Leerevaluatie cyberaanval

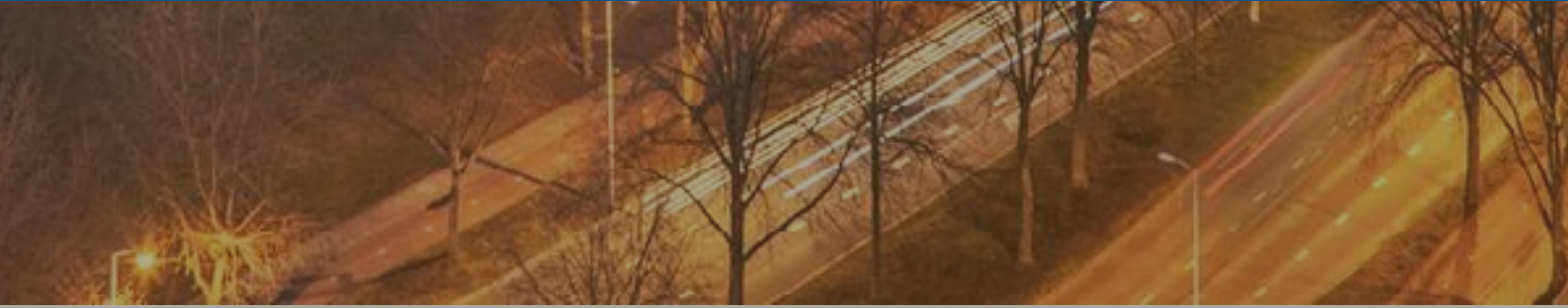
TU Eindhoven op 11 januari 2025

Naar nog meer (cyber)weerbaarheids-DNA

Datum: 14-05-2025

TU/e EINDHOVEN UNIVERSITY OF TECHNOLOGY

COT | Instituut voor Veiligheids- en Crisismanagement



Inhoudsopgave

Bestuurlijke managementsamenvatting

Casus en doel van de leerevaluatie

Op 11 januari 2025 werd de Technische Universiteit Eindhoven (TU/e) getroffen door een cyberaanval. De TU/e haalde het netwerk vervolgens preventief offline om verdere schade te voorkomen. Dit leidde tot een week waarin onderwijs en onderzoek stilstond en studenten en medewerkers geen toegang hadden tot netwerkgebonden systemen. De crisismanagementorganisatie van TU/e werkte samen met externe partners om de impact te beperken en de universiteit weer operationeel te krijgen.

De leerevaluatie van de cyberaanval op TU/e op 11 januari 2025 heeft als doel inzicht te verkrijgen in het functioneren van de crisismanagementorganisatie en de genomen crisisbeheersingsmaatregelen. TU/e streeft ernaar om leerpunten te identificeren en aanbevelingen te formuleren om de weerbaarheid betreffende toekomstige (cyber)crises te versterken en de impact ervan te minimaliseren.

Hoe heeft de TU/e crisisorganisatie gefunctioneerd in het licht van de cyberaanval?

Tijdens de cyberaanval toonde de TU/e zich weerbaar en bleken zij een sterk herstelvermogen te hebben. De crisisaanpak kenmerkte zich door snelle en effectieve technische maatregelen, waarbij de crisisstructuur van TU/e centraal stond en volgens betrokkenen de cultuur binnen TU/e bijdroeg aan ‘alle neuzen dezelfde kant op’ hebben. Ondanks de uitval van standaard communicatiekanalen, slaagde TU/e volgens betrokkenen erin om de impact van de crisis te beperken door de besluitvorming en aanpak te centraliseren en korte lijntjes te onderhouden met faculteiten en diensten. De saamhorigheid binnen de organisatie was volgens betrokkenen duidelijk zichtbaar tijdens nachtelijke en weekenduren en in het sterke vertrouwen in elkaars capaciteiten en verantwoordelijkheden. Ook dit reflecteert de cultuur binnen TU/e. Een belangrijke uitdaging was het werken met gemandateerde besluitvorming binnen het Centrale Crisis Team (CCT) en het waarborgen van transparante communicatie. TU/e moest snel schakelen en handelen, waarbij de IT-crisisteams en het CCT vanaf de eerste meldingen werden geactiveerd. De crisisstructuur en -aanpak waren gebaseerd op het crisisplan, aangevuld met specifieke maatregelen voor de crisissituatie. Faculteiten en diensten werden via vertegenwoordigers in het CCT betrokken en regelmatig communiceerden zij met het hoger management en andere doelgroepen. Een uitdaging was de preventieve afsluiting van het netwerk om verdere criminele schade te voorkomen. Dit besluit leidde tot de tijdelijke stillegging van onderwijs en onderzoek, wat aanzienlijke gevolgen had voor studenten, onderzoekers en medewerkers. TU/e moest snel alternatieve werkwijzen en communicatiemethoden implementeren om de continuïteit van onderwijs en onderzoek te herstellen en de doelgroepen hierover te informeren. De samenwerking met externe partners, zoals IT-contractpartner, autoriteiten en relevante stakeholders, was cruciaal voor een uniforme aanpak en gerichte informatiedeling. TU/e reflecteerde tijdens en na de crisis en scherpte haar aanpak waar nodig aan, wat aantoont dat de organisatie leert van haar ervaringen en deze verwerkt in haar crisisorganisatie en -aanpak. De afschaling van crisisteams en de overdracht naar de reguliere organisatie waren belangrijke stappen in de nafase van de crisis, waarbij TU/e zorg droeg voor een gestructureerde en gecoördineerde afhandeling van de crisis.

Hoe kan TU/e (cyber)weerbaarder worden en haar herstelvermogen versterken voor toekomstige cyberaanvallen?

De aanbevelingen richten zich op het verbeteren van de efficiëntie, coördinatie en veerkracht van TU/e tijdens en na een (cyber)crisis. De specifieke aanbevelingen zijn:

1. **Gestroomlijnde procedures:** Ontwikkel gestroomlijnde procedures voor informatiemanagement en samenwerking tussen crisisteams bij systeemuitval.
2. **Vastleggen IT-mandaten:** Leg kritieke IT-besluiten en bijbehorende mandaten duidelijk vast om verwarring te voorkomen en besluitvorming te stroomlijnen.
3. **Business Continuity Management (BCM) rollen faculteiten en diensten:** Definieer de werkwijze en BCM-rollen van faculteiten en diensten bij uitval van kritieke systemen.
4. **Randvoorwaarden crisisorganisatie:** Leg randvoorwaarden en uitgangspunten voor de crisisorganisatie vast, inclusief eenduidige teamaanduidingen.
5. **Nafase werkwijze:** Werk de werkwijze en opzet voor de nafase uit en integreer deze in het crisisplan.
6. **Samenwerking partners:** Leg de werkwijze van informeren en samenwerken met partners en de onderwijssector vast.
7. **Delen leerevaluatie:** Deel de uitkomsten van de leerevaluatie intern en extern omwille van transparantie en het versterken van het vertrouwen.

1. Inleiding

Zaterdag 11 januari 2025 trof een cyberaanval de Technische Universiteit Eindhoven (hierna: TU/e). TU/e besloot - als één van de maatregelen - hierop (delen van) haar netwerk preventief offline te halen. Na deze maatregelen waren gedurende anderhalve week (alle) netwerkgebonden systemen van TU/e niet beschikbaar. Dit had grote gevolgen voor de kerntaken van TU/e onderwijs en onderzoek. Het onderwijs lag voor de 14.000 studenten van TU/e een week grotendeels stil en hervatte pas volledig weer op maandag 20 januari. De circa 4.700 medewerkers konden niet of moesten op een andere manier aan het werk. Onderzoekers hadden geen toegang meer tot hun onderzoeken die opgeslagen stonden op TU/e servers. Eén van de getroffen maatregelen was ook dat de TU/e haar lessen en tentamens opschoof. Dit om de impact van de cyberaanval zoveel mogelijk te beperken.

Om de crisis het hoofd te bieden schaalde de crisismanagementorganisatie van TU/e gedurende bijna twee weken op, werkte zij samen met diverse partners en nam zij maatregelen om de impact van de cyberaanval te beperken.

1.1 Doel en scope

TU/e wil graag inzicht in het functioneren van de crisismanagementorganisatie en de genomen crisisbeheersingsmaatregelen. Ook wil TU/e leren van de gebeurtenissen en handvatten krijgen voor als zich in de toekomst een soortgelijke situatie voordoet. Daarom vroeg TU/e het COT Instituut voor Veiligheids- en Crisismanagement (COT) een leerevaluatie uit te voeren naar het crisismanagementproces tijdens de opschaling. Parallel aan deze leerevaluatie liep een technische/forensische evaluatie naar de toedracht van de cyberaanval, welke Fox-IT uitvoerde[1].

Het doel van deze leerevaluatie is om op basis van de bevindingen leerpunten te benoemen en aanbevelingen te doen ten behoeve van de voorbereiding op eventuele toekomstige (cyber)crises. Dit om de impact van deze (cyber)crises zoveel mogelijk te beperken en om zo (cyber)weerbaarder te worden.

De hoofdvraag van deze leerevaluatie is als volgt: *Hoe heeft de TU/e crisisorganisatie gefunctioneerd in het licht van de cyberaanval en hoe kan TU/e (cyber)weerbaarder worden en haar herstelvermogen versterken voor toekomstige cyberaanvallen?*

Hierbij zien wij weerbaarheid als een mix van[2]; *risicomanagement* (capaciteit om bedreigingen op de doelstellingen te voorkomen), *continuïteitsmanagement* (capaciteit die een organisatie heeft om na (of anticiperend op) een verstoring de continuïteit op een vooraf vastgesteld niveau te houden) en *crisismanagement* (capaciteit om strategische doelen, reputatie en voortbestaan onder afwijkende, abnormale en complexe omstandigheden te waarborgen).

Om deze hoofdvraag te beantwoorden, keken wij naar enkele deelvragen.

- Wat waren sleutelmomenten en -besluiten, dilemma's en uitdagingen voor de crisisteams en reguliere organisatie?
- Wat is het effect van het handelen van het Centraal Crisisteam (CCT) en Team Operations en haar besluitvorming op de interne doelgroepen (studenten, docenten en medewerkers) en primaire processen Onderzoek en Onderwijs?
- Hoe is het informatiemanagement en de samenwerking tussen het CCT en het Team Operations en tussen de crisisteams en reguliere organisatie verlopen?
- Hoe is de interne en externe crisiscommunicatie verlopen?
- Wat kunnen we leren van de afhandeling van het incident en hoe kunnen lessen in het TU/e crisisplan (en eventueel continuïteitsplan) en OTO-plan (opleiden, trainen en oefenen) worden geborgd?

[1] Het onderzoek van Fox-IT focuste op hoe de detectie, incident response en het forensisch onderzoek bij de TU/e plaatsvond. Ook geeft het een reconstructie van de cyberaanval op basis van het forensisch onderzoek en aanbevelingen die het risico verkleinen dat de TU/e nogmaals slachtoffer wordt van een cyberaanval in de toekomst.
[2] Naar ISO 3100: 2009, BS ISO 22300: 20212 en BS PAS 200: 2011 en CEN/TS 17091

Ter verduidelijking van het escalatieproces is een tijdlijn opgesteld. Deze is te vinden in bijlage A.

1.2 Onderzoeksaanpak

Deze leerevaluatie is uitgevoerd in de periode tussen 3 maart en 12 mei 2025. Voorafgaand aan het onderzoek is met TU/e, als opdrachtgever, overleg gevoerd over de aanpak en afbakening van onderzoeksdoelen en -vragen.

Voor het beantwoorden van de onderzoeksvragen analyseerden wij verschillende documenten, zoals het technische rapport van Fox-IT, interne evaluaties, vragenlijsten, tijdlijnen, notulen van crisisvergaderingen, planvorming, protocollen en afspraken, etc. In bijlage B is een overzicht opgenomen van de gebruikte documenten die door TU/e voor dit onderzoek ter beschikking zijn gesteld. Naast de documentenanalyse voerden de onderzoekers 22 gesprekken met betrokkenen vanuit TU/e, waaronder leden van het CCT en Library and Information Services Crisis Management Team (LIS-CMT). Ook spraken de onderzoekers met partners van TU/e als Surf, de inspectie van het onderwijs, ministerie van Onderwijs, Cultuur en Wetenschap (OCW) en Universiteiten van Nederland (UNL). De bevindingen in dit rapport zijn gebaseerd op de informatie verkregen uit de gesprekken met respondenten. Zoals gebruikelijk bij dit type evaluaties is de informatie die door de onderzoekers in de gesprekken met respondenten werd verkregen getoetst bij andere respondenten. Dit om een zo compleet mogelijk beeld te krijgen van de situatie. In de evaluatie zijn geen indicatoren gebruikt die konden objectiveren. Hierbij valt te denken aan of een alarmering “op tijd”, “laat” of “te laat” was. Of: een besluit “goed” of “fout”. Of: aldus norm x of y. In bijlage C is een overzicht van de afkortingen die in het rapport zijn gebruikt te vinden.

Het streven was primair om een schets te geven van de bijzondere ontwikkelingen die met de cyberaanval gepaard gingen en waar de aanpak in resulteerde. Het is nadrukkelijk geen verantwoordingsrapportage. Het doel is om alertheid te creëren die TU/e kan helpen om in de toekomst beter met dit type calamiteiten om te gaan. Vanwege de vertrouwelijke aard van de gesprekken zijn geen schriftelijke verslagen gemaakt. De opbrengst van de gesprekken is direct verwerkt in deze rapportage. In bijlage D is een overzicht opgenomen van de respondenten.

Tot slot organiseerden wij op 17 april 2025 een interne lessensessie. Doel van de lessensessie was om informatie op te halen, leerpunten uit de interviews scherper te krijgen en deze informatie en leerpunten, in samenspraak met betrokkenen, beter te duiden. Daarnaast hebben we voorbeelden, uitdagingen en dilemma’s verzameld en geïnventariseerd waar de deelnemers kansen zien voor versterking. In de weken van 28 april tot en met 11 mei 2025 is de opdrachtgever in staat gesteld om feitelijke onjuistheden in het rapport te corrigeren.

1.3 Leeswijzer

In hoofdstuk 2 behandelen wij de tijdlijn. In hoofdstuk 3 bespreken wij het overkoepelend beeld. In hoofdstuk 4 gaan wij in op onze observaties.

2. Tijdlijn

Op zaterdag 11 januari 2025 om 21.21 uur ontvangen de systeem administratoren van TU/e, het CERT van TU/e en de IT-contractpartner Fox-IT een geautomatiseerde melding. Een medewerker van Library and Information Services (LIS) die zijn mail checkt en de melding leest, ziet dat sprake is van verdachte activiteit op de servers van de TU/e. De melding markeert het begin van een omvangrijke crisis voor TU/e met grote gevolgen voor de primaire taakstelling van TU/e; onderwijs en onderzoek.

De medewerker is direct alert wanneer hij de eerste melding ziet en roept de hulp van zijn collega's in. Zij overleggen vervolgens via Teams. De PAL (Product Area Lead) platforms worden geïnformeerd. Een half uur na de initiële melding belt Fox-IT het Computer Emergency Response Team (CERT) om hen te waarschuwen voor de verdachte activiteiten op de servers van TU/e. Twee uur na de initiële melding komen de PO (product owner) Security Operations, PAL platforms, plaatsvervangend directeur LIS en Chief Information Security Officer (CISO) bij elkaar voor een eerste LIS-CMT overleg met beperkt comité. Hierin zijn zij voornemens het besluit te nemen de verbinding met het netwerk te verbreken. De CISO belt hierover met de programmadirecteur integrale veiligheid (de technisch voorzitter van het CCT) en spreekt af dit voorgenomen besluit zo snel mogelijk in werking te laten treden alsook het CCT bijeen te laten komen en op te schalen. Ook wordt de politie geïnformeerd. Rond middernacht schaalt Fox-IT haar operatie op en vertrekt zij richting de campus. De politie arriveert korte tijd later. Op zondag 12 januari 01.00 uur overleggen de CISO, PAL platforms, plaatsvervangend directeur LIS en de programmadirecteur integrale veiligheid. Rond dit tijdstip wordt voor het eerst contact gelegd met een bestuurslid van TU/e, de Secretaris van het College van Bestuur. Zij toetsen bij hem het voorgenomen besluit rondom het afsluiten van het netwerk. Pas rond kwart over één ligt het TU/e netwerk volledig plat. Rond 03.00 uur arriveren medewerkers van Fox-IT op de campus. De rest van de crisis blijven zij aangehaakt in een adviesrol.

