Får vi de standardene vi fortjener?

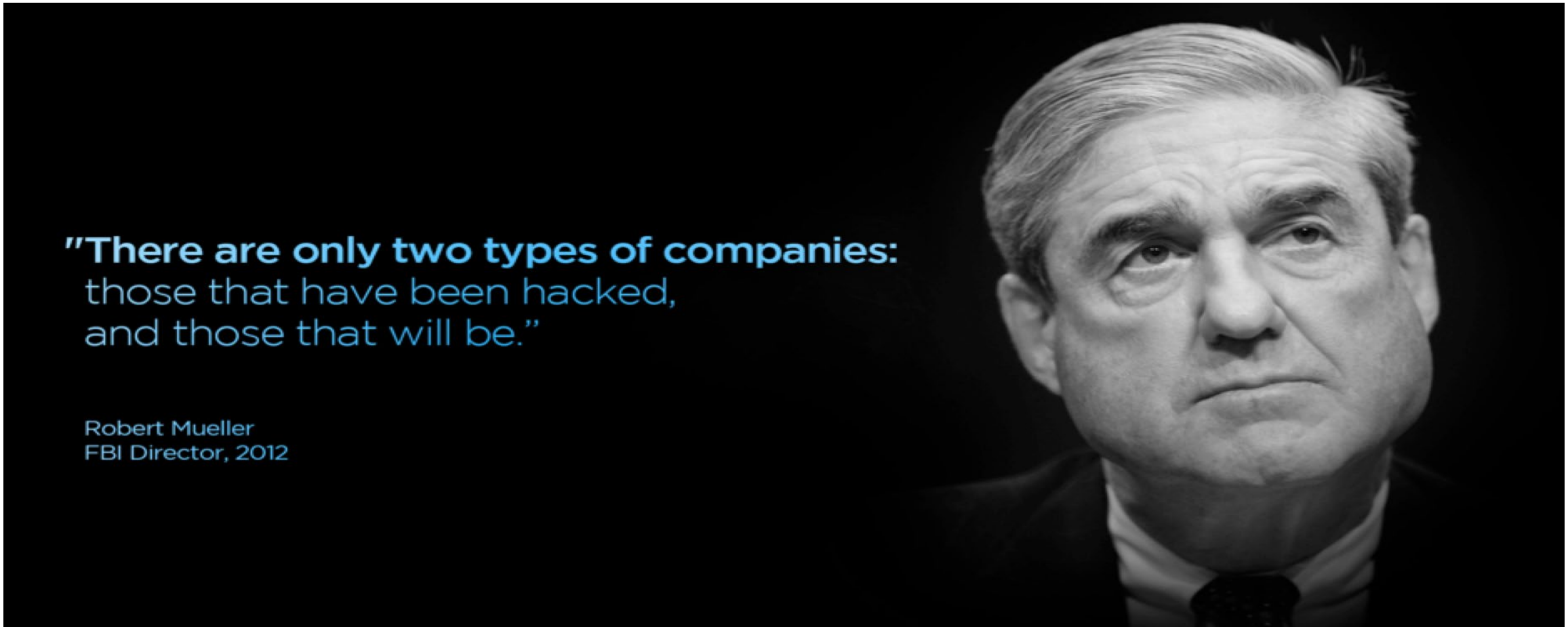
Hvordan sikre et større norsk fotavtrykk i internasjonale standarder for cyber sikkerhet?

Lars E Jensen

Prosjektleder

Sitat, Robert Muller

….er dette riktig for Norge…



Mål for Nasjonal strategi for digital sikkerhet

Med bakgrunn i sikkerhetsutfordringene, legges følgende overordnede mål til grunn:

