

„Planspiel“ – Scripted Exercise, June 2012

Report is a bit late, but.... Just another Cyber Exercise? Yes and No ☺

- The Background:

- Development of a National IT Security Strategy (ev. adopted Dec. 2012)
- Existing Exercises were seen as a tad limited, also in (political) visibility

- Goals:

- involve Public Administration and Industry, across industry sectors
- involve all parties all the way up the escalation tree (to EKC,SKKM)
- come up with a „credible“ attack/outage scenario (I borrowed from reality)
- create awareness for cross-sector inter-dependencies
- provide the logistics to observe, log, report and evaluate afterwards!
 - ~50 active players / 100+ exercise managers („gods“) / 100+ observers

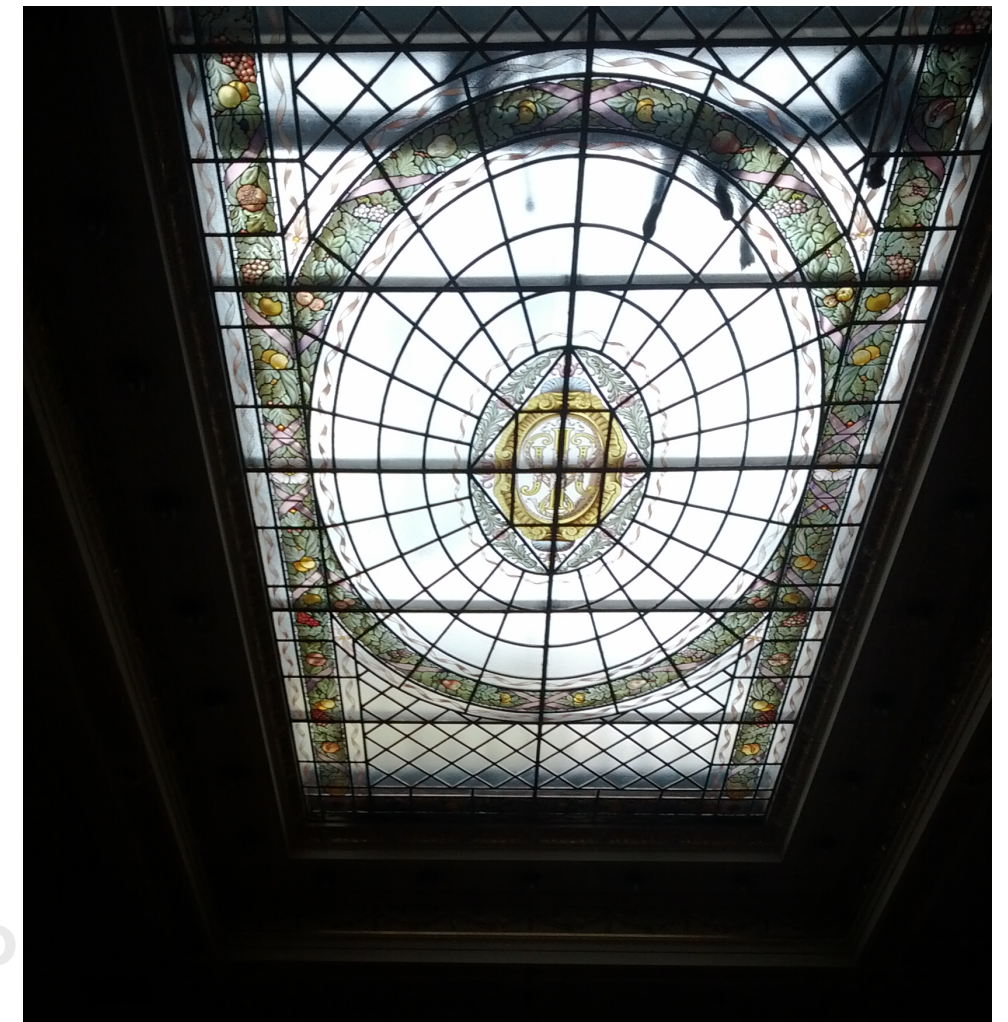
- Pre-existing escalation and management structure, but NOT (yet) for Cyber

