

## SCUDO – a research project

### Topics:

- The goal
- Those involved
- Where are we now?
- Next steps
- Lessons learned
- Anyone doing similar things?

## The goal (and some background)

Some background...

- in a small country, the „Security Croud“ is a pretty small bunch of people ☺
- quite a few activities have been going on since 2011, but mostly 2012
  - the „Planspiel“ in June 2012
  - the National IT Security Strategy
  - the National Cyber Security Strategy
- Ideas and results – some in parallel:
  - provide a toolset for interested organisations to adapt, plan and run exercises – alone, within a group and on a large scale
  - help an initial set of organisations to set up their exercises, and
  - learn by doing so, and improve the material, processes (and doc.)
  - establish and improve the communication between actors in AT
  - have legal expertise in the project

## The consortium and the formalities

The consortium is a quite diverse group:

- a big company with varied security background (leader of the consortium)
- a company specialising in exercises, BCM advice, and then some
- entities of Public Administration in AT and a business consulting firm
- a local security research spin-off from Technical University Vienna
- the national ccTLD administration
- the National CERT / GovCERT.at
- Department of Law of Vienna University
- „us“, Vienna University „Computer Center“
  - 1 member from the DNS operations group,
  - 1 from the NREN and VIX (and GovIX)
  - myself
- funded by KIRAS
- started in September 2012, to conclude in February 2015

## snapshot... (1)

We want to enable organisations to perform exercises and to learn from them:

- table-top, but may be extended
- a set of guidelines, mix-and-match components, and tools for follow-up
- highly adaptable and configurable (a „backpack“ of tools and guidelines)
- definition of roles, preparation of „play“, de-briefing and „KPIs“

Focus on processes and communication, rather than on „hacking“, try to make things comparable and re-usable → some simplification and abstraction:

- 3 classes of typical problem scenarios: DNS, Certificates, Network Equipment

Focus on staged approach

- applicable for a single organisation
- for a group within an industry sector (or public administration)
- for a „bigger“ group of diverse organisations, physically not in one place

## snapshot... (2)

Already played all 3 „games“ internally (eat your own dog-food ☺)  
and with some individual organisations –

- insurance company, financial services, public administration
- a group of health services providers

Next round is coming up before summer and early autumn

The „big play“ is scheduled for mid-January 2015,  
interested parties already lining up (and being lined up)

Currently we are improving the material for the 3 scenarios,  
based on the feedback and observation of exercises

## Lessons learned (so far)

Some initial assumptions were wrong,  
i.e. that most organisations would have an emergency procedure.  
So the exercise may be seen as an incentive to devise such a procedure,  
instead of to check it 😊

The players tend to focus on technical aspects of the problem, instead of thinking about communication (internally and externally), (early) escalation and PR.

The legal aspects of incident handling needs more attention  
and maybe changes in the legal framework, too! (→Cyber Sec. Strategy)

Different types of organisations live in different types of management structures, various environments of out-sourcing, and contractual / competitive legal land(s)

This still needs a bit more attention and some improvements to the tools in the backpack

The world moves on while you wait for the grant, but you are bound... 😞

## Turning the table, and questions?

So, here comes my question:

Has anyone of you been involved in a similar project  
or happens to know about similar results or pointers?

<insert your questions here>

The project is supported by the Security Research Program KIRAS:

<http://www.kiras.at/gefoerderte-projekte/detail/projekt/scudo/> (german)

Homepage (work in progress!)

<http://scudo.infraprotect.at/>



# Questions?

