Sårbarheter i Internett

Aasmund Thuv, Ronny Windvik, Kjell Olav Nystuen og Tormod Sivertsen

Forsvarets forskningsinstitutt

17. mai 2007

FFI-rapport 2007/00903

1014

ISBN 978-82-464-1184-2

Emneord

Informasjonsteknologi

Informasjonsinfrastruktur

Informasjonssikkerhet

Internett

Sårbarhetsanalyse

Godkjent av

Håvard Fridheim	Prosjektleder
Jan Erik Torp	Avdelingssjef

Sammendrag

I de siste årene har Internett blitt et viktig kommunikasjonssystem for samfunnet, både som et kommunikasjonsmedium og som en plattform for stadig mer avanserte tjenester. Internett har blitt en viktig integrert del av mange virksomheters forretningsmodell, også de som anses å være samfunnskritiske. Private brukere har på samme måte i stor grad gjort seg avhengige av ulike typer internett-tjenester.

Målet med dette arbeidet er en sårbarhetsvurdering av Internett med et anvendelsessyn. Dette innebærer at det ses på sikkerhet og sårbarhet fra tjenesteanvenders ståsted, og ikke fra internettinfrastrukturleverandørenes ståsted. Videre konsekvenser innover i sluttbrukersystemer faller dog utenom. Det er lagt størst vekt på å gjøre en sårbarhetsvurdering av internettinfrastrukturen som er felles for de fleste tjenester, fremfor å vurdere trusler som rammer brukerne direkte som for eksempel virus og uønsket e-post.

Analysen har hatt fokus på villede handlinger og angrep, men ikke-villede handlinger dekkes også i noen grad. Arbeidet har primært vært en litteraturstudie, supplert gjennom møter med i hovedsak norske aktører innen offentlig forvaltning og næringslivet.

Sårbarhetsvurderingen er svært sammensatt, og det fremkommer ingen entydig konklusjon. På den ene siden viser våre funn at Internett er sårbart for mange allment kjente angrep. Eksempler på slike sårbarheter ligger i viktige funksjoner som ruting (BGP) og navnetjenesten (DNS). På den annen side er det til tross for disse og andre mer eller mindre kjente sårbarheter ikke dokumentert angrep mot Internett som har hatt omfattende konsekvenser i tid og omfang. Samtidig gjennomføres det kontinuerlig tiltak i infrastrukturen for å håndtere og redusere sårbarheter. Mye tyder derfor på at Internett virkelig er en robust infrastruktur, selv om dette på ingen måte er verifisert.

Avslutningsvis gis det kort noen tanker og refleksjoner om tiltak og muligheten for regulering av Internett.

English summary

In recent years, the Internet has become an important communication system for our society, both as a medium for communication and as a platform for increasingly advanced services. The Internet has become an important integrated part of the business models of many organizations, including those considered to be critical for society. Similarly, private users have made themselves dependent on different kinds of Internet services.

It is the intention of this report to give a vulnerability assessment of the Internet from a user point of view. This means that security and vulnerabilitiy are viewed through the lens of service users as opposed to service providers, although further consequences in end user systems are not considered. The primary aim has been to do a vulnerability assessment of the Internet infrastructure that is common for most services, in preference to studying threats that are carried over the infrastructure to affect users directly like viruses, worms and spam.

The assessment is focused on deliberate actions against the infrastructure, although unintentional actions are covered to some degree. The primary work has been done through a study of available literature, supplemented with meetings with mainly Norwegian actors in government administration and the private industry.

Our vulnerability assessment covers a wide range of complex topics, and no clear-cut conclusion is possible. On one hand, our results show that Internet is vulnerable with regards to many publicly known attacks. Vulnerabilities in important functions like routing (BGP) and name services (DNS) exemplify this. On the other hand, despite these and other less known vulnerabilities, there is a lack of documented attacks against the Internet with extensive consequences in time and scope. At the same time, measures are continuously being implemented in the infrastructure to handle and reduce vulnerabilities. This may imply that the Internet really is a robust infrastructure, although this has in no way been verified.

As an informal addendum we give some thoughts and reflections on Internet regulation and the possibility of recommending measures for making the Internet more robust.

Innhold

1 Innledning

Prosjektet “Beskyttelse av samfunnet 5” (BAS5) har hatt som tema utfordringer knyttet til sikkerhet og sårbarhet i nasjonal kritisk informasjonsinfrastruktur. Prosjektets innretning er relativt overordnet med et sterkt fokus på metoder, der utvikling av metoder for risiko- og sårbarhetsanalyse utgjør en sentral del av målsettingen. En klar utfordring i dette bildet er imidlertid at metodeverket skal omfatte systemer der ulike former for IKT-systemer og -nettverk inngår som viktige bidragsytere til systemenes effektivitet.

Som basis for dette arbeidet har det vært nødvendig i en viss detalj å gå inn i de konkrete teknologiske systemene som utgjør kjernen i den mer overordnende problemstillingen. Både for å oppnå en nødvendig forståelse av problemet, og for å kunne utprøve det metodeapparat som skulle utvikles, var det behov for konkrete casestudier.

Casestudiene omfattet anvendelsesorienterte IKT-systemer innen flere infrastrukturer som kraft og energi, helse og finans. Et fellestrekk ved alle disse er at de i en eller annen form igjen er avhengig av kommunikasjonssystemer for å fungere. Tidligere har man blant annet gjennom BAS2-prosjektet fått et meget godt innblikk i sikkerhet og sårbarhet i offentlige telekommunikasjonstjenester, som dannet et vesentlig bidrag til casestudiene. Den økende anvendelsen av Internett som kommunikasjons-bærer og som plattform for andre tjenester førte imidlertid også til et behov for å se nærmere på sårbarhet direkte i internettbaserte tjenester. Tidligere studier har i mindre grad reflektert denne utviklingen.

1.1 Formål

Som grunnlag for metodearbeider og tilhørende casestudier i BAS5-prosjektet ble det satt i gang et arbeid med en sårbarhetsvurdering av internettinfrastrukturen for brukere i Norge. Sårbarhets-vurderingen ser på de deler av Internett som ansees å være sentrale for produksjon av varer og leveranse av tjenester som betraktes som vitale for det moderne samfunn. Eksempler på dette kan være kraftforsyning eller finanstjenester. Arbeidet har derfor hatt et klart anvendelsessyn, det vil si at det ses på sikkerhet og sårbarhet fra tjenesteanvenders ståsted og ikke fra internettinfrastruktur-leverandørens ståsted. Denne rapporten beskriver de vurderingene og analyser som er foretatt og gir arbeidets konklusjon.

Som det vil fremgå av rapporten utgjør Internett i sin fulle bredde og dybde en svært kompleks masse i stadig endring. Å foreta en slik vurdering for det globale Internett vil ikke være realistisk. Vi søker derfor å avgrense dette til den norske delen av Internett, blant annet ved å bruke norske aktører som direkte kilder.

Tiltak for å redusere sårbarhet i Internett var ikke en del av formålet med rapporten. Med bakgrunn i arbeidet med rapporten og tidligere BAS-arbeider ble likevel det funnet hensiktsmessig å gi noen refleksjoner rundt tiltak og mulighet for regulering. Dette er lagt til et etterord.

1.2 Metode for arbeidet

Med utgangspunkt i ressursene som var satt av har det ikke vært mulig å gjøre en komplett analyse av sårbarheter på Internett. Det har også vært problematisk å få tilstrekkelig med informasjon fra aktørene. Med denne bakgrunn ble det valgt følgende fremgangsmåte for arbeidet:

- Utgangspunktet var tidligere BAS-arbeid, særlig innen området telekommunikasjon [23]
- Det ble gjennomført litteraturstudier av akademiske publikasjoner og offentlige utredninger
- Det har løpende blitt gjennomført diskusjoner om studien i prosjektrådet til BAS5
- Prosjektet har hatt samtaler med internettilbydere, Post- og teletilsynet i Norge, Post- och telestyrelsen i Sverige, SIS[1], Nasjonal sikkerhetsmyndighet og eiere av kritisk infrastruktur
- Prosjektet har hentet noen erfaringer ifm. en studietur til USA høsten 2005.

Legg merke til at internettinfrastrukturen er i stadig endring, og at denne rapporten gir en sårbarhetsvurdering for Internett slik det er tidlig i 2007.

1.3 Rapportens oppbygning

Kapittel 1, “Innledning”, beskriver rapportens formål og metode.

Kapittel 2, “Bakgrunn”, gir en kort historisk fremstilling av Internetts utvikling frem til i dag, beskriver anvendelsen av Internett for flere brukergrupper, ser på organisatorisk sårbarhet knyttet til internettbruk samt egenskaper og trender ved angrep over Internett.

Kapittel 3, “Sikkerhet og sårbarhet”, gir en introduksjon til grunnleggende informasjonssikkerhet og beskriver trusler, sårbarhetstyper og mulige årsaker til sårbarheter i datasystemer.

Kapittel 4, “Internettinfrastrukturen”, presenterer en lagdelt referansemodell over Internetts oppbygging og virkemåte, gir innblikk i de ulike aktørene som finnes på Internett og beskriver eksisterende regimer for administrasjon og regulering av Internett.

De neste kapitlene beskriver lagene i internettinfrastrukturen i større detalj, herunder ulike systemer og tjenester som har virke på lagene og deres sårbarheter.

Kapittel 5, “Brukeren”, beskriver de mest kjente trusler og farer som en bruker møter direkte ved bruk av Internett.

[1] Nå NORSIS.

Kapittel 6, “Applikasjonslaget”, omfatter systemer og tjenester som har direkte innholdsverdi for endebrukeren, herunder e-post, web og tjenestedistribusjon.

Kapittel 7, “Fundamentale tjenester”, omhandler de tjenester som er nødvendige for at Internett som kommunikasjonsinfrastruktur skal være anvendbar, herunder navnetjenesten (DNS) og tidstjenesten (NTP).

Kapittel 8, “Kommunikasjonsinfrastrukturen”, introduserer de laveste lagene i internettinfrastrukturen som frakter pakker fra kilde til destinasjon, herunder overføringslaget og transport- og aksessnettet.

Kapittel 9, “Overføringslaget”, omhandler kort de grunnleggende internettprotokollene og beskriver de protokoller og tjenester som står for overføring av trafikk mellom rutere i nettet, herunder ekstra-AS-ruting (BGP).

Kapittel 10, “Nettverksarkitektur for internettilbydere”, ser på nettverksstruktur og trender i utviklingen for denne.

Kapittel 11, “Aktørenes drift og styring av nett og tjenester”, går nærmere inn på kontroll og vedlikehold av nettverk og tjenester på tvers av de foregående lagene.

Kapittel 12, “Sikkerhetslaget”, fokuserer på mekanismer, løsninger og systemer for sikkerhet på tvers av de foregående lagene.

Kapittel 13, “Helhetsvurdering”, trekker sammen trådene til en helhetlig vurdering av sårbarheter i Internett.

Et etterord løfter deretter synet opp fra teknologien og diskuterer problemstillinger rundt regulering og tiltak samt erfaringer fra tidligere BAS-prosjekter.

Vedlegg A, “Forkortelser”, gir en liste over forkortelsene nevnt i rapporten.

Vedlegg B, “Begreper”, forklarer en del begreper som blir brukt i rapporten.

2 Bakgrunn

Opprinnelsen til det som i dag kalles Internett ble utformet i 1968 av det daværende Advanced Research Project Agency (ARPA). Dette var en virksomhet innenfor det amerikanske forsvarsdepartementet, som hadde ansvaret for å utvikle ny teknologi til militær bruk. Internett startet opp med 4 noder i drift i 1969, og i 1972 hadde Internett 15 noder i drift. De første nodene utenfor USA ble lagt til Kjeller (Norge) og London i 1973.

Det har blitt hevdet at Internett ble utviklet for å kunne ha et kommunikasjonsnett som selv etter en påkjenning fra et kjernefysisk angrep skulle kunne være overlevelsesdyktig. Denne forklaringen har imidlertid blitt tillagt mindre vekt av flere som den gang var involvert i utviklingen av nettet, og den største drivkraften bak nettet hevdes å ha vært muligheten for å kunne dele på bruken av kostbart datautstyr [32]. Likevel er det klart at robusthet var et viktig designmål for pakkesvitsjingen[2] som Internett er basert på.

Internett ble ikke utviklet som et sikkert nett, i den forstand at det skulle være sikkert mot ondsinnede aktører på nettverket. Sikkerheten lå i stedet i at antallet brukere av nettet var få og at disse kjente hverandre eller var under et felles sikkerhetsregime. Internett utviklet seg med tiden til å bli et datanett som knyttet mange universitets- og forskningsmiljøer sammen. Kommersialiseringen av Internett i begynnelsen av 90-årene, som skjøt fart ikke minst på grunn av World Wide Web, satte i gang en kolossal vekst i antall brukere tilknyttet nettet. Både offentlig forvaltning og private virksomheter så etter hvert Internett som et velegnet medium for ugradert, åpen kommunikasjon og informasjonsutveksling.

I dagens samfunn er Internett i økende utbredelse som kommunikasjonsmedium mellom enkeltpersoner og virksomheter. I Norge oppfattes nok Internett enda av mange som ”et sted” der man enkelt kan legge ut informasjon om egen virksomhet eller hente informasjon om andre. En ser nå imidlertid en klar utvikling mot at Internett i stadig større grad blir integrert i bedrifters elektroniske kommunikasjon med omverdenen. Dette gjelder også offentlig sektor, der Internett i stadig større omfang blir plattform for formidling av offentlige tjenestetilbud, som for eksempel innlevering av selvangivelse og behandling av byggesaker. Også for enkeltindividene er Internett blitt en viktig plattform for en rekke viktige tjenester, som dreier seg om hele spennet fra tradisjonelle kommunikasjonstjenester mellom mennesker til avanserte kombinasjoner av kommunikasjons-, transaksjons- og innholdstjenester.

Internett er dermed i ferd med å få posisjon som et viktig allemannseie på linje med telefonens posisjon i siste halvdel av forrige århundre. Internett i dag er dermed også ganske fjernt fra den opprinnelige ideen om Internett, til tross for at teknologien i det store og hele bygger på det samme. Dagens svært sammensatte infra- og tjenestestruktur bygger på at utviklingen de senere årene har vært drevet frem gjennom en nær rendyrket kommersiell utvikling, en utvikling som i stor grad påvirker egenskaper knyttet til anvendelse, sikkerhet og sårbarhet i tjenester og infrastruktur.

[2] Pakkesvitsjing innebærer at datapakker i teorien kan bruke alle mulige veier i nettverket for å komme fra en node til en annen.

2.1 Internett for privatpersoner

Internett har blitt og vil fremdeles i økende grad være en del av privatpersoners liv. For den voksne delen av samfunnet er dette i stor grad begrenset til bruk av praktiske internettjenester som nettbank, levering av selvangivelse, søknad om barnehageplass og informasjonssøk. For den unge delen av samfunnet viser undersøkelser at Internett har blitt et integrert kommunikasjonsverktøy [1]. Internett er for de unge dermed en viktig del av dagliglivet. Dette peker på en trend hvor Internett blir en integrert og svært viktig del av privatpersoners liv, især som et kommunikasjonsverktøy.

2.2 Internett i virksomheter

Internett har tradisjonelt vært benyttet til web, e-post og filoverføring. Dagens Internett benyttes også som en kommunikasjonstjeneste mellom de forskjellige delene av en bedrift, samt at det i større grad er åpnet for aksess til egne IKT-systemer over Internett for eksterne. En bedrift vil typisk ha åpnet sine IKT-systemer via Internett for kunder, samarbeidspartnere, leverandører og service-personell. Internett har med andre ord blitt en kritisk komponent for mange bedrifter.

Økonomi er en viktig faktor for hvorfor Internett i økende grad har blitt en kritisk komponent for bedriftene. Dette har vært særlig tydelig i finansbransjen, hvor for eksempel introduksjonen av nett-bank drastisk har påvirket den gamle måten å drive bank og forsikring på. Kundeforholdet mellom bank- og forsikringselskaper og deres kunder foregår nå over Internett, noe bankene sparer mye penger på. Flybransjen undergår også forandringer på grunn av dette, og en undersøkelse av 98 selskaper i denne bransjen viser at 28% av det globale billettsalget foregår over Internett [75]. Undersøkelser blant reisende viser også et ønske om å benytte dette mer i fremtiden [76]. I flere andre bransjer med kjøp og salg av tjenester ser en også endringer som følge av økt kundekontakt over Internett.

2.3 Internett i det offentlige

Arbeids- og administrasjonsdepartementet la i 2003 frem en strategi for IKT i offentlig sektor 2003-2005 [6]. Med det offentlige menes både statlig og kommunal virksomhet, og målet med strategien var å styrke lokal tjenesteutvikling gjennom enklere utveksling av data og tilretteleggelse av elektronisk signatur. Med andre ord, en strategi for løpende å kunne utnytte de mulighetene teknologi kan gi [6]. Sentralt i arbeidet var et eget organ som skal koordinere innføringen av elektronisk signatur, noe som krever et omfattende system for tillitshåndtering[3] mellom aktørene.

Regjeringen besluttet 17. juni 2004 at det skulle utarbeides en felles spesifikasjon for elektronisk ID, elektronisk signatur og konfidensialitet. Forenklet er dette en kravspesifikasjon for tillitshåndtering

[3] Se kapittel 12.

[52]. Beslutningen var motivert av potensialet som ligger i bruken av offentlige elektroniske tjenester, slik som innleveringer av søknader, selvangivelser, meldinger, rapportering, utveksling av dokumenter og oppslag i registre og databaser. I skrivende stund er det ni godkjente leverandører av såkalte kvalifiserte sertifikater, benyttet for elektronisk ID i Norge. Utstedere av kvalifiserte sertifikater skal følge reglene spesifisert i blant annet esignaturloven [22].

2.4 Organisatorisk sårbarhet

Virksomheter i det private og det offentlige vil i mange tilfeller organisere seg slik at de blir sårbare overfor et utfall av Internett. Stort sett baserer avhengigheten seg på behovet for kommunikasjon over Internett, innhenting av informasjon og realiseringen av ett logisk nett for flere fysisk atskilte lokasjoner.

Dagens moderne virksomheter er meget avhengige av e-post som et kommunikasjonsmedium mellom kunder, leverandører og partnere. Hvis en angriper klarer å hindre en virksomhet i å sende og motta e-post over et par uker, vil dette nok få alvorlige konsekvenser.

Innhenting av informasjon og bruken av elektronisk saksbehandling over Internett blir stadig en viktigere del for virksomhetene. For eksempel vil anbud legges ut på og tilbud leveres inn over Internett, og viktig informasjon fra kommuner publiseres på deres nettsider. En virksomhet som over en lengre periode hindres tilgang til Internett, mister fort informasjon som er viktig i dagens informasjonssamfunn.

De aller fleste virksomheter har i dag egen webside, noe som nå er forventet. I forbindelse med planlagte kjøp av produkter eller tjenester benyttes Internett i stor grad til å sammenlikne leverandører. En leverandør uten webside vil i så måte risikere å diskvalifisere seg selv som leverandør. En virksomhet som over en lengre periode hindres i å presentere sine produkter eller tjenester over Internett, vil utvilsomt kunne miste potensielle og eksisterende kunder. Et eksempel kan være at websidene til stadighet blir byttet ut med støtende innhold eller referanser til konkurrenter. Det er kanskje ikke på slike websider man ønsker å legge igjen kredittkortopplysninger eller levere søknader.

Virksomheters ønske om ett logisk eller virtuelt privat nett (VPN) over flere fysisk atskilte lokasjoner, introduserer en del utfordringer i forhold til viktige interne tjenester. Med fysisk atskilte lokasjoner menes blant annet avdelingskontor, hjemmekontor og ansatte på reise, og et VPN realiseres i stor grad over Internett. Organisatorisk vil mange velge en sentralisering av drift, og viktige tjenere plasseres naturlig samlet. Viktige interne tjenere inkluderer filtjenere, databaser, antivirustjenere, navnetjenere, webtjenere, domenekontrollere, katalogtjenere og tynnklienttjenere. Ved utfall av Internett vil ansatte ved avdelingskontor ikke være i stand til å hjelpe kundene, fordi ”dataen er nede”.

Et lengre utfall av Internett for en virksomhet vil med andre ord kunne få alvorlige økonomiske konsekvenser. Potensielle kunder vil neppe velge virksomheten som leverandør og eksisterende

kunder vil trolig velge andre leverandører grunnet treghet eller stans i saksbehandlingen. Et ustabilt IKT-system vil også gjøre ansatte meget frustrerte. I CSI/FBI sin årlige datakriminalitetsundersøkelse[4] i USA, rapporterte 17% av de i underkant av 500 respondentene at de har blitt utsatt for tilgjenglighetsangrep. Til sammen har disse tapt omtrent 26 millioner dollar på tilgjenglighetsangrepene i løpet av ett år [26]. Til sammenlikning ble det rapportert om et samlet tap på omtrent 6,7 millioner dollar på tyveri av laptoper. Merk at det eksisterer mange forskjellige modeller for å estimere økonomisk tap hvis kunder eller andre ikke når organisasjonens tjenester, eller hvis egne ansatte ikke får benyttet Internett. Hvis man ser på den årlige omsetningen til en stor nettbutikk og på hva en stor organisasjon taper hvis de ansatte ikke får gjort jobben sin, kan til og med 26 millioner doller årlig for 500 bedrifter virke lite.

