Riksrevisjonen

Når revisor låner metoder fra etiske hackere

IIA Cybersecurity webinar 15. april 2021

Christian Andresen, seniorrådgiver i Riksrevisjonen

Informasjonssikkerhet i 2021?

Risiko 2021 (NSM)

- Flertallet av uønskede hendelser relatert til sky skyldes feilkonfigurasjon eller feil bruk.
- Passordsikkerhet er en vedvarende utfordring.

DBIR 2020 Takeaways (Thycotic)

- Cyber criminals still use the most common techniques at the lowest cost.
- Human error and misconfigurations are on the rise.

Helseforetakenes forebygging av angrep mot sine IKT-systemer (Riksrevisjonen)

- I alle helseregioner er det vesentlige svakheter i grunnleggende tekniske sikkerhetstiltak.
- Ikke tilstrekkelig opprydding og utfasing av eldre systemer og tilganger.

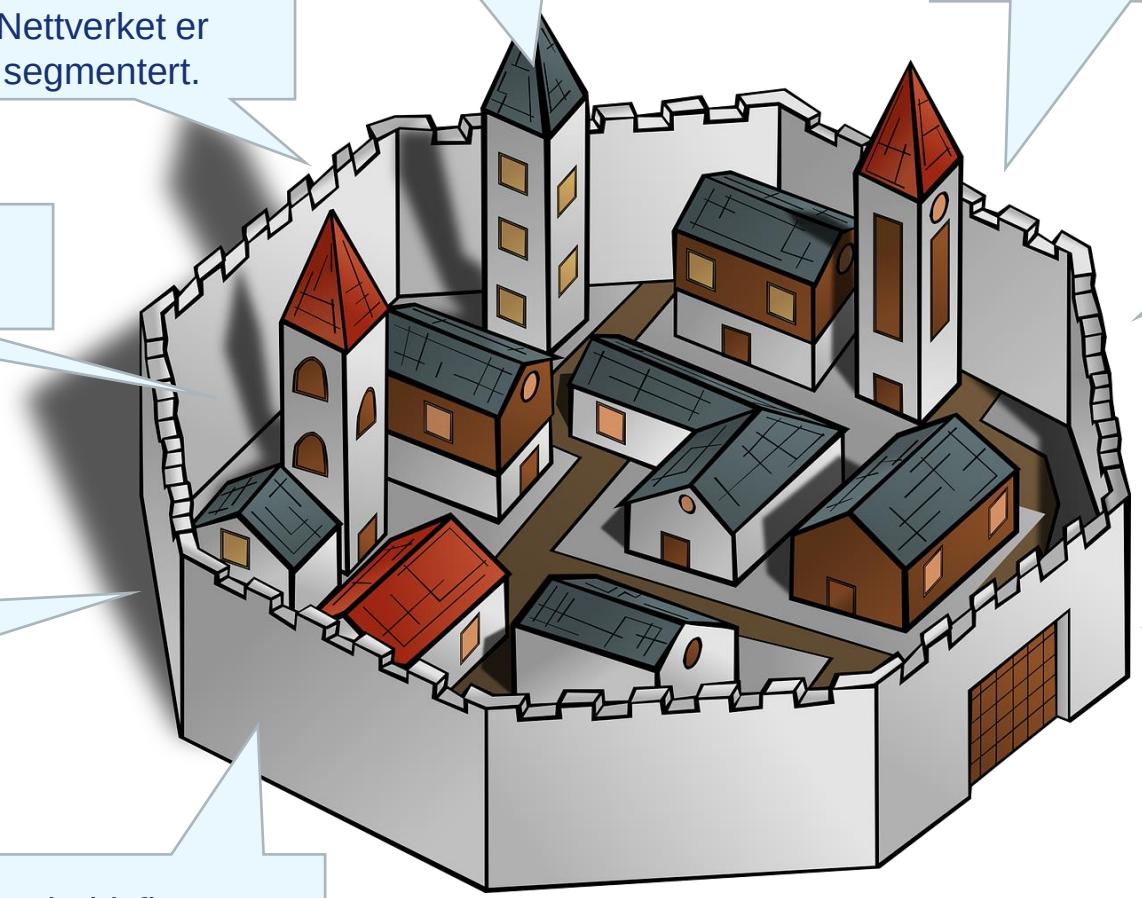
Sikkerhetstesting i revisjoner – en utvikling