- EKC: Einsatz- und Krisen-Koordinationscenter
- BMI – Ministry of the Interior

„Planspiel“ – Scripted Exercise, June 2012

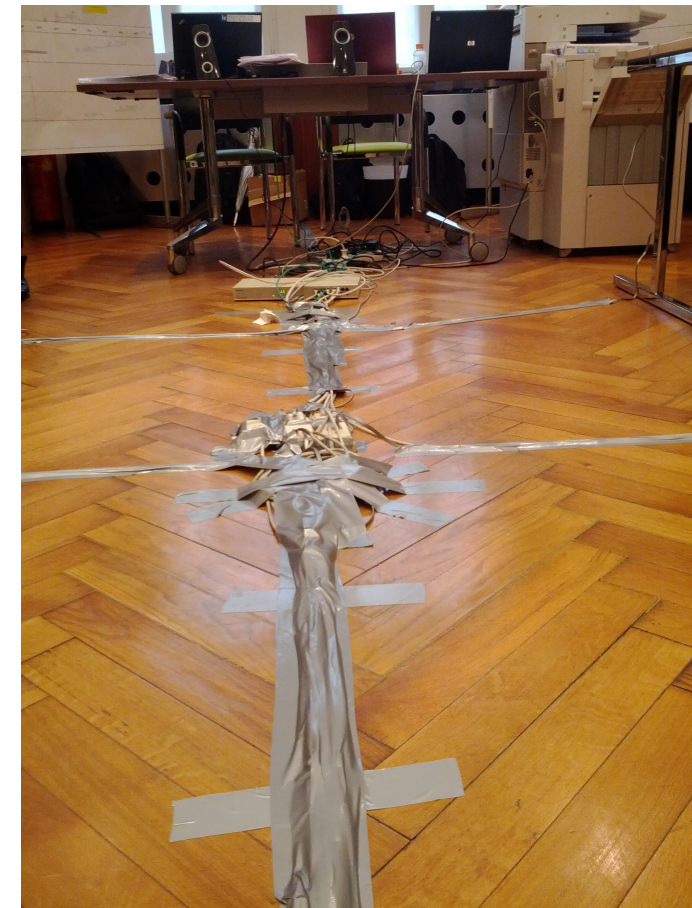
What and where? Everybody @
the Chamber of Commerce /
„Haus der Industrie“, in Vienna

← (Observers' Room)



