zijn waardoor ze niet als realistisch worden gezien. In paragraaf 3.10 wordt verder ingegaan op de scenario's.




**Uitkomst technisch onderzoek** Uit het technische onderzoek blijkt dat in totaal 62 servers zijn gecompromitteerd. Daarbij zijn ten minste 11 gebruikersaccounts, waarvan 10 beheeraccounts en alle 3 de domeinen in de infrastructuur van de instelling zijn gecompromitteerd. Gesproken wordt van gecompromitteerd als:

- gebruikersaccounts gebruikt zijn door de aanvaller;
- er op systemen code is uitgevoerd door de aanvaller;
- de aanvaller toegang heeft weten te bemachtigen tot een account met (domein)-beheerdersrechten.

De aanvaller heeft in ieder geval gebruikersinformatie en netwerkinformatie benaderd.

Fox-IT stelt op basis van onderzoek niet met zekerheid vast te kunnen stellen wie de aanval heeft uitgevoerd. De conclusie van de CISO en het CERT is dat met middel tot grote zekerheid vastgesteld kan worden welke aanvaller de HvA/UvA heeft aangevallen. Fox-IT beschouwt het als uiterst onwaarschijnlijk dat de aanvaller die achter de besmetting van de laptop zit dezelfde is als de latere aanvaller bij de HvA/UvA. De tweede aanvaller heeft als doel om ransomware te installeren en start die route door eerst zoveel mogelijk informatie te vergaren over het Active Directory-domein en de trust-relaties tussen de domeinen. Er is geen verklaring waarom de aanvaller koos voor de HvA/UvA, anders dan toeval, voortkomend uit de gecompromitteerde gegevens van patiënt-0.

**Geen 'strijd'** De aanvallers kunnen weten dat ze gedetecteerd zijn doordat de HvA en UvA al eerste maatregelen hebben getroffen, zoals het wijzigen van enkele wachtwoorden. De aanvallers hebben na de genomen eerste maatregelen door de HvA en UvA geen verdere actie ondernomen. De inschatting vanuit Fox-IT is dat de aanvallers mogelijk hun aandacht hebben gericht op een ander slachtoffer om mogelijk later terug te keren naar de HvA/UvA.

**Risico's hoger onderwijsinstellingen** De openheid van de organisatie met verschillende devices, wachtwoorden van studenten/medewerkers, bring your own device etc. brengt een risico met zich mee waar alle hoger onderwijsinstellingen last van hebben. De HvA/UvA is zich hier bewust van.

| | |
|---|---|
| **Vasthouden** | - Tijdige attributie (waar mogelijk): dit biedt houvast bij het inschatten van de mogelijke ernst en impact en de mogelijke vervolgdreiging.<br>- Het uitleggen van technische aspecten in begrijpelijke taal om zo de security en bestuurlijke wereld dichter bij elkaar te brengen. |

| | |
|---|---|
| | - Het bepalen van het dominante scenario: dit biedt houvast in de aanpak en maakt focus mogelijk.<br>- Het blijven investeren in het SOC en CERT. |

## 3.5 Signalering en incident respons

**Signalering door het SOC** Op 15 februari 2021 is de verdachte situatie opgemerkt door het SOC. Rond 9.00 uur wordt in de weekstart van het SOC gemeld dat er verdachte zaken gezien worden. Het SOC analyseert de situatie en verifieert bij Change Management of de vrijdag ervoor changes zijn uitgevoerd die deze activiteiten verklaarden. Dat is niet het geval. Hierdoor weet het SOC zeker dat dit een aanval is. Het SOC beschikt over een goed situationeel bewustzijn, dit volgt uit het feit dat zij het verband hebben kunnen leggen tussen meerdere signalen. Door de vroege signalering en genomen maatregelen hebben cruciale systemen kunnen doordraaien. Het SOC heeft daarnaast goed doorgezet na de signalering en de ernst weten over te brengen in de lijn. Het SOC geeft aan geen barrières te voelen bij het melden en escaleren.

**Verdere opschaling in de IT-respons** Om 10.30 uur informeert het SOC het CERT. Om 11.00 uur vindt het eerste crisisoverleg plaats tussen functionarissen van het SOC, CERT en Serverbeheer. Rond 11:45 uur belt het CERT de CISO. De CISO belt vervolgens met de Directeur ICTS. De opschaling van het CERT naar de CISO om 11.45 uur wordt opgevolgd door twee Prio-1 vergaderingen om 12.30 uur en 14.30 uur. Om 13.25 uur zijn de bestuurders van de HvA en UvA ingelicht door de CISO en Directeur ICTS. Om 15.30 uur is een breder overleg met betrokken bestuurders en andere functionarissen. Direct volgt het besluit om een samengevoegd CCT in te zetten voor de incident respons. De HvA en UvA schakelen daarnaast op 15 februari Fox-IT in.

**Eerste maatregelen** Vlak na de eerste signalering van de aanval op maandag 15 februari voert het CERT de eerst defensieve acties uit. Dit betreft het wijzigen van wachtwoorden en het blokkeren van een aantal beheeraccounts die gecompromitteerd zijn. De rest van de ochtend werken de teams aan het verkrijgen van een beter inzicht. Om te zien of de aanvaller zich nog in het netwerk bevindt of nieuwe aanvallen uitvoert, wordt de monitoring uitgebreid. Met de eigen monitoringtools heeft het SOC (vooralsnog) te beperkt zicht. Fox-IT adviseert op 15 februari om netwerk monitoring tools aan te sluiten, dit loopt vanaf 16 februari. Fox-IT adviseert daarnaast op 16 februari om een Fox-IT detectietool op servers te gebruiken. Dit wordt de dagen erna geïnstalleerd op de Windows-servers.

**Samenspel security teams** De rolverdeling tussen de betrokken security teams is niet direct duidelijk maar krijgt gaandeweg steeds meer vorm en is effectief. Binnen de HvA en UvA is geen eenduidige werkwijze voor de respons op cybersecurity-incidenten. Er is geen incident-responsplan aanwezig. Hierdoor ontstaan onduidelijkheden over de verdeling van de inhoudelijke rollen en dat leidt tot een zoektocht die extra tijd en energie heeft gekost. Zo heeft het actieve Prio 1-team mede tot doel om het CERT te ontlasten en de verbinding te leggen met de verschillende betrokken IT-professionals breed in de organisatie. De samenwerking tussen het CERT en serverbeheer loopt op momenten niet soepel: ook hier moet een goede rolverdeling gevonden worden en moet de aanwezige expertise optimaal worden samengebracht.

Een groot aantal specialisten werkt hard, zowel aan de respons als aan mitigerende maatregelen, vervanging van de wachtwoorden en het herstel. Het CERT-team (5 à 6 medewerkers), SOC (4 medewerkers) en serverbeheer hebben met elkaar alle zeilen bijgezet om de aanval af te wenden, waarbij ook de betrokkenheid en inzet van de ICTS Security Officers en Security Managers van belang is. Het is voor de medewerkers een uitdaging om dagelijks goed in beeld te krijgen welke servers precies geraakt waren en om dit beeld bij te houden.

Over en weer zijn vragen over de rol- en taakverdeling. Het SOC neemt de coördinatie op zich waarbij de CISO nauw de ontwikkelingen volgt. Het SOC heeft al snel de coördinatie bij het CERT neergelegd vanwege de werkdruk. Het CERT heeft een uitgebreid mandaat in de incident respons, waaronder het

rode knop-mandaat (het stopzetten/offline halen van systemen etc.). Achteraf – na het incident – moet het uitvoeren van het mandaat verantwoord kunnen worden. Tijdens deze aanval is het CCT tijdig geïnformeerd en geconsulteerd waar nodig.

**Bewuste externe hulp ter aanvulling** De directeur ICTS heeft op maandag 15 februari het besluit genomen om Fox-IT als externe security partner in te zetten. Dit is een bewuste keuze om een second opinion, hulp bij attributie en inzet voor schaarse forensische expertise te krijgen. De inzet van externe expertise versterkt daarnaast de interne advieskracht. De rolverdeling tussen de interne organisatie en Fox-IT is volgens sommige medewerkers niet altijd helder. Het CERT is in the lead voor de incident respons. Echter onderhoudt ICTS ook (andere) communicatielijnen met Fox-IT. Dit leidt in sommige gevallen tot onduidelijkheid bij het CERT en andere functionarissen. Terugkijkend zijn de organisaties tevreden over de externe hulp, ook als het gaat om het proces en de focus.

