



Trådløse nettverk øker i bruk som supplement til vanlige fysiske datanettverk eller som primært kommunikasjonsmedium for datatrafikk. Dette reiser en rekke sikkerhetsmessige problemstillinger som må håndteres hvis denne typen utstyr skal benyttes i helsesektoren. Dette informasjonsarket beskriver noen av problemstillingene og hvilke tiltak som bør vurderes ved innføring av slike nettverk.

BAKGRUNN

Målgruppe

Denne veiledningen er ikke ment som en fullstendig teknisk gjennomgang og implementasjonsveiledning for trådløse nettverk, til dette finnes det andre mer fullstendige oversikter, men sikter seg inn mot prosjektledere, beslutningstakere og andre som har behov for informasjon omkring trådløse nettverk. Veiledningen vil ha fokus på sikkerhetsutfordringer vedrørende bruk av trådløse nettverk. Fordeler og mer teknisk bruk av trådløse nettverk blir ikke berørt i vesentlig grad.

Hva menes med trådløse nettverk

I denne veiledning refererer dette til tradisjonelle datanettverk (av typen 802.11). Nettverk som for eksempel GSM eller bluetooth (som begge også kan sies å være trådløse nettverk) er ikke omtalt i denne veiledningen.

Noen egenskaper ved trådløse nettverk

- Det er et delt medium som betyr at kapasiteten blir delt mellom brukerne av det trådløse nettverket
- Den opplevde kapasiteten er ofte langt mindre enn teoretisk kapasitet for et trådløst nettverk
- Trådløse nettverk forutsetter som regel at det finnes et godt utbygd kabelbasert infrastruktur. En må sette opp en eller flere basestasjoner for å få et trådløst nettverk.
- Alle innenfor rekkevidden til et trådløst nettverk har i utgangspunkt tilgang til nettverket. Dvs. at trådløse nettverk ofte er tilgjengelige også utenfor det fysiske området hvor basestasjonen(e) er plassert.

BRUK AV TRÅDLØSE NETTVERK I HELSEVIRKSOMHETER

Det er flere forhold som gjør at bruk av trådløse nettverk i helsevirksomheter er spesiell i forhold til i andre typer virksomheter. Sikkerhetsmessige utfordringer bør alltid vurderes ved innføring av trådløse nett, men det blir ekstra viktige for helsevirksomheter.

Sensitiv informasjon

En helsevirksomhet har IT-systemer som inneholder sensitive (helse)opplysninger. Dette er opplysninger som ikke utenforstående må få

tilgang til. Det er derfor særdeles viktig at all IT-infrastruktur har god sikkerhet mot innsyn.

Lov- og regelverk

Helsevirksomheter er underlagt særskilte lovreguleringer som også omfatter krav til informasjonssikkerhet. Eksempel på dette er Helseregisterlovens § 16 som setter krav til sikring av konfidensialitet, integritet, tilgjengelighet og kvalitet.

Omdømme

Dersom det "glipper" i datasikkerheten på en helsevirksomhet kan dette gi et dårlig omdømme hvis det blir kjent. Dette kan skade tilliten både hos ansatte og brukere av helsevesenet. Særlig gjelder dette hendelser hvor personopplysninger har vært tilgjengelig for uautoriserte. Det har vært omtalt flere eksempler på slike hendelser hos andre typer virksomheter i riksmidia.

Tilgjengelighet kritisk

I en helsevirksomhet kan tilgang til informasjon

være særs kritisk i visse situasjoner. Dersom et trådløst datanettverk skal brukes mot kritiske systemer må en derfor sikre høy tilgjengelighet som ivaretar dette behovet.

Overføringskapasitet

Hos noen helsevirksomheter kan det være behov for stor overføringskapasitet. Eksempelvis vil bilder skape store datamengder som setter krav til god kapasitet i nettverket som kan være utfordrende for trådløse nett.

Viktige punkter å vurdere

Påkoblingssikkerhet

Den viktigste faktoren for sikkerheten er hvem som skal ha tilgang til det trådløse nettverket. Skal nettverket kun benyttes av autoriserte brukere, spesielle brukergrupper eller være åpent tilgjengelig?

Kryptering

Kryptering fyller flere funksjoner i et trådløst nettverk. Primært sikrer det at informasjon som sendes over det trådløse nettverket ikke kan avlyttes. Dette hindrer blant annet at passord og sensitiv informasjon som sendes ikke kommer

på avveie. I tillegg hindrer krypteringen at uautoriserte brukere kan utgi seg for å være autoriserte ved å stjele brukeridentiteten til påloggede brukere.

Tilgjengelighet

Hvilke behov for tilgjengelighet har løsningen? Skal løsningen benyttes for tidskritisk tilgang til helseinformasjon, eller er anvendelsen primært rettet mot informasjon og underholdning? Dette vil avgjøre hvilke tiltak som må iverksettes for å sikre at nettet er tilgjengelig.

