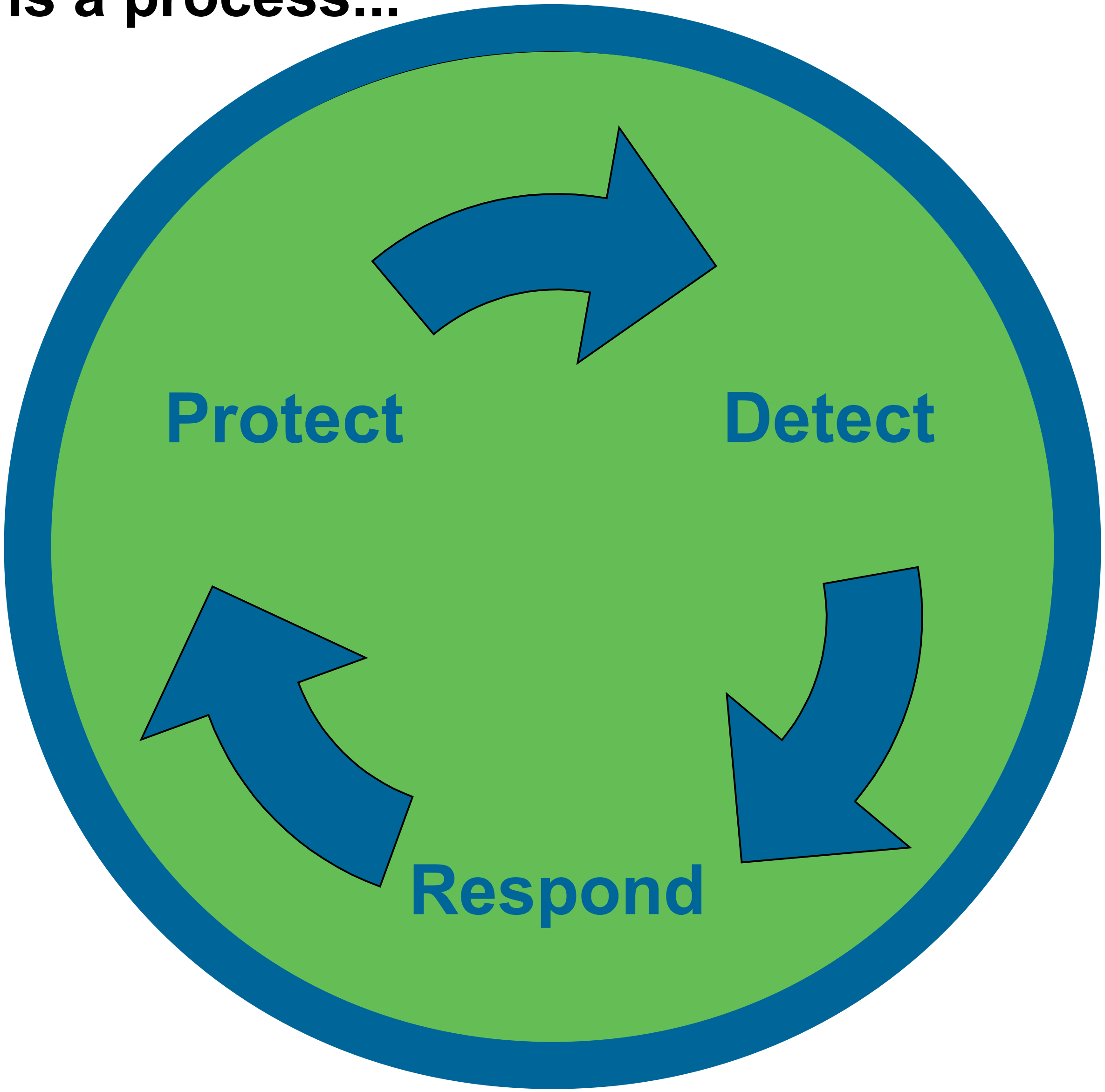
Security Incidents

Ursula Epting

STEINBUCH CENTRE FOR COMPUTING - SCC

Security is a process...



Security Incident – definition and terms

„Any real or suspected adverse event in relation to the security of computer systems or computer networks

-or

The act of violating an explicit or implied security policy“ [1]

- CSIRT – Computer Security Incident Response Team
- CERT – Computer Emergency Response Team