**Een tweede incident** Naast de hack komt een tweede incident aan het licht: er zijn kwetsbaarheden ontdekt bij de Microsoft Exchange Servers die actief worden misbruikt door statelijke actoren. Dit incident speelt internationaal. Deze Microsoft Exchange situatie zorgt voor een complicatie: het lukte beperkt om dat op te lossen. Er ontstaat spanning tussen CERT en de Windows experts binnen ICTS over de aanpak en over factoren die de situatie bemoeilijkt. Het serverbeheerteam heeft een update niet uitgevoerd, waardoor ze achterlopen. Een snelle patch is hierdoor niet mogelijk. Doordat de Exchange acceptatie-omgeving instabiel is geworden door de hack en het forensisch onderzoek is ook een upgrade niet mogelijk. De CISO en ICTS besluiten om de tijdelijk on-hold gezette migratie naar de Cloud, versneld te af te ronden, waardoor de on-premise Exchange omgeving niet meer nodig is. De migratie brengt risico's met zich mee, maar een upgrade on-premise brengt meer risico's met zich mee vanwege de langere doorlooptijd. De CISO en ICTS zijn het daarover eens en om die reden wordt gekozen voor de versnelde migratie. Het CCT stemt in met de versnelde mail-migratie naar de Cloud.

**Toewerken naar sein 'brand meester'** In de dynamiek van een cyberaanval is één van de uitdagingen het bepalen van het moment waarop het weer veilig genoeg is. Er blijven altijd onzekerheden en risico's. Dit is heel doeltreffend geadresseerd in deze situatie. Op verzoek van het CCT is gekeken naar een situatie waar naartoe kan worden gewerkt richting een sein 'brand meester' en afschaling. In totaal zijn na uitgebreid overleg 10 randvoorwaarden benoemd waaraan voldaan moet worden om het sein 'brand meester' te kunnen geven (zie kader).

**Kader voor vaststellen 'brand meester'**

1. Enige mate van zekerheid dat de aanvaller niet meer binnen is.
2. Enige mate van zekerheid dat de aanvaller zich geen toegang kan verschaffen.
3. Detectie en monitoring dusdanig op orde dat mogelijke aanvallen door deze aanvaller kunnen worden gedetecteerd.

De daar bijpassende actiepunten luiden als volgt:

1. Alle Microsoft servers zijn geanalyseerd (beperkt aantal forensisch onderzocht)
2. Exchange mail omgeving is veilig
3. Office365 is veilig
4. Inhoud van de Account databases zijn te vertrouwen
5. ADFS (SSO oplossing Microsoft) is te vertrouwen
6. Noodcompartimentering van de serveromgeving
7. Alle Microsoft servers zijn voorzien van Intrusion Detection software
8. Citrix omgeving gecontroleerd, gemonitord
9. Continuïteit SOC (7x10 uur)
10. Serverhardening (lateraal bewegen van aanvaller voorkomen)

| | |
|---|---|
| **Leerpunten** | - Maak duidelijke afspraken met een externe partij over de rol- en taakverdeling om deze expertise nog beter in te zetten.<br>- Maak crisisteams bewust van de bestaande planvorming (zoals Prio 1 Handboek) en werk volgens deze planvorming. Het CERT is volgens deze planvorming verantwoordelijk voor de incident respons.<br>- Zorg naast de technische respons voor een goede procesaansturing als het gaat om focus, scenario's, rolverdeling en het monitoren van de voortgang. |
| **Vasthouden** | - Goede monitoring en tijdige detectie.<br>- Houd het werken met vaste thema's en periodieke updates over feitelijke situatie en stand van zaken van acties vast.<br>- Het uitwerken van de 10 punten voor 'brand meester' is een voorbeeld van een uitgewerkt kritiek besluit: dit geeft richting en houvast in de besluitvorming en vergemakkelijkt de dialoog tussen de security experts en het crisisteam. |

## 3.6 Crisismanagement

**Opschaling en rolverdeling CCT** Beide besturen zijn op 15 februari 2021 direct (rond 13.30 uur) geïnformeerd zodra de aanvallers door het SOC gesignaleerd zijn en de eerste acties zijn uitgezet. Kort hierop vindt de eerste CCT-bijeenkomst plaats. Beide bestuurders nemen deel, evenals de Secretarissen van beide instellingen, de directeur ICTS, de CISO, de woordvoerder en de plotter. De crisisorganisatie is op basis van de opgave aangevuld met benodigde expertise. In het CCT is gekozen om zowel de Directeur ICTS als de CISO onderdeel van het CCT te maken. Het werken met een gecombineerd HvA/UvA CCT is als positief ervaren.

**Rolverdeling CISO en directeur ICTS** De rolverdeling tussen CISO en directeur ICTS is helder en de samenwerking is complementair binnen het CCT. Door de CISO in het CCT te hebben is een directe lijn gecreëerd tussen CISO en CCT, dit werkt prettig en efficiënt. Zowel de HvA als de UvA hebben eerder incidenten gehad waarbij de CISO een sleutelrol vervult tussen beide organisaties. Het feit dat de vergaderingen digitaal plaatsvinden, biedt in dat opzicht een uitkomst, omdat de CISO en Directeur ICTS makkelijker aan alle vergaderingen deel kan nemen. Het blijft een uitdaging om zicht te houden op de totale operatie, waaronder serverbeheer, gelet op het grote aantal betrokkenen en acties.

**Vergadercyclus** Het CCT vergadert de eerste dagen zo'n drie keer per dag vanwege het hoge aantal te nemen besluiten om de aanval te weren en de impact te beperken. Daarnaast wordt door alle teams hard gewerkt in het verkrijgen van een overzicht van de ernst van de aanval. Dit is van belang voor het CCT om een weloverwogen en snel besluit te kunnen nemen. Een nadeel van virtueel vergaderen is dat geen flipovers aanwezig zijn om het overzicht te bewaren van de situaties. Een benoemd leerpunt door secretarissen en bestuurders is het werken met 'situatierapporten': een document met een overzicht van de stand van zaken en de belangrijkste acties. Tussen de crisisteams gaat het werk in hoog tempo door. Dit vergt van CCT-leden om binnen korte tijd besluiten te nemen zodat de andere teams weer verder kunnen. En het vergt van de voorzitter veel vragen stellen en een check doen op eerdere punten waardoor een duidelijk overzicht gewenst is.

**Vergaderen op afstand** De vergaderingen van het CCT en de andere teams vinden grotendeels plaats in Microsoft Teams. Het virtuele vergaderen bevalt over het algemeen goed, het maakt het voor functionarissen makkelijker om bij meerdere teams aan de sluiten. De security teams zullen normaal gesproken vaker bij elkaar naar binnen lopen. Het virtuele afstemmen maakt het omgaan met de spanning van de dreiging wel lastiger, omdat minder informele momenten plaatsvinden om te 'ontluchten'.

**Kernteams A & B** Het is vanwege de complexiteit van de crisis ingewikkeld om zicht te krijgen op de feiten en de aanwezige en mogelijke impact op de organisaties. Doordat al snel blijkt hoe groot de ernst van de aanval is, hebben de secretarissen van beide instellingen twee kernteams rond het CCT

ingericht ter ondersteuning. Op 17 februari komen zij met een nieuw voorstel voor de wijze van organiseren: CCT + Kernteams A en B voor bedrijfscontinuïteit en impact van de aanval. Team A voor impact en Team B voor het uitwerken van het 'zwarte scenario' waarin "alle schermen op zwart" gaan. Dit wordt de eerste dagen gevoeld als een reëel scenario.
Ze bespreken naast de eigen impact ook de impact op partners (zoals bijvoorbeeld de Vrije Universiteit waar cijfers en opleidingen gezamenlijk zijn opgezet en organisaties als Amsterdam University College (AUC) en de Academisch Centrum Tandheelkunde Amsterdam (ACTA)) en hoe dit is opgepakt.
Op 18 februari wordt het plan voor de crisisorganisatie verder uitgewerkt. De rolverdeling tussen het CCT en de kernteams is helder verwoord en neergezet. Er is een plan voor een Kernteam C met verschillende adviseurs (waaronder de FG's), maar de conclusie is dat vanuit dit team geen verdere actie benodigd is.

**Besluitvorming CCT** Het CCT heeft gedurende de aanval meerdere sleutelbesluiten genomen. Onder andere:

- Terugvechten ('enige reële scenario');
- Wijze van communiceren (transparant maar 'geminimaliseerd'; meenemen maar geen paniek, in- en externe stakeholders op de hoogte houden en de community);
- Wijzigen wachtwoorden en 'wachten' tot organisatie er klaar voor is;
- Bepalen en communiceren sein 'brand meester'.

De besluiten zijn door het CCT steeds zorgvuldig genomen door consequent de volgende stappen te doorlopen: eerst de randvoorwaarden op orde, dan pas het besluit nemen en communiceren. Zo heeft het CCT besloten om de wachtwoorden gefaseerd aan te passen en niet in een keer. Dit is technisch gezien niet mogelijk/te zwaar voor het systeem om te verwerken. Als een groot aantal netwerkgebruikers tegelijk hun wachtwoord aanpast, dan verstoort de activiteit die hierdoor op het netwerk wordt veroorzaakt het onderzoek van het incident en het herstel van de infrastructuur. Daarnaast vergt het organisatorisch te veel.

**Bescherming gebruiker** Tijdens de CCT-vergadering op 18 februari worden de consequenties voor de gebruiker besproken waar de laptop van gecompromitteerd is. Daarnaast is direct aandacht voor de zorg van de gebruiker. Besproken wordt dat diegene uitleg dient te krijgen over het proces, dat een nieuw account wordt aangemaakt en dat de gecompromitteerde laptop wordt omgeruild voor een nieuwe. Ook wordt besproken dat de gebruiker goed beschermd moet worden, zijn/haar naam mag niet bekend worden om privacy te kunnen borgen.