2.5 Internett og kritisk infrastruktur

Presidenten i USA sitt IT-rådgivningsutvalg (President's Information Technology Advisory Committee) leverte i februar 2005 rapporten Cyber Security: A Crisis of Prioritization [63]. Rapporten beskriver hvordan IT-infrastrukturen i USA er avhengig av Internett. Dette gjelder ikke bare vanlige systemer som e-handel og web, men også i stor grad kritiske infrastrukturer som kraft, flykontroll (ATC[5]), finans, det militære og etterretning.

I mange tilfeller vil kritisk infrastruktur være tilknyttet Internett, fordi denne tjenesten er påkrevd. Dette kan for eksempel være informasjon om tog og fly er i rute, og for å kunne realisere slike typer tjenester må det være lagt opp til kommunikasjon fra det kritiske styringsnettet og ut på Internett. Spørsmålet en angriper da vil stille er nok om det er mulig å komme inn til det kritiske styringsnettet fra Internett.

I den norske Mørketallsundersøkelsen for 2006 rapporteres det om at 57% av virksomhetene som forvalter kritisk infrastruktur gir sine kunder tilgang til datasystemet utenfra [42]. Undersøkelsen viser også at virksomheter som forvalter kritisk infrastruktur i større grad enn andre virksomheter setter bort IT-driften.

I en artikkel om myter og fakta bak angrep mot SCADA-systemer[6] [12], beskrives noen datahendelser som direkte har påvirket kritiske systemer. Dette inkluderer blant annet ormen Slammer sin infiltrasjon i datasystemet til et atomkraftverk i Ohio. De viktigste årsakene til hendelsene er trolig at SCADA-systemer i større grad baseres på billig internetteknologi som TCP/IP, Windows og Unix, samtidig som de blir koblet direkte eller indirekte til Internett.

[4] "CSI/FBI Computer Crime and Security Survey", en samarbeidsrapport av Computer Security Institute og FBIs Computer Intrusion Squad.

[5] Air Traffic Control.

[6] Supervisory Control And Data Acquisition (SCADA), benyttes gjerne som betegnelse på et sentraltstyrt datasystem for overvåkning og kontroll av gjerne distribuerte prosessnett.

2.6 Karakteristikker ved angrep over Internett

Internett kan på mange måter sees på som et stort verdensomspennende system av systemer som utvikles, driftes, vedlikeholdes og styres av en rekke uavhengige aktører. Sammenliknet med et mindre datasystem under sentralisert kontroll har Internett derfor en rekke karakteristikker som påvirker muligheter for både angrep og vern mot angrep.

Den frie flyten av trafikk gjør det i prinsippet mulig å rette et angrep mot enhver maskin koblet til Internett fra en vilkårlig fysisk lokasjon. Ved å gå gjennom mellomliggende noder på veien, kan et angrep med utspring fra for eksempel USA gå gjennom Russland, Sveits, Polen, England og Norge for å villede før det går tilbake mot et mål i USA. Maskiner som er under lite oppsyn kan dermed benyttes som et springbrett for anonymiserte angrep over landegrensene mot systemer der det er større sannsynlighet for logging og overvåking.

For å lokalisere en angripers opprinnelige IP-adresse må et angrep spores bakover fra målmaskinen. Hver gang en angriper har benyttet en mellomliggende maskin, må nye administratorer kontaktes for å kunne følge sporet videre inn i et nytt system. I utgangspunktet er ingen pliktig til å assistere i en slik etterforskning, og det kan være særlig problematisk å spore angrep over landegrensene. Legg merke til at dette fort kan bli mer et organisatorisk, juridisk eller politisk problem, fremfor et teknologisk problem.

Tilgangen til verktøy som kan benyttes av angripere er stor. Verktøy som er enkle å bruke og som krever lite teknisk innsikt utvikles av noen få dyktige personer, som publiserer disse på kjente websider. Verktøyene spres hurtig til mangfoldige nysgjerrige som tester ut disse uten å tenke spesielt på konsekvensene av sine handlinger. Det holder dermed at én person finner en sårbarhet, for at den raskt kan bli forsøkt utnyttet mot mange systemer.

Mange verktøy gjør angrep til en automatisert prosess som kan søke gjennom et vilkårlig stort adresserom. En angriper i Asia kan for eksempel sette i gang angrepsforsøk mot alle IP-adresser til en internettilbyder i Norge, før han selv går på arbeid og lar egen datamaskin utføre angrepene alene. Systemer tilkoblet Internett er med andre ord under stadige angrepsforsøk, og vil bli truffet selv om systemene ikke inneholder noe en skulle tro er av interesse eller har verdi for andre enn systemeier. Ressurser som lagringskapasitet, regnekapasitet og nettverkskapasitet er et mål i seg selv, og et system på Internett vil angripes rett og slett fordi det eksisterer og er tilkoblet nettverket.

Eksempelvis kan Honeynet-prosjektet[7] nevnes. Prosjektet har som konsept å sette opp og overvåke usikre maskiner, for å samle inn informasjon om angrep og ondsinnet programvare. Erfaringer viser at selv maskiner som ikke er registert i navnetjenesten eller i søkemotorer også blir funnet og angrepet [81].

[7] `http://www.honeynet.org`

2.7 Trender

Alle systemer tilknyttet Internett vil på et eller annet tidspunkt være sårbare overfor angrep. Dette kan være alt fra et sikkerhetshull i en tjeneste til et sikkerhetshull i en avansert teksteditor, og i 2004 ble det til CERT/CC[8] rapportert om 3.780 sårbarheter, i 2005 5.590 sårbarheter og i 2006 8.064 sårbarheter [13]. Antall sårbarheter som blir kjent ser derfor ut til å være økende.

Tiden fra et sikkerhetshull blir kjent til noen prøver å utnytte dette er kort. I gjennomsnitt tar det 3 dager fra et sikkerhetshull blir kjent til første program for å utnytte dette dukker opp [79]. Samtidig tar det i gjennomsnitt 31 dager fra et sikkerhetshull blir kjent til det kommer en korrigerende oppdatering (patch) fra leverandøren, noe som gir et vindu på 28 dager hvor man er eksponert. Dette vinduet har blitt mindre siden 2005, hvor det i første halvdel av året var et vindu på 60 dager og siste halvdel et på 50 dager.

Å sikre seg ved å stenge tjenester eller linjer til Internett mens man venter på en oppdatering, er ikke realistisk med dagens krav til oppetid. Eksterne brukere av egne systemer, som for eksempel kunder, krever tilgang til tjenester fra Internett, og ansatte krever tilgang til Internett for å løse sine arbeidsoppgaver. Samtidig er det ikke slik at en oppdatering nødvendigvis bør installeres så fort som mulig [8]. En oppdatering kan virke mot sin hensikt ved at systemet blir mer sårbart eller ustabilt. Av den grunn venter mange administratorer med å installere oppdateringer, og eksponeringsvinduet blir i praksis større.

Trenden med et høyt antall publiserte sårbarheter kombinert med et stort tidsvindu hvor maskinen er sårbar, åpner dermed for at systemer er ubeskyttet mot angrep fra Internett over en relativt lang periode. Dette er tilfelle selv om korrigerende oppdateringer installeres med en gang de blir publisert. Sammen med en vridning mot flere rettede angrep motivert av økonomisk vinning, *"the shift from hacking for fame to hacking for fortune"* [80], stiller dette høye krav til virksomheters IKT-sikkerhet ved anvendelse av Internett og andre systemer som er åpne mot omverdenen.

Flere studier har forsøkt å kartlegge hvor dataangrep over Internett kommer fra. I studiene har det blitt plassert ut sensorer eller inntrengingsdeteksjonssystemer (IDS-er) hos organisasjoner, som automatisk rapporterer tilbake om mulige dataangrep og hvilke avsenderadresser som er forbundet med angrepene. Slike målinger kan imidlertid være misvisende på grunn av falske avsenderadresser og fjernstyring av overtatte mellommaskiner.

Symantec utarbeider for hvert halvår en rapport om sikkerhetstrender på Internett, basert på et stort sensornettverk med over 40.000 noder [80]. Rapporten viser at USA ligger på topp over landene hvor angrepene kommer fra med 31%. På de neste plassene følger Kina med 7%, UK med 6% og Tyskland med 5%.

[8] Computer Emergency Response Team Coordination Center, en del av det føderalt finansierte Software Engineering Institute ved Carnegie Mellon University.

Høsten 2000 startet EOS-tjenestene[9] i Norge samarbeidsprosjektet Varslingssystem for Digital Infrastruktur[10] (VDI), som senere ble gjort permanent under Nasjonal sikkerhetsmyndighet (NSM) i 2003. VDI er et system for å identifisere, sammenstille og varsle angrep over Internett, basert på data fra VDI-deltakernes[11] IKT-systemer. VDI utgir månedsrapporter hvor det rapporteres om sikkerhetshendelser og gis statistikk om forsøk på tilgjenglighetsangrep, ormer, innbruddsforsøk og kartleggingsforsøk. For desember 2006 [56] ble det registrert at 31% av innbruddsforsøkene kommer fra Norge, 29% fra USA og 9% fra Spania. I samme periode ble det for kartleggingsforsøk registrert at 47% kommer fra Norge, 11% fra USA og 4% fra Kina.

I sin kartlegging av internettrelaterte trusler hevder svenske Krisberedskapsmyndigheten at 46,3% av angrepene kommer fra Kina [43]. På andre plass følger USA med 12,3% og på de neste plassene Sverige med 9,9% og Norge med 6,5%.

Det er interessant at tallene fra NSM VDI viser at de fleste innbrudd og nesten 50% av kartleggingen mot norsk samfunnskritisk infrastruktur stammer fra Norge. En medvirkende faktor til dette kan være spredningsmekanismer i ormer som automatisk velger nære IP-adresser. En annen faktor kan være falske positiver som vil ha en bias mot norsk trafikk.

[9] Etterretnings-, overvåknings- og sikkerhetstjenestene, som i dag består av Etterretningstjenesten, Politiets sikkerhetstjeneste (PST) og Nasjonal sikkerhetsmyndighet (NSM).

[10] `http://www.nsm.stat.no/Arbeidsomrader/Internettsikkerhet-NorCERT/Internettsikkerhet---NorCERT/VDI/`

[11] VDI-deltakerne inkluderer offentlige etater og private bedrifter som samlet representerer samfunnskritisk infrastruktur.

3 Sikkerhet og sårbarhet

På et overordent plan handler sikkerhet og sårbarhet om å verne mot uønskede hendelser. Hva slags uønskede hendelser og årsaker som står i fokus varierer med metodikk, målsetning og fagmiljø. En kan løst gruppere de ulike tilnærmingene i to hovedretninger, hvor fokus enten er på hendelser som skyldes bevisst utførte og planlagte handlinger, eller på utilsiktede konsekvenser av ulykker, tilfeldigheter eller force majeure som ikke er utført med menneskelig overlegg. Førstnevnte betegnes villede handlinger eller hendelser, mens sistnevnte betegnes ikke-villede handlinger eller hendelser.

Dette skillet er på engelsk gjenspeilet i begrepene "safety" og "security", som er henholdsvis vern mot ikke-villede hendelser og vern mot villede hendelser. Dette blir allikevel ikke helt korrekt, da "safety"-begrepet vanligvis avgrenses til de ikke-villede hendelser som direkte påvirker helse og sikkerhet for mennesker og miljø. Uansett finnes det ingen tilsvarende norske begrep som skiller mellom disse to[12], og dette viser seg vanskelig å etablere da noen miljøer utelukkende bruker sikkerhet om det ene eller andre. Eksempler på dette er ROS-miljøet i industrien (safety) og vakt- og alarmselskaper (security).

Innen IKT-miljøene finnes en tilsvarende deling. Miljø med utspring i "system engineering" bruker ofte sikkerhet om tilgjengelighet, pålitelighet, stabilitet og tjenestekvalitet[13], mens miljø med bakgrunn fra blant annet kryptografi benytter sikkerhet om integritet, tilgjengelighet, konfidensialitet, autentisering og autorisasjon.

Selv med enighet om hva slags uønskede handlinger og hendelser sikkerhet skal verne mot, er det ulike meninger om hva som skal omfattes av begrepet. Er sikkerhet tiltak eller mekanismer, en tilstand som oppnås eller prosessen som leder frem til og opprettholder sikker tilstand? Tradisjonelt har datasikkerhetsmiljø hatt fokus på beskyttelsesmekanismer mot villede handlinger, noe som fremdeles er utbredt. Beskyttelse er imidlertid bare en fase i en større sikkerhetsprosess, eller syklus, som omfatter beskyttelse, deteksjon, reaksjon og gjenopprettelse av normal tilstand [31]. Det tradisjonelle fokuset har gjort at rutiner og metodikk i de tre sistnevnte fasene ikke er like bevisstgjorte og gjennomtenkte som for beskyttelsesfasen.

Denne rapporten har et fokus på villede handlinger, det vil si sikkerhet i konteksten "security". Det er dog verdt å merke seg at det til tider er betydelig overlapp mellom "safety" og "security", og at mange uønskede hendelser kan skyldes både villede og ikke-villede handlinger. I de tilfeller hvor mennesker lett kan påvirke systemet negativt med uvøren bruk, vil dette også tas med.

[12] En mulig definisjon med *trygghet* for "safety" og *sikring* for "security" er gitt i NOU 2006:6 "Når sikkerhet er viktigst" [62], men denne begrepsbruken er konstruert og lite tatt i bruk.

[13] Legg merke til at engelsk terminologi på dette feltet ikke er "safety", men andre begreper som "dependability" og "reliability".

3.1 Grunnleggende informasjonssikkerhet

Vi anser begrepene konfidensialitet, integritet og tilgjengelighet[14] som førende for vår tolkning av informasjonssikkerhet. Dette er uproblematisk når vi snakker om informasjon eller data, som ikke skal kunne leses av andre enn autoriserte brukere (konfidensialitet), skal bare kunne endres eller slettes av autoriserte brukere (integritet) og skal være tilgjengelig for autoriserte brukere (tilgjengelighet).

I nyere tid har man oppdaget at det er mer enn informasjon som skal vernes. Et system i seg selv og dets tjenester og ressurser som nettverkskapasitet, lagringskapasitet og regnekapasitet er også verneverdig. Dette har ofte ført til at begrepet informasjonssikkerhet utvides til å omfatte systemer, ressurser og tjenester, og at sikkerheten også her forsøkes beskrevet i lys av konfidensialitet, integritet og tilgjengelighet. Dette fører imidlertid frem til en noe kunstig begrepsbruk, som ikke er allment godtatt av fagmiljøene.

Vi velger å la konfidensialitet, integritet og tilgjengelighet dekke data og informasjon som behandles av et system, mens systemet i seg selv, deriblant tjenester og ressurser, dekkes av samlebegrepet systemkontroll[15]. Med dette menes at systemet skal være under full kontroll av autorisert driftsperonell til enhver tid. Ved å tolke "kontroll" i en vid forstand kan manglende tilgjengelighet, misbruk av ressurser og tjenester, ufrivillig kjøring av ondsinnet kode og andre uønskede hendelser tolkes som brudd på sikkerheten.

Både villede handlinger og uplanlagte hendelser kan lede til et brudd på sikkerheten. Det kan diskuteres om et sikkerhetsbrudd er en hendelse med uønskede konsekvenser, et brudd på en regel i skreven eller uskreven sikkerhetspolicy, traversering av en barriere eller forbigåelse av en sikkerhetsmekanisme. For vårt formål er det tilstrekkelig å si at et sikkerhetsbrudd har inntruffet når konfidensialitet, integritet, tilgjengelighet eller systemkontroll har blitt påvirket i en negativ forstand.

I beskrivelsen av sikkerhet benyttes hyppig begrepet "autorisert bruker". En bruker ansees som autorisert for en handling når han har implisitt eller eksplisitt tillatelse til å utføre handlingen. Generelt håndteres dette ved først å autentisere brukeren, som er å verifisere og dermed knytte en identitet til brukeren, og videre benytte tilgangskontrollmekanismer for å kontrollere at brukeren oppfører seg innenfor tillatte rammer. Således er korrekt identitetsverifikasjon en forutsetning for opprettholdelse av konfidensialitet, integritet, tilgjengelighet og systemkontroll.

3.2 Trusler

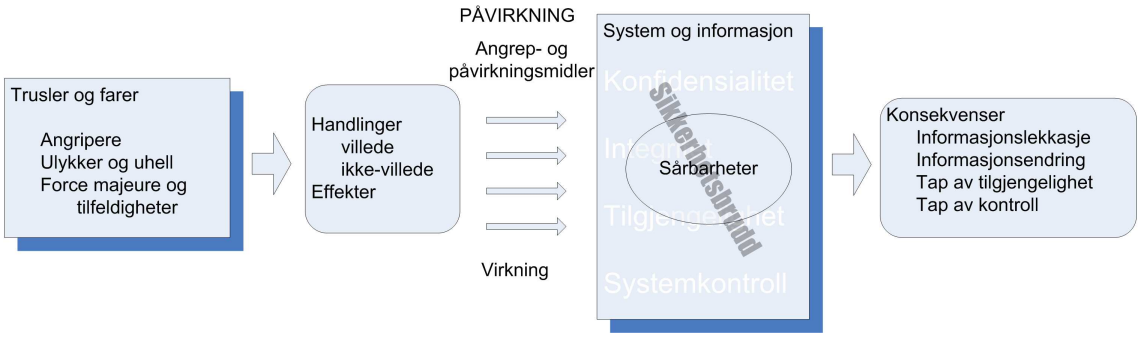
På Internett finnes det en rekke aktører med ulike intensjoner og med varierende evne til å angripe systemer og brukere. Aktører som bevisst går inn for å påvirke med villede handlinger kan potensielt

[14] "De tre sikkerhetspillarene" [77].

[15] Dette er gjort da en god inndeling tilsvarende konfidensialitet, integritet og tilgjengelighet ikke finnes for systemer, tjenester og ressurser.

skape problemer for enhver person som direkte eller indirekte er tilknyttet Internett. Samtidig kan også ikke-villede handlinger få konsekvenser som påvirker andre.

I figur 3.1 er det gjengitt en skisse som forsøker å illustrere dette. En angriper utfører villede handlinger med angrepsmidler for å utnytte en sårbarhet i et system, og et resultat kan være sikkerhetsbrudd med negative endringer i konfidensialitet, integritet, tilgjengelighet eller systemkontroll. Tilsvarende kan skje ved ulykker eller uhell hvor ikke-villede handlinger påvirker systemet. I den grad en potensiell angriper har intensjon og kapabilitet utgjør førstnevnte en trussel, mens sistnevnte betegner vi som farer. En tredje klasse årsaker fanger opp force majeure og andre tilfeldigheter som har negative virkninger på systemet.



Figur 3.1: Fra trussel til konsekvens.

Denne rapporten har et fokus på sårbarheter som kan utnyttes av angripere med villede handlinger, og til en viss grad sårbarheter som kan utløses ved uvøren bruk. Det er naturlig å ville søke informasjon om aktørene som angriper, det vil si de personer og grupper som faktisk utgjør trusselen. Dette er på ingen måte en triviell oppgave.

Det er vanlig å dele potensielle trusler opp i forskjellige grupper ut i fra for eksempel aktører eller kapabilitet og motiv. Et eksempel på dette er gitt i figur 3.2 på neste side. Slike oversikter kan være et godt utgangspunkt for en diskusjon, men vil alltid ha sine svakheter.

Et moment er fraværet av statistikk over trusler og angrep som kan brukes for å forutsi fremtidige rettede angrep. Dette skyldes blant annet at de vanligste informasjonskildene ved et vellykket eller mislykket angrep sier noe om hendelsesforløpet til angrepet, men meget lite om angriperen og dennes motiv. Direkte kilder er ofte brannmurlogger og andre systemlogger som for eksempel kan gi et klokkeslett med en IP-addresse, portnummer til en utnyttet tjeneste og observerbare endringer i filer eller annen informasjon. Utover dette kan man bare spekulere om aktør og motiv.

Noe mer informasjon kan utledes hvis man har muligheten til å sammenlikne data med andre bedrifter eller brukere. En større bedrift har mer datamateriale og kan se flere aspekter av et angrep, for eksempel om flere maskiner eller systemer ble angrepet og om spesielle områder ble forsøkt aksessert. Med dette kan man til en viss grad anta mer om mål og motiv. Overvåkningsnettverk

Trusselanalyse					
Motivasjon	**Virkemiddel**	**Aktører**	**Sannsynlighet**	**Konsekvens**	**Kommentarer**
			Svært sannsynlig Meget Sannsynlig Sannsynlig Lite Sannsynlig	Katastrofalt Kritisk Farlig Lite Farlig	
Utforskning, nysgjerrighet	logiske angrep	hackere kunder			Automatiske verktøy, manipulering av webinterface og databaser
Prestisje	logiske angrep sosiale angrep	hackere			Ukjente sårbarheter i infrastruktur, mangelfulle sikkerhetsrutiner
Hevn	logiske angrep fysiske angrep sosiale angrep	oppsagt ansatt forvirret ansatt andre tilknyttede			God kjennskap til interne rutiner og system, ikke tilbaketrukket autorisasjon, kjennskap til passord
Økonomisk (direkte eller via utpressing	logiske angrep sosiale angrep	organisert kriminalitet enkeltpersoner ansatte insidere			Manipulere databaser til egen fordel, uthenting av informasjon. Trusler om logiske angrep. Insidere med ekstra informasjon.
Publisitet (feks "hacktivisme")	logiske angrep fysiske angrep	politiske grupper terroristgrupper			Angrep som ikke trenger være "effektive" - feks defacing
Spre kaos og usikkerhet	fysiske angrep sosiale angrep logiske angrep	terroristgrupper fremmede stater			
Politiske/militære mål	logiske angrep fysiske angrep	terroristgrupper fremmede stater utilsiktet skade fra fremmede staters			Rettet angrep mot infrastruktur, angrep fra interne nettverk. Manipulering av applikasjonsdata.

