IN1020 - Datasikkerhet:
Øvingsoppgaver gruppetime 10 (uke 44)

1. Trusselmodellering:

   Et konsulentselskap har spesialisert seg på og tilbyr ekspertise innen innføring av store og små IT-systemer i bedrifter og organisasjoner. Kundene er virksomheter i både offentlig og privat sektor.

   Konsulentselskapet har egne tjenermaskiner og drifter og forvalter en lagringstjener for alle interne dokumenter, samt en server som kjører en applikasjon for timeføring på de ulike konsulentoppdragene. Timeførings-systemet er tilgjengelig via et web-grensesnitt, som er tilgjengelig over internett for både ansatte og kunder. Det benyttes brukernavn og passord for innlogging i dette web-grensesnittet.

   De ansatte disponerer hver sin laptop som sin arbeidsflate, og bringer også denne med seg når de er ute hos kunden på oppdrag.

   Gjennomfør en enkel trusselmodellering etter illustrasjon på forelesning 23.10.2024. Trusselmodelleringen skal ha utgangsfokus på trusselaktør. Identifiser noen mulige trusselaktører, angrepsvektorer, sårbarheter, mulige sikkerhetstiltak, samt tekniske konsekvenser og konsekvenser for konsulentselskapet.

2. Personvern og trusselmodellering: Eksamensoppgave 3.7 fra eksamenssettet H22[1].

3. Case-oppgave fra NSM: NSMs rapport Nasjonalt digitalt risikobilde 2023[2], beskriver på side 8 og 9 et tenkt hacker-angrep.

   (a) Hvilke(n) angrepvektor(er) bruker trusselaktøren?

   (b) Hvorfor tror dere dette skjer akkurat Ola Nordmann?

   (c) Diskuter sikkerhetstiltak dere kjenner til som kunne stoppet eller redusert skadeomfanget av en hendelse som dette. Se gjerne også på NSMs grunnprinsipper for IKT-sikkerhet[3]

4. Nulldagssårbarheter:

   (a) Hva er en nulldagssårbarhet?

   (b) Se nærmere på en varslet sårbarhet i det som heter Cisco IOS XE Web UI[4]. Er dette en nulldagssårbarhet? Hvilke tiltak anbefaler produsenten (Cisco) for å håndtere sårbarheten?

5. Innsidebruker som trussel: Innsidebrukere som trussel er en reell risiko, også påpekt i NSMs rapport Risiko 2024[5] side 26-28 og NSMs rapport Nasjonalt digitalt risikobilde 2023 s. 34-36. Diskuter tiltak man kan iverksette for å beskytte en virksomhet mot innsidetrusler.

6. Eksamensoppgaver 3.2, 3.3 og 3.4 fra eksamenssettet H22.

[1] https://www.uio.no/studier/emner/matnat/ifi/IN1020/h23/tidligere-eksamensoppgaver/xh2022-no.pdf

[2] https://www.uio.no/studier/emner/matnat/ifi/IN1020/h23/undervisningsmateriell/nasjonalt-digitalt-risikobilde-2023.pdf

[3] https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/ta-i-bruk-grunnprinsippene/

[4] https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/varsler-fra-ncsc/aktiv-utnyttelse-av-sarbarhet-i-cisco-ios-xe-web-ui-cve-2023-20198

[5] https://www.uio.no/studier/emner/matnat/ifi/IN1020/h24/undervisningsmateriell/nsm-risiko-2024.pdf