Leerevaluatie ‘datalek september 2021’

Hogeschool Arnhem Nijmegen
1 maart 2022

Inhoudsopgave

Samenvatting

Op 1 september 2021 ontvangt de voorzitter van het College van Bestuur (CvB) van de HAN University of Applied Sciences (HAN) een dreigmail van een hacker. Deze hacker claimt data te hebben gestolen en eist een bedrag bitcoins. De crisisorganisatie van de HAN wordt snel opgeschaald en werkt hard om de situatie te duiden en de impact van het datalek te minimaliseren. Het lek is op 4 september 2021 gedicht. Binnen enkele weken is bovendien de volledige scope van het incident in beeld en zijn nagenoeg alle betrokkenen geïnformeerd, tot in 2022 lopen er nog enkele vervolgacties. De inzet en werkwijze van de crisisorganisatie is geëvalueerd, doel hiervan is het ophalen van leerpunten ten behoeve van versterking van de crisisorganisatie bij volgende crises.

Overkoepelend beeld

In de respons op deze crisis heeft de crisisorganisatie veel zaken goed opgepakt. Wij zien op enkele punten mogelijkheden om de respons te versterken met het oog op toekomstige crises. We hebben deze punten onderverdeeld in succesfactoren die hebben bijgedragen en aandachtspunten.

Succesfactoren:

- De snelle opschaling van het CMT;
- De goed werkende en geoefende crisisstructuur met een opgeschaald CMT en enkele gespecialiseerde ondersteunende teams;
- De duidelijk opgestelde uitgangspunten: ‘niet betalen’ en ‘transparant communiceren’;
- De externe expertise die is ingezet ter aanvulling op de experts uit de crisisorganisatie;
- De korte lijnen tussen betrokkenen en gezamenlijke momenten voor gemeenschappelijk beeld (zoals briefing afhandeling informeren betrokkenen en communicatieboodschap per groep betrokkenen);
- De inzet van één extern informatiekanaal: han.nl/datalek maakte duidelijk waar informatie beschikbaar was.

Aandachtspunten:

- Het volwassenheidsniveau van de HAN met betrekking tot privacy/AVG verdient aandacht;
- De afstemming van de informatiebehoefte van het CMT versus de uitvoeringstijd en de informatiebehoefte van de ondersteunende teams;
- In het verlengde van het vorige punt kan ook de terugkoppeling van besluiten en ratio hierachter van het CMT naar andere ondersteunende teams scherper. Denk hier bijvoorbeeld aan het besluit rond de inzet van externe expertise;
- Het ontbreken van planvorming met betrekking tot het afhandelen van grote hoeveelheden verzoeken van betrokkenen bij een crisis als deze;
- Het zicht van een aantal betrokkenen op de hele crisisstructuur en verdeling van taken tussen teams; welke overleggen zijn er? Waar liggen de mandaten?

Aanbevelingen

Benut het ‘momentum’ van verhoogd bewustzijn ter versterking van de privacy volwassenheid en informatiebeveiliging van de HAN. De crisis toont enkele kwetsbaarheden van de HAN in relatie tot het thema privacy en cyber. Privacy is een thema dat doorlopend aandacht verdient. Alle medewerkers moeten doorlopend bewust zijn van de risico’s en hun eigen verantwoordelijkheid. De inspanningen van het team Techniek en de rapportage van Fox-IT maken daarnaast mogelijk enkele cybersecurity verbetermogelijkheden inzichtelijk.

Prepareer doorlopend op een crisis: investeer in continuïteitsmanagement, ontwikkel een draaiboek datalekken en een afwegingskader ransomware.

- **Continuïteitsmanagement** Maak de afhankelijkheden van IT voor de continuïteit van de organisatie inzichtelijk. Denk na over herstelmaatregelen en *workarounds* om eventuele verstoringen op te kunnen vangen. Het is belangrijk om hierop voor te bereiden in het kader van continuïteitsmanagement

- **Stel een draaiboek datalek op**. Neem in dit draaiboek o.a. de werkwijze rond het informeren van betrokkenen op, zorg voor een checklist met acties/maatregelen, stel vast welke functionarissen betrokken zijn en welke teams etc. Bereid medewerkers voor op deze onverwachte acute taak door het geven van een training of het houden van een intervisiesessie waarin de ervaringen van deze crisis gedeeld worden.
- **Stel een afwegingskader ransomware op.** In de eerste fase van deze crisis vroeg de hacker diverse keren om losgeld en zette de HAN onder druk. Doordat de continuïteit niet in gevaar was en omdat vrij snel duidelijk was dat het lek was gedicht, kon de HAN het zich permitteren hier niet op in te gaan. Niet betalen was ook een duidelijk uitgangspunt tijdens de crisis. Deze omstandigheden kunnen bij een volgende crisis afwijken. Daarom is het belangrijk om in de koude fase een afwegingskader te maken waarin voorzienbare dilemma's worden besproken en doorleefd. Denk hierbij ook na over de 'tenzij…', de uitzondering op het uitgangspunt om niet op eisen van een hacker in te gaan. Betrek bij het opstellen van dit kader belangrijke stakeholders (bijv. RvT vanuit hun adviserende/toezichthoudende rol).

Versterk de informatievoorziening naar ondersteunende teams en interne stakeholders.

- **Ondersteunende teams** Het CMT werd door de teams nadrukkelijk gevoed met informatie onder andere ten behoeve van besluitvorming. De informatie paste bij de vragen en verzoeken van het CMT. Een aandachtspunt is de terugkoppeling aan de ondersteunende teams van de genomen besluiten die voor hen relevant zijn of waarvoor zij informatie hebben aangeleverd. Zorg ervoor dat dit op gezette tijden voldoende wordt besproken, bijvoorbeeld door dit op te nemen als vast agendapunt en hier expliciet bij stil te staan. Dit leidt tot meer begrip over de uitvragen aan de ondersteunende teams. Ook stelt het de teams in staat om op basis van de ratio achter de genomen CMT-besluiten zelfstandiger te opereren. Voor dit laatste is het ook belangrijk om het mandaat van de ondersteunende teams nadrukkelijk te bepalen.
- **Interne stakeholders** De HAN hanteerde in de communicatie het duidelijke uitgangspunt: transparantie. De HAN gaf updates via een liveblog en betrok collega-instellingen nadrukkelijk. Informeer medewerkers van de HAN direct via een update, dit verhoogt de interne betrokkenheid. Het is belangrijk dat zij worden geïnformeerd kort voordat de HAN extern communiceert. De inhoudelijke boodschap en duiding blijft gelijk, wel geeft dit gelegenheid het bericht aan te vullen met enkele specifieke interne aangelegenheden. Een aparte en directe communicatielijn naar de RvT kan mogelijk in overleg worden versterkt.

Markeer expliciet de omslagpunten tijdens de crisis, in het bijzonder die naar de nafase. Deze crisis kende een aantal duidelijke kantelpunten. Ten eerste de overgang van de cybercrisis naar de privacycrisis. In de eerste fase is veel onduidelijkheid over het beveiligingslek en de precieze aard van het incident. Dit vereist veel technisch onderzoek en duiding van de dreiging. Dit verschuift naar de privacycrisis. Vanaf die fase treft de HAN veel organisatorische maatregelen en is de voornaamste opgave om alle betrokkenen te informeren. Daarnaast kwam de overgang van de acute fase naar de nafase. In de acute fase is veel onzeker en moet alles in het werk worden gesteld om inzichtelijk te maken wie betrokken zijn en hoe deze te informeren. In de nafase is de stuurgroep nog bezig is met de afhandeling van alle verzoeken. Wij adviseren om deze omslagpunten duidelijker te markeren. Bijvoorbeeld door dit te communiceren naar alle betrokkenen of door het werk na zo'n moment anders te verdelen (wie is in de lead?).

Verlaag het aantal informatiekanalen ter versterking van het gemeenschappelijk informatiebeeld. Tijdens de crisis maakte de HAN veelvuldig gebruik van MS Teams. Vanwege het aantal betrokkenen en aantal teams werden door de opgeschaalde teams naast het CMT verschillende MS Teams-omgevingen ingericht. Dit ontstond veelal organisch tijdens de crisis. Het risico hiervan is dat documenten en informatie niet op alle omgevingen en kanalen worden gedeeld en dat niet met up to date documenten gewerkt wordt. Wij adviseren daarom om het aantal informatiekanalen tussen teams zo veel mogelijk te beperken of uitsluitend voor specifieke doeleinden (zoals onderlinge communicatie en één aparte omgeving met de meest actuele documenten/informatie) te benutten om op die manier regie en overzicht te houden.

Deel opgedane ervaringen (zowel intern als extern) van deze crisis. Al tijdens de crisis had de HAN aandacht voor het delen van ervaringen met collega-instellingen. Met name om bewustwording rondom dergelijke dreiging te vergroten. Wij adviseren om de leerpunten die daarvoor geschikt zijn zowel intern als extern te delen. Dit ter verhoging van de algehele bewustwording binnen het onderwijs.

1 Aanleiding, aanpak & context

1.1 Aanleiding

Op 1 september 2021 ontvangt de voorzitter van het College van Bestuur (CvB) van de HAN University of Applied Sciences (HAN) een dreigmail van een hacker. De hacker claimt data te hebben gestolen en eist een bedrag in bitcoins. De crisisorganisatie van de HAN werkt hard om de situatie te duiden en de impact van het datalek te minimaliseren. Het lek is op 4 september 2021 dichtgezet. De situatie is in oktober 2021 onder controle, wel lopen er tot in 2022 nog enkele vervolgacties. In reactie op de cyberaanval heeft een operationele technische respons plaatsgevonden. Ook is de crisisorganisatie opgeschaald die zich richtte op de brede impact.

