Samen aanjagen van vernieuwing

Tabletop crisisoefening

Crisis: Geen toegang tot Office365

Auteur: Charlie van Genuchten

Versie: 1
Datum: 5 augustus 2025
Kenmerk: Tabletop crisisoefening

Inhoudsopgave

Samenvatting **2**

Tabletop crisisoefening **3**

Algemene info **3**
Oefendoelen **3**
Opzet oefening **3**
Timing *3*
Oefenteam *3*
Rollen oefenleiding *3*
Rondes *4*
Persconferentie *4*
Nabespreking *4*
Voorafgaand aan de oefening **4**
Verhaal van de oefening (voor oefenleiders) **5**

Samenvatting

Dit is een kant en klare crisisoefening die gemaakt is voor onderwijsinstellingen in het kader van NOZON. De oefening kan met drie oefenleiders en vijf of meer deelnemers worden uitgevoerd in twee uur, inclusief nabespreking.

Tabletop crisisoefening

Algemene info

Lengte oefening: 2 uur
Nodig voor oefenleiding: 3 mensen
Max aantal spelers: 5 per oefenteam, eventueel kunnen rollen door twee mensen worden gespeeld of kun je meerdere teams tegelijk de oefening laten spelen
Elementen oefenpakket: In dit document vind je eerst een uitleg van de oefening ter voorbereidign en daarna een slidedeck om te gebruiken tijdens de oefening.

Oefendoelen

De oefendoelen van deze oefening zijn:

- Bewustwording van het thema cybercrisis
- Oefenen met een crisisoverleg structuur (BOB methode)
- Teambuilding

Opzet oefening

Timing

Tijd	**Wat**
15 minuten	Welkom, doornemen slides startinformatie en casus, rollen oefenteam verdelen
Ronde 1	
5 minuten	Updates
10 minuten	Crisisvergadering
Ronde 2	
5 minuten	Updates
10 minuten	Crisisvergadering
Ronde 3	
5 minuten	Updates
10 minuten	Crisisvergadering
10 minuten	Persconferentie
Afronding	
20 minuten	Pauze
30 minuten	Nabespreking

Oefenteam

Het oefenteam zal de oefening in gaan als het crisisteam van het Dyson Institute of Fine Arts. Binnen dit crisisteam zullen zij de volgende rollen spelen:

- CvB lid
- Crisis coördinator
- Secretaris
- Hoofd communicatie
- Directeur IT

Rollen oefenleiding

De oefenleiding bestaat uit drie personen.

Eén van hen is de hoofd oefenleider die de intro van de oefening plenair doet.
Daarnaast spelen alle drie de oefenleiders tijdens de updates een rol:

- De gedetacheerde sysadmin
- Een communicatiemedewerker van het Dyson Institute of Fine Arts
- De bestuurssecretaris van het Dyson Institute of Fine Arts

Rondes
Elke ronde start met een update waarbij de volgende mensen gelijktijdig informatie krijgen van de oefenleiders:

- De directeur IT krijgt een update van de gedetacheerde sysadmin
- De secretaris en hoofd communicatie krijgen een update van de communicatiemedewerker
- De crisis coördinator en het CvB lid krijgen een update van de bestuurssecretaris

NB: het is de bedoeling dat iedereen alleen de informatie hoort van hun update en dat het crisisteam dus de informatie bij elkaar moet leggen om een geheel beeld van de situatie te krijgen. Zorg er daarom voor dat de updates fysiek in verschillende ruimtes/ verschillende hoeken van de kamer worden gegeven.
Tijdens de updates mogen de spelers ook dingen vragen aan de oefenleiders en opdrachten geven.
Tijdens de crisisvergadering lopen omstebeurt de oefenleiders de kamer in om de injects op papier te geven. De timing hiervan bepalen de oefenleiders zelf.

Persconferentie
Aan het eind van de oefening vindt een persconferentie plaats. Hier spelen de drie oefenleiders de verschillende journalisten die vragen stellen over wat er precies is gebeurd.

Nabespreking
Bij de nabespreking haal je met elkaar op wat men van deze oefening heeft geleerd. Hieronder een aantal vragen om die de oefenleiders kunnen vragen om dit proces te begeleiden:

- Hoe gingen de crisisvergaderingen? Wat ging er goed en wat kan beter?
- Hoe was dit gegaan als het een echte crisis in onze organisatie was geweest?
- Hebben we zaken geleerd waardoor we onze procedures aan moeten passen?

