Title: Incident handling in the Norwegian academic sector
Name: Rune Sydskjør
Affiliation: Team Leader UNINETT CERT
Five keywords: Incident response, TLP, communication, cooperation
authors names (if different from the presenter)
author's affiliations
presenter's biography:
Rune Sydskjør has worked with incident response and security for UNINETT CERT for 16 years where the last 5 years has been as the team lead. UNINETT CERT is a part of UNINETTs network department, so Rune also has a background from network operations.

presentation description:
Our society has become more and more digitalized and dependent of IT infrastructure. The threats and threat actors are more and more sophisticated, and no individual is able to stand up against this on their own. Cooperation and sharing of threat information is a key success factor.

In Norway we have established a close cooperation between NorCERT (The Norwegian National Security Authority) and incident response teams representing a number of sectors, e.g. banking, energy, and education (UNINETT CERT). One of the most useful things we do is the sharing of information according to the TLP (1) protocol.

The lack of formalized cooperation with our customers has, however, hampered our ability to share this information further with our customers. In order to remedy this situation, UNINETT CERT organized two training workshops for incident response teams in 2017 and established formal relationships. We have now facilitated the establishment of incident response teams in all Government owned universities and university colleges in Norway (25 teams), as well as 9 teams for other customers. In this way we are now able to share sensitive and time critical information within our sector.

This talk will present how we cooperate in Norway. With the authorities, NorCERT, the other sectors and with our constituency. We will also present the preparations for both workshops, the importance of anchoring incident handling in top management, and how IR teams can be a vital part in global and nation-wide information security crisis management and other contents the workshops covered.

Following up on teams are important, particularly for newly established teams, both daily and by organizing events and gatherings. The presentation will also cover the contents of such follow-up activities.

(1) https://www.us-cert.gov/tlp