1.2 Doel

De HAN wil leren van wijze waarop de crisisrespons gewerkt heeft rond het hack en datalek. Doel van deze leerevaluatie is te komen tot een overkoepelend beeld van wat er gebeurde, wat er is gedaan in reactie op de gebeurtenissen en welke leerpunten hieruit volgen. Dit laatste heeft betrekking op zowel crisismanagement, communicatie en technische/IT-kant.

De HAN heeft 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.

1.3 Thema's

Voor de inhoudelijke scope van deze evaluatie hebben we gekeken naar onderstaande thema's:

- Informatiebeveiliging & Cyber security beleid en aanpak algemeen;
- Voorbereiding op incidenten (protocol/escalatie/expertise);
- Signalering en detectie;
- Leiding en coördinatie (inclusief dilemma's, doelen en uitgangspunten);
- Situationeel bewustzijn & scenariodenken;
- Privacy;
- Communicatie intern;
- Communicatie extern;
- Breder stakeholder management (medezeggenschap, RvT, andere onderwijsinstellingen, Ministeries, Autoriteit Persoonsgegevens);
- Overgang naar de nafase / fase van herstel.

Per thema reflecteren we op de gevolgde aanpak en benoemen we relevante leerpunten.

1.4 Gevolgde aanpak

Deze evaluatie is uitgevoerd in de periode tussen oktober 2021 en februari 2022. Het COT startte met een analyse van verschillende documenten. Het betreft onder andere de verslagen van de CMT-vergaderingen, beleidsdocumenten, interne en externe communicatie-uitingen etc. De beschikbaar gestelde documenten zijn met de grootste zorgvuldigheid behandeld. Ze zijn uitsluitend gebruikt om de gebeurtenissen scherp te krijgen en inzicht te krijgen in de beschikbare informatie en de gemaakte afwegingen.

Vervolgens voerden wij in totaal twaalf individuele gesprekken met direct betrokkenen[1]. De opbrengst van de gesprekken is verwerkt in een werkdocument van het COT. In de gesprekken is aan de hand van thema's besproken wat, terugkijkend, de belangrijkste lessen zijn. Daarnaast was er expliciet aandacht voor wat goed is gegaan en moet worden behouden voor toekomstige crises. Wij gebruikten de interviews als input voor vier 'leertafels' met de teams die tijdens de crisis actief zijn: crisismanagementteam (CMT), communicatieteam en team Techniek (opgesplitst in twee leertafels: datalek & data-analyse en AskHAN & privacy). Tijdens de leertafels is besproken waar de deelnemers terugkijkend trots op zijn, wat ze willen vasthouden voor de toekomst en wat leerpunten zijn. Ten slotte

[1] Een overzicht van deze functionarissen is te vinden in de bijlage

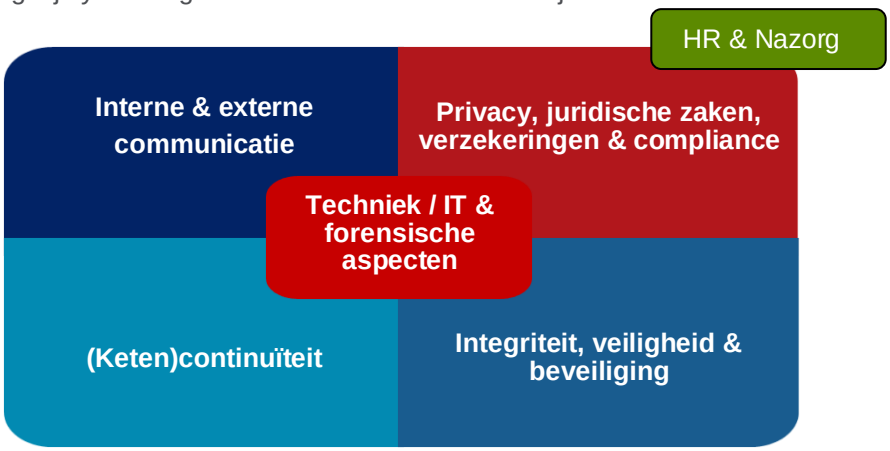
vond een sessie plaats met de Raad van Toezicht om de eerste rode draden te delen en vanuit hun rol als stakeholder leerpunten op te halen.

1.5 Visie COT op cybercrises

De wijze waarop de fysieke en digitale wereld vrijwel onlosmakelijk met elkaar verbonden zijn brengt verschillende cyberrisico's met zich mee. Het Nationaal Cyber Security Centrum (NCSC) ligt deze dreiging toe in het Cybersecuritybeeld Nederland 2021 dat in juni dat jaar gepresenteerd werd. Hierin benadrukt het NSCS niet alleen de technische en digitale risico's, maar ook de risico's en effecten op de gehele samenleving. Cyber gerelateerde incidenten blijven dan ook onverminderd grote risico's voor organisaties. Het verlies of de diefstal van data 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).

Informatieveiligheid 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.

Hoger onderwijsinstellingen hebben extra maatregelen getroffen om hun weerbaarheid tegen cyberdreigingen te vergroten. 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 waar meerdere organisatie mee te maken hebben. De mogelijkheid om tijdig technische mitigerende maatregelen te treffen hangt in belangrijke mate af van de voorbereiding en de inrichting van de systemen. Naast het belang om als individuele organisatie de weerbaarheid te vergroten, is gezamenlijk optrekken als onderwijssector belangrijk. Hiermee groeit de bewustwording bij cyberveiligheid verder binnen het onderwijs.



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 om steeds 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: qua mogelijke 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.

Daarnaast blijft ransomware 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.[2] 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.

1.6 Crisisorganisatie HAN

De HAN heeft een crisisplan (versie 23 juli 2021) met daarin een beschrijving van de interne crisisorganisatie. Het plan is opgesteld als onderdeel van de voorbereiding op mogelijke crises en om de crisisfunctionarissen te voorzien van een uniforme denk- en werkwijze. Tevens biedt het crisisplan handvatten aan de betrokken crisisteams tijdens een crisis en de nafase.
De crisisorganisatie van de HAN bestaat uit verschillende crisisteams, ieder met eigen rollen en doelen tijdens het crisismanagementproces. Alle teams beschikken over een vaste samenstelling die aan de hand van het type crisis en behoeften kan worden aangevuld vanuit een flexibele schil.

In het plan staan de volgende teams beschreven:

- **Crisismanagementteam (CMT).** Het CMT is verantwoordelijk voor bestuurlijke besluiten tijdens een crisis. Het CMT komt bijeen als een crisis meerdere academies of services binnen de HAN raakt of de reputatie in het geding is. Het CMT geeft richting aan het crisismanagementproces en formuleert doelen en uitgangspunten voor de crisisoperatie. Vaste leden van het CMT zijn: voorzitter, plotter, communicatieadviseur (woordvoerder HAN), crisiscoördinator, afgevaardigde Services en afgevaardigde Onderwijs. Afhankelijk van het type crisis kunnen flexibele leden zoals een Privacy Officer of Chief Information Security Officer (CISO) toegevoegd worden aan het CMT.
- **Supportteam (ST).** Bij situaties met een brede impact werkt het ST samen met het CMT. Het ST is verantwoordelijk voor het vertalen van de bestuurlijke besluiten van het CMT naar passende maatregelen. Meerdere ST’s kunnen tegelijk actief zijn die zich buigen over de operationele afhandeling van de crisis.
- **Crisiscommunicatieteam (CCT).** Om tijdig en adequaat te kunnen communiceren is in veel crisissituaties meer communicatiecapaciteit nodig. Het CCT voorziet hierin en voert de crisiscommunicatie uit op basis van beslissingen genomen door het CMT of ST. De woordvoerder van de HAN activeert en coördineert het CCT.
- **Security Operations Center (SOC).** IT-problemen en incidenten worden door het SOC opgespoord, beoordeeld en behandeld. Het SOC werkt aan de operationele technische response ten tijde van een cybercrisis.

Tijdens het datalek in september 2021 is maatwerk toegepast om de crisisorganisatie vorm te geven. Het CMT is opgeschaald met daarnaast een team Techniek voor onder meer de data-analyse, dichten van het lek en de afhandeling van de inzage- en verwijderverzoeken. Ook was een team communicatie actief, waar de communicatielijn is voorbereid op basis van mogelijke scenario’s en de communicatie aan betrokkenen en stakeholders is voorbereid.

[2] SURFnet: lessen ransomware Universiteit Maastricht

1.7 Opbouw rapportage

Zoals benoemd presenteren wij in deze rapportage de uitkomsten van de leerevaluatie. In hoofdstuk 2 beschrijven wij de gebeurtenissen. De nadruk ligt hierbij op de besluiten die vanuit de verschillende teams zijn genomen en op de interne en externe communicatie-uitingen. Hoofdstuk 3 bevat onze observaties per thema. In hoofdstuk 4 beschrijven wij onze overkoepelend beeld en doen wij op basis van de observaties en leerpunten aanbevelingen voor toekomstige crises.

2 Gebeurtenissen

In dit hoofdstuk geven wij de belangrijkste gebeurtenissen en ontwikkelingen weer in relatie tot het datalek. Dit is een selectie van de vele kritieke momenten en acties. Dit betekent dat niet alle overlegmomenten in deze tijdlijn zijn beschreven. We beschrijven de gebeurtenissen en belangrijkste activiteiten in onderstaande tijdlijn. De tijdlijn is opgesteld op basis van de door de HAN beschikbaar gestelde documenten en de interviews.