**Wachtwoord wijzigen** Het CCT heeft weloverwogen het besluit genomen om de wachtwoorden te wijzigen, wetende dat de gebruikers belast zouden worden met dit besluit. Het gaat in totaal om het wijzigen van 177.000 wachtwoorden. Het besluit gaat verder dan alleen mensen informeren: ze moeten ook het belang inzien van het wijzigen van het wachtwoord, zodat ze daadwerkelijk actie nemen. Er zit daarnaast een harde deadline op: als het te lang duurt, wordt het account geblokkeerd. De ICTS Service Desk heeft hierin een belangrijke taak gehad en meegeholpen om het wijzigen van de wachtwoorden in goede banen te leiden. In totaal zijn circa 140 medewerkers van onder meer UB/AC en andere afdelingen ingezet voor de Service Desk. Deze medewerkers zijn binnen twee dagen opgeleid en ingeroosterd.

Bestuurlijk wordt daarnaast het risico gevoeld dat het enige tijd kost (van vrijdagmiddag tot woensdag uiteindelijk) voordat de randvoorwaarden op orde zijn (o.a. Service Desk instellen). In de tussentijd kan de aanvaller misbruik maken van de wachtwoorden. Dit levert voor het CCT lastige vragen op: wat als studenten/medewerkers schade oplopen?

**Continuïteit Administratief Centrum** De continuïteit van de kritische systemen die het Administratief Centrum nodig heeft om dienstverlening uit te kunnen voeren, is van belang. Zo moeten studenteninschrijvingen doorgaan, de jaarrekening verder opstellen en facturaties en salarisbetalingen plaats vinden. Het Administratief Centrum is direct na de eerste signalen van de aanval zaken gaan veiligstellen voor de komende periode (o.a. jaarrekeningen, kopie salarisadministratie). Het CCT is

hierover geïnformeerd. Vanuit de eigenaar (Administratief Centrum) van het systeem is de impact bepaald voor de organisatie als de Windows SAP-systemen worden uitgezet en is voor een workaround gezorgd. De Windows SAP-systemen worden vervolgens uitgezet.

**Trots, maar realistisch over het risico** Terugkijkend zijn de deelnemers trots op de interne samenwerking en op de samenwerking tussen beide instellingen. De bereidwilligheid om te helpen is groot, waardoor iedereen het gevoel heeft het samen te doen. De bestuurders hebben duidelijke keuzes gemaakt, ondanks de complexe situatie. Daarnaast is iedereen trots op de security teams: SOC/CERT/ICTS/Prio 1 en de CISO. Door iedereen is hard en goed gewerkt, waardoor grote schade is voorkomen. Tijdens het incident weten de afdelingen elkaar goed te vinden, waardoor sprake is van een integrale aanpak voor security. Deelnemers realiseren zich dat nog steeds kwetsbaarheden aanwezig zijn en dat voldoende leerpunten te halen zijn uit het incident en de respons.

| | |
|---|---|
| **Leerpunten** | - Zorg voor zicht op feiten van de aanval (de actuele situatie). Zeker indien de vergaderingen virtueel plaatsvinden. |
| **Vasthouden** | - Ga per crisissituatie na of de juiste functionarissen in het CCT zitten. Vul expertise aan indien nodig, zoals bij deze situatie is gedaan.<br>- Durf de structuur aan te passen aan de opgave. Houd rekening met noodzaak van aanvullende teams om te voorkomen dat druk op CCT te groot wordt (ook bij andere type crisis).<br>- Houd de mogelijkheid open om te werken met virtuele crisisteamvergaderingen. Maak bewuste keuzes over benodigde fysieke momenten.<br>- Houd aandacht voor de zorg van de betrokkenen gedurende het hele proces. |

## 3.7 Communicatie

**Crisiscommunicatieteam** De detectie van de aanval is op 15 februari jl. Woordvoering is vanaf het begin betrokken bij het CCT. Op 16 februari is het crisiscommunicatieteam geactiveerd en op 17 februari wordt de aanval intern richting medewerkers en studenten bevestigd. Deze berichtgeving vindt plaats via een bericht op de website, waardoor het bericht direct extern zichtbaar is. De daaropvolgende periode verstuurt het team updates via sociale media, de websites van HvA en UvA worden FAQ's aangevuld. De onzekerheid over de omvang en de duur is het grootste knelpunt in de eerste dagen. Uit voorzorg worden vier communicatieteams (zowel vanuit HvA als UvA) geactiveerd die elkaar om de dag afwisselen. Als blijkt dat het worst case scenario ("alle schermen op zwart") zich niet ontvouwt, blijven twee crisiscommunicatieteams actief die elkaar om de week afwisselen.

In een subteam wordt nagedacht over alternatieve communicatiemiddelen als e-mail, intranet en andere reguliere, digitale kanalen onverhoopt niet meer toegankelijk zijn. Hoewel de onzekerheid over de omvang en de duur in de eerste dagen de opschaling van vier communicatieteams (40 communicatieprofessionals) rechtvaardigt, brengt dit veel coördinatie met zich mee. Bovendien is het niet bevorderlijk als andere crisisteams dagelijks met wisselende gezichten te maken hebben. Daarnaast neemt communicatie deel aan het CCT. De koppeling met het communicatie-uitvoeringsteam werkt goed.

**Beperkte zorgen en onrust** De onrust onder medewerkers en studenten blijft (zeer) beperkt. Op bestuurlijk niveau wordt snel gekeken naar de rol van communicatie in de crisis. In het CCT wordt met de woordvoerder beoordeeld hoe de HvA en UvA in deze crisis willen communiceren. Vanuit de communicatieprofessionals is met het CCT (en vanuit deelname aan het CCT) strategisch nagedacht over de toon van berichtgeving: het moet voor begrip vanuit de organisatie zorgen, omdat een aantal processen vertraagd zal zijn.


Er wordt nagedacht over de interne en externe 'tone of voice' en de mate van betrokkenheid, waarbij communicatie een belangrijke adviesrol heeft in het CCT. Daarnaast lijkt de beperkte onrust het effect te zijn van een heldere communicatieaanpak en de beperkte (zichtbare) impact op de continuïteit van onderwijs en onderzoek. De context speelt ook mee; in dezelfde periode trekken cyberaanvallen bij andere organisaties (bijv. Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO)) de aandacht en hebben nieuwsmedia hun handen vol aan de politiek in aanloop naar de Tweede Kamerverkiezingen.

**Wachtwoordwijziging** Na het besluit van het CCT om de wachtwoordwijziging in gang te zetten, heeft het crisiscommunicatieteam het CCT op de hoogte gebracht van hun aanpak. Een belangrijk aandachtspunt is dat gebruikers weinig hinder ondervinden van de aanval, maar wel het belang in moeten zien van een wachtwoordwijziging. Het complexe landschap zorgt er bovendien voor dat via veel verschillende kanalen gecommuniceerd moet worden om alle betrokkenen binnen een paar dagen tijd te bereiken. Op 23 februari stuurt het CvB een e-mail naar alle medewerkers en studenten met het verzoek om het wachtwoord te wijzigen. De mail wordt in batches van 10.000 per instelling per uur verstuurd. Ook via sociale media komen oproepen voor wachtwoordwijziging. Op 1 maart zijn 70.000 wachtwoorden gewijzigd. Op 3 maart is dit aantal fors opgelopen en zijn 153.000 wachtwoorden gewijzigd. In totaal moeten 177.000 wachtwoorden worden gewijzigd.

**Overzicht kernboodschappen**

**17 februari –** "Onbekende derden hebben zich toegang verschaft tot de ICT-omgevingen van de HvA en UvA, dat heeft het Security and Operations Center van de HvA en UvA geconstateerd. Maatregelen zijn en worden getroffen om de gevolgen te beperken en te zorgen dat onderwijs en onderzoek zoveel mogelijk ongestoord doorgang kan vinden.

Om de impact op ons onderwijs en onderzoek zo veel mogelijk te beperken, zullen we de komende tijd proactief systemen tijdelijk uitzetten. Deze systemen en de informatie in die systemen zijn op dat moment niet beschikbaar. We begrijpen dat dit overlast geeft en proberen dit zoveel mogelijk te beperken.

In het belang van het onderzoek kunnen we nu niet verder ingaan op de achtergrond en omvang van deze aanval. De laatste informatie vind je op uva.nl en hva.nl of op services.hva.nl en services.uva.nl."

**22 februari –** "Er wordt achter de schermen hard gewerkt om de gevolgen van de cyberaanval te beperken. Met name bij ICT Services zijn medewerkers meer dan fulltime bezig om te zorgen dat onderwijs en onderzoek

zo goed mogelijk doorgang kunnen vinden. De Colleges van Bestuur spreken hun grote dank en waardering uit naar iedereen die meehelpt om de hinder van de aanval te beperken. Aan alle medewerkers en studenten vragen we hier de updates te volgen en hun mailbox in de gaten te houden. Blijf ook alert op phishing."