Figur 3.2: Aktører og motiv.

som VDI-nettverket og Symantecs Deep Sight gir mer rom for å gjøre antakelser. Ved angrep som dekker flere mål og har stor utspredning, som ormer og phishingangrep, er intensjonen ved angrepet som oftest meget synlig. Dette hjelper dog lite hvis et angrep er lite, rettet og har mangfoldige konsekvenser.

Et annet moment er antallet potensielle angripere, som satt på spissen kan sies å være alle med en gyldig IP-adresse. Det faktum at et angrep mot hvem som helst kan utføres av enhver person med tilknytning til Internett fra sofakroken, gjør at sannsynligheten for å bli utsatt for et angrep er meget høy. Dette kan på mange måter ansees som en form for urettet støy, som alltid vil være til stede og som alle vil treffes av jevnlig.

Det som muligens er enda verre er at det ikke finnes grenser for hva en person eller et miljø kan mene er “morsomt”, og at verktøy og metoder er tilgjengelig hvis man har nok tid og kunnskap. Dette gjør at resonnementer som knytter sannsynlighet til motiv til en viss grad kan bryte sammen. Selv om det ikke er noen gevinst å hente ved å ta ned journalsystemet til et sykehus eller stanse togtrafikken, så kan det for noen være underholdene nok til å gjennomføres.

3.3 Sårbarheter i datasystemer

Et datasystem er en kompleks sammensetning av teknologi, programvare og mennesker. Gjennom et systems levetid vil sårbarheter knyttet til disse tre dimensjonene være til stede. Litt forenklet kan vi kalle disse fundamentale kategoriene for den fysiske verden, det logiske domenet og den menneskelige faktor, som gir opphav til fysiske, logiske og sosiale sårbarheter. En sårbarhet i denne konteksten kan kort beskrives som en svakhet ved systemet som muligjør uønskede endringer eller hendelser og som dermed gir systemet annerledes oppførsel enn tiltenkt ved systemets design og daglige virke.

Da vi ofte ser på datasystemer som samarbeider med andre datasystemer, eller delsystemer som er komponenter i større systemer, har vi også en gruppe sårbarheter som oppstår gjennom avhengigheter til ytre komponenter og systemer. Denne fjerde kategorien er en form for sårbarheter grunnet avhengigheter og vil kunne omfatte både fysiske, logiske og sosiale sårbarheter.

- **Fysiske sårbarheter.** Denne kategorien omfatter i første rekke sårbarheter grunnet materiellfeil, materiellsabotasje og manglende fysisk redundans. Virkemidler som fysisk maktbruk og elektronisk krigføring retter seg direkte mot denne type sårbarheter.
- **Logiske sårbarheter.** Denne kategorien omfatter sårbarheter realisert i programvare, herunder protokoller og tjenester samt logisk redundans. Angrepsmidler med virke primært i dette domenet kan være alt fra utnyttelse og bruk av allmenn tilgjengelig infrastruktur og kode som publiserte nettverksverktøy på Internett, til angrepskode og mer spesialskrevne verktøy. Alle komponenter som kjører programvare, og alle systemer som er helt eller delvis realisert eller styres via programvare, kan være sårbare i det logiske domenet.
- **Sosiale sårbarheter.** Denne kategorien dekker den menneskelige kontakten og innflytelsen på et datasystems utvikling, drift og vedlikehold, styring og bruk. Herunder faller krav til menneskelig kompetanse, håndtering av konfigurasjonsendringer, oppdateringer, uvøren bruk og organisatoriske aspekter. “Social engineering” er en type angrep som utnytter det menneskelige elementet direkte.
- **Avhengigheter.** Denne kategorien dekker sårbarheter som oppstår grunnet avhengigheter mellom systemet og andre systemer, eller avhengigheter innad i systemet. Dette kan være avhengigheter til helt andre infrastrukturer (strøm, vann), en tjenestes avhengighet av en annen tjeneste eller indre avhengigheter av spesielle noder i systemet grunnet arkitektur og design.

Et angrepsmiddel vil som oftest både kunne utnytte og ha effekter i flere av disse dimensjonene. For eksempel vil svake driftsrutiner grunnet menneskelig svikt kunne føre til åpne angrepsvektorer som utnyttes i det logiske domenet.

Vi vil i første rekke se på strukturelle og iboende sårbarheter i selve systemene som utgjør Internett, og i deres grensesnitt mot menneskene som bruker og drifter dem.

3.3.1 Når oppstår sårbarheter

Sårbarheter kan oppstå når som helst i et systems levetid, dette være seg under design og utvikling, ved drift og vedlikehold, under styring eller ved bruk av systemet. Det er ikke nødvendigvis noen sammenheng mellom når sårbarheter oppstår og når de avdekkes, og det siste kan skje lang tid etter at et system er i bruk. Det er derfor viktig med rutiner for vedlikehold og oppdatering av systemet. Kontinuerlig drift og vedlikehold er nødvendig for å opprettholde kvaliteten, funksjonaliteten og sikkerheten i et datasystem. Dette gjøres blant annet ved komponentovervåkning og komponentutbytting, konfigurasjonsendringer og oppdateringer av programvare.

Når leverandørene publiserer sine sikkerhetsoppdateringer, er det svært viktig å installere disse etter eventuelle stabilitetstester. Grunnen til dette er at angripere relativt enkelt kan finne hvilke sikkerhetshull som blir tettet ved å analysere systemet før og etter en sikkerhetsoppdatering. Sikkerhetshull blir i så måte avdekket gjennom sikkerhetsoppdateringer fra leverandørene, især de sikkerhetshull som kun én leverandør visste om. Kommersielle programmer som blant annet BinDiff[16] er laget for å avdekke forskjeller, her tetting av sikkerhetshull, mellom versjoner av programmer.

Avgjørelser tatt under design og utvikling kan påvirke potensialet for sårbarheter i et system. For eksempel kan et system bevisst bli designet med en sikkerhetsarkitektur hvor mye av sikkerheten legges hos klientene som er under kontroll av brukerne, fremfor hos tjenere under profesjonell og sentralisert kontroll. Det vil typisk være lettere for en angriper å ta over en klient administrert av en vanlig bruker enn en tjener under administrasjon av kyndig personell.

At konfigurasjonsmuligheter og avgjørelser med konsekvenser for sikkerheten flyttes til brukerne har blitt mer og mer vanlig. Brukerne er en uunngåelig del av ethvert datasystem, og selv til vanlige hjemmebrukere stilles det nå urealistiske forventninger om at informasjonssikkerhet skal forstås og håndteres på en god måte. For eksempel forventes det at det trådløse nettet skal krypteres, maskiner skal kjøre antivirusprogramvare, e-postvedlegg skal filtreres, personlige brannmurer skal være aktive, og usikre og ubrukte tjenester være avslått. Mange slike tiltak er utenfor kompetansen til både vanlige brukere og små bedrifter.

Samtidig som brukerne trekkes aktivt inn i sikkerhetsregimet, ser man ofte en konflikt mellom sikkerhet og funksjonalitet. Et system i bruk vil ha en rekke mulige konfigurasjoner, og vil gjerne bli styrt med fokus på korrekt og best mulig produksjon eller tjenesteleveranse. Konfigurasjonen vil dermed fort bli tilpasset økt funksjonalitet fremfor begrensende sikkerhet. Dette gjelder også datasystemer som kontorverktøy og administrasjonsverktøy som støtter bedriften i sitt virke, og som ofte har en stor brukermasse som ikke vil forstyrres av tunge sikkerhetsmekanismer i sitt daglige arbeid.

Det finnes ulike teorier om hva som er bakenforliggende årsaker til at usikre systemer stadig utvikles og benyttes. Både teknologiske, menneskelige og økonomiske forklaringer har blitt foreslått. De neste delkapitlene vil se nærmere på forklaringer ut i fra kompleksitet og økonomiske hensyn.

[16] `http://www.sabre-security.com`

3.3.2 Kompleksitet som bakenforliggende årsak

Kompleksitet er et problem som springer ut fra kombinasjonen av programvare, teknologi og den menneskelige faktor. Informasjonssystemer er nå blitt så store at oversiktlighet og forutsigbarhet ved uventede situasjoner har gått tapt. Systemene består av flere millioner linjer med kildekode, det eksisterer ofte svært mange mulige interaksjoner mellom komponenter, og de er vanskelige å få testet fullt ut [73]. Et vanlig program for kontordatamaskiner vil inneholde mange millioner logiske operasjoner og kombinasjoner av slike, der feil i kun én operasjon vil føre til feilfunksjon. Moderne dataprogrammer er nå så store og komplekse at dette også er et problem for programmereren. Programvarepålitelighet er derfor blitt et eget fagområde.

Komplekse systemer er med andre ord vanskelige å designe, implementere, konfigurere, bruke og forstå. Denne kompleksiteten kan benyttes av en angriper til å gi de IKT-baserte systemene bestemte logiske funksjoner som er uheldig for totalsystemets funksjonsevne. Det finnes en rekke ulike teknikker for slike angrep, og flere verktøy er tilgjengelig på Internett som kan hjelpe en inntrenger. Disse er til dels markedsført som sikkerhetsprodukter, fordi de også kan hjelpe en systemeier med å analysere egen sårbarhet. Med en kombinasjon av flere tilsvarende og andre teknikker vil det være mulig også å trenge seg igjennom forsvarsmekanismer som brannmurer og lignende.

3.3.3 Økonomiske hensyn som bakenforliggende årsaker

I en hverdag hvor økonomiske hensyn er sentrale, vil utvikling, implementasjon, drift og vedlikehold ha et fokus på funksjonalitet for minst mulig penger, noe som ofte går utover fordyrende sikkerhetstiltak. På utviklingssiden vil det være et press for å rulle ut produkter tidligst mulig, noe som forsterkes ved en viss ansvarsfraskrivelse fra produsentenes og tjenesteleverandørenes side. Dagens programvare kommer med lange lisensavtaler som fraskriver utvikler ethvert ansvar i forbindelse med bruk av programvaren. For eksempel vil ansvaret for tapene en ondsinnet orm påfører en bedrift ikke kunne plasseres hos utviklerbedriften av programvaren. Slike klausuler er ganske unike for IKT-bransjen i forhold til andre bransjer.

Med et fokus på økonomiske hensyn og lite ansvarlighet vil teknikker for å øke og beholde markedsandeler bli benyttet. Det vil være ønskelig at flest mulig benytter produktet, at brukerne ikke enkelt kan bytte til et annet produkt (lock-in) og at konkurrenter må betale dyre lisenser for å utvikle produkter som er kompatible med eller på en annen måte kan benytte ditt produkt. For å få til dette må produktene slippes på markedet i rett tid, og sikkerheten håndteres typisk i en senere versjon. Motivasjonen for å utvikle produkter er derfor å oppnå monopol i markedet, noe som også er gjeldende for utvikling av sikkerhetsprodukter. Dette fører naturlig til lite kompabilitet mellom slike produkter, noe som i liten grad er med på å øke sikkerheten i systemene.

I tillegg vil en vilkårlig organisasjon i stor grad håndtere risiko i forhold til egen vinning. Organisasjonen vil med andre ord utelate forbedringer som øker informasjonssikkerheten for fellesskapet hvis dette totalt sett innebærer merkostnader for organisasjonen. For eksempel er det vanlig å benytte

en brannmur til å filtrere ut ondsinnet trafikk inn til organisasjonen, men det er nok mindre vanlig å filtrere ut ondsinnet trafikk som går ut fra organisasjonen. Gevinsten ved å filtrere inngående trafikk er stor, da all ondsinnet trafikk treffer organisasjonen og kan potensielt gjøre stor skade. For utgående trafikk er imidlertid gevinsten liten, da trafikken treffer alle andre og kun marginalt medfører skade for organisasjonen selv. Dette prinsippet er i litteraturen ofte referert til som ”the Tragedy of the Commons” [33].

Dette har vært synlig ved forskjeller i policy overfor minibanksvindel hos amerikanske og visse europeiske banker. De amerikanske bankene hadde bevisbyrden hvis en kunde bestred en transaksjon, mens for de europeiske bankene var det motsatt. Førstnevnte styrket sikkerheten av egeninteresse, mens sistnevnte lot kundene ta byrden [4].

Etter at et system er tatt i bruk vil økonomiske hensyn spille inn på drift og vedlikehold av systemet. En virksomhet vil av økonomiske årsaker forsøke å minimalisere ressursene som det er behov for. Uten klare økonomiske verdier knyttet opp til datasystemene, vil virksomheten prioritere andre områder. Dette er for eksempel synliggjort ved forskjeller i sikkerhet for datasystemer i finansnæringen som forvalter store mengder penger med direkte påvirkning på nasjonal økonomi, og for datasystemer i helsesektoren som bidrar indirekte med støtte for en primærvirksomhet som kan være kritisk på individnivå, men ikke på nasjonalt nivå.

4 Internettinfrastrukturen

Hva Internett i dag egentlig er vil det kunne være ulike oppfatninger om. De fleste vil antagelig legge vekt på de tjenestene som Internett tilbyr formidlingen av gjennom en internettilbyder. Mange vil nok også fokusere mest på innholdet som er tilgjengelig via Internett, uten å være særlig opptatt av tjenestene disse tilbys gjennom. I denne rapporten er det infrastrukturen i Internett som vil stå mest i fokus, men det er imidlertid ikke helt trivielt å definere hva denne infrastrukturen er.

Fra grunnen av er Internett et nett for sammenknytting av datamaskiner slik at disse kan kommunisere med hverandre. I første omgang kan disse datamaskinene være plassert innenfor en bygning som for eksempel rommer en arbeidsplass. Ved en sammenkobling av flere datamaskiner i et nett vil hver datamaskin kunne få tilgang til informasjon fra alle de andre datamaskinene som er tilknyttet det samme nettet. Et slikt nett kalles gjerne et lokalnett.

Imidlertid vil det være behov for å kommunisere også ut over et slikt begrenset geografisk område. Dette realiseres ved å koble sammen datamaskiner i nett over større områder gjennom bruk av ytre kommunikasjonsnett. Internett er en stor mengde slike nettverk, som gjennom gjensidige avtaler igjen er koblet sammen for å gjøre deler av nettressursene tilgjengelige for hverandre. Disse nettene dekker nå store deler av verden. Internett eies og kontrolleres dermed av mange aktører i fellesskap, og nettet kjennetegnes av en svært liten grad av overordnet styring. Dette gjør Internett til et svært komplekst system.

Historisk sett har internettinfrastrukturen vært karakterisert ved en relativ enkel intelligens i forhold til det tradisjonelle telenettet. Filtrering og annen regulering av nettverket som utgjør Internett foregår typisk på høyere lag, mens mekanismene for pakkeleveranse fungerer uavhengig. Nettverket i Internett har frakt av pakker som hovedoppgave, og andre tjenesteleverandører benytter seg av denne basale pakkeleveransen når de selv utvikler tjenester. Tjenesteutvikling kan dermed skje i endene av nettverket, uten noen direkte sammenheng med utvikling og utvidelse av infrastrukturen for pakkeleveranse. Sikkerheten vil også bli ivaretatt i enden, da det ikke er noen garantier om beskyttelse mot avlytting eller manipulasjon av pakker i nettverket. Prinsippet med prosessering og kontroll i endene fremfor det underliggende kommunikasjonssystemet refereres til som ende-til-ende-prinsippet [69].

Dette er i kontrast til det eldre, tradisjonelle telenettet hvor utvikling og utvidelser av tjenester var sterkt bundet til infrastrukturen, og ble foretatt av teleoperatørene selv. Sikkerheten ble ivaretatt primært av infrastrukturen og ikke av endenodene. Internettinfrastrukturen muliggjør et mangfold av aktører som tjenesteleverandører og innovative drivere av utvikling, mens det tradisjonelle telenettet i større grad begrenser muligheten for utvikling til et lite sett av operatører. Dette er imidlertid ikke uten videre sammenlignbart sett i lys av nyere utvikling innen EKOM[17].

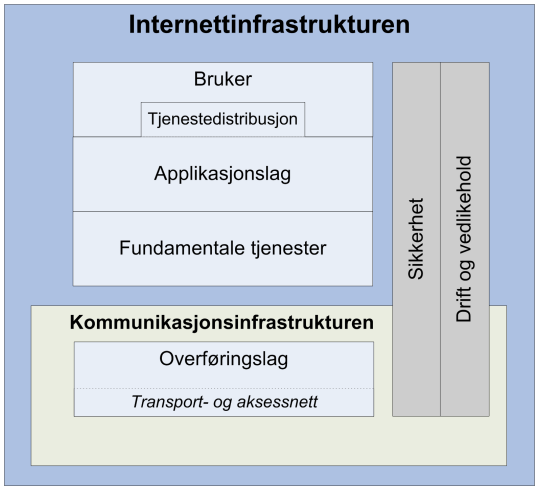
[17] Elektronisk kommunikasjon. All overføring av lyd, tekst, bilder og andre data. Omfatter også det som dekkes av det tidligere begrepet telekommunikasjon.

4.1 En referansemodell av Internett

Det finnes mange forskjellige utgangspunkt en kan bruke når en skal beskrive eller forklare Internetts oppbygning og virke. Et utgangspunkt er å bruke en "bottom-up"-tilnærming, hvor man begynner nederst med den underliggende kommunikasjonsinfrastrukeren, for så å arbeide seg oppover gjennom tjenestene som tilbys på høyere lag. En slik tilnærming brukes gjerne av miljø som arbeider med kommunikasjonsteknologi på et teknisk nivå.

Dette står i konstrast til en "top-down"-tilnærming, hvor man tar utgangspunkt i tjenestene som ligger nærmest brukeren, men man legger i dette synet mindre vekt på funksjoner i den laveste delen av kommunikasjonsinfrastrukturen. Et slikt utgangspunkt er mer vanlig for miljø hvor applikasjoner og grensesnittet mot brukeren er i fokus.

Vi velger i denne rapporten å følge en "top-down"-tilnærming. Som et hjelpemiddel introduserer vi en lagdelt modell der vi søker å illustrere Internett som et nettverk av funksjoner og tjenester.[18] Denne modellen dekker det vi kaller *internettinfrastrukturen*, som omfatter både brukere, organisatoriske aspekter og teknologi. Som en del av internettinfrastrukturen inngår *kommunikasjonsinfrastrukturen*, som dekker de nødvendige lagene for å frakte IP-pakker[19] fra kilde til destinasjon. Modellen består av horisontale og vertikale lag, og har sitt utspring i OSI-modellen. Denne modellen er imidlertid mer uformell da man ønsker å illustrere flere dimensjoner ved å dekomponere Internett i flere temaer. Se figur 4.1.



Figur 4.1: En lagvis modell av internettinfrastrukturen.

Under følger korte introduksjoner av hvert lag i modellen. Disse følges opp med egne beskrivelser senere i rapporten.

[18] Denne modellen er nøytral med tanke på retning.
[19] Se kapittel 9.

- **Brukere.** Disse består av sluttbrukere i form av enkeltindivider og virksomheter, som benytter tjenester fra applikasjonslaget basert på Internett. Brukere kan også være tilbydere av innholds- og transaksjonsstjenester, der Internett er benyttet som formidlingsmedium, men uten selv å tilby de underliggende tjenestene. Eksempel på slike er nettbanker eller nettbutikker.

- **Applikasjonslaget.** På dette laget finnes de internettbaserte tjenestene og protokollene som brukeren har direkte nytte av enten enkeltvis eller i kombinasjon. Eksempler er IP-telefoni (VoIP), web, e-post, filoverføring (FTP) og sikker fjerninnlogging (SSH).

- **Tjenestedistribusjonslaget.** Dette laget er delvis integrert i applikasjonslaget, og står for effektiv distribusjon av tjenester over Internett. Dette er nødvendig for blant annet å unngå flaskehalser.

- **Fundamentale tjenester.** På dette laget finner man fundamentale tjenester. Dette er tjenester som er av fundamental betydning for at Internett som kommunikasjonsinfrastruktur skal kunne anvendes, herunder navnetjenesten (DNS) og tidstjeneste (NTP).

- **Overføringslaget.** Dette laget er et sammenkoblet nett med IP-rutere, som til sammen muliggjør kommunikasjon av IP-pakker mellom geografisk adskilte datamaskiner.

- **Transport- og aksessnettet.** Dette laget omfatter de forskjellige teknologiene for å frakte IP-pakker på overføringslaget. Dette omfatter de laveste lagene i OSI-modellen, fra og med det fysiske laget med kabler og radiobærende overføringsmedium til og med lag 2.