Diezelfde ochtend vindt om 09.00 uur het eerste CCT plaats. Naast alle CCT-leden zijn hierbij ook een aantal LIS-CMT leden aanwezig, namelijk de PAL Platforms, Chief Privacy Officer, Directeur LIS en plaatsvervangend Directeur LIS. In het CCT besluiten de crisisfunctionarissen meer informatie te verzamelen, informatiebijeenkomsten voor de decanen en directeuren te gaan organiseren, het College van Bestuur en de Raad van Toezicht te informeren, om 12.00 uur te communiceren via de website alsook het darkweb en sociale media te monitoren. Rond 15.00 uur staat uiteindelijk het eerste communicatiebericht op de website van TU/e. Zij geven hierin aan dat maandag geen onderwijs mogelijk is. De TU/e stelt de media dezelfde dag nog op de hoogte.

Een dag later, op maandag 13 januari om 08.45 uur, start het eerste LIS-CMT met uitgebreid comité. Gedurende dit overleg stellen het LIS-CMT en LIS-CRT doelen en een prioritering vast. Het primaire doel van het LIS-CMT is om te begrijpen wat gebeurd is en wat op dit moment gaande is in het netwerk. Dit om inzicht te krijgen in de situatie. Het secundaire doel is om de systemen te herstellen en weer online te brengen. Het tertiaire doel is om de verwerking op forensisch vlak te voltooien. Het Crisis Response Team (CRT) van LIS stelt zich tot doel om de IT-infrastructuur weer voldoende veilig te maken, zodat de systemen weer terug online kunnen worden gebracht. Verder besluit het LIS-CMT onder andere om Signal voor de crisisoverleggen in te zetten en de privacy afdelingen te informeren wanneer zij een rapport hebben over de impact op persoonlijke data voor de Autoriteit Persoonsgegevens.

Om 10.00 vindt een tweede CCT plaats. Hier stemt het CCT in met het voorstel vanuit Education and Student Affairs (ESA) om dinsdag geen onderwijs te verzorgen. De eerste signalen wijzen erop dat de dader op heterdaad betrapt is. Later op de dag stelt het LIS-CMT vast dat de hackers geen data stalen of versleutelden. Verder besluit het CCT dat zij elke dag om 16.00 uur een communicatiebericht met een update over de situatie op de website te gaan zetten en zet TU/e een balie op waar studenten en medewerkers heen kunnen als zij vragen hebben.

Op dinsdag 14 januari wijzigt het CMT haar doelen en bijbehorende prioritering. Het primaire doel richt zich nu op het herstellen en weer online brengen van de systemen. Het secundaire doel richt zich op het begrijpen en onderzoeken wat gaande is. Het tertiaire doel is om voldoende ondersteuning te bieden om het opnieuw activeren van het netwerk en de applicaties mogelijk te maken. Het quartaire doel om de forensische verwerking te voltooien. Verder besluit het CCT die dag om de academische kalender één week op te schuiven en de onderwijsweek waarin de cyberaanval plaatsvindt te laten vervallen; het formele onderbouwde besluit hierover volgt op 16 januari. Ook besluit het CCT om de SaaS-applicaties (Software as a Service) die beheerd worden door LIS maar niet op het netwerk van

TU/e staan, weer online te brengen. De servers die LIS niet beheert, hetgeen voornamelijk onderzoeksservers zijn, hebben een lagere prioriteit gezien een beperkte groep hier gebruik van maakt. Daarom besluit het CCT deze nog langere tijd ontoegankelijk te laten en andere servers prioriteit te geven.

Op woensdag 15 januari vindt een grote Distributed Denial-of-Service (DDoS) aanval plaats op het netwerk van Surf. Hierdoor ontstaan zorgen over of dit een relatie heeft met de cyberaanval op de TU Eindhoven. Later blijkt dit niet het geval te zijn. Verder meldt TU/e dat zij verwacht dat een groot deel van haar netwerk voor het weekeinde weer veilig en beschikbaar is en de daders op heterdaad betrapt zijn. Aan het einde van de dag kunnen gebruikers weer inloggen in de SaaS-systemen, maar lukt dit in de praktijk nog niet overal. Ook is de Teams omgeving weer beschikbaar. Op donderdag 16 januari stemt het CCT in met de aanpassingen op het assessmentplan met betrekking tot studeerbaarheid. Ook organiseert het CCT een ander telefoonnummer ter vervanging van de noodnummers. Deze zijn niet meer bereikbaar door de DDoS-aanval. Op vrijdag 17 januari meldt TU/e dat zij naar verwachting maandag het onderwijs weer kunnen hervatten. Ook besluit het CCT die dag om een regeling te treffen voor studenten die reeds vakanties boekten en hierdoor niet aanwezig kunnen zijn bij verplaatste tentamens of herkansingen. Zij stellen een alternatieve tentamenmogelijkheid beschikbaar als studenten kunnen aantonen dat zij in de knel komen. Verder gaan zij het selectieproces voor nieuwe studenten met vijf werkdagen verlengen.

Gedurende het weekend vinden tests van de systemen plaats om te zorgen dat hervatting van het onderwijs en de bedrijfsvoering soepel verloopt. Op zaterdag 18 januari past het LIS-CMT haar uitgangspunten aan. Het primaire doel is het verder beveiligen en ondersteunen van de organisatie op het gebied van beveiliging, algemene ondersteuning voor de hele organisatie en ondersteuning voor onderzoeksdoelen. Het secundaire doel is het voltooien van de forensische verwerking en rapportage. Op zondag 19 januari communiceert TU/e om 16.00 uur op haar website dat het testen van de systemen succesvol verliep en het onderwijs maandag hervat.

Maandag 20 januari start het onderwijs weer zonder grote problemen. Op dat moment zijn nog enkele onderzoeksservers onbereikbaar gezien LIS deze nog niet hersteld heeft. Op dinsdag 21 januari vond om 09.00 uur de laatste CCT-vergadering plaats. Om 16.00 uur publiceerde TU/e een laatste communicatiebericht op haar website, waarin zij een afschaling van de crisisorganisatie aankondigen. Ook geven zij aan een forensisch onderzoek en een externe evaluatie uit te voeren.
Op 23 januari besluit het College van Bestuur dat studenten die financiële schade leden door de cyberaanval gebruik kunnen maken van een noodfonds. Hiervoor maken zij tienduizend euro vrij.

Op 27 januari vindt het laatste LIS-CMT-overleg plaats. Een aantal onderzoeksservers zijn dan nog niet hersteld. Het verdere herstel van deze servers pakt LIS vanuit de reguliere lijn op. Het crisisafhandelingsteam van ESA blijft uiteindelijk het langste opgeschaald. Pas vier weken na de start van het incident schalen zij af.

3. Overkoepelend beeld en aanbevelingen

3.1 Overkoepelend beeld

Hoe heeft de TU/e crisisorganisatie gefunctioneerd in het licht van de cyberaanval en hoe kan TU/e (cyber)weerbaarder worden en haar herstelvermogen versterken voor toekomstige cyberaanvallen?

Op basis van de leerevaluatie is het antwoord op het eerste deel van de onderzoeksvraag (*Hoe heeft de TU/e crisisorganisatie gefunctioneerd in het licht van de cyberaanval* …) als volgt:

Tijdens de cybercrisis toonde de TU/e zich weerbaar en bleken zij een sterk herstelvermogen te hebben. De crisisaanpak kenmerkte zich door snelle en effectieve technische maatregelen, waarbij de crisisstructuur van TU/e centraal stond en volgens betrokkenen de cultuur binnen TU/e bijdroeg aan 'alle neuzen dezelfde kant op' hebben. Ondanks de uitval van standaard communicatiekanalen, slaagde TU/e volgens betrokkenen erin om de impact van de crisis te beperken door de besluitvorming en aanpak te centraliseren en korte lijntjes te onderhouden met faculteiten en diensten. De saamhorigheid binnen de organisatie was volgens betrokkenen duidelijk zichtbaar tijdens nachtelijke en weekenduren en in het sterke vertrouwen in elkaars capaciteiten en verantwoordelijkheden. Ook dit reflecteert de cultuur binnen TU/e. Een belangrijke uitdaging was het werken met gemandateerde besluitvorming binnen het Centrale Crisis Team (CCT) en het waarborgen van transparante communicatie. TU/e moest snel schakelen en handelen, waarbij de IT-crisisteams en het CCT vanaf de eerste meldingen werden geactiveerd. De crisisstructuur en aanpak waren gebaseerd op het crisisplan, aangevuld met specifieke maatregelen voor de crisissituatie. Faculteiten en diensten werden via vertegenwoordigers in het CCT betrokken en regelmatig communiceerde de TU/e met het hoger management en andere doelgroepen. Een uitdaging was de preventieve afsluiting van het netwerk om verdere criminele schade te voorkomen. Dit besluit leidde tot de tijdelijke stillegging van onderwijs en onderzoek, wat aanzienlijke gevolgen had voor studenten, onderzoekers en medewerkers. TU/e moest snel alternatieve werkwijzen en communicatiemethoden implementeren om de continuïteit van onderwijs en onderzoek te herstellen en de doelgroepen hierover te informeren. De samenwerking met externe partners, zoals IT-contractpartner Fox-IT, autoriteiten en relevante stakeholders, was cruciaal voor een uniforme aanpak en gerichte informatiedeling. TU/e reflecteerde tijdens en na de crisis en scherpte haar aanpak waar nodig aan, wat aantoont dat de organisatie leert van haar ervaringen en deze verwerkt in haar crisisorganisatie en -aanpak. De afschaling van crisisteams en de overdracht naar de reguliere organisatie waren belangrijke stappen in de nafase van de crisis, waarbij TU/e zorgdroeg voor een gestructureerde en gecoördineerde afhandeling van de crisis.

Hieronder volgt de meer specifieke onderbouwing van het antwoord op het eerste deel van de onderzoeksvraag.

Tijdige crisisaanpak en saamhorigheid bij TU/e. Volgens betrokkenen heeft TU/e met haar (crisis)organisatie snel gehandeld met betrekking tot haar technische maatregelen, is zij vanaf de start met haar IT-team en organisatiebrede crisisstructuur opgeschaald. Zij gebruikte haar crisisstructuur om de impact van de crisis te beperken, de besluitvorming en aanpak te centraliseren en zorg te dragen voor korte lijntjes met faculteiten en diensten. Zij heeft dit gedaan in een situatie waarbij de meeste standaard communicatiekanalen niet betrouwbaar waren om in te zetten. Zij heeft de crisisaanpak vormgegeven ondanks (of dankzij) uitval van systemen en communicatiemiddelen.

TU/e heeft met vele betrokkenen de schouders eronder gezet en gehandeld. De saamhorigheid was volgens betrokkenen mede zichtbaar in de overleggen, het doorwerken in de nachtelijke/weekend uren en het vertrouwen in elkaars verantwoordelijkheden en kunnen (capaciteit/competenties) wat meermaals naar elkaar is uitgesproken en ook zo ervaren is. *Het weerbaarheids-DNA (of familiegevoel zoals sommige betrokkenen het noemen) van TU/e is hierin naar voren gekomen en heeft erger voorkomen.*

Gemandateerde besluitvorming bij CCT en transparante communicatiestrategie. TU/e werkte met gemandateerde besluitvorming en handelde en stemde af met de betrokken stakeholders,

diensten en faculteiten. Allen waren in het CCT vertegenwoordigd en haakten hun achterban/doelgroepen aan waar nodig. De impact is inzichtelijk gemaakt (zowel op fysieke gebouwen, systemen, onderwijs, onderzoek, doelgroepen, etc.). Besluiten en dilemma's bereidde TU/e voor in de teams van de diensten en faculteiten. De adviezen/scenario's werkte TU/e uit, legde zij voor aanvullingen en draagvlak voor en communiceerde na besluitvorming in het CCT over de genomen besluiten. TU/e slaagde erin de interne doelgroepen te blijven bereiken en betrekken, onder andere door te focus te leggen op middelen en werkwijze. Het gebruik van de website, dagelijkse updates, aanhaken en informeren van doelgroepen en eenduidige inzet van onder andere 1 telefoonnummer en systeem, etc.). Transparant zijn over de situatie en aanpak was een belangrijk onderdeel van de communicatiestrategie.

Volgens betrokkenen zijn de crisisteams tijdig geactiveerd na systeemuitval en vond coördinatie en herstel plaats in nauwe samenwerking met faculteiten en diensten. De IT-organisatie schakelde in de nacht van zaterdag 11 januari snel na de eerste meldingen. Betrokkenen geven aan dat de IT-crisisteams (LIS-CMT en LIS-CRT) en het CCT vervolgens al snel werden geactiveerd. Vanaf zondagochtend 12 januari lag de regie bij het CCT. Dit ging in nauwe samenwerking met het LIS-CMT (en LIS-CRT). De crisisteams werkten met een afgestemde vergaderklok. De crisisstructuur en -aanpak was hiermee gebaseerd op het crisisplan, aangevuld en gespecifieerd naar de crisissituatie. Zo waren de faculteiten en diensten aangehaakt via vertegenwoordigers/directeuren in het CCT (denk aan onderwijs, onderzoek en bedrijfsprocessen) en hadden zij veelal hun eigen (operationele) crisisteams. Daarbij werd het hoger management (directeuren en decanen) geïnformeerd en bevraagd via dagelijks, periodieke/frequente momenten. Andere doelgroepen werden bevraagd en geïnformeerd via onder andere de ESA-ketens.

Inhoudelijke voorbereiding lijkt beperkt vast te zijn gelegd. Bijvoorbeeld wat faculteiten en diensten moeten doen bij volledige uitval van systemen, wat zijn alternatieve werkwijzen, wat zijn afspraken hoe elkaar te bereiken of onderwijs of onderzoek te verzorgen. Bij de applicaties/systemen is een overzicht van 'kroonjuwelen' aanwezig en is verder geprioriteerd op wat technisch mogelijk was of is en zijn in samenspraak met vertegenwoordigers keuzes gemaakt ten behoeve van herstel.

Communicatie tijdens de crisis: rol voorzitters, gebruik Signal-appgroepen en flexibele structuur voor faculteiten en diensten. Het informeren van de crisisteams is met name via de voorzitters verlopen tijdens de fysieke crisisoverleggen. Ook gebruikten de crisisteams nieuw aangemaakte Signal-app groepen om informatie, crisisoverlegverslagen en andere documentatie met elkaar te delen. Omdat de toegang tot de applicaties niet consistent was voor de circa 14.000 studenten en circa 4.700 medewerkers, heeft TU/e haar crisisstructuur gebruikt om deze groepen te bereiken. Zij gebruikte hiervoor verder met name dagelijkse updates via haar website, nieuw aangemaakte Signal (of Whatsapp)-appgroepen van de diverse interne stakeholders en één kanaal voor vragen: een TU/e Whatsapp nummer. Verder was het vrij aan de faculteiten en diensten om zich te organiseren en op een voor hun passende wijze te communiceren met de eigen doelgroepen die aansloot op de reguliere manier van communiceren. Dit gaf veel vrijheid en maatwerkmogelijkheden, alleen verschilde de manier en wijze van communiceren hiermee wel tussen de faculteiten en diensten.