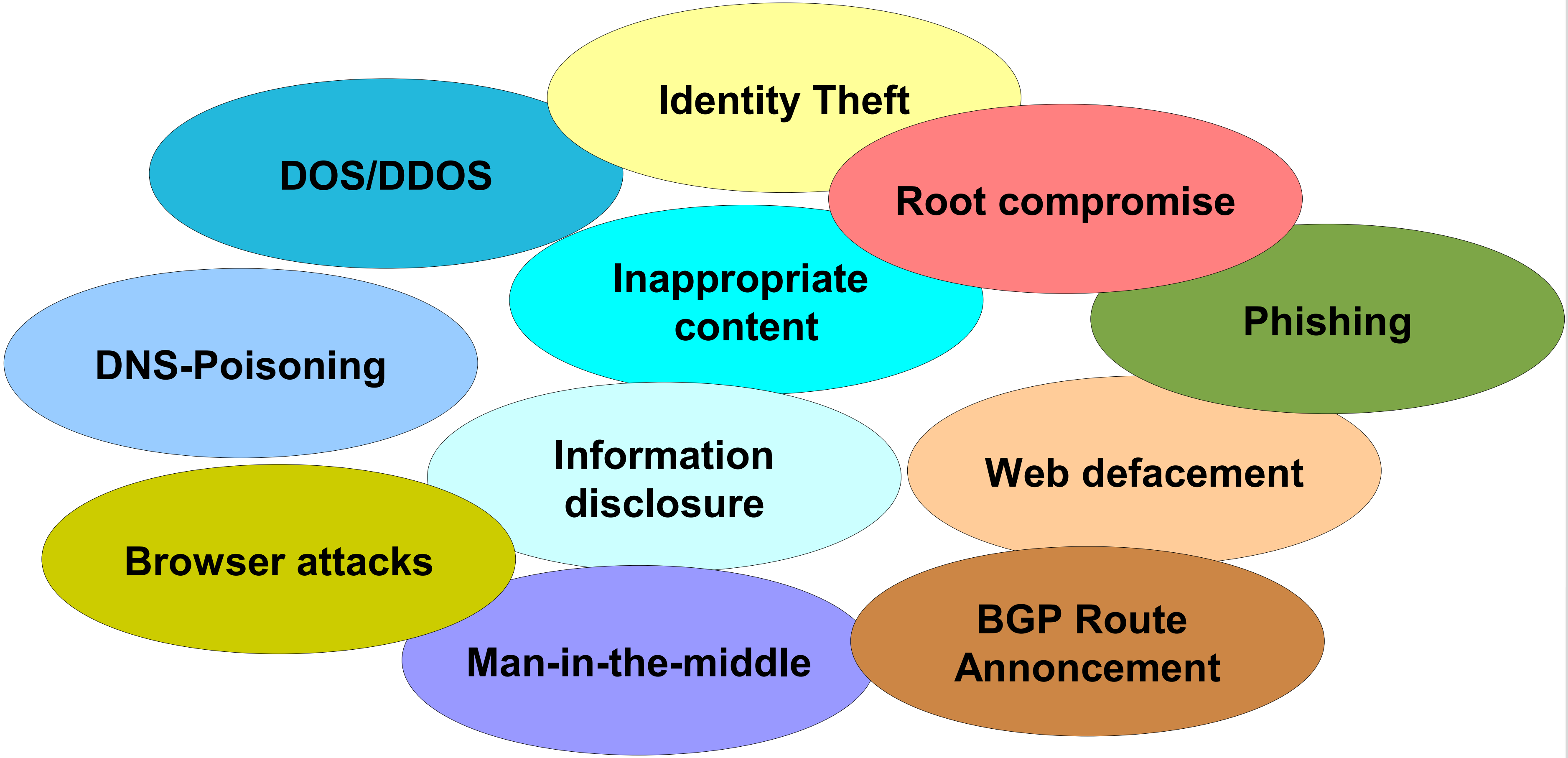
mean the same thing

Security Incidents

Which types do you know?

Security Incidents

Which types do you know?



Identity Theft

DOS/DDOS

Root compromise

Inappropriate content

Phishing

DNS-Poisoning

Information disclosure

Web defacement

Browser attacks

BGP Route Annoncement

Man-in-the-middle

What should I do?

Keep your wits -

Bewahre Köpfchen

Locally –

- Do you have a CERT at your site?
- Do you know your security officer?
- Do you know other security experts at your site?

Where can I get help?

Locally – contact your CERT, security officer or other security team/experts

---

Germany

DFN-CERT: dfncert@dfn-cert.de [2]

NGI-DE: NGI-DE-csirt@listserv.dfn.de

(includes DFN-CERT and KIT-CERT)

