IN1020 - Datasikkerhet:
Løsningsforslag oppgaver gruppetime 5 (uke 39)

1. Kommunikasjon i datanettverk

   (a) Med http som protokoll går all kommunikasjon mellom Bruker og Server i klartekst, og hvem som helst (som har teknisk innsikt) kan lytte til kommunikasjonen.

   (b) Med sikker forbindelse mellom Bruker og WiFI-ruter forhindres Lytter1 i å fange opp kommunikasjonen. Alle de andre aktørene kan fremdeles se data i klartekst.

   (c) Kun Bruker og Server ser data de sender seg imellom i klartekst.

   (d) Kun Bruker og Server ser data de sender seg imellom i klartekst.

   (e) Hvis man bruker et usikret trådløst nettverk, kan Lytter1 (og alle de andre) se headere i datapakkene som sendes, f.eks. at Bruker har en «dialog» med serveren devilry.ifi.uio.no. Men kryptert trådløsforbindelse krypteres også headerne mellom Bruker og WiFi-ruter, og Lytter1 forhindres i å fange opp noe som helst fornuftig.

2. Bruk av HTTPS som sikkerhetstiltak:

   https med digitale sertifikater hindrer falske nøkler og falske tjenester. Den offentlige nøkkelen til en entitet inngår i en ubrutt kjede av sertifikater (med nøkler) som går god for hverandre, helt opp til det øverste nivået, rot-sertifikatet. Det er vanskelig for svindlere å generere og spre falske nøkkelpar til allerede etablerte tjenester.

   Digitale sertifikater hindrer ikke svindler i å opprette et gyldig domene, f.eks. sparebnak1.com, generere privat/offentlig nøkkelpar, og få dette signert av en tiltrodd sertifikatutsteder. Denne fremgangsmåten benyttes ofte i svindel-angrep.

   HTTPS bidrar altså **kun** til å krypterer kommunikasjonen og verifiserer motparten.

3. Tjenestenektangrep:

   (a) Tjenestenektangrep berører sikkerhetsmålet tilgjengelighet, i og med at tjenester som utsettes for angrepet blir utilgjengelig for den som har legitimt behov for tjenesten.

   (b) Å spre skadevaren løsepengevirus (kryptevirus/ransomware) er en vanlig angrepsform. Skadevarer virker ved å kryptere sentrale (ofte alle) filer i et IT-system (på f.eks. en datamaskin), med en for offeret ukjent krypteringsnøkkel, slik at systemet ikke fungerer og blir utilgjengelig. En annen form er tradisjonelle DDoS-angrep, som består i å "bombardere" tjenester med nettverktrafikk på en slik måte at tjenestene/serverne overbelastes og dermed ikke er tilgjengelige for andre . I DDoS-angrep bruker hackerne ofte såkalte *botnett*, som er nettverk av maskiner de har tatt kontroll over med f.eks. skadevare, uten av eier/bruker av maskinen er klar over det. Det skal som regel ganske store mengder samtidig nettverkstrafikk til for å kjøre en tjeneste i senk. En annen form for tjenestenektangrep (nevnt i læreboka) er f.eks. å bombardere en bruker med så mye søppel-epost (spam) at vedkommende ikke får tak i og lest epost som er reell.

   (c) Tiltak mot løsepengevirus er nevnt i løsningsforslag til oppgave 9 c) uke 2. Mot DDoS-angrep kan det være vanskelig å beskytte seg, men et tiltak er å ha tilstrekkelig robuste systemer, men f.eks. redundans, samt mulighet til avvis en del trafikk fra spesielle domener/IP-ranger

i f.eks. en brannmur. Internettleverandører kan også gjøre tiltak for å stanse denne typen skadelig trafikk på et nivå utenfor selve virksomheten som er målet for angrep. For søppel-epost kan spam-filtrering være et godt tiltak.

4. Se fasit til eksamensoppgaver 3.5 og 3.6 fra eksamenssettet m/fasit H22.

5. Se fasit til eksamensoppgaver 12 og 13 fra eksamenssettet m/fasit H20.

6. Case-oppgave:

   Mulige scenarier: Brukere havner på en falsk nettside (følger en falsk lenke, Googler bankens navn istedenfor å huske adressen el.). Bruker må selv vite forskjell på www.dnb.no, www.d-nb.com, d-nb.org, osv. TLS-basert autentisering er syntaktisk, og gir ikke brukeren bevis for at en nettside er ekte. Bruker benytter et åpent trådløst nett: DNS-forfalskning i et kompromittert eller falskt aksesspunkt kan også sende brukeren til en falsk nettside.

7. Case-oppgave:

   Nei. Kanksje brukeren har forlatt maskinen sin for å få en kaffe eller gå på toalettet? Om maksinen da ikke er låst kan en annen person bruke denne, utgi seg for å være brukeren og sende data til tjeneren. En annen mulighet er at brukerens datamaskin er infisert med en trojaner som genererer og sender data til serveren uten at brukeren vet om det (til tross for at brukeren fysisk sitter foran datamaskinen og aktivt utfører transaksjoner, f.eks. til en nettbank).

   Hvis sesjonen mellom klient og server ikke er beskyttet med TLS (Transport Layer Security) eller f.eks. VPN (Virtual Private Network), kan sesjonen også være et offer for et Man-in-the-middel-angrep (MITM). I et MITM-angrep bryter uvedkommende inn i kommunikasjonen og kan endre eller slette data utvekslet mellom klienten (brukerens datamaskin) og tjener