Security workshop ISGC 2023

Sven GABRIEL, Nikhef, EGI CSIRT
Introduction to the Security Workshop ISGC-2023
Agenda

- Risk Management
- Security Service Challenge
- Forensics exercise (Remote)
- Threat Intelligence and Security Operations Centers
Risk Management
Subsection 1

Introduction to the introduction
Security Teams, ... a look back

196x: ARPANET
1984: creation of global DNS
1988: Morris Worm led to creation of CERT et al.
1996: Aleph1
2000: "Smashing the Stack for Fun and Profit"
2000: Burst of Dot-Com Bubble
2001: TF-CSIRT started & Budapest Convention signed
2003: World Summit on the Information Society
2005: IGF
2007: Cyber attack on Estonia
2010: Stuxnet
2011: Dighotar
2015: GFCE
2017: 1st IoT botnets

Timeline courtesy FIRST
Communications in Operational Security

Communications on security related matters require trust between the communication endpoints. Trust is in organizations and in peers (individuals)

- Trust groups
  - Higher base trust.
  - Fragile, maintenance depends on individuals.
  - Limited in growth.

- Organisations, Network of CERTs/CSIRTs
  - Lower base trust, communicating to groups you do not personally know.
  - Endpoint description in official templates (RFC-2350)
  - (Checked) Canonical contact addresses like abuse@, security@, postmaster@, rfc2142
  - Maintained contact information available in directories (TF-CSIRT Trusted Introducer (TI) Directory)
Emergency Numbers, a short history

Until 1973 no standardized emergency phone numbers existed.

- Response times unnecessarily slow.
- Deadly traffic accident of a 8 year old kid in 1969 triggered an initiative to standardise it.
- Instead of checking a phone book to find the local emergency number, just call 112.

Since Feb. 1991 the same emergency number 112 is in place in all EU member states, EFTA, . . .
You usually don’t call a colleague and ask for an introduction to one of the local firefighters, you call 112.
Emergency contacts, use the system

Translated to the situation in IT emergency response . . .

- Use the standard contact addresses.
- If they do not meet the standards wrt response times, confidentiality, report it to coordinating bodies (TF-CSIRT, FIRST, NREN-CERTs).
- . . . as you would in case that calling 112 does not lead to the expected result.
Subsection 2

Introduction
Motivation

- Decision making process
  - Reflecting systems, conscious/controlled.
  - Automatic system/gut feeling, interpretations, auto correction.
- Decision making and Information Security Projects
  - Information systems are complex, to get to quick results often "gut feeling" approaches, "drive-by risk assessment" is used.
  - Doing incident response activates the "reflecting system". (Oh look, this log file entry looks interesting . . .).
  - Implementing a Risk management system requires you to reflect on your security posture.
When doing incident response, you usually ask:

- Why could this incident happen? (Status of your security controls).
- Why wasn’t it detected? (Status of your sensors)
- How can we prevent the same incident from happening again?
Introduction

Risk and Vulnerability Management is a wide area. We will only have a generic view on Risk Management and some hints why this would be very helpful for the organisations Operational Security team. As for vulnerability management we will take a look on how its done in EGI. A much more complete online training on Vulnerability Management is available at GÉANT: https://learning.geant.org/
domain-name-system-dns-protection-operational-network-
Subsection 3

Towards Risk Management
Definitions of Risk in context of Risk management:

- Old: chance or probability of loss (assets)
- New: effect of uncertainty on (reaching the) objectives (of an organisation) (ISO 31k).

Risk Management is management of an organisation while taking into account the risks.
Towards Risk management Processes
ad-hoc IS management, questions

- What was the impact? were you just lucky that not more happened? or . . .
- Do you really know your assets?
- Do you really know the risks to your assets?
- Did you know the affected entities in your organisation?
- Could you do proper communications related to the incident?
- If these left a nagging feeling with you, continue . . .
Risk management Process

- Context, answer to questions:
  - Scope, boundaries of the assessment
  - Roles and Responsibilities
  - Basis criteria

- Risk Identification
  - List of Assets (primary (processes) and their supporting secondary (hard/software, network, personal, etc) assets)
  - Risks to the (primary assets), Risks are the uncertainties achieving the goals of the organisation.
  - Threat Root cause for an unwanted event with negative impact
  - Vulnerability: A threat uses a vulnerability to create the unwanted event.