2.1 Gebeurtenissen per dag op hoofdlijnen

Woensdag 1 september

Op woensdag 1 september ontvangt de voorzitter CvB einde middag een dreigmail van een hacker. De hacker claimt data te hebben gestolen en eist een bedrag in bitcoins. De HAN moet binnen 24 uur contact opnemen en heeft daarna 72 uur om te betalen. Naar aanleiding van de eerste mail en analyse van de echtheid van de mail, schaalt de HAN op. In de eerste CMT-vergadering duidt het team de situatie. De HAN schakelt Fox-IT in voor technische ondersteuning.

De Functionaris Gegevensbescherming (FG) maakt een voorlopige melding van het datalek bij de AP. Daarnaast licht de Security Manager SURFcert in, waarna het SURFcert het NSCS inlicht. NCSC informeert vervolgens Team Cyber Crime Oost-Nederland.

Donderdag 2 september

Het eerste overleg met de politie, HAN en Fox-IT vindt plaats. Deze overleggen hebben vooral betrekking op de wijze van contact met de aanvaller en de analyse van de modus operandi van de aanvaller. De HAN bespreekt hierin ook het dilemma over het wel of niet contact opnemen/onderhouden met de dader en het ingaan op de eisen van de dader. De HAN heeft uiteindelijk contact met de hacker om antwoord te krijgen op de vraag hoe de hacker aan de data is gekomen. De hacker deelt vervolgens enige informatie met de HAN.

De HAN informeert de interne organisatie over het datalek.

Vrijdag 3 september

Gedurende de dag wordt steeds duidelijker dat het één lek betreft. De hacker heeft toegang gehad tot één server. Het CMT gaat vanaf dan vrij snel uit van het *worst-case scenario* waarin alle data van de getroffen server gelekt is.
De FG heeft de resultaten van de eerste analyse persoonsgegevens in de databases. Duidelijk is dat veel personen getroffen zijn, maar exacte aantallen zijn nog niet duidelijk.

De HAN plaatst een update op de eigen website. Daarin bevestigt de HAN dat de hacker een geldbedrag eist. Daarnaast benadrukt de HAN dat er onderzoek wordt gedaan en dat in het belang daarvan geen verdere mededelingen worden gedaan.

De hacker stuurt nog enkele dreigmails. De HAN besluit om op één van de mails te reageren. Vanwege het verdere verloop blijkt het verder niet meer noodzakelijk om contact te onderhouden met de hacker. De hacker zal zelf nog wel diverse keren een dreigmail sturen.

Zaterdag 4 september

Na uitgebreide technische analyse is het lek gevonden en gedicht.

Zondag 5 september

De HAN plaatst een uitgebreide update op de liveblog. De communicatiestijl is transparant. Dit is een bewuste keuze van de HAN. De update gaat onder andere in op het informeren van betrokkenen en welke keuze daarin door de HAN is gemaakt: de keuze om uit voorzorg alle studenten en medewerkers te informeren en dat later de betrokkenen rechtstreeks zullen worden geïnformeerd.

Maandag 6 en dinsdag 7 september

In de dagen na het plaatsen van de update is toenemende aandacht vanuit de media voor het datalek. De berichtgeving is overwegend neutraal en volgt de tekst van de liveblog van de HAN. Vanuit één

nieuwsmedium is de toon negatiever. Op basis van dit artikel plaatst de HAN een nieuwe update op de liveblog.

Woensdag 8 september

Gezamenlijke bijeenkomst team Communicatie, team Techniek, FG en jurist. Deze bijeenkomst gaat over de duiding van de data en de communicatie per groep betrokkenen. Op basis hiervan komt de HAN tot een onderscheid in drie groepen betrokkenen en drie communicatieboodschappen.

Kern van dit advies is: - Geef informatie en bevestig geluiden en toon begrip; - Neem mogelijke onrust weg en duid onduidelijkheid; - Laten zien welke mogelijkheden er zijn voor getroffenen voorondersteuning. FG vult de voorlopige melding datalek verder aan bij AP.

Gezamenlijke bijeenkomst team Communicatie, team Techniek, FG en jurist. Deze bijeenkomst gaat over de duiding van de data en de communicatie per groep betrokkenen. Op basis hiervan komt de HAN tot een onderscheid in drie groepen betrokkenen en drie communicatieboodschappen.

Kern van dit advies is: - Geef informatie en bevestig geluiden en toon begrip; - Neem mogelijke onrust weg en duid onduidelijkheid; - Laten zien welke mogelijkheden er zijn voor getroffenen voorondersteuning. FG vult de voorlopige melding datalek verder aan bij AP.

Er is een e-mail verzonden naar 4300 e-mailadressen van personen wiens wachtwoorden mogelijk zijn gelekt. Advies is om wachtwoorden te wijzigen die vóór 2018 gebruikt zijn. Hetzelfde bericht plaatst de HAN op de liveblog.

De FG deelt de voorlopige classificatie van de gelekte data. In de daaropvolgende periode heeft de FG regelmatig met de AP (telefonisch) contact over het datalek en beschikbare informatie.

Woensdag 22 september

Bij de CMT-vergadering sluit een IT- en privacyrecht-advocaat van Dirkzwager aan. Ook legt het CMT contact met de ethische adviescommissie over de te nemen stappen. Tot slot bespreekt het CMT het knelpunt rond het informeren van een bijzondere, kwetsbare groep betrokkenen.

Vrijdag 24 september

Fox-IT presenteert hun eindrapportage over het datalek. Het rapport bevat een beschrijving van de modus operandi van de aanvaller, de impact voor de HAN en enkele aanbevelingen voor maatregelen die e.e.a. in het vervolg kunnen voorkomen. In de CMT-vergadering deelt het team Techniek de voorlopige resultaten van de technische analyse. In de bestanden zijn ruim 500.000 unieke en ontdubbelde mailadressen aangetroffen. Uit de voorlopige resultaten blijkt dat er groepen personen zijn van wie gevoelige persoonsgegevens zijn gelekt. Mogelijk dient deze groep met prioriteit te worden geïnformeerd. Het CMT bespreekt of dit onderscheid wenselijk is of dat het liever alle betrokkenen tegelijk wenst te informeren.

Maandag 27 september

Gezamenlijke bijeenkomst team Communicatie, team Techniek, FG en jurist. Deze bijeenkomst gaat over de duiding van de data en de communicatie per groep betrokkenen. Op basis hiervan komt de HAN tot een onderscheid in drie groepen betrokkenen en drie communicatieboodschappen.

Kern van dit advies is:
- Geef informatie en bevestig geluiden en toon begrip;
- Neem mogelijke onrust weg en duid onduidelijkheid;
- Laten zien welke mogelijkheden er zijn voor getroffenen voorondersteuning.

FG vult de voorlopige melding datalek verder aan bij AP.

Maandag 11 oktober

De stand van zaken met betrekking tot het informeren is als volgt:
- 515.172 mails verstuurd om betrokkenen te informeren.
- 43.934 mails zijn teruggekomen (circa 8,5%)
- Instellingen waar de HAN veel mee samenwerkt (bijv. voor stages) worden ook geïnformeerd.

HAN.nl/datalek wordt regelmatig geüpdatet op basis van de resultaten van het onderzoek en de stand van zaken over het informeren van betrokkenen.
Bij het informeren van betrokkenen ervaart de HAN enkele knelpunten. Sommige emailadressen zijn niet langer in gebruik. De HAN krijgt dan ook een grote hoeveelheid meldingen dat mails niet zijn aangekomen. Het CMT bespreekt naar aanleiding hiervan in hoeverre aanvullende acties moeten worden ondernomen om deze betrokkenen alsnog te informeren.

Begin/half November

Op 1 november moet de HAN nog ruim 200 inzage- en verwijderverzoeken verwerken. De HAN richt een projectorganisatie voor de inzage- en verwijderverzoeken in en classificeert de verschillende verzoeken. Om onterechte inzage in potentieel bijzonder gevoelige gegevens en/of ongewenste gevolgen van onjuiste verwijderingen te voorkomen, worden de verzoekers gevraagd uiterlijk 20 december de identiteit bij de HAN aan te tonen (fysiek dan wel online).

Eind november

De FG en twee vertegenwoordigers vanuit het CMT maken de melding bij de AP definitief.

Vrijdag 7 januari

Alle verwijderverzoeken zijn afgehandeld.

Eind januari 2022

Alle aanvullende vragen van verzoekers zijn beantwoord, de enkele verzoeker die zich na de deadline van 20 december alsnog identificeerde heeft alsnog een inhoudelijke reactie ontvangen; het project wordt afgebouwd.

3 Observaties

In dit hoofdstuk beschrijven wij onze observaties per thema. Deze thema's zijn in overleg met de HAN bepaald. Dit hoofdstuk is verdeeld in drie paragrafen: de voorbereiding, acute fase en nafase. In de eerste paragraaf beschrijven we de relevante thema's ten aanzien van de voorbereiding. Vervolgens beschrijven we de observaties per thema die relevant zijn voor de acute fase. Tot slot gaan we in op de observaties ten aanzien van de nafase. De observaties zijn gebaseerd op de interviews en de leertafels.

3.1 Voorbereiding

3.1.1 Informatiebeveiliging & beleid en aanpak algemeen

Informatiebeveiligingsbeleid. De HAN heeft een informatiebeveiligingsbeleid. De informatiebeveiliging is in 2017 voor het eerst expliciet neergelegd in een beleidsdocument en nadien steeds aangevuld. Dit beleid is opgesteld met inachtneming van de geldende wet- en regelgeving. Het informatiebeveiligingsbeleid is door het CvB vastgesteld en geldt voor de gehele organisatie. Informatiebeveiliging gaat over alle IT- en informatiemiddelen en -processen binnen de HAN, waarbij drie elementen van belang zijn: beschikbaarheid, integriteit en vertrouwelijkheid. Daarnaast benoemt het beleid het belang van de controleerbaarheid: niet alleen weten of iets in orde is, maar dat ook achteraf kunnen verifiëren. Het doel van het informatiebeveiligingsbeleid is het bieden van een kader, het stellen van normen, het bieden van een daadkrachtige procesbenadering en voldoen aan compliance.