Ulike typer anvendelser

Eksternt åpent nettverk

En enkel anvendelse av trådløse nettverk er som et åpent publikumsnettverk, med åpen eller lett tilgjengelig tilgang, og med eller uten tilgang til internett.

Flere helsevirksomheter vurderer eller har innført trådløse publikumssoner. Disse sonene kan gi pasienter og besøkende tilgang til informasjon fra helseforetaket, f.eks. kvalitetssikret helseinformasjon. Sonene kan også gi brukerne tilgang til internett. I så fall må grensene mellom helsevirksomhetens interne nett og internett være klare og sikres med tilstrekkelige sikkerhetsmekanismer.

Internt lukket nettverk

Trådløse nettverk kan også benyttes som et supplement eller til erstatning for helsevirksomhetens fysiske nettverk. Tjenestetilbudet vil da kunne være hele eller deler av det som kan nås via det fysiske nettverket. Avhengig av en trusselvurdering og de sikkerhetstiltak foretaket ønsker å innføre kan man velge å kun gjøre enkelte tjenester tilgjengelig, f.eks. vanlige kontorstøtteverktøy og internett-tilgang, mens tilgang til helseopplysninger kun gis fra det fysiske nettverket. Hvis sikkerhetstiltakene vurderes som tilstrekkelig kan man også gi tilgang til journaler og andre helseopplysninger.

SIKKERHETSTRUSLER OG RISIKOFAKTORER

Avlytting av nettverket

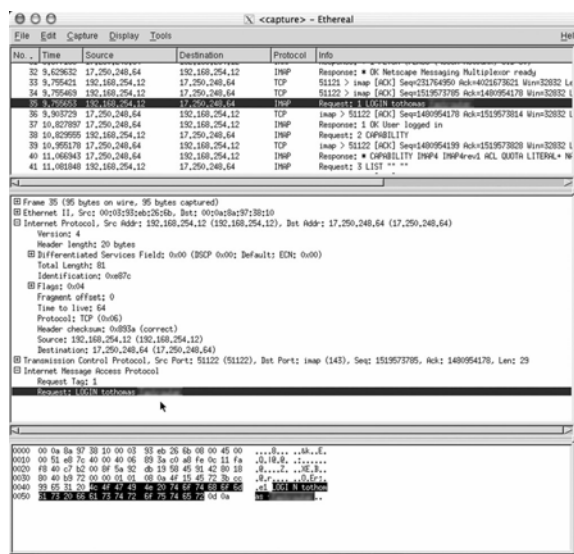
Mens tilgang til nettverket tidligere var begrenset til de som hadde tilgang til en fysisk nettverkskabel, gir trådløse nettverk større utfordringer. Radiosignalene som benyttes når utenfor virksomhetens egne vegger, til parkeringsplasser, publikumssoner eller naboer, og informasjonen som går over radiobølgene kan hvis det ikke er tatt forhåndsregler både avlyttes og misbrukes for å gi uvedkommende tilgang til nettverket. Dette kan være passord for pålogging (se figur) eller sensitive opplysninger. Mens fysiske nett i stadig større grad baserer seg på svitsjing – slik at andres nettverkstrafikk i liten grad er tilgjengelig fra det enkelte nettverkspunkt, kringkastes trådløs trafikk til alle.

Inntrenging

Det trådløse nettverket kan være en mulig inngangsport for angripere som vil komme inn i nettet. Siden nettet når utenfor bygningsmassen vil alminnelige fysiske sikkerhetstiltak være utilstrekkelig. Sikkerheten avhenger derfor av tilstrekkelige autentiseringsmekanismer som kan bekrefte identiteten til systemet/brukeren som prøver å koble seg til nettet.

Uautoriserte aksesspunkt

Også utro eller uvitende ansatte i egen organisasjon kan medvirke til at uvedkommende får tilgang ved å installere uautoriserte trådløse aksesspunkt som virksomhetens



Figur – Avlytting av passord over nettverket

nettverksansvarlige ikke kjenner til, og som kan være konfigurert på en åpen og usikker måte.

Tjenestenekt-angrep

Trådløse nettverk kan utsettes for ulike typer tjenestenekt-angrep. Noen typer kan avverges ved sikker autentisering av brukere slik at kun autoriserte brukere kan koble seg til nettverket, mens andre henger sammen med radioteknologien som brukes i trådløse nettverk. Radiobølger kan forstyrres, både med og uten hensikt og dermed gjøre nettverket utilgjengelig. Årsaken til dette kan være ulike støykilder som dårlig isolerte mikrobølgeovner o.l. og konsekvensen kan være at tilgang til kritiske fagsystemer er umulig.