Laat de deelnemers hun feedback per onderwerp op post its schrijven. Check daarna of er acties nodig zijn naar aanleiding van de feedback en zorg dat deze acties elk een eigenaar krijgen zodat deze worden opgevolgd.

Voorafgaand aan de oefening

De hoofd oefenleider print de volgende zaken uit:

- De rolbeschrijving en tekst oefenleiders slides -> op zo'n manier dat elke rol hun eigen rolbeschrijving en updates heeft
- De injects op papier slides -> daarna uitknippen zodat deze los kunnen worden verspreid tijdens de oefening

Verhaal van de oefening (voor oefenleiders)

- Dyson Institute of Fine Arts is een kleine hogeschool met weinig budget voor en kennis over IT. Ze hebben daarom een paar jaar geleden alles overgezet naar Office365 en huren een hoofdsysteembeheerder in van een detacheringsbedrijf. Er is wel een servicedesk voor (en grotendeels door) studenten, voor kleinere vragen en problemen. Het hoofd bedrijfsvoering heeft als één van zijn/haar vele petten ook 'directeur IT'.
- De nacht voor onze oefening, heeft een student die werkt bij de servicedesk toegang tot alle Microsoft systemen onmogelijk weten te maken door alle wachtwoorden te veranderen.
- De recovery key van ActiveDirectory staat ergens op de laptop van de hoofdsysteembeheerder (gespeeld door De sys admin), die niet meer kan inloggen want zijn wachtwoord is gewijzigd. Zijn laptop is met BitLocker encrypted en de recovery key van de BitLocker staat in de ActiveDirectory, dus hij kan dit niet zomaar even fixen.
- Dit betekent dat alle mensen die opnieuw inloggen in de systemen die in de Microsoft cloud staan of via Microsoft worden ontsloten, nergens meer binnenkomen. En aangezien Dyson Institute of Fine Arts geheel 'in de cloud' zit, is de impact groot:
    - Voor de studenten is het vrij snel chaos. Zeker eerstejaars studenten kunnen nergens bij om info te vinden over hun eerste colleges en raken gestresst en gefrustreerd.
    - Docenten kunnen al snel ook nergens meer bij en kunnen geen colleges meer geven, cijfers invoeren etc. Het wordt extra frustrerend als zij ook niet meer in hun laptop komen als ze deze herstarten, aangezien die ook alleen werkt met Microsoft toegang
    - Het events team is ook alles kwijt voor de Dies Natalis de volgende dag: contactgegevens, gastenlijst etc. Extra problematisch omdat veiligheid van gasten scherp moet worden gewaarborgd.
    - Bij bedrijfsvoering is het ook chaos: het intranet loopt via Microsoft, dus officiële interne communicatie is moeilijk. Via onofficiële chat kanalen beginnen steeds meer geruchten te ontstaan dat er een ransomware aanval gaande is.
- Contact met Microsoft krijgen gaat moeizaam, omdat alle credentials etc in het dashboard zitten waar men niet meer bij kan. Na lang proberen via het algemene nummer, kan de hoofdsysteembeheerder uiteindelijk bij Microsoft bevestiging krijgen dat:
    - inderdaad zo'n 2000 wachtwoorden zijn gewijzigd afgelopen nacht
    - er geen aanwijzingen zijn dat er iets anders gaande is (zoals ransomware)
    - de systeembeheerder weer toegang kan krijgen om het systeem weer in handen te krijgen.
- Het is daarna aan het crisisteam om te beslissen wat de prioriteit is van het uitrollen van nieuwe wachtwoorden. Uiteindelijk kan daarmee aan het eind van de oefening worden geconcludeerd dat alles weer up and running is.
- De vraag is aan het eind dan vooral: is er nagedacht over wie er achter deze aanval zat? Als oefenleiders weten wij dat dit alleen maar een student was die zat te treiteren, maar het had ook een crimineel of zelfs een statelijke actor kunnen zijn (je hebt per slot van rekening een spreker bij je Dies Natalis die zich heel vaakt uitspreekt tegen het Chinese regime). Mochten de teams hier dus niet bij stil hebben gestaan tijdens hun gesprekken, hebben ze eigenlijk de vraag gemist hoe je kan achterhalen dat dit niet nogmaals gaat gebeuren.