Het CvB is juridisch gezien eindverantwoordelijk voor informatiebeveiliging. In de governance van informatiebeveiliging wordt die verantwoordelijkheid verder binnen de HAN belegd. In de rolverdeling van informatiebeveiliging zijn een aantal cruciale rollen benoemd:

- **Information Security Officier (ISO):** rol op strategisch niveau, heeft direct toegang tot het bestuur en is zelf geen lijnverantwoordelijke.
- **Information Security Managers (ISM):** tactisch en operationeel niveau. De ISM is de verbindende schakel tussen het strategische niveau en de dagelijkse inrichting en uitvoering van informatiebeveiliging.
- **Computer Emergency Response Team (CERT):** de zogenaamde 'brandweer'. Het CERT komt in actie als er een dreiging is of een beveiligingsincident. Het CERT opereert zowel preventief als curatief.

De HAN interpreteert informatiebeveiliging in de brede zin. Informatiebeveiliging betreft alle vormen van informatie waar de HAN voor verantwoordelijk is. Het gaat hier niet alleen digitale informatie, maar bijvoorbeeld ook om informatie op papier. Er bestaat een belangrijke relatie en een gedeeltelijke overlap met zaken als sociale veiligheid, fysieke beveiliging en bedrijfscontinuïteit. Op strategisch niveau vindt hier integraal afstemming over plaats. Dit past bij de denkwijze van "integrale veiligheid".

Jaarplanning security & privacy. Naast het informatiebeveiligingsbeleid stelt de CISO jaarlijks een jaarverslag en jaarplan op. Deze wordt ter goedkeuring voorgelegd aan het CvB. Het jaarplan van 2021 heeft een thematische aanpak:

- Aanscherpen van beleid, organisatie, inventarisatie en classificatie
- Verbeteren van basis security en privacy maatregelen
- Verhogen van security en privacy bewustwording
- Realiseren van inzicht in actuele dreigingslandschap
- Waarborgen van privacy wetgeving (Algemene Verordening Gegevensbescherming (AVG))
- Verbeteren van security en privacy management informatie en rapportage

Binnen elk thema staan verschillende activiteiten benoemd om tot het gewenste resultaat te komen. De eigenaar per activiteit staat benoemd en de status van de activiteiten wordt bijgehouden in de planning. De opzet van de jaarplanning is gebaseerd op het NIST-framework met als toevoeging aanvullingen op het gebied van privacy.

De HAN vult het informatiebeveiligingsbeleid en het privacybeleid aan met een jaarlijkse planning op het gebied van security en privacy. Dit zorgt ervoor dat de actuele risico's en acties meegenomen worden. Een aantal activiteiten zoals archief plichtige documenten opslaan volgens bewaartermijn en het inzetten van Vulnerability scanning tools staan nog op 'lopend' op het moment dat het datalek

plaatsvindt. Dit is een aandachtspunt voor de HAN. Eerder is vanuit ICT een bewuste keuze gemaakt over de wijze van monitoring.

3.1.2 Voorbereiding op incidenten

Crisisoefeningen. De HAN organiseert periodiek crisisoefeningen. Het crisisteam oefent met verschillende scenario's, waaronder cyber gerelateerde. Crisisoefeningen verhogen de ervaring van de crisisorganisatie en het samenwerken onder dreigende, urgente en onzekere omstandigheden. Daarnaast deden de leden van het crisisteam veel ervaring op tijdens de coronacrisis vanwege de langdurige opschaling tijdens deze crisis.

In maart 2021 nam de HAN deel aan de OZON-oefening. Dit was een grootschalige cyberoefening voor het hoger onderwijs, waarbij het functioneren van de keten is getest en de effectiviteit van de interne communicatie is getoetst.[3] Het oefendoel van de HAN was het "oefenen met de samenstelling van het CMT bij een cybercrisis en de samenwerking met een decentraal (cyber)team." Het grootste leerpunt uit de oefening is de behoefte aan verduidelijking in de structuur en de rollen en rolverdeling tussen het centrale team en het decentrale team. In onderstaande tabel staan zowel de verbeterpunten vanuit de externe als de interne evaluatie:

Verbeterpunten vanuit de OZON 2021 oefening
- Leg de nieuwe crisisstructuur en de rol- en taakverdeling vast in een actueel crisisplan - Zorg dat een aantal praktische tools toegevoegd worden aan het crisisplan; Vergaderagenda met een thematische BOB, crisisdiagnose en format voor verslaglegging gebaseerd op de thema's; - Zorg voor een training/oefening met crisiscommunicatie; - Bespreek en leg vast hoe de afstemming tussen decentraal en centraal verloopt. - Train een keer op de overdracht en briefing tussen decentraal en centraal. Gaat ook over strategische advisering tijdens crisis en het denken in scenario's, kritieken momenten en besluiten en het hanteren van uitgangspunten. - Formaliseer crisisplannen, scenariokaart en crisisorganisatie verder, zodat rol, samenstelling en verantwoordelijkheden in geval van een cybercrisis vooraf bekend zijn - Verbeter bewustzijn onder medewerkers voor de herkenning van security incidenten. Formaliseer en beoefen het incident management proces, specifiek voor security. - Verbeter de identificatie van afwijkend gedrag op het netwerk, dan wel op andere belangrijke componenten binnen de IT-infrastructuur van de HAN. - Zorg dat het netwerk voor ICT-beheer niet toegankelijk is voor willekeurige laptops/desktoppen of andere apparatuur van 'kwaadwillenden'.

Vanwege de korte periode tussen de evaluatie van de OZON-oefening (maart) en het datalek (september), zijn ten tijde van het datalek niet alle verbeterpunten vanuit de oefening doorgevoerd. De betrokken functionarissen bij het datalek geven wel aan dat ze de verbeterpunten vanuit OZON direct toepasten in de crisisrespons en dat dit de snelle opschaling en afstemming ondersteunde.

3.2 Acute fase

3.2.1 Signalering en opschaling

E-mail 'hacker' en opschaling. Op 1 september 2021 om 17.26 ontvangt de voorzitter van het CvB een mail van een hacker met daarin de mededeling dat data is buitgemaakt. De afzender eist een bedrag in bitcoins binnen een termijn van 72 uur en dreigt met openbaar making van de gestolen data. Na ontvangst van deze mail verifieert de HAN de authenticiteit van de mail. De bij de mail bijgevoegde *sample line* met data blijkt data te zijn waar de HAN over beschikt. Het CMT besluit daarom tot een eerste overleg. Deze vindt plaats om 21.15 uur (minder dan 4 uur na de mail van de hacker). De eerste CMT-vergadering wordt gevoerd via MS Teams nadat ICT controleerde of dit veilig te gebruiken was. In het CMT delen de functionarissen de eerste situatieschets met daarin als belangrijkste thema's: start onderzoek impact en oorzaak, voorbereiden communicatie en informeren stakeholders. De desbetreffende database waar de data vandaan komt is op dat moment al offline gezet.

Respondenten kijken tevreden terug op de alarmering en opschaling. Zij ervaren dat snel wordt gealarmeerd en opgeschaald nadat de eerste signalen over een hack bekend zijn. Respondenten ervaren hierin een verschil met eerdere oefeningen.

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

Eerste duiding. Vanaf het moment dat de eerste mail van de hacker binnen is, onderzoekt het technische team het beveiligingslek. Vanuit de technische respons zoekt het team contact met SURFsoc, SURFcert en Fox-IT voor externe expertise. De technische analyse (Welke data is gelekt? Hoe kwam de hacker binnen? Wat is de impact? etc.) kost tijd. Het CMT gaat daarom tijdens de eerstvolgende vergaderingen uit van het *worst-case scenario*; het beveiligingslek kan groter worden of tot ransomware leiden. Samen met Fox-IT onderzoekt het technische team de oorsprong van het beveiligingslek, alle beschikbare logdata van de servers wordt gedeeld om vast te stellen of de aanvaller achterdeurtjes heeft gecreëerd. Fox-IT voert daarnaast forensisch onderzoek uit.

Eerste maatregelen. Na de eerste mail van de hacker licht de CISO de technische organisatie van de HAN in. Het eigen interne SOC komt bijeen. Daarin zit een vertegenwoordiging van de serverdiensten. Na de eerste analyses is vrij snel duidelijk om welke server het gaat en dat de omgeving *on premise* (lokaal bij de HAN in beheer) staat. Voordat het eerste CMT-overleg plaatsvindt is de database al offline gehaald. De HAN houdt er rekening mee dat de data op dat moment al gecompromitteerd is. De omvang van het datalek is op dat moment nog niet helder. Een nadere analyse hierover loopt dan nog. De analyse richt zich enerzijds op de impact en anderzijds op de vraag hoe de data gelekt kan zijn.

Kritiek besluit: niet betalen. De hacker vraagt een bedrag in bitcoins en dreigt met het openbaar maken van de gestolen data wanneer de HAN niet betaalt. Het CMT hanteert als uitgangspunt dat de HAN niet zal betalen. Op advies van de politie en Fox-IT houdt de HAN vast aan dit uitgangspunt, ook op het moment dat de hacker op 3 september de druk opvoert (zie onderstaande tabel). Het CMT baseert dit besluit op basis van twee omstandigheden. Ten eerste bestaat er geen garantie dat de hacker de data niet openbaar maakt als de HAN betaalt. Daarnaast is geen sprake ransomware, waardoor de continuïteit van de HAN niet in het geding is.

