TDT4185 – Øving 3 – 10077

Oppgave 1
Antar jeg kan velge noen konsekvenser fra hver av skalakategoriene. F.eks at jeg kan velge både 1=Ubetydelig, punkt a (Ubetydelig stans i tjenesten) og 2=Moderat, punkt f (gjennopprettelig økonomisk tap) for en hendelse. Dette gjør jeg fordi jeg på flere hendelser ikke mener alle punktene under en kategori passer.

1. Her vil jeg sette opp konsekvensene til å være 1a, b, d, f og 2c, e, g, h. Dette fordi jeg mener at en kunde som manipulerer på strømmåleren ikke stopper tjenesten, derfor ubetydelig stans i tjenesten (**1a**). I tillegg er det ingen *uautorisert* innsyn i måledata, kunden har rett til å se sin egen data (**1b**). Videre er det ingen fare for ledninger eller andre fysiske komponenter, da jeg antar manipuleringen skjer elektronisk (**1d**). Jeg vil også si denne hendelsen har ubetydelig økonomisk tap, siden denne kun gjelder for et fåtall kunder, hvor de umulig kan svindle for mer enn under tusenlappen i måneden (**1f**). Jeg har satt opp at det er svært få mangler i datasett, da det igjen kun gjelder et fåtall kunder (**2c**). Jeg har også satt opp at det er et mindre brudd på lovverk, når manipulasjon går under svindel (**2e**). Selskapet mister også litt rykte og omdømme ovenfor kunder og virksomhetens omgivelser, siden manipulasjon viser at de har for dårlig sikkerhet (**2g og h**). Alt i alt kategoriserer jeg denne hendelsen som moderat-.
2. For denne hendelsen vil jeg sette opp **4a**, da ødeleggelser kan føre til dagers arbeid med reparasjon og lang stans i tjenesten (i dette området). Setter også opp **3b, c, og e**, siden personen(e) som tar seg inn i nettstasjonen har tilgang til å ta styring over systemene som er der, og dermed også manipulere og se data, samt fysisk ødelegge komponentene som befinner seg der. Dette kan også føre til **3h**, alvorlig økonomisk tap. Dette fordi måledata for store områder kan slettes eller gjøres utilgjengelige for nettselskapet (og f.eks selges tilbake til de for høye summer). Denne dataen kan også selges til en bruker i en ekstern virksomhet, og jeg setter også opp **3d**. Hendelsen er også et ganske seriøst lovbrudd og at jeg setter opp **3g** følger av dette. Alt i alt vil jeg kategorisere konsekvensene til denne hendelsen alvorlig.
3. Det er ingenting som sier dette skal føre til noe stans i tjenesten, det er kun salg av data. Derfor setter jeg opp **1a**. Ved salg av data til eksterne aktører får disse full innsyn i datasett, så **4b** følger av dette. Det er ingen mangler i datasettet, da det kun selges, ikke slettes, så jeg setter også opp **1c**. Det er helle ingen fare for ledninger eller fysiske komponenter, så jeg setter opp **1d**. Jeg mener dette er et kritisk lovbrudd, da det bryter med eventuelle taushetserklæringer og kontrakter kunder har (hvor de er beskyttet mot slik uautorisert innsyn i måledata) (**4e**). I tillegg vil virksomheten få alvorlig tap av renommé og rykte ovenfor både kunder og virksomhetens omgivelser, da de kan bli sett på som useriøse og illojale (**3i**). Selv om jeg har satt opp få konsekvenser under «kritisk», vil jeg allikevel kategorisere denne hendelsen som kritisk, da jeg synes det er en ganske alvorlig hendelse.
4. Jeg ser for meg at datakyndige personer i virksomheten klarer å stenge hackerene ute på relativt kort tid. Derfor setter jeg opp **3a** (stans inntil en dag), istedenfor **4a** (mange dager). I tillegg ser jeg for meg at når de først er inne i systemet, kan de få tilgang til data også, så jeg setter opp **4b**. Det er ingen fare for skade på ledninger eller fysiske komponenter, da angrepet skjer elektronisk. Derfor setter jeg opp **1d**. Denne hendelsen viser at virksomheten har for dårlig sikkerhet og de får nedsatt renommé og rykte, så jeg setter opp **3i**. Dersom hackerene får til å stenge

