ISO/IEC TR 18044-2004:

Information security incident management

Maria Bartnes Dahl
maria.b.dahl@sintef.no

Dagens tekst

- Hva er TR 18044?
- Hvorfor TR 18044?
- Hendelseshåndtering
- Hvorfor god hendelseshåndtering?
- Innholdet i TR 18044

Om TR 18044

- Utarbeidet av ISO/IEC JTC 1 SC27
  - JTC 1: Information technology
  - SC 27: IT security techniques
- TR: Technical report
  - *Ikke* en standard, mer som state-of-the-art
  - Ingen krav stilles – dermed ikke sertifisering
- Utgitt oktober 2004 (første gang)
  - Ny gjennomgang når nødvendig
- Anskaffelse: kjøp fra Standard Norge
  - www.standard.no

Hvorfor TR 18044?

- Uansett forarbeid – hendelser vil komme til å inntreffe...
  - Oppdage, rapportere og undersøke hendelser
  - Reagere på hendelser, hindre/redusere konsekvenser, gjenoppretting
  - Lære av hendelser, forbedre hendelseshåndteringen til neste gang
- Råd og retningslinjer om håndtering av hendelser
  - Hendelse: uventet eller uønsket, truer informasjonssikkerheten
  - Informasjonssikkerhet: konfidensialitet, integritet, tilgjengelighet
- Systematisk tilnærming

Hvorfor TR 18044? (forts)

- Målgruppe:
  - ansvarlige for informasjonssikkerhet
  - ansvarlige for informasjonssystemer, -tjenester og -nettverk

- Kan leses: når som helst!
  - For nybegynnere – grundig innføring i hendelseshåndtering
  - I planleggingsfasen – strukturert og oversiktlig tilnærming
  - Brukes som oppslagsverk

Incident Response Management

- **Organisasjon**
  - Sikkerhetspolicy, risikostyring
  - ISIRT/CSIRT
  - Rutiner, prosedyrer
  - Rapportering
- **Teknologi**
  - Logging, deteksjon av sikkerhetsbrudd
  - Gjenoppretting – tilbake til normal drift
  - Bevissikring
  - Konfigurasjonsendringer, nytt utstyr
- **Mennesker – både ledelse, driftere og sluttbrukere**
  - Kompetanseutvikling
  - Læring av hendelser
  - Utvikling av sikkerhetskultur

Hvorfor god hendelseshåndtering?

- Forbedrer informasjonssikkerheten
- Reduserer skade på forretningsvirksomheten
- Økt fokus på forebyggende og holdningsskapende arbeid
- Økt oversikt over budsjett og ressurser
- Til hjelp i risikovurdering og –styring
- Gir input til arbeidet med sikkerhetspolicy

Prosesser

- 1. Plan and prepare
  - Policies, defined roles and responsibilities, briefing, training, testing
- 2. Use
  - Detection, reporting, collecting information, response
- 3. Review
  - Forensic analysis, identifying improvements in safeguards and IR scheme
- 4. Improve
  - Revising risk analysis, improving scheme, safeguards, documentation

Plan – Do – Check – Act

...og så da?

- Anskaff TR 18044 – les og lær
- Gjør en evaluering av eksisterende praksis
  - Få oversikt over arbeidet med hendelseshåndtering internt
    - inkl. risikostyring, kostnader, faktiske hendelser, personell, prosedyrer, ansvarsfordeling
- Bruk TR 18044 til å gjøre forbedringer