- **Drifts- og vedlikeholdslaget.** Dette vertikale laget inneholder tjenester og protokoller for styring og vedlikehold av alle komponenter og tjenester i alle lag.

- **Sikkerhetslaget.** Dette vertikale laget inneholder sikkerhetstjenester og sikkerhetsprotokoller som er delvis integrert i de andre lagene, for eksempel sikker fjerninnlogging (SSH) som er en del av applikasjonslaget. Andre tjenester som tillitshåndtering dekker flere lag og må sees under ett.

Som vi ser av modellen omfatter kommunikasjonsinfrastrukturen overføringslaget og transport- og aksessnettet, samt deler av sikkerhetslaget og drifts- og vedlikeholdslaget. Internettinfrastrukturen omfatter alle lag.

4.2 Aktører på Internett

Tjenester i ulike nyanser på de ulike nivåene vil kunne ha mange leverandører. Aktørfloraen i dagens Internett er svært omfattende, med en blanding av store og små aktører. I dette kapittelet presenteres et utvalg av forskjellige aktører på Internett. Aktørene blir også forsøkt plassert i referansemodellen i figur 4.1 på forrige side.

- **Klienter.** Klienter representerer brukersiden av tjenestene som tilbys. En klient kan for eksempel være en e-postleser, webleser, IP-telefon eller chatklient. Klientene tilhører applikasjonslaget og benyttes av brukere.

- **Innholdsleverandører.** Denne gruppen besitter redaktøransvaret for innholdet som genereres via den gitte tjenesten. Innholdsleverandører plasseres her naturlig blant brukerne.

- **Verter.** Denne gruppen tilbyr infrastruktur til innholdsleverandører for at disse skal kunne presentere sine tjenester på Internett. Dette kan for eksempel være såkalte webhoteller som tilbyr maskin- og programvare nødvendig for å realisere den gitte tjenesten. En vert kan i tillegg til båndbredde og plass for eksempel tilby innholdsleverandørene backup.

- **Søkemotorer.** En søkemotor samler inn og indekserer sider på Internett. Forskjellige søkemotorer har ulike strategier for å presentere og rangere sidene opp mot søket som gis. En søkemotor kan således velge å filtrere ut sider basert på innhold, domenetilhørighet eller andre kriterier. Google og andre søkemotorer mottar jevnlig forespørsler om å fjerne sider, og i mange tilfeller gjør de også dette. Søkemotorer er en tjeneste som stort sett aksesseres via weblesere, og hører hjemme på applikasjonslaget.

- **Tjenestedistributører.** En tjenestedistributør står for en mangfoldiggjøring av en tilbudt tjeneste. Kundene til denne gruppen aktører er typisk store, kritiske eller populære organisasjoner. Eksempler kan være Microsoft, forskjellige meteorologiske websider under store orkaner og NASA som viser bilder fra Mars. En tjenestedistributør benytter ofte noen egenskaper vedrørende navneoppslagstjenesten for å sende klientene til den tjeneren som ansees som nærmest eller best.

- **Dynamisk navneoppslag.** Fremfor å benytte verter for å tilby websider, eksisterer det et marked hvor domenenavn kan kobles dynamisk til en maskin med skiftende IP-adresse. Aktørene i denne gruppen tilbyr navneoppslag for et domenenavn, som for eksempel `www.minprivatewebside.com`, slik at navnet hele tiden korresponderer med IP-adressen internettleverandøren dynamisk tilordner.

- **Internettilbydere.** En internettilbyder gir som et minimum sine kunder IP-tilgang til Internett og gjerne til en navnetjener som gjør navneoppslag på vegne av kundens maskiner. Aktører i denne gruppen velges å plasseres på overføringslaget og som tilbydere av navneoppslag.

- **Transportnettilbydere.** Transportnettilbydere eier kabler, fiber eller radiolinjer. Forretningsmodellen her er å leie ut båndbredde til internettilbydere. Aktørene i denne gruppen tilhører transportnettet.

4.3 Administrasjon og regulering

Internett som samfunnskritisk infrastruktur har vokst frem fra å være et tema i forsvarsforskning til å flyte inn i sivil forskning, for så å ende opp som en kommersiell infrastruktur for tjenester.

Denne utviklingen har gått gradvis, men har de siste ti årene akselerert kraftig. Tradisjonell telekommunikasjon har gjennom de siste 50 år i stor grad vært gjenstand for myndighetsregulering, selv om dette har blitt sterkt endret med forandringene i de sikkerhetspolitiske omgivelsene og den samtidige avmonopoliseringen av telesektoren tidlig på 90-tallet. Man ser nå at tjenestenett basert på tradisjonelle telenett og tjenestenettet Internett er i ferd med å konvergere. Regulatorisk er dette også søkt fanget opp gjennom den nye ekomloven[20] [21] med tilhørende forskrifter.

Det er imidlertid ikke enkelt å sammenlikne Internett og tradisjonell telekommunikasjon i en reguleringskontekst. Selv om Internett inneholder en kommunikasjonsinfrastruktur, vil Internett slik det er i ferd med å utvikles være mye mer enn dette. Dette setter store krav til videre utvikling av et ekomreguleringsregime.

Denne utviklingen viser en global trend som ikke er begrenset til Norge. I en rekke land og fora foregår det aktive debatter om hvordan konvergensen av Internett og telenett bør reguleres, spesielt med tanke på at telesektoren tradisjonelt er regulert kraftig mens Internett i det store og hele har vært fri for tilsyn.

4.3.1 Det internasjonale regimet

Internet Engineering Task Force (IETF) er en åpen organisasjon av i hovedsak frivillige som ønsker å bidra i arbeidet med utviklingen av teknologibasen til Internett. IETF har ingen direkte regulatorisk rolle for Internett, men er i stor grad førende for teknologien som benyttes på Internett ved å utvikle, vedlikeholde og markedsføre internettstandarder. Fra en sped start i 1986 med 21 deltakere har organisasjonen nå over tusen medlemmer. Det meste av arbeidet foregår i mindre grupper som ofte samarbeider via e-postlister. IETF håndterer blant annet de mange Request for Comments (RFC-ene), og IETFs egen misjon kan leses i RFC 3935[21].

Internet Architecture Board (IAB) er en del av IETF, med ansvar for langtidsplanlegging og koordinering på tvers av alle aktiviteter i IETF. IAB opparbeider seg på denne måten en god oversikt over aktivitetene i IETF, og bidrar til at langtidsperspektiver blir ivaretatt i IETF sine arbeider.

Internet Society (ISOC) er en internasjonal organisasjon med mål om å støtte den globale utviklingen til Internett. ISOC har siden 1992 fungert som den internasjonale organisasjonen for global koordinering og samarbeid om Internett, og noe av det viktigste ISOC håndterer er prosessen rundt ratifisering av reglene og prosedyrene for utviklingen av standarder for Internett. Standardene utvikles i hovedsak av IETF. På denne måten påvirker ikke ISOC direkte utviklingen av Internett og dets teknologi, men ISOC setter reglene for hvordan Internett skal utvikles. ISOC kan dermed sees på som en global regulatør for Internett, og har som medlemmer over 100 organisasjoner og over 20.000 enkeltpersoner.

[20] EKOM - Elektronisk kommunikasjon. All overføring av lyd, tekst, bilder og andre data. Omfatter også det som dekkes av det tidligere begrepet telekommunikasjon.

[21] `http://www.ietf.org/rfc/rfc3935.txt`

Internet Corporation for Assigned Names and Numbers (ICANN) har gjennom en MoU[22] med det amerikanske handelsdepartementet fått ansvaret for å globalt koordinere unike identifikatorer på Internett. Bakgrunnen for at amerikanske myndigheter har autoritet til gjøre dette skyldes at oppdrag og utvikling helt i fra begynnelsen av har skjedd på grunnlag av kontrakter fra amerikanske statlige organisasjoner eller myndigheter [25]. I prinsippet betyr kontrakten mellom amerikanske myndigheter og ICANN at sistnevnte har fått i oppgave å håndtere Internet Assigned Numbers Authority (IANA[23]). Dette inkluderer blant annet tildeling av toppnivå domenenavn (com, net, org, no, se og så videre) og at forespørsler om oppslag innenfor disse domenene gis nødvendig informasjon i jakten videre på riktig IP-adresse.

I forbindelse med tildeling av IP-adresser og AS-nummer[24], har IANA gitt denne oppgaven videre til fem forskjellige regionale registratorer. Disse kalles Regional Internet Registries (RIR) og dekker hver sin del av jordkloden. I skrivende stund opereres Internett med følgende RIR-er [67]:

- AfriNIC, Afrika
- APNIC, Asia Stillehavsregionen
- ARIN, Amerika
- LAPNIC, Latin-Amerika og Karibien
- RIPE NCC, Europa, Midt-Østen, Sentral-Asia

4.3.2 Det nasjonale regimet

Nasjonalt vil ekomloven være førende for regulering av Internett. Ekomloven har til formål å sikre alle brukere i Norge gode, rimelige og fremtidsrettede elektroniske kommunikasjonstjenester, samt sørge for bærekraftig konkurranse, næringsutvikling og innovasjon [21].

Post- og teletilsynet (PT) er underlagt Samferdselsdepartementet og har som oppgave å regulere og overvåke post- og telekommunikasjonsbransjen i Norge. Ekomloven gir PT rom for å utarbeide nærmere forskrifter vedrørende IT-sikkerhet hos leverandører av kommunikasjonstjenester.

Norid har fått ansvaret for å regulere og implementere no-domenet, samt at forespørsler om oppslag innenfor no-domenet gis nødvendig informasjon i jakten videre på riktig IP-adresse. Dette betyr at ethvert domene under no-domenet, slik som `ffi.no` og `dagbladet.no`, må være godkjent og registrert hos Norid. Tjenesten Norid tilbyr er regulert av en egen forskrift med PT som tilsynsmyndighet. Norid er en del av UNINETT og er en ikke-kommersiell aktør.

[22] Memorandum of Understanding.
[23] Legg merke til at IANA ikke er en organisasjon, men en funksjon.
[24] Se kapittel 9.

5 Brukeren

Hovedfokus for denne rapporten er sårbarheter i internettinfrastrukturen, og i mindre grad sårbarheter hos sluttbrukere som privatpersoner og virksomheter. Angrep rettet mot sluttbrukere som bæres av en fungerende internettinfrastruktur ligger således utenfor rapportens omfang. Dette er likevel en sannhet med modifikasjoner, da angrep mot sluttbrukere ofte utnytter sårbarheter i infrastrukturen i tillegg til sårbarheter hos sluttbrukeren.

Komponentene som utgjør infrastrukturen er til syvende og sist maskinvare som kjører programvare, om enn noe spesialisert programvare. Således er infrastrukturen sårbar for en rekke av de samme angrepsmidler en vanligvis retter mot sluttbrukere. Internettinfrastrukturen kan dermed være både bærer og mål for et angrep.

Vi velger derfor å beskrive en rekke trusler som den vanlige sluttbruker og driftspersonell av infrastrukturen må forholde seg til. Hovedfokuset vil være på ulike varianter av programvare skrevet med onde eller kriminelle hensikter kalt ondsinnet kode (malware). Av disse beskrives spionprogramvare, ormer og virus samt trojanere og bakdører. Vi vil også dekke andre relevante internettrusler som kartlegging og informasjonsinnsamling, tjenestenektsangrep, botnett, phishing og uønsket e-post.

5.1 Kartlegging og informasjonsinnsamling

Med kartlegging menes enhver form for aktivitet som har til hensikt å samle inn informasjon om et målsystem, en virksomhet eller en person. Som forberedelse til angrep er gjerne innsamling av informasjon gjennom åpne kilder et av de første skrittene. På Internett er det en rekke åpne kilder som kan benyttes for dette, deriblant søkemotorer, nyhetsgrupper, geolokasjon for å plassere en IP-adresse i et geografisk område og registreringsmyndighet for IP-adresser. Sistnevnte kan benyttes for å finne ut hvilke IP-adresser en virksomhet er tildelt.

Avanserte søk i søkemotorer på Internett, som for eksempel beskrevet i artikkelen Googling Up Password av Scott Granneman [28], kan benyttes relativt enkelt for å finne informasjon om målet. For eksempel vil man ved å skrive inn “site:offer.no passord filetype:xls”, få ut alle filer av typen Excel som innholder ordet “passord” hos `offer.no`. Dette kan gjøres uten at angriperen sender en eneste pakke til `offer.no`, da informasjonen allerede er samlet inn av søkemotoren ved et tidligere tidspunkt.

Det eksisterer nyhetsgrupper for ethvert tema, og stort sett er alle innlegg på nyhetsgrupper søkbare gjennom blant annet Google Groups[25]. Ved å søke etter for eksempel “@offer.no” vil man få ut nyhetsinnlegg assosiert med noen som har e-postadresse hos `offer.no`. Ved å kombinere “@offer.no” med andre utvalgte ord, kan en finne store mengder av informasjon.

[25] `http://groups.google.com`

I motsetning til slike passive teknikker finnes det også aktive teknikker for informasjonsinnsamling, som innebærer en form for kontakt med målet. En mye brukt teknikk, både for normale aktiviteter og som forberedelse for angrep, er skanning av tjenester hos målets maskiner (IP-adresser). Alle maskiner som er tilgjengelige på Internett vil sannsynligvis treffes av denne typen kartlegging. Hensikten med skanning kan være å finne alle tjenester (som web, e-post og navneoppslag) målet tilbyr utilsiktet eller med hensikt mot Internett. Hvis en av disse tjenestene er sårbare, vil en angriper kunne få tilgang til maskinen tjenesten kjøres på.

I tillegg til å benytte søkemotorer kan en angriper selv lete etter informasjon på målets websider. Ulike verktøy kan benyttes for å gjøre dette mer automatisk. For eksempel leter gratisverktøyet Strikeout[26] etter Word-dokumenter på en adresse som `www.offer.no`, og laster disse ned til angriperens maskin. Etter nedlasting leter Strikeout etter sporendringsinformasjon (track changes)[27] i dokumentene.

5.2 Overvåkning med spionprogramvare

Spionprogramvare (spyware) er programmer som er laget for overvåkning av brukere og datamaskiner uten brukerens samtykke og viten. Slik programvare er svært utbredt [74]. Formålet med spionprogramvare kan variere fra det som er klart ondsinnet til aktiviteter som ligger mer i gråsonen. Ondsinnet spionprogramvare samler ofte inn passord, kredittkortinformasjon, påloggingsinformasjon eller annen informasjon som kan brukes videre i kriminelle øyemed. I gråsonen finner vi ellers legitime applikasjoner, som i tillegg til sin egentlige funksjonalitet samler inn statistikk om bruksmønstre eller miljøet på maskinen. Ondsinnet spionprogramvare kan spres via generelle mekanismer som ormer eller virus, rettede angrep eller som påheng til annen programvare. Den mer legitime spionprogramvaren er ofte knyttet til en vanlig applikasjon.

En annen form for overvåkning er elementer i websider og e-post som varsler overvåkeren om når de blir lest. Et slikt element kan være en referanse eller link til et bilde på størrelsen med en piksel, lokalisert på en datamaskin kontrollert av overvåkeren. Når offeret leser e-posten eller surfer innom websiden, sendes automatisk en forespørsel til overvåkeren om å laste ned ”bildet”. Overvåkeren får da oversikt over når filen leses og hvilken maskin eller nett filen ble lest på. Slike teknikker kalles ofte for “web bugs”.

5.3 Datavirus og ormer

Begrepet datavirus i sin opprinnelige forstand brukes om en type ondsinnet kode som repliserer en mulig endret versjon av seg selv via eksekverbare filer eller spesielle områder på lagringsmedier.

[26] `http://lcamtuf.coredump.cx/strikeout`

[27] Sporendringer finner man under Verktøy/Tools i Word og dette benyttes når noen for eksempel skal kommentere et dokument.

Aktivering av et virus foregår ved at infiserte filer benyttes eller en starter fra infiserte lagringsmedier. Dette står i en viss kontrast til ormer, som er en type ondsinnet kode som kan spre seg over nettverk uten å ha behov for et annet program. En kan dermed trekke en viss parallell mellom datavirus og biologiske virus som begge trenger bærere, mens ormer likner mer på "selvstendige" plager som rotter. Mengden og variasjonene av ormer spredd i nettverk har økt dramatisk de siste årene, og enkelte har begynt å definere ormer som en type nettverksvirus da grensen mellom disse blir mer og mer uklar. Videre vil vi bruke virus som fellesbetegnelse for både virus og ormer.

Virus kan spre seg raskt. Hvis en sender et virus fra ett sted til 50 mottakere, der hver enkelt mottaker igjen sender det til 50 nye mottakere, vil viruset etter fem generasjoners spredning potensielt ha nådd frem til over 312 millioner brukere. Typisk for virusangrep er at de også rammer mange som nødvendigvis ikke trenger å være i en eventuell målgruppe for angrepet.

Oppdaterte antivirusprogrammer på klientmaskiner og tjenere er i dag et viktig forsvar mot trusselen fra virus. Problemene med virus vil ikke forsvinne i overskuelig fremtid, og nye typer og varianter dukker stadig opp. Eksisterende og fremtidige tjenestetilbydere på Internett må regne med at destruktive virus vil forsøke å stjele, endre eller slette data på deres tjenerne. Tilsvarende vil medbrakte laptoper kunne fungere som bærere, og dermed spre virus til maskiner på baksiden av eventuelle brannmurer. Virus spredd via e-post som ikke blir filtrert bort utgjør også en stor fare for maskiner på interne nettverk i en organisasjon, da disse kan aktiveres når vedlegget til e-posten åpnes.

5.4 Trojanere og bakdører

Trojanske hester er programmer som utgir seg eller blir utgitt for å ha fordelaktig funksjonalitet, men som i tillegg eller i stedet inneholder ondsinnet kode. En trojaner trenger typisk autorisasjon fra brukeren eller kallende prosesser for å kjøre, og villeder derfor om sin funksjonalitet. Når trojaneren er installert, kan den for eksempel vente på forhåndsdefinerte tidspunkt eller forhåndsdefinerte tilstander for senere aktivering. Ved aktivering vil den så kunne utføre ondsinnede handlinger som for eksempel sletting, endring eller lekking av informasjon, åpne maskinen opp for tilgang fra utsiden eller sette maskinen opp som en deltaker av et botnett.

Utviklerne av programvare kan legge inn bakdører i programvaren som brukerne ikke kjenner til. Dette kan gjøres av det firma som utvikler programmet eller av en enkelt programmerer som deltar i utviklingen. De som kjenner til de logiske funksjonene i en slik bakdør har blant annet mulighet til å komme seg inn på en datamaskin, uten å gå gjennom sikkerhetsmekanismer som passord eller andre autentiseringsmekanismer. Dette kan for eksempel være et problem der sentralt IT-personell har sluttet i sitt arbeid og gått over til en konkurrent.

5.5 Tjenestenektsangrep

Et alternativ til ondsinnet kode som direkte manipulerer informasjon på et system ved sletting, endring eller lekking av informasjonen er tjenestenektsangrep (DoS-angrep[28]). Slike angrep har som mål å påvirke systemressurser som nettverksbåndbredde, regnekraft og lagringskapasitet fremfor å manipulere systemets informasjon. Et angrep mot nettverksbåndbredden til et system kan for eksempel bestå av å sende store mengder trafikk til målet slik at båndbredden brukes opp, mens et angrep mot regnekraft kan være å få et målsystem til å bruke prosessortid på andre oppgaver enn de som er opprinnelig tiltenkt. Dette kan i visse tilfeller føre til at maskinen blir meget treg, og slutter å reagere på inndata fra mus eller tastatur. Angrep mot minne eller harddisk kan bestå av å få en maskin til å sette av plass til så store datamengder at lite ressurser er igjen til andre programmer.

Flere store nettsteder på Internett er blitt utsatt for det som kalles distribuerte tjenestenektsangrep (DDoS-angrep[29]). Dette innebærer at angriperne bruker flere datamaskiner til samtidig å sende store mengder forespørsler mot datamaskinene og tjenestene de ønsker å angripe. Dette fører til at de angrepne datamaskinene i verste fall bryter sammen, som igjen fører til tap av tjeneste-tilgjengelighet.

5.6 Botnett

Kompromitterte maskiner kan logisk kobles sammen og styres som en sammensatt enhet. Slike nettverk av kompromitterte maskiner kalles ofte botnett[30] [24], og brukes i stor grad til å sende ut uønsket e-post og utføre tjenestenektsangrep. For å kunne motta ordre vil en agent (bot) typisk koble seg opp mot en IRC-tjener[31] på Internett, hvor den venter på kommandoer. Angriperen kontrollerer agentene ved å sende kommandoer til IRC-tjeneren, for eksempel “send denne e-posten til denne listen med e-postadresser”.

Symantec observerte i gjennomsnitt 57.717 aktive maskiner i botnett i første halvår 2006 [79]. I løpet av denne perioden ble 4.696.903 unike maskiner identifisert som aktive på et eller annet tidspunkt.