Preventieve netwerkafsluiting bij TU/e om criminele schade te voorkomen en gevolgen voor onderwijs en onderzoek te beperken. Het afsluiten van het netwerk heeft verdere criminele schade voorkomen. In de nacht van 11 januari is het netwerk preventief afgesloten om hackers geen toegang meer te verschaffen tot het netwerk en schade en datadiefstal te voorkomen en/of te beperken. Het vertrouwen en mandaat om dit besluit te nemen is tijdens deze crisis binnen de IT-organisatie gevoeld en bestendigd door het bestuur. Wel kan TU/e het mandaat en de werkwijze volgens betrokkenen verder uitwerken en waren deze niet altijd bekend bij betrokkenen in de crisisorganisatie. Door het besluit was het ook niet mogelijk om op de reguliere wijze onderwijs te volgen en onderzoek uit te voeren of bijv. examens en promoties doorgang te laten vinden. Op zondag is daarom besloten om medewerkers en studenten op te roepen niet naar de campus te komen. Op dinsdag is in het CCT besloten om de hele onderwijsweek te verplaatsen en verschuiven. Op die manier kreeg IT de tijd alle systemen weer te testen en online te brengen. De organisatie had hierdoor tijd om deze wijziging voor te bereiden (denk aan impact op tentamens, onderwijs, activiteiten, examenregelingen, etc.). TU/e is, zoals veel universiteiten decentraal georganiseerd, waardoor veel binnen een faculteit is en wordt georganiseerd. Via zogenaamde ESA-ketens werkt TU/e met vertegenwoordigers en in stappen toe naar centrale besluitvorming. Deze ketens zijn ook gehanteerd ten behoeve van de besluitvorming en (scenario)uitwerkingen.

Autoriteiten, Fox-IT en relevante stakeholders betrokken bij crisisaanpak en informatiedeling. TU/e heeft aangifte gedaan bij de politie en de Autoriteit Persoonsgegevens is geïnformeerd. Fox-IT is direct ondersteunend aangesloten als technisch IT-contractpartner vanaf de eerste uren van de inzet. Met de Raad van Toezicht, Surf, het netwerk van Universiteiten van Nederland (UNL), het ministerie van OCW (Onderwijs, Cultuur en Wetenschap) is nauw en frequent (persoonlijk) contact. Ook had de TU/e contact met de inspectie van het onderwijs. De contacten met deze stakeholders gingen veelal via de bestuurlijke of IT/operationele lijn. Dit droeg volgens betrokkenen bij aan een uniform(e) aanpak, beeld en communicatie-uitingen. Ook konden zo andere instellingen preventief voorbereid/geïnformeerd worden indien nodig. De samenwerking en informatiedeling intensiveerde toen de onderwijssector en Surf in dezelfde week werden getroffen door een DDoS aanval.

Reflectie en verbetering van crisisaanpak bij TU/e tijdens en na incident. De TU/e crisisorganisatie heeft tijdens de inzet al gereflecteerd, geleerd en op momenten haar aanpak aangescherpt. Dit blijkt bijvoorbeeld uit enkele klankbordrollen in de crisisteams (onder andere bij het CCT en LIS-CMT) en het aanscherpen van procedures (volgorde van informeren/betrekken voorafgaande aan het updaten van de website). Ook is TU/e na de inzet gaan evalueren binnen de faculteiten, diensten en crisisteams. Hierin hebben zij diverse inzichten en (praktische) leerpunten opgehaald, zowel omtrent de (crisis)teams en aanpak alsook de werkwijze binnen de faculteiten en diensten. Dit laat zien dat TU/e leert van haar inzetten en dit verwerkt in haar (crisis)organisatie en aanpak. Een verbeterpunt is dat in de praktijk diverse termen worden gehanteerd voor de teams; ‘crisisteam’, ‘operationele teams’, ‘facultaire/diensten crisisteams’, etc., waardoor op momenten spraakverwarring ontstaan.

Afschaling van crisisteams en overdracht naar reguliere organisatie. De crisisteams zijn op verschillende momenten afgeschaald, nafase plannen en werkwijzen blijven hierbij noodzakelijk. Bij de afschaling is de aanpak weer overgedragen aan de reguliere organisatie. Zij koos er expliciet voor om het CCT af te schalen na ruim één week en zorg te dragen voor versnelde besluitvorming voor benodigde CvB-besluiten. Het LIS-CMT (IT) is afgeschaald na circa 2 weken en bijvoorbeeld het ESA-crisisteam na circa een maand. In met name de tweede, derde en vierde week is wel gebleken dat ook deze fase onderdeel uitmaakt van de crisisafhandeling (nafase) en dat waar nodig capaciteit vrijgespeeld moet blijven. Ook vraagt dit bewustwording bij de rest van de organisatie.

3.2 Aanbevelingen

Op basis van deze leerevaluatie is het antwoord op het tweede deel van de onderzoeksvraag (‘…*en hoe kan TU/e (cyber)weerbaarder worden en haar herstelvermogen versterken voor toekomstige cyberaanvallen?*) als volgt:

1. **Ontwikkel een gestroomlijnde procedure voor informatiemanagement en samenwerking tussen crisisteams juist bij uitval van systemen en leg dat vast**. Hetzelfde geldt voor het bereiken (en inzichtelijk maken) van alle interne doelgroepen. Maak hierover afspraken en verwerk dit in de planvorming. De opbrengst van deze aanbeveling is een verbeterde efficiëntie en coördinatie tijdens crises door gestroomlijnde procedures voor informatiemanagement en samenwerking tussen crisisteams. Daarnaast zorgt het voor duidelijkheid en betere bereikbaarheid van interne doelgroepen, wat de organisatie beter voorbereidt op toekomstige crises.

2. **Leg kritieke IT-besluiten en de mandaten die daarbij horen duidelijk vast**.
   Voor het vastleggen van de meest kritieke IT-mandaten tijdens een crisis bij TU/e, is het cruciaal om duidelijke rollen en verantwoordelijkheden te definiëren voor reguliere mandaten, evenals voor het operationeel en strategisch crisisteam. Dit zorgt ervoor dat dit niet persoonsafhankelijk is en *iedereen* weet wie welke beslissing mag nemen, hetgeen verwarring voorkomt en de besluitvorming stroomlijnt. Hierdoor kan TU/e effectief en efficiënt reageren op crisissituaties en versterkt het de huidige mandaat-/verantwoordelijkheidsverdeling. We denken hierbij aan het opstellen van een mandatenmatrix. Kritieke IT-besluiten omvatten het:
   - onmiddellijk stopzetten van geïnfecteerde of verdachte IT-systemen;
   - activeren van back-upsystemen en het herstellen van gegevens;
   - segmenteren van het netwerk om verdere verspreiding van de aanval te voorkomen;
   - beperken of intrekken van gebruikersrechten om verdere schade te voorkomen;
   - onmiddellijk toepassen van beveiligingspatches en updates op kwetsbare systemen.

3. **Leg vast wat de werkwijze/Business Continuity Management (BCM) rollen zijn van faculteiten en diensten bij uitval van (kritieke) applicaties/systemen.**
Draag zorg – op hoofdlijnen – voor duidelijkheid wat de werkwijze is bij uitval en wat op welke wijze is vorm te geven. Leg hierin ook vast welke afspraken worden gemaakt ten behoeve van onderwijs, onderzoek en bedrijfsprocessen. Zo wordt het ook makkelijker afhankelijkheden inzichtelijker te maken en prioriteiten te bepalen. De opbrengst van deze aanbeveling is dat het vastleggen van procedures voor faculteiten en diensten bij uitval van kritieke systemen zorgt voor duidelijkheid en structuur in de werkwijze. Dit maakt afhankelijkheden en prioriteiten inzichtelijker en versterkt de samenwerking met de IT-organisatie bij mogelijke uitval.

4. **Leg de randvoorwaarden/uitgangspunten voor de crisisorganisatie vast en zorg voor eenduidige teamaanduidingen.**
De organisatie heeft veel vormgegeven in haar crisisafhandeling en veel gerealiseerd. Leg deze (gewenste) werkwijze, locaties en dergelijke vast. Denk hierbij aan crisisteam locaties/ruimten, randvoorwaarden en uitgangspunten voor de aflossing en continuïteit crisisteams, rol van observator, communicatiemiddelen en structuur, etc. Wees daarbij scherp op teamnamen/duidingen en leg dit vast.

5. **Werk in aanvulling op het integraal crisisplan de werkwijze en opzet voor de nafase uit**.
De nafase is gericht op het effectief afhandelen van de lange termijn uitdagingen van een crisis. Het doel is om TU/e in staat te stellen thema's voor de nafase te inventariseren en een gedetailleerd nafase(project)plan op te stellen. De nafase begint vaak al tijdens de acute fase van een crisis en is uniek in omvang, complexiteit en dynamiek. Een systematische aanpak kan veel onnodige problemen op middellange en lange termijn voorkomen en helpt bij het herstellen en zoeken naar een nieuw normaal. Het is belangrijk om sleutelfunctionarissen te trainen, een diagnose van de nafase uit te voeren en een duidelijke organisatiestructuur en doelstellingen vast te stellen. Integreer deze werkwijze in het integraal crisisplan.

6. **Leg de werkwijze van informeren en samenwerken met de partners en onderwijssector vast en initieer, waar nodig, afspraken.**
Het informeren en betrekken van het netwerk heeft diverse, over het algemeen positieve inzichten opgeleverd over informeren, betrekken en gezamenlijk optrekken (o.a. ook bij de DDoS-aanval). Dit heeft de sectoraanpak en samenwerking versterkt. Verwerk deze inzichten in de sectorafspraken, bestendig dit en laat dit niet afhangen van betrokken personen. Zo wordt ook voorkomen dat stakeholders te laat worden geïnformeerd/aangehaakt.

7. **Deel de uitkomsten van deze leerevaluatie intern met studenten en medewerkers (TU/e community) en extern met geïnteresseerde partijen, zoals de onderwijssector.**
Het delen van de uitkomsten van de leerevaluatie is essentieel voor transparantie en het versterken van vertrouwen bij studenten, medewerkers en externe partijen. Het bevordert het leren en verbeteren van crisismanagementprocedures, zowel binnen TU/e als in andere onderwijsinstellingen. Daarnaast ondersteunt het de samenwerking en bevordert het best practices in crisismanagement.

4. Observaties

4.1 Inleiding

In dit hoofdstuk schetsen wij onze observaties ten aanzien van de tijdens de cyberaanval ingezette crisisstructuur en -teams van TU/e. De thema's die aan bod komen zijn: de crisisstructuur en -teams van TU/e, de besluitvorming, dilemma's en scenario's tijdens de crisis, de interne en externe communicatie, de impact van de cyberaanval op onderwijs, onderzoek en interne doelgroepen, de samenwerking met externe partners, het leren als organisatie en de evaluatie van de crisisaanpak, de nafase en afschaling van crisisteams, specifieke aspecten van de cyberaanval en de technische respons en de planvorming.

4.2 De crisisstructuur en -teams

TU/e beschikt over een crisisstructuur met verschillende crisisteams om de samenwerking in crisistijd vorm te geven. TU/e organiseert de crisisrespons centraal. TU/e beschikt over een strategisch crisisteam: het Centrale Crisis Team (CCT). Dit team bepaalt de overkoepelende strategie en aanpak, neemt de strategische besluiten en heeft de regie over de crisisrespons. De IT(crisis)organisatie valt onder de dienst LIS. Zij heeft een tactisch crisisteam (LIS-CMT) en een operationeel/respons team (LIS-CRT). Hiermee valt het LIS-CMT onder het CCT. Het LIS-CMT zorgt op tactisch niveau voor de uitwerking van de door het CCT genomen besluiten. Bij een cyberincident zit het LIS-CRT op operationeel niveau en geven zij vorm aan de cybercrisisrespons. Onder het CCT opereren ook nog diverse andere crisisteams die uitvoer en uitwerking geven aan de besluiten van het CCT. Zo doen de facultaire crisisteams dit voor de facultaire crisisrespons, doet het ESA crisisteam dit voor de crisisrespons met betrekking tot de onderwijsondersteunende taken, doet het HR-crisisteam dit voor de crisisrespons van HR en doet het crisiscommunicatieteam dit voor de crisisrespons rondom communicatie. Naast de crisisteams heeft TU/e ook projectteams ten behoeve van de uitwerking. Daarnaast heeft TU/e overleggremia voor het ophalen van informatie, afstemmen en creëren van draagvlak. Denk hierbij bijvoorbeeld aan de gedecentraliseerde gremia per faculteit als de examencommissie, toetsingscommissie en planning die centraal samenkomen in één ESA-keten.

Volgens betrokkenen gaf TU/e de samenwerking ten tijde van de crisis gestructureerd vorm. De verschillende crisisteams sloten zoveel mogelijk aan op reguliere lijnen binnen de organisatie. De faculteiten en diensten haakte TU/e aan door vertegenwoordigers hiervan aan te laten sluiten bij het CCT. Ieder CCT-lid informeerde haar eigen achterban en zette daar de acties/besluiten uit (het 'halen en brengen'). De directeur LIS en CISO vertegenwoordigden het LIS-CMT in het CCT. Dit zorgde voor een goede en nauwe samenwerking en uitwisseling van informatie, vragen, besluiten en dergelijke, aldus respondenten. Verder informeerde het CCT dagelijks het hoger management door middel van informatiebijeenkomsten, waar ook informatie werd opgehaald en (de impact) besproken. Overige doelgroepen bevroegen de crisisteams via hun geëigende (en reguliere) kanalen. De crisisteams onderhielden daarnaast regelmatig contact met stakeholders om hen te informeren en af te stemmen.

In algemene zin is TU/e trots op haar crisisaanpak en heeft zij voor een crisisstructuur die paste bij de situatie gekozen. Betrokkenen geven aan dat zij vinden dat TU/e adequaat op de cyberaanval reageerde. Volgens hen is de opschaling snel verlopen en heeft TU/e de juiste professionals betrokken. Onder regie van het CCT heeft de crisisorganisatie nauw samengewerkt. Door een duidelijke structuur en een vergaderklok in te zetten, heeft de crisisorganisatie haar regierol behouden. Hierbij hebben de crisisteams nadrukkelijk oog voor de impact van de besluiten gehad. Dit blijkt bijvoorbeeld uit het besluit om alternatieve tentaminering te verzorgen voor studenten die al eerder plannen hadden gemaakt en in de knel kwamen door de verschuiving van de lesweek, maar ook uit het besluit om de stekker uit het netwerk te trekken en zo grotere schade te voorkomen.

Betrokkenen waren tevreden over de werking van de crisisstructuur. Zij gaven aan dat de crisisteams goed op elkaar aansloten, sleutelpersonen rolvast waren en goed samenwerkten. Het CCT had de leiding en de andere crisisteams volgden haar lead. TU/e baseerde de crisisstructuur in eerste instantie op het model zoals vastgelegd in het crisisplan. Vervolgens improviseerde TU/e al naar gelang hetgeen wat de crisis van hen vroeg. Dit deden zij mede op basis van structuren en lessen uit de coronaperiode.

De benamingen van de diverse (crisis)teams lopen op momenten door elkaar. De terminologie die TU/e gebruikt voor haar crisisteams verschilt, soms gaat het over crisisteams, operationele teams, één operationeel team, facultaire (crisis)teams, etc. Betrokkenen gebruiken in de gesprekken soms de naam van het ene team, maar doelen dan op een ander team, hetgeen verwarrend werkt. Het gebruiken van eenduidige terminologie is dan ook een aandachtspunt wat naar voren komt uit de gesprekken.