- Risk Analysis

- Risk Evaluation/Prioritisation
  - Modification
  - Risk Retention
  - Risk Avoidance
  - Risk sharing (old; transfer)
  - Residual Risk/Risk acceptance
  - Risk Communication and Consulting
  - Risk Monitoring
Risk management Process

Risk Monitoring

- Risk Assessment
  - Risk Identification
  - Risk Analysis
  - Risk Evaluation/Prioritization

- Context, Scope of the RM

- Risk Communication/Consulting

YES

- RA OK? (depth, completeness, accuracy)

NO

- Risk Treatment
  - Risk treatment OK, accepted?
    - Yes
      - Risk acceptance

2 S. Klipper, Information Security Risk Management
Risk, Threats and all the rest

When entering the Risk Assessment, one needs to identify risks. Threats are a component of Risks, therefore ...
Oh Dear, a lot input needed

To implement a Risk Management Process a lot of information is needed, good thing ISO 2700{1,2,5} and 31010 can help.

- 27005 Information Security Risk Management (Annex on Threats, Vulnerabilities.)
- ENISA ThreatLandscape
- SANS YYYY Top New Attacks and Threat Report (also Controls)
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Monitoring of the Risk Management Process requires current input on threats and security controls.
Risk, Threats and all the rest

- STRIDE: A model of what can go wrong:
- Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege.
- Is used in threat modelling, see Adam Shostack’s book Threat Modeling: Designing for Security
  https://shostack.org or
  https://www.youtube.com/watch?v=DMFF8zQqEVQ
Elevation of privilege, threat modelling card game for developers.

Not prepared yet, please come back later this year . . .
https://attack.mitre.org/ MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. From here you get information on:

- Which APT group is focusing on your sector?
- What is their motivation?
- What are the typical attacks, tools (threats) they use to exploit the resp. vulnerabilities.
Threat Modelling with MITRE ATT&CK

- Pick an organisation,
- Set up context,
- Find Threats to this organisation's Assets.
- Threat modeling in security operations

A first version in the Hands-On, please come back next year for a more complete version . . .
Why Risk management?

Leverage the outcome of a Risk Assessment, examples
Incident Response for High impact incident

- To get started, ... let's look at the debriefing of a successful ransom attack and the problems you may run into, like:
  - How to prioritize what systems to bring back first. (Business Continuity Plan)
  - What is lost? GDPR relevant data loses need to be reported to the authorities.
  - Do useable back-ups of important (for business continuity) datasets exist?
  - Note, at this stage it's not about what security controls failed.
  - Risk analysis helps to know your assets and protective measures in place.
Subsection 4

Preparation for Risk Analysis
What is Risk Analysis?

Risk Analysis is a process. An objective analysis of the effectiveness of the current security controls that protect an organization’s assets and a determination of the probability of losses to those assets. When doing it for an organisation, this is rather a project with involvement of senior management and other key-personal. At the end of this project the Risk Management Process should be started.

---

Phases/Steps in Risk Analysis

There are multiple methods and frameworks available for Risk Management. Remember, this is a project which requires the usual project management (with senior management contribution/support). The methods differ in details/organisation of the following phases. Which method to use is also subject to the goal of the Risk assessment (Compliance with security regulations, ISO-27K, NIST-800, etc)

Info Gathering Phase

Large parts of the info gathering is already done in the project planning part. Information Gathering, Identify:

- Assets, Primary Assets (Business Processes), Secondary Assets (Hardware, Software, Personal/Experts, Data Sets/Bases) supporting the primary Assets, are used in the processes.
- Threats, use OSINT, see also the hands-on ⁵.
- identify Critical systems (ex. systems that automate critical business functions)

---

Get Info on available Controls

- Administrative (policies, procedures)
- Technical (Design, Architecture, Configuration, AuthNZ)
- Physical (physical access control, CCTV etc)
Subsection 5

Risk Analysis
Risk Analysis

Bringing together the gathered data/information.