virksomheten ute fra sitt eget system, kan de kreve penger for å gi tilbake tilgang, som fører til alvorlig økonomisk tap (**3h**). Igjen er dette også et alvorlig lovbrudd (**3g**). Jeg kategoriserer konsekvensene av denne hendelsen som ganske høyt oppe i alvorlig skalaen.

5. Denne hendelsen ser jeg på som kritisk. Dersom boksene A1, A4 og A5 feiler, vil ikke kontrollsenteret ha noen måte å kommunisere med noen av strømmålerne og vil dermed mangle kritisk informasjon (**4c**). (som nevnt i oppgaveteksten; strømpriser, målinger osv..). Denne hendelsen bryter ikke med noen lovbrudd, det er bare en ting som kan skje (**1e**). Jeg antar dataen de ikke vil få lest/sendt er lagret og vil bli tilgjengelig så fort aksesspunktene er oppe og går igjen, derfor ser jeg ikke for meg at det kan være noe mer enn et (**1f**) gjennopprettelig økonomisk tap. Denne hendelsen gir virksomheten et moderat tap av renommé og rykte, både ovenfor kunder og omgivelser. Dette fordi de over en kortere periode (**3a** inntil en dag stans, ser ikke for meg det kan ta lengre til å få aksesspunktene opp igjen) ikke kan utføre tjenesten de skal (**2g og h**).

Oppgave 2:

1. **2 – Mindre sannsynlig**. Jeg tenker at det er gjort tiltak for å unngå manipulasjon av måledata. Samtidig, dersom en datakyndig medarbeider har kjennskap til disse tiltakene, kan det være mulig å manipulere. At dette skjer årlig (**2a**) ser jeg for meg at kan være litt lite, derfor vil jeg også sette opp **3a** – flere ganger i året. Det kan være flere kunder som f.eks får hjelp av medarbeidere i virksomheten, eller at de er ekstremt datakyndige selv.
2. **3 – Mulig.** Det er ganske lav terskel for å dirke opp låsen på en nettstasjon. Dette kan være ondsinnet, eller det kan være noen som tenker det er morsomt å prøve. Nettstasjonene er tilgjengelige for allmenheten, så tilgang er ikke et problem. Jeg tenker nødvendige sikkerhetstiltak er tatt, men at det er relativt greit å dirke opp en lås.
3. **3 – Mulig.** For å få tak i data skal det nok ikke så veldig mye mer til enn å jobbe i virksomheten. Derfor passer **3c** ganske godt her. I tillegg kan det tenkes at ansatte tenker dette er en «lett» måte å tjene litt ekstra penger på. Jeg tror likevel ikke det skjer flere ganger i året, så derfor vil jeg bytte ut **3a** med **2a – årlig.** Dette fordi de aller som jobber i en virksomhet vet at det er en personlig risiko å selge data, samt hvis det oppdages at data selges vil det settes i gang en «etterforskning», som vil skremme eventuelle andre som vil selge data.
4. **1 – Usannsynlig.** Hacking er krevende og ting skal klaffe. Du trenger som regel informasjon og hjelp innenfra. Derfor synes jeg **1e** passer veldig bra her. Utenforstående må ha spisskompetanse og et samarbeid med personer i virksomheten. I tillegg er nok sikkerheten satt opp slik at egne medarbeidere må ha god kunnskap om tiltakene.
5. **4 – Sannsynlig.** Uhell skjer. Det er ikke så veldig mange «sikkerhetstiltak» en kan ta for denne hendelsen. Strømmen kan gå ved en oppgradering av software, som får aksesspunktet til å få en feil, menneskelig feil er veldig vanlig, dette kan oppstå ved konfigurasjon av aksesspunktene. Ved planlagt nedetid kan de som skal skru av aksesspunktene være utålmodige og skru av før all kommunikasjon er lagret osv...