Het CCT bestond uit enkele vaste rollen, aangevuld met enkele adviseurs passend bij de crisissituatie en gewenste aanpak. Gedurende de crisis had het CCT een voorzitter, een secretaris, diverse adviseurs, een notulist en een observator. De voorzitter gaf leiding aan de overleggen en was eindverantwoordelijk voor de besluitvorming. De secretaris was aangehaakt vanuit zijn reguliere kennis, netwerk en kunde en pakte zaken op waar extra ogen of handen nodig waren. Tijdens de interviews benoemden respondenten deze rol als relevant, maar deze staat niet vermeld in de planvorming. De adviseurs waren experts op verschillende disciplines, waaronder op het gebied van IT, de faculteiten, onderwijsondersteuning, veiligheid, facilitaire zaken en communicatie. De notulist maakte verslagen van de crisisoverleggen met hierin de belangrijkste punten, acties en besluiten. De observator gaf feedback op het proces en de besluitvorming tijdens het crisisoverleg. Dit was een geïmproviseerde rol en deze stond niet benoemd in de planvorming. TU/e maakte geen gebruik van een plotter al staat deze rol wel benoemd als vast onderdeel van het CCT in de planvorming. De reden hiervoor was dat CCT-leden hierover verschillende verwachtingen hadden en de plotter vervolgens niet gemist werd door het team. Dit kwam mede door de aanwezigheid van de secretaris en de observator. Overkoepelend vonden betrokkenen dat het crisisteam volledig was en qua deelnemers goed aansloot op de crisisaanpak.

De crisisoverleggen van de crisisteams verliepen volgens alle betrokkenen prettig. De crisisteamleden gaven aan dat de voorzitter goed de regie nam op de aanpak en structuur aanbracht in het overleg. Veelal maakten de crisisteams gebruik van de BOB-methode (Beeldvorming, Oordeelsvorming en Besluitvormingsmethode) of BOBOC-methode (Beeldvorming, Oordeelsvorming, Besluitvorming, Opdracht en Controlemethode) om het overleg te structureren. De crisisteamleden meenden dat tijdens en buiten de crisisoverleggen sprake was van een goede sfeer en een grote gezamenlijkheid. De crisisteamleden zette volgens de respondenten hun potentiële ego's aan de kant. Waar normaliter besluitvorming binnen TU/e lang kan duren doordat deze over veel verschillende schijven gaat, hakten de crisisteamleden volgens betrokkenen nu snel knopen door als CCT. Urgente besluiten namen zij aan het begin van het crisisoverleg. Het lijkt erop dat de informatie en uitwisseling op IT-vlak (begrippen, definities, etc.) duidelijk was tijdens de crisis.

Vergaderklokken stemden de crisisteams met elkaar af. Door vergaderklokken af te stemmen konden crisisteams de input van het ene overleg direct in het andere overleg inbrengen. Het vergaderritme gedurende de dag ontwikkelde zich als volgt door de eerste dagen heen. Om 10.00 uur was het CCT. Om 12.00 uur praatte zij het hoger management bij. Vervolgens om 13.30 uur kwam het LIS-CMT bijeen. Daarna bereidde de communicatie afdeling de communicatie voor. Het communicatiebericht stond uiteindelijk om 16.00 uur op de website. Om 17.00 uur vond vaak nogmaals een CCT plaats.

Betrokkenen geven aan dat de crisisoverleggen in het LIS-CMT en LIS-CRT goed verliepen. Volgens hen waren de juiste personen qua kennis en rollen vertegenwoordigd. Enkelen gaven aan dat de groep mogelijk op momenten wat groot was voor efficiënt overleg bij het LIS-CRT, hetgeen het proces overigens niet hinderde. Deelnemers gaven aan dat beide teams werden voorgezeten door pragmatische en efficiënte voorzitters met een prettige voorzittersstijl.

De crisisstructuren binnen de faculteiten functioneerden over het algemeen goed, aldus betrokkenen. Iedere faculteit had haar eigen crisisteam. Het CCT nam de besluiten en facultaire vertegenwoordigers die deelnamen aan het CCT zorgden er vervolgens voor dat hun facultaire crisisteam de besluiten uitwerkte en hier uitvoer aan gaf. TU/e had geen planvorming voor de facultaire crisisteams gezien zij werken met een centrale crisisstructuur. Het was aan de faculteiten wie zij lieten plaatsnemen in hun crisisteam. De faculteiten hanteerden ook verschillende aanpakken, afgestemd op hun reguliere werkwijze binnen de faculteit. Desondanks was de facultaire aanpak en coördinatie volgens betrokkenen duidelijk en speelde de faculteiten goed in op de centrale crisisstructuur. Hierdoor was sprake van verbinding tussen de teams en verliep deze samenwerking prettig.

Informatiemanagement bij uitval was niet voorbereid. TU/e had geen gestroomlijnde procedure met betrekking tot informatiemanagement en samenwerking ingeval van uitval. In het

informatiemanagement en de manier van samenwerken moest TU/e dan ook veel improviseren, bijvoorbeeld omtrent welke middelen in te zetten om elkaar te contacteren.

Gedurende de crisis was beperkt sprake van aflossing. De crisisteams werkten met een vaste kern van betrokkenen. Tijdens de inzet was dezelfde groep werknemers iedere dag aan zet om de crisis af te handelen. Alleen wanneer leden een goede reden hadden om afwezig te zijn in verband met andere afspraken nam een collega het werk over. Het LIS-CRT was een uitzondering op deze regel. Zij zorgden wel voor aflossing met een bepaalde frequentie. Binnen de andere crisisteams spraken zij wel over aflossing, maar kozen zij er bewust voor om dit niet te doen. De voornaamste reden hiervoor was dat dan overdrachten moesten plaatsvinden.

Op sommige medewerkers kwam tijdens de crisisrespons behoorlijk druk te staan doordat zij specifieke kennis en kunde hadden. Dit was bijvoorbeeld het geval bij ESA. Daar had een beperkt aantal medewerkers kennis van het opnieuw plannen van tentamens. Zij kregen een extreem hoge werkdruk ten gevolge van de crisis, maar hierbij kon niemand hen ontlasten. In de gesprekken kwam naar voren dat hier wel aandacht voor was, maar dit niet of beperkt tot lastenverlichting leidde.

De crisisteamleden vonden de faciliteiten die de TU/e tijdens de crisisrespons beschikbaar stelde voldoende toereikend. De crisisteams eigenden zich vanaf de start van het incident enkele ruimten en gebieden in het gebouw toe en werkten op deze locaties de rest van de week samen. Dit zorgde volgens betrokkenen voor korte lijntjes in de afstemming, een saamhorigheidsgevoel en een duidelijke tafelschikking bij het CCT. De voorzieningen in de toegeëigende ruimten en gebieden werkten en TU/e zorgde al vroeg in de crisis voor randvoorwaarden, waaronder eten en drinken voor de crisisteamleden. Vaste crisisruimten en randvoorwaarden had de TU/e niet vooraf vastgelegd, waardoor dit improvisatie behoefte. Het aanwijzen van vaste crisisruimten en vastleggen van randvoorwaarden was dan ook een aandachtspunt.

4.3 Besluitvorming, dilemma's en scenario's

Tijdens deze crisissituatie zijn diverse kritieke besluiten genomen:

1. Het besluit om het netwerk af te sluiten na een situatiebeeld te vormen en deze af te stemmen.
2. Het besluit om op te schalen naar de crisisorganisatie, zowel op IT-gebied als TU/e breed en de centrale regie en mandaat bij het CCT te beleggen en dit vol te houden de gehele crisisperiode.
3. Het bepalen en uitvoeren van de communicatiestrategie, waaronder ook het plaatsen van een update over de situatie op de website.
4. Het bepalen van de herstelaanpak en -strategie. Dit besluit nam TU/e in twee fasen. Op zondag en maandag bepaalde zij dat onderwijs/onderzoek niet mogelijk/gewenst was. Op dinsdag besloot het CCT gezien herstel en impact op het onderwijs/onderzoek om onderwijs/onderzoek weer op te starten op de maandag erop.
5. Het besluit om al het onderwijs en onderzoek stil te leggen voor uiteindelijk een week en bijbehorende consequenties met betrekking tot het jaarrooster te accepteren en te verwerken in het jaarrooster van TU/e.

Gedurende de crisis was het CCT in de lead en nam zij bijna alle belangrijke besluiten. De afstemming betreffende de besluiten en dilemma's vond in het CCT in gezamenlijkheid en met alle crisisteamleden aanwezig plaats. Het CCT informeerde de Raad van Toezicht en het College van Bestuur dagelijks, maar de crisisafhandeling bleef bij het CCT. Het LIS-CMT nam de tactische en operationele besluiten, de strategische besluitvorming deed het CCT. In de praktijk legde het LIS-CMT veel besluiten voor aan het CCT. Betrokkenen gaven aan dat de besluitvorming over het algemeen effectief was en gestructureerd verliep. Bij de besluitvorming waren verschillende teams betrokken met ieder hun eigen aandachtsgebied. Deze adviseerden en/of dachten mee vanuit hun rol.

Het LIS-CMT heeft in afstemming met enkele direct betrokkenen besloten het netwerk af te sluiten (zonder een voltallig CCT). In de nacht van zaterdag op zondag heeft de Information Security Officer (ISO), in combinatie met de CISO, plaatsvervangend directeur LIS en operationeel betrokken collega's besloten om het netwerk af te sluiten van de buitenwereld. Dit proces is in gang gezet en vervolgens getoetst en afgestemd met onder andere de programmadirecteur integrale veiligheid (technisch voorzitter CCT). Later die nacht zijn, zoals geschetst, meer personen, onder andere van het CCT, geïnformeerd en betrokken bij de crisisaanpak. De respondenten geven aan dat binnen het

huidige mandaat[3], (gegeven) vertrouwen, de tijdsdruk om ergere impact te voorkomen, afstemming en samenwerking het juiste keuze was op het juiste moment. Hierom werd niet gewacht op een voltallig CCT om het besluit mee af te stemmen.

Crisisteams werkten scenario's uit. De crisisteams en ketens in de crisisorganisatie bereidden de scenario's/uitwerkingen voor het CCT voor. Vervolgens overwoog/besprak het CCT de opties/uitwerkingen en nam zij hierover een besluit. Bij het scenariodenken maakte TU/e geen gebruik van standaard formats. De scenario's kregen vorm in het moment en richtten zich voornamelijk op de strategie en aanpak rondom de crisis of bijvoorbeeld vraagstukken van planning, impact op onderwijs, etc. Zo zette de crisisorganisatie het scenariodenken onder andere in rondom het besluit omtrent het verschuiven van het onderwijs. Ook dacht de crisisorganisatie na in scenario's over de vraag wat als de cybercrisis langer gaat duren, rondom het vormgeven van het IT-herstel, omtrent het herstarten van het onderwijs en betreffende het afsluiten van het netwerk. Dit om de impact van de besluitvorming in kaart te brengen.

Tijdens de crisis verloopt de besluitvorming rondom het stilleggen van het onderwijs stapsgewijs om de impact op de community (studenten, onderzoekers en medewerkers) zoveel mogelijk te beperken. Op zondag besluit het CCT om het onderwijs in ieder geval maandag stil te leggen, omdat het niet duidelijk is hoe lang het herstel gaat duren en wanneer onderwijs weer mogelijk is. Op maandag is hier nog altijd geen zicht op, waarna zij besluit ook op dinsdag geen onderwijs te verzorgen. Dinsdag besluiten zij de rest van de week geen onderwijs te verzorgen. Volgens betrokkenen geeft de stapsgewijze aanpak en het uiteindelijke besluit om de rest van de week het onderwijs stil te leggen rust en verschaft deze duidelijkheid, zowel voor de IT'ers als de studenten, medewerkers en onderzoekers. Ook menen de respondenten dat het de organisatie de ruimte gaf om zich rustig voor te bereiden, vragen die leven te stellen en het beantwoorden van deze vragen centraal op te pakken.

Het CCT en LIS-CMT formuleerde nadrukkelijk doelen tijdens de cybercrisis. Het CCT stelde zich de gehele crisis tot doel om zo snel, veilig en verantwoord mogelijk de continuïteit van het onderwijs, onderzoek en de bedrijfsvoering te realiseren. Het LIS-CMT bepaalde de doelstellingen middels mondelinge afstemming en kleurde deze tijdens de crisisoverleggen verder in door te kijken hoe zij de doelstellingen in de praktijk vorm konden geven en door de consequenties van de doelstellingen nader te bezien. Het LIS-CMT stelde haar doelen, waar nodig, bij. Op maandag 13 januari zijn de doelstellingen en bijbehorende prioritering van het LIS-CMT als volgt:

1. Begrijpen wat gebeurd is en onderzoeken wat op dit moment gaande is in het netwerk;
2. Systemen herstellen en weer online te brengen;
3. De verwerking op forensisch vlak voltooien.

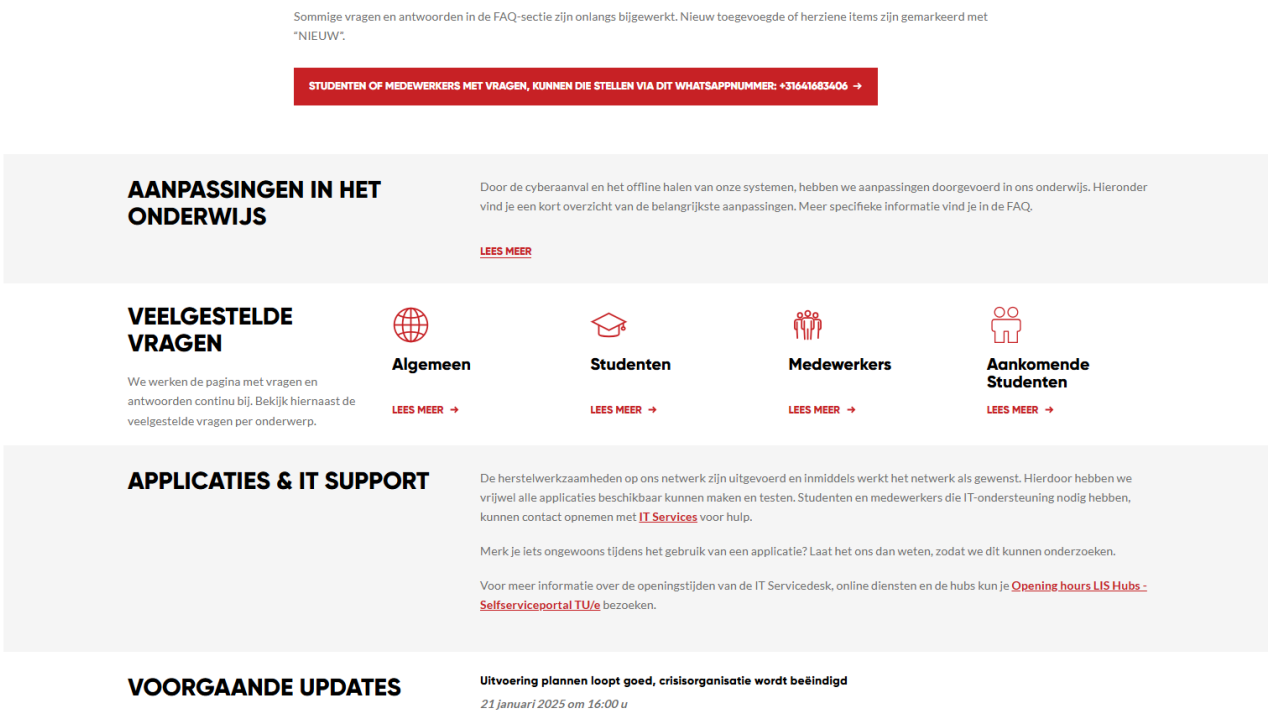
De doelen en prioritering van het LIS-CMT zijn meermaals gewijzigd. Zo wijzigt het LIS-CMT dinsdag 14 januari haar doelen en prioritering. Het LIS-CMT verandert de secundaire doelstelling naar de primaire doelstelling. Als tertiaire doelstelling voegt het LIS-CMT de volgende doelstelling toe, namelijk om voldoende ondersteuning te bieden om het opnieuw activeren van het netwerk en de applicaties mogelijk te maken. De voormalige tertiaire doelstelling schuift op naar de quartaire plaats. Zaterdag 18 januari verandert het LIS-CMT de doelen nogmaals. Het primaire doel is nu het verder beveiligen en ondersteunen van de organisatie op het gebied van beveiliging, het bieden van algemene ondersteuning voor de hele organisatie en het verzorgen van ondersteuning voor onderzoeksdoelen. Het secundaire doel is het voltooien van de forensische verwerking en rapportage.