5.7 Uønsket e-post

Uønsket e-post (spam) dekker e-post som sendes ut til et stort antall mottakere uten deres samtykke, ofte med et tilbud om en forretningshandel. Handelen kan omfatte alt fra kjøp som fremstilles som gunstige til rene svindelforsøk. En betydelig mengde av e-posten som sendes i dag antas å være slik e-post, og informasjonssikkerhetsselskapet Comendo estimerer i sin årlige sikkerhetsrapport at

[28] DoS: Denial of Service.
[29] DDoS: Distributed Denial-of-Service.
[30] Utspring fra ordet “robot”.
[31] IRC: Internet Relay Chat; et chat-system som tilbyr sanntidskommunikasjon.

i gjennomsnitt var 82,4% av all e-post av denne typen i 2006 [14]. Tilsvarende tall for 2005 var 84,6% og for 2004 58,5%. Estimert gjennomsnitt for 2007 er 86%.

Slike estimater bør dog ikke aksepteres uten reservasjoner. Symantec estimerer i sin trusselrapport om Internett for første halvdel 2006 at 54% av all e-post var uønsket e-post [79]. Årsaken til denne store estimatsforskjellen er trolig metodene og datagrunnlaget som benyttes. Vanligvis tas det utgangspunkt i et større nettverk som monitoreres, og mengdene med uønsket e-post estimeres på bakgrunn av målinger i disse. Forskjellige nettverk ser ulike mengder med uønsket e-post og programmene som klassifiserer e-postene er trolig heller ikke helt enige om hva som er uønsket e-post.

Den økonomiske motivasjonen som ligger til grunn for en avsender av uønsket e-post gjør at problemet neppe vil forsvinne med det første. Fordi kostnadene for utsendelse er tilnærmet null med liten risiko, og det alltid er noen som svarer med fullt navn og kredittkortinformasjon, vil utsendelse av uønsket e-post i de aller fleste tilfeller lønne seg for avsender. Det er tvilsomt at tekniske løsninger vil stoppe problemet, selv om ulike filtreringsmekanismer hos mottaker i mange tilfeller i det minste gjør problemet mindre synlig for sluttbrukeren.

Et resultat av problemene rundt uønsket e-post kan være en fremtidig sterk reduksjon i tilliten og bruken av e-post som elektronisk kommunikasjon. En kan dog spekulere i om dette i så fall allerede burde ha skjedd. Det er for tiden mye aktivitet for å håndtere problemet, men det er fortsatt få effektive løsninger som angriper roten av problemet, avsenders økonomiske gevinst.

5.8 Phishing

Begrepet phishing dekker en viss type forsøk på å lure ut sensitiv informasjon fra intetanende personer. Phishing krever ikke at ondsinnet kode kjører på målmaskinen, men baserer seg på at personer vil følge instrukser mottatt via tilsynelatende reelle og autentiske e-poster og internettsider. Et typisk eksempel er når en person mottar en e-post tilsynelatende fra sin bank, og blir bedt om å besøke en internettside hvor informasjon om kredittkort må oppgis.

For desember 2006 ble det rapportert inn 23.787 unike phishingforsøk til Anti-Phishing Working Group [5]. Til sammenlikning ble det i desember 2004 rapportert inn 1.707 unike forsøk og i desember 2005 15.244 unike forsøk.

Noen definerer også phishing til å være oppkjøp av domenenavn som er varianter av mer kjente og brukte domenenavn for å lure til seg sensitiv data fra brukerne. For eksempel kan en angriper kjøpe opp domenet `netbank.no` og sette opp en webtjener som likner på webtjeneren til `nettbank.no`. Personer som ved en feil taster `www.netbank.no` i stedet for `www.nettbank.no`, kommer da til angripers side.

6 Applikasjonslaget

Applikasjonslaget er det øverste teknologiske laget i modellen beskrevet i kapittel 4. Informasjonsinnholdet her transporteres av lavere lag og består av formatert innhold som behandles av applikasjoner.

Kapittelet tar for seg e-post, web og innholdsdistribusjon. Andre viktige tema på dette laget, som for eksempel filoverføring, fjernstyring og telefoni, er ikke behandlet separat.

6.1 E-post

E-post brukes gjerne som en fellesbetegnelse på flere elektroniske meldingssystem basert på "store and forward". Med "store and forward" menes at e-post transporteres via mellomnoder som lagrer og sender videre til neste node. Per i dag fungerer også e-post som et "pull"-system, der meldinger først leveres når en brukerapplikasjon tar kontakt med en tjener og ber om nye meldinger. Begge disse egenskapene står i motsetning til lynmeldinger (instant messages) som typisk blir levert direkte mellom brukerapplikasjoner i sanntid.

I dag brukes begrepet e-post vanligvis om meldingssystemet basert på internettprotokollene, men det finnes likevel flere proprietære system med egne meldingsutvekslingsstandarder. Disse brukes typisk i interne nett, men de fleste implementasjoner av disse har også funksjonalitet for å sende og motta e-post basert på internettprotokollene. Det er internettprotokollene som vil bli behandlet her.

6.1.1 Protokoller

Mange protokoller og standarder er involvert når en sender en enkelt e-post. Den sentrale protokollen er SMTP (Simple Mail Transfer Protocol), som står for transport av meldinger mellom noder. ESMTP er er en utvidelse til SMTP som først og fremst gir en standard måte å angi utvidelser og kapabiliteter til SMTP på, for eksempel for autentisering, kryptert transport, 8-bit transport, leveringsrapporter og så videre.

Det basale formatet på en e-postmelding er definert i den første SMTP-standarden, men omtrent alle meldinger blir nå sendt i henhold til MIME-standarden (Multipurpose Internet Mail Extensions). Dette muligjør vedlegg av vilkårlig type og støtter flere tegnsett enn det opprinnelige 7-bit ASCII.

Utover lokal konfigurasjon av klienter og tjenere inneholder DNS-hierakiet all nødvendig adresseinformasjon for e-post. DNS har et eget felt (MX-feltet) som angir hvilken maskin en melding til et gitt domene skal sendes til, og videre er en også avhengig av andre DNS-felt for å finne IP-adressen til denne maskinen.

For å hente e-post fra en tjener til en brukerapplikasjon brukes vanligvis POP3 (Post Office Protocol) eller IMAP4 (Internet Message Access Protocol). POP er opprinnelig tenkt for klienter uten kontinuerlig nettverkstilgang, og er en forholdvis rudimentær protokoll som stort sett bare kan hente all

tilgjengelig e-post til en bruker og kun i mindre grad kontrollere hva som skal hentes og hva som forstatt skal lagres på tjener. Opprinnelig benyttet POP brukerautentisering med klartekstpassord, og dette er ennå mye i bruk til tross for at det er standardisert sterkere autentiseringsmekanismer som tillegg til protokollen. Den ene, APOP (Authenticated POP), gir autentisert innlogging mens den andre, POP over TLS, gir autentisering i tillegg til transportbeskyttelse.

IMAP er en mer omfattende protokoll, som er laget både for å kunne hente e-post til lokal klient (som POP) og for å kunne gi en klient funksjonell tilgang til e-post som forblir lagret på tjener. Protokollen støtter tjenermapper, flere brukere mot samme e-postkonto, søk på tjener, henting av enkeltvedlegg og tilstand for meldinger (lest, besvart og så videre).

SMTP, POP og IMAP går alle over TCP-forbindelser. For SMTP og POP3 opprettes disse ved behov, mens IMAP typisk har en stående TCP-forbindelse så lenge brukeren har e-postklienten åpen. I stedet for å bruke SMTP og POP eller IMAP har det også blitt vanlig å bruke et webgrensesnitt mot e-postkonto.

I motsetning til en del andre meldingssystem er ikke lokal håndtering av e-post hos sluttbruker standardisert. Hvordan e-post arkiveres og lagres er dermed avhengig av brukerens e-postklient.

6.1.2 Forløp

Et typisk forløp ved sending og mottak starter med at brukeren forbereder en melding i sin lokale e-postklient. Internt består denne av to deler, meldingshode og meldingskropp. Meldingskroppen består av selve e-postinnholdet mens meldingshodet inneholder informasjon om avsender, mottaker, dato og emne. I tillegg kan e-posten inneholde vilkårlige vedlegg, formatet på disse er beskrevet i MIME-standarden.

Klienten sender denne e-posten med SMTP til brukerens lokale e-posttjener (MTA[32]). Den lokale MTA-en bruker DNS for å gjøre et oppslag på domenenavnet i mottakeradressen. Et eget felt i DNS (MX-feltet) lister i prioritert rekkefølge hvilke maskiner som mottar e-post for det gitte domenet. Den lokale MTA-en kontakter så en tilgjengelig e-posttjener for mottakerdomenet og bruker SMTP for å levere meldingen videre. Denne maskinen kan enten selv være mottakerens e-postmottak (MDA[33]), eller så er den ansvarlig for å levere meldingen til den. Til slutt kobler mottaker seg til sin lokale MDA og laster ned e-post med POP eller IMAP.

Flere unntak finnes fra dette forløpet. Dersom en organisasjon har et annet internt e-postsystem vil eksterne meldinger først bli sendt til en internettgateway som konverterer til riktig format og deretter sender videre. For intern e-post vil en da ikke benytte internettprotokollene i det hele tatt. Det har også blitt mer og mer vanlig at en bruker et webgrensesnitt mot e-postsystemet. Ulike former for innholdskontroll er per i dag også vanlig i de fleste e-postsystemer. Mest vanlig er filtrering eller merking av uønsket e-post og filtrering av ondsinnet kode via signaturscanning eller ved enkel

[32] Message Transfer Agent.
[33] Message Delivery Agent.

filtrering basert på vedleggstyper. Filter for uønsket språkbruk og liknende er også i bruk flere steder. Denne type innholdskontroll kan plasseres flere steder i kjeden, både på innkommende og utgående e-post.

6.1.3 Fysiske sårbarheter

Ettersom e-postinfrastrukturen er direkte avhengig av de underliggende TCP-forbindelsene, vil sårbarhet overfor fysiske feiltilstander og virkemidler som regel være de samme som for de lavere lagene i modellen. Unntaket er først og fremst måten e-post leveres på gjennom transportkjeden - dersom en SMTP-tjener ikke kan nås, vil avsendertjeneren prøve på gjentatte leveringer før den gir opp og sender feilmelding bakover i kjeden igjen. I tillegg tilbyr SMTP utvidet redundans, siden en kan (og bør) spesifisere flere MX-felt i DNS og dermed få flere maskiner som e-posttjenere for et domene. Standarden sier at en klient som ikke får kontakt med den høyest prioriterte tjeneren skal prøve de neste etter tur. Dersom e-posttjenerene i tillegg står i ulike nettverk, vil systemet til en viss grad også være robust mot lokale nettverksfeil.

Tidligere var det vanlig å la SMTP-tjenere videresende e-post til vilkårlige mottakere og dette var med på å gjøre e-postinfrastrukturen mer robust. Utnyttelse av disse til masseutsendt e-post har nå satt en stopper for praksisen, og per i dag anser de fleste et slikt åpent relé som et sikkerhetsproblem. I praksis blir domener som videresender vilkårlig e-post raskt svartelistet av spamfiltreringssystem.

6.1.4 Logiske sårbarheter

De basale e-postprotokollene som beskrevet over har ingen mekanismer for å beskytte integritet eller konfidensialitet og heller ingen mekanismer for å sikre opphavsautentisitet. Dette innebærer at alle trivielt kan sende e-post med valgt innhold, for eksempel med en falsk avsenderadresse. Mottaker- og avsenderfeltene som normalt vises i en brukerklient er de som står i meldingshodet, og disse brukes faktisk ikke i det hele tatt av transportkjeden - SMTP har en egen protokolldel for å spesifisere dette. Noe informasjon i meldingshodet (’Received’ og ’Return-Path’) legges til av mellomliggende noder. Disse kan også forfalskes av avsender, men de som blir lagt til i transportkjeden har avsender normalt ikke kontroll over.

En angriper som kontrollerer en komponent i kjeden fra sender til mottaker kan også fange opp og endre en e-post etter eget ønske, mens en som har lesetilgang noe sted i kjeden umiddelbart kan lese all e-post som passerer. Metoder for å sikre innholdet i e-postmeldinger (PGP og S/MIME) blir behandlet i kapittel 12.

Som allerede nevnt settes det gjerne opp flere SMTP-tjenere for et gitt domene, og dette gir via DNS automatisk redundante leveringsveier. Noe tilsvarende finnes normalt ikke for henting av e-post.

Autentisering mot SMTP-tjenere var tidligere ikke aktuelt, men har blitt et tema på grunn av store mengder uønsket e-post. Tidligere har ad-hoc løsninger som POP-autentisering før SMTP blitt

brukt, men det finnes også en egen SMTP-utvidelse for autentisering som kan brukes for å autorisere en bruker eller en annen tjener for riktig tilgang. Bruk av TLS for SMTP er standardisert, og er etter hvert flere steder tatt i bruk sammen med passord for brukerautentisering.

Som allerede nevnt brukes POP fortsatt ofte med klartekstpassord. I slike tilfeller kan en angriper med tilgang til nettverkstrafikk mellom klient og tjener trivielt få tilgang til brukernavn og passord, og dermed ha full kontroll over brukerens e-postmottak. Protokollutvidelser som kan gi sikrere autentisering er implementert i de fleste klienter og tjenere.

IMAP har på samme måte som POP muligheter for klartekstpassord, men standarden her sier for eksempel at alle implementasjoner skal ha muligheter for å slå av bruk av klartekstpassord og at alle implementasjoner må støtte IMAP over TLS. IMAP har i tillegg en generell autentiseringsfunksjonalitet som kan støtte flere ulike beskyttelsesmekanismer.

E-postprotokollene er i utgangspunktet spesifisert slik at en sender skal få melding tilbake (bounce) dersom brukeren er ukjent på angitt domene, eller om meldingen av andre grunner ikke kan sendes til mottakers postboks. Varierende konfigurasjon (stort sett som en følge av massive bouncer på grunn av spam og annen masseutsendt e-post) gjør likevel at e-post kan forsvinne uten tilbakemelding til opprinnelig avsender. En avsender har uansett ikke kontroll på hva som skjer med e-posten etter at den er levert av siste SMTP-node (for eksempel om e-posten er hentet til brukers lokale klient eller om den er framvist i brukerens lokale klient).

Som for de fleste andre programmer som håndterer nettverkstrafikk, er det også funnet og utnyttet mange sårbarheter i e-posttjenere. Med tiden kan tjenerne synes å ha blitt mer robuste, mens det samtidig har vært et økt fokus på sårbare klienter. Sårbarheter i klienter kan i verste fall føre til overtagelse av klientmaskiner, men mer utbredt er ulike former for manipulasjon av framvisning som for eksempel kan brukes i et phishingangrep. En utstrakt bruk av HTML-vedlegg som primært meldingsformat bidrar til å øke dette problemet.

6.1.5 Sosiale sårbarheter

På tross av sårbare protokoller, skjer trolig de fleste uønskede e-posthendelsene på grunn av brukerfeil. Sensitiv informasjon og sensitive dokumenter kan enkelt sendes til feil personer ved hjelp av få tastetrykk og det er lite tekniske sperrer kan bidra med her. Et mye omtalt norsk tilfelle var da en e-post til statsministerens kontor ble sendt til domenet `smk.no` i stedet for til `smk.dep.no`. Domenet `smk.no` var på den tiden eid av en opposisjonspolitiker [2]. Det er gjort flere forsøk på å implementere "fjernstyrt" innholdskontroll for å kunne trekke tilbake sendt innhold eller på andre måter begrense bruken av sendt innhold (for eksempel hindre videresending eller utskrift). Dette implementeres typisk ved hjelp av kryptografi og restriktive klienter, men vil aldri kunne gi noen tilfredsstillende beskyttelse.

Et annet problem som gjerne oppstår er feilstaving av domenenavn i e-postadresser. Dersom det feilstavede domenenavnet ikke eksisterer, vil e-posten normalt bli returnert, men det er ikke uvanlig

at feilstavinger av kjente eller verdifulle domenenavn er registrert av andre. Disse vil enkelt kunne sette opp e-posttjenere som mottar all e-post til domenet, og det er flere eksempel på misbruk av denne type feilsendt e-post.

I tillegg til de vanlige mulighetene for datatap og konfidensialitetsbrudd, har en for e-post en tilleggsfare. Store mengder viktig informasjon og dokumenter blir ofte liggende usortert og uarkivert som personlig e-post. Dersom nøkkelpersoner i en organisasjon slutter, kan viktig informasjon forsvinne. Spesielt vanskelig blir dette dersom e-post blir lagret kryptert uten nøkkeldeponering. På den andre siden vil det også være kritisk dersom en lagret postboks havner i feil hender. En ansatts samlede e-post vil ofte inneholde mye sensitiv informasjon for en organsisasjon, mens en privatpersons e-post typisk vil inneholde mye informasjon som for eksempel kan benyttes ved identitetstyveri (passord, personnummer, kontonummer og så videre).

For mange e-postbrukere utgjør mengden av uønsket e-post et alvorlig tilgjengelighetsproblem. Problematikken er nærmere diskutert i kapittel 5, og noen mulige beskyttelsesmekansimer er diskutert i kapittel 12.

E-postadresser har også blitt viktige som globale navn på enkeltpersoner. For eksempel er unike navn meget viktige dersom en skal utstede offentlig nøkkel-sertifikater. Typisk benyttes også e-postaddresse som brukernavn for autentisering i for eksempel nettbutikker. I slike tilfeller bruker en i tillegg gjerne e-post som en form for autentiseringsmekanisme, der en ved å taste inn e-postadressen kan få tilsendt et passord per e-post.

6.1.6 Avhengigheter

I tillegg til avhengiheter til den underliggende infrastrukturen (TCP/IP) og maskinene og programvaren som utgjør infrastrukturen, er e-posttjenestene avgjørende avhengig av DNS. Som allerede nevnt brukes DNS både som “adressebok” (det vil si MX-felt) og for å oversette navn til IP-addresser. Se kapittel 7 for mer om dette.

6.2 Web

Med web menes det globale og sammenkoblede hypertekstsystemet som distribueres over Internett. Den samme teknologien benyttes også i stor grad i interne nettverk, men kalles da gjerne intraweb eller lignende. Sårbarheter forbundet med web generelt er et meget stort tema, og bare et kort riss av sikkerhetsproblemstillingene vil bli gitt her.

Teknologien og protokollene ble først standardisert rundt 1990, og var ment for å understøtte et interaktivt hypertekstsystem. Populariteten og utbredelsen økte raskt, og web var en av de viktigste driverene bak den eksplosive utviklingen Internett fikk utover 1990-tallet. Per i dag har teknologien flere steder overtatt som en integrerende protokoll der en tidligere brukte spesialiserte protokoller, og den blir også vidt benyttet som et generelt brukergrensesnitt mot vilkårlige applikasjoner. Eksempler

kan være overføringsmekanismer for andre protokoller, generell filoverføring, fjernstyring og fjerninnlogging.

De grunnleggende protokollene består av HTTP (Hypertext Transport Protocol) og HTML (Hypertext Markup Language). HTTP brukes for å transportere innhold mellom klienter og tjenere (og eventuelt også til og fra en proxytjener). HTTP har funksjonalitet både for å hente objekt fra en tjener og for å poste objekt til en tjener. I tillegg overfører protokollen informasjon om typen til objektet som skal sendes (HTML-dokument, JPG-bilde og så videre) og hvilken måte det skal sendes på. Protokollen går over TCP-forbindelser som enten kan være stående for en sesjon eller som kan opprettes ved behov. Uansett er HTTP i seg selv en tilstandsløs protokoll, og en må bruke for eksempel cookies[34] eller URL-parametre for å opprettholde en sesjon mellom klient og tjener.

For å markere tekstlig innhold brukes HTML. Med markering menes spesifikasjon av hva som er linker, overskrifter, avsnitt, lister og så videre. HTML brukes også til en viss grad for å spesifisere utseende på dokumentet.

For å lokalisere et objekt på web på en unik måte benyttes URL-er. I eksempelet `http://www.example.com/example.html?id=200` har en angitt protokoll (HTTP), maskinnavn (`www.example.com`), sti og objektnavn (example.html) og en parameter (id=200). I tillegg kan en URL på web også spesifisere brukernavn, passord, portnummer samt posisjon i objektet.

En typisk sesjon mellom en brukerklient og en tjener starter med at brukeren taster inn `http://www.example.com/example.html`i webleseren. Denne gjør så et DNS-oppslag på navnet `www.example.com` og får en IP-adresse i retur. Deretter settes det opp en TCP-forbindelse til riktig IP-adresse og en sender forespørsel etter dokumentet `/example.html?id=200`. Tjeneren svarer og returnerer et HTML-dokument. Webleseren tolker dette dokumentet og leter opp URL-er til andre objekt i siden (for eksempel bilder eller klientsideapplikasjoner), gjør eventuelt nye navneoppslag og henter disse objektene. Objekter som tidligere er hentet og ikke endret siden sist blir ikke hentet på ny.

HTTP har standardiserte funksjoner for autentisering, men disse brukes i mindre grad. Den ene autentiseringsmekansimen (Basic) er i praksis en form for klartekstpassord, mens den andre (Digest) benytter en sikrere utfordring-svar protokoll basert på hashfunksjonen MD5. I stedet for disse brukes normalt en eller annen form for passord som sendes til tjeneren som vanlig innhold gjennom HTTP. I tillegg benytter en da TLS for å beskytte hele sesjonen.