- Asset valuation, example: Low (little to no impact), Medium, High, Critical (Indicates that compromise of the asset would have grave consequences). Various valuation approaches.
- Threat and Vulnerability mapping,
- Risk Calculation. (Here the above information is used to get a qualitative (low, moderate, high) or quantitative value)
- Risk Mitigation: Safeguard selection, Safeguard effectiveness(cost-value ratio)
Risk mitigation

- Safeguard/Control selection
- Safeguard/Control effectiveness (cost-value ratio)
- Risk reduction (improve existing controls, apply additional controls)
- Result: Residual security risk (that remains after implementation of recommended safeguards). This will be treated in the next step.
Senior manager must decide to reduce the security risk, accept the residual security risk, or delegate the security risk to someone else (example: insurance).

- Risk transfer.
- Risk acceptance.
- Risk assignment.
Finally

The Risk assessment report will help the Operational Security team to prioritize the available resources to:

- Security Monitoring (ex. access control)
- System audits, log processing, alerting
- Back-up Strategy
Threat Modelling with MITRE ATT&CK
Subsection 1

MITREATT&CK
https://mitre-attack.github.io/attack-navigator/
MITRE ATT&CK Matrices capture the relationship between:

- **Tactics** (Column headers), Represent (intermediate) goals of an adversary, for example lateral movement.
- **Techniques** (Column entries)
  - are the means/tools how the adversary achieve their goals/tactics
  - are written/used by the adversaries, entries describe and capture how an adversary performs each action or behaviour.
- **Subtechniques** describe adversary behaviour at a lower level then the resp. technique.
- are often platform specific, Example: Technique = Command + Scripting Interpreter, the Subtechniques are: Powershell . . . Windows; Unix shell . . . Unix; python, Javascript . . . Cross platform.
TTPs of ATT&CK

https://www.youtube.com/watch?v=1cCt2XZr2ms
https://apt.etda.or.th/cgi-bin/listtools.cgi
https://apt.etda.or.th/cgi-bin/listtools.cgi

Database search

Actor
- Source country: ...
- Victim country: Netherlands
- Victim sector: Education
- Motivation: ...
- Free text search: (can use '*' and '?' wildcards)
  Search!

Tool
- Category: ...
- Type: ...
- Free text search: (can use '*' and '?' wildcards)
  Search!
## OSINT

https://apt.etda.or.th/cgi-bin/listgroups.cgi?c= &v=Netherlands&s=Education&m=&x=

<table>
<thead>
<tr>
<th>Name</th>
<th>Country</th>
<th>Observed</th>
</tr>
</thead>
<tbody>
<tr>
<td>APT 17, Deputy Dog, Elderwood, Sneaky Panda</td>
<td>🇨🇳</td>
<td>2009-Sep 2017</td>
</tr>
<tr>
<td>APT 29, Cory Bear, The Dukes</td>
<td>🇨🇳</td>
<td>2006-Oct 2022</td>
</tr>
<tr>
<td>APT 41</td>
<td>🇨🇳</td>
<td>2012-Aug 2022</td>
</tr>
<tr>
<td>Circus Spider</td>
<td>[Unknown]</td>
<td>2019-Feb 2022</td>
</tr>
<tr>
<td>Cutting Kitten, TG-2839</td>
<td>🇩🇪</td>
<td>2012-Mar 2016</td>
</tr>
<tr>
<td>Dark Caracal</td>
<td>🇩🇪</td>
<td>2007-2020</td>
</tr>
<tr>
<td>FIN11</td>
<td>[Unknown]</td>
<td>2016-Dec 2022 🌡</td>
</tr>
<tr>
<td>MuddyWater, Seedworm, TEMP.Zagros, Static Kitten</td>
<td>🇩🇪</td>
<td>2017-Late 2021</td>
</tr>
<tr>
<td>Shadow Network</td>
<td>🇨🇳</td>
<td>2016-2010</td>
</tr>
<tr>
<td>Solacy, APT 28, Fancy Bear, Soonti</td>
<td>🇨🇳</td>
<td>2004-Sep 2022</td>
</tr>
<tr>
<td>TeamSpy Crew</td>
<td>🇨🇳</td>
<td>2010-Feb 2017</td>
</tr>
<tr>
<td>Turla, Waterbug, Venomous Bear</td>
<td>🇨🇳</td>
<td>1996-Sep 2022</td>
</tr>
</tbody>
</table>

### Other groups

<table>
<thead>
<tr>
<th>Name</th>
<th>Country</th>
<th>Observed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fxmsp</td>
<td>🇨🇳</td>
<td>2016-Jul 2020</td>
</tr>
</tbody>
</table>
Use the APT group information from the previous step in MITRE ATT&CK . . .
MITRE ATT&CK® Navigator

The ATT&CK Navigator is a web-based tool for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more.

