Comparing Mental Models on Cyber Security

Janosch Maier

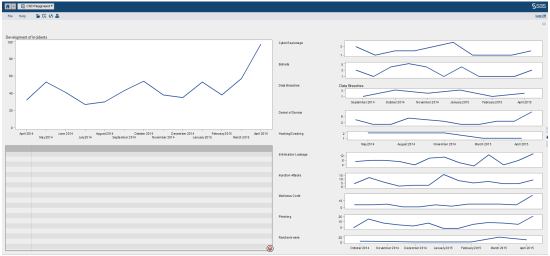
Technische Universität München

maierj@in.tum.de

Cooperation with Hogeschool Rotterdam & Wetenschappelijk Onderzoek- en Documentatiecentrum

28. December 2015

Goal: Cyber Security Dashboard

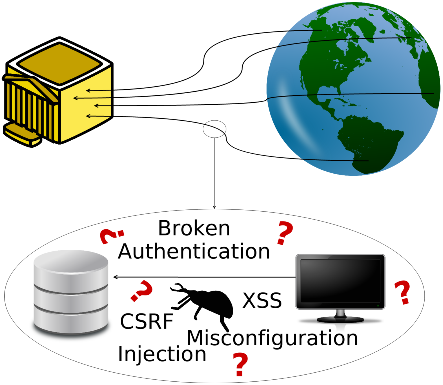


Cyber Security Dasboard as Tool e.g. for National CERTs

- Problem: What should be visualized in such a dashboard?

Mental Model on Cyber Security

- What do potential users think about cyber security?
- Interview with 7 experts from Dutch Governmental Institutions
- Potential users are from: Operation, Analysis, Management



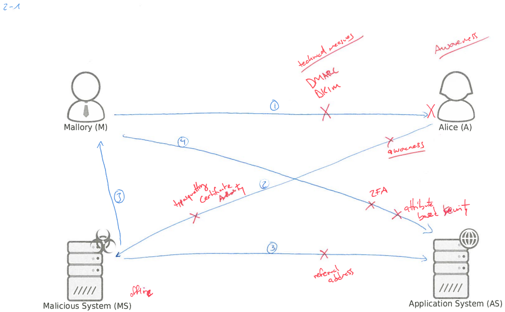
Exercise

“Alice Works for a Bank. She regularly accesses data from the application system via the internet. Mallory does not like the bank. How can he steal data from the application system?”

Mallory (M)
Alice (A)
Malicious System (MS)
Application System (AS)

Analyst

P: Mallory send an e-mail to Alice. This e-mail looks identical to the one from the bank. [...] And it says: [...], your account has been attacked, [...] we have taken measures to secure it, but you need to login and make sure, everything is secure. [...] When she clicks on the link, she doesn't go to the bank, she actually goes his, Mallory's malicious system, which looks identical to bank. [...] as she fills in her password and username [...] [t]he password and username is send back to Mallory.

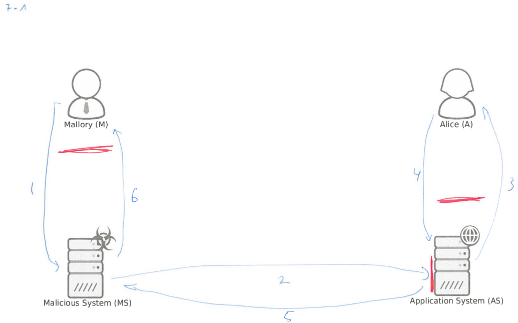


Manager

P: Mallory would give some input for the malicious system to start the attack. Then the system would try to hack or break into the application system. Of course, disguised. So Alice sees something, but does not realize, that it's malicious attack, or it's a malicious question or a malicious query. She then gives some input to the application system to send out information which would get back to the malicious system [...].

I: [...] What kind of attack could this be?

P: For instance a DDOS attack. Or?



Results & Perspective

Management people are less able to describe cyber attacks and countermeasures:

- Mixing the order of steps
- Less fluent with the language
- Missing important details

⇒ More superficial mental models

⇒ Next step: Use this knowledge to design a meaningful Cyber Security Dashboard (probably for operational & analytical people).