Cybercrisisexercise OZON 2016

FROM IT TO BOARDROOM – A GAP BRIDGING EXERCISE

Remon Klein Tank
(SURFcert / Wageningen University and Research)

SURF NET

Introduction

Remon Klein Tank (CEH, CISSP)
Remon.KleinTank@WUR.NL

- Initiator and projectleader OZON
- Cybersecurity specialist at Wageningen University and Research
- Member of SURFcert (first Dutch Computer Emergency Response Team)
- SCIRT / SCIPR member (cybersecurity community)

Global set-up

Distrubuted
Players stay in their known environment

Two days
One and a half day for the exercise
Half a day for the evaluation

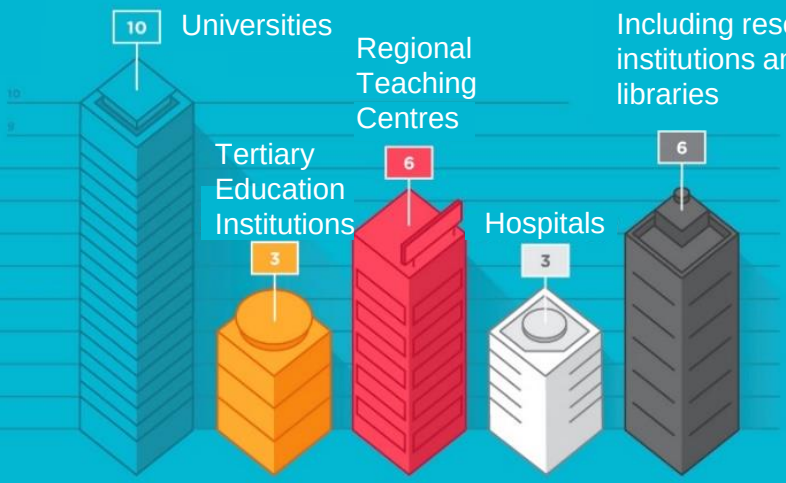
Dynamic
Outside world is being simulated by a responce cell when needed
Responce team creates events on demand to steer exercise back on track

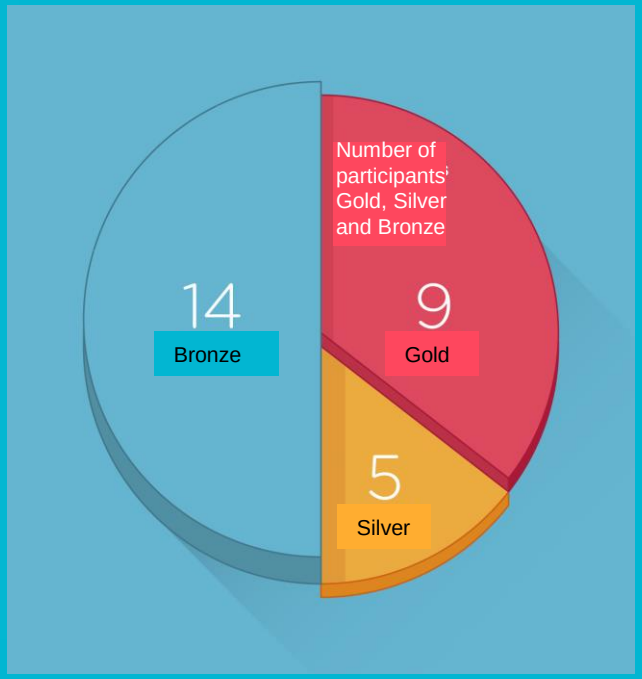
Realistic
Players know there is an exercise, they play themselves, they have no idea what is going to happen
Simulation rather then tabletop
Use of trusted community mail/chat

