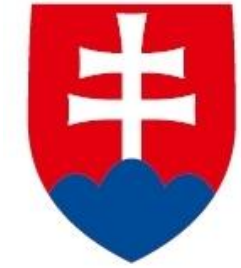


Under the Radar

(The Unheard Song
of Missed Incidents)

Rastislav Janota

SK NBÚ CERT

We usually identify

- Vulnerabilities and threats
  - CVE, security and news feeds, twitter accounts, intelligence reports
- Vulnerable assets, list of assets for future reference
  - Using scanning tools to identify assets and threats
  - By matching vulnerabilities to assets provided by constituency
- Events and incidents
  - By our own sensor network (IPS, WAF, anti-virus, firewall, log analysis)
  - From incident reports by constituency

Vulns from feeds

- Many feeds readily available, the best understood source of quality information, but still...
  - Do we have the right feeds, or do we miss something important?
  - Do all the feeds really work?
  - What about zero days?

Vulns by scanning ???

- Scanning cycle too slow
- Scanning too shallow (mostly public IP addresses)
- Do we have enough tools? New tool for each new threat type needed
- Are we even permitted to scan?

Volunteered assets ?!?

- How to obtain the information on assets from our constituency?
  - Legal trouble
  - Unwillingness
  - No data available (no procedures, technical incompetence)
- And what about consequent maintenance of such information?

Events from sensors

- Data lost in noise on public IPs
  - Malware and spam, search engines, previous users of your IP address, live attackers AND white-hat security researchers, honest mistakes and typos, DoS
  - Impossible to give attention to all events; DoS special case
- Missing sensors inside the LAN and DMZ => no APT visibility
- No sensors, wrong sensors, encryption?
- Permission to collect data? Maintenance and security?

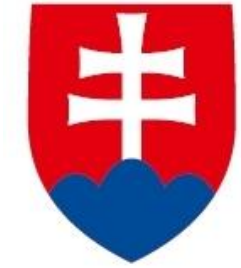
Reports from const. ?!?!?

- Is our constituency capable of accurate and timely reporting?
  - And are they skilled enough not to destroy evidence during attempted incident response?
- Is our constituency willing to report?
- Are there any other obstacles on both sides (working hours, legal issues, different mind set or priorities)?

Discussion

- So what blind spots do we really have? (incl. unknown unknowns)
- What incidents and threats are we missing?
- What to do about it?

- What is role of CSIRT? National / sectorial / private (serving market) / private (serving own company-companies)
- Do National CSIRT need to have own visibility over nation?
- How to deal with trend to move CSIRT as close as possible to the customer?



THANK YOU

sk-cert@nbu.gov.sk