Dichten lek. Op 4 september 2021 wordt de modus operandi van de hacker duidelijk. Dezelfde avond wordt het lek gedicht. Het team Techniek had de behoefte om het lek al eerder te dichten. Dit is niet gedaan in afwachting van nader forensisch onderzoek van Fox-IT. Beide belangen zijn navolgbaar. Op 6 september concludeert Fox-IT dat er geen andere dreigingen te verwachten zijn en dat zij geen andere kwetsbaarheden hebben gevonden. Op basis hiervan besluit het CMT om niet langer te communiceren met de hacker. De dynamiek van de crisis verandert hierdoor. De bedreiging van de continuïteit van de HAN is voorbij. De focus van de technische respons kan worden verlegd van het beveiligingslek naar de gestolen data. Het feit dat er sprake is van een datalek zorgt er bovendien voor dat er veel organisatorische maatregelen zullen moeten worden genomen (informeren betrokkenen).

3.2.2 Crisismanagement

Inrichting crisisorganisatie. Zoals eerder benoemd in paragraaf 1.6 is het CMT snel opgeschaald. Het CMT wordt ondersteund door verschillende teams. Zo is er een team Techniek voor onder meer de data-analyse, het dichten van het beveiligingslek en de afhandeling van de inzage- en verwijderverzoeken. Gedurende de crisis is het team Techniek gesplitst in twee subteams: datalek & data-analyse en AskHAN & privacy-team. Dit hangt nauw samen met het de veranderende dynamiek van de crisis en het feit dat het datalek tot veel organisatorische taken leidt (informeren betrokkenen etc.). Daarnaast is een team Communicatie actief. Het team Communicatie houdt zich primair bezig met het voorbereiden van de berichtgeving (externe communicatie). Daarnaast denkt het team Communicatie na over mogelijke scenario's.

Het onderscheid tussen de verschillende teams (CMT, Techniek en Communicatie) werkt goed. Dit maakt de crisis beter behapbaar. Respondenten zijn tevreden over de wisselwerking tussen deze teams en het CMT. De betrokken functionarissen zijn trots op de samenwerking, de bereidheid om elkaar te helpen en gezamenlijk het probleem op te lossen. In korte tijd is veel werk verzet, met elkaar en in goede harmonie. Betrokkenen zijn trots op de eigen kennis en kunde. Zij kennen en begrijpen de systemen en kunnen Fox-IT hierdoor goed van antwoord voorzien en inhoudelijk uitdagen.

Tegelijkertijd volgt uit de interviews en leertafels ook dat niet alle betrokkenen binnen de crisisorganisatie zicht hadden op de inrichting en werking van de hele crisisorganisatie. Zo was niet voor iedereen was duidelijk welke teams actief waren en hoe taken zich precies tot elkaar verhouden. Dit gold voor een aantal leden van de ondersteunende teams en speelt zowel in de acute fase als in de

nafase. Daarnaast gaf een aantal RvT-leden aan behoefte te hebben aan meer zicht op de werking van de crisisorganisatie.

Inrichting en functioneren CMT. Een veelvoorkomende uitdaging tijdens cybercrises is het verbinden van twee 'werelden' (technisch-bestuurlijk/operatie) en het spreken van verschillende 'talen': specifieke IT-terminologie is vaak niet goed bekend bij crisisfunctionarissen (zie 1.5). De CISO sluit direct aan in het CMT. Dit is mede ingegeven door de ervaringen in crisisoefeningen van de HAN. De CISO blijkt goed in staat om de twee 'werelden' te verbinden. De CISO en de voorzitter van het team communicatie maken steeds een heldere koppeling tussen de techniek en de belangrijke dilemma's die spelen. Zij blijken goed in staat om helder uit te leggen wat de impact is van de technische kant van de crisis. Dit stelt het CMT in staat om te focussen op de (strategische) besluiten.

Het CMT wordt aangevuld met externe expertise. De HAN schakelt Fox-IT, een crisiscommunicatie-expert en een IT en privacyrecht-advocaat in. De ervaring van deze externen leidt er volgens CMT-leden toe dat de vergaderingen over de 'juiste' onderwerpen gaan en dat voorzienbare dilemma's al op voorhand worden besproken. Bijvoorbeeld over het eventueel communiceren met de hacker en het eventueel ingaan op betalingseisen van de hacker.

Samenwerking CMT en ondersteunende teams. Het CMT vraagt met grote regelmaat om statusupdates aan de teams. Dit is belangrijk voor het verkrijgen en behouden van een (gedeeld) situationeel beeld. De frequentie waarmee deze statusupdates worden gevraagd is volgens de ondersteunende teams aan de hoge kant. De teams ervaren dat zij op momenten veel bezig zijn met het maken statusoverzichten dat gaat ten koste van het onderzoek en de uitvoering. De teams hebben daarnaast behoefte aan meer terugkoppeling op de analyse en de besluitvorming van het CMT. Dit is belangrijk, vooral als het gaat om de context waarbinnen een besluit is genomen. Bijvoorbeeld rond het besluit om het datalek niet direct te dichten. Dit besluit werd in het CMT op advies van Fox-IT genomen. De ratio hierachter was voor het team Techniek onduidelijk. Een aantal functionarissen geeft aan dat zij graag een terugkoppeling hadden ontvangen van het CMT met hoe de informatie is ingezet en welke afwegingen er rond besluitvorming zijn geweest. Op deze manier kan het team beter anticiperen op de informatievraag.

De perceptie van de ernst van het incident verschilt soms per team. Het CMT heeft een andere perceptie dan de 'nuchtere' blik van team Techniek. Dit is deels te verklaren vanuit de andere kijk op de aanwezige risico's en uitdagingen. Technisch gezien zijn de risico's snel beperkt zodra het lek is dichtgezet. Voor het CMT blijven de risico's over de ernst en omvang van het datalek aanwezig en de daarbij behorende uitdagingen. Enkele CMT-leden vinden het soms lang duren voordat een goed en betrouwbaar beeld aanwezig is van de omvang, aard en feiten. Er is een nadrukkelijke wens om dit proces te versnellen. Betrokkenen bij team Techniek benoemen dat vrij snel duidelijk was dat er sprake was van een datalek met weinig technische vervolgrisico's. Nadat voor het CMT duidelijk was dat het om een datalek gaat, heeft het CMT grote zorgen over de omvang van het aantal gelekte gegevens. Ondanks het verschil in perceptie heeft het datalek de onverminderde prioriteit bij alle betrokkenen.

Informatiekanalen. De opgeschaalde teams hebben eigen MS Teams kanalen met daarin relevante documentatie en verslagen. Na verloop van tijd ontstaat verwarring waar de meest recente informatie vindbaar is en is het lastig om het overzicht goed te houden doordat de informatie verspreid over de verschillende Teams-kanalen staat. Betrokkenen benoemen dat het aantal MS Teams kanalen aan de hoge kant is (circa 19) en bij een volgende crisis verminderd zou kunnen worden. Het CMT ervaart dit probleem niet doordat één vaste MS Teams-omgeving als informatiekanaal wordt gebruikt.

Belasting leden CMT en afdelingen. Door de aard van de crisis vraagt dit van enkele leden van het CMT een ruime inzet en hebben andere leden juist een minder actieve rol. Vooral de CISO en Stafdirecteur IM, inclusief hun achterban (team Techniek en de serviceafdeling) en het team Communicatie zijn erg druk. Het informeren van alle betrokkenen leidt tot honderden informatieverzoeken, 250/300 inzage en verwijderverzoeken en een tiental claims. Binnen de HAN is zowel in de bezetting van de AskHan als in de afhandeling van de verzoeken opgeschaald. Bovendien ontstaat discussie over waar dit 'vervolgwerk' thuishoort (Services of IM) en zijn de medewerkers die hiermee aan de slag moeten onvoldoende meegenomen. Dit verschil in hoeveelheid werk tussen teams zien we vaker bij cyber- en privacy-gerelateerde incidenten. De hoeveelheid werk is nauwelijks te behappen voor het beperkte aantal medewerkers met de benodigde expertise.

3.2.3 Situationeel bewustzijn & scenariodenken

Betrokkenen ervaren dat het CMT duidelijk onderscheid maakt tussen feiten en de geldende onzekerheid. Het CMT neemt besluiten op basis van de feiten. De onzekerheden werkt het CMT consequent uit in drie scenario's (*good, most likely* en *worst-case scenario*). Zo gaat het CMT in eerste instantie lang uit van de mogelijkheid dat een ransomware-aanval de continuïteit van de organisatie ernstig kan verstoren. Dit omdat nog niet is vastgesteld hoe ver het beveiligingslek strekt. Betrokkenen hebben hierdoor het gevoel dat het CMT controle heeft over de situatie.

Vervolgens blijkt definitief dat het lek de enige kwetsbaarheid is en dat er geen andere ingangen open zijn. De hacker heeft toegang gehad tot één server. Het CMT gaat vanaf dan vrij snel uit van het *worst-case scenario* waarin alle data van de getroffen server gelekt is. Dit zorgt voor focus en geeft sturing welke betrokkenen geïnformeerd moeten worden.

Ook in het contact met de hacker is steeds in scenario's gedacht. Dit heeft meer een beslisboom-structuur: wat doen we als HAN als de hacker niet reageert; wat doen we als HAN als de hacker toch publiceert?

Tot slot bespreekt het CMT de gevolgen van de getroffenen/betrokkenen van het datalek. Het CMT weegt steeds de impact van het datalek op de betrokkenen mee. De verschillende belangen spelen een rol in de strategische besluitvorming.