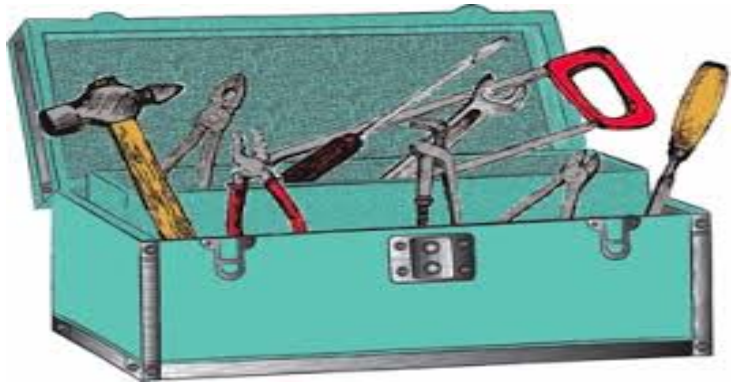
1. Norske virksomheter digitaliserer på en sikker og tillitvekkende måte, og har bedre evne til egenbeskyttelse mot uønskede digitale hendelser.

2. Kritiske samfunnsfunksjoner er understøttet av en robust og pålitelig digital infrastruktur.

3. Styrket digital sikkerhetskompetanse i tråd med samfunnets behov.

4. Samfunnet har en bedre evne til å avdekke og håndtere digitale angrep.

5. Politiet har styrket sin evne til å bekjempe data- og IKT relatert kriminalitet.



Tiltaksoversikt til nasjonal strategi for digital sikkerhet

TILTAK 17: STANDARD NORGE

- Norge skal være til stede på internasjonale arenaer hvor standarder for digital sikkerhet utvikles.
- I 2016, 2017 og 2018 har Standard Norge fått tilsagn om bevilgning til programmet «Standardisering innen IKT-sikkerhet».
- Det er reetablert en norsk speilkomite 1/SC 27, **under ledelse av NSM,** som skal bidra til å avklare behov for standarder innenfor IKT-sikkerhetsområdet.
- Videre skal det prioriteres deltakelse i en nystartet komite 1/SC 41 «Internet of Things».
- Det skal engasjeres eksperter og samarbeid med forskningsmiljøer inngår i prosjektet.
- Ansvarlig virksomhet: JD og NSM
- Gjennomføres: Løpende

Hvordan komme i gang med bedre Informasjonssikkerhet, cybersikkerhet og personvern