Participants

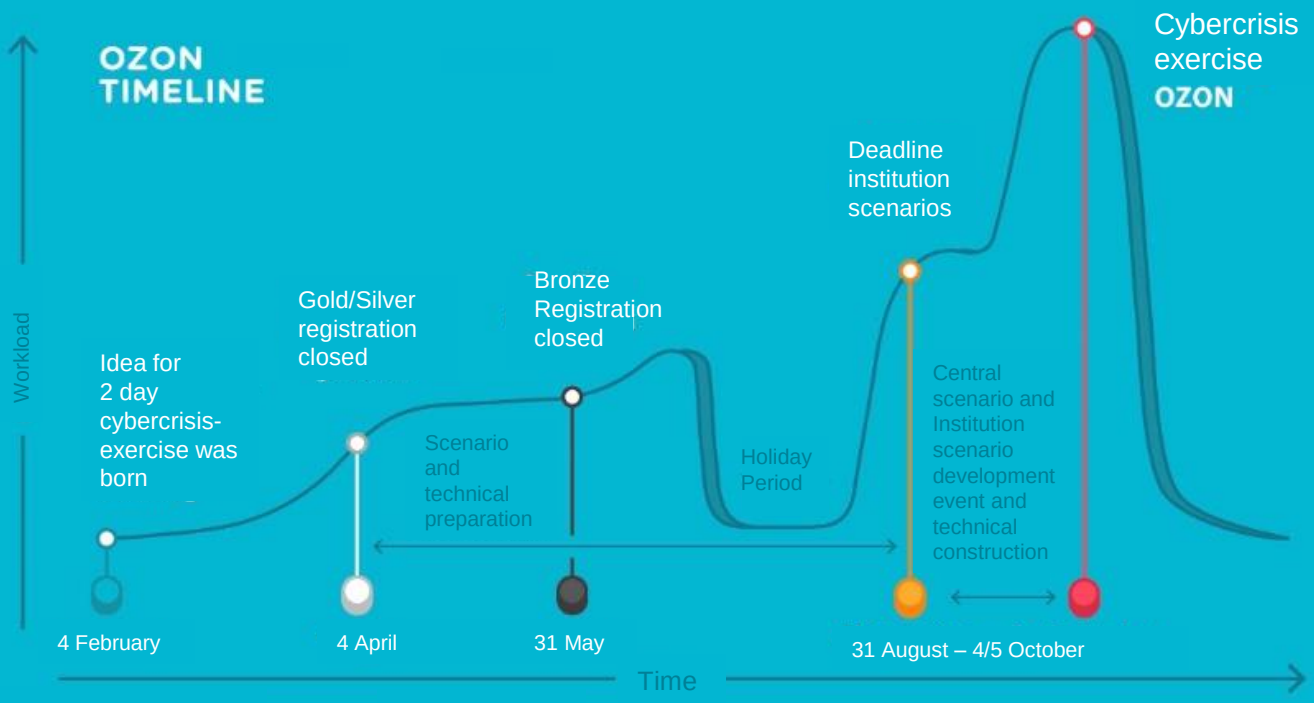
Participating institutions

Total: 28 institutions

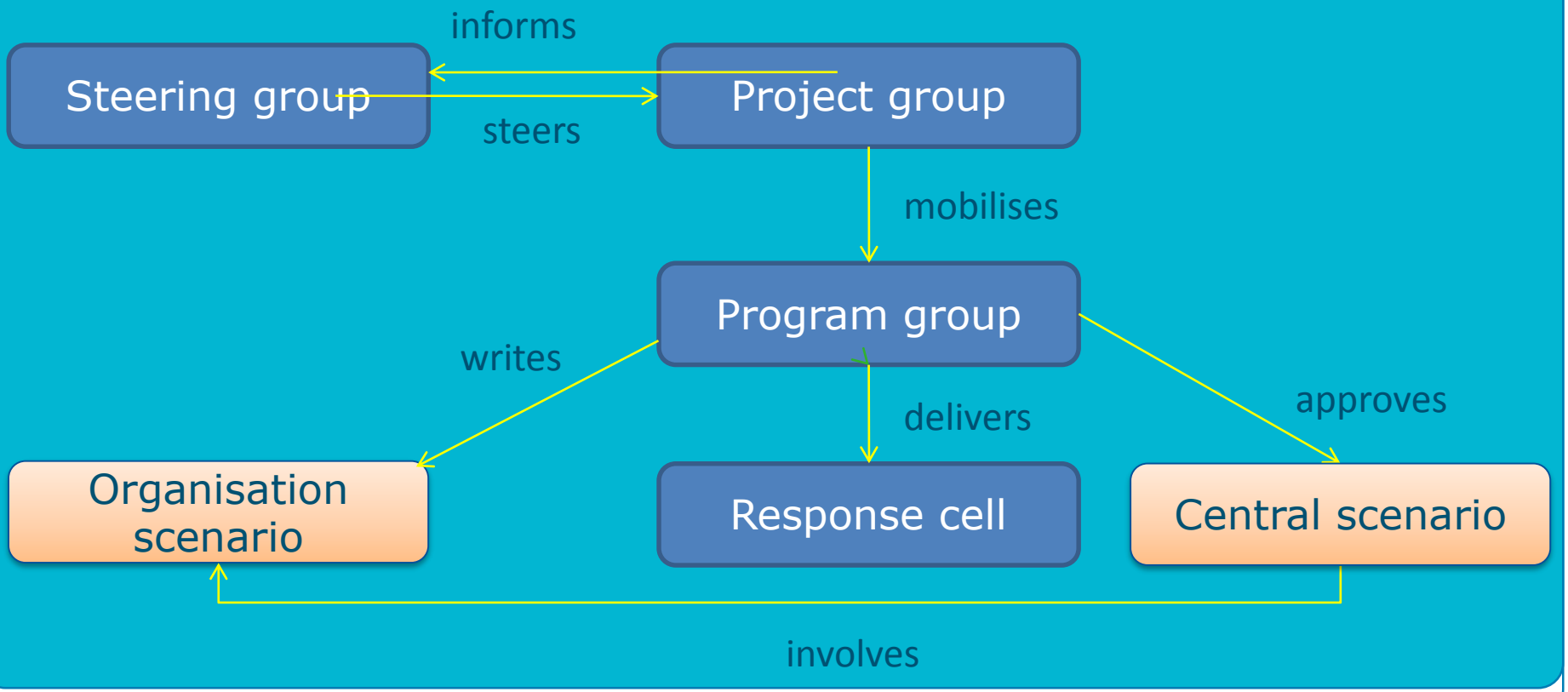




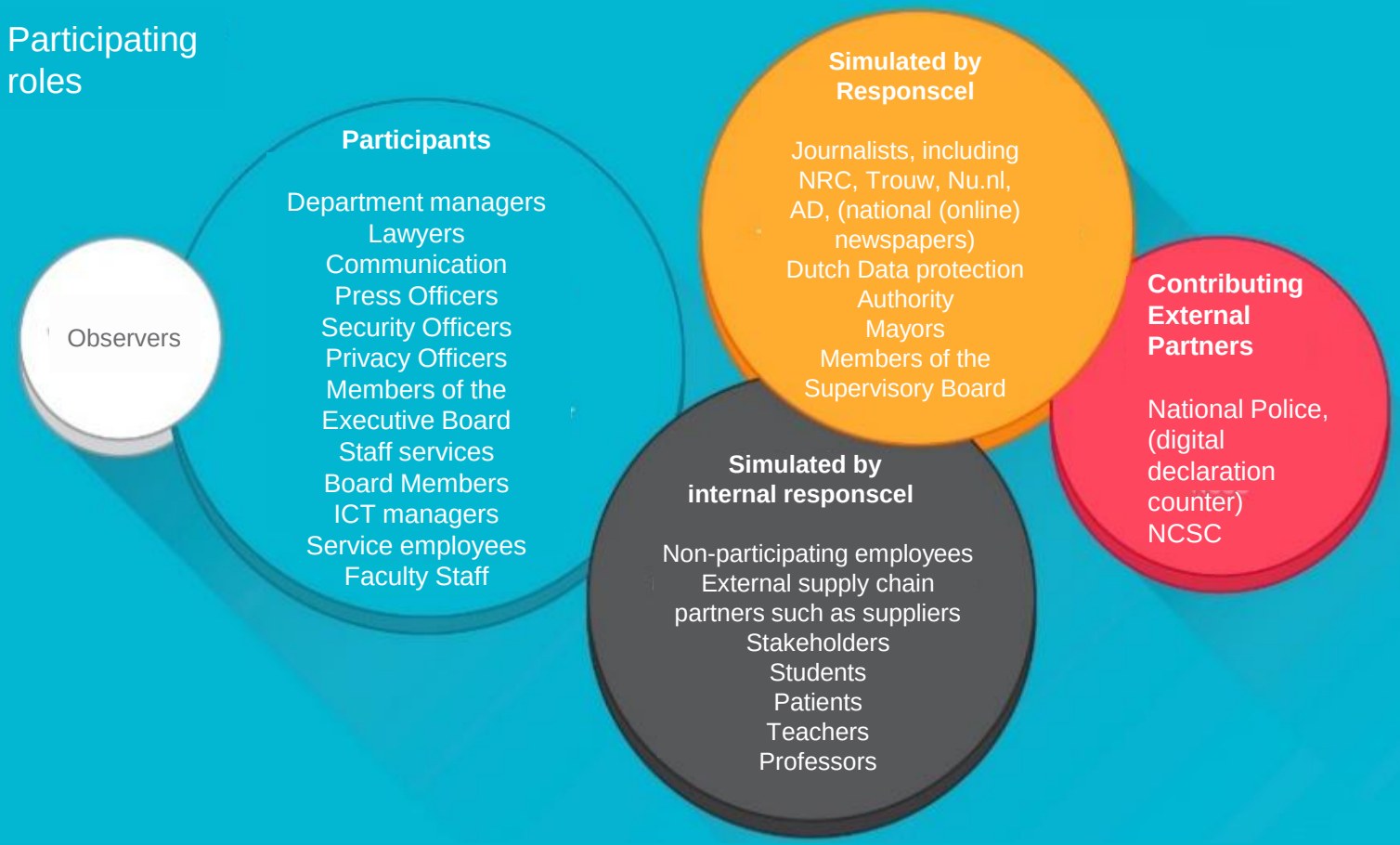
Workload


OZON
TIMELINE
Workload
Idea for
2 day
cybercrisis-
exercise was
born
Gold/Silver
registration
closed
Bronze