3.2.4 Privacy

AVG-compliance. Respondenten uiten hun zorgen over de privacy-volwassenheid van de HAN. Dit maakt de organisatie kwetsbaar voor onder meer datalekken. Bij het datalek zijn gegevens gelekt die volgens de bewaartermijnen al verwijderd hadden moeten zijn. In het jaarplan 2021 staan meerdere activiteiten om de AVG binnen de HAN te waarborgen. Ten tijde van het datalek zijn die activiteiten nog niet afgerond. Ook blijkt tijdens de crisis dat data verspreid is opgeslagen. Dit maakt het complex om verwijderverzoeken van betrokkenen volledig af te ronden.

Rol FG. Gedurende de crisis is de FG geen onderdeel van het CMT. De benodigde expertise is – door middel van een externe advocaat – later wel geborgd. De FG heeft de wens om vanuit zijn eigen rol en expertise wel deel te nemen in het CMT. Het is niet noodzakelijk de FG (vast) onderdeel te maken van een crisisteam maar de FG kan bijvoorbeeld agenda-lid zijn. Op die manier kan de FG actief inspelen op de thema's die op de agenda staan en een advies geven op privacy-thema's. De FG heeft tijdens deze crisis een actieve deelname in het team Communicatie. Bovendien adviseert de FG het CMT diverse malen. Zo adviseert hij onder meer over de handelswijze met betrekking tot een geïdentificeerde kwetsbare groep wiens bijzondere persoonsgegevens zijn gelekt.

Melding AP. Vanuit de AVG is de HAN verplicht om uiterlijk binnen 72 uur na bewust worden van een inbreuk melding te maken bij de AP. Op 1 september 2021 om 21.42 uur maakt de FG een voorlopige melding bij de AP over het datalek. Dit is binnen de gestelde termijn. De analyse van het type persoonsgegevens en de grootte van het datalek is op dat moment nog aan de gang. Gedurende het datalek heeft de FG contact met de inspecteur van de AP. De melding wordt enkele keren aangevuld. Dit contact wordt door de AP gewaardeerd. De FG maakt de melding bij de AP op eind november definitief samen met vertegenwoordigers van het CMT.

3.2.5 Communicatie

Team Communicatie. De coördinator van het team Communicatie is in de reguliere organisatie de stafdirecteur informatiemanagement. Dit lijkt een bijzondere keuze, maar had een positief effect. De coördinator is samen met de CISO de verbindende schakel tussen team Techniek en het CMT en kan de vertaalslag maken van de meer technische duiding en informatie naar de strategische besluiten. Dit was tijdens deze crisis van groot belang.

Transparantie als uitgangspunt. Het CMT hanteert een duidelijk uitgangspunt in relatie tot de communicatie: transparantie. De HAN richt een speciale website in waarop ze met enige regelmaat updates geven over het incident. Ook publiceert de HAN een document met uitleg over welke (gevoelige) gegevens zijn gelekt. Betrokken functionarissen hebben hierdoor het gevoel steeds de regie over de communicatie en berichtgeving te hebben.

Het uitgangspunt transparantie zorgt in de beginfase voor een dilemma op het moment dat het lek gedicht is. Communiceren dat het lek dicht is, kan een reactie van de hacker oproepen. Tijdens het CMT op 4 september is dit dilemma uitvoerig besproken. Het CMT besluit om niet dezelfde avond te communiceren, maar de volgende dag vóórdat de deadline van de hacker verloopt om te betalen.
Het uitgangspunt staat ook kort ter discussie als een nieuwsmedium begin september bericht over het datalek. Door de meer negatieve toon van deze berichtgeving en de wens om hier een reactie op te geven, is de communicatie vanuit de HAN hierdoor korte tijd meer reactief in plaats van transparant en proactief. Snel daarna heeft de HAN de regie op de communicatie weer terug.

Op 5 oktober geeft de HAN een persstatement. In dit statement wordt een bijlage toegevoegd met daarin de verschillende categorieën persoonsgegevens en het aantal gevallen. Dit laat zien dat de HAN vasthoudt aan het uitgangspunt transparantie.

Informeren betrokkenen. Op 6 september wordt vanuit het team Communicatie duidelijk dat de gelekte data is op te delen in drie categorieën. Op 9 september is dit verder gespecificeerd:

1. Bijzondere persoonsgegevens (meest gevoelig, hoogste risico); 1-2% van gevallen
2. Gevoelige persoonsgegevens (gevoeligheid en risico midden); 5-10% van gevallen
3. Persoonsgegevens in algemene zin (minst gevoelig, lager risico); 90-95% van gevallen

Het team Communicatie past de communicatie per groep betrokkenen aan. Het team Communicatie overlegt met het team Techniek over de communicatieboodschap. In de beginfase van de crisis hebben de teams een verschillend beeld over de duiding van de persoonsgegevens en communicatie per groep betrokkenen. Om de informatielijnen en de communicatie beter op elkaar af te stemmen, komt op 27 september een grote groep functionarissen bij elkaar: team Techniek, team Communicatie, FG en jurist. Dit moment werkt voor alle betrokkenen verhelderend. Het leidt tot een nadere duiding van de data waardoor de communicatieboodschap kan worden versterkt en tot een duidelijk afgestemd tijdspad voor de komende periode. Voor openstaande acties maken de betrokkenen een draaiboek.

De communicatieboodschappen en correspondentie met betrokkenen worden aan het CMT voorgelegd voordat ze worden verstuurd. Dit brengt extra zorgvuldigheid in het proces en leidt bovendien tot een extra juridische check vanwege de IT en privacyrecht-advocaat die inmiddels onderdeel uitmaakt van het CMT. De teamleden begrijpen de wens van het CMT om berichtgeving af te stemmen. De tussenstap zorgt echter wel voor een gevoel van vertraging, ondanks dat de feitelijke vertraging beperkt blijft. Door de toewijding van de teamleden leidt dit soms tot frustratie/ongeduld.

Communicatiemiddelen. De liveblog op de website is tijdens de crisis het belangrijkste communicatiemiddel van de HAN. Daarnaast gebruikt de HAN verschillende andere communicatiemiddelen. Mail (naar medewerkers en studenten op verschillende momenten), FAQ op website HAN, Insite, een pagina met updates/links en WhatsApp-groepen voor interne communicatie CMT. De ondersteunende communicatiemiddelen verwijzen naar de liveblog op de website. Op die manier is de HAN eenduidig in de informatieverstrekking.

Vanuit de studentenvakbond is de vraag gesteld waarom social media niet is ingezet. Dit medium heeft een breed bereik onder studenten. Vanuit het team Communicatie is het weloverwogen besluit genomen om de liveblog als hoofdcommunicatiemiddel in te zetten. Achteraf gezien vragen een aantal functionarissen zich af of social media niet ook een passend middel was om meer mensen te bereiken, bijvoorbeeld om te verwijzen richting de liveblog.

Tijdens de evaluatie stellen betrokkenen de vraag welk middel het beste ingezet kan om intern richting medewerkers te communiceren. Tijdens deze crisis is uitsluitend de website ingezet. De vraag is of de HAN aanvullend en separaat intern had moeten communiceren. De HAN koos ervoor dit niet te doen vanwege het risico dat de informatie afwijkt. In de evaluatie doen respondenten de suggestie om onderscheid wel te maken.

3.2.6 Breder stakeholder management

Interne stakeholders. Vrij snel na ontvangst van de eerste mail van de hacker licht het CMT de RvT in. Medewerkers van de HAN ontvangen op 2 september de eerste informatie over de hack en het datalek. De HAN verwijst medewerkers naar de liveblog voor de meest recente informatie. Direct betrokkenen en getroffenen ontvangen – net als de extern betrokkenen/getroffenen – een persoonlijke mail met daarin het handelingsperspectief (bijv. wijzig je wachtwoord).

Externe stakeholders. De HAN informeert betrokkenen over het datalek volgens de wettelijke verplichting. In aanvulling hierop communiceert de HAN specifiek naar partners waarvan meerdere medewerkers (meer dan 50) zijn gedupeerd. Dit toont aan dat de HAN zich bij een crisis bewust is van belangrijke externe stakeholders. Ook via de partners krijgen de betrokkenen een handelingsperspectief (bijv. wijzig je wachtwoord). Dit vergroot de kans op het gewenste resultaat (voorkomen van een nieuw datalek of dat meer gegevens worden buitgemaakt).

De HAN heeft vanaf de start ook contact met collega-instellingen (onder andere de Universiteit van Amsterdam en Universiteit Maastricht) om ervaringen en tips uit te wisselen. De bestaande samenwerkingsverbanden worden volop benut. Voor het CMT is het prettig om de meer praktische zaken te kunnen overleggen met deze instellingen. Uiteindelijk is de respons bepaalt op basis van eigen afwegingen in samenwerking met Fox-IT en de politie. Ook vanuit SURFcert en NCSC zijn hulpaanbiedingen gekomen. Vanwege de drukte en hectiek lukt het aannemen van hulp en bijpraten van partijen niet altijd. Vanuit team Techniek is contact met het Radboud UMC over de vorm van data-analyse (o.a. hoe categoriseren we de data, verdere afhandeling en tips over de aanpak). De tips en adviezen helpen in de verdere aanpak. Naar aanleiding van het datalek bij de HAN zijn Kamervragen gesteld in de Tweede Kamer. De HAN is betrokken geweest bij de beantwoording van deze vragen.