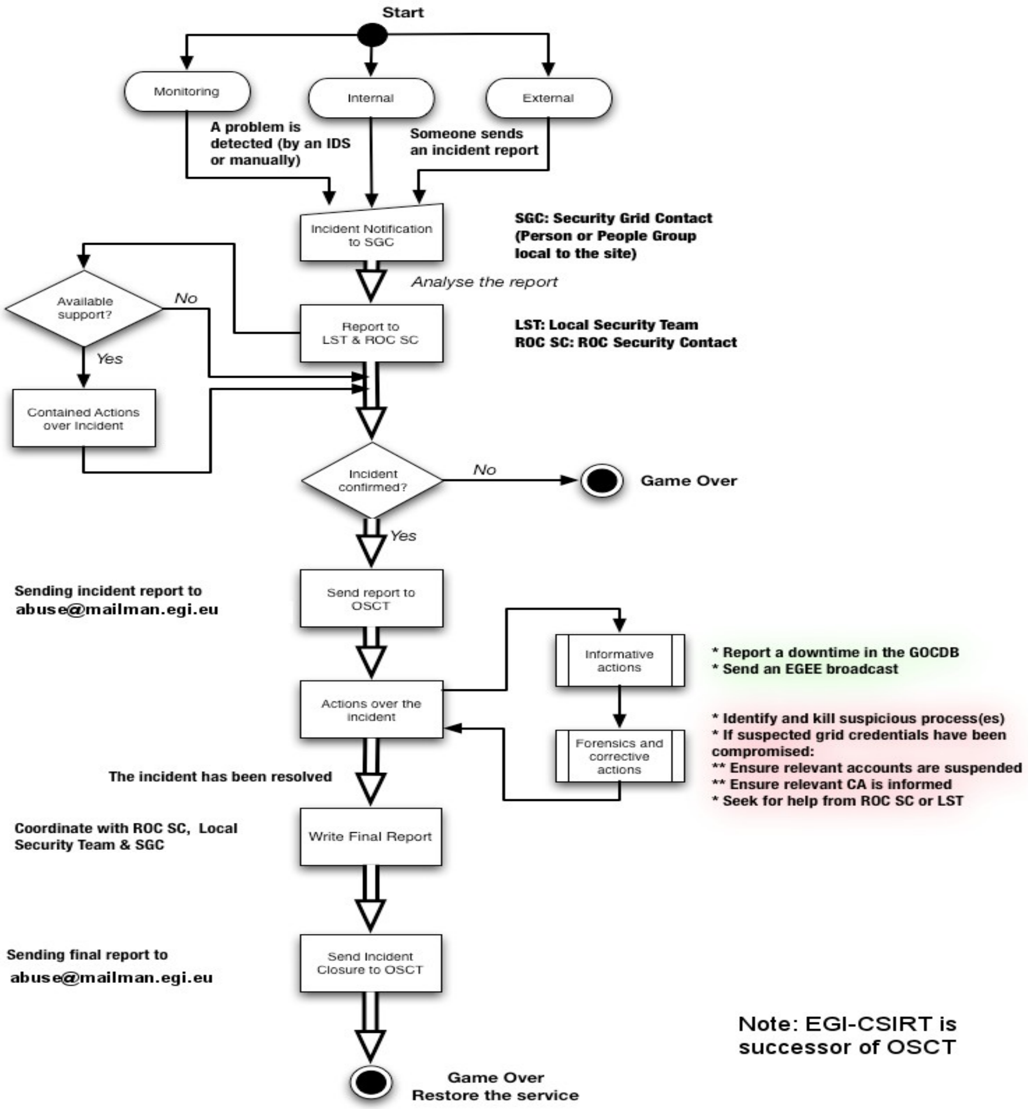
Other countries: many NREN's fulfill CERT-functions!

EGI-Inspire: egi-csirt-team@mailman.egi.eu [3]

Report security incidents to all EGI-sites via:

egi-csirt@mailman.egi.eu or abuse@egi.eu

IR Workflow - Example



Start

Monitoring

Internal

External

A problem is detected (by an IDS or manually)

Someone sends an incident report

Incident Notification to SGC

SGC: Security Grid Contact (Person or People Group local to the site)

Analyse the report

Available support?

No

Yes

Report to LST & ROC SC

LST: Local Security Team
ROC SC: ROC Security Contact

Contained Actions over Incident

Incident confirmed?

No

Game Over

Yes

Sending incident report to abuse@mailman.egi.eu

Send report to OSCT

Informative actions

- * Report a downtime in the GOCDB
- * Send an EGEE broadcast

Actions over the incident

Forensics and corrective actions

- * Identify and kill suspicious process(es)
- * If suspected grid credentials have been compromised:
- ** Ensure relevant accounts are suspended
- ** Ensure relevant CA is informed
- * Seek for help from ROC SC or LST

The incident has been resolved

Coordinate with ROC SC, Local Security Team & SGC

Write Final Report

Sending final report to abuse@mailman.egi.eu

Send Incident Closure to OSCT

Game Over
Restore the service

Note: EGI-CSIRT is successor of OSCT

- Good to have such workflow drafted at your site
- Write down all needed contact addresses/phone numbers etc.

[4]

Links/Sources

[1] http://www.cert.org/csirts/csirt_faq.html

[2] https://www.cert.dfn.de/

[3] https://wiki.egi.eu/wiki/EGI_CSIRT:Main_Page

[4] Workflow diagram: Carlos Fuentes Bermejo (RedIRIS/ Spain, EGI-CSIRT)