Startinformatie en casus

Doelen oefening

- Bewustwording van het thema cybercrisis
- Oefenen met een crisisoverleg structuur (BOB methode)
- Teambuilding

Verloop oefening

Tijd	Wat
15 minuten	Welkom, achtergrond oefening, rollen oefenteam verdelen, casus
Ronde 1	
5 minuten	Updates
10 minuten	Crisisvergadering
Ronde 2	
5 minuten	Updates
10 minuten	Crisisvergadering
Ronde 3	
5 minuten	Updates
10 minuten	Crisisvergadering
10 minuten	Persconferentie
Afronding	
20 minuten	Pauze
30 minuten	Nabespreking

Achtergrond oefening 1/2

- Jullie spelen als het centrale crisismanagement team van de fictieve kleine hogeschool Dyson Institute of Fine Arts (1800 studenten en 200 medewerkers)
- De rollen in dit crisismanagement team zijn:

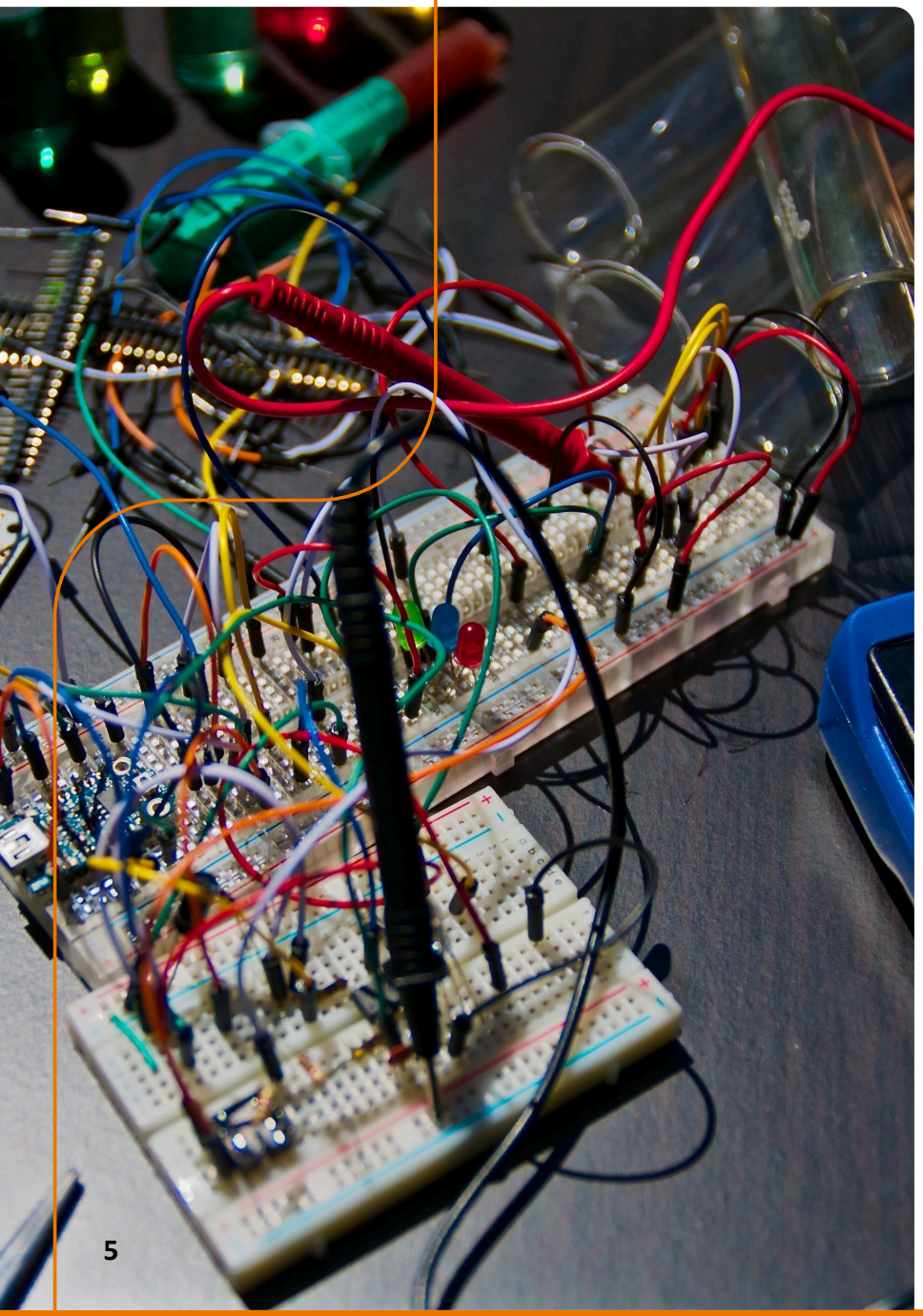
  → CvB lid

  → Crisis coördinator

  → Secretaris/plotter

  → Hoofd communicatie

  → Directeur IT



Achtergrond oefening 2/2

- Dyson Institute of Fine Arts is een kleine hogeschool met weinig budget voor en kennis over IT.
- Jullie hebben daarom een paar jaar geleden alles overgezet naar Office365 en huren een hoofdsysteembeheerder in van een detacheringsbedrijf.
- Er is wel een servicedesk voor (en grotendeels door) studenten, voor kleinere vragen en problemen.
- Het hoofd bedrijfsvoering heeft als één van zijn/haar vele petten ook ‘directeur IT’.

Casus info

- Het is de eerste week van het collegejaar. Het is heerlijk weer, er zijn veel studenten op de campus en morgen is de Dies Natalis van het Dyson Institute of Fine Arts. Omdat het instituut 200 jaar bestaat, zal de wereldberoemde Chinese kunstenaar en dissident Ai Weiwei komen spreken.
- Rond 10:00 beginnen meldingen binnen te stromen bij de helpdesk dat mensen geen toegang meer hebben tot hun instellingsaccounts. Eerst zijn het vooral eerstejaars, dus het eerste twintigtal meldingen wordt niet heel serieus genomen. Na anderhalf uur is echter duidelijk dat het niet om onbegrip of een tijdelijke storing gaat. Ondertussen kunnen ook steeds meer medewerkers niet meer in hun systemen en beginnen kunnen steeds meer mensen ook niet meer inloggen op hun laptop.
