Logging – hvorfor og hvordan

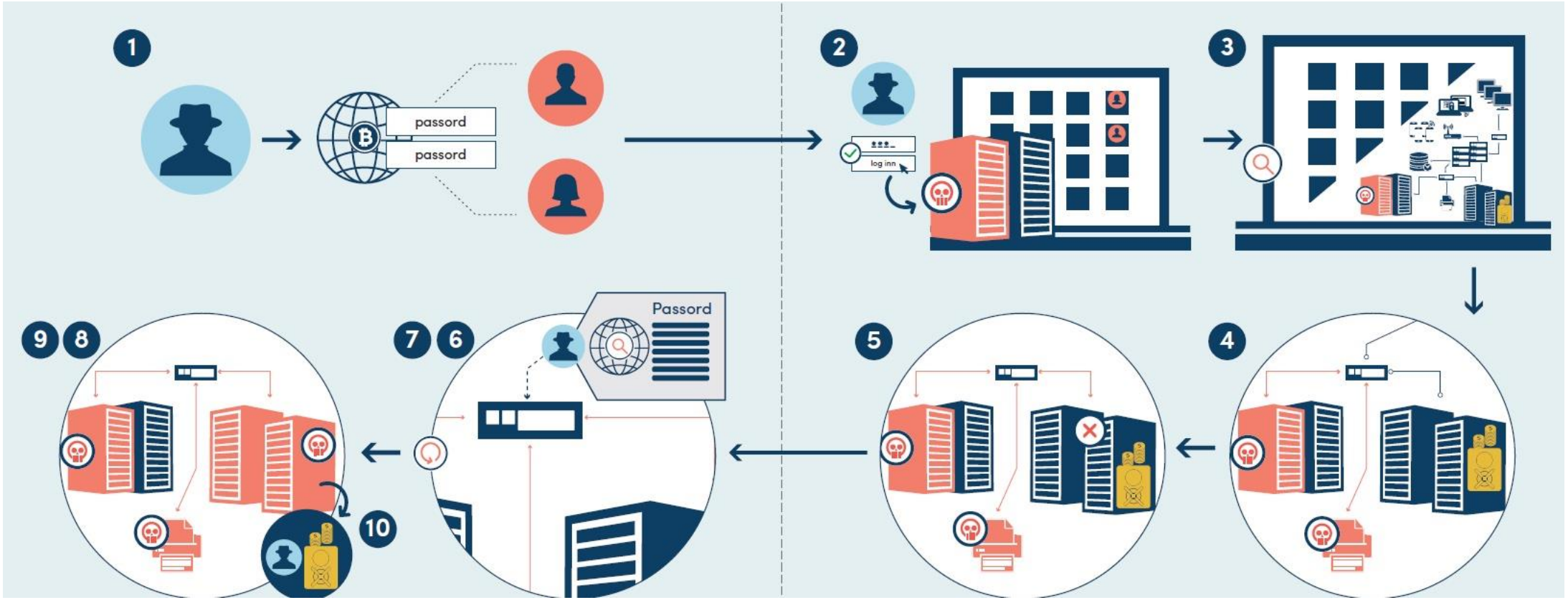
Erfaringer fra Nasjonalt cybersikkerhetssenter