For å kunne autentisere endepunktene, og samtidig beskytte webtrafikk mot avlytting og manipulasjon, benyttes HTTPS. Her settes det opp en TLS-forbindelse (se kapittel 12) mellom klient og tjener, før en fortsetter med vanlig HTTP-trafikk gjennom TLS-forbindelsen. Med denne metoden er det mulig å autentisere både klient og tjener, men i praksis benyttes nesten bare tjenerautentisering[35]. Sertifikatene til tjenerne verifiseres ved hjelp av rotnøkler som er forhåndsinnlagt i webleserne. En

[34] En "cookie" er et lite informasjonsobjekt som webtjeneren lagrer hos brukerklienten. Neste gang klienten oppretter forbindelse med samme webtjener returneres den til tjeneren.

[35] Dette betyr at klienten vet hvem tjeneren er uten at tjeneren vet noe mer om hvem klienten er.

toveis-autentisering via TLS vil kreve at brukeren genererer eller mottar private nøkler, og at det blir laget sertifikat ut fra disse. Dette er lite i bruk, delvis på grunn av at det har vist seg vanskelig å få til i praksis, og delvis på grunn av at en ikke stoler på klientmaskinenes sikkerhet. I stedet foregår normalt klientautentisering ved hjelp av passord og/eller engangskoder, men det er verdt å merke seg at heller ikke dette vil hjelpe dersom klientmaskinen er kompromitert.

En vanlig misforståelse blant brukere er at HTTPS-beskyttelse innebærer at en kommuniserer med en "vennligsinnet" webtjener. Dette er ikke riktig, autentiseringen binder bare den gjeldende forbindelsen til det navnet som er angitt i sertifikatet. Sikkerhetsnivåer og sertifikatpolicyer varier til dels mye mellom de ulike sertifikatutstederne og heller ikke denne forskjellen er synlig for brukeren. I 2006 ble de første "Extended Validation"-sertifikatene tatt i bruk. Målet med disse er å få etablert strengere krav til sertifiseringsprosessen og samtidig gi muligheter for webleseren å signalisere dette til brukeren. Teknologien bak disse er ellers den samme som for de andre sertifikatene.

6.2.1 Fysiske sårbarheter

Ettersom webinfrastrukturen er direkte avhengig av de underliggende TCP-forbindelsene, vil sårbarhet overfor fysiske feiltilstander og virkemiddel som regel være de samme som for de lavere lagene. Distribusjonsmodellen med en tjener og mange klienter tilføyer likevel en del problematikk. Delkapittel 6.3 omhandler dette.

6.2.2 Logiske sårbarheter

En av de største risikoene forbundet med bruk av web kommer fra sårbare klientapplikasjoner eller sårbare tjenerapplikasjoner. Som allerede nevnt har web blitt et generelt grensesnitt for mange ulike tjenester på Internett og dette fører til at mange applikasjoner eksponeres.

I starten var tjenersiden av en webforbindelse i essens bare en filtjeneste som leverte enkle dokumenter etter klientens ønske. Dette er nå i stor grad endret til en situasjon der tjenersiden består av en eller flere applikasjoner (webapplikasjoner) som leverer dynamisk innhold basert på parametre fra klientene. Dette gir også klientene gode muligheter for å manipulere tjenerne. I den enkleste formen kan for eksempel webapplikasjonen lures til å kjøre input direkte fra klienten.

Det finnes mange enkle verktøy for å sette opp denne typen applikasjoner, og dette, sammen med en manglende sikkerhetstradisjon på området, har ført til at en per i dag finner mange sårbare webtjenester på Internett.

Flere og flere webtjenere tilbyr også klienter å lagre egengenerert innhold på tjenere som senere vises fram til klienten selv eller til andre brukerklienter. Dersom dette brukergenererte innholdet ikke kontrolleres godt nok på tjenersiden, kan en ondsinnet klient laste opp egne skriptingprogrammer som senere kjøres av andre[36].

[36] Denne typen angrep kalles gjerne Cross Site Scripting (XSS).

På klientsiden har weblesere stadig blitt mer komplekse, med støtte for mer og mer funksjonalitet. I praksis betyr dette at de skal være i stand til å tolke flere forskjellige typer innhold, noe som igjen øker sannsynligheten for feiltolking og sårbarheter. For eksempel kan noe så enkelt som et feilkonstruert bilde få webleseren til å kjøre vilkårlig kode - se for eksempel Microsoft Security Bulletin MS04-028 [46].

I tillegg har en på klientsiden også hatt en utvikling med mer dynamikk. Brukerklientene er i stand til å kjøre applikasjoner skrevet i for eksempel Java eller Flash og skriptspråk som JavaScript. Disse applikasjonene kjører normalt i et beskyttet område, slik at de ikke har tilgang til å lese og skrive eller kjøre kode på maskinen, men også her kan det oppstå feil.

Weblesere inneholder også ofte passord og annen sensitiv informasjon, og konsekvensene kan være alvorlige dersom ondsinnede klientsideapplikasjoner får tilgang til disse.

Sårbarheter i klientapplikasjoner kan også brukes for å få en ondsinnet webside til å fremstå som en annen side, gjerne slik at det ser ut som om siden benytter HTTPS med et gyldig sertifikat. Mange angrep av denne typen foregår ved å manipulere navn og URL-er. Innføring av internasjonale domenenavn (IDN) har til en viss grad bidratt til å gjøre dette enklere - domenenavnet `blå.no` er for eksempel et annet enn `bla.no`. Teknikker der forfalskede e-poster med linker til forfalskede websider sendes til tilfeldige brukere kalles gjerne “phishing” (se kapittel 5), og målet er typisk å samle inn informasjon som passord, kredittkortnummer eller annen personlig informasjon fra brukere.

I likhet med de andre basale internettprotokollene, går HTTP-trafikk i klartekst uten integritetsbeskyttelse, og uten at det normalt benyttes autentisering av klienter eller tjenere. I praksis fører dette likevel til få problemer sammenlignet de overnevnte. Avlytting eller manipulasjon av innhold vil kreve tilgang til nettverksutstyr langs ruter som TCP-forbindelsen benytter, og forfalsking av et av TCP-endepunktene vil være vanskelig. Et angrep mot denne infrastukturen vil normalt være lettere å utføre indirekte, for eksempel via DNS.

6.2.3 Sosiale sårbarheter

Anvendelsen av sterke mekanismer for autentisering og beskyttelse gjør ofte at en bruker må ta sikkerhetsrelaterte avgjørelser under normal bruk. En støter for eksempel ofte på sertifikat som ikke er riktige på alle punkt, eller en får spørsmål fra tiltrodde klientsideapplikasjoner som vil ha utvidete rettigheter. For mange sluttbrukere vil det være vanskelig å forholde seg til disse avgjørelsene og de aller fleste vil av og til velge feil i slike sammenhenger.

All informasjon som er tilgjengelig i digital form er det enkelt å indeksere og søke i, og web er et av de beste eksemplene på dette. Søkemotorene på web fanger raskt opp nye sider og gjør de enkelt tilgjengelig for alle. Med litt ekstra innsats kan sluttbrukere også automatisere søk både i søkemotorer og andre tilgjengelige databaser, og raskt få ut store mengder aggregert informasjon om spesifikke tema. I enkelte tilfeller kan også dette utgjøre en sårbarhet. For eksempel vil informasjon

om viktig infrastruktur eller personidentifiserende informasjon som tidligere har vært ansett som lite sensitivt, fort blir sensitivt når store mengder blir aggregert.

En “billig” og forholdsvis utbredt måte å begrense tilgang til et webdokument på, er å legge dokumentet på en webtjener uten å ha noen referanser til det andre steder. Deretter sendes URL-en til de som skal ha tilgang til dokumentet. Dette er ikke en god måte å begrense spredning på. I tillegg til at andre kan gjette på URL-en, er det godt mulig at referanser til dokumentet likevel blir spredt. For eksempel vil HTTP normalt sende med en “referer”-streng som forteller hvilken side en er kommet fra. Dersom et dokument som er skjult på denne måten, inneholder referanser til andre webtjenere vil en dermed risikere å spre URL-en til andre. Dersom i tillegg denne referansen videre inkluderes i loggfiler som er tilgjengelig på web, vil den også raskt bli plukket opp av søkemotorer.

6.2.4 Avhengigheter

Foruten underliggende infrastruktur og tilhørende tjenere, er DNS sentralt for web. Alle linker i en webside er normalt gitt som referanser med DNS-navn, og dette gir en umiddelbar avhengighet til en velfungerende DNS-infrastruktur.

6.3 Tjenestedistribusjon (Content Delivery)

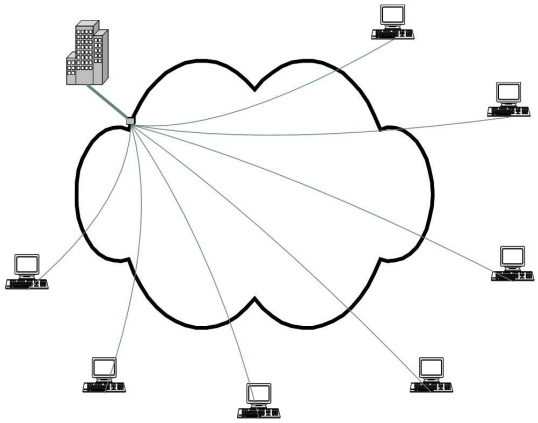
Vi vil i dette avsnittet diskutere noen av utfordringene forbundet med storskala innholdsdistribusjon, se på hvordan dette løses i praksis og vurdere sårbarheter forbundet med disse metodene.

Selv om Internett i seg selv har mange desentraliserte aspekt, så går store deler av den totale trafikkmengden i en hierarkisk struktur. Tjenester på Internett, slik som for eksempel web, har tradisjonelt vært tilbudt gjennom en sentralisert distribusjonsmodell. I denne modellen har tilbyderne av tjenesten et begrenset sett med ressurser og maskiner lokalisert på et fåtall steder på Internett. Alle klienter som vil hente innhold fra leverandøren setter opp egne separate forbindelser til tjenesten, og dette skjer selv om det samme innholdet lastes ned samtidig til to maskiner i samme lokalnettverk. Figur 6.1 illustrerer dette.

Kvaliteten på en tjeneste realisert i en slik sentral distribusjonsmodell er avhengig av ressursene lokalt hos tilbyderen og av tilgjengelig nettverksforbindelse mellom klient og tjener. Mulige flaskehalser i nettverksforbindelsen mellom tilbyder og kunde blir gjerne delt i fire:

- Første mil: forbindelsen mellom tjenestetilbyders maskiner og tjenestetilbyders nettverksleverandør.
- Peering: forbindelsene mellom de autonome systemene mellom tilbyders AS[37] og klients AS.
- Backbone: forbindelsene internt i nettverkene som transporterer den gjeldende trafikken.

[37] Autonomt System, se kapittel 8.



Figur 6.1: Sentralisert distribusjonsmodell

- Siste mil: klientens forbindelse mot egen nettverksleverandør.

Flaskehalsen sluttbrukerne er mest kjent med er fortsatt den siste milen. Tilknytningen her kan være alt fra modem til raske fiberforbindelser, og etter hvert som sluttbrukerne får raskere og raskere tilknytning, øker trykket på de tre andre flaskehalsene. Tjenestetilbydere med stor trafikk merker som regel mest til disse siste tre. Selv om innholdet de leverer ikke krever mye båndbredde per bruker, kan summen av mange samtidige klienter overbelaste leverandørens tilknytning til Internett. Ofte er det stor forskjell på gjennomsnittlig belastning og maksimal belastning, og tilbyder må dimensjonere første mil i forhold til antatt maksimal belastning for å sikre høy tilgjengelighet.

De flaskehalsene som oppstår i backbone eller på grunn av peering er det som regel ingenting hverken kunder eller tilbyder selv kan gjøre noe direkte med.

For flere tjenestetilbydere vil en sentralisert distribusjonsmodell gi for dårlig kvalitet på tjenesten, ikke minst ved et variert bruksmønster av tjenesten slik som for eksempel Windows Update. Ved publisering av en ny sikkerhetsoppdatering vil man få stor tilgang rett etter publiseringen. Etter hvert vil pågangen avta før den så økes drastisk ved neste publisering. Et annet typisk eksempel som blir viktigere og viktigere er levering av multimediastrømmer. Ved for eksempel større nyhetshendelser vil trafikk av denne typen brått øke dramatisk.

Det er i utgangspunktet flere måter å løse disse flaskehalsene på ved hjelp av de nåværende internett-standardene. Tilfeldig lastdistribuering løses enklest med å angi flere IP-adresser (til ulike tjenere) for det aktuelle navnet i DNS. Navnetjenesten vil da returnere de konfigurerte IP-adressene i ulik rekkefølge, og effekten blir en tilfeldig distribuering av tjenere til klienter. Denne metoden vil ikke hjelpe dersom en av tjenerne går ned - DNS vil ikke vite noe om tilstanden og vil fortsette å dele ut IP-adressen til tjeneren som ikke svarer (men det finnes tilleggsprogramvare som kan løse dette).

Manuell klient-multipleksing har også vært brukt lenge. Tilbyderen speiler da innholdet på flere tjenere og ber brukeren manuelt velge et speil som ligger geografisk nært. Med litt mer arbeid kan

også leverandøren gjøre dette automatisk ved hjelp av HTTP-redirects. Da må webtjeneren velge riktig innholdstjener for klienten og sende forespørsler videre dit.

Cachende webproxyer er mye brukt i mindre nettverk for å redusere oppstrøms webtrafikk[38] og samtidig gi bedre respons til brukerne. Enkelte ISP-er har også tatt i bruk transparente (intercepting) webproxyer for sine kunder. Dette betyr at ISP-en ruter utgående TCP-oppkoblinger til port 80 til sin egen proxytjener. Dermed får alle brukerne automatisk en webproxy, og ISP-en får redusert oppstrøms trafikk og dermed også reduserte utgifter. Teknikken blir ofte reagert på av brukere, siden den bidrar til å bryte ende-til-ende-prinsippet.

En annen måte å løse samme problem på er å bruke P2P-nettverk (peer-to-peer). Der er alle noder i utgangspunktet både klienter og tjenere, og innhold fordeles i et desentralisert nettverk av deltakere. Disse nettverkene står for en betydelig del av den totale trafikkmengden på Internett, men er til nå stort sett bare brukt mellom private brukere. Så langt har det vist seg vanskelig å bruke P2P-nettverk for kommersielle aktører, blant annet på grunn av uforutsigbar tjenestekvalitet.

6.3.1 Innholdsdistributører

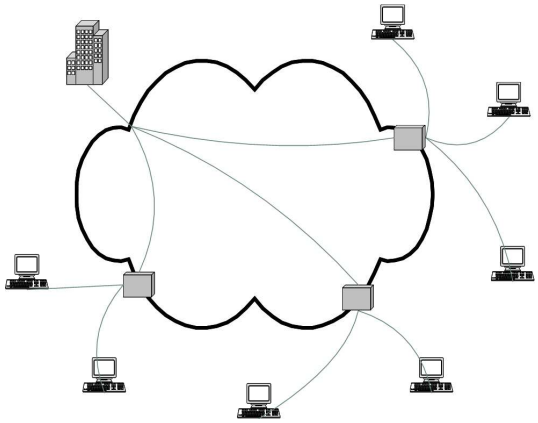
Alle de overstående metodene har sine svakheter. Proxyer kan ikke kontrolleres av innholdsleverandøren og gir heller ingen tilgjengelighetsgaranti for leverandøren. Intelligent lastbalansering med geografisk spredte tjenere vil gi dette, men er kostbart å implementere. I dette markedet har innholdsdistributørene[39] oppstått som aktører. De tilbyr geografisk distribuerte mellomlagringssystem sammen med en mekanisme for å koble klienter til riktig mellomtjener. Figur 6.2 illustrerer hvordan dette ser ut i forhold til den tradisjonelle distribusjonsmetoden. For innholdsleverandører vil dette gi økt tjenestekvalitet til sluttbrukere, samtidig som det er enkelere å skalere enn et eget geografisk spredt nettverk.

Den per i dag mest brukte måten for å dirigere brukere til riktig speil på er ved hjelp av "intelligente" DNS-tjenere. Generelt er målet å plukke ut tjenere som gir best respons (dette kan innebære færrest hopp, korteste rundetid eller minst belastet tjener). Tilbydere har et eget nettverk av tjenere plassert hos forskjellige ISP-er. De kan dermed levere innhold raskt og får samtidig en meget god sanntidsoversikt over nettverket.

Markedet for innholdsdistributører er allerede stort og vil vokse mye etter hvert som flere og flere sluttbrukere får raskere nettforbindelser. Likevel fører logikken i tjenestene til at markedet blir dominert av et fåtalls store distributører. En aktør med et stort fysisk nettverk av innholdstjenere spredt rundt i mange nettverk vil kunne gi bedre tjenester til kundene enn en med et lite nettverk. På samme måte vil en distributør med et stort nettverk ha bedre oversikt over global trafikkflyt.

[38] Med oppstrøms trafikk menes her trafikk som går fra et nettverk til et større nettverk, denne trafikken er typisk forbundet med større kostnader enn for eksempel lokal trafikk.

[39] Også kalt tjenestedistributører.



Figur 6.2: Desentralisert distribusjon ved hjelp av innholdsleverandør

Den desidert største aktøren i dette markedet er Akamai, som i følge egne opplysninger har over 20.000 tjenere plassert i over 1000 ulike nettverk (autonome system). I januar 2007 hadde de oppimot 3 millioner HTTP-treff mot sine tjenere per sekund, og de antar selv at distribusjonsnettverket deres står bak 20% av den totale webtrafikken [3].

En innholdsleverandør som benytter Akamai sin tjeneste for levering av HTTP-trafikk endrer sin egen navnetjener til å peke på et navn i Akamai sin infrastruktur. Når en bruker gjør et oppslag på innholdsleverandørens domene vil dermed Akamai sine navnetjenere overta i stedet, og disse vil via to nivå med DNS-oppslag dirigere klienten til en passende innholdstjener. Riktig innholdstjener velges ut på bakgrunn av klientens IP-adresse og annen tilgjengelig informasjon (for eksempel status på andre tjenere og generell nettverksstatus). Både navnetjenerene på det siste nivået og innholdstjenerene står fysisk hos ulike ISP-er rundt i verden. Informasjon om status henter Akamai inn ved hjelp av "read only" BGP-sesjoner med partnere samt ved hjelp av egne overvåkingsagenter. I praksis betyr dette at når en norsk internettbruker henter informasjon fra for eksempel `download.microsoft.com`, så vil i de fleste tilfellene all trafikk gå mellom brukerens maskin og en tjener plassert hos en norsk ISP.

For å muliggjøre effektiv fjernstyring, vil de fleste distribusjonsnettverk i stor grad være homogene. Det vil si at maskinvare, operativsystem og annen programvare er identiske, eventuelt bare med små versjonsforskjeller.

Mange av innholdsdistributørenes kunder er innholdsprodusenter som leverer mye volum med varierende pågang. I tillegg brukes distributørene til mange kritiske tjenester der kontinuerlig tilgjengelighet og rask respons på tjenestene er viktig. Dette kan for eksempel være offentlig informasjon eller oppdateringer til antivirus og annen programvare.

Det er flere Akamai-tjenere som leverer innhold hos norske ISP-er, men så langt har få norske organisasjoner tatt i bruk tjenestene for å få levert ut sitt eget innhold.

6.3.2 Fysiske sårbarheter

Akamai har et stort distribuert system der mesteparten av tjenerene er fjernstyrte. Hoveddelen av maskinvaren står plassert hos ulike ISP-er og er fysisk utenfor Akamai sin kontroll. Mulighetene for direkte tilgang til maskinvaren bestemmes dermed av de ulike ISP-enes fysiske tilgangskontroll, og en kan anta at denne er varierende. Likevel vil fysisk ødeleggelse av tjenerene hos et fåtalls ISP-er ikke ha noen særlig innvirkning på systemets evne til å levere innhold - innholdsnettverket er nettopp laget med tanke på å motstå slike hendelser. På tilsvarende måte er sårbarhetene overfor fysisk skade eller ødeleggelse på innholdsleverandørens utstyr redusert.

Akamai sine egne hovedsentraler utgjør sårbare punkt i systemet, men det er lite tilgjengelig informasjon om hvordan disse er sikret.

6.3.3 Logiske sårbarheter

Det finnes en del litteratur om innholdsnettverk (se for eksempel [60]), men det aller meste tar for seg ytelse og ikke sårbarhet forbundet med bruk av nettverkene.

Selv om et av hovedmålene for innholdsnettverkene er å sikre tilgjengelighet og dermed redusere sårbarhet, så har en samtidig blitt globalt avhengig av i praksis én leverandør. Dersom den største innholdsdistributøren skulle få noen form for kvalitetsproblem, vil det bli vanskelig for mange innholdsleverandører å få ut innhold. Selv om en leverandør raskt vil kunne omdirigere trafikk til egen infrastruktur, vil denne trolig ikke være dimensjonert for å takle den totale trafikkmengden. En total stopp i det største distributørnettverket vil føre til store trafikkforskyvninger og overbelastninger, og dermed også ha en global påvirkning på hele Internett. Mange vil mene at tjenestene tar bort et "single point of failure" hos de enkelte leverandørene, men innfører et nytt på et høyere nivå. Spesielt gjelder dette når en globalt er avhengig av bare én aktør.