4.4 Interne en externe communicatie

Gedurende het cyberincident maakte TU/e gebruik van vele alternatieve communicatiemiddelen. Zo gebruikten de crisisteams tijdens de crisis vooral (sociale) media, de website, SMS, bellen, briefings en berichtenapps als Whatsapp en Signal voor de communicatie. De website (zie ook onderstaand figuur) was het primaire medium voor de interne en externe crisiscommunicatie richting studenten en de buitenwereld. Reguliere communicatiemiddelen en samenwerkingsplatforms als mail, Teams en Canvas waren niet beschikbaar of onbetrouwbaar. De

[3] In het crisisplan van TU/e staat op pagina 22 het volgende: Vanaf het moment dat twee leden van het IMS-CERT-team starten met werkzaamheden zijn zij bevoegd om alle noodzakelijke besluiten te nemen die nodig zijn en slechts op die momenten dat nadere afstemming niet mogelijk is.

TU/e achtte deze dan ook ongeschikt voor de crisiscommunicatie richting specifieke doelgroepen, bijvoorbeeld groepen studenten van een bepaalde studie of medewerkers van een bepaalde afdeling. Om de verschillende interne doelgroepen toch te bereiken, zette TU/e centraal een Whatsapp nummer op waarnaar zij vervolgens verwezen op hun website. Via dit Whatsapp nummer konden studenten contact leggen met medewerkers van ESA als zij specifieke vragen, zorgen of problemen hadden. De input zette ESA vervolgens intern door en diende ook een functie in de beeldvorming tijdens de crisisoverleggen. Door het gebrek aan samenwerkingsplatforms overlegden de crisisteamleden buiten de crisisoverleggen vooral fysiek of telefonisch.



Figuur: screenshot van de gehanteerde crisiscommunicatie webpagina TU/e

De communicatie verliep volgens betrokkenen over het algemeen gestructureerd. Gedurende de crisis koos het CCT vanaf maandag ervoor om iedere dag om 16.00 uur via de website updates aan de community en andere geïnteresseerden over de huidige stand van zaken te geven. Deze cadans droeg bij aan de betrouwbaarheid van de TU/e. Op zondag is de eerste publieke communicatie gepubliceerd op de eigen website om 15.00 uur. Waar noodzakelijk gaf het crisisteam eventueel op een eerder moment een update. Voorafgaand aan het online zetten van het communicatiebericht van 16.00 uur briefde TU/e mondeling iedere dag om 12.00 uur de decanen en managing directors (het 'hoger management'). Hierbij gaf het crisisteam het hoger management ook een kort geformuleerd bericht met de belangrijkste besluiten en informatie mee. Voor 16.00 uur lazen ESA, de communicatie afdeling, LIS en een vertegenwoordiging van het bestuur de communicatieberichten tegen. In het begin ontbrak LIS nog als tegenlezer waardoor niet alle (IT)berichtgeving volledig klopte. Na deze constatering is de berichtgeving aangepast en LIS als tegenlezer aangehaakt. Betrokkenen kijken positief terug op het gebruik van deze structuur. Zij geven aan dat de structuur een grote bijdrage leverde aan het creëren van duidelijkheid en het managen van de verwachtingen bij de community, hetgeen het aantal vragen die de betrokkenen kregen significant verminderde.

De mondelinge briefings van decanen en managing directors hadden een positief effect op de crisisaanpak en communicatie met interne doelgroepen. Het zorgde ervoor dat zij beschikten over actuele informatie over de genomen besluiten en konden inzetten op de uitvoering hiervan. Ook was het een goede manier om de temperatuur te meten over genomen besluiten, het hoger management inspraak te geven en daarmee draagvlak te creëren. Bij veel weerstand kon het CCT besluiten dan ook eventueel nog bijstellen voordat de communicatie hierover naar buiten ging. Gedurende het overleg gaf het CCT het hoger management ook een korte notitie mee met de belangrijkste informatie uit de meeting, zodat het hoger management deze vervolgens intern met de medewerkers kon delen.

Dit om te voorkomen dat besluiten een eigen leven gingen leiden binnen de organisatie. Betrokkenen geven aan positief terug te kijken op deze aanpak.

De communicatiestrategie die TU/e hanteerde was gericht op het informeren van de primaire doelgroepen; de medewerkers, onderzoekers en studenten. De crisisteamleden geven aan dat toen de studenten, onderzoekers en medewerkers maandag naar de campus gingen, zij allemaal wisten van de cyberaanval en dat het netwerk uit de lucht was. Ook waren zij op de hoogte waar zij de meest actuele informatie konden vinden en wanneer zij een update kregen. De crisisteamleden zijn het erover eens dat de website als primair informatieplatform prettig en afdoende werkte.

Crisisteamleden worstelden ook onderling met het gebrek aan communicatiemiddelen. Zij stemden veelal (fysiek) bilateraal af of hadden contact via Signal groepen of telefonisch contact.
Bij externe communicatie achtten de crisisteamleden het belangrijk dat TU/e een eenduidig beeld naar buiten brengt. Zowel intern als extern gaven zij duidelijk mee wat wel en niet extern te delen. Ook waren zij zich sterk bewust van het feit dat hetgeen zij intern bekend maakten, extern ook al snel bekend kon worden.

Gedurende de crisis koos het CCT een duidelijke koers met betrekking tot de communicatie en kozen zij voor transparantie over de situatie en aanpak. Het CCT en de communicatieafdeling formuleerden een heldere strategie en maakten bewuste afwegingen over of, waarom, richting welke doelgroep, via welk platform en wat zij wel of niet gingen communiceren. Zo koos TU/e ervoor om direct de media te informeren over dat het netwerk niet langer werkte en de gehele TU/e community een SMS te sturen op de eerste zondag van de crisis. Dit gezien zij de community op de hoogte wilden brengen, hen wilden verzoeken de website in de gaten te houden, zij zelf geen betrouwbare communicatiemiddelen meer hadden en het uiteindelijk vanwege de grote impact toch uit ging lekken. Ook maakte het CCT weloverwogen de keuze om weinig (technische) details te delen om de hacker(s) niet in de kaart te spelen. Verder besloten zij weinig interviews te geven. Dit om twee redenen. Allereerst, vanwege de behoefte regie op de communicatie en het eindproduct te houden. Ten tweede, omdat het mediasentiment over het algemeen positief was. De algemene tendens was dat TU/e goed en tijdig had ingegrepen en daarmee erger had weten te voorkomen.

Lessen uit de coronaperiode verwerkte TU/e nadrukkelijk in de gekozen communicatie-strategie. Denk hierbij bijvoorbeeld aan de standaard communicatiemomenten, de regie bij het CCT, een specifiek webcare team/aanpak en het werken met een communicatieteam.

Faculteiten en diensten stemden communicatie af op hun eigen werkwijze. Dit om deze aan te laten sluiten bij hun gangbare wijze van communiceren en contact. Zo organiseerde de ene faculteit ‘townhalls’ en werkten anderen met name via Signal/Whatsapp groepen. Het crisisteam was zich verder voortdurend bewust van het feit dat informatie snel kon verouderen, waardoor continu de oproep was om te verwijzen naar de centrale communicatiepagina en niet zelf berichten te plaatsen op andere platforms.

TU/e zocht de aansluiting op de community. Hierom nam zij tijdens de crisis een filmpje op waarin de vicevoorzitter van TU/e ingaat op de situatie. Aan het einde van de crisis, toen de herstart van het onderwijs naderde, merkte TU/e op dat de media minder begripvol begon te worden over de beperkte mediaoptredens en interviews. Hierop besloten zij interviews te geven aan de NOS, Omroep Brabant en Cursor; de NOS gezien de nationale impact en bereik, Omroep Brabant om de lokale banden en doelgroepen te bereiken en Cursor vanwege het feit dat zij het interne universiteitsblad zijn en om studenten/medewerkers bereiken. Enkele betrokkenen geven aan dat TU/e achteraf gezien beter wel iets meer mediaoptredens of interviews had kunnen doen. Dit wegens het feit dat studenten en andere personen die toevallig aanwezig waren op de campus wel interviews gaven en TU/e hierdoor sowieso al niet de volledige regie had over de beeldvorming in de media. Overigens had dit volgens betrokkenen geen (grote) negatieve impact.

Ondanks de communicatie hadden velen nog vragen voor onder andere ESA. Hoewel betrokkenen de communicatiestructuur over het algemeen prettig vonden werken, leverde de structuur bij ESA in het begin wat moeilijkheden op. Gedurende de crisis waren zij verantwoordelijk voor het beantwoorden van vragen van studenten, medewerkers en onderzoekers. Zij kregen echter de update over de genomen besluiten die TU/e om 16.00 uur op de website zette op hetzelfde moment als de rest van de organisatie. Hierdoor was het voor hen lastig om te anticiperen op vragen en reacties van studenten en medewerkers die komen gingen. Later in de week zorgde het CCT ervoor dat zij ESA op

de hoogte brachten voorafgaand aan de communicatie update op de website, zodat zij eventueel bij konden dragen aan de antwoorden en berichten die ESA teruggaf aan de community.

Hoewel de informatievoorziening over het algemeen goed op orde was, geven betrokkenen aan dat op twee momenten de communicatie onvoldoende was. Allereerst, rondom de zorgen over inloggen en phishing. Gedurende de crisis konden sommige studenten, medewerkers en onderzoekers nog op het netwerk van TU/e. Zij ontvingen soms nog mails of berichten op Canvas. Sommigen waren hierdoor bang dat de hackers deze berichten stuurden en/of bezig waren met phishing. TU/e had namelijk al in de media, op de website en via SMS gecommuniceerd dat zij te maken hadden met een cyberaanval, dat zij het netwerk uit de lucht hadden moeten halen en men geen gebruik meer kon maken van de systemen en applicaties. Berichtgeving was hierdoor of voelde hierdoor zonder toelichting en duiding bij sommige betrokkenen tegenstrijdig. De tegenstrijdigheid merkte de crisisteamleden wel op, maar volgens sommigen werd hier later op gereageerd dan nodig was. Ten tweede, rondom de livegang van de VPN door LIS. Deze communiceerde LIS niet naar medewerkers. Uit de organisatie kwamen diverse signalen dat gebruikers het fijn hadden gevonden als LIS dat wel had gedaan. Dit gezien de gebruikers dan weer sneller aan de slag hadden gekund.

Verder noemden de betrokkenen nog enkele kleine aandachtspunten met betrekking tot de communicatie. Zo vonden communicatiemedewerkers dat goed gekeken dient te worden naar de bereikbaarheid en beschikbaarheid van woordvoerding en communicatie bij crises die buiten kantoortijden plaatsvinden. Zij benoemden als reden hiervoor de kwaliteitsborging en dat de afdeling communicatie niet over een piketdienst voor woordvoerders beschikt. Een ander aandachtspunt waren de Signal groepen. Signal benoemden betrokkenen als een goed alternatief voor de onderlinge communicatie tussen de crisisteamleden. Het gebruik van de app was echter niet voorbereid. Gedurende het incident moesten crisisteamleden de app nog installeren, uitvinden hoe deze werkte en groepschats aanmaken voor de afstemming. Op het aanmaken van de Signal groepen bestond weinig regie. Doordat dit niet was voorbereid, kostte dit op momenten (te veel) tijd. Ook bracht dit het risico met zich mee dat mensen langs elkaar heen gingen werken. Verder benoemde een enkeling als aandachtspunt dat de communicatieboodschap die TU/e per SMS stuurde communicatief sterker had gekund. De IT-afdeling stuurde deze SMS zonder betrokkenheid van de communicatieafdeling. De SMS stuurde TU/e uit naam van Odido en bevatte geen contactnummer voor informatie. Als laatste benoemen betrokkenen dat TU/e HSE (Health, Safety en Environment) medewerkers die belangrijk zijn voor het garanderen van de veiligheid van de labs niet aanhaakte in de Signal appgroepen. Hierdoor behoorden zij niet tot de medewerkers die TU/e opriep naar de campus te komen. Later vroeg TU/e hen alsnog op naar de campus te komen, maar dit had volgens betrokkenen eerder gemoeten.

4.5 Impact op onderwijs, onderzoek en interne doelgroepen

De impact van de cyberaanval en daaropvolgende crisisaanpak op de primaire processen en TU/e community was groot. Gedurende een hele week lag (bijna) al het onderwijs, onderzoek en werk stil. Studenten konden geen tentamens maken en hadden geen toegang tot hun studiemateriaal. Onderzoekers hadden niet langer de mogelijkheid te werken aan hun onderzoeken. Promovendi mochten hun proefschriften niet verdedigen. Medewerkers waren niet in staat bestanden te openen en de primaire processen van TU/e draaiende te houden. Het CCT besluit uiteindelijk tot het verschuiven van de onderwijsperiode met een week vanwege de hersteltijd. In deze periode bleef in de eerste paar dagen onduidelijk wanneer studie, onderzoek en werk wel weer doorgang kon vinden en wat de consequenties daarvan zouden zijn, hetgeen tot veel onzekerheid leidde. Ook leverde het TU/e in die weken erna veel extra werk op. Denk bijvoorbeeld aan het aanbieden van een extra tentamenmogelijkheid en het verschuiven van de planning. Tot op de dag van vandaag is TU/e bezig met de nasleep van de cyberaanval.

Gedurende de crisis probeerde TU/e doorlopend inzicht te krijgen in hetgeen dat leeft onder de community en de impact van de crisis te reduceren. Om zicht te krijgen op de zorgen van studenten schakelde TU/e al vroeg in de crisis met een breed scala aan interne en externe partners, waaronder studie- en studentenverenigingen, de Joint Program Committee, Program Committees, ESA en studieadviseurs. De respondenten geven aan dat dit een goede manier was om vinger aan de pols te houden.

Desondanks was onrust niet volledig te voorkomen. Met name studenten maakten zich in het begin veel zorgen over of hun tentamens wel doorgingen of niet en wat de uitval zou betekenen voor hun persoonlijk. Met name over het besluit het onderwijs een week te verplaatsen riep veel vragen op

en veroorzaakte veel onrust in de community. Sommigen hadden al vakanties, een terugreis of andere zaken gepland staan en waren bang dat dit geen doorgang kon vinden. Dat de zorgen groot waren blijkt uit de vele vragen die binnenkwamen bij bijvoorbeeld het centrale Whatsapp nummer, de ESA-balies en onder andere uit het feit dat studenten een petitie startten waarin zij vroegen om alternatieve oplossingen voor het verschuiven van de tentamenweek.

Het besluit om het onderwijs stil te leggen zorgde, naast onrust, ook voor enige verwarring. Het CCT nam het besluit om het onderwijs volledig stil te leggen en dit communiceerde zij ook op TU/e website. Richting docenten gaven leden van het crisisteam echter aan dat zij dit besluit niet gingen handhaven. Sommige docenten hadden geen toegang tot het netwerk nodig om les te geven en voelden hierdoor de ruimte om toch onderwijs te organiseren. Hierdoor vond een beperkt aantal onderwijsactiviteiten en lessen toch doorgang. Hoewel de docenten dit met de beste intenties deden, namelijk om de impact voor hun studenten zoveel mogelijk te beperken, leidde dit onder studenten tot onduidelijkheid over of het onderwijs en hun lessen nu wel of niet doorgingen. De crisisfunctionarissen geven aan dat zij achteraf gezien beter hun besluit wel hadden kunnen handhaven om deze verwarring te voorkomen.