- **Intervju** (f. eks ledelse, sikkerhetspersonell, driftspersonell)
- **Dokumentanalyse** (f. eks retningslinjer, rutiner, interne revisjoner)
- **Spørrebrev** (f. eks få innledende informasjon, avklare foreløpige funn)

- **Dataanalyse** (f. eks tilganger, konfigurasjon, brannmurregler)

- **Sikkerhetstesting** (f. eks kartlegge, utvide tilgang)

Virksomhetens respons etter en stor revisjon med mange funn … (anno 2010-2015)



De *andre* databasene er skikkelig herdet.

Vi er midt i en prosess …

Nettverket er segmentert.

Perimeteret er sikkert.

Vi har nylig anskaffet en overvåkningsløsning...

Folk er til å stole på.

Vi kan ikke se at dette har hatt noen konsekvens.

Sikkerheten er god selv om vi ikke følger egne retningslinjer.

Arbeidsflaten er helt nedlåst.

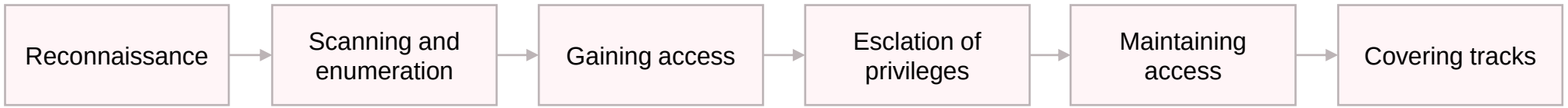
FOTO: Pixabay

Hvorfor sikkerhetstesting?

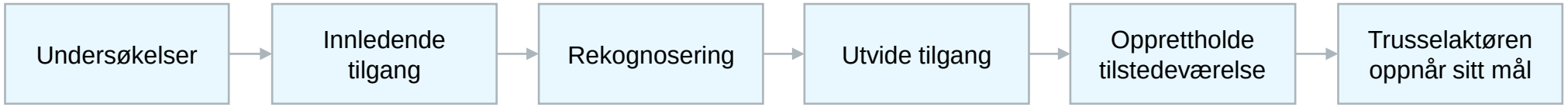
- **Enighet om fakta, men ikke om risiko.**
- Informasjon fra virksomheten som revisjonsbevis er ikke alltid god nok:
  - Mangelfull kunnskap om sikkerhetstilstanden
  - Er ofte utdatert eller ufullstendig
  - Nåsituasjon vs. målbilde
- Revisors utvalg av både sikkerhetstiltak og datakilder kan diskuteres – vil aldri kunne dekke alt.
- Direkte og mer fleksibel innsamling av data.

Hva gjør (etiske) hackere?

Kilde: Lockheed Martin Cyber Kill Chain (CKC)



Kilde: EC-Council Certified Ethical Hacker (CEH)



Kilde: NSM Risiko 2017

Hva gjør (etiske) hackere?

FOTO: The MITRE Corporation

ID	Eksempler på teknikker
T1595	Aktiv skanning (f. eks skanne etter utdatert programvare)
T1110	Passordangrep (f. eks passordspray)
T1190	Utnytte sårbarheter i applikasjoner (f. eks SQL injection)
T1557	Man-in-the-Middle (f. eks LLMNR/NBT-NS Poisoning)

FOTO: Red Canary

Hjelpemidler for test av teknikker i ATT&CK Matrix: Red Canary Atomic Red Team

Revisjon av helseforetakene

Hovedfunn (rapport)

- I tre av fire regioner fikk vi høy grad av kontroll over viktige IKT-systemer.
- En angriper kan gjøre betydelig skade selv uten høy grad av kontroll over IKT-systemene.
- En region oppdaget flere av våre aktiviteter, mens de andre tre oppdaget lite eller ingenting.

Hvor kan revisor starte?

