IN1020 - Datasikkerhet 4
: Løsningsforslag gruppetime 10 (uke 44)

1. Trusselmodellering

   Noen forslag:

   1. Innsidebrukeren, f.eks. en tidligere ansatt som har fått sparken. Ønsker hevne seg på konsulentselskapet, og siden vedkommende forsatt har tilgang til systemet logger vedkommende seg inn og sletter alle data hen kommer over. Sikkerhetstiltak som kan hindre denne type hendelser: Umiddelbart deaktivere brukerkontoer når ansatte slutter. Sørge for en policy for tilgang som sikrer at ansatte aldri har tilgang til flere ressurser enn det som er nødvendig for utførsel av jobben deres. Gode backuprutiner, som gjør det enkelt og raskt å gjenopprette fra denne type hendelser. Teknisk konsekvens er at data/informasjon slettes fra datasystemet. Konsekens for virksomheten kan være at ansatte ikke får gjort jobben sin fordi data er forsvunnet, som igjen fører til økonomisk tap pga. stillstand.

   2. Angriper med et litt rettet mål, som sender phishing-epost som utgir seg fra å komme fra ledelsen, for å få tak i brukerkontoer/passord. Sårbarheten er dårlig opplæring av brukere med dertil dårlig sikkerhetskultur. Sikkerhetstiltak kan være bedre opplæring, eller kanskje å bruke 2-faktor-autentisering ved innlogging. Kan det i tillegg finnes tekniske tiltak i en epost-tjener, som stopper denne typen angrep? Tekniske konsekvenser vil være at uvedkommende har tilgang til systemet som en vanlig ansatt, med mulighet for å stjele, endre eller slette dokumenter, timelster i timeføringssystemet, osv. Konsekvenser for virksomheten kan være tapt omdømme som følge av (muligens virksomhetskritisk) informasjon på avveie, også om kunder. Mulige juridiske konsekvenser?

   3. Tilfeldig angriper som kommer over og utnytter en sårbarhet i web-applikasjonen, f.eks. ved SQL-injisering. Sikkerhetstiltak vil være hyppige sikkerhetsoppdateringer av programvare, kreve bruk av VPN eller annen sikker tunnell i all kommunikasjon med web-tjeneren. Teknisk konsekvens kan være datalekkasje. Konsekvenser for virksomheten kan være tapt omdømme som følge av (muligens virksomhetskritisk) informasjon på avveie, også om kunder. Mulige juridiske konsekvenser?

   4. Konkurrent til en av konsulentfirmaets kunder som ønsker opplysninger om et større IT-prosjekt kunden er i ferd med å innføre. Angrepsvektor kan være svindelepost som lurer en ansatt til å utlevere informasjonen, eller kanskje bestikke en ansatt til å utlever informasjonen. Bevissthetstrening, opplæring, ha policyer som sørger for at en ansatt ikke har tilgang til informasjon om andre prosjekter enn de hen jobber på. Teknisk konsekvens er datalekkasje, for virksomheten vil det være juridiske konsekvenser, i tillegg til sannsynlig tapt omdømme.

2. Se fasit til eksamensoppgaven 3.7 i løsning eksamenssett H22[1].

3. Case-oppgave fra NSM

   (a) Målrettet og sosialt avansert phishing, deretter spionprogramvare.

   (b) Sannsynligvis fordi Ola Nordmann er IT-Adminstrator, og derfor (muligens?) kan ha ekstra tilganger og rettigheter i IT-systemene.

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

(c) Diskuter. F.eks: Bruke 2FA istedenfor kun brukernavn og passord. Gode og gjennomtenkte policyer for å styre tilgangskontroll i alle IT-systemer og appllikasjoner, og minimere rettigheter slik at en ansatt ikke har tilgang til mer informasjon enn vedkommende har behov for i jobben. Vanskeliggjøre tilgang til sensitive data og f.eks. bedrifsthemmeligheter (kryptering av data, ekstra tilgangskontroll, loggføring av hvem som leser eller kopierer data, etc, samt ha rutiner for å analysere/gjennomgå loggene med mål å avdekke unormal adferd).

4. Innsidebruker som trussel

   Grundig IT-sikkerhetsopplæring av alle brukere. Skape en god sikkerhetskultur, skape lojalitet til f.eks. arbeidsgiver. Se også svar på oppgave 2 c).

5. Nulldagssårbarheter

   (a) En nulldagssårbarhet (zero-day vulnerability) er en sårbarhet som andre får kjennskap til før produsent/leverandør av den sårbare tjenesten (og før brukerne av tjenesten). Begrepet nulldagssårbarhet spiller på at man har 0 dager til å forberede seg på utnyttelse av sårbarheten.

   (b) Ja, dette virker være en nulldagssårbarhet. Det sies "Det finnes ingen tilgjengelige oppdateringer for sårbarheten for øyeblikket.", i tillegg til at man vet at sårbarheten er blitt utnyttet. Tiltak: Cisco anbefaler rett og slett at man som forebyggende tiltak deaktiverer de sårbare komponentene, i dette tilfelle HTTP og HTTPS. Som avdekkende (detekterende) tiltak anbefaler de å sjekke potensielt berørte systemer for tegn på kompromittering.

6. Se fasit til eksamensoppgavene 3.2, 3.3 og 3.4 her: løsning eksamenssett H22.