Registration
closed
Scenario
and
technical
preparation
Holiday
Period
Deadline
institution
scenarios
Central
scenario and
Institution
scenario
development
event and
technical
construction
Cybercrisis
exercise
OZON
4 February
4 April
31 May
31 August – 4/5 October
Time

Project organisation

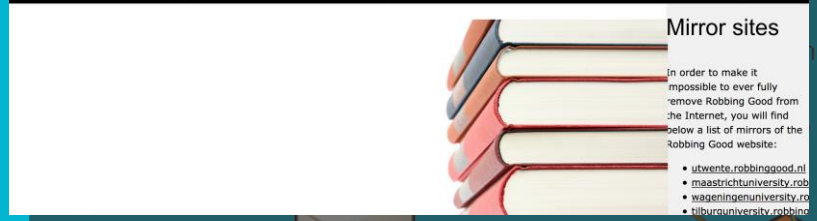


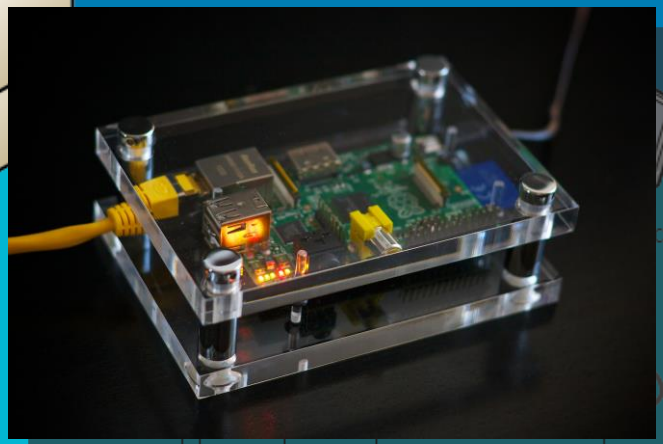
Participating roles



Robbing Good

knowledge is Power, Power to the People!





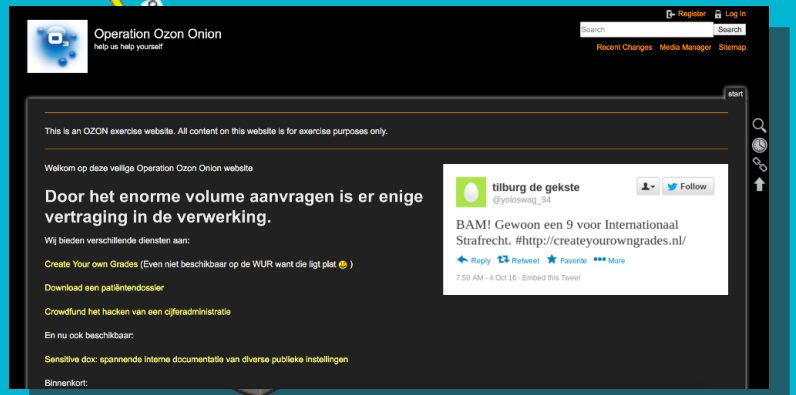
Org. network

Internet

DNS
www.robbingood.nl
organisation1.robbingood.nl
organisation2.robbingood.nl
organisationx.robbingood.nl