Gedurende en na de crisis poogde TU/e de impact op de community zo klein mogelijk te houden en stelden zij zich op als ‘’caring university’’ richting studenten. Zo kozen zij ervoor om coulant om te gaan met studenten die hun vakanties, terugreis of andere zaken al gepland hadden en in de knel kwamen met de verschoven tentamenweek. Studenten waarbij dit speelde en dit aantoonden bij de examencommissie mochten gebruik maken van een alternatieve tentamenmogelijkheid. Door te vragen om bewijs probeerde TU/e te voorkomen dat docenten onnodig een extra hoge werklast kregen en veel extra toetsen moesten maken. Ook maakten zij na de crisis geld vrij om evenementen van studieverenigingen die niet door konden gaan of verplaatst moesten worden te bekostigen. Volgens respondenten maakten studieverenigingen hier beperkt gebruik van. Verder realiseerde TU/e bij NWO uitstel met betrekking tot subsidieaanvragen nadat hen ter attentie kwam dat onderzoekers problemen hadden met het tijdig indienen hiervan.

Verder bekeken de crisisteams in de besluitvorming over het herstarten van de systemen nadrukkelijk naar welke servers het belangrijkst waren en de hoeveelheid mensen die hiervan gebruik maakten. Op basis daarvan brachten zij een prioritering aan om de beperkte hoeveelheid IT-medewerkers in te zetten waar het er het meest toe deed.

4.6 Samenwerking met externe partners

Tijdens de cybercrisis werkte TU/e met diverse partners, waaronder de directe IT-partner (Fox-IT), de Autoriteit Persoonsgegevens, politie, Surf, het ministerie van OCW, de inspectie van het onderwijs, UNL en de universiteiten. Gedurende het incident betrok TU/e Fox-IT al vroeg in het incident als ondersteunend technisch partner. Ook informeerde TU/e al snel de Autoriteit Persoonsgegevens. TU/e betrok de politie om aangifte te doen, hetgeen zij al in de eerste uren van de crisis deden. Surf raakte betrokken nadat zij zelf te maken kregen met de DDoS aanval. Het ministerie van OCW, waaronder ook de minister, informeerde TU/e al vroeg over de actuele stand van zaken om zorgen te voorkomen. De inspectie van het onderwijs raakte op eigen initiatief betrokken op maandag gezien zij zorgen hadden over de continuïteit van het onderwijs en de integriteit van de data. TU/e informeerde UNL in haar rol als bestuurlijk trekker op het gebied van cyber en integrale veiligheid. TU/e hield de universiteiten via de appgroepen met alle CISO’s en ISO’s op prettige wijze op de hoogte.

De samenwerking en afstemming met partners, stakeholders en het netwerk verliep prettig en overwegend effectief. De crisisorganisatie informeerde en betrok haar partners, stakeholders en netwerk snel, zowel op technisch als bestuurlijk vlak. Dit zorgde voor uniformiteit in de aanpak, het beeld en de communicatie-uitingen. De lijntjes waren kort en TU/e zorgde voor frequente informatiedeling en afstemming. De doorlopende informatievoorziening vanuit TU/e op technisch vlak hielp onderwijspartners om op het gebied van IT voorzorgsmaatregelen te treffen.

De samenwerking met de IT-contractpartner verliep naar wens. Tijdens het incident haakte TU/e Fox-IT direct ondersteunend aan als technisch partner vanwege haar kennis, kunde en ervaring met cybercrisisrespons. Ten tijde van haar inzet verleende Fox-IT monitoring, incidentrespons en forensisch onderzoek. Bij de incident respons betrof het voornamelijk het adviseren van TU/e op dit vlak, het meedenken op maatregelen en het monitoren van de uitvoering van maatregelen. Wat betreft het forensisch onderzoek ging het met name om het verzamelen en analyseren van verzamelde data.

Gedurende de crisis nam Fox-IT een adviesrol op zich met betrekking tot het netwerk en de techniek. TU/e bleef verantwoordelijk voor de besluitvorming en het inschatten, in kaart brengen en beperken van de impact op de bedrijfsvoering. De deelname van Fox-IT aan het LIS-CRT zorgde voor een snelle en efficiënte afstemming.

De inspectie van het onderwijs is geïnformeerd tijdens de crisisinzet. De inspectie van het onderwijs heeft hierdoor kennis gehad van het incident en van direct betrokkenen een update ontvangen. De inspectie benoemt met het oog op haar toezichttaken, nu en in de toekomst, twee aandachtspunten. Allereerst, ziet zij in het vervolg graag dat onderwijsinstellingen, indien dit plaatsvindt, hen eerder en uit eigen beweging informeren bij een dergelijk incident vanwege de potentieel grote impact op de onderwijscontinuïteit en -data. Een tweede aandachtspunt is volgens de inspectie van het onderwijs de opvolging van de afspraken die zij met TU/e maakten over de uitvraag van de evaluatie in verband met hun betrokkenheid bij eventuele eigen onderzoeken. Dit is nader afgestemd.

Parallel aan de cyberaanval op TU/e kampte Surf van woensdag tot en met vrijdag met een grootschalige DDoS aanval. De DDoS aanval zorgde voor onrust, omdat Surf en de rest van de onderwijswereld de link legden met de cyberaanval bij TU/e. De zorg bestond dat mogelijk dezelfde hacker als die van TU/e verantwoordelijk was voor de DDoS aanval. TU/e onderhield dan ook contact met Surf en informeerde andere onderwijsinstellingen via het netwerk van bestuurders (UNL) en CISO's over de stand van zaken onder andere met betrekking tot hun forensisch onderzoek. Deze informatielijnen en afstemming worden door de sector als positief bestempeld, aldus de respondenten.

4.7 Cyber impact en aanpak

De eerste tekenen van de ophanden zijnde cyberaanval ontvangt TU/e op zaterdag 11 januari om 21.21 uur. Nadat een oplettende TU/e medewerker de eerste signalen opmerkt, schaalt de IT-organisatie al snel op. Een kat-en-muis spel tussen de hacker en de IT-organisatie gaat van start. Wanneer de hacker admin-rechten verwerft, besluiten zij om het netwerk offline te halen om verdere schade te voorkomen. De dagen na de cyberaanval wacht de IT-organisatie een grote klus. Het onderzoeken van de servers om deze vervolgens weer online te kunnen brengen, neemt veel tijd in beslag. Donderdag 16 januari werken de eerste systemen weer. Vrijdag 17 januari werken bijna alle servers weer. Het weekend gebruikt TU/e om tests uit te voeren om de doorgang van het onderwijs op maandag te kunnen garanderen. Wanneer het onderwijs start, zijn nog niet alle servers in gebruik. Een beperkt aantal onderzoeksservers zijn nog niet in gebruik. Maandag 27 januari vindt het laatste LIS-CMT overleg plaats. Ook dan zijn nog niet alle onderzoeksservers in gebruik. Volgens het LIS-CMT is afschaling echter wel mogelijk gezien de reguliere organisatie vanaf dat moment in staat is om de laatste nazorg te leveren.

Veel betrokkenen zijn vol lof rondom de IT-organisatie die midden in de nacht eigenstandig het besluit nam om het netwerk geheel stil te leggen. Betrokkenen geven aan dat zij het bijzonder en dapper vinden dat de IT-organisatie de ruimte voelde om een dergelijk ingrijpend besluit te nemen, al helemaal gezien de IT-organisatie nog geen bestuurder had weten te bereiken. De IT'ers geven hierover terug dat zij voldoende vertrouwen vanuit het bestuur voelden om de beslissing te nemen het netwerk offline te halen. Voorafgaand aan de cyberaanval hadden de IT'ers al bijeenkomsten gehad met het bestuur, waarin het bestuur uitsprak dat de IT'ers moeten doen wat nodig is in een dergelijke situatie. Hoewel het mandaat in eerste instantie bij het bestuur ligt, mandateerden zij de IT'ers dit besluit, indien nodig, te nemen. Dit om in een dergelijk geval verdere schade te voorkomen. Het stekkermandaat nam TU/e ook op in de planvorming. Desondanks was het een lastig besluit om te nemen als IT-organisatie vanwege de grote consequenties die dit heeft.

De opschaling binnen de IT-organisatie verliep volgens de betrokkenen naar wens. Een IT-medewerker die zijn werkmail bekeek en de mail met verdachte activiteiten opmerkte, zag direct dat het niet goed zat. Hij informeerde zijn collega's, waarna zij een gezamenlijke Teams call aanmaakten. Een half uur na de eerste melding belde Fox-IT het CERT van TU/e. De eerste LIS-CMT vergadering vond een half uur daarna plaats met een beperkt comité. Hierin waren zij voornemens het besluit te nemen de verbinding met het netwerk te gaan verbreken. De CISO belde hierover met de programmadirecteur integrale veiligheid (de technisch voorzitter van het CCT) en sprak af dit voorgenomen besluit zo snel mogelijk in werking te laten treden alsook het CCT bijeen te laten komen en op te schalen. De politie arriveerde niet veel later. Rond middernacht schaalde Fox-IT haar operatie op en vertrok zij richting de campus. Om één uur 's nachts vond een overleg plaats tussen de CISO,

PAL platforms, vervangend directeur LIS en de programmadirecteur integrale veiligheid en besloten zij een CCT te plannen om negen uur in de ochtend. Rond één uur kreeg LIS ook iemand van het bestuur aan de lijn, de Secretaris van het College van Bestuur en toetsten zij het voorgenomen besluit rondom het afsluiten van het netwerk. Rond kwart over één lag het TU/e netwerk volledig plat. Om kwart over drie arriveert Fox-IT. Om negen uur vond het crisisoverleg van het CCT plaats. De betrokkenen waren het erover eens dat de opschaling snel verliep en dat zij tijdig de juiste expertise betrokken. Zij gaven aan hier dan ook positief op terug te kijken.

Het besluit om het netwerk offline te halen was volgens alle betrokkenen het enige juiste besluit. De hacker had op dat moment de hoogste administrator rechten verworven. Hierdoor lukte het niet om de hacker buiten te sluiten. De enige optie die TU/e nog had was om het netwerk af te sluiten om verdere schade te voorkomen. Fox-IT adviseerde TU/e dan ook sterk dit te doen. Achteraf bleek uit het forensisch onderzoek dat de aanval de karakteristieken van een ransomware aanval had, maar waarbij de aanvaller niet zo ver heeft kunnen komen door het snelle ingrijpen. Door tijdig in te grijpen is volgens TU/e en Fox-IT dus erger voorkomen. Als zij weer voor de keuze stonden dan hadden zij hetzelfde besluit genomen.

Tijdens het cyberincident duurt het uitzetten van het netwerk langer dan gehoopt en brengt het verschillende cascade-effecten met zich mee die niet in kaart waren. TU/e maakt in haar netwerk gebruik van een generieke structuur met algemeen geldende afspraken. Per faculteit bestaan uitzonderingen en wijkt de digitale infrastructuur af. Generiek bepalen de (technische) structuur van het netwerk, diversiteit tussen de netwerken en benodigde beveiligingsmaatregelen de aanpak omtrent het uitzetten van het netwerk. Voorafgaande aan het uitzetten van het netwerk oefende TU/e hier niet mee. Om hiermee te oefenen moet TU/e haar hele netwerk afsluiten, hetgeen een te grote impact heeft op de reguliere bedrijfsvoering. Hierdoor is het ten tijde van de crisis ook niet inzichtelijk wat nog wel en niet werkt en bestaat verschil tussen de werking van applicaties op het netwerk en SaaS applicaties. Ook is niet duidelijk dat het uitzetten van het netwerk leidt tot problemen met de meldkamer calamiteiten. Doormeldingen zijn niet langer mogelijk, waardoor een medewerker van de meldkamer permanent aanwezig moet zijn op de campus.

Bij het herstellen van het netwerk maakte TU/e en het LIS-CMT gebruik van een standaard lijst met kroonjuwelen om te prioriteren. Op de kroonjuwelen lijst stonden de applicaties kritiek voor de bedrijfsvoering. De applicaties op de lijst herstelde de IT'ers eerst. Vervolgens brachten zij een prioritering aan betreffende welke applicaties zij hierna als eerste moesten opstarten. Dit deden de IT'ers in samenwerking met het onderwijs. Zij hadden namelijk meer zicht op welke servers belangrijk waren om als eerste te herstellen. Zo stemden de IT'ers met decanen en professoren af over welke onderzoeksservers belangrijk waren en als eerste weer in de lucht moesten komen. Dit werkte volgens de betrokkenen goed. Als aandachtpunt benoemen de IT'ers dat zij de prioritering niet altijd volgden vanwege druk vanuit de organisatie. Zij vinden het belangrijk dat dit in het vervolg wel gebeurt gezien dit weloverwogen keuzes waren.

In de samenwerking tussen de IT-organisatie en de rest van TU/e organisatie vielen een aantal zaken op. Bij TU/e bestond veel oog voor de menselijke maat met betrekking tot de IT-organisatie. Zo namen zij aan het begin van de week het besluit om het onderwijs stil te leggen om rust te creëren bij de IT-organisatie en druk weg te nemen. Ook voegde TU/e aan de berichtgeving dat zij de hackers op heterdaad betrapt hadden toe dat geen volledige garantie kon worden gegeven dat de hackers uit de systemen waren. Verder vonden IT'ers het moeilijk naar huis te gaan als hun collega's moesten doorwerken, waarna TU/e besloot hen iedere keer op hetzelfde moment gezamenlijk naar huis te sturen. Dit om te voorkomen dat zij druk voelden om te blijven en uitvielen. Wel haakte TU/e expertteams in de periferie van LIS onvoldoende aan. Als TU/e hen wel had aangehaakt dan hadden zij directer een bijdrage kunnen leveren in het oplossen van de crisis.

De betrokkenen merken enkele aandachtspunten op. Zo geven zij aan dat de facultaire netwerken en faculteiten minder goed voorbereid zijn op een cybercrisis en hier beter naar gekeken dient te worden. Ook merken zij op dat zij in de toekomst bij voorkeur het netwerk met zones uit willen zetten door middel van segmentatie, want dan hoeft TU/e niet het gehele netwerk uit de lucht te halen, maar enkel een gedeelte. Daarnaast benoemen zij dat TU/e haar beleid met betrekking tot verouderde systemen onvoldoende handhaaft, waardoor deze nog altijd aan het netwerk hangen en een zwakke plek en veiligheidsrisico vormen. Een ander aandachtspunt dat betrokkenen noemen is het gebruik van alternatieve systemen, bijvoorbeeld Google Drive. TU/e dacht hier volgens betrokkenen relatief laat over na. Een dag later was Teams alweer in de lucht, waardoor de noodzaak hiertoe verdween, maar eerder in de crisis had dit van grote toegevoegde waarde kunnen zijn. Verder hadden Teams en

Canvas beter benut kunnen worden volgens sommigen. Een groot deel van de organisatie had hiertoe namelijk nog toegang.

4.8 (Crisis)Planvorming en voorbereiding

Planvorming is nog niet volledig aanwezig. Betrokkenen noemen een aantal aandachtspunten met betrekking tot de planvorming. Zij geven, allereerst, aan dat TU/e niet beschikt over planvorming met betrekking tot de uitval van een gebouw. Volgens betrokkenen is het echter wel belangrijk om te bekijken welke mogelijkheden TU/e dan nog heeft, bijvoorbeeld omtrent wat alternatieve locaties kunnen opvangen en wat prioriteit hoort te krijgen in een dergelijk geval. Ten tweede, benoemen zij dat de faculteiten niet beschikken over alarmeringslijsten, hetgeen problematisch kan zijn ingeval van langdurige uitval. Ten derde, zien betrokkenen meerwaarde in het verder uitwerken van de IT-escalatieladder met betrekking tot het stekkermandaat. Zij willen duidelijker uitwerken hoe de escalatieladder eruit ziet en welke ruimte iemand heeft om beslissingen te nemen op het moment dat iemand niet te bereiken is.

TU/e beschikt over een algemeen crisisplan, een IT-crisisplan en een OTO-plan. In het crisisplan staat beschreven wanneer TU/e crisisorganisatie en bijvoorbeeld wat bijzonderheden en aandachtspunten zijn ingeval dat bepaalde scenario's zich voordoen. De TU/e beschikt over een OTO-plan (opleiden, trainen oefenen) waarin de aanpak met betrekking tot het opleidingsprogramma op crisismanagement gebied staat. Verder legt TU/e vast hoe een escalatie ingeval van een opschaling op cybergebied plaatsvindt (een IT-crisisplan/2-pager). Een crisisstructuur is dan ook aanwezig en voorbereid om een effectieve crisisaanpak te bewerkstellingen.

