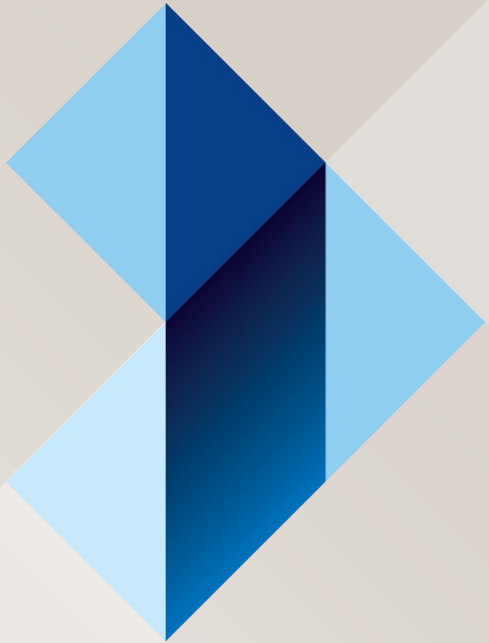
New requirements for incident handling

Rune Sydskjør – Uninett CERT

EUNIS June 6, 2019



UNINETT

Norway's Norsk Hydro lost $50 million in cyber attack

Norsk Hydro was targeted in a cyber attack. Photo: Bjoertvedt/Wikimedia Commons

A cyber attack that targeted Norwegian industry giant Norsk Hydro in March cost the company around $50 million.

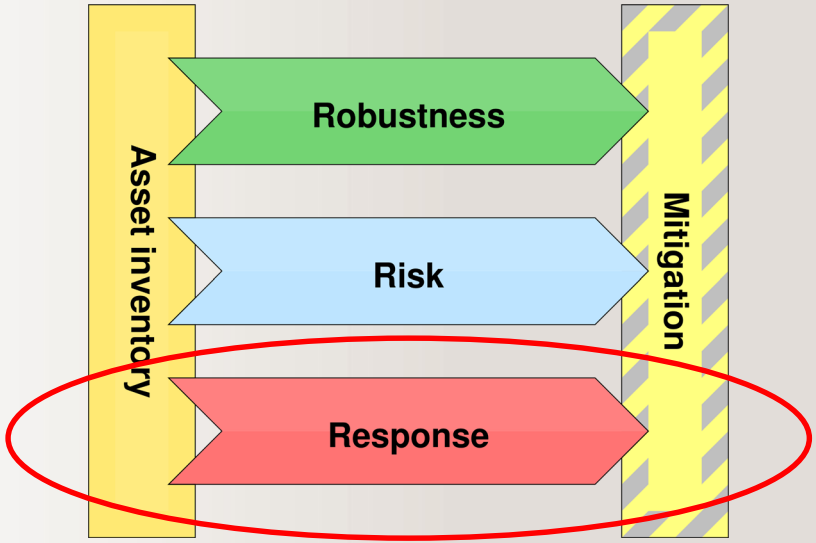
«New» requirements in the framework

- overview of the sectors critical infrastructure or systems that support critical functions.
- routines for sharing information on incidents and risks in sector
- contingency plan for larger incidents
- skillz on relevant systems and ability to consider the severity and consequences of the incident
- be able to decide if critical infrastructure in our sector is in danger or if its possible that it is going to be affected by the incident
- overview of the scope of the incident and see incidents in the same sector in context
- reporting to NSM/NorCERT (The norwegian national security authority)

«New» requirements in the framework

- overview of the sectors critical infrastructure or systems that support critical functions.
- routines for sharing information on incidents and risks in sector
- contingency plan for larger incidents
- skillz on relevant systems and ability to consider the severity and consequences of the incident
- be able to decide if critical infrastructure in our sector is in danger or if its possible that it is going to be affected by the incident
- overview of the scope of the incident and see incidents in the same sector in context
- reporting to NSM/NorCERT (The norwegian national security authority)

Why asset inventory is important?