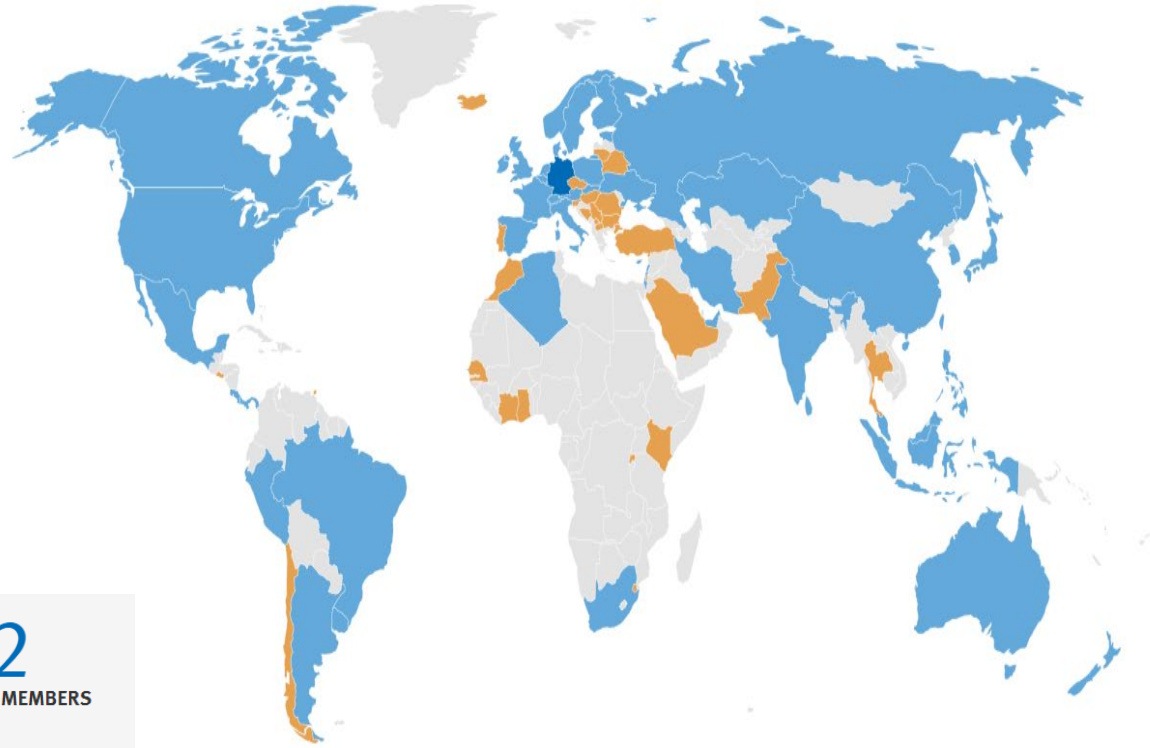
Grunnpakke 1,2 og 3

SN/K 171 Informasjonssikkerhet, cybersikkerhet og personvern

ISO/IEC JTC1 SC 27 Information Security, cyber Security and Privacy

- **Forebygge og redusere cyberrisikoen**
- **Begrense virkningen av cyberangrep**
- **Begrense den økonomiske risikoen**

….gjennom å sikre IT-baserte systemer, tjenester og infrastruktur for å beskytte sensitiv, kritisk og



198	86	48	32
PUBLISHED ISO STANDARDS * under the direct responsibility of ISO/IEC JTC 1/SC 27	ISO STANDARDS UNDER DEVELOPMENT * under the direct responsibility of ISO/IEC JTC 1/SC 27	PARTICIPATING MEMBERS	OBSERVING MEMBERS

Great things happen when the world agrees

Grunnpakkene 1- 3
- Ta kontroll på egen cyberrisiko

Grunnpakke 1

Standarder som alle virksomheter må være kjent med for å gjennomføre basissikkerheten. Typiske standarder i denne pakken er NS-ISO/IEC 27001 og NS-ISO/IEC 27002, men pakken inneholder også flere andre viktige standarder. **Grunnpakke 1 er vår Standardsamling for IT-sikkerhet.**

- NS-ISO/IEC 27000 Informasjonsteknologi - Sikringsteknikker - Ledelsessystemer for informasjonssikkerhet - Oversikt og terminologi (ISO/IEC 27000:2016). Engelsk og norsk utgave.
- NS-ISO/IEC 27001 Informasjonsteknologi - Sikringsteknikker - Ledelsessystemer for informasjonssikkerhet - Krav. Engelsk og norsk utgave.
- NS-ISO/IEC 27002 Informasjonsteknologi - Sikringsteknikker - Tiltak for informasjonssikring. Engelsk og norsk utgave.
- NS-ISO/IEC 27003 Informasjonsteknologi - Sikringsteknikker - Ledelsessystemer for informasjonssikkerhet - Veiledning. Engelsk utgave.
- NS-ISO/IEC 27004 Informasjonsteknologi - Sikringsteknikker - Ledelsessystemer for informasjonssikkerhet - Overvåking, måling, analyse og evaluering. Engelsk utgave.
- NS-ISO/IEC 27005 Informasjonsteknologi - Sikringsteknikker - Risikostyring for informasjonssikkerhet. Engelsk utgave.
- NS-ISO/IEC 27701 Sikringsteknikker - Utvidelse av NS-ISO/IEC 27001 og NS-EN ISO/IEC 27002 for håndtering av personvernsinformasjon - Krav og retningslinjer. Engelsk utgave.

Grunnpakke 1 er tilgjengelig her som Standardsamling for IT-sikkerhet.

Grunnpakke 2

Standardene har en utvidet funksjon som går lenger og som inkluderer hjelp til å implementere kontroll funksjoner for å forebygge mot cybersikkerhetsrisikoer, hvor blant annet standarder for Cloud inngår og hvor personlig sensitiv informasjon skal håndteres ut fra GDPR-kravene, samt Information security governance.