TDT4185 – Øving 3 – 10077

Oppgave 3:

Konsekvens/Sannsynlighet	Usannsynlig	Mindre Sannsynlig	Mulig	Sannsynlig
Kritisk			Hendelse 3	Hendelse 5
Alvorlig	Hendelse 4		Hendelse 2	
Moderat	Hendelse 1			
Ubetydelig				

Oppgave 4:

1. I og med at konsekvensene for denne hendelsen er lavt på moderatskalaen, vil jeg velge strategien **accept**. Dersom noen først får til å manipulere strømmåleren er de datakyndige, og vil mest sannsynlig finne en måte å få det til uansett.
2. **Transfer.** Siden en nettstasjon er nødvendig for tjenesten, vil jeg si at det er best å sette opp en forsikring for denne hendelsen, istedenfor de andre strategiene.
3. **Avoid**. Selv om bruk av denne strategien ofte fører til store ulemper, ser jeg på denne hendelsen som verdt det (og lett å unngå ved f.eks sparking av personer som selger og strengere krav til de ansatte). Samtidig er det en del «lettere» å unngå enn de andre hendelsene.
4. Jeg ville nesten satt opp **avoid** på denne hendelsen, da det er en såpass seriøs hendelse. Jeg føler det er verdt å ha noen ulemper (som kan fikses på andre måter), men ikke ha angrep fra utsiden. Problemet er at det kan være vanskelig å unngå dette for alltid, det kan skje feil ved software-oppgradering som ikke en ikke oppdager, eller ikke kan unngå. Derfor ville jeg brukt strategien **reduce** her. Det kan f.eks være å ha god rutine for patching av kontor-PCer og god oppfølging etter software-oppgradering.
5. **Reduce.** Det er egentlig ganske lett å redusere risikoen for at aksesspunkter feiler. Dette kan f.eks være rutinemessig sjekk på aksesspunktene og rutinemessig utskiftning av disse, eller plassere de steder hvor risikoen for naturødeleggelser er liten.

Oppgave 5:
Som jeg skrev litt i oppgave 4 kan en redusere risikoen for hendelse 3 ved å ha strengere krav til de ansatte og sparking av de som selger informasjon. Med strengere krav mener jeg altså bakgrunnssjekk av nytilsatte og kun la personer med lengre erfaring i virksomheten ha tilgang til sensitiv data. Ved sparking av ansatte vil terskelen for å selge informasjon være høyere blant de resterende ansatte. I tillegg kan en installere overvåkning på maskinene/brukarene til personene som har tilgang til dataen som kan bli solgt. Med disse tiltakene er det **sannsynligheten** som reduseres. Mottiltakene er **administrative og fysiske**.

Jeg skrev også litt om hvordan en kan redusere risikoen for at aksesspunkter feiler i forrige oppgave. Ved rutinemessig sjekk og utskiftning av aksesspunktene unngår en at det blir slitasje og skader på disse. I tillegg kan det være lurt å ha disse under bakken, hvor sannsynligheten for at de blir ødelagt på grunn av flom/regn/ras/storm osv er mindre. Nå var jo feilene som kunne skje en følge av softwarefeil i oppgradering, planlagt nedetid eller feilkonfigurering. Feil i oppgradering kan skje, men en løsning når feil oppstår er å ha ekstra aksesspunkter tilgjengelige som kan brukes dersom noen feiler. I tillegg bør det lages en enkel «rollback», slik at hvis det er en nyere software som det er noe galt med, kan en enkelt

rulle tilbake til forrige (samme med feilkonfigurering). Dette reduserer også **sannsynligheten** for at feilene oppstår. Tiltakene er **tekniske og fysiske.**