- Het crisisteam is bijeengeroepen om beslissingen te nemen over de voortgang van onderwijs en verdere consequenties voor de Dies Natalis


Rolbeschrijving
en tekst
oefenleiders

Rolbeschrijving IT persoon

- Gedetacheerde hoofdsysteembeheerder
- Goed in zijn baan, maar heeft ook drie andere bedrijven waar hij aandacht aan moet besteden
- Heeft al vaker aangegeven bij Dyson IoFA dat er meer FTE beschikbaar moet zijn in hun eigen organisatie voor IT en zeker security zaken
- Heeft goed contact met de directeur IT

Rolbeschrijving communicatie medewerker

- Communicatie medewerker van Dyson IoFA
- Heeft media en crisis communicatie training gehad
- Is pro actief en pakt zaken zelf op
- Maar legt grotere beslissingen en vraagstukken terecht terug bij hoofd communicatie

Rolbeschrijving bestuurssecretaris

- Bestuurssecretaris Dyson IoFA
- Werkt al 30 jaar bij deze hogeschool en kent iedereen
- Is faciliterend en weet goed contact te houden met iedereen
- Pakt zelf niet vanzelf dingen op, wacht opdrachten af

Ronde 1

Update IT Ronde 1

- Zenden (onafhankelijk van wat men vraagt):
  - Alle systemen die afhankelijk zijn van Microsoft zijn onbereikbaar:
    - De Elektronische Leeromgeving (ELO), Intranet, Email, Videoconferencing omgeving, Document deelomgeving, Toegang tot laptops etc.
  - Als hoofdsysteembeheerder kom jij ook niet in jouw laptop en kan daar niet omheen werken. Jij hebt al heel vaak gevraagd aan de vorige directeur IT om master key en die is nooit gekomen (mopper mopper)
  - De servicedesk wordt compleet overvraagd op dit moment en zij kunnen niets betekenen -> **Je suggereert om de servicedesk te laten sluiten en hen te laten helpen met uitzoeken wat er gaande is**
  - Jij moet eigenlijk door naar een andere klant -> **Je suggereert dat de directeur IT met jouw baas regelt dat je de rest van de dag op campus kan blijven**