Create New Layer
Create a new empty layer

Enterprise
Mobile
ICS

More Options

Open Existing Layer
Load a layer from your computer or a URL

Create Layer from other layers
Choose layers to inherit properties from

Create Customized Navigator
Create a hyperlink to a customized ATT&CK Navigator
### MITRE ATT&CK, New Layer

<table>
<thead>
<tr>
<th>Layer 1</th>
<th>Layer 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reconnaissance 10 techniques</td>
<td>Resource Development 7 techniques</td>
</tr>
<tr>
<td>Initial Access 7 techniques</td>
<td>Execution 13 techniques</td>
</tr>
<tr>
<td>Persistence 19 techniques</td>
<td>Privilege Escalation 13 techniques</td>
</tr>
<tr>
<td>Defense Evasion 42 techniques</td>
<td>Credential Access 17 techniques</td>
</tr>
</tbody>
</table>

- **Active Scanning**
  - Acquire Infrastructure
  - Gather Victim Host Information
  - Gather Victim Identity Information

- **Resource Development**
  - Compromise Accounts
  - Acquire Infrastructure
  - Compromise Accounts
  - Compromise Infrastructure

- **Initial Access**
  - Drive-by Compromise
  - Exploit Public-Facing Application
  - External Remote Services

- **Execution**
  - Command and Scripting Interpreter
  - Container Administration Command
  - Deploy Container

- **Persistence**
  - Account Manipulation
  - BITS Jobs
  - Boot or Logon Autostart Execution

- **Privilege Escalation**
  - Access Token Manipulation
  - Boot or Logon Autostart Execution

- **Defense Evasion**
  - Build Image on Host
  - Debugger Evasion
  - Deobfuscator/Decode Files or Information

- **Credential Access**
  - Adversary-In-The-Middle
  - Brute Force
  - Credentials from Password Stores

### Techniques (594)

- **Abuse Elevation Control Mechanism**
- **Abuse Elevation Control Mechanism**: Bypass User Account
- **Abuse Elevation Control Mechanism**: Elevated Execution

---

Security workshop ISGC 2023
MITRE ATT&CK, New Layer

Security workshop ISGC 2023
MITRE ATT&CK, New Layer
MITRE ATT&CK, New Layer

Security workshop ISGC 2023
Add a score value, for example 1 for all layers for equal weight in the overlay.
<table>
<thead>
<tr>
<th>Create New Layer</th>
<th>Create a new empty layer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open Existing Layer</td>
<td>Load a layer from your computer or a URL</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Create Layer from other layers</th>
<th>Choose layers to inherit properties from</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain</td>
<td>Choose the domain and version for the new layer. Only layers of the same domain and version can be merged.</td>
</tr>
<tr>
<td>Enterprise ATT&amp;CK v12</td>
<td>Use constants (numbers) and layer variables (yellow, above) to write an expression for the initial value of scores in the new layer. A full list of supported operations can be found here. Leave blank to initialize scores to 0. Here’s a list of available layer variables:</td>
</tr>
<tr>
<td>score expression</td>
<td>$a + b$</td>
</tr>
<tr>
<td>$a$ (layer)</td>
<td>$b$ (layer1)</td>
</tr>
<tr>
<td>$c$ (layer)</td>
<td>$d$ (layer by operation)</td>
</tr>
</tbody>
</table>
Subsection 2

What to do with MITRE ATT&CK
Use MITRE ATT&CK, for...

- Threat modelling with MITRE ATT&CK is certainly not complete.
- It depends on your (time consuming) OSINT, to get the groups that could possibly be interested in your assets.
- Still it will give you a pretty good start on . . .
Use MITRE ATT&CK, for...

- Data Sources (do you have the logs for the threats identified).
- Detection/analysis (sensors, where to place them)
- Mitigation (security controls)

As a result you get a good indication of your security posture against the groups, techniques in scope. Map it against your SOC settings/capabilities.
Thanks for your attention, Questions?