Oblig 2 Mats Andersen (matande), IN1020

1) Det boer tas saerlig hensyn til alle private opplysninger; alt vedroerende journaler, loggfoering, resepter, behandlingshistorikk, etc.

2) Konfidensialitet maa opprettholdes for aa beskytte pasientenes rett til privatliv. Reguleringer for dette staar sterkt i Norge og Europa, og maa etterfoelges for aa kunne i det hele drifte en klinikk. Ved et brudd paa konfidensialiteten kan sensitive personvernsopplysninger lekkes og brukes til diverse ondsinnede formaal. En trussel mot konfidensialiteten er utro-tjener-angrep (angrep fra innsiden).

Integritet er kanskje det viktigste sikkerhetsmaalet; du oensker ikke aa bli gitt feil blodtype, f.eks. Det finnes uendelig mange trusler mot integriteten; felles nevner er skadevare som endrer/korrupterer/sletter data. I verste fall kan dette foere til tap av liv, ved at det f.eks. blir gitt feil medisiner.

Tilgjengligheten soerger for at tjenestene er tilgjengelige; at nettsider er aapne, logger tilgjengelige, etc. Et trussel er DDoS-angrep. I utgangspunktet boer det foreligge backup-loesninger mot tilgjengelighetsangrep, men i vaar digitale tidsalder ... osv. I vaerste fall blir behandlinger utsatt.

3) Politiske aktoerer kan vaere ute etter aa skade en viktig person som gaar til klinikken, ved aa korruptere hans journal, eller paa en eller annen maate gjoere det slik at han blir gitt feil medisin. Klassiske profittjegere kan angripe IT-systemet vha. et loespengevirus; altsaa kryptere all data. Kanskje, i bytte mot penger, gir de den private dekrypteringsnoekkelen.

4) Konfidensialitet: God sikkerhetskultur for aa beskytte mot utro tjenere, og kryptering av all data, samt gode og sikre OAuth-loesninger med sykehusene, for trygg overlevering av journaler m.m.

Integritet: Brannmurer for aa beskytte mot inntrenging, antivirus for deteksjon, kanskje implementasjon av sjekksummer for aa sikre at data ikke endres av uautoriserte? Jeg er usikker paa om dette tiltaket er realistisk; kanhende det introduserer for mye kompleksitet.

Tilgjengelighet: *DDoS-mitigation*-systemer for aa forhindre DDoS-angrep, offline-backup-loesninger i tilfelle alt gaar skeis.

5) a) Det maa settes opp en ruter som tillater oversetting av IP-adresser (NAT-ruter). Denne tar den offentlige IP-adressen fra StokkeNet og bruker den som sin *wide area network* (WAN), men bruker private IP-adresser intern for disse syv datamaskinen som *local area network* (LAN). Deretter vil trafikk fra og til de interne IP-adressene oversettes av NAT-ruteren, naar det foregaar kommunikasjon paa internett.

b) Problemet med NAT-rutere er at de oversetter trafikken til kun en offentlig IP-adresse. Dermed er det noe komplisert aa koble sammen roentgenmaskinen med noeyaktig den ene datamaskinen som leverandoeren skal logge inn paa.

c) Jeg tror den mest brukervennlige loesningen her er aa sette opp en sikker “tunnel” fra leverandoeren til nettverket, vha. *virtual private network* (VPN). Det finnes mange kommersielle loesninger som tilbyr denne tjenesten. VPN tillater at leverandoeren kobler seg til LAN-nettverket, som om han var inne i det.

d) Foerst konverterer vi stoerrelsen paa kopien (1,4 GB) til megabits:

1.4 * 8 * 1024 = 11200 Mb

Deretter beregner vi tiden det vil ta aa overfoere:

11200 Mb / 50 MBps = 224s

Det vil ta ca. 224 sekunder aa overfoere denne sikkerhetskopien. Det er litt under 4 minutter.

6) a) Hvis IP-adressen er 172.16.1.1/26, faar vi ved CIDR-notasjonen at de 26 foerste bits er nettverksdelen. Dvs. at nettmasken (binaert) bestaar av 26 enere, og resten av den er 0.

11111111.11111111.11111111.11000000

Naar du konverterer dette til desimal, faar du 255.255.255.192. De tre foerste delene er lett aa konvertere, siden 255 er maksimalen. Dette er nettmasken.

Naar det gjelder broadcast-adressen: IP-adresser bestaar av fire oktetter (32 bits totalt). Hvis de 26 foerste bits er satt til nettverksdelen, har vi seks bits igjen. 2 opphoey i sjette er 64. Vi kan altsaa ha 64 adresser. Den siste adressen er satt av til broadcast-adressen. Siden vi starter paa null, er den siste den som ender paa 63. Dette gir oss at broadcast-adressen er 172.16.1.63.

b) Hvis nettverksadressen er den foerste, den som ender paa 0, og broadcast-adressen er den siste, den som ender paa 63, faar vi 64 minus to adresser, som er 62 adresser totalt. Vi kan altsaa ha 62 IP-adresser til fritt bruk.

7) Foerst og fremst maa gjestenettverket vaere sikkert, baade sett fra utsiden og innsiden. Med sistnevnte menes at ingen som er koblet paa gjestenettet, skal kunne kommet seg inn til det interne nettet. De maa mao. vaere to ulike nettverk. Med foerstnevnte menes at all trafikk er kryptert, og at pasientene maa koble seg paa vha. passord, -- eller kanskje en slags loesning som kun tillater pasienter aa bruke det? Eller kanskje de maa logge seg paa en portal med email, og godta en rekke vilkaar, osv. Det finnes mange muligheter her. Uansett boer ikke en gjest kunne vaere paakoblet til evig tid. Noen timer er nok per sesjon. Til sist vil jeg oppfordre klinikken til aa blokkere enkelte nettsider/tjenester, for aa filtrere ut upassende/unoedvendig og evt. skadelig innhold.

8) Phishing er alltid den mest effektive angrepsvektoren. Jeg ville rett og slett ha spoofet meg inn, kanskje ved aa sende en mail til resepsjonisten og si at jeg kommer paa vegne av en eller annen stroemleverandoer/IT-konsulent, for aa fikse noe som har med datamaskinene aa gjoere. Saa ville jeg ha moett opp og gjort en grei jobb som ikke vekker mistanke; men paa et tidspunkt ville jeg ha stukket en USB-pinne inn i resepsjonistens PC, overlevert en exploit, og derfra ha kommet meg inn paa regnskapssystemet, for aa endre beloepet paa regningen. I samme slengen ville jeg ha soerget for aa slette mailen jeg sendte, og -- hvis mulig -- kameraopptak.