- NS/IEC ISO 29100 Information technology — Security techniques —Privacy framework + Amendment 1
- NS ISO/IEC 29134 Information technology -- Security techniques -- Guidelines for privacy impact assessment
- NS-ISO/IEC 27017 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- NS-ISO/IEC 27018 Information technology — Security techniques — Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors
- NS-ISO/IEC 27014 Information security governance
- NS-ISO/IEC 27031 Guidelines for information and communication technology readiness for business continuity
- NS-ISO/IEC 27035 Information technology — Security techniques — Information security incident management (parts 1 & 2 published)
- NS-ISO/IEC 27036 Information technology — Security techniques — Information security for supplier relationships (four parts)

Standardene i Grunnpakke 2 kan kjøpes på denne siden

Grunnpakke 3

Standardene inkluderer blant annet sektorspesifikke standarder, men inkluderer også ulike standarder som setter fokus på sikker lagring, og samling av bevis dersom en hendelse har inntruffet.

- NS-ISO/IEC 15408-1 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model
- NS-ISO/IEC 15408-2 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional components
- NS-ISO/IEC 15408-3 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance components
- NS-ISO/IEC 18045 Information technology – Security techniques – Methodology for IT security evaluation
- NS-ISO/IEC 19790 Information technology - Security techniques - Security requirements for cryptographic modules
- NS-ISO/IEC 27010 Information technology - Security techniques - Information security management for inter-sector and inter-organizational communications
- NS-ISO/IEC 29147 Information technology – Security techniques – Vulnerability disclosure
- NS-ISO/IEC 30111 Information technology - Security techniques - Vulnerability handling processes
- NS-ISO/IEC 27006 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems
- NS-ISO/IEC 27007 Information technology - Security techniques - Guidelines for information security management systems auditing
- NS-ISO/IEC 27011 Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- NS-ISO/IEC 27019 Informasjonsteknologi - Sikringsteknikker - Informasjonssikkerhetskontroller for energiforsyningsindustrien.
- NS-ISO/IEC 27034 Information technology — Security techniques — Application security
- NS-ISO/IEC 27037 Guidelines for identification, collection, acquisition and preservation of digital evidence
- NS-ISO/IEC 27039 Information technology — Security techniques — Selection, deployment and operation of intrusion detection and prevention systems (IDPS) Intrusion prevention
- NS-ISO/IEC 27040 Information technology — Security techniques — Storage security
- NS-ISO/IEC 27041 Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method
- NS-ISO/IEC 27042 Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence
- NS-ISO/IEC 27043 Information technology — Security techniques — Incident investigation principles and processes
- NS-ISO/IEC 27050 Information technology — Security techniques — Electronic discovery (parts 1, 2 & 3 published)
- NS-ISO 27799:2016 Health informatics — Information security management in health using ISO/IEC 27002 (second edition)

Standardene i Grunnpakke 3 kan kjøpes på denne siden

Hvordan sikre at verktøykassen for cyber sikkerhet oppdateres og er til hjelp for norske virksomheter?

- **Utvikle verktøykassen**
  - Avdekke egen risiko og sårbarhet,
  - Beslutte akseptabel risiko av egen cybersikkerhet
  - Implementere riktige tiltak.
- **Utvikle kurs basert på grunnpakkene**
- **Oversettelser**
  - NS-ISO/IEC 27701 GDPR

Great things happen when the world agrees

Får vi de standardene vi fortjener?

– Kan vi bli bedre på samspill mellom virksomhetene og styrke Cyber sikkerhetsarbeidet

Veien videre…….. skape et STØRRE Norsk engasjement for påvirkning

NORSKE EKSPERTER

…de beste standardene får vi når norske eksperter deltar aktivt og påvirker nye internasjonale standarder…..

….vil du være med…….. ?

..ta kontakt med Standard Norge,

Prosjektleder Lars Erik Jensen, lej@standard.no
eller Mobil: 92660390

Takk for meg!

Spørsmål