3.3 Nafase

Lange nasleep inzage- en verwijderverzoeken. Een omvangrijke datalek leidt tot een grote hoeveelheid werk. Betrokkenen worden verrast door het grote aantal verzoeken. Er is geen planvorming waardoor ter plekke een werkwijze moet worden bedacht voor het informeren van alle betrokkenen en het behandelen van de reacties. In de beginfase is dit werkbaar, maar de schaal van de verzoeken en daarmee de schaal van de afwikkeling bemoeilijkt de afhandeling. De reacties zijn bovendien divers; verwijderverzoeken, inzageverzoeken, informatieverzoeken en claims. Per categorie is een andere (wettelijke) reactietermijn en expertise vereist. Daarnaast is het door de veelheid aan systemen, decentrale opslag en verschillende eigenaren lastig om met zekerheid te kunnen zeggen dat alle data gevonden of verwijderd is. Dit maakt de afhandeling van de verzoeken complex en tijdrovend. Hierin is de HAN niet uniek, dit speelt bij veel organisaties die te maken hebben met een datalek/aanval.

Tot ver in januari is de organisatie bezig met het afronden en uitvoeren van de verwijder- en inzageverzoeken of vragen van betrokkenen. Dit is belegd bij een stuurgroep, waarvan tijdens de leertafels blijkt dat deze niet bij iedereen bekend is. Het CMT is nog steeds opgeschaald om vinger aan de pols te houden over openstaande acties en voortgang en deze met de benodigde urgentie te laten verlopen. Alhoewel de gevolgen van het datalek nog lopen, is de acute fase en crisis (dreiging, urgentie en onzekerheid) voorbij. Om deze reden vinden meerdere respondenten het tijd om af te schalen en de taken te beleggen bij in de reguliere lijn of een projectteam.

4 Overkoepelend beeld en aanbevelingen

4.1 Inleiding

In dit hoofdstuk reflecteren wij op de crisisrespons van de HAN naar aanleiding van het datalek. Deze reflectie baseren wij op de interviews en leertafels en eerdere vergelijkbare evaluaties. In dit hoofdstuk schetsen wij eerst ons overkoepelend beeld met samenvattend de succesfactoren en aandachtspunten. Tot slot doen wij aanbevelingen met het oog op toekomstige soortgelijke crises.

4.2 Overkoepelend beeld

De AVG is sinds mei 2018 van kracht. Voorafgaand en sindsdien zijn bijna alle organisaties, waaronder de HAN, druk bezig met het implementeren van verschillende maatregelen om AVG-compliant te worden en blijven. De nieuwe privacyregels hangen nauw samen met breder informatiebeveiligingsbeleid. Een accurate bescherming is belangrijk om te voorkomen dat iemand onrechtmatig toegang verkrijgt tot gegevens. Ook hierin investeert de HAN doorlopend, middels informatiebeveiligingsbeleid en een jaarplanning.

Ondanks deze inspanningen wordt de HAN begin september benaderd door een hacker. De hacker claimt toegang te hebben tot gegevens van de HAN en dreigt deze openbaar te maken als de HAN niet betaalt. De crisisorganisatie van de HAN schaalt snel op nadat wordt vastgesteld dat sprake is van een serieuze dreiging. Daarbij maakt de HAN ook gebruik van externe expertise op verschillende vlakken (technisch, juridisch, communicatie) voor meer comfort en om de situatie zo spoedig mogelijk te kunnen duiden. Dit is begrijpelijk. Een aandachtspunt hierbij is om een dergelijk besluit intern goed te communiceren en uit te blijven leggen wat de toegevoegde waarde is. Dit is belangrijk omdat het inschakelen van externe expertise de interne organisatie het gevoel kan geven dat de interne kracht onvoldoende wordt benut.

In de eerste fase van de crisis is er weinig informatie en zekerheid. Het CMT denkt in scenario's en is met name bezorgd over eventuele ransomware. De continuïteit van de HAN zou hierdoor ernstig en langdurig kunnen worden verstoord, blijkt uit diverse cases wereldwijd. Hierin valt positief op dat de verbinding tussen de techniek en mogelijke gevolgen voor de operatie/continuïteit goed is geborgen. De CISO vormt hierin een belangrijke schakel en sluit – vanwege eerdere crisiservaringen van de HAN – direct aan in het CMT. Het is belangrijk deze verbinding te behouden voor toekomstige cybercrises.

Binnen enkele dagen blijkt dat er sprake is van een datalek en de hacker toegang had tot een omkaderde omgeving. Ten opzichte van het 'worst-case-scenario' valt dit relatief gezien mee. Toch staat de HAN voor een gigantische opgave. De HAN heeft immers de wettelijke plicht om alle betrokkenen (ruim 500.000) te informeren. Daarbij moet bovendien onderscheid worden gemaakt in de communicatie op basis van het type persoonsgegevens dat is gelekt. De HAN kan hierbij niet terugvallen op een draaiboek of plan. Ter plekke wordt een proces bedacht waarbij succesvol een groot beroep wordt gedaan op het improvisatievermogen van de betrokken medewerkers. Achteraf geven een aantal medewerkers aan het fijn te vinden als ze in de voorbereiding meer houvast hebben.

In de crisisrespons gaat veel goed en zien wij enkele mogelijkheden om deze respons te versterken met het oog op toekomstige crises. Door het hoge aantal informatiekanalen en MS Teams groepen is het soms een uitdaging om een eenduidig informatiebeeld te krijgen voor de opgeschaalde teams buiten het CMT. Een ander aandachtspunt is de terugkoppeling van de CMT-besluiten. De behoefte om op kritieke momenten eerder te worden meegenomen leeft bij de RvT. Ook de ondersteunende teams hebben behoefte aan meer terugkoppeling en context. Dit vergemakkelijkt de opgave omdat dan op basis van de ratio van de besluiten verder kan worden gewerkt. Bijkomend effect kan zijn dat de verschillende teams meer zicht hebben op de hele crisisstructuur en de verdeling van taken tussen teams. Wij adviseren om dit ook breder te doen. Zorg ervoor dat de interne communicatie richting (betrokken) medewerkers steeds voorloopt en via een direct kanaal gebeurt ten opzichte van de communicatie naar de 'buitenwereld'.

De betrokkenheid en duidelijke structuur (CMT met ondersteunende teams) vallen op. Gezamenlijk klaren de betrokken de klus. Op een aantal belangrijke momenten door gezamenlijk (met alle teams en betrokkenen) na te denken over een onderwerp of werkwijze. Vanaf de start hanteert de HAN duidelijke uitgangspunten. 'Niet betalen' en 'transparante communicatie' zijn daar de meest aansprekende

voorbeelden van. Dit geeft houvast en richting. De gebeurtenissen vanaf september maken de direct betrokkenen zeer bewust van de risico's die samenhangen met privacy en informatiebeveiliging. Het is belangrijk om de opgedane ervaring te borgen en benutten richting de hele organisatie. Het incident geeft aanleiding om enkele maatregelen (soft en hard) te nemen om het risico op dergelijke incidenten te verlagen. Onze aanbevelingen in de volgende paragraaf zijn dan ook gericht op een preparatie op brede cybercrises en het gezamenlijk managen van de impact die dit met zich meebrengt.

Samenvattend zien wij de volgende succesfactoren en aandachtspunten voor de HAN naar aanleiding van de crisisrespons op het datalek:

Succesfactoren
De snelle opschaling en goed werkende crisisstructuur met een opgeschaald CMT en gespecialiseerde ondersteunende teams
De flexibiliteit, het improvisatievermogen en de toewijding van alle betrokkenen uit de crisisorganisatie
De duidelijke opgestelde uitgangspunten: 'niet betalen' en 'transparant communiceren'
Aanvulling crisisorganisatie met specifieke (externe) expertise
Continu blijven denken in scenario's
Korte lijnen tussen betrokkenen én gezamenlijke momenten voor gemeenschappelijk beeld (zoals briefing afhandeling informeren betrokkenen en communicatieboodschap per groep betrokkenen)
Eén extern informatiekanaal: han.nl/datalek
Aandachtspunten
Afstemming van informatiebehoefte CMT vs. uitvoeringstijd en -behoefte teams
Het ontbreken van planvorming met betrekking tot het afhandelen van grote hoeveelheden verzoeken betrokkenen
Volwassenheidsniveau HAN met betrekking tot privacy/AVG
Terugkoppeling besluiten en ratio hierachter van CMT naar andere teams (ook m.b.t. de inhuur van externe expertise)
Zicht van betrokkenen op hele crisisstructuur en verdeling van taken tussen teams; welke overleggen zijn er? wie communiceert met wie?
Hoog aantal interne informatiekanalen en MS Teams groepen
Het ontbreken van separate interne communicatie richting bij het datalek betrokken medewerkers (buiten de opgeschaalde teams)

4.3 Aanbevelingen

Op basis van bovenstaande analyse doen wij de volgende aanbevelingen voor toekomstige crises met soortgelijke omstandigheden:

1. **Benut het verhoogde bewustzijn ter versterking van de privacy volwassenheid en informatiebeveiliging van de HAN.** De crisis toont enkele kwetsbaarheden van de HAN in relatie tot het thema privacy en cyber. Zo blijkt dat de gelekte data de bewaartermijnen hadden overschreden en dat veel informatie decentraal is opgeslagen. Privacy is een thema dat periodiek en doorlopend aandacht verdient. Alle medewerkers moeten doorlopend bewust zijn van de risico's en hun eigen verantwoordelijkheid. De inspanningen van het team Techniek en de rapportage van Fox-IT maken daarnaast mogelijk enkele cybersecurity verbetermogelijkheden inzichtelijk. Voor de uitvoering van de noodzakelijke acties helpt het om vanuit deze ervaring te kijken naar de huidige risico's van de HAN en wat de gevolgen hiervan zijn. Investeer in de capaciteit, het updaten en opvolgen van de jaarplanning, het (her)prioriteren van acties, bewustwording en gezamenlijk eigenaarschap.