Et distribuert tilgjengelighetsangrep mot en kunde av Akamai, som for eksempel `download.microsoft.com`, vil ha mindre effekt siden det vil bli kanalisert til mange forskjellige fysiske maskiner, som i tillegg står i forskjellige fysiske nettverk. Et angrep mot et utvalg av maskinene som betjener navnet kan stoppe leveransene fra disse, og dette vil i tillegg stoppe andre tjenester som leveres fra de samme fysiske maskinene. Likevel vil dette også ha liten effekt på grunn av den massive redundansen i systemet. Et velrettet angrep mot Akamai sine øverste navnetjenere kan bli mye verre.

I juni 2004 ble Akamais DNS-infrastruktur utsatt for et tilgjengelighetsangrep som førte til problemer for mange sluttbrukere. Angrepet gav alvorlige ytelsesproblemer for bl.a Microsoft, Google og Yahoo [16]. Paul Vixie, medforfatter på bl.a mange av DNS-standardene, uttalte dette i forbindelse med angrepene: *"The basic internet technology was built to military specifications and is meant to be 'survivable' in the sense that there is no single point of failure. Akamai is a single point of failure, as evidenced by yesterday's problems and a similar problem that occurred a few weeks ago"* [38].

Som diskutert over kan en anta at det er mulig for en angriper å få fysisk tilgang til noen av Akamai sine tjenere. Logisk manipulasjon av disse vil videre være mulig, men en kan anta at dette raskt vil oppdages av automatiske overvåkingsverktøy og deretter raskt rettes på. Tyveri av globale autentiseringsnøkler er trolig heller ikke mulig fra disse tjenerne. Likevel vil det trolig være mulig å hente ut sentral informasjon om operativsystem og applikasjoner, og eventuelt også ta med seg kopier av disse for videre analyse.

En angriper med tilstrekkelig tilgang på denne type informasjon vil i teorien kunne finne utnyttbare sårbarheter som kan ha alvorlige konsekvenser. Ved hjelp av mange DNS-forespørsler kan en angriper få tilgang til IP-adressen til mange av tjenerne i et tjenestedistribusjonsnettverk [72]. Med en videre antagelse om at tjenerne til et gitt tjenestedistribusjonsnettverk kjører samme programvare (med versjonsvarianter) og at de innholder en sårbarhet, vil en angriper kunne lage ormer som overtar mesteparten av tjenerne. Etter overtagelse kan ormen for eksempel skru av alle nettverkskort på tjeneren og bytte alle lokale passord. Dette forhindrer tjenestedistribusjonsaktøren eksternt å vedlikeholde tjeneren, og man vil lokalt få problemer med å logge inn på tjeneren. Dette vil kunne ta ned hele tjenestedistribusjonsnettverket. Dette vil videre kunne få alvorlige ringvirkninger på Internett, ved at tjenestesteder og dermed nettverksutstyr på veien blir overbelastet.

6.3.4 Sosiale sårbarheter

Siden innholdsleverandørene bruker proprietære system, kan det være vanskelig å gjøre egne vurderinger av risiko forbundet med avhengighet til systemene. Store aktører implementerer gjerne egne løsninger selv (for eksempel Google), eller benytter seg av egen lastbalansering mellom flere distributørnettverk i tillegg til egne løsninger (for eksempel Microsoft).

Bedre muligheter for flere aktører ville vært ønskelig, for eksempel kunne en tenke seg standardprotokoller eller i det minste standardterminologi som vil forenkle samtidig bruk av flere aktører og også gi muligheter for å sammenligne ulike aktører bedre.

Noe standardiseringsarbeid finnes. Content internetworking (CDI) beskrives i RFC 3466. Her gis en generell beskrivelse av systemer, og noe felles terminologi defineres, mens RFC 3507 beskriver “Internet Content Adaptation Protocol” som er en protokoll for innholdslevering. En egen IETF-arbeidsgruppe, “Open Pluggable Edge Services”, jobber med lignende standardiseringsarbeid [37].

6.3.5 Avhengigheter

Som nevnt over er det forholdsvis vanskelig å avdekke hvilke interne og eksterne avhengigheter et proprietært distribusjonsnettverk har. Avhengigheten til en velfungerende DNS-infrastruktur er åpenbar, mens det er mer usikkert i hvilken grad distributørnettverkene er avhengige av pålitelig sanntidsinformasjon om de ulike nettverkene.

7 Fundamentale tjenester

I dette kapitlet beskrives to tjenester som er vurdert til å være *fundamentale* tjenester for internett-infrastrukturen, nemlig navnetjenesten og tidstjenesten. Førstnevnte er et hyppig mål for ulike logiske angrep, og pekes ut som en viktig tjeneste som bør sikres for å gjøre Internett mer robust [19]. Sistnevnte er nok mer ukjent og mindre kritisk, men det antas at korrekt tid er viktig for en rekke brukere og vil bli mer viktig for den vanlige bruker i fremtiden.

Uten navnetjenesten ville Internett vært lite anvendbart. Mennesker foretrekker å operere med navn fremfor IP-adresser, og er således helt avhengig av et system som oversetter riktig mellom domenenavn og IP-adresser. En kompromittert navnetjeneste vil kunne forhindre brukerne i å benytte Internett ved at navnetjenesten ikke returnerer IP-adresser, eller villede brukerne ved å returnere feil IP-adresser. Navnetjenesten gjør det også mulig å ha et nivå av indireksjon slik at IP-adressen til en maskin kan endres uten at navnet er påvirket. Dette gjør at det ikke er nødvendig å gjøre endringer i applikasjoner på andre maskiner som skal kommunisere med en maskin kjent ved navn, hvis denne endrer IP-adresse eller byttes ut.

Distribusjon av korrekt tid over Internett blir også sett på som en fundamental tjeneste i referansemodellen brukt i denne rapporten. Bakgrunnen for dette er at mange protokoller og applikasjoner, i sær sikkerhetsprotokoller, er avhengig av rimelig riktig tid. For fremtiden antas det at applikasjoner og protokoller vil bli mer avhengig av korrekt tid. Eksempler på mulige tidskritiske tjenester er systemer for levering av elektroniske bud over Internett, distribuerte systemer for håndheving av digitale rettigheter, logistikksystemer med utstrakt bruk av RFID[40] og systemer for tillitshåndtering. En sentral forskjell mellom tidstjenesten og navnetjenesten er imidlertid muligheten for å benytte egne referanseklokker, for eksempel GPS, fremfor å være avhengig av en tidstjeneste fra Internett. I den grad dette er gjort for kritiske systemer, er tidstjenesten fra Internett nærmest irrelevant i direkte forstand. Indirekte avhengigheter via andre systemer kan fremdeles være et problem.

7.1 Navnetjenesten

Navnetjenesten, Domain Name System (DNS), er en protokoll og en infrastruktur for å håndtere navn på Internett. Den primære oppgaven er å oversette mellom domenenavn og IP-adresser. For eksempel vil `www.ffi.no` kunne oversettes til IP-adressen 193.69.165.21. DNS støtter også oversettelse fra IP-adresse til domenenavn, der dette er registrert.

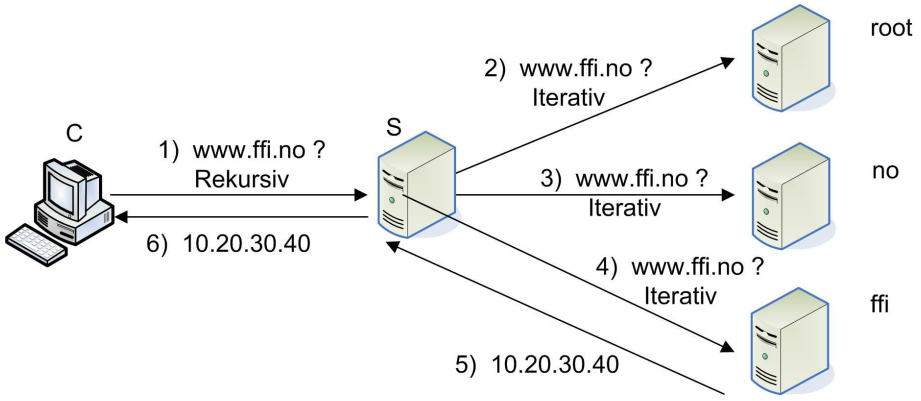
DNS brukes også i andre sammenhenger der en trenger hierarkisk navnegiving. For eksempel lagres adresseringsinformasjon for e-post i DNS, og to av de viktigste spamfiltreringsmekanismene bruker også DNS for distribusjon av både informasjon og autoritet. Et annet eksempel er ENUM (Telephone Number Mapping), en standard som beskriver hvordan en ved hjelp av DNS kan over-

[40] Radio Frequency Identification.

sette vanlige telefonnumre til URI-er (Uniform Resource Identifier) for bruk på Internett. I Norge er domenet `7.4.e164.arpa` satt i prøvedrift for å kunne støtte opp om en slik infrastruktur.

I tillegg til den åpenbare funksjonaliteten som en ren oversetter fra navn til nummer, er også navngiving viktig som første steg i en autentiseringsprosess. De aller fleste autentiseringssystem på Internett består av å knytte en entitet til et DNS-navn (maskinnavn eller e-postadresse). Hvordan navnegivingen foregår er dermed meget viktig.

Forenklet kan det sendes ut to forskjellige typer DNS-forespørsler. Disse er rekursivt (finn det ut for meg) og iterativt (gi meg all informasjon relatert til forespørselen). Som vist i figur 7.1, vil vanligvis en organisasjon sin navnetjener (S) motta rekursive forespørsler fra de interne maskinene i organisasjonen (C). S vil basert på en rekursiv forespørsel gjerne sende ut flere iterative forespørsler til andre navnetjenere på Internett, og til slutt finner S en navnetjener som gir svaret. Dette svaret sender S til C.



Figur 7.1: Eksempel på navneoppslag.

7.1.1 Fysiske sårbarheter

Det eksisterer i skrivende stund 12 forskjellige operatører av 13 unike sett av DNS-rottjenere. En DNS-rottjener har oversikt over IP-adressene til navnetjenerne for toppnivådomene, slik som for eksempel com, net, no, se og org. Denne oversikten utarbeides av Internet Assigned Numbers Authority (IANA), og lagres på noen "hemmelige" distribusjonstjenere til fordeling til de 12 operatørene. For 2004 ble det utarbeidet 90 versjoner av toppnivåfilen for distribusjon. Hver av filene var på omtrent 120KB [41].

I skrivende stund har følgende operatører ansvaret for de angitte DNS-rottjenere med tilordnet IP-adresse:

- A.root-servers.net - VeriSign Global Registry Services - 198.41.0.4
- B.root-servers.net - University of Southern California - 192.228.79.201

- C.root-servers.net - Cogent Communications - 192.33.4.12
- D.root-servers.net - University of Maryland - 128.8.10.90
- E.root-servers.net - NASA Ames Research Center - 192.203.230.10
- F.root-servers.net - Internet Systems Consortium, Inc - 192.5.5.241
- G.root-servers.net - U.S. DOD Network Information Center - 192.112.36.4
- H.root-servers.net - U.S. Army Research Lab - 128.63.2.53
- I.root-servers.net - Autonomia/NORDUnet -192.36.148.17
- J.root-servers.net - VeriSign Global Registry Services - 192.58.128.30
- K.root-servers.net - RIPE NCC - 193.0.14.129
- L.root-servers.net - ICANN - 198.32.64.12
- M.root-servers.net - Wide Project - 202.12.27.33

En operatør har for redundans flere fysisk atskilte rottjenere med samme IP-adresse (flere instanser). Dette betyr at den samme IP-adressen formidles ut på Internett fra flere forskjellige lokasjoner (anycast). Det blir så opp til rutingen på Internett å bestemme hvilke instans som har foretrukket vei til den som forespør. Hvis for eksempel en maskin i Norge ønsker å kommunisere med `I.root-servers.net`[41], vil forespørselen fra maskinen kunne bli rutet til en instans i Stockholm, London eller Helsinki. En identisk forespørsel sendt fra Italia vil kunne ende i en instans av `I.root-servers.net` i Milano. Under et stort tilgjengelighetsangrep mot DNS-rottjenerne 6. februar 2007, viste anycast seg som en svært effektivt geografisk distribuert lastbalanseringsmekanisme, og det antas at rottjenerne uten anycast[42] snart vil implementere dette [36].

Ved å telle med alle instanser hos alle operatører, eksisterer det minst 80 forskjellige rottjenere fordelt på 34 forskjellige land [41]. Den eksakte fysiske lokasjonen til alle instanser er meget vanskelig å oppdrive. Grunnen til dette er at operatørene av frykt for fysiske angrep ikke publiserer alle lokasjoner. Det å fysisk ta ned DNS ser dermed ut til å være en vanskelig oppgave. I tillegg har det blitt utarbeidet et ”beste-praksis-dokument” for operatører av DNS-rottjenere [10]. Her anbefales det blant annet at alle DNS-rottjenere må ha nødstrøm for minst 48 timer, samt flere andre gode sikkerhetstiltak.

Navnetjenere for land og toppnivådomener kalles gjerne Top-Level Domain servers (TLD-navnetjenere), og er delt inn i landspesifikke (ccTLD)[43] og generiske (gTLD)[44]. For Norge eksisterer det i skrivende stund 6 ccTLD-er, som vist i listen under.

- x.nic.no - 128.39.8.40

[41] Maskinen i Norge ønsker for eksempel en liste over navnetjenerne som håndterer com-domenet.
[42] D, E, G, H og L
[43] Country code TLD (ccTLD). Eksempelvis no, se og dk
[44] Generic TLD (gTLD). Eksempelvis com, net og org.

- y.nic.no - 193.71.199.51
- z.nic.no - 158.38.8.133
- not.norid.no - 198.133.199.104
- njet.norid.no - 198.133.199.105
- slave1.sth.netnod.se - 192.36.144.116

Legg merke til at navnetjenerne for Norid ligger på samme nettsegment, slik at en feil i BGP kan sette navnetjenerene til Norid ut av spill. Dette beskrives nærmere i kapittel 7.1.4. Basert på informasjon[45] fra Internett oppgis x.nic.no å befinne seg i Trondheim, y.nic.no å befinne seg i Oslo og z.nic.no å befinne seg i Ålesund. Navnetjeneren slave1 befinner seg i Sverige og er den eneste navnetjeneren for no-domenet som selv ikke er avhengig av no-domenet.

Tross i en relativ god fysisk redundans, antar vi at et langvarig tilgjengelighetsangrep mot alle navnetjenerene til no-domenet kan få konsekvenser for Norge. For eksempel kan et stort botnett deles inn i flere deler, som angriper navnetjenerne etter tur. Et slik angrep vil være svært vanskelig å beskytte seg mot, og vil måtte involvere mye kompetent personell utover norske ISP-er for å bli løst. Dette kan med andre ord ikke håndteres rent nasjonalt.

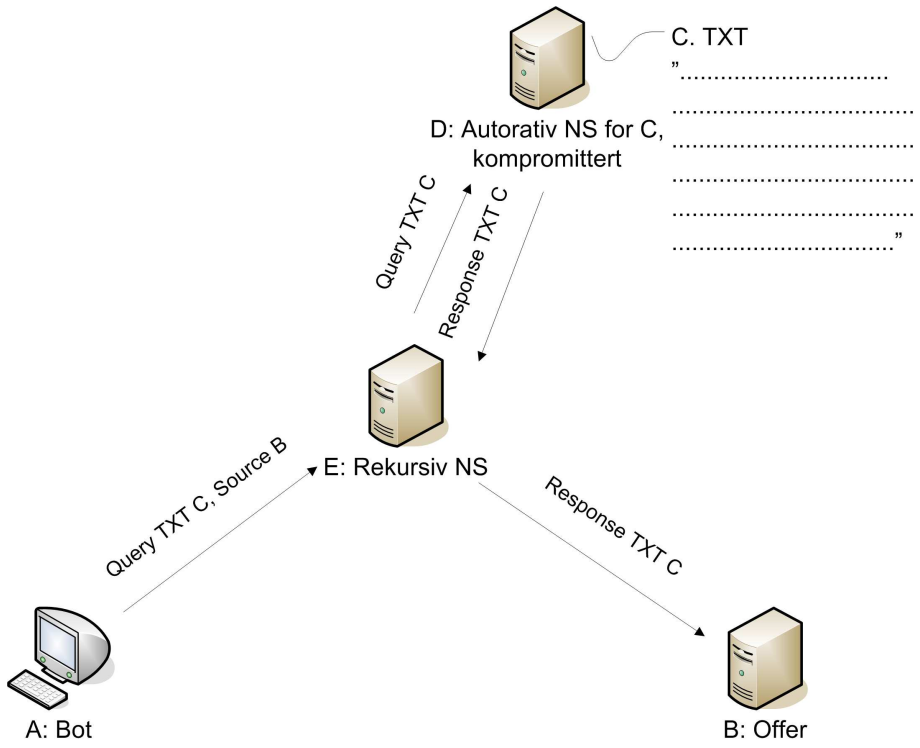
7.1.2 Logiske sårbarheter

Hvis en angriper klarer å endre på toppnivåfilen på de ”hemmelige” distribusjonstjenerne, vil dette for en kort periode kunne få alvorlige konsekvenser. For eksempel kunne alle IP-adressene til navnetjenerne for no-domenet settes til angripers maskin, og angriper ville dermed slippe å kompromittere no-navnetjenerne. Mest sannsynlig ville dette angrepet raskt blitt oppdaget av DNS-rottjeneroperatørene.

Antageligvis er det store forskjeller i typen operativsystem og programvare som kjøres på DNS-rottjenerne [41]. Sannsynligheten vil derfor være liten for at alle DNS-rottjenere kan rammes av den samme sårbarheten, slik at alle instanser ”samtidig” kan kompromitteres av for eksempel en orm. Det vil også være vanskelig å kunne nå alle rottjenere, siden trafikken vil rutes til den ”nærmeste”. Dermed er det mest effektive angrepet mot rottjenerne sannsynligvis et tilgjenglighetsangrep mot de 80 instansene fra et godt utspredt botnett.

Generelt sett vil man ved å angripe navnetjenere over målet i DNS-hierarkiet, kunne lede alle forespørsler om navn-til-adresse oversettelse til angripers falske navnetjener, som igjen svarer slik angriperen vil. Hvis for eksempel en eller flere av de seks navnetjenerne for no-domenet kompromitteres, vil forespørsler om IP-adressene til navnetjenerne tilhørende `ffi.no` bli besvart av angripers falske no-navnetjener. I andre omgang vil dermed forespørsler om IP-adressene til web-

[45] `http://www.geobytes.com/IpLocator.htm`



Figur 7.2: Åpne rekursive navnetjenere brukt som DDoS-forsterkere.

tjeneren eller e-posttjeneren på FFI også sendes til angripers falske FFI-navnetjener. På denne måten vil blant annet all e-post til FFI for en periode kunne havne hos angriperen.

Tidligere var de fleste navnetjenere på Internett satt opp til å besvare rekursive oppslag fra alle. Denne funksjonaliteten er i det siste tatt i bruk som en forsterker i forbindelse med distribuerte tjenestenektsangrep. Dette gjøres ved at maskiner i et botnett sender DNS-forespørsler med forfalsket avsenderadresse til en åpen rekursiv navnetjener. Forespørselen lages slik at den rekursive navnetjeneren vil gå til en (gjerne kompromittert) navnetjener og hente et langt svar. Dette svaret lagres hos den rekursive navnetjeneren, og vil siden sendes til den forfalskede adressen ved hver gjentatte forespørsel. Figur 7.2 illustrerer dette. Et slik angrep kan typisk gi en forsterkningsfaktor på rundt 70 - det vil si at for hver byte en angriper sender vil målet motta 70 byte. Et dokumentert angrep fra februar 2006 involverte 51000 rekursive navnetjenere og trafikk oppimot 6 Gb/s mot målmaskinene [53, 15].

I dag er det ansett som nødvendig praksis å separere rekursive og autorative navnetjenere. Den autorative funksjonaliteten må nødvendigvis være tilgjengelige fra hele verden, mens den rekursive kan beskyttes slik at den bare er tilgjengelig fra interne nett.

7.1.3 Sosiale sårbarheter

Berkeley Internet Name Domain (BIND) er en implementasjon av DNS som benyttes på en stor andel av navnetjenerne på Internett. I BIND versjon 4 og 8 eksisterer en sårbarhet som lar en ekstern angriper plante gale oversettelser mellom navn og IP-adresser i en navnetjener sin cache (cache forgiftning). Sårbarheten betinger at navnetjeneren er satt opp som en såkalt forwarder, som betyr at navnetjeneren utfører DNS-oppslag på vegne av andre gjerne interne navnetjenere ut mot Internett. I en test utført av Dan Kaminsky fra Doxpara Research i midten av juli 2005, ble 2,5 millioner navnetjenere kontaktet for å sjekke om de var sårbare [40]. Resultatet viste 230.000 potensielt sårbare navnetjenere og 16.000 som helt sikkert var sårbare for dette angrepet. BIND utgis i dag av Internet Software Consortium[46] (ISC). På ISC sine hjemmesider står det eksplisitt at BIND versjon 4 og 8 ikke må benyttes som forwarder, noe som har vært kjent siden april 2005. Allikevel er det et stort antall navnetjenere på Internett som ikke er oppgradert til BIND versjon 9, hvor denne sårbarheten er fjernet.