Organisation firewall

Internet



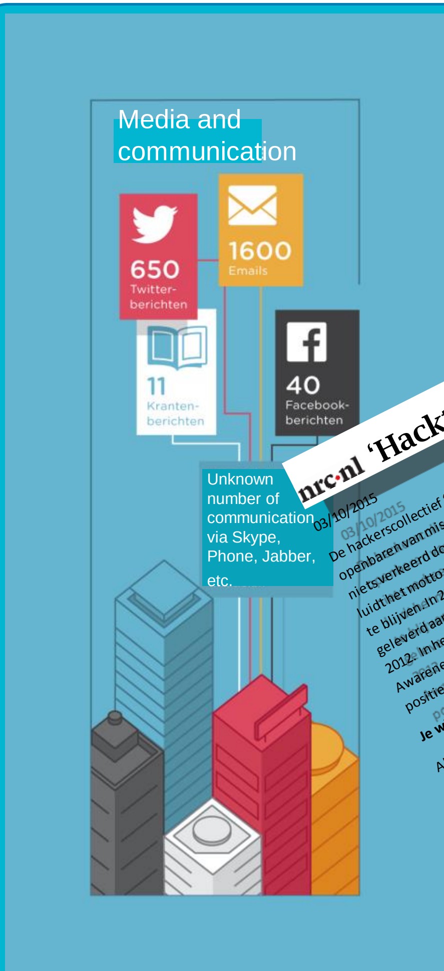
www.createyourowngrades.nl, www.medisearch.nl
Webserver with darkweb howto, credentials, reference to ozonecld53t4surf.onion

ozonecld53t4surf.onion
- Grades
-Medical
-Feedback page
-Crouwdfunding page
-malware distributie howto

SURF NET

SURF NET

Events



nrc·nl 'Hacktivisten' voor transparantie

03/10/2015

De hackerscollectief 'Robbing Good' streeft naar het openbaren van misstanden in de organisatie-top. 'Wie niets verkeerd doet, heeft dus ook niks te verbergen' luidt het motto van de groepsleider die anoniem dient te blijven. In 2010 heeft het collectief een bijdrage geleverd aan WikiLeaks en het hacken van Stratfor in 2012. In het teken van de internationale Cyber Security Awareness-week praat NRC met de groep over de positieve kanten van hacken.

Je wilt graag anoniem blijven. Zijn jullie een soort Anonymous?

Alhoewel Anonymous een hoop geweldig hacktalent heeft waar wij bijzonder jaloers op zijn, willen wij Robbing Good daar niet mee vergelijken. Anonymous staat bekend om het uitvoeren van targeted attacks en het platleggen van systemen van individuen of groepen waar zij het niet mee eens zijn. Wij daarentegen vinden het vooral belangrijk dat informatie vrij te verkrijgen is bij een bedrijf of publieke organisatie onheuse praktijken kan verschuilen achter intellectuele eigendom, privacy en veiligheid.

Ozon.onion – Een onvoldoende? 40 Euro lost het op

Aad Gille – 04/10/2016

nrc·nl

Cyberveiligheid 101

05/10/2016

De acties van het hackerscollectief Robbing Good en het dark webportal Ozon.onion hebben het belang van cyberveiligheid weer op de kaart gezet. Om uzelf en uw organisatie zo goed mogelijk te beschermen tegen cybercriminelen, is bewustzijn van cyberrisico's en het nemen van beveiligingsmaatregelen van groot belang. Informatiebeveiligingsexpert Sanne Drievliet spreekt in een interview met *NRC* over de need-to-knows in de cyberjungle.

Wie zit er achter cyberaanvallen en datalekken?