TESTING AV TRÅDLØSE NETT

Systemadministratorer som ønsker å verifisere sine egne trådløse nettverk kan benytte en rekke verktøy for å utføre sikkerhetsrevisjoner. Noen tiltak kan være å scanne etter uautoriserte tilgangspunkter eller prøve å knekke tilgangskontrollen på eget nettverk. Flere verktøy kan være aktuelle for å bistå i denne prosessen – noen eksempel er:

- ❑ **NetStumbler:** Verktøy for Windows for å detektere trådløse nettverk. Kan benyttes til å oppdage nett (som sender SSID), måle signalstyrke (peile) og annet.
- ❑ **Kismet:** Lignende som NetStumbler, men kjører på Linux, og støtter også å avsløre skjulte nettverk (uten SSID

broadcast) ved å lytte passivt på nettverkstrafikken.

- ❑ **AirCrack:** Verktøy for Windows og Linux som gitt nok datatrafikk kan knekke WEP-nøkler.
- ❑ **AiroPeek NX:** Kommersielt verktøy for administrering og testing av trådløse nett. Funksjonalitet for å filtrere og studere nettverkspakker.
- ❑ **AP Skanner:** Gir en grafisk oversikt over de trådløse nettverkene i nærheten, viser kanaler og kollisjoner mellom nettverkene.
- ❑ **Fake AP:** I mindre grad et testverktøy, men genererer tusenvis av falske aksesspunkter, f.eks. for å skjule virksomhetens punkt blant en mengde falske.

Sukkerhuset
7489 Trondheim

TELEFON:
73 59 86 00

FAX:
73 59 86 11

E-POST:
firmapost@kith.no

KITH's webside!

Besøk oss på:

www.kith.no

SIKKERHETSTILTAK

Det eksisterer en rekke tiltak som kan implementeres for å sikre tilgangen til trådløse nettverk. Dette er ikke en fullstendig oversikt, for mer utfyllende informasjon henviser vi til nettsidene listet opp nedenfor.

Kryptering

To hovedstandarder for kryptering er etablert i markedet. Den første, WEP, er å anse som usikker. WPA regnes som sikrere så lenge konfigurasjonen gjøres riktig.

Autentisering

Mens WEP baserer seg på en delt kode som må spres til de som kobler seg til nettet, kan WPA benyttes mot andre autentiseringsmekanismer, også sentrale autentiseringsservere, og dermed bedre integreres i virksomhetens nettverksinfrastruktur. Mens WPA kan gi en god sikkerhet regnes tilgangsstyring gjennom VPN som det sikreste alternativet. Siden VPN også kan benyttes for hjemmekontorløsninger er det mulig å dele infrastrukturen. Det trådløse nettverket kan da holdes åpen for gjestetilgang, noe som også reduserer administrasjonsbehovet for det trådløse nettet.

Tjenestenekt-angrep

God autentisering kan redusere muligheten for at noen prøver seg på dette, men få/ingen tiltak vil beskytte mot fysiske angrep mot radiosignalet.

Annet

Aksesspunkt bør ikke ha fabrikkfigurert SSID – dette muliggjør identifisering av produsent og type, og gjerne dermed også fabrikkfigurerte passord.

Aksesspunktet kan plasseres bak et eget grensesnitt på ruter, slik at det er enkelt å "kvele" trafikken til og fra punktet ved behov. Ved å sperre for grensesnittet mot det trådløse nettverket er det da mulig å redusere trusselen fra uautoriserte brukere på nettverket til tilstanden er rettet opp.

KITH - INFORMASJONSSIKKERHET

Informasjonssikkerhet er et av hovedområdene hvor KITH har bred kompetanse til å bistå med blant annet følgende:

- ❑ Utarbeiding av strategi for informasjonssikkerhet, sikkerhetspolicy og sikkerhetsorganisering
- ❑ Etablering av styringssystem for informasjonssikkerhet (iht. Datatilsynets krav)
- ❑ Gjennomføre seminarer, workshops og opplæring
- ❑ Vurdering og innføring av (tekniske) sikkerhetsløsninger
- ❑ Gjennomføre risikovurderinger og sikkerhetsrevisjoner
- ❑ Sikkerhetsrådgivning og prosjektledelse/prosessledelse

Se KITH's webside (www.kith.no/informasjonnssikkerhet) for mer informasjon. KITH vil etter forespørsel kunne ta rådgivningsoppdrag innen informasjonssikkerhet - ta kontakt med fagansvarlig Bjarte Aksnes i KITH.

YTTTERLIGERE INFORMASJON

- ❑ **Wireless Security - Tom M. Thomas** – God og omfattende oversikt over trådløs sikkerhet:
<http://www.informit.com/articles/article.asp?p=177383>
- ❑ **The Unofficial 802.11 Security Web Page** – Lang rekke lenker til sikkerhetsinfo:
<http://www.drizzle.com/~aboba/IEEE/>

ANNET FRA KITH

- ❑ **Risikofokus**
På KITH's websider kan du også finne vårt halvårlige nyhetsbrev om trusler og utfordringer innenfor informasjonssikkerhet i helsesektoren.
- ❑ **Informasjonssikkerhet ved bruk av lommedatamaskiner – KITH-rapport 11/02**
Tilgjengelig fra KITH's websider