Update IT (vervolg) Ronde 1

- Mocht er naar worden gevraagd:
  - Het is nog niet te zeggen of het hier om een fout bij Microsoft gaat
  - Het is nog niet te zeggen of dit een aanval is
  - Er zijn geen aanwijzingen dat China betrokken is
  - Partijen die hierbij kunnen helpen zijn SURFcert en een commerciële partij zoals Fox IT
  - Het is nu nog niet te voorspellen hoe lang dit probleem zal voorduren
  - Het is ook niet duidelijk of dit probleem ook bij andere instellingen speelt
- Bij alle andere vragen zeg je: dat moet ik uitzoeken

Update Communicatie Ronde 1

- Zenden (onafhankelijk van wat men vraagt):
  - Het is redelijke chaos in de organisatie: De grootste problemen liggen nu bij de servicedesk: zij weten niet wat zij moeten zeggen tegen alle studenten die zich melden -> **suggereer dat de servicedesk vooral een communicatietaak moet krijgen en vraag om een eenduidige boodschap**
  - Op social media komt er wat gemopper van studenten langs. Op dit moment is het nog geen enorme storm aan tweets, maar als we niet snel met een statement komen, kan het uit de hand lopen -> **suggereer een veilig soort statement om op dit moment te geven**
  - Er is nog geen aandacht vanuit de nieuws media
  - Er gaan veel geruchten over ransomware de ronde.
  - Jij moet snel weten wat er daadwerkelijk aan de hand is om verder te kunnen communiceren.

Update Communicatie (Vervolg) Ronde 1

- Mochten ze ernaar vragen:
  - Je hebt via de social media kanalen niets gezien van Microsoft of andere instellingen dat er een bekend probleem is wat breder speelt
  - Over het feit dat Ai Wei Wei komt spreken is veel minder reuring geweest dan van tevoren gedacht.

- Bij alle andere vragen zeg je: dat moet ik uitzoeken

Update Impact Ronde 1

- Zenden:
  - Grootste problemen op dit moment voor studenten en onderwijs: ELO, email, toegang tot laptops allemaal niet mogelijk
  - Cijfers kunnen niet in het systeem worden gezet
  - Studenten weten niet waar ze moeten zijn voor hun colleges
  - Het events team zit ook op hete kolen, want alle info voor de Dies is onbereikbaar
  - Alle interne communicatie is onmogelijk via normale kanalen
  - Jij hebt gehoord dat dit een ransomware aanval is

Update Impact (vervolg) Ronde 1

- Mochten ze ernaar vragen:
  - Bedrijfsvoering nog geen grote problemen, behalve dat mensen hun werk niet kunnen doen.
  - Er zijn geen fysieke gevaren voor zover nu duidelijk: de gebouw beheersystemen zijn onafhankelijk van Microsoft

Ronde 2

Update IT Ronde 2

- Zenden:
  - Ondertussen heb jij contact kunnen krijgen met Microsoft en is duidelijk dat er inderdaad zo'n 2000 wachtwoorden zijn veranderd afgelopen nacht.
  - Jij bent nog bezig met kijken of jij aan de verificatiecode kan komen om Microsoft zo ver te krijgen om jou een nieuw wachtwoord te geven en toe te sturen -> **Suggereer dat er iemand vanuit de organisatie daarbij helpt, aangezien jij zelf een gedetacheerde bent**
  - In de tussentijd zijn er geen workarounds, dus ga er vanuit dat in ieder geval de rest van de dag alles eruit ligt.
  - Via SCIRT wordt gevraagd om info te delen over de hack, aangezien andere security professionals door beginnen te krijgen dat er iets mis is bij ons -> **Vraag of we in ieder geval via SURFcert kunnen delen wat we tot nu toe weten onder TLP:RED**

Update IT (vervolg) Ronde 2

- Mocht er naar worden gevraagd:
  - Er zijn geen aanwijzingen dat het om een ransomware aanval gaat

Update Communicatie Ronde 2

- Zenden:
  - Jij hebt de volgende dingen al gedaan:
    - Voor interne communicatie is er een bericht uitgegaan op verschillende slack channels
    - Extern is via twitter is een bericht uitgegaan dat we op de hoogte zijn van de problemen en een update geven als er meer duidelijkheid is.
  - Ondertussen is er steeds meer aandacht vanuit de pers. We hebben nu vragen van de Trouw, NRC en NOS gekregen. Men wil weten of dit een ransomware aanval is en of China hier wellicht achter zit.
  - **Jij vraagt om een eenduidige boodschap wat er nu precies gaande is en hoe lang dit nog gaat duren**