**10 maart –** "Door monitoring en snelle reactie is serieuze cyberaanval afgeslagen. Tot een gijzeling of verzoeken om losgeld is het niet gekomen. Onderwijs en onderzoek hebben geen hinder ondervonden. Verder onderzoek (o.a. politie) loopt."

Terugkijkend heeft het crisiscommunicatieteam snel, transparant, proportioneel en feitelijk gecommuniceerd. Het team heeft prettig samengewerkt met ICTS en spreekt ook waardering uit voor de daadkracht van het CCT. Het crisiscommunicatieteam is daardoor goed in staat om de technische informatie te vertalen naar impact op medewerkers en studenten. Afstemming met de politie vindt plaats over de communicatieboodschap en timing rondom de aangifte en het sein 'brand meester'.

**Empathie** Uit de gesprekken en leertafels blijkt een grote tevredenheid over de communicatie. Zowel intern als extern is redelijk de rust bewaard. De Q&A op de website is helder en feitelijk. Wel wordt aangegeven dat het in de communicatie gewenst is om op sommige momenten meer empathie te tonen. Crisiscommunicatie bestaat uit drie pijlers, ook wel het IBS-model genoemd: informatievoorziening, betekenisgeving en schadebeperking. De crisisorganisatie heeft zich tijdens deze crisis met name gericht op informatievoorziening (wat is er aan de hand?) en schadebeperking (wat is het handelingsperspectief om schade te beperken?). De pijler betekenisgeving (wat betekent dit voor studenten, medewerkers en de organisatie?) gaat over empathie en aansluiten op het sentiment dat leeft. Ruimte voor verbetering zit in het segmenteren van doelgroepen waarbij meer 'betekenisgeving' van toepassing is. Zo ervaren medewerkers die veel met SAP werkten meer hinder dan overige medewerkers. Een empathische boodschap (op maat) is dan passend. Empathie in de crisiscommunicatie hoeft niet alleen met woorden overgebracht te worden, maar kan ook door middel van vorm. Zo wordt de communicatie tijdens de cyberaanval vooral geuit in tekst, terwijl een persoonlijke videoboodschap van een bestuurder (over het belang van digitale veiligheid) ook uiting kan geven aan betekenisgeving.

**Procesupdates** Diverse medewerkers geven aan dat ze in het vervolg graag meer procesupdates ontvangen: wat is de huidige status? Wat betekent sein 'brand meester'? Waar hebben we nog last van de komende periode? Medewerkers denken dat het na het sein 'brand meester' klaar is, maar er zit nog een langere periode van herstelwerkzaamheden in waar zij eventueel hinder van kunnen ondervinden.

**Nieuwe communicatieprofessionals** Verschillende (nieuwe) communicatieprofessionals die een rol hebben tijdens deze crisis zijn nog onbekend met de crisiscommunicatie werkwijze van de HvA en UvA. Zij zijn met een instructie aan de slag gegaan en hebben hun rol goed vervuld. Om ook in de toekomst goed uit de startblokken te komen bij een (potentiele) crisis is het verstandig om te blijven investeren in het opleiden van nieuwe medewerkers. Investeer met name in het trainen van goede omgevingsanalisten. Als zij weten welke (in- en externe) informatie nodig is, hoe zij deze informatie kunnen ophalen en hoe zij deze informatie moeten duiden, dan vormt dat de basis voor een krachtige communicatiestrategie.

| **Leerpunten** | - Beperk de organisatie van de crisiscommunicatie tot twee teams die enkel werken aan de crisis en elkaar om de 4 á 7 dagen afwisselen.<br>- Ga per situatie na op welke wijze empathie in de communicatie overgebracht kan worden. Dit kan door middel van woorden, maar ook door vorm om zo een passend niveau van betrokkenheid/begrip over te brengen.<br>- Geef waar mogelijk procesupdates aan de organisatie, zodat ze weten wat er in grote lijnen speelt. |
|---|---|

| | |
|---|---|
| **Vasthouden** | - Houd de strategische advies rol van het crisiscommunicatieteam binnen het CCT vast.<br>- Blijf de strategie expliciet maken zodat iedereen deze kent.<br>- Blijf investeren in het opleiden van nieuwe medewerkers (dit geldt breder dan alleen communicatie). |

## 3.8 Informatiemanagement

**Complexe uitdaging** Informatie speelt een belangrijk rol tijdens crisis. Dit gaat onder meer over het tijdig delen van informatie en het vervolgens – in samenhang – duiden hiervan als input voor besluitvorming en acties. Hoe meer professionals betrokken zijn, hoe groter de uitdaging om tot tijdige en correcte uitwisseling van informatie te komen. De crisisvergaderingen zijn digitaal: dit zorgt voor een grotere uitdaging omdat sleutelfunctionarissen elkaar niet fysiek ontmoeten en zo de kleine momenten voor controle/uitwisseling missen. De verslaglegging is een extra uitdaging als digitaal wordt gewerkt: het kan goed gaan, maar het vergt goede afspraken op welke wijze verslaglegging plaatsvindt en waar functionarissen de informatie terug kunnen vinden. Geheel gezien verloopt het informatiemanagement goed. HvA/UvA beschikken niet over een ondersteunend systeem/applicatie voor informatiemanagement tijdens crisis, dit kan helpen in het creëren van een eenduidig informatiebeeld.

**Vertaalslag technische informatie** De CISO en het CERT fungeren als belangrijke schakels tussen de verschillende teams – zowel in de respons als in het verder uitwisselen van informatie met andere teams. De CISO maakt de vertaalslag van de technische situatie en informatie voor het CCT en de overige teams. Zo heeft de CISO een overzichtelijke uitleg van de *cyber kill chain* gegeven en verteld hoe de aanval verloopt. Dit overzicht is gewenst om de brug te slaan tussen de daadwerkelijke technische informatie en gevolgen en consequenties voor de bestuurlijke wereld.

**Kernteams A & B** De kernteams A en B krijgen een eigen opdracht om continuïteits- en impactvraagstukken op te pakken en uit te werken. Deze opdrachten zijn door het CCT uitgezet. De informatiebehoefte voor beide teams is hoog. De teams benutten informatie vanuit de organisatie om tot scenario's te komen. Zo wordt een overzicht gemaakt welke processen als kritisch worden beschouwd bij het overgaan naar een ander systeem. Informatie om deze scenario's uit te werken is echter versnipperd. Teams A en B ervaren een gevoel van terughoudendheid om technische informatie op te halen bij de CISO, gelet op de reeds grote belasting. Naast de verslaglegging van het CCT is er geen structureel overzicht met relevante informatie. Wel hebben alle teams die afstemmen in Prio 1 een eigen Teams-omgeving waar documentatie gedeeld kan worden. De kernteams A en B waren veel tijd kwijt aan het ophalen van relevante informatie vanuit de lijn voor het uitwerken van scenario's.

**Informatiebehoefte** De informatiebehoefte op faculteitsniveau is hoog. Naast de centrale berichtgeving en terugkoppeling hebben een aantal faculteiten de berichtgeving 'door vertaald' naar de eigen organisatie. Een voorbeeld hiervan is de impact van het uitvallen van systemen op faculteitsniveau. De informatievoorziening richting faculteiten is zorgvuldig. De faculteiten worden via de BVO/CBO-update op de hoogte gehouden. De CISO heeft vanuit het technische perspectief elke dag een bijpraatmoment met de informatiemanagers van de faculteiten om de situatie verder toe te lichten. Er zijn daarnaast regelmatig bredere momenten waarin updates worden gegeven aan verschillende interne stakeholders (technisch/gebruikers).

Niet alle informatie kan breed gedeeld worden. Hierbij is het onderscheid tussen *need to know* en *nice to know* relevant. Een factor is dat informatie niet bij de hacker terecht mag komen en/of een onbedoeld effect heeft op de situatie, omdat bijvoorbeeld anderen eventuele kwetsbaarheden kunnen misbruiken.

**Afstemming teams** Een aandachtspunt met betrekking tot de vergaderstructuur is het moment van CCT-vergaderingen en de invloed daarvan op de informatievoorziening naar andere teams. Het CCT vergadert gedurende de respons in verschillende frequenties. In het begin is dit logischerwijs frequenter dan later in de tijd. Het CCT vergadert op een gegeven moment s 'middags omdat ze dan

meer informatie beschikbaar hebben om snel besluiten te kunnen nemen. Dit heeft indirect gevolgen voor andere teams, zoals het crisiscommunicatieteam. Uit de leertafels blijkt dat zij vaak nog na het CCT-overleg berichten uitwerken. Uiteindelijk komt door het tijdstip van de CCT-vergadering een extra druk op dit team om op dezelfde dag nog te communiceren.

| | |
|---|---|
| **Leerpunten** | - Deel informatie structureel via dezelfde tools/ middelen.<br>- Stem een standaard tijdstip af voor de dagelijkse informatiedeling om te voorkomen dat dit ad-hoc plaatsvindt. Bij urgente ontwikkelingen volgt waar nodig ad-hoc aanvullende informatie.<br>- Toets periodiek de informatiebehoefte van de stakeholders in de crisis- en reguliere organisatie. |
| **Vasthouden** | - Deel informatie op basis van een *need to know* en *nice to know* classificatie.<br>- Blijf technische informatie vertalen in begrijpelijke taal voor andere crisisteamleden. |

## 3.9 Breder stakeholder management

**Interne organisatie** Het is belangrijk om de rest van de organisatie te betrekken zodat ze de ernst van de situatie begrijpen en de mogelijke lange duur van de implicaties van de cyberaanval en de genomen maatregelen. Door de crisisrespons ondervinden andere IT-projecten/trajecten vertraging. Ook leveranciers nemen contact op. Voorlopig is alle inzet nodig op het bestrijden van de aanval.

