Title: OZON, a gap bridging exercise
Proposer: Sandy Janssen, SURFnet
Authors: Sandy Janssen, SURFnet, (speaker)
Alf Moens, SURFnet

Keywords: Crisis simulation, security, large scale exercise, incident response

Biography Sandy Janssen
Sandy Janssen participates in the Young Talent Program of SURFnet since may 2016 and is currently working on projects in information security at SURFnet together with Alf Moens. She is one of the organizers of the cybersecurity exercise OZON.
In 2013 she graduated as Master of Law at the University of Groningen (RUG) on the safety regulations for High Voltage Power Lines. During her studies, she worked at the Centre of Information Technology of the University of Groningen.

Biography Alf Moens
Alf Moens is the Corporate security officer of SURF and responsible for information security management at SURF, SURFnet, SURFmarket and SURFsara. He coordinates compliance and control in information security for the SURF and SURFnet subsidiaries. In 2007 Alf graduated as Master of Information Security Management at Tilburg University (TIAS). He has been security manager at Delft university for 8 years and is a board member of the Dutch association of information security professionals (PvIB). Alf is one of the initiators of the TERENA Special Interest Group in information Security Management (SIG-ISM) and is chairman of the steering committee of this SIG. In 2015 he co-founded WISE, the global security management community for e-infrastructures.

Abstract
In October 2016 SURFnet organised a two-day cybersecurity exercise under the name Ozon. 28 constituents participate in this exercise which had a challenging and realistic scenario for both technicians and board members. The exercise simulated a complicated, multi stage attack form a hacker group with strategic dilemmas for ICT management and board members.
In this paper we will discuss how we designed and prepared this exercise, we will discuss different kind of exercises and the benefits of each for an NREN and an university and we will present the outcome of the exercise in terms of recommendations for both the way you can organise crisis exercises and for improving your crisis organisation, processes and tooling. The exercise was an initiative of SURFcert who had a leading role in preparation and execution. Ozon was a very high appreciated exercise with a lot of lessons learned both for the art of doing crisis exercises and for all participating organisations. Ozon bridged gaps between tactical, strategic and operational levels and between constituents.

Paper
NRENs and her constituents are mostly well trained in handling security incidents. There are processes in place, technology for analysis and mitigation, expertise for handling frequently occurring incidents. A large scale cyber-attack cannot be treated as a security incident, it needs an other approach especially when multiple organisations are involved and when the impact and urgency need management attention. That is a crisis. There is no clear division

between large incidents and crises, mostly because you cannot predict the kind of situations you will encounter in future but you can prepare with plausible and realistic scenarios.

Ozon 2016 was a two day cybercrisis exercise. From conceptual idea to crisis took 8 months, partly because it was the first time we prepared for this kind of exercise, partly because of planning. For the exercise we developed a realistic scenario involving a hackergroup that had both sympathetic ideals and a criminal purpose. To make the exercise scenario realistic for participating organisations they had to develop their own “implementation” of the scenario, tuned to their own, specific exercise goals and tuned to their own situation. As the exercise was targeted at both technical levels and board levels we had to prepare plausible evidence of hacked systems and leaked information. This is where the customisation of the exercise scenario came in play.

When we advertised for participation we were overwhelmed with interest of our constituents. Participating was possible on different levels of intensity: “Gold” participation meant having your board involved, “Gold” and “Silver” meant setting up a customised scenario for you own organisation, “Bronze” meant an observing role and a capture-the-flag exercise. The interest was enormous; we have had to disappoint a lot of people when we reached our target of 30 participants. SURFnet also participated as a player with on own scenario on Gold level, and SURFcert participated in its own role. The latter proved a bit of a challenge as large part of the SURFcert team was involved with preparing and running the exercise and therefore only a small team was left for normal operations.

For preparation of the exercise we set up a project team, a program group and a steering committee. In the program team was a representative of all gold and silver players. They were tasked with setting up the localised scenario for their organisation and they were the exercise coordinator for their organisation during the exercise.

Technique
As part of the exercise several websites of the hacking group were build. These were externally hosted and mirrored at the sites of several locations using Raspberry Pi systems and virtual systems. The website and her mirrors exposed a growing number of “disclosed” documents containing sensitive data of students, patients, employees and research. For credibility we also operated several command-and-control servers and had students with “infected” laptops visit participating organisations for a capture-the-flag exercise.

8 months of preparation resulted in a realistic and instructive two day exercise with more than 200 participants from universities, science partners, hospitals and libraries. Ozon bridged gaps between tactical, strategic and operational levels and between constituents.

In this paper we will discuss the key success factors for setting up a large crisis exercise, the lessons learned for SURFnet and for her constituents, and the crisis-exercise-playbook we developed.