Gedurende de crisis verschilt de aanpak binnen de faculteiten en diensten sterk. TU/e beschikt niet over planvorming met betrekking tot de basiscrisisstructuur van de faculteiten. Hierdoor bestaat beperkt regie op de vorm waarin de faculteiten en diensten deze gieten. Veelal werkt men met operationele en onderliggende crisisteams, maar de aanpak en uitwerking verschilt sterk. Tijdens de crisis leidt dit overigens tot weinig negatieve effecten. Het enige negatieve effect dat betrokkenen noemden, is dat het leidde tot minder formalisatie tijdens de eerste paar dagen. Zo communiceren sommige faculteiten in het begin ook de besluitvorming via sociale media, hetgeen niet wenselijk was doordat deze al snel achterhaald kon zijn. De verschillende ketens, waaronder ESA en communicatie, pakken later in de week de regie op en stroomlijnen vervolgens de aanpak.

Uit de gesprekken met betrokkenen komt naar voren dat de voorbereiding bij grootschalige uitval, zoals nu bij IT, niet tot beperkt is voorbereid door de faculteiten en diensten. Zo is niet duidelijk wat faculteiten doen op het moment dat zij geen gebruik kunnen maken van de IT-voorzieningen. Met behulp van de crisisstructuur en inzet van medewerkers is dit pragmatisch opgepakt en in het moment op gereageerd. Wel wordt duidelijk dat hierdoor tijdens de crisis is bepaald hoe te communiceren met eigen studenten en medewerkers, afwegingen zijn gemaakt welke diensten of onderdelen prioriteit hadden en bekeken is wat eerst weer zou moeten werken. De zogenoemde uitdagingen voor het continueren van onderwijs en onderzoek zijn daarmee in het moment afgehandeld, terwijl dit ook (vanuit BCM) voor te bereiden is.

Verschillende betrokkenen gaven aan dat de inhoud van het crisisplan en de werking van de crisisorganisatie beperkt bekend is en dat dit ook bleek tijdens de crisis. Medewerkers wisten niet altijd wat het betekende als het CCT actief wordt, waardoor zij in eerste instantie de reguliere besluitvormingslijnen bleven volgen. Betrokkenen gaven aan dat zij het geen goed idee vinden om het crisisplan organisatiebreed te delen. Wel vonden zij het wenselijk dat TU/e op intranet informatie deelt over hoe de verschillende crisisteams werken, welk team welke bevoegdheden heeft en welke rollen in de teams plaatsnemen, bijvoorbeeld middels een filmpje of korte tekst met uitleg.

4.9 Leren als organisatie en evalueren

Voorafgaand aan de cyberaanval had TU/e al aandacht voor leren en het treffen van voorbereidingen op crisissituaties. Binnen TU/e is de wens/afspraak dat ieder crisisteamlid jaarlijks minimaal één crisismanagementtraining en één crisismanagementoefening bijwoont. Deze trainingen en oefeningen richten zich op het bijbrengen van basisvaardigheden als de BOB-structuur, bekend raken met de eigen rol in het crisisteam, kennis opdoen van de organisatie specifieke planvorming

alsook samenwerking in het crisisteam, tussen de crisisteams en met ketenpartners. De meeste crisisteamleden geven aan dat zij zich voldoende voorbereid voelden op hun rol. Veel respondenten geven aan dat met name de OZON-oefening, een sector brede cybercrisisoefening voor het onderwijs, en de ervaringen met eerdere crisissituaties, met name de coronacrisis, bijdroegen aan de goede voorbereiding van TU/e op dergelijke cyberincidenten. Enkele respondenten gaven suggesties hoe het OTO-aanbod van TU/e verbeterd kan worden. Zij opperden onder andere het organiseren van opfristrainingen met betrekking tot de basiscrisisvaardigheden, mediatrainingen voor bestuurders en crisismanagementtrainingen voor het communicatieteam alsook het mee laten oefenen van het communicatieteam bij gezamenlijke oefeningen.

Gedurende de crisis bestond ook aandacht voor leren. TU/e reflecteerde in het crisisteam voortdurend op haar aanpak. Dit blijkt onder andere uit het feit dat TU/e twee observatoren inzette bij de crisisteams; één bij het CCT en de ander bij het LIS-CMT. Deze observatoren hadden als taak om uit te zoomen, verbeterpunten te identificeren en feedback te geven, zowel procesmatig als in de crisisaanpak. De lessen die TU/e leerde zette zij in om hun aanpak aan te scherpen. Een voorbeeld hiervan is het aanscherpen van de volgorde van betrekken en tegen laten lezen van de communicatieberichten door onder andere ESA en het LIS-CMT en de uitkomsten van de call met het hoger management te verwerken in de communicatieberichten. Dit ten behoeve van de volledigheid en kwaliteit van berichten.

De rol van observator werkte prettig. Hoewel de rol van observator niet vastligt in het crisisplan en deze tijdens de crisis improvisatie was, gaven respondenten aan dat dit prettig werkte en voor herhaling vatbaar was. Zo ontstond tijdens de crisisinzet namelijk ook een werkwijze omtrent het geven van feedback en scherpte dit de werkwijze en aanpak tijdens de crisis aan. Dit maakte dat niet alleen achteraf teruggekeken en geëvalueerd werd. Wel benoemden respondenten dat crisismanagementervaring cruciaal is om deze rol goed in te vullen.

Na afloop evalueerde TU/e met als doel te leren voor in de toekomst. Intern evalueerde TU/e per team, discipline en faculteit de crisisrespons van TU/e. Ook liet TU/e direct na de crisis twee externe evaluaties uitvoeren. De ene voerde Fox-IT uit en richtte zich op de toedracht van de cyberaanval en het technische/forensische onderzoek; de ander richtte zich op de crisisrespons van TU/e als geheel (het voorliggende rapport). TU/e had bij het evalueren ook oog voor de behoeften van haar netwerk en partners. De belangrijkste overkoepelende lessen die voortkomen uit de evaluaties maakte TU/e openbaar, zodat ook andere organisaties zich hiermee hun voordeel kunnen doen. Wel bleef het gedurende dit onderzoek onduidelijk of en in hoeverre TU/e de sentimenten van studenten betreffende de crisisaanpak evalueerde. Ook deze groep is een belangrijke doelgroep voor evaluatie en kan in de toekomst als standaard deelnemer worden meegenomen bij dergelijke evaluaties.

4.10 Nafase en afschaling

Op dinsdag 21 januari startte de nafase met de afschaling van het CCT. Het onderwijs was de dag daarvoor zonder al teveel problemen herstart. Het afschalen was een weloverwogen besluit. Betrokkenen gaven aan dat de primaire taakstelling van TU/e inmiddels weer grotendeels doorgang kon vinden en alleen operationele afhandeling nog een aandachtspunt was. Dit kon TU/e volgens betrokkenen prima in de lijnorganisatie beleggen mits zij in de nafase korte lijntjes onderhielden met het bestuur van TU/e, besluitvorming in het kader van de afhandeling van de crisis versneld kon plaatsvinden en de crisisorganisatie weer kon opschalen indien nodig. Wel geven betrokkenen aan dat het juiste moment van afschalen veelal lastig in te schatten is, want als organisatie wil je niet te vroeg, maar ook niet te laat afschalen. Het LIS-CMT schaalde een kleine week na het CCT af (27 januari) en ESA nog een week later (begin februari).

De dag dat de crisis eindigt voelt voor iedereen binnen TU/e anders. Voor de een is de crisis voorbij op 20 januari; de dag dat het onderwijs herstartte. Voor anderen is de crisis nog steeds niet voorbij, omdat zij nog iedere dag bezig zijn met de nasleep. Met name de faculteiten en ESA ervaren in de nasleep grote impact van de crisis. Betrokkenen geven aan dat ESA een grote achterstand met betrekking tot haar reguliere werkzaamheden opliep en zij grote klus had aan het opnieuw plannen van onderwijsactiviteiten. Ook noemen respondenten dat de examencommissies extra verzoeken van studenten om gebruik te maken van alternatieve tentamenmogelijkheden moesten beoordelen. Verder hebben docenten extra werk verzet om een additionele tentamenmogelijkheid mogelijk te maken. Zicht op de benodigde (extra) capaciteit is door zowel de reguliere organisatie als de crisisorganisatie niet expliciet gemaakt.

De crisisorganisatie schaalde 21 januari af. De lopende activiteiten droegen de crisisteams toen over aan de reguliere organisatie. Volgens de respondenten verliep deze overdracht prettig en gebeurde dit op een logisch moment, namelijk toen duidelijk was dat het onderwijs zonder grote problemen herstartte. Wel bestond bij degenen die langer in de crisis zaten soms het beeld dat na afschaling weinig aandacht voor hen was. Zij zaten nog in een crisis voor hun gevoel, maar de crisisteams schaalden naar hun inziens al voortijdig af en voor de rest van de organisatie was de crisis al voorbij. Dit voelde soms eenzaam, vooral ook gezien de reguliere organisatie soms wel van hen verwachtte dat zij hun reguliere taken uitvoerden. TU/e probeerde dit alles wel te adresseren. Zo poogden zij onder andere te zorgen voor korte lijntjes wanneer zich knelpunten voordeden en plaatsten zij in interne nieuwsartikelen en -bladen over de nasleep om te zorgen dat degenen die nog in de crisis zaten zich gezien voelden. Desondanks lukte het TU/e niet om deze gevoelens volledig weg te nemen.

Verschillende aandachtspunten komen naar voren in de interviews. Zo bestond in de nafase enige onduidelijkheid over wie de regie voerde op de nafase en op welke manier deze was belegd. Respondenten geven aan dat zij hierdoor tijdens de nafase een duidelijk aanspreekpunt misten om mee te schakelen. Ook benoemden respondenten dat enige verwarring bestond binnen LIS over de vergaderdata en -tijden nadat de crisisorganisatie afschaalde. Hierdoor waren medewerkers niet of te laat aanwezig bij het eerste afdelingsoverleg na afschaling. Verder bestond enige onduidelijkheid rondom de alternatieve tentamens en proctoring. Het crisisteam had hieromtrent wel een besluit genomen, maar uitwerking betreffende de aanpak van de alternatieve tentamens ontbrak. Hierdoor was niet altijd duidelijk wie wat moest doen, bestond onduidelijkheid over het aanvragen en werken met de proctoring en moest ESA op de werkvloer op momenten improviseren.

BIJLAGE A – Tijdlijn

Datum	Tijd	Gebeurtenis
11 – 01	21.21	Een automatische melding wordt verstuurd naar het CERT, Fox-IT en de systeem administratoren van TU/e. Een medewerker van LIS die geen dienst heeft, ziet dat sprake is van verdachte activiteit op de servers van TU/e en roept de hulp in van collega's. De PAL Platforms wordt geïnformeerd.
11 – 01	+/- 21.51	Fox-IT belt het CERT van TU/e.
11 – 01	22.37	De directeurs LIS worden op de hoogte gebracht van de mogelijke cyberaanval.
11 – 01	23.45	Eerste LIS-CMT in beperkt comité. Aanwezig zijn de PO Security Operations, CISO, PAL platforms en plaatsvervangend directeur LIS. Zij nemen zich voor het besluit te nemen het netwerk af te gaan sluiten. Na het overleg spreekt de CISO met de programmadirecteur integrale veiligheid (de technisch voorzitter van het CCT) af dit voorgenomen besluit zo snel mogelijk in werking te laten treden alsook het CCT bijeen te laten komen. Ook informeert TU/e na het overleg de politie en de programmadirecteur integrale veiligheid.
12 – 01	+/- 00.00	Fox-IT schaalt haar operatie op en vertrekt richting de TU/e campus.
12 – 01	+/- 1.00	LIS weet contact te leggen met een bestuurslid, de Secretaris van het College van Bestuur, om het besluit rondom het afsluiten van het netwerk te toetsen.
12 – 01	01.18	TU/e schakelt alle netwerkactiviteit uit.
12 – 01	+/- 03.00	Fox-IT arriveert op de TU/e campus.
12 – 01	09.00	Eerste CCT-vergadering. Hierbij zijn ook de PAL platforms, Chief Privacy Officer, directeur LIS en plaatsvervangend directeur LIS aanwezig. Het CCT besluit meer informatie te verzamelen, informatiebijeenkomsten voor de decanen en directeuren te gaan organiseren, het College van Bestuur en de Raad van Toezicht te informeren, om 12.00 uur te communiceren via de website alsook het darkweb en sociale media te monitoren.
12 – 01	Middag	Eerste MT-overleg.
13 – 01	08.45	Eerste LIS-CMT met uitgebreid comité. Het LIS-CMT en LIS-CRT stellen doelen en een prioritering vast. Het primaire doel van het LIS-CMT is om te begrijpen wat gebeurd is en wat op dit moment gaande is in het netwerk. Dit om inzicht te krijgen in de situatie. Het secundaire doel is om de systemen te herstellen en weer online te brengen. Het tertiaire doel is om de verwerking op forensisch vlak te voltooien. Het LIS-CRT stelt zich tot doel om de IT-infrastructuur weer voldoende veilig te maken om de systemen weer terug online te kunnen brengen. Het LIS-CMT besluit om Signal voor de crisisoverleggen in te zetten en de privacy afdelingen te informeren wanneer zij een rapport hebben over de impact op persoonlijke data voor de Autoriteit Persoonsgegevens.
13 – 01	09.00	Tweede CCT-vergadering. De eerste signalen wijzen erop dat de dader op heterdaad betrapt is. Het CCT stemt in met het voorstel vanuit ESA om het onderwijs op dinsdag 14 januari geen doorgang te laten vinden.
13 – 01	15.00	Het LIS-CMT stelt vast dat data niet gestolen of versleuteld is. Het CCT besluit dat vanaf vandaag elke dag om 16.00 uur een communicatiebericht op de website van TU/e komt te staan en een balie op te zetten waar studenten en medewerkers heen kunnen als zij vragen hebben.
14 – 01	08.00	Het LIS-CMT wijzigt haar doelen en bijbehorende prioritering. Het primaire doel richt zich nu op het herstellen en weer online brengen van de systemen. Het secundaire doel richt zich op het begrijpen en onderzoeken wat gaande is. Het tertiaire doel is om voldoende ondersteuning te bieden om het opnieuw activeren van het netwerk en de applicaties mogelijk te maken. Het quartaire doel is om de forensische verwerking te voltooien.
14 – 01	09:00	Het CCT besluit om de academische kalender één week op te schuiven en de onderwijsweek waarin de cyberaanval plaatsvindt te laten vervallen; het formele onderbouwde besluit hierover volgt op 16 januari. Ook besluit het CCT om de SaaS applicaties die beheerd worden door LIS maar niet op het netwerk van TU/e staan, weer online te brengen. De connectie tussen het TU/e netwerk en de buitenwereld besluiten zij nog niet te leggen. De servers die LIS niet beheert, hetgeen voornamelijk onderzoeksservers zijn, hebben een lagere

		prioriteit gezien een beperkte groep hier gebruik van maakt. Daarom besluit het CCT deze nog langere tijd ontoegankelijk te laten.
15 – 01		Grote DDoS aanval op het netwerk van Surf vindt plaats. Hierdoor ontstaan zorgen over of dit een relatie heeft met de cyberaanval op TU/e. Aan het einde van de dag kan iedereen weer inloggen in de SaaS systemen.
15 – 01	16.00	TU/e meldt op haar website dat zij verwacht dat een groot deel van haar netwerk voor het weekeinde weer veilig en beschikbaar is en de daders op heterdaad betrapt zijn.
16 – 01		Iedereen kan weer inloggen en de Teams omgeving is weer beschikbaar.
16 – 01	09.00	Het CCT besluit in te stemmen met de aanpassingen op het assessmentplan met betrekking tot de studeerbaarheid en het publiceren van een 06-nummer ter vervanging van de noodnummers. De noodnummers zijn niet beschikbaar vanwege de DDoS aanval op Surf.
17 – 01	09.00	Het CCT besluit in te stemmen met het voorstel om het selectieproces met vijf werkdagen te verlengen.
17 – 01	16.00	TU/e meldt dat zij naar verwachting maandag het onderwijs kunnen hervatten. Het CCT besluit om een regeling te treffen voor studenten die reeds vakanties boekten en hierdoor niet aanwezig kunnen zijn bij verplaatste tentamens of herkansingen. Zij stellen een alternatieve tentamenmogelijkheid beschikbaar als studenten kunnen aantonen dat zij in de knel komen. Verder gaan zij het selectieproces voor nieuwe studenten met vijf werkdagen verlengen.
18 – 01 t/m 19 – 01		TU/e test het netwerk.
18 – 01	08.00	Verandering van de doelen door het LIS-CMT. Het primaire doel is het verder beveiligen en ondersteunen van de organisatie op het gebied van beveiliging, algemene ondersteuning voor de hele organisatie en ondersteuning voor onderzoeksdoelen. Het secundaire doel is het voltooien van de forensische verwerking en rapportage.
19 – 01	16.00	TU/e communiceert dat het testen van de systemen succesvol verliep en zij het onderwijs maandag hervatten.
20 – 01		TU/e hervat het onderwijs en onderzoek. Een beperkt aantal onderzoeksservers moeten zij nog herstellen, waardoor deze nog niet beschikbaar zijn.
21 – 01	09.00	Laatste CCT overleg. Tijdens de vergadering besluiten zij tot afschaling van de crisisorganisatie en het uitvoeren van forensisch onderzoek en een externe evaluatie.
21 – 01	16.00	TU/e plaatst een laatste communicatiebericht op haar website en kondigt de afschaling aan.
23 – 01		Het College van Bestuur besluit een noodfonds vrij te maken om evenementen van studieverenigingen die niet door konden gaan of verplaatst moesten worden te bekostigen.
27 – 01	15.00	Laatste LIS-CMT-overleg.
10 – 02		Laatste overleg van crisisafhandelingsteam ESA.