Met behulp van verschillende communicatielijnen worden stakeholders geïnformeerd. Het CCT informeert naast de studenten en medewerkers ook het RvT, de Centrale Medenzeggenschapsraad (CMR), de Centrale Ondernemingsraad (COR) en de Centrale Studentenraad (CSR). De informatievoorziening richting het RvT wordt als volledig ervaring.

**Extern stakeholdermanagement CCT** Naast dat het CCT haar interne stakeholders met regelmaat op de hoogte houdt van de stand van zaken met betrekking tot de aanval, informeert het CCT ook externe stakeholders. Dit zijn onder meer het ministerie van Onderwijs, Cultuur en Wetenschap, de inspectie, andere instellingen waar nauwe contacten mee zijn geïnformeerd, zoals de Vrije Universiteit van Amsterdam en de gemeente Amsterdam. Daarnaast heeft de CRIM afstemming met de politie voor de aangifte. Daarnaast heeft het High Tech Crime van de politie de HvA/UvA doorverwezen naar een specialist binnen de eenheid. Ook is contact opgenomen met het NCSC.


Afbeelding: overzicht interne en externe stakeholders

**Stakeholdermanagement CISO en ICTS** Vanuit de CISO en ICTS is een dagelijks een bijpraatmoment met een groep interne stakeholders. De CISO informeert de FG's, de Faculty Information Managers (FIM), Faculty Information Security Officers (FISO), Privacy Contact Persons (PCP) en andere interne stakeholders. Daarnaast informeren de CISO en het CERT de overige vertrouwde partners zoals SURFcert, SURF Community van Incident Response Teams (SCIRT), NCSC en CISO's van andere universiteiten en hogescholen. Ondanks alle drukte (vanwege NWO hack) hebben de HvA/UvA hulp vanuit SURFcert gekregen. De samenwerking met SURFcert verliep goed.

**Geen actieve inmenging** Tijdens de leertafels benoemen deelnemers dat het prettig is dat de stakeholders hen de ruimte geven en zich niet actief mengen in het incident.

**Delen lessons learned** Een advies dat medewerkers vanuit de gesprekken en leertafels meegeven, is om de lessons learned van deze aanval met andere instellingen te delen net als Maastricht destijds gedaan heeft. De HvA en UvA hebben vanuit de ervaringen en leerpunten van de Maastricht-casus binnen de eigen organisatie wijzigingen doorgevoerd. Mogelijk kunnen de lessons learned vanuit de HvA/UvA-hack input zijn voor reflectie vanuit andere instellingen op de eigen weerbaarheid en voorbereiding.

| | |
|---|---|
| **Leerpunten** | - Update de lijst met belangrijk(st)e stakeholders bij dit soort type incident.<br>- Vraag expliciet naar de informatiebehoefte bij deze (externe) partners. |
| **Vasthouden** | - Houd vast aan het tijdig en breed informeren van stakeholders. Dit geeft vertrouwen.<br>- Benut de gemaakte overzichten van stakeholders (bestuurlijk en technisch) en leg deze vast in de voorbereiding op mogelijke crisis. Ga ook voor andere crisistypen na welke bijzondere (andere) stakeholders er zijn. |

## 3.10 Situationeel bewustzijn & scenariodenken

**Scenariodenken** Tijdens de respons is continu aandacht voor het denken in scenario's en het verkrijgen van een gedeeld situationeel beeld.

Tijdens het tweede CCT-overleg op 15 februari zijn drie scenario's besproken:

1. Systemen uitzetten/alles offline: Alles van het internet afsluiten en systemen uitzetten om te behoeden dat deze geraakt worden door de aanvaller;
2. Ratrace/terugvechten: Direct counteren van de activiteiten van de aanvaller met de mogelijkheid dat de aanvaller zich terugtrekt en dat systemen nog te redden zijn;
3. In stilte een nieuwe omgeving opbouwen: Niet reageren op de aanval, maar observeren wat er gebeurt en parallel een nieuwe omgeving opbouwen.

Terugvechten brengt het risico met zich mee dat de hacker escaleert en versnelt alsnog de data van de HvA en UvA gijzelt. Dit risico is met Fox-IT besproken en samen zijn de scenario's verder uitgewerkt. Het vergt beslissen in onzekerheid, omdat niet bekend is hoe ver de hacker al is en de instellingen willen de hacker niet verstoren. Fox-IT helpt bij het scherp krijgen van de scenario's en het houden van focus. Samen stellen ze een duidelijk doel vast, kiezen een scenario (terugvechten) en monitoren dit scenario. Volgens de betrokkenen is 'terugvechten' het enige realistische scenario. De impact van scenario 1 is zeer groot en scenario 3 is geen optie omdat al tegenacties zijn uitgevoerd, zoals het blokkeren van misbruikte beheeraccounts en het resetten van wachtwoorden. Verder kost scenario 3 veel tijd en capaciteit en blijven de instellingen kwetsbaar.

Bestuurlijk is daarnaast het scenario ransomware 'verkend'. De secretarissen hebben een eerste kader uitgewerkt, maar de situatie is nooit zover gekomen. Het is van belang om dit scenario met elkaar uit te denken, vooral wat betreft de uitgangspunten en de te doorlopen stappen om tot zorgvuldige besluitvorming te komen.

De Kernteams A en B nemen een aantal fall back scenario's door voor het geval dat de reguliere contactmethoden uitvallen: wat is het alternatieve kanaal dat beschikbaar is voor de gehele organisatie?

**Prioritering activiteiten** Tijdens de leertafels is het belang van prioritering/uitgangspunten benoemd. Zo is besproken dat de continuïteit van onderwijs voorrang krijgt op andere activiteiten. Het uitvallen van de Active Directory werd als hoogste risico ingeschat en als prioriteit gezien. Als deze wegvalt valt de bedrijfsvoering weg. Deze inzichten heeft Team B geholpen om in de beperkt beschikbare tijd goed op de juiste zaken te kunnen focussen. Een ander benoemd uitgangspunt is dat financiën geen drempel vormen in de besluitvorming. Teams hebben hierdoor acties ondernomen die logisch worden geacht, zonder tegen het obstakel van financiën aan te lopen.

| | |
|---|---|
| **Leerpunten** | - Bespreek sectoraal wat het scenario ransomware betekent voor hoger onderwijsinstellingen en hoe de instellingen hiermee omgaan.<br>- Ontwikkel een afwegingskader en een procesbeschrijving over hoe om te gaan met besluitvorming bij ransomware mocht dit zich voordoen. |
| **Vasthouden** | - Houd het werken met basisscenario's en het maken van expliciete keuzes vast.<br>- Het ontwikkelen van fallback-scenario's voor de uitval van reguliere contactmethoden en communicatiemiddelen.<br>- Benut de uitgewerkte scenario's en uitgevoerde inventarisaties en analyses als input voor het versterken van het continuïteitsmanagement. Houd het benoemen van prioriteiten en uitgangspunten vast. |

## 3.11 Privacy

**Melding AP** Op 16 februari jl. wordt duidelijk dat de aanvallers toegang hebben tot de ID's en versleutelde wachtwoorden van studenten en medewerkers. De verzameling die is buitgemaakt door de aanvaller, onder andere email adressen, studentennummers en telefoonnummers, worden gezien als een set van persoonsgegevens volgens de Algemene Verordening Gegevensbescherming (AVG). Hierdoor is het belangrijk dat de FG van de HvA en de FG van de UvA in stelling worden gebracht en advies geeft over privacy gerelateerde zaken. De FG is de functionaris die binnen de organisatie toezicht houdt op de toepassing en naleving van de AVG. Daarnaast kwalificeert de hack als een datalek. De inbreuk op de beveiliging leidt tot ongeoorloofd toegang tot persoonsgegevens.
Vanuit de AVG zijn de HvA en UvA verplicht om uiterlijk binnen 72 uur na bewust worden van een inbreuk melding te maken bij de AP. De FG doet de voorlopige melding namens het bestuur van de HvA en UvA. In deze fase is het nog niet volledig duidelijk om hoeveel betrokkenen het gaat.