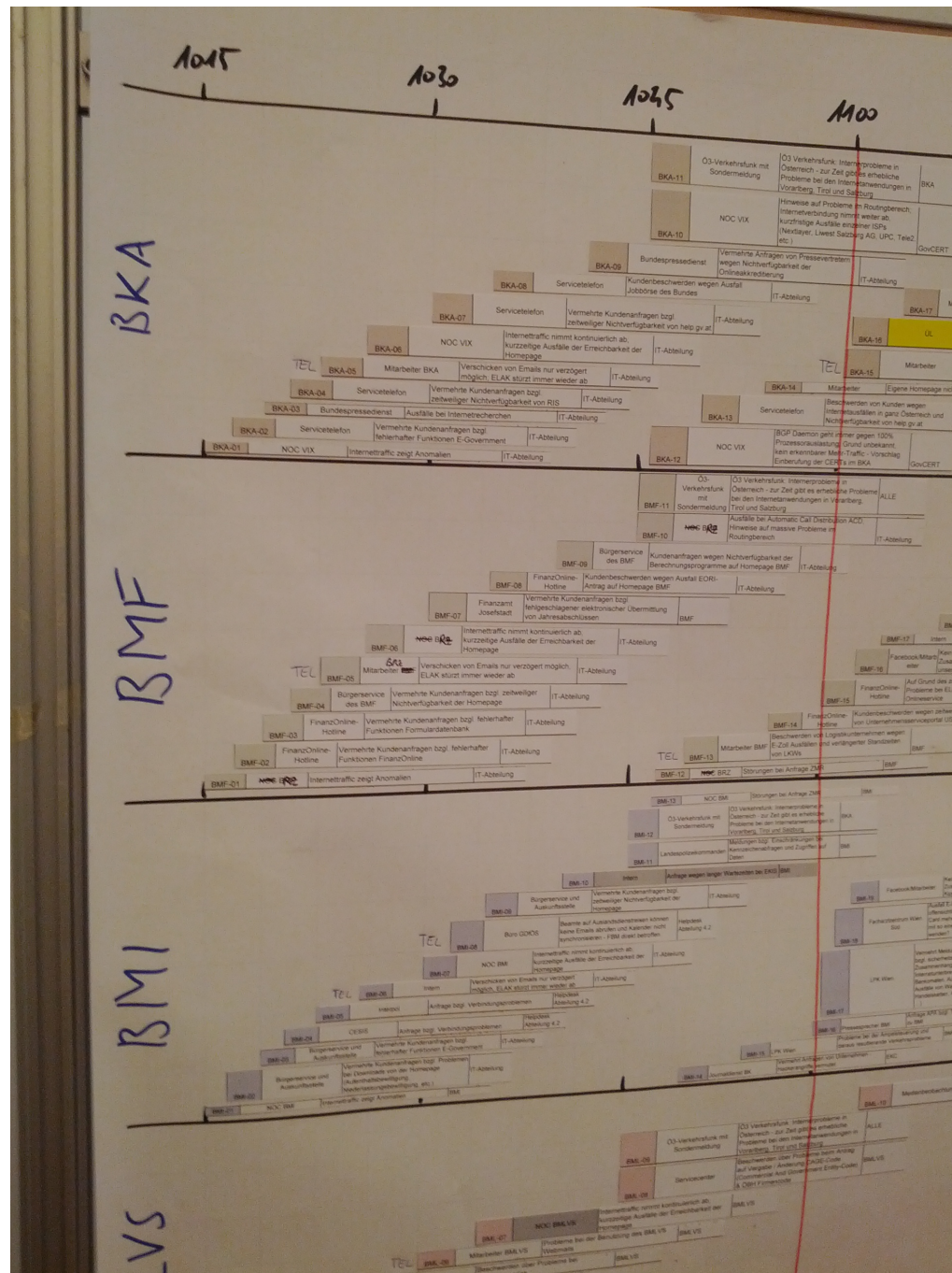
„Planspiel“ – Scripted Exercise, June 2012

- Players:
 - Public Administration (BKA, BMI/BVT/Toplevel Police, BMF, BMLVS, Federal State Admins, Federal IT-Service,...)
 - Financial Industry Rep.s (ÖNB, Geldservice Austria, RI Informatik)
 - Power Distribution (Wien Energie, e-Control, ...)
 - A1 Telekom, CERT.at
 - ...distributed across different rooms in building
- Experts (aka Gods):
 - Power Distribution (APG)
 - ISPs (ACOnet-CERT, UPC, A1Telekom)
 - Regional Health Services, Public Administration
 - Financial Industry, Telekom Regulator
 - IBM, Microsoft
 - Infraprotect (scripting engine and logistics)



„Planspiel“ – Scripted Exercise, June 2012

Incident „reality“ based on sophisticated scripts:



„Planspiel“ – Scripted Exercise, June 2012

- Interesting results (from my point of view!):
 - Possibility / Opportunity to (also) play against the own organisation at home
 - done by ACOnet, A1Telekom,...
 - Preparation needs much more time to involve „all relevant“ players on a national level
 - both for the player role and the „god“ role (and observation)
- Some lessons learned:
 - (not a surprise:) need for more human resources and split of responsibility
 - some organisations are well-prepared. others should start with internal exercises
 - internal communication and preparedness (helpdesk, management,...)
 - incompatibility of federal model for dealing with emergencies with the cyber environment
 - PR work at the end became a disaster^Wchallenge → integrate into scenario and better prepare for the real-world challenges at the end

„Planspiel“ – Scripted Exercise, June 2012

- Some lessons learned (cont.):
 - mutual trust is a fundamental requirement
 - try to define, agree and document structures / responsibilities / interfaces
 - exchange of information across „sectors“ is vital
 - health services sector is important, but was missing → next time ☺
 - while the lack of legal provisions sometimes helps in being „creative“,
 - the existing (future) legal framework must provide possibilities to share information and protect the „players“
 - and
 - management of human resources is vital!
- Next steps:
 - repeat the exercise
 - research project SCUDO
 - follow-up on national ICT-Security Strategy and Cyber-Security Strategy

<http://www.kuratorium-sicheres-oesterreich.at/login/cyberplanspiel-2012/>

Questions?