BIJLAGE B – Documentenoverzicht

Documenten
01. 2-0012 Quick Reference Card_LIS Crisis_V1.2.pdf
01. Actiepunten- en besluitenlijst CCT – januari 2025.xlsx
01. Briefing CCT 13-01, 10.00 uur.pdf
01. Publicaties website – cyberaanval (NL).pdf
02. 20250117 – Definitief besluit CCT geboekte vakanties NED.pdf
02. Briefing vanuit CCT 13-01, 17.00 uur.pdf
02. Publicaties website – cyberattack (ENG).pdf
03. 20250117 – Definitief besluit CCT onderwijs Q3 NED.pdf
03. CONFIDENTIEEL - Briefing CCT 14-01, 10.00 uur.pdf
04. Briefing CCT 14-01, 17.00 uur.pdf
05. 20250120 – Inbreng Daisy besluitenlijst CCT.docx
05. Briefing CCT 15-01, 10.00 uur.pdf
06. 20250121 – Definitief 21-01-2025 besluit CCT besluit over onderwijs NED.pdf
06. Briefing CCT 15-01, 17.00 uur.pdf
07. Briefing CCT 16-01, 10.00 uur.pdf
07. Document promoties.docx
08. Briefing CCT 17-01, 10.00 uur.pdf
09. Briefing CCT 21-01, 10.00 uur.pdf
12-01 0830u LIS operationeel crisisteam.jpg
12-01 1530u LIS operationeel crisisteam.jpg
12-01 1900u LIS operationeel crisisteam.jpg
13-01 0915u LIS operationeel crisisteam.jpg
13-01 1500u LIS operationeel crisisteam.pdf
13-01 2100u LIS operationeel crisisteam.pdf
14-01 1300u LIS operationeel crisisteam.pdf
14-01 1900u LIS operationeel crisisteam.pdf
15-01 0900u LIS operationeel crisisteam.pdf
15-01 1500u LIS operationeel crisisteam.pdf
16-01 0900u LIS operationeel crisisteam.pdf
16-01 1500u LIS operationeel crisisteam.pdf
17-01 0900u LIS operationeel crisisteam.pdf
17-01 1500u LIS operationeel crisisteam.pdf
17-01-2025 ENG decision CCT booked holidays.pdf
17-01-2025 ENG decision CCT postponed examinations 17-01-2025.pdf
17-01-2025 NED besluit CCT geboekte vakanties.pdf
17-01-2025 NED besluit gevolgen verschuiven tentamens.pdf
18-01 1100u LIS operationeel crisisteam.pdf
18-01 1500u LIS operationeel crisisteam.pdf
20-01 1000u LIS operationeel crisisteam.pdf
2025 januari 21 Memo exchange studenten.docx
2025 januari 27 Verklaring exchange studenten.docx
20250115 – Besluiten en actielijst – CCT.docx
2025-01-15 – Recovery priorities.xlsx
20250117 – actiepunten- en besluitenlijst CCT – januari 2025.xlsx
20250117 – Inbreng ESA – cp besluit CCT ivm geboekte vakanties.docx
20250117 – Inbreng ESA – cp Besluit gevolgen verschuiven tentamens versie 17-01-2025 versie 3.docx
20250117 – Inbreng ESA – cp Besluit onderwijs versie 17-01-2025 versie 3 .docx
20250121 – Definitief 21-01-2025 besluit CCT besluit over onderwijs NED.docx

20250121 DEFINITIEF verslag update cyberaanval TUe.pdf
20250226 Evaluatie CMT.pptx
21-01 1000u LIS operationeel crisisteam.pdf
21-01-2025 ENG decision CCT on Teaching.pdf
21-01-2025 NED besluit CCT over onderwijs .pdf
23-01 1000u LIS operationeel crisisteam.pdf
23-01-2025 CvB decision on financial consequences.pdf
2425-F2 Follow-up Letter – New Master Students.docx
250122 Communication to secretaries EC about exams Q2.pdf
250128 Brief explanation secretaries EC to the procedure for handling alternative exam requests.pdf
250128 Communication to exchange students eligible for accelerated procedure (group E).docx
Aanpassing proces decentrale selectie vanwege cyberattack definitief.docx
Achter de schermen bij het ED_'Alle poorten bij de TU_e gingen dicht, niet alleen de digitale'_Opinie_ednl.pdf
Achtergrondinformatie uitnodiging gesprek leerevaluatie cyberaanval TU/e concept.docx
Achtergrondinformatie uitnodiging gesprek leerevaluatie cyberaanval TU/e concept.pdf
Actiepunten- en besluitenlijst CCT – januari 2025.xlsx
Actions and agreements MESA cyber attack crisis.xlsx
AEB AEM to EduB_Advice regarding CCT decisions following the cyberattack_extra meeting 17 January_20250117.pdf
AEB AEM to EduB_Advice regarding the proposed decision to extend the pre-BSA and unenrolment deadlines_20250203.pdf
AEB AEM to EduB_Advice to choose scenario 1, recarding scenarios systems down ESA following the cyberattack_extra meeting 14 January_20250114.pdf
AEB AEM to EduB_Advice_Final advice regarding two proposals_email Basten to de Haan_20250124.pdf
Answers to questions regarding proposal to resolve bsa issues due to postponed Q2 exams final.pdf
Begrip voor uitstel tentamenweek na hack TU_e, maar ook veel vragen over geboekte vakanties_Eindhoven_ed.nl.pdf
Besluitenlijst CCT januari 2025.xlsx
CMT evaluatie CoPilot Summary.docx
Crisis evaluatie Services.xlsx
Crisis situatie 2025 definitief.docx
Crisis Survey – LIS(1-61).xlsx
Crisisplan TUE versie 1.0 – Definitief, excl. Alarmeringslijst 08092022.pdf
Cyberaanval TU/e.docx
Cyber Crisis Evaluatie LIS.pdf
Evaluatie CERT.docx
Evaluatie crisisorganisatie TUE cyberaanval 11 januari 2025 – def.lijst van te interviewen personen 1.0.docx
Evaluatie Cyberaanval binnen HR Operations en met faculteiten met een lab.docx
Hack bij TU/e hakt erin_ tentamens week later, weken nodig voordat systemen weer hersteld zijn_Eindhoven_ed.nl.pdf
Hackers TU_e 'op heterdaad betrapt'_Eindhoven_ed.nl.pdf
Hackers vallen netwerk TU_e aan; universiteit haalt netwerk offline, maandag geen onderwijs_Instagram_ed.nl.pdf
Impact roosteraanpassing op aantoning IND voorganseis definitief.docx
LIS Crisis Management Team (CMT) – anoniem.xlsx
Maandag geen onderwijs door cyberaanval op TU/e_'Uitzetten netwerk heeft vervelende gevolgen'_Binnenland_ed.nl.pdf

Meeting minutes MESA crisis meeting Monday January 13 2025 1610h.docx
Meeting minutes MESA crisis Tuesday January 14th 0900h.docx
Memo bachelor before master rule impact cyber attack final.pdf
Memo financial consequences final.pdf
Memo Follow-up procedure for alternative exams due to cyberattack definitief.docx
Memo resuming master graduation ceremonies final.pdf
Memo sharing of person contact information during cyber attack final.pdf
Minutes Mesa crisis meeting hack 10 februari 2025.docx
Minutes Mesa crisis meeting hack 14 januari 202 afternoon5.docx
Minutes Mesa crisis meeting hack 14 januari 2025.docx
Minutes Mesa crisis meeting hack 15 januari 2025 afternoon.docx
Minutes Mesa crisis meeting hack 15 januari 2025.docx
Minutes Mesa crisis meeting hack 17 januari 2025 afternoon.docx
Minutes Mesa crisis meeting hack 17 januari 2025.docx
Minutes Mesa crisis meeting hack 20 januari 2025.docx
Minutes Mesa crisis meeting hack 21 januari 2025.docx
Minutes Mesa crisis meeting hack 22 januari 2025.docx
Minutes Mesa crisis meeting hack 23 januari 2025.docx
Minutes Mesa crisis meeting hack 24 januari 2025.docx
Minutes Mesa crisis meeting hack 27 januari 2025.docx
Minutes Mesa crisis meeting hack 28 januari 2025.docx
Minutes Mesa crisis meeting hack 6 februari 2025.docx
Notulen 01 CMT_LIS – Cybercrisis januari 2025.docx
Notulen 02 CMT_LIS – Cybercrisis januari 2025.docx
Notulen 03 CMT_LIS – Cybercrisis januari 2025.docx
Notulen 04 CMT_LIS – Cybercrisis januari 2025.docx
Notulen 05 CMT_LIS – Cybercrisis januari 2025.docx
Notulen 06 CMT_LIS – Cybercrisis januari 2025.docx
Notulen 07 CMT_LIS – Cybercrisis januari 2025.docx
Notulen 08 CMT_LIS – Cybercrisis januari 2025.docx
Notulen 09 CMT_LIS – Cybercrisis januari 2025.docx
Notulen 10 CMT_LIS – Cybercrisis januari 2025.docx
Notulen 11 CMT_LIS – Cybercrisis januari 2025.docx
Notulen 12 CMT_LIS – Cybercrisis januari 2025.docx
Notulen 13 CMT_LIS – Cybercrisis januari 2025.docx
Notulen 13 CMT_LIS – Cybercrisis januari 2025.docx
Onderwijs op TU/e wordt maandag hervat, gehackte computersystemen afdoende gerepareerd_Eindhoven_ed.nl.pdf
Ook dinsdag geen colleges op TU/e door cyberaanval_'Er is geen contact met de hackers'_Eindhoven_ed.nl.pdf
OTO Plan Crisisorganisatie TUe.pdf
Overzicht notulen werkgroep Facilities RE-FMC inzake cyberaanval.pdf
Overzicht notulen werkgroep Facilities RE-FMC inzake cyberaanval.pdf
Pre-bsa in view of cyber-attack -approved by CvB final.docx
Procedure for handling alternative exam requests final.pdf
Process for memo financial consequences final.pdf
Promoties.docx
Proposal to resolve bsa issues due to postponed Q2 exams final.pdf
RE archief cyberattack.eml
RE Startgesprek Evaluatie crisisorganisatie cyberaanval 11 januari 2025.eml
REP_Armstrong_221856_TechnicalReport_v1.0_FINAL_REDACTED.pdf
Rest punten vanuit CMT_LIS – Cybercrisis januari 2025.docx

Revised calendar_EN_2024-2025.pdf
Scenarios systemen down ESA definitief.docx
Schade cyberaanval TU/e valt mee_Instagram_ed.nl.pdf
Tentamens TU/e uitgesteld na cyberaanval_volledig herstel systemen duurt weken_Binnenland_ed.nl.pdf
Tijdslijnen eerste uren cybercrisis – Timeline ARMSTRONG_v1.1 .pptx
Timeline LIS cirisis.xlsx
timeline LIS crisis kopie 24-03-2025
Topic list rescheduling education final.xlsx
Update Partner Education final.docx
Verslaglegging CCT januari 2025.docx
Verslaglegging CCT tot 15 januari.docx
Voorstel team Educational Planning definitief.docx

BIJLAGE C – Afkortingenlijst

Afkorting	Begrip
BCM	Business Continuity management
BOB	Beeldvorming, Oordeelsvorming en Besluitvorming
BOBOC	Beeldvorming, Oordeelsvorming, Besluitvorming, Opdracht en Controle
CCT	Centraal Crisis Team
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
CRT	Crisis Response Team
CvB	College van Bestuur
DDoS	Distributed Denial of Service
ESA	Education and Student Affairs
M&CS	Mathematics & Computer Science
HR	Human Resources
HSE	Health, Safety and Environment
LIS	Library and Information Services
LIS-CMT	LIS-Crisis Management Team
NWO	Nederlandse Organisatie voor Wetenschappelijk Onderzoek
OCW	Onderwijs, Cultuur en Wetenschap
OTO	Opleiden, Trainen, Oefenen
PAL	Product Area Lead
PO	Product Owner
SaaS	Software as a Service
UNL	Universiteiten van Nederland
VPN	Virtual Private Network

BIJLAGE D – Respondentenlijst

Respondenten
Chief Information Officer / Adviseur CCT
CISO / Adviseur CCT
COO SURF - Lid RvB - SURF
Dean M&CS / Adviseur CCT
Deputy Director of TU/e Communication Expertise Center (CEC)
Directeur-Generaal Hoger onderwijs OCW
HR Manager / Adviseur CCT
Information Security Officer / Member LIS CERT
Manager Education and Students Affairs (ESA)
Manager Internal Audit / Observator CCT
Managing Director C&CS / Adviseur CCT
Managing Director ESA / Adviseur CCT
Managing Director Real Estate / FMC a.i. / Adviseur CCT
Policy Advisor Integral Safety
Product Area Lead Data & Insights / plaatsvervangend directeur LIS / LIS Crisis Management Team
Programmadirecteur integrale veiligheid / Hoofd safety en security / Tech. Voorzitter CCT
Projectleider/Senior inspecteur hoger onderwijs
Secretaris van de Universiteit
Secretary Executive Board / Notulist CCT
TU/e Mediawoordvoerder / Adviseur CCT
Vicevoorzitter CvB / Voorzitter CCT
Voorzitter CvB OU / UNL bestuurlijk trekker voor Cyber en Integrale Veiligheid
Voorzitter Raad van Toezicht TU/e
Deelnemers interne lessensessie – divers

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 wetgevings- en toezichtsdoeleinden.

Over het COT

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 betrokken zijn. Advies, onderzoek, training en oefening vormen de basis van onze dienstverlening. Het COT is een volledige dochteronderneming van Aon Nederland.

Meer informatie: https:/www.cot.nl of cot@cot.nl.