NASJONAL
SIKKERHETSMYNDIGHET

Gullik Gundersen
Juridisk seniorrådgiver
2021-09-16

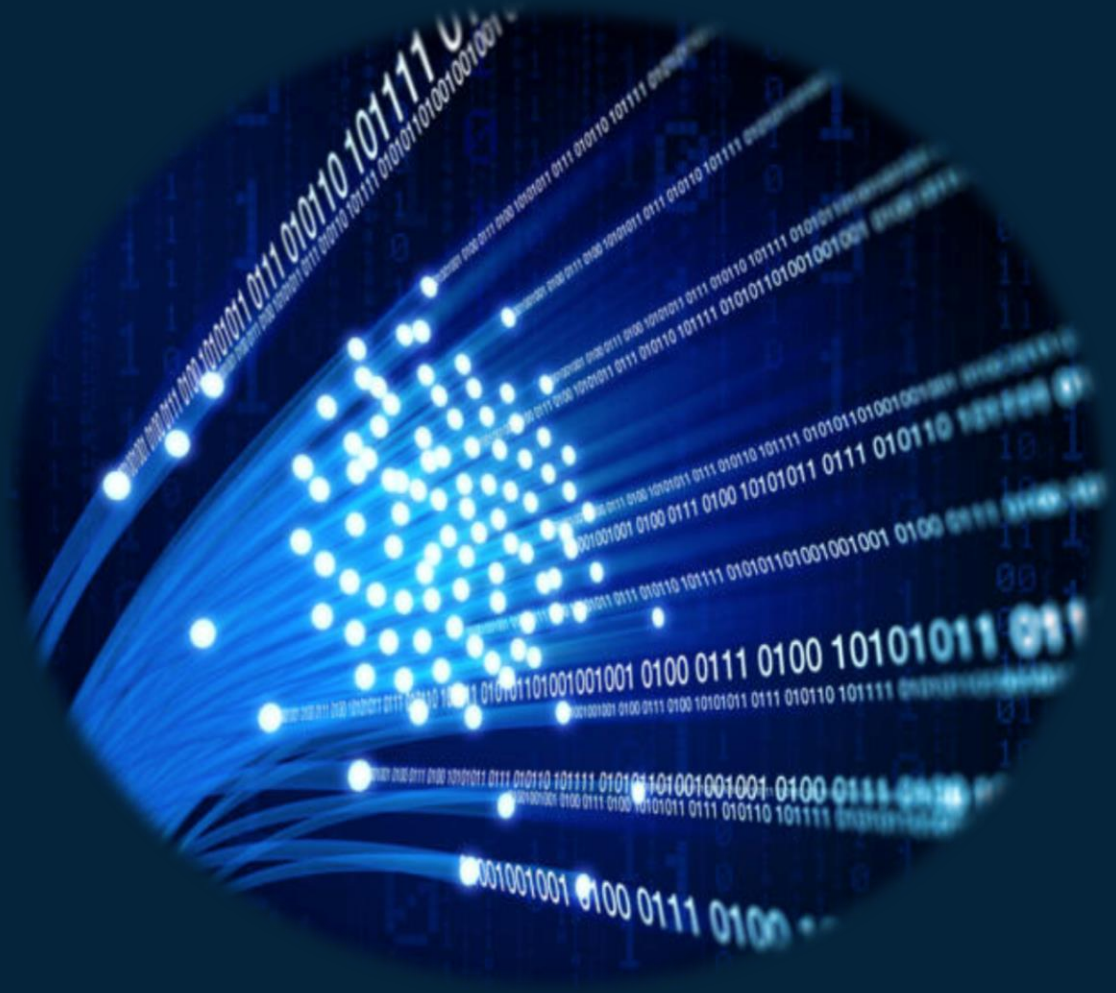
NASJONAL
SIKKERHETSMYNDIGHET

Digital operasjon mot norsk virksomhet



Logging – hva og hvordan

- Logg lenge nok
- Logg riktig ting
  - Operativsystemlogger
  - Nettverkslogger
  - Tjenestelogger
- Logg på riktig måte
  - Riktig konfigurert
  - Integritet og tilgjengelighet



Når uhellet først er ute

- Nasjonalt cybersikkerhetssenter – operasjonssenteret
- Bemannet 24/7/365

- norcert@cert.no
- 02497

1. Kartlegg enheter i bruk i virksomheten.
2. Kartlegg programvare i bruk i virksomheten.
3. Kjøp moderne og oppdatert maskin- og programvare.
4. Ta ansvar for virksomhetens sikkerhet også ved tjenesteutsetting.
5. Del opp virksomhetens nettverk etter virksomhetens risikoprofil.
6. Etabler et sentralt styrt regime for sikkerhets-oppdatering.
7. Konfigurer klienter slik at kun kjent programvare kjører på dem.
8. Deaktiver unødvendig funksjonalitet.
9. Endre alle standardpassord på IKT-produktene før produksjons-setting.
10. Minimer rettigheter til sluttbrukere og spesialbrukere.
11. Minimer rettigheter på driftskontoer.
12. Legg en plan for regelmessig sikkerhets-kopiering av alle virksomhetsdata.
13. Avgjør hvilke deler av IKT-systemet som skal overvåkes.
14. Beslutt hvilke data som er sikkerhetsrelevant og bør samles inn.
15. Etabler et planverk for hendelses-håndtering.

Helhetlig digitalt risikobilde 2020

RISIKO 2021

– helhetlig sikring mot sammensatte trusler

NASJONAL
SIKKERHETSMYNDIGHET