- Teste om virksomheten har kontroll på «de kjedelige tingene».
- Ikke nødvendig å gjennomføre alle stegene av en sikkerhetstest, men må sette funn i kontekst og forklare risiko.
- Testing som innebærer lav risiko, for eksempel **undersøkelser** og **rekognosering**.
- Benytt enkle metoder og standard verktøy.
- Få hjelp av IT- og sikkerhetspersonell.

Datatilsynet anbefaler NSM Grunnprinsipper for IKT-sikkerhet.

Eksempel:

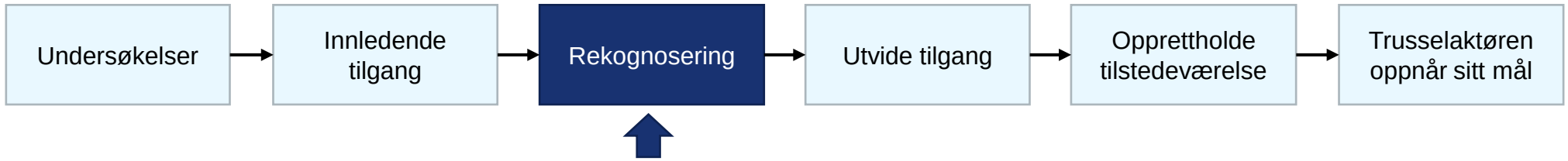
- God kontroll med tilganger i Active Directory (AD) er viktig for å oppnå tilfredsstillende informasjonssikkerhet.

To utvalgte grunnprinsipper:

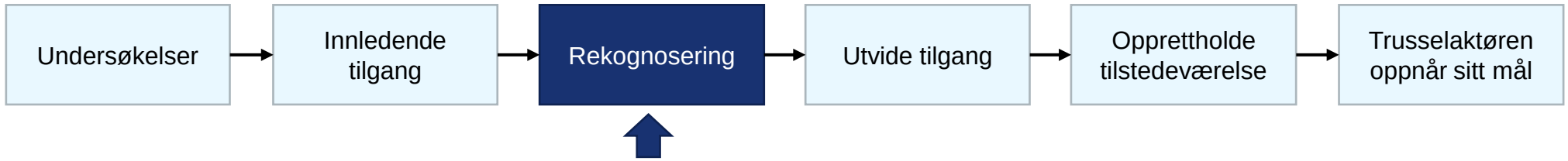
- 2.6.4 Minimer rettigheter til sluttbrukere og spesialbrukere.
- 2.6.5 Minimer rettigheter på driftskontoer.

Helt konkret, hvilke tilganger gjelder dette?

- Ikke bare «Domain Admins».
- Microsoft Enterprise Access Model gir støtte her.



Formål	Datagrunnlag / verktøy	Kommentar
Kartlegg katalogtjenesten: • forstå miljøet • finne sårbarheter • planlegge videre angrep	Data fra Active Directory: • kontoer • grupper • maskiner • GPO-er • OU-er • rettigheter • trusts • sesjoner	• Hvem har de mest utvidede rettighetene? • Hvem kan utøve kontroll over viktige verdier? • Finnes det åpninger for å eskalere rettigheter? • Hva har «alle / nesten alle» tilgang til?



Eksempler på funn

- **Tilganger er tildelt langt utover tjenstlig behov, herunder tilgang til å administrere kontoer, servere, databaser og nettverk.**
- Alle ansatte har fri tilgang til:
  - store mengder sensitive opplysninger
  - verktøy som driftspersonell og utviklere benytter
- Det er gode muligheter for angripere som ønsker å utvide sin tilgang gjennom Active Directory.
  - Fokus på det øverste nivået av tilganger, men glemmer «ekvivalenter» og lavere nivåer som kan volde betydelig skade.

Cybersecurity – en god match for revisor

- Revisor har et solid faglig fundament for kontroll og forbedring.
- Mange av utfordringene innen cybersikkerhet er ikke dypt tekniske.
- Stadig bedre tilgang på revisjonskriterier, verktøy og data.
- Revisor har kjennskap til virksomheten og/eller erfaring fra lignende virksomheter.
- Et etablert tillitsforhold og god tilgang på interne ressurser.
- Avstand til de daglige utfordringer, resultatmål mv.
- Internrevisor: den foretrukne budbringeren av dårlige nyheter?

- Spørsmål?
- Kommentarer?