Update Communicatie (vervolg) Ronde 2

- Mocht ernaar worden gevraagd:
  - Het events team van de Dies Natalis wil graag weten hoe zij moeten communiceren over dit alles

Update Impact Ronde 2

- Zenden:
  - Het gebrek aan een eenduidige lijn zorgt ervoor dat docenten op dit moment zelf maar beslissen of lessen doorgaan.
  - Sommige faculteiten zijn via twitter, facebook en instagram gaan communiceren over de introductie activiteiten.
  - Op de campus zelf is het een chaos, want alle info over waar men moet zijn voor welk college is nu niet te vinden. Er is fysieke begeleiding nodig om dit in goede banen te leiden, want de secretariaatsmedewerkers kunnen de vragen niet opvangen.
  - Het events team heeft ondertussen een eigen crisisberaad gehouden en zij hebben in ieder geval hun draaiboek weer op een rij kunnen zetten. Volgens hen is het grote pijnpunt de toegang tot de gastenlijst, omdat ze anders morgen de veiligheid van het evenement niet kunnen garanderen.

Ronde 3

Update IT Ronde 3

- Zenden:
  - Jij hebt Microsoft zover gekregen om jouw te voorzien van een nieuw wachtwoord (hoera!) en jij kan nu beginnen met het uitrollen van de toegang voor alle anderen.
  - Jij moet hiervoor weten wie er prioriteit moet krijgen, want de mensen die gelijk toegang moeten krijgen, zullen van jouw een SMSje moeten krijgen.
  - De mensen die individueel van jou een reset krijgen, zullen binnen een uurtje weer up and running zijn. Maar: hoe groter die groep, hoe langzamer dat proces wordt.
  - De rest (alle studenten etc) worden en masse gereset en moeten een brief krijgen voor het aanmaken van een nieuw wachtwoord. Voor hen zal het een paar dagen duren voor alles rond is

Update Communicatie Ronde 3

- Zenden:
  - Ondertussen hebben de NOS, Trouw en NRC artikels gepubliceerd dat DysonIoFA is gehackt.
  - Jij hebt de geruchten over ransomware klein weten te houden, maar jullie zijn verder niet in een goed daglicht komen te staan door de chaos op de campus.
  - Andere newsoutlets (de regionale krant *Plains of Rous Weekly* en de Telegraaf) plus de studentenkrant hangen nu ook aan de lijn. Zij vragen hoe dit heeft kunnen gebeuren en hoe veilig de data van studenten zijn.
  - Het ministerie en vier andere hogescholen willen ondertussen weten wat er aan de hand is -> **suggereer dat de onderwijskoepel wellicht kan helpen met het verspreiden van informatie**
  - **Er zal een persconferentie plaatsvinden over een kwartier,**dus het is van belang om duidelijk te kunnen communiceren wat de lijn is die we willen volgen.

Update Communicatie (vervolg) Ronde 3

- Mochten ze ernaar vragen:
  - Door alle externe aandacht, kom jij niet toe aan de interne communicatie (naast dat dit nog steeds heel moeilijk is door het gebrek aan officiële communicatie).
  - Als zij vinden dat je juist de interne communicatie voorrang moet geven, kun je switchen, maar dit betekent wel dat externe communicatie tijdelijk niet wordt opgevangen

Update Instellingsbrede Impact Ronde 3

- Zenden:
  - Een aantal docenten heeft het heft in eigen handen genomen en zijn grote co-creatie sessies begonnen in het atrium en een paar grotere zalen. Zo hoeft niemand precies te weten waar hij/zij hoort te zijn en wordt er van de chaos gebruik gemaakt om nieuwe vragen te stellen en verbindingen te leggen.
  - Niet alle studenten zijn hiermee geholpen, maar de druk is voor nu van de pan voor het grootste deel eerstejaars.
  - Voor de Dies Natalis moet **binnen een kwartier** duidelijk zijn of het gaat lukken om weer in de systemen te komen. Als dat niet lukt, moet de hele dag worden afgezegd of verzet, wat een enorme domper en financiële klap zou zijn.

Persconferentie

Vragen Persconferentie

- Carola van de *Plains of Rous Weekly:*
  - Hoe zijn jullie gehackt?
  - Wie zat erachter?
- Alex van de NOS:
  - Wat is de impact geweest van deze hack?
  - Komt studentendata straks op straat te liggen?
- Helga van het NRC:
  - Wat zijn jullie volgende stappen?
  - Wanneer is het weer business as usual?