**Betrokkenheid FG's** Tijdens de aanval zijn de FG's geen vast onderdeel van het CCT of formeel agendalid. Hierdoor zijn ze niet direct op de hoogte van agendapunten en uitkomsten daarvan. Vanuit het CCT is het idee dat de FG's deel kunnen nemen aan het CCT indien nodig. De FG's kunnen hier voor hun gevoel niet actief op inspelen, doordat ze voorafgaand geen inzicht in de agenda hebben. Achteraf gezien vinden ook de functionarissen in het CCT het beter als de FG's betrokken zijn bij het CCT op momenten dat het over privacy-thema's gaat. Dit betekent niet dat de FG's standaard onderdeel zijn van het CCT, maar aansluiten wanneer nodig. De FG's zijn op bepaalde momenten betrokken en hebben tweemaal een adviesmemo geschreven voor het CCT, bijvoorbeeld met betrekking tot het wijzigen van de wachtwoorden.

De informatielijn tussen CCT en de FG's verloopt via de CISO en incidenteel via andere lijnen (zoals via de Secretarissen van HvA/UvA). De FG's ervaren dit als een kwetsbare structuur omdat de informatie-uitwisseling grotendeels afhankelijk is van één functionaris. Het is ook minder efficiënt aangezien het CCT en FG's niet direct schakelen met elkaar over privacy-kwesties.

**Definitieve melding AP** Na het sein 'brand meester' maken de FG's de definitieve melding bij de AP. De FG's schakelen proactief met de AP-inspecteur, onder andere over het verhoogde aantal betrokkenen. Vanuit de AP komen geen opmerkingen op de melding. Dit betekent dat de melding inhoudelijk goed is.

| | |
|---|---|
| **Leerpunten** | - Zorg voor duidelijke informatielijnen tussen functionarissen en CCT/andere functionarissen die in de crisis anders kunnen zijn dan bij reguliere besturing en spreek dit bewust af, zodat het niet afhankelijk is van één functionaris/functietitel.<br>- Identificeer hoe reguliere lijnen (bijv. tussen FG en CvB) beïnvloed worden bij het activeren van een crisisstructuur. Besteed aandacht aan de lijnen die herbelegd moeten worden. |
| **Vasthouden** | - Blijf de FG's actief informeren bij cyberincidenten.<br>- Breng de FG in stelling zodra sprake is van een privacy-incident/crisis.<br>- Behoud de mogelijkheid van het betrekken van de FG bij CCT-vergaderingen indien privacy een thema op de agenda is. Laat de FG hier proactief op anticiperen door de FG agendalid te maken van het CCT.<br>- Blijf het proces richting AP zorgvuldig doorlopen. |

## 3.12 Overgang naar de nafase/fase van herstel

**Sein 'brand meester'** Op 10 maart adviseert de CISO aan het CCT om het sein 'brand meester' te geven en het CCT neemt dit advies over. Uit input van de CISO volgt dat op dat moment aan één randvoorwaarde nog niet volledig voldaan is. De overgebleven punten worden als aanvaardbaar risico ingeschat. Aan randvoorwaarde 1 (alle Microsoft servers zijn geanalyseerd (beperkt aantal forensisch onderzocht)) is niet volledig voldaan; op 22 systemen na zijn alle Microsoft systemen onderzocht. Het gaat hierbij voornamelijk om test- en ontwikkelsystemen die voor een deel al herbouwd zouden worden, en indien ze geïnfecteerd blijken alsnog herbouwd moeten worden. Op 10 maart wordt het sein 'brand meester' gecommuniceerd op intranet, de nieuwsbrief en in de BVO/CBO-update. Stakeholders zijn op de hoogte gebracht. Daarnaast wordt een persstatement naar buiten gebracht.

**Nafase** De werkwijze voor de nafase is uitgewerkt en vastgesteld.

| **Afschaling** |
|---|
| Vanaf het moment van sein 'brand meester' gaat de crisisorganisatie een nieuwe fase in, 'fase 3'. Deze fase bestaat uit verschillende stappen:<br>- Stap 1: Afronden en technische analyse. Volledig schoonmaken van IT-systemen en nalopen om dit zeker te stellen. Opstellen rapport met technische analyse waarin o.a. de oorzaak, (technische) handelingen en systemenveiligheid wordt beschreven.<br>- Stap 2: Herstel - Herstel naar de normale situatie door herstel van onderdelen die zijn aangetast. Overdracht onderdelen naar verbeterplannen<br>- Stap 3: Verbeterplan - Verbeterplan opstellen op basis van de uitkomsten van de technische analyse. Ook moeten de verbeterpunten uit stap 2 opgenomen worden, inclusief prioritering: korte termijn realiseren en meerjarenplanning naar lijn brengen).<br>- Stap 4: Evaluatie en afronding - Evaluatierapport van totale crisisbestrijding met aanbevelingen. |

**Herstel en opbouw** Het sein 'brand meester' betekent niet dat het incident 'klaar' is. Naar de interne gebruikers is gecommuniceerd dat herstel en opbouw nog maanden in beslag kan nemen en gevraagd wordt om begrip. Aanvullende communicatie over de herstelperiode is gewenst, dat creëert meer begrip in de organisatie dat nog niet alles gelijk werkt en maakt duidelijk dat ICTS de komende maanden druk is met de herstelwerkzaamheden. Hierdoor is het mogelijk dat reguliere dienstverlening minder snel kan worden uitgevoerd. Met betrekking tot de maatregelen die genomen moeten worden

om de schade te herstellen, wordt een onderscheid gemaakt tussen quick wins – zoals de scheiding op servers – en maatregelen die langere tijd in beslag nemen.

| | |
|---|---|
| **Leerpunten** | - Geef procesupdates over de betekenis van sein 'brand meester' en de herstelperiode. |
| **Vasthouden** | - Houd het benoemen van randvoorwaarden voor het zorgvuldig kunnen bepalen wanneer een crisis 'voorbij' is en een volgende fase in kan gaan, vast. Benut dit bij andere crises (met voorwaarden die passen bij dit situatie).<br>- Houd het coördineren in de nafase / de fase van herstel vast. De scope en intensiteit hiervan kunnen per situatie verschillen. Maak op basis van een diagnose van de vraagstukken een bewuste keuze over de wijze van organiseren en de goede aansluiting met de staande organisatie. Leg vast wanneer de projectorganisatie 'klaar' is. |

# 4. Overkoepelende bevindingen en aanbevelingen

## 4.1 Inleiding

In eerdere hoofdstukken hebben we de crisisorganisatie en gebeurtenissen beschreven en daarnaast per thema de observaties gegeven en leerpunten benoemd. Op basis van deze hoofdstukken koppelen we in dit hoofdstuk onze overkoepelende bevindingen terug. We schetsen het overkoepelende beeld en benoemen de zogenoemde sleutelmomenten en sleutelbesluiten die mede de dynamiek hebben bepaald. Wij sluiten dit hoofdstuk af met enkele overkoepelende aanbevelingen.

## 4.2 Overkoepelend beeld

Op basis van alle gesprekken en leertafels komen wij tot het volgende overkoepelende beeld.

| Overkoepelend beeld |
|---|
| - De aanvallers zijn binnengekomen nadat malware gedownload wordt op een laptop een student. Er zijn gegevens gestolen op de laptop door een aanvaller en een andere aanvaller is daarmee binnengekomen en heeft steeds meer rechten verzameld.<br>- De impact van de aanval is relatief beperkt gebleven op onderwijs en onderzoek maar vergt een grote inspanning, ook in de nafase. Het gaat om een zeer risicovolle situatie waarvan de gevolgen veel ernstiger hadden kunnen zijn.<br>- De HvA en UvA zijn voortdurend bezig met het verbeteren van informatiebeveiliging. Naar aanleiding van de cyberaanval bij de Universiteit Maastricht zijn extra maatregelen getroffen en is aanvullende expertise aangenomen. Niet alle maatregelen zijn al geïmplementeerd op het moment van de aanval, en er zijn deels bekende en onbekende restrisico's.<br>- Er is sprake van breed gedeelde trots over de aanpak, maar ook realisme over het risico.<br>- Het is gelukt om de impact van de cyberaanval tot een minimum te beperken zowel in continuïteit als in vertrouwen.<br>- Er is door velen hard gewerkt om dit voor elkaar te krijgen. Veel mensen in de organisatie hebben bijgedragen, het commitment is groot. Tussen sleutelfunctionarissen zit onderling vertrouwen.<br>- De interne samenwerking is – enkele knelpunten daargelaten – effectief. Hierbij is op integrale wijze gewerkt (technisch, continuïteit, communicatie, juridisch, e.a.). Er is flexibel gereageerd op de opgave die voorligt.<br>- Vanwege beperkt zicht op een aantal zaken en beperkte uitwerking in draaiboeken moet veel worden geïmproviseerd. Dit is krachtig gebeurd vanuit ervaring en expertise.<br>- De kwetsbaarheid in Microsoft Exchange vraagt aanvullende inzet. Dit staat los van de hack, maar geeft extra druk en belasting.<br>- Specialisten zijn niet verrast dat een dergelijke aanval zich voor kan doen. Er waren en blijven kwetsbaarheden als het gaat om preventie en mitigatie, ondanks alle inspanningen. Respondenten benadrukken het belang van een paradigmashift naar cyberweerbaarheid. |