CERT/IRT/CSIRT/SOC - Web of trust

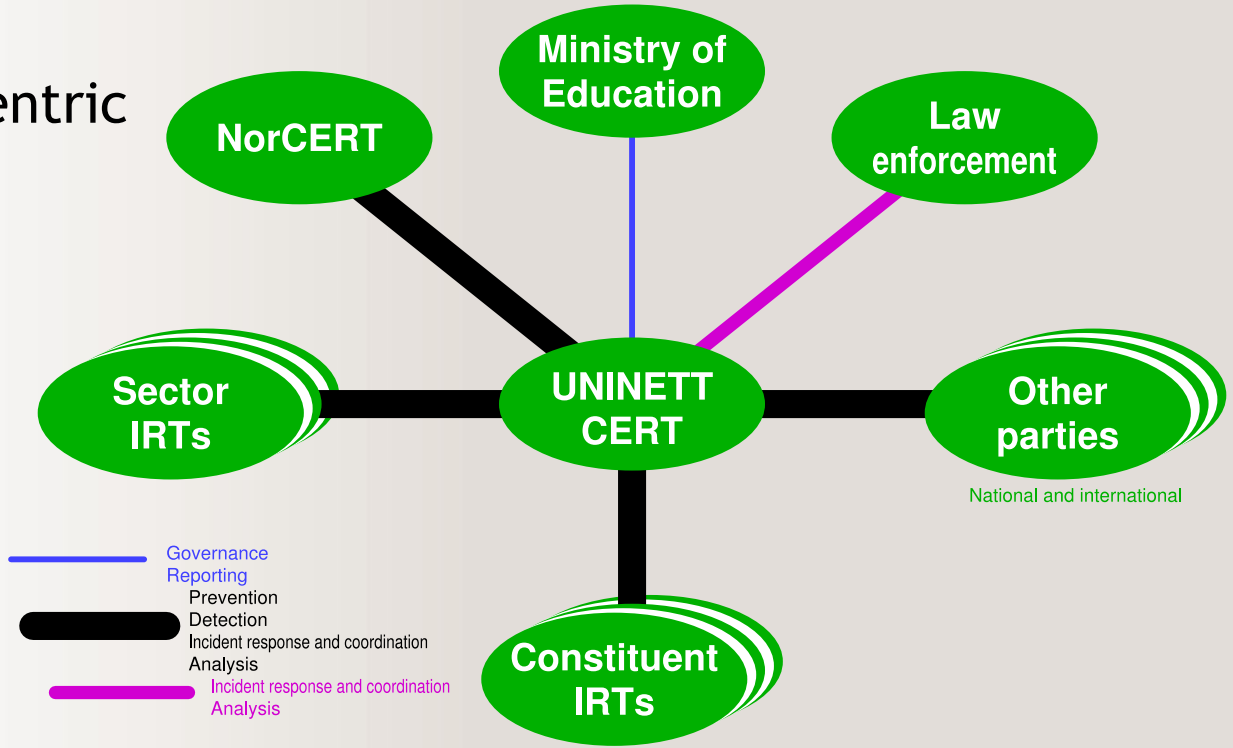
- Cyber security is a global problem. No one has the full overview and maybe not all the necessary capabilities.
- Trusted partners and safe communication is crucial.
- Close cooperation with other teams is necessary.
- Uninett CERT is a member of several national and international networks where we receive information, tools and methods which will benefit our sector.

TF-CSIRT Trusted Introducer

FIRST Improving Security Together

Communications map – National level

Uninett centric



UNINETT

TLP – Traffic light protocol

Color	When should it be used?	How may it be shared?
RED	Sources may use TLP: RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.
AMBER	Sources may use TLP: AMBER when information requires support to be effectively acted upon, but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP: AMBER information with members of their own organization who need to know, and only as widely as necessary to act on that information.
GREEN	Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.
WHITE	Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	TLP: WHITE information may be distributed without restriction, subject to copyright controls.

37 IRT's in our sector

Arkitektur- og designhøgskolen i Oslo (irt@aho.no)
Chr. Michelsen Institutt (irt@cmi.no)
Det teknologiske menighetsfakultet (irt@mf.no)
Fagskolen i Ålesund (fials_irt@fials.no)
Fagskolen Innlandet (irt@fagskolen-innlandet.no)
Handelshøyskolen BI (cert@bi.no)
Høgskolen i Innlandet (irt@inn.no)
Høgskolen i Molde (irt@himolde.no)
Høgskolen i Oslo og Akershus (csirt@hioa.no)
Høgskolen i Sørøst-Norge (usn-irt@usn.no)
Høgskulen i Volda (irt@hivolda.no)
Høgskolen i Østfold (irt@hiof.no)
Høgskulen på Vestlandet (csirt@hvl.no)
Kompetanse Norge (csirt@kompetansenorge.no)
Kunsthøgskolen i Oslo (irt@khio.no)
Nasjonalbiblioteket (irt@nb.no)
NMBU (csirt@nmbu.no)
Nord universitet (irt.nord@nord.no)
Norges forskningsråd (irt@rcn.no)
Norges Handelshøyskole (irt@nhh.no)
Norges idrettshøgskole (irt@nih.no)
Norges musikkhøgskole (hendelsesresponsteam@nmh.no)
Norsk institutt for luftforskning (csirt@nilu.no)
Norsk regnesentral (irt@nr.no)
NTNU (soc@ntnu.no)
Sámi allaskuvla (irt@samiskhs.no)
Uninett CERT (cert@uninett.no)
Uninett Sigma2 (csirt@sigma2.no)
UiT Norges arktiske universitet (csirt@uit.no)
UNIS (irt@unis.no)
Unit (irt@unit.no)
Universitetet i Agder (csirt@uia.no)
Universitetet i Oslo (cert@uio.no
Universitetet i Bergen (irt@uib.no)
Universitetet i Stavanger (irt@uis.no)
Utdanningsdirektoratet (irt@udir.no)

https://www.uninett.no/cert-team-list

Handle information - experience from incidents and exercises

Questions?

- Rune Sydskjør
- Team leader Uninett CERT
- rune.sydskjor@uninett.no

- cert@uninett.no
- cert-info@uninett.no