2. **Prepareer doorlopend op crises: investeer in continuïteitsmanagement, ontwikkel een draaiboek datalekken en een afwegingskader ransomware.**
    a. **Continuïteitsmanagement** In de eerste fase van deze crisis vreesde de HAN voor een ransomware-aanval. Dit zou de continuïteit van de organisatie ernstig of langdurig in gevaar kunnen brengen blijkt uit verschillende externe casuïstiek. Het is belangrijk om hierop voor te bereiden in het kader van continuïteitsmanagement. Maak de afhankelijkheden van IT voor de continuïteit van de organisatie inzichtelijk. Denk na over herstelmaatregelen en *workarounds* om eventuele verstoringen op te kunnen vangen.

b. **Draaiboek datalekken** Het datalek vraagt veel van het improvisatievermogen van alle betrokkenen. Zo moet een organisatie worden ingericht voor de grootschalige communicatie aan betrokkenen en de afhandeling van alle terugkomende vragen en verzoeken. Wij raden aan om deze ervaring en organisatie-inrichting vast te leggen in een draaiboek. In dit draaiboek kan bijvoorbeeld de werkwijze rondom het informeren van betrokkenen worden opgenomen, een checklist met acties/maatregelen, betrokken functionarissen en teams etc. Bij een onverhoopt volgend (grootschalig) datalek kan deze benut worden om snel en adequaat op te schalen. Bepaal binnen welke directie deze taak het best kan worden belegd. Bereid medewerkers voor op deze onverwachte acute taak door het geven van een training of het houden van een intervisiesessie waarin de ervaringen van deze crisis gedeeld worden. Onderzoek of een (ervaren) flexibele schil kan worden voorbereid of ingehuurd als zich een incident voordoet om de werkdruk van de eigen organisatie te verlichten.

c. **Afwegingskader ransomware** Daarnaast adviseren wij om een afwegingskader ransomware op te stellen. In de eerste fase van de crisis vroeg de hacker diverse keren om losgeld en zette de HAN onder druk. Doordat de continuïteit niet in gevaar was en omdat vrij snel duidelijk was dat het lek was gedicht, kon de HAN het zich permitteren hier niet op in te gaan. Niet betalen was ook een duidelijk uitgangspunt tijdens de crisis. Deze omstandigheden kunnen bij een volgende crisis afwijken. Dit kan het uitgangspunt ‘niet betalen’ sterk onder druk zetten en tot spanning leiden binnen het CMT. Daarom is het belangrijk om in de koude fase een afwegingskader te maken waarin voorzienbare dilemma’s worden besproken en doorleefd. Denk hierbij ook na over de ‘tenzij…’, de uitzondering op het uitgangspunt om niet op eisen van een hacker in te gaan. Betrek bij het opstellen van dit kader belangrijke stakeholders (bijv. RvT vanuit hun adviserende/toezichthoudende rol).

3. **Versterk de informatievoorziening naar de ondersteunende teams en interne stakeholders.**

a. **Ondersteunende teams** Het CMT werd door de teams nadrukkelijk gevoed met informatie. De informatie paste bij de vragen en verzoeken van het CMT. Een aandachtspunt is de terugkoppeling van de besluiten aan de ondersteunende teams. Zorg ervoor dat dit op gezette tijden voldoende wordt besproken, bijvoorbeeld door dit op te nemen als vast agendapunt en hier expliciet bij stil te staan. Dit leidt tot meer begrip over de uitvragen aan de ondersteunende teams. Ook stelt het de teams in staat om op basis van de ratio achter de genomen CMT-besluiten zelfstandiger te opereren. Voor dit laatste is het ook belangrijk om het mandaat van de ondersteunende teams nadrukkelijk te bepalen. Welke acties kan het team zelf in gang zetten en welke soort besluiten moeten worden voorgelegd aan het CMT?
Dit geldt in het bijzonder voor de externe inhuur, zowel van Fox-IT als de IT en privacyrecht-advocaat. Vanuit een aantal functionarissen in de ondersteunende is ervaren dat de externen in een behoefte voorzagen waar zij ook zelf in hadden kunnen voorzien. Het is ook voorstelbaar dat het CMT bij een dergelijke crisis behoefte heeft aan extra comfort en deze in die externe inhuur vindt. Maak duidelijk waarom bepaalde externe expertise aansluit bij het CMT en waarom deze partij toegevoegde waarde heeft. Probeer de externe experts in een rustige/koude fase ook alvast bekend te maken met de interne processen en organisatie, dit verhoogt de snelheid van handelen tijdens een crisis.

b. **Interne stakeholders** De HAN hanteerde voor communicatie een duidelijk uitgangspunt van transparantie. Via een liveblog werd steeds een update gegeven en collega-instellingen zijn nadrukkelijk betrokken en gewaarschuwd. Ons advies is om te kijken naar de manier waarop intern gecommuniceerd is. Wij adviseren om de medewerkers van de HAN via een aparte update direct van informatie te voorzien. Het is daarbij belangrijk dat intern kort (seconden/minuten) voor extern gaat. De inhoudelijke communicatieboodschap en duiding hoeven niet af te wijken. Het geeft wel de gelegenheid om enkele interne aangelegenheden te belichten of toe te voegen (bijvoorbeeld aandacht besteden aan de medewerkers die bezig zijn met het afhandelen van alle verzoeken) als de crisis hierom vraagt. Directe communicatie specifiek gericht aan medewerkers verhoogt namelijk op de eerste plaats de betrokkenheid bij de HAN. Interne communicatie versterkt daarnaast ook de externe communicatie; wanneer medewerkers goed geïnformeerd en betrokken zijn dan dragen zij extern de (juiste) boodschap uit. Deze wisselwerking heeft een positief effect op de crisisbeheersing en daarna. Een aparte en directe communicatielijn naar de RvT behoort ook tot de mogelijkheden.

4. **Markeer de omslagpunten tijdens de crisis, in het bijzonder die naar de nafase.** Deze crisis kende een aantal duidelijke kantelpunten. Ten eerste de overgang van de cybercrisis naar de privacycrisis. In de eerste fase is veel onduidelijkheid over het beveiligingslek en sprake van een dreigende ransomware. Dit vereist veel technisch onderzoek en duiding van de dreiging. Dit verschuift naar de privacycrisis. Vanaf die fase treft de HAN veel organisatorische maatregelen en is de voornaamste opgave om alle betrokkenen te informeren. Daarnaast kwam de overgang van de acute fase naar de nafase. In de acute fase is veel onzeker en moet alles in het werk worden gesteld om inzichtelijk te maken wie betrokken zijn en hoe deze te informeren. In de nafase is de stuurgroep nog bezig is met de afhandeling van alle verzoeken. Wij adviseren om deze omslagpunten duidelijker te markeren. Bijvoorbeeld door dit te communiceren naar alle betrokkenen of door het werk na zo'n moment anders te verdelen (wie is in de lead?). Het CMT bleef tot in januari overleggen, terwijl de werkzaamheden vanwege de urgentie zouden kunnen worden belegd in de reguliere lijn of een projectorganisatie.

5. **Verlaag het aantal informatiekanalen ter versterking van het gemeenschappelijk informatiebeeld.** Tijdens de crisis maakte de HAN veel gebruik van MS Teams. Het aantal betrokkenen binnen de crisismanagement organisatie en aantal teams naast het CMT zorgde voor verschillende MS Teams-omgevingen (circa 19). Dit ontstond veelal organisch tijdens de crisis. Het risico hiervan is dat documenten en informatie niet op alle omgevingen en kanalen worden gedeeld en dat niet met up to date documenten gewerkt wordt. Het gemeenschappelijk beeld kan hierdoor vertroebelen. Ons advies is het aantal informatiekanalen tussen teams te beperken of uitsluitend voor specifieke doeleinden (zoals onderlinge communicatie en één aparte omgeving met de meest actuele documenten/informatie) te benutten.
   Bepaal op gezette tijden of de noodzaak van de Teams-omgeving nog steeds aanwezig is. Dit is een verantwoordelijkheid/discipline voor alle betrokkenen, maar er zou ook specifiek iemand voor kunnen worden aangewezen.

6. **Deel de opgedane ervaringen (zowel intern als extern) van deze crisis.** Betrokkenen zijn terecht trots op het vele werk dat is verzet en de samenwerking. Zij waarderen de korte lijnen en gezamenlijke toewijding om de klus te klaren. Al tijdens de crisis had de HAN aandacht voor het delen van ervaringen met collega-instellingen. Met name om bewustwording rondom dergelijke dreiging te vergroten. Wij adviseren om de uitkomsten van de technische en crisismanagement-evaluatie intern en extern te delen. Dit ter verhoging van de algehele bewustwording binnen het onderwijs.

Bijlage 1 Respondenten

Functies
Academiedirecteur
CISO /coördinator team Techniek
Coördinator team Communicatie
Coördinator web team/data-analyse team
Crisiscoördinator
FG
Hoofd ICT
Leden CERT/SOC
Plotter CMT
Scenariohouder Services
Voorzitter CMT
Woordvoerder

Bijlage 2 Afkortingen

Afkortingen	Betekenis
AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
CCT	Crisiscommunicatieteam
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
CMT	Crisismanagementteam
CvB	College van Bestuur
FAQ	Frequently Asked Questions
FG	Functionaris Gegevensbescherming
IE	Intellectueel Eigendom
IM	Informatiemanagement
ISO	Information Security Officer
NCSC	Nationaal Cyber Security Centrum
RvT	Raad van Toezicht
SOC	Security Operations Center
ST	Supportteam

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.