Iedere crisis heeft sleutelmomenten en sleutelbesluiten die van grote invloed zijn op het verloop van de situatie. In deze situatie zien wij de volgende sleutelmomenten en sleutelbesluiten:

| Sleutelmomenten | Sleutelbesluiten |
|---|---|
| - 'Binnenkomen' aanvallers en start tweede aanval<br>- Eerste attributie en aanvallen blokkeren<br>- Uitblijven nieuwe activiteit aanvallers<br>- Moment dat breed interne bekendheid is<br>- Eerste externe communicatie<br>- Reactie op verzoek wijzigen wachtwoorden<br>- Microsoft Exchange kwetsbaarheid | - Besluiten ombestuur bijeen te brengen<br>- Besluit van het CCT dat het een crisis is<br>- Eerste mitigerende/beschermende maatregelen<br>- CERT/SOC blokkeren admin-accounts<br>- Inschakelen aanvullende externe expertise<br>- 'Terug vechten'<br>- Communicatie uitgangspunten en strategie<br>- Versnelde migratie naar de Cloud (i.v.m. Microsoft Exchange) |

| | |
|---|---|
| - De start van de versnelde migratie naar de Cloud (i.v.m. de Exchange kwetsbaarheid)<br>- Moment dat sein 'brand meester' gegeven wordt<br>- Afsluitende communicatie 'brand meester'<br>- Het weer 'aanzetten' van servers in het kader van herstel<br>- Voorlopige en definitieve melding aan de AP. | - Wachten tot randvoorwaarden op orde zijn voor oproep vervangen wachtwoorden<br>- Vervangen van alle wachtwoorden medewerkers en studenten<br>- Het uitvallen van de Active Directory als hoogste risico benoemen<br>- Besluit benoemen randvoorwaarden voor sein 'brand meester'<br>- Sein 'brand meester' geven<br>- Afschalen crisisorganisatie en werken met projectorganisatie |

## 4.3 Bevorderende en belemmerende factoren

In hoofdstuk drie hebben we per thema observaties benoemd. Samenvattend zien we de volgende bevorderende factoren en belemmerende factoren:

| Bevorderende factoren | Belemmerende factoren |
|---|---|
| ✓ Eerder geleerd van Maastricht en aanvullend is actief contact gelegd met Maastricht op verschillende niveaus tijdens het incident<br>✓ Zelf gedetecteerd door het SOC en herkend als 'gevaarlijk'<br>✓ Aanwezige ervaring en expertise SOC/CERT/ICTS en bredere crisiservaring in organisatie<br>✓ Snel inschakelen extra externe expertise<br>✓ Goede samenwerking tussen beide organisaties HvA en UvA<br>✓ Zorgvuldige maar daadkrachtige besluitvorming. Duidelijke prioriteiten die worden gesteld<br>✓ Actief scenariodenken met duidelijke uitgangspunten<br>✓ Specifieke aandacht voor impact: continuïteit en 'zwart scenario'<br>✓ Gelukt om gezamenlijk het technisch-bestuurlijk gat te overbruggen en te werken aan gedeeld situationeel bewustzijn<br>✓ Beperkte aanvullende activiteit aanvallers en het uitblijven van gijzeling<br>✓ Effectieve, afgestemde externe communicatie<br>✓ Sterk opgeschaalde en goed functionerende servicedesk<br>✓ Tijdig en gericht informeren stakeholders: intern en extern. En steun van de stakeholders<br>✓ Op afstand kunnen werken met virtuele crisisteams<br>✓ Onderling vertrouwen<br>✓ Adequate melding aan de AP | × Maandag 'pas' ontdekt<br>× Rolverdeling CERT/ICTS/Prio 1 nog wat zoeken<br>× Beperkingen in beschikbare capaciteit voor technische coördinatie richting de organisatie<br>× Grote vermoeidheid mede vanwege lange duur en intensiteit<br>× Merendeel een digitale crisisrespons (vergaderingen via MS Teams) door Coronamaatregelen<br>× In operatie soms frustratie/botsing tussen specialisten<br>× Beperkt zicht op assets, de processen die verbonden zijn met deze assets en de impact erop: er moest veel nog in kaart worden gebracht tijdens de crisis<br>× Er waren interne kwetsbaarheden/ beperkingen die maken dat impact groot kan worden<br>× Een tweede incident: Microsoft Exchange<br>× Veel inspanning nodig om beeld actueel te houden in het CCT<br>× Afhankelijkheid informatielijn één functionaris/functietitel<br>× Interne informatiebehoefte vs beschikbare informatie<br>× Beperkt inzicht in besluitvorming/actiepunten van andere teams binnen de crisisorganisatie |

## 4.4 Overkoepelende aanbevelingen

De eerder benoemde belemmerende en bevorderende factoren bieden aangrijpingspunten voor het versterken van de voorbereiding en respons op cyberincidenten en dreigende (digitale) crises, zowel voor zaken die behouden moeten worden als zaken die verbeterd kunnen worden. In de eerdere paragrafen hebben we de leerpunten per thema benoemd. Wij sluiten deze rapportage af met enkele overkoepelende aanbevelingen.

1. **Maak lange termijn keuzes in het kader van cybersecurity.** Vergroot de weerbaarheid binnen de organisatie door het uitvoeren van de volgende stappen:
    - **a)** Stel met elkaar vast wat het risico is dat wordt gelopen op het gebied van cyber. Kijk hierbij naar het brede landschap van digitale risico's en dreigingen: van ransomware tot spionage.
    - **b)** Stel met elkaar bestuurlijk vast wat de mate van kwetsbaarheid is en wat een reëel niveau van beveiliging, mitigatie en voorbereiding op de respons is. Hierbij hoort ook een update van de *risk appetite* bij en het uitvoeren van assetmanagement. Benut hierbij de inzichten zoals benoemd door Fox-IT en door interne sleutelfunctionarissen.
    - **c)** Maak keuzes hoe om te gaan met het dilemma tussen de mogelijkheid van beveiliging en de praktische behoefte van docenten en studenten wat betreft gebruiksgemak. Voorbeelden hiervan zijn het al dan niet werken met MFA en hoe om te gaan met '*bring your own device'*.
    - **d)** Benut de opgedane ervaring als extra aansporing om naar integrale veiligheidsrisico's te kijken, waarvan informatieveiligheid, kennisveiligheid en privacy drie belangrijke thema's zijn.

2. **Benut ervaringen in de voorbereiding op nieuwe incidenten en dreigende crisis:**
    - **a)** Ontwikkel een draaiboek cyberincidenten (incidentrespons-plan)- en crisis met rolverdeling SOC/Prio 1/CERT, maar ook met aandacht voor impact & scenario's, monitoring, capaciteit, welke functionarissen aanvullend een rol hebben (bijv. bij privacyvraagstukken/dilemma's de FG betrekken) en stakeholders. Dit zorgt voor een eenduidige werkwijze in de respons op cyberaanvallen en gerelateerde cybersecurity-incidenten.
    - **b)** Versterk de voorbereiding in het kader van bedrijfscontinuïteit: maak gerichte keuze op welke onderdelen voorbereiding nodig is en waar improvisatie volstaat.
    - **c)** Oefen specifiek met cybercrises en maak het een gespreksonderwerp binnen teams.
    - **d)** Behoud de mogelijkheid van op afstand kunnen werken in crisisteams.
    - **e)** Verwerk de 'kleine' verbeterpunten in werkwijze crisismanagement onder meer rond het betrekken en informeren van agendaleden van het CCT.
    - **f)** Neem bij de werving van nieuwe professionals die een (potentiële) rol hebben in een crisisteam mee dat crisisvaardigheden van belang zijn voor de functie;
    - **g)** Behoud de mogelijkheid om met een scenario/impactteam te werken (ook bij andere type crises).

3. **Werk aan gerichte voorbereiding op de mogelijke situatie van ransomware en hoe te komen tot zorgvuldige besluitvorming** vanuit het uitgangspunt dat niet wordt betaald en tegelijkertijd vanuit de realiteit dat er extreme omstandigheden kunnen zijn waar dit uitgangspunt opnieuw getoetst moet worden.

4. **Deel de opgedane ervaringen** breed in de organisatie en met andere instellingen. Doe dit op de verschillende niveaus/vanuit verschillende functies (technisch, bestuurlijk en communicatief). Benut andere middelen om het 'verhaal' te vertellen zoals interviews met sleutelfunctionarissen en/of een animatie.

5. **Communiceer intern actief over de gemaakte keuzes rond cyberweerbaarheid en blijf in gesprek over de voortgang**. Betrek hierbij een brede vertegenwoordiging vanuit de organisatie professionals ervaringen, vragen en zorgen in kunnen brengen. Op deze wijze wordt duidelijk dat gewerkt wordt aan versterking en dat dit de verantwoordelijkheid van een ieder is.