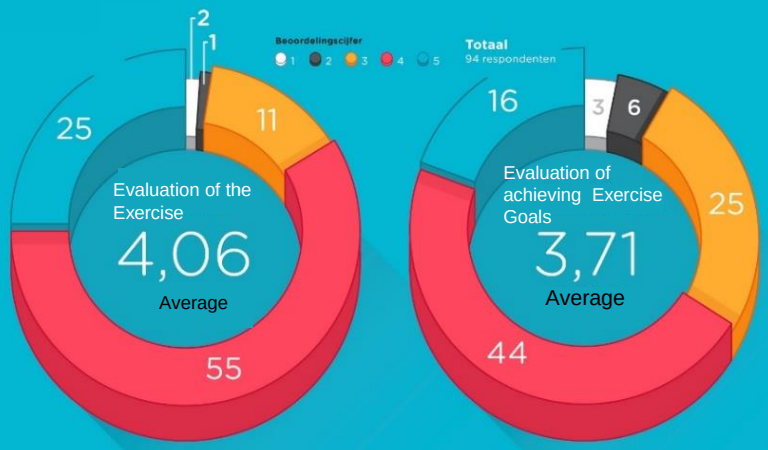
In tegenstelling tot wat er vaak op tv te zien is zijn hackers doorgaans geen pokdalige pubers die voor de lol organisaties aanvallen. Het zijn professional, georganiseerde hackers die doelgericht computersystemen betreden. Zij kunnen hun sporen zo uitwissen zonder dat de gehackte organisatie daar nooit achter komt. Infiltraties worden meestal veroorzaakt door:

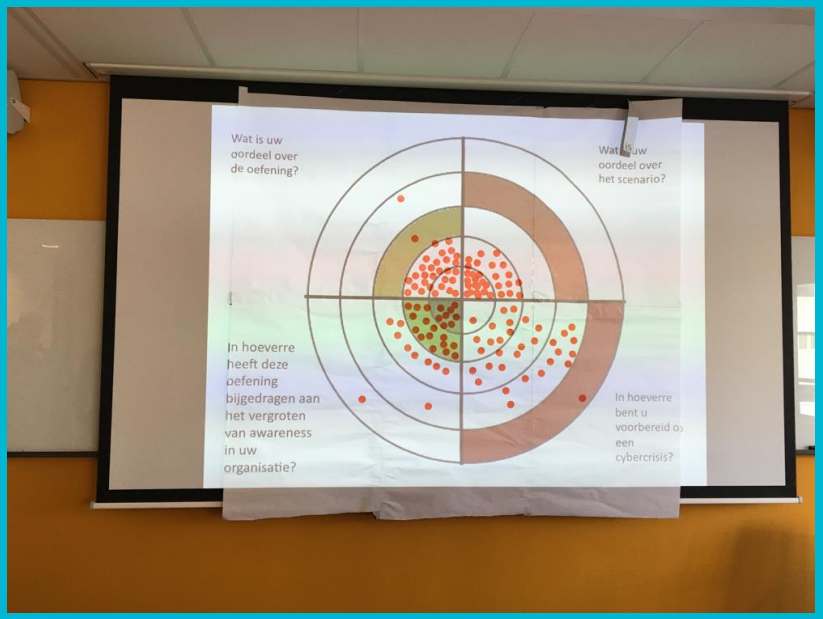
- Cybercriminelen: zij zijn achter geld aan en plegen hiervoor fraude of verkopen informatie door;
- Bedrijfsconcurrenten en buitenlandse inlichtingendiensten: zij stelen informatie om economische- of politieke voordelen te behalen;
- Hackers: het infiltreren van goed beveiligde systemen is een leuke uitdaging;
- Hacktivisten zoals Robbing Good: plegen cyberaanvallen uit politieke of ideologische doeleinden;

Evaluation

Ratings

Evaluation





To know more? / Questions?

- White paper available in Dutch and English
- https://www.surf.nl/kennisbank/2016/
- whitepaper-cybercrisisoefening-ozon.html

- Script of OZON in Dutch
- https://www.surf.nl/kennisbank/2017/handleiding-en-draaiboek-opzetten-cybercrisisoefeningen.html
- Soon also in English available

- Video impression with English subtitles
- https://www.youtube.com/watch?v=DqS0g9kuDmc