Injects op papier

RONDE 1


Pierre
ICT
Ik zou nog even nagaan of er ransome notes gevonden waren. Ben dit nagegaan en tot is dat niet het geval (voor zover ik kan nagaan).


Suzanne
Communications
Hee, Alvast een heads-up. Het is onduidelijk hoe officieel kan worden gecommuniceerd: Zowel email als de ELO en het intranet zijn namelijk van Microsoft, dus er zijn geen officiële interne communicatiekanalen.


Robin
Bestuurssecretaris
Heb nog even verder nagevraagd wat de impact aan de bedrijfsvoering is. Vanuit Finance kreeg ik het volgende door: Er zijn nog geen problemen voor de verloning: het financiële systeem is onafhankelijk van Microsoft en we zitten vlak na de eerste salaris uitbetaling. Dus dat is een meevaller.

RONDE 2


Pierre
ICT
Net doorgekregen van Microsoft: zij hebben verder niets verdachts kunnen zien na de verandering van de wachtwoorden

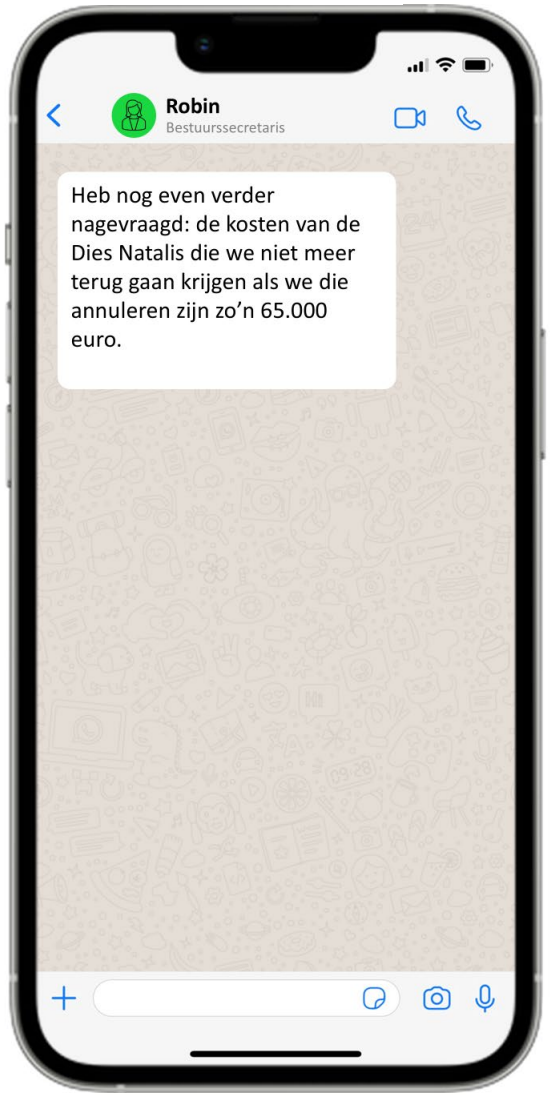

Suzanne
Communications
Op social media is er ondertussen veel onrust. En gaan er veel geruchten rond over ransomware aanvallen en inmenging van de Chinese regering. Kunnen we dit ontkennen? Of is dit een echte mogelijkheid?


Suzanne
Communications
Ik werd net gebeld door de woordvoerder van de Vereniging Hogescholen, die op zijn beurt weer was gebeld door OCW. Beiden willen weten wat er gaande is. Moet ik hier prioriteit aan geven? Of pakken jullie dit vanuit CMT op?

RONDE 3


Pierre
ICT
Heb even verder gekeken en een drietal wachtwoorden is niet gewijzigd. Volgens mij zijn het studentenaccounts, want ik één ervan werkt bij de servicedesk.
Willen jullie dat ik aangifte doe bij de politie van deze studenten?


Suzanne
Communications
Voor de persconferentie: wie zal daar het woord doen? Is dat het CvB lid of hoofd communicatie?


Robin
Bestuurssecretaris
Heb nog even verder nagevraagd: de kosten van de Dies Natalis die we niet meer terug gaan krijgen als we die annuleren zijn zo'n 65.000 euro.