# Bijlage 1 Aanbevelingen Fox-IT

Fox-IT heeft een aantal aanbevelingen benoemd. Fox-IT doet aanbevelingen om het beveiligingsniveau verder te verbeteren. De aanbevelingen betreffen aandachtspunten voor meerdere beveiligingsrisico's en zijn onderverdeeld in de categorieën Preventie, Detectie en Respons.

| | |
|---|---|
| **Preventie** | 1. **Multifactor-authenticatie.** Opdrachtgever gaf aan dat de Citrix-omgeving geen multifactor-authenticatie vereist. Voor het authenticatieproces zijn een gebruikersnaam en wachtwoord voldoende. Authenticatie op basis van alleen een gebruikersnaam en wachtwoord wordt onveilig geacht wanneer het een hoog-risico-omgeving betreft of wanneer de dienst vanaf het internet benaderbaar is. Het is aan te bevelen om dergelijke diensten/systemen te beveiligen door middel van multifactor-authenticatie.<br>2. **Wachtwoordsterkte en wachtwoordbeleid.** Fox-IT heeft door middel van tests op het Active Directory-databasebestand (dat alle gebruikersnamen en wachtwoorden bevat) vastgesteld dat een significant aantal gebruikersaccounts over een zwak wachtwoord beschikt. Het is van belang dat organisaties een wachtwoordbeleid configureren en afdwingen waardoor gebruikers periodiek wachtwoorden moeten wijzigen en welke gebruikers verplicht om sterke wachtwoorden te gebruiken.<br>3. **Netwerksegmentatie en -segregatie.** Fox-IT adviseert om de huidige netwerksegmentatie en -segregatie te inventariseren en een verbeterde inrichting, inclusief jumphosts, te realiseren, waardoor het voor aanvallers moeilijker gemaakt wordt om zich door het netwerk te bewegen.<br>4. **Publieke DNS- gegevens.** Fox-IT heeft geobserveerd dat een groot deel van de apparaten en systemen in het servernetwerk van Opdrachtgever zijn voorzien van een publiek IP-adres inclusief een bijbehorend publiek opvraagbare DNS-naam. De DNS-namen, in de situatie van Opdrachtgever, geven regelmatig prijs welke rol een systeem heeft. Fox-IT raadt aan om de huidige DNS-situatie te evalueren en daarbij te overwegen dit niet langer publiekelijk inzichtelijk te maken. |
| **Detectie** | 1. **Logboekregistratie.** Om de mogelijkheid te hebben om gedegen onderzoek te doen naar gebeurtenissen in het verleden raadt Fox-IT aan om op verschillende niveaus (systeem, netwerk, applicatie) voldoende logboekregistratie aan te brengen. Hierbij moet men denken aan voldoende bewaartermijn van de logboeken (retentie), maar ook voldoende detail in de logboekregistraties zelf. Idealiter loggen alle systemen naar een centrale plek waar de loggegevens gecorreleerd, gemonitord en veilig bewaard kunnen worden, zoals in een SIEM.<br>2. **Netwerkmonitoring.** Het continu monitoren van het netwerkverkeer waarbij de focus ligt op het detecteren van potentieel kwaadaardige activiteit, kan ervoor zorgen dat een aanval niet leidt tot een grootschalig security incident. Hierbij kan gebruik worden gemaakt van een groot aantal indicatoren die bij de aanwezigheid van malware op het netwerk een incident zouden veroorzaken. Fox-IT adviseert om ook voor de langere termijn een dekkende netwerkmonitoring-oplossing te implementeren en te (laten) onderhouden.<br>3. **Endpoint Detection and Response.** EDR-software kan per systeem in de gaten houden wat zich op dat moment op het systeem afspeelt en rapporteert dat terug naar een centrale console. Het kan gebruikt worden om securityincidenten al in een vroeg stadium op te laten vallen of om een al groter incident sneller inzichtelijk en daarmee sneller onder controle te krijgen. Fox-IT raadt aan om deze of een soortgelijke EDR-oplossing te hanteren of te implementeren, zodat nieuwe incidenten spoedig kunnen worden gesignaleerd en de kans dat deze uitmonden in een groter incident wordt geminimaliseerd. |
| ***Respons*** | 1. **Assetmanagement.** Het spoedig kunnen beschikken over actuele informatie zoals welke systemen binnen de IT-omgeving aanwezig zijn is tijdens incident response van groot belang. Een van de grootste voordelen van goed assetmanagement tijdens een |

grootschalig incident is inzage in welke systemen in een netwerk aanwezig zijn, waarbij zo'n overzicht kan dienen als checklist waarmee bijgehouden kan worden welk systeem wel of nog niet is onderzocht, kwetsbaar is of op welk systeem mitigatiemaatregelen zijn toegepast. Fox-IT adviseert om een assetmanagement-oplossing te implementeren en deze actueel te houden.

2. **Incident-response-plan.** Fox-IT heeft geobserveerd dat Opdrachtgever tijdens het incident niet de beschikking had over een incident-response-plan waar tijdens dit incident goed op teruggevallen kon worden. Een crisisteam was aanwezig, maar niet afgestemd op een inhoudelijke IT-security-crisissituatie. Fox-IT raadt aan om een incident-responseplan op te stellen, te onderhouden en te controleren op praktische uitvoerbaarheid door deze periodiek te (laten) toetsen.
3. **Geautomatiseerd kunnen beheren van systemen.** Improvisatie om op grote schaal systemen te kunnen aansturen kan tijdens een incident leiden tot vertraging bij het onder controle krijgen van het incident. Het georkestreerd aansturen van systemen kan ervoor zorgen dat een incident eerder onder controle komt door o.a. massaal EDR-software uit te kunnen rollen of bepaalde forensische sporen op te kunnen halen van diverse systemen.
4. **Back-up en herstel.** Het hebben van een goed back-up- en herstelplan is essentieel in de strijd tegen ransomware. Mocht ondanks alle preventieve maatregelen een aanvaller erin slagen ransomware uit te rollen dan is vaak de enige uitweg tot herstel het terugzetten van back-ups. Fox-IT adviseert om een back-up- en herstelplan op te stellen, waar offline back-ups onderdeel van zijn, en dit plan periodiek te (laten) toetsen op volledigheid en werkbaarheid.

# Bijlage 2 Afkortingenlijst

| Afkortingen | Betekenis |
|---|---|
| ACTA | Academisch Centrum Tandheelkunde Amsterdam |
| AIVD | Algemene Inlichtingen- en Veiligheidsdienst |
| AP | Autoriteit Persoonsgegevens |
| AUC | Amsterdam University College |
| BOGD | Bestuurlijk Overleg Gemeenschappelijke Diensten |
| BVO | Bedrijfsvoeringsoverleg |
| CBO | Centraal Bestuurlijk Overleg |
| CCT | Centraal Crisisteam |
| CERT | Computer Emergency Response Team |
| CISO | Chief Information Security Officer |
| CMR | Centrale Medenzeggenschapsraad |
| COR | Centrale Ondernemingsraad |
| CRIM | Chief Risk Insurance Manager |
| CSR | Centrale Studentenraad |
| CvB | College van Bestuur |
| DCT | Decentraal Crisisteam |
| FAQ | Frequently Asked Questions |
| FG | Functionaris Gegevensbescherming |
| FIM | Faculty Information Manager |
| FISO | Faculty Information Security Officer |
| ICTS | ICT Services |
| ISM | Information Security Manager |
| ISO | Information Security Officer |
| MFA | Multifactor-authenticatie |
| NCSC | Nationaal Cyber Security Centrum |
| NWO | Nederlandse Organisatie voor Wetenschappelijk Onderzoek |
| PCP | Privacy Contact Person |
| RvT | Raad van Toezicht |
| SCIRT | SURF Community van Incident Response Teams |
| SOC | Security Operations Center |
| WMI | Windows Management Instrumentation |

Het COT is een gespecialiseerd bureau op het gebied van veiligheids- en crisismanagement. Ons werkterrein strekt zich uit van vraagstukken over de vormgeving van veiligheidsbeleid tot de voorbereiding op crisissituaties. Met onze kennis en kunde helpen we opdrachtgevers in complexe situaties waarbij grote risico's worden gelopen, strategische belangen op het spel staan en vaak vele stakeholders zijn betrokken. Advies, onderzoek, en training en oefening vormen de basis van onze dienstverlening. Het COT is een volledige dochteronderneming van Aon Nederland.

Meer informatie: **www.cot.nl of cot@cot.nl.**

## Disclaimer leerevaluatie

Deze leerevaluatie is gebaseerd op informatie die ter beschikking is gesteld, en verkregen, tijdens de periode waarin de evaluatie is uitgevoerd. Nieuwe of aanvullende informatie kan van invloed zijn op de inhoud en de geformuleerde conclusies en aanbevelingen. Het COT beschikt alleen over informatie waar het rechtswege toegang tot heeft. Rapporten worden in beginsel in opdracht van de opdrachtgever gemaakt en niet gepubliceerd. Eén kopie wordt bewaard voor juridische, IT- en wetgeving- en toezichtdoeleinden.