IN1020: Øvingsoppgaver gruppetime 12 (uke 46)

Oppgave 1: Case-oppgave

Året er 2017. På jobben din er bruk av datamaskiner en essensiell del av arbeidet. Hver av de ansatte sitter på harddisker fulle av halvferdig arbeid og businesshemmeligheter som til sammen er verdt milliarder! En dag blir du møtt med denne meldingen på desktoppen din:

```
"Ops, your important files are encrypted"
```

Videre ber meldingen deg å kjøre en dekrypterings-programvare, som allerede har poppet opp. I dekrypterings-programvaren ser du en klokke som teller ned, og en melding som ber om 300 bitcoin (som var mye penger i 2017). Du ser rundt deg og flere og flere av kollegaene dine ser ut til å bli rammet. Full panikk! Hva nå?

a) Hvordan tror dere hovedpersonen ble rammet av denne skadevaren? Har de gjort noe dumt eller kan dette skje uansett om man er flink selv?

b) Diskuter hva slags skadevare det er snakk om her.

c) Hvordan kunne arbeidsplassen forhindret angrepet? (Kunne de det i det hele tatt?) Hva er lurt å gjøre når angrepet først har begynt?

d) Hvilke sikkerhetsmål er svekket av angrepet?

e) Denne oppgaven er basert på ekte hendelser. Kjenner dere til dette angrepet?

Oppgave 2: Tjenestenektangrep er en form for angrep som gjerne forbindes med herverk og sabotasje, eller økonimisk kriminalitet i form av utpressing.

a) Hvilke sikkerhetsmål påvirkes av denne type angrep?

b) Hvilke ulike former for tjenestenektangrep benyttes ofte av hackere i dag?

c) Hva kan virksomheter gjøre for å sikre seg mot denne typen angrep?

Oppgave 3: EUs *"The cookie law"*, eller *ePrivacy Directive* trådde for alvor i kraft i 2011, og regulerer bruk av informasjonskapsler (cookies) på nettsider. Dette har du nok lagt merke til ettersom nesten alle nettsiden i dag spør om lov til å bruke cookies. Hvorfor ønsker/ønsker vi ikke at nettsider skal lage cookier for oss?

Oppgave 4: Kom med forslag til hvordan en angriper kan bruke sosial manipulering til å:

a) få uautorisert tilgang til en virksomhets/en bedrifts lokaler/bygg

b) installert skadevare på de personlige datamaskinene til selskapets direktør

Oppgave 5:

a) Hvilke sårbarheter er det vanlig å utnytte i det vi kaller phishing attacks?

b) Foreslå sikkerhetstiltak for å forebygge slike angrep (phishing attacks).

Oppgave 6: På semestersiden til IN1020 finner dere et bilde:

https://www.uio.no/studier/emner/matnat/ifi/IN1020/h21/ukeoppgaver/vinterblomst.jpg

a) Finn ut hvor bildet er tatt ved å se på metadataene som følger med i bildefilen.

b) Finner du annen interessant informasjon i bildets metadata?

Oppgave 7: Case-oppgave

Til tross for at en webtjeneste for en nettbank er svært sikkert konfigurert, kan ting gå galt f.eks. når en bruker skal bruke (logge seg inn til) banken for å betale en regning. Diskuter mulige feil som kan oppstå (hint: brukerfeil, trådløst nett, etc).

Oppgave 8: Case-oppgave

I oppkobling mot en online webtjeneste autentiseres brukeren i starten av sesjonen. Data utveksles så med webtjeneren til og fra vedkommendes lokale maskin (endenode). Kan tjenestetilbyder på bakgrunn av brukerautentiseringen anta at data som mottas gjennom den etablerte forbindelsen er autentiske?

Oppgave 9: Enkel 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 10.11.2022. Trusselmodelleringen skal ha utgangsfokus på trusselaktør. Identifiser noen mulige trusselaktører, angrepsvektorer, sårbarheter, mulige sikkerhetstiltak, samt tekniske konsekvenser og konsekvenser for konsulentselskapet.