I 2004 gjennomførte Luis Grangeia en undersøkelse vedrørende en sårbarhet/konfigurasjonsfeil som kalles DNS-cache snooping [27]. En DNS-cache skal lagre alle oversettelser navnetjeneren finner ut av for en viss tid. Formålet med cachen er at navnetjeneren skal slippe å slå opp alle forespørsler, hvis den allerede har lagret svaret. Oversettelsene lagret i DNS-cachen tilhørende en organisasjon bør kun være tilgjengelige for de interne i organisasjonen. Hvis eksterne over Internett kan slå opp en oversettelse i en organisasjons DNS-cache, betyr dette at en intern i organisasjonen tidligere har slått opp det gitte navnet. En ekstern angripers mulighet for å ”snuse rundt” i organisasjonens DNS-cache vil dermed kunne avsløre mye av hvem organisasjonen har kommunikasjon med. Hvis for eksempel oversettelsen til e-posttjeneren til organisasjon A ligger i DNS-cachen til organisasjon B, betyr dette at noen i B mest sannsynlig har sendt e-post til noen i A.

Dette viser viktigheten av at systemadministratorer oppgraderer sine navnetjenere ved slike sikkerhetshull. Årsaken til at flere tusen navnetjenere fortsatt er sårbare er kun menneskelig svikt.

7.1.4 Avhengigheter

Et gitt domenenavn, slik som for eksempel `whitehouse.gov`, er avhengig av flere navnetjenere for at hvilken som helst klient på Internett skal kunne få tak i den korresponderende IP-adressen. I en studie om tillit i DNS, beskrives hvordan forskjellige domenenavn er avhengig av integriteten i andres navnetjenere [18]. Blant annet viser studien at `whitehouse.gov` er avhengig av integriteten til 40 navnetjenere, med forskjellige eierskap. Grunnen til dette er at navnetjeneren til `whitehouse.gov` blant annet må stole på navnetjeneren `a.gov.zoneedit.com`, og er dermed avhengig av alle navnetjenere for å finne IP-adressen til dette domenenavnet. I tillegg er det seks andre navnetjenere som har ansvaret for `whitehouse.gov`, som igjen har avhengigheter til

[46] `http://www.isc.org`

andre domenenavn. Hvilke navnetjenere som da involveres i et tilfeldig navneoppslag av domenenavnet, vil variere basert på blant annet lastbalansering. Hvis en av navnetjenerne `whitehouse.gov` er avhengig av kompromitteres, vil denne navnetjeneren kunne dirigere navnforespørslene til en valgt IP-adresse, eid av angriperen og med for eksempel en passordinnsamlende applikasjon. Dette er med andre ord et angrep mot massene, i og med at angriperen ikke kan bestemme hvilke navnetjenere en gitt klient benytter i navnoppslaget. Samtidig som man blir avhengig av integriteten til mange andre navnetjenere, vil også dette lage mange forskjellige muligheter for å finne riktig IP-adresse. Om dette gjør muligheten for å få riktig IP-adresse mer robust, kan dermed diskuteres.

I teorien skal det være mulig å utføre alvorlige angrep mot DNS via rutingprotokollen Border Gateway Protocol (BGP)[47]. Ved å få en eller flere BGP-rutere til å formidle kort vei til samtlige 13 IP-adresser tilhørende DNS-rottjenerne, vil man kunne rute forespørslene et helt annet sted. Angriperen kan i teorien sette opp mange falske DNS-rottjenere som svarer på forespørslene, men mest sannsynlig vil nok den store trafikkmengden skape store problemer for ruterne på Internett. Legg merke til at dette angrepet langt fra vil ramme alle DNS-rottjenerbrukere, da mange vil være nærmere de ekte instansene av DNS-rottjenerne enn de falske. BGP kan også (u)tilsiktet sette navnetjenerne til en organisasjon ut av spill. Hvis alle navnetjenere plasseres på et subnett og BGP tilbakekaller dette subnettet, vil ingen eksterne kunne kommunisere med navnetjenerne. Dette vil blant annet føre til at få på Internett klarer å sende e-post til organisasjonen.

Generelt bør man ha flere enn en navnetjener, navnetjenerne bør ikke stå på samme subnett eller bak samme ruter, samt man bør få andre organisasjoner til å kjøre en av navnetjenerne. For eksempel er en av no-navnetjenerne plassert under se-domenet (`slave1.sth.netnod.se`). Med andre ord, navnetjenerne tilhørende et domene bør ha fysisk og logisk redundans. I perioden 1998 til 2003 ble det blitt utført undersøkelser av com- og landdomene i forhold til fysisk og logisk redundans [20]. Undersøkelsene plukket ut tilfeldige domener under com- og landdomenet og kontaktet de tilhørende navnetjenerne. Domenene ble sjekket for om de hadde flere enn en navnetjener og om de eventuelt hadde plassert alle sine navnetjenere på et subnett. I oktober 2001 viste undersøkelsen at blant de tilfeldig utvalgte domenene under no-domenet, hadde 29,5% alle sine navnetjenere på samme subnett og 5,7% hadde kun én navnetjener. I 2001 ble alle navnetjenere tilhørende Microsoft tatt ned i over et døgn blant annet på grunn av at alle navnetjenerne var plassert på et subnett.

7.1.5 Oppsummering

Dette kapittelet har vist at navnetjensten er sårbar for angrep på alle nivåer i DNS-hierarkiet. Resultatet av angrepene er enten tilgjengelighetsangrep eller at det gitte navnet oversettes til feil IP-adresse. På denne måten kan en angripe stoppe eller styre kommunikasjonen til brukerne.

Vellykkede angrep mot de ”hemmelige” distribusjonstjenerne til IANA vil gi mulighet for å endre toppnivåfilen som benyttes av de minst 80 rottjenerne. Langvarige tilgjengelighetsangrep mot rottjenerne vil føre til at oversettelser registrert i cacher hos nanvetjenere på Internett utgår på dato.

[47] Se kapittel 9.

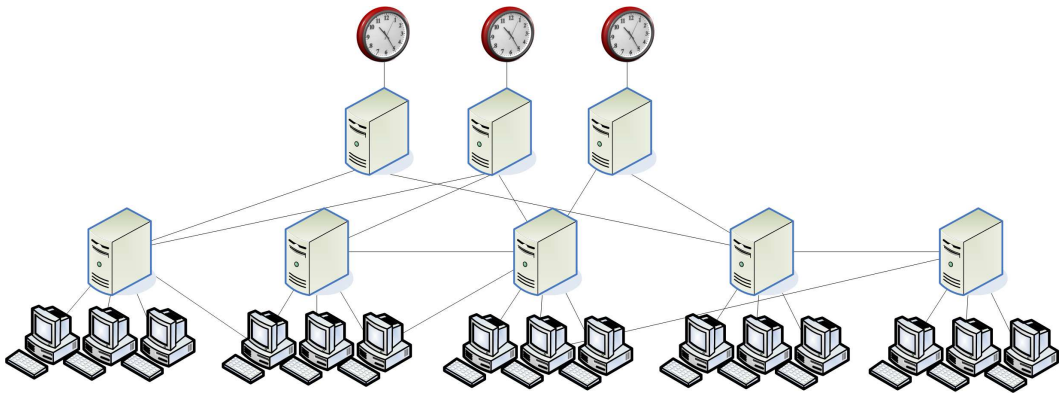
Dette vil føre til at brukerne av disse navnetjenerne ikke får oversatt navn til IP-adresse. I teorien vil dette kunne stoppe store deler av datatrafikken på Internett, men i praksis vil nok slike angrep i de fleste tilfeller raskt oppdages og etterhvert rettes. Langvarige tilgjengelighetsangrep mot navnetjenerne til forskjellige land og toppnivådomener vil naturlig nok skape problemer, men også her antas det at dette vil kunne bli rettet ved hjelp av mye kompent personell i ISP-ene.

Ved å angripe internettilbyderens eller organisasjonens navnetjener, vil man kun ramme de som er avhengig av denne i form av tjenestenekt eller villedning. Dette blir i realiteten alle privatkunder tilhørende internettilbyderen eller organisasjonens ansatte, og brukere av tjenester organisasjonen tilbyr (web og e-post).

7.2 Tidstjenesten

Network Time Protocol (NTP) er en distribuert tidshåndteringstjeneste for distribusjon og synkronisering av UTC-tid uten sentral styring. Tjenesten er en av de lengst kontinuerlig kjørende distribuerte tjenestene på Internett, og kan spores tilbake til begynnelsen av 1980-tallet [48].

Maskinene som deltar i et NTP-system danner en hierarkisk samling. Toppnodene er direkte tilknyttet hver sin tidskilde, kalt referanseklokke, og sprer tiden til noder på nivået under. Nivået til referanseklokkene kalles stratum 0, og kan for hver av disse kun aksesseres av sin direkte tilknyttede toppnode på stratum 1. Påfølgende nivå av maskiner, stratum 2, kobler seg opp mot en eller flere stratum 1-maskiner for å motta tid, og slik fortsetter hierarkiet nedover. Ved å koble seg opp mot flere maskiner på et høyere nivå sikrer man seg både mot frafall av tjenere og øker sannsynligheten for å få korrekt tid. Se figur 7.3.



Figur 7.3: Eksempel på NTP-hierarki fra stratum 0 til 3.

Tidstjenere under nivå 1 blir ofte synkronisert horisontalt dersom det er flere tidstjenere på samme nivå i nettverket. Slik oppnår man bedre konsistens i et større NTP-hierarki.

Utregningen av korrekt tid foregår ved matematiske algoritmer som med tiden har blitt relativt

komplekse. Klienter og tjenere utveksler UDP-pakker med tidsstempler på en slik måte at estimater av pakkenes prosesseringstid og overføringstid er med i utregningen. NTP estimerer også ujevnheter ved lokal klokke og korrigerer for dette. Usymmetrisk og ujevn overføringstid samt uregelmessigheter ved lokal klokke kan føre til at tidspunktene som benyttes i utregningene forskyves og resultatet blir unøyaktig. Vanligvis vil variasjoner i nettverksforbindelsene dominere usikkerheten for klientene. På Internett kan man typisk oppnå en tid med nøyaktighet innenfor 1 til 50 millisekunder, avhengig av tidskilden og nettverksforbindelsen [49].

NTP er meget forsiktig med å justere tiden på en abrupt måte. Ved tidsforskjeller under 128 ms vil NTP gradvis redusere forskjellen mellom lokal og estimert korrekt tid[48]. Ved tidsforskjeller mellom 128 ms og 900 sekunder vil klokken foreta et hopp, og ved forskjeller over 900 sekunder vil NTP-algoritmen nekte å tilpasse lokal klokke [48].

I motsetning til DNS, som brukes for diskrete og uavhengige navneoppslag, må klokken til en datamaskin vedlikeholdes jevnlig for å opprettholde korrekt tid. Hvis en maskin mister all kontakt med dens tidstjenere, vil maskinens klokke begynne å drive fra referansetiden. Hvor fort dette skjer, og om brukeren blir gitt beskjed, avhenger av de fysiske komponentene til klokken i maskinen og implementasjonen av NTP-klienten.

I de tilfeller hvor nøyaktigheten til tiden ikke er kritisk, kan en forenklet versjon av NTP, kalt Simple Network Time Protocol (SNTP), benyttes. SNTP benytter enklere algoritmer, har kun enkle forbindelser[49] og gir dårligere nøyaktighet sammenliknet med NTP. NTP og SNTP er kompatible ved at en (S)NTP-klient ikke ser forskjell på en NTP-tjener og en SNTP-tjener, og ved at en (S)NTP-tjener ikke ser forskjell på en SNTP-klient og en NTP-klient. SNTP kan benyttes der hvor en full NTP-implementasjon er for stor eller kompleks [49].

7.2.1 Fysiske sårbarheter

Det eksisterer ikke noe felles NTP-hierarki på Internett som alle må delta i for å benytte seg av NTP-tjenester, slik som det gjør for DNS-tjenesten. Hvem som helst kan sette opp en NTP-tjener som stratum 1 og gjøre den tilgjengelig for andre. Dette innebærer at det i utgangspunktet ikke finnes noe sett med kritiske toppnoder hvis frafall vil lamme en global NTP-infrastruktur.

Dette er dog en sannhet med visse modifikasjoner. Selv om det ikke er satt opp ett offisielt og autoritativt tidskilderegime for allmenn bruk på Internett, tilbyr noen organisasjoner, deriblant National Institute of Standards and Technology (NIST) og US Naval Observatory (USNO), åpen tilgang til egne tidstjenere. USNO og NIST er kilder for offisiell UTC-tid i USA, og NTP-nettverket som disse og andre tidstjenere utspenner kalles for det offentlige NTP-subnettet [48].

[48] De gitte absoluttverdier er konfigurerbare.

[49] Tilstandsløse klient/tjener-forbindelser, i motsetning symmetriske peer-til-peer-forbindelser mellom synkroniserende NTP-tjenere på samme nivå.

Andre tidstjenere kan også tilhøre private eller mer avgrensede NTP-nettverk, med varierende grad av åpenhet for andre internettbrukere. Blant annet vedlikeholder utviklerne av referanseimplementasjonen av NTP lister over offentlig tilgjengelige internettidstjenere på stratumnivå 1 og 2 med ulik åpenhet[50].

Lasten på offentlig tilgjengelige tidstjenere kan bli meget stor, og NIST har nå rundt 2 milliarder forespørsler per dag, noe som innebærer over 20.000 NTP-forespørsler per sekund. Antall brukere estimeres til 100 millioner [58]. På grunn av overbelastningsproblemet er det på frivillig basis satt opp en egen lastbalanserende samling (pool) av NTP-tjenere, hvor tilbydere av tidstjenere kan registrere sine tjenere[51]. En bruker kan konfigurere sin maskin til å slå opp `0.pool.ntp.org`, `1.pool.ntp.org` og `2.pool.ntp.org`, eller med et mer begrenset geografisk omfang som `0.europe.pool.ntp.org` eller `0.no.pool.ntp.org`, som så plukker tilfeldige tidstjenere fra samlingen.

Per januar 2007 var det 895 medlemstjenere i samlingen, hvorav 541 var i Europa og 236 i USA. Fordelingen innad i Europa er dog ujevn, med Tyskland, England og Nederland på topp med henholdvis 137, 61 og 49 tidstjenere. Norge har 9 registrerte tidstjenere i denne listen. Det er uvisst hvor mange brukere det er av disse offentlige tidstjenerne, men `ntp.pool.org` estimerer et sted mellom 2 og 6 millioner brukere.

I Norge er det Justervesenet[52] som har ansvaret for måleteknisk infrastruktur, deriblant tid. Justervesenet har ikke noen åpen leveranse av tid på samme måte som NIST, men har hatt et prøveprosjekt gående i flere år med distribusjon av tid via NTP over Internett til en mindre kundegruppe. Disse kundene lar kun et fåtall tidstjenere kommunisere direkte med Justervesenet, for så å distribuere tiden i egen virksomhet via egen tidsinfrastruktur. Det er ikke planer om å åpne opp for allmenheten på dette tidspunkt.

7.2.2 Logiske sårbarheter

NTP benytter forbindelsesløse UDP-pakker og det er derfor meget lett å forfalske avsenderadresser. Dette muliggjør en rekke typer angrep som er mer kompliserte å gjennomføre med en forbindelsesorientert protokoll som TCP. En maskin som lytter på utgående tidsforespørsler på nettverket og som svarer raskere enn den ekte tidstjeneren, kan få falske tidspakker godtatt av klienten. Det er imidlertid ikke helt trivielt å få falske tidsstempler godtatt, da NTP-protokollen ikke liker store eller raske endringer av tiden.

Maskiner som villet eller ved en feiltakelse sender feil tid kalles feiltikkere (falsetickers), i motsetning til sanntikkere (truechimers) som leverer korrekt tid. NTP har mekanismer for sikring mot slike maskiner. Hvis en klient bruker flere tidstjenere, vil en algoritme velge ut de tidsstemplene som sannsynligvis er mest korrekte.

[50] `http://ntp.isc.org/bin/view/Servers/WebHome`
[51] `http://www.pool.ntp.org`
[52] `http://www.justervesenet.no`

For å beskytte seg mot feiltikkere anbefales man å følge formelen $n \geq 2k + 1$, hvor n er antall tidstjenere, og k antall feiltikkere man ønsker å beskytte seg i mot. Formelen brytes for $k = 1$, og det anbefales at antall tidstjenere ikke er mindre enn 4 [68]. Denne regelen krever imidlertid flere tidskilder enn det som er strengt nødvendig for å beskytte mot feiltikkere, fordi den også tar hensyn til andre algoritmer som forbedrer tidsestimatet [7].

Versjon tre og fire av NTP innehar mekanismer for autentisering basert på kryptografi. Versjon tre støtter meldingsautentisering basert på symmetrisk kryptografi med forhåndsdelte nøkler. Versjon fire går videre og støtter en variant av offentlig nøkkelkryptografi med protokollen Autokey [48]. Dette er en mer komplisert oppgave enn ved første øyekast, da en i utgangspunktet trenger et tillitshåndteringssystem (PKI) for å spre verifisert tid, men samtidig er avhengig av korrekt tid for at et slikt system skal fungere. Dette krever at autentiseringsmekanismen og synkroniseringsmekanismen samarbeider meget tett [48]. Tidstjenesten stiller også effektivitetskrav som en tradisjonell løsning basert på offentlig nøkkelkryptografi ikke vil tilfredsstille [47].

Det er vanskelig å estimere i hvilken grad mekanismene for autentisering benyttes. Versjon fire er beskrevet som operasjonelt, men ikke spesielt utbredt [48], og behovet ved bruk av versjon tre for forhåndsdelte nøkler gjør at en offentlig tilgjengelig tidstjeneste neppe vil tilby autentisert tid med tanke på de ekstra omkostningene rundt drift og administrasjon. Konsekvensene ved kompromittering av en nøkkel delt av mange ville påført mye arbeid. Dette gjør at man i mange situasjoner vil se NTP brukt uten kryptering.

Eksempelvis har NIST i skrivende stund ingen planer om å tilby autentisering av sin tidstjeneste over Internett, og foretrekker heller å overlate dette til private firmaer som så kan tilby utvidede tjenester basert på tidstjenerne til NIST mot betaling [58]. Hvis NIST skulle ha drevet et autentiseringssystem av nødvendig størrelsesorden ville kostnadene antakelig vært så store at NIST måtte ha tatt seg betalt for en slik tjeneste, noe som ville ha ført til et behov for utvidelse av det organisatoriske apparat.

Manglende data gjør det vanskelig å estimere konsekvensene av et rettet angrep mot flere tidstjenere på Internett, men for den vanlige sluttbruker er det rimelig å anta at et slikt angrep vil være mindre synlig enn et angrep mot DNS-tjenere. Et tjenestenektangrep mot DNS vil ha umiddelbare konsekvenser for anvendbarheten av Internett, mens NTP ikke er kritisk på samme måte. Brukere som anser seg selv som meget avhengige av tid har muligheten til å sette opp egne referansekilder som ikke er avhengige av Internett, men lite er kjent om i hvilken grad dette gjøres.

7.2.3 Sosiale sårbarheter

Det finnes flere eksempler på at dårlig design og feilkonfigurasjon av NTP-klientprogramvare fører til at lasten på offentlige tidstjenere blir stor. For eksempel oppfører flesteparten av brukerne av NIST sin tidstjeneste seg normalt, mens noen relativt få brukere skaper mye unødvendig trafikk [50].

I en studie av tidstjenere på Internett i 1999 ble det funnet at et overraskende antall stratum 1-tjenere hadde stor tidsforskyvning [51]. Av totalt 907 tjenere som hevdet å være stratum 1 var det kun 363 (40%) som lå innenfor en tidsforskyvning på ett sekund. Av de 391 stratum 1-tjenerne som hadde mer enn 10 sekunder med tidsforskyvning var 373 (95%) satt til kun å bruke lokal klokke som referansekilde. Et lyspunkt var at mekanismene NTP benytter for å luke ut dårlige tidstjenere fungerte bra, da kun 157 av 175,000 maskiner valgte en slik dårlig klokke for synkronisering[53].

Det har vært flere eksempler på at leverandører av nettverksenheter som benytter seg av tidssynkronisering med NTP eller SNTP har konfigurert enhetene med en naiv standardkonfigurasjon. I mai 2003 ble NTP-forespørslene til en offentlig tidstjener hos universitetet i Wisconsin-Madison mer enn doblet i løpet av et par timer, før trafikken ble blokkert. Hendelsen ble antatt å være et distribuert tjenestenektangrep, men det viste seg etter hvert at programvaren i en serie rutere hadde blitt hardkodet med IP-adressen til universitetets tidstjener. Ruterne sendte én forespørsel per sekund hvis svar ikke ble returnert. Over tid steg antall forespørsler fra et normalt gjennomsnitt på 40.000 pakker til over 250.000 pakker per sekund [61].

Mer enn 700.000 enheter med denne standardkonfigurasjonen er levert, og på tross av tilgjengelige oppdateringer av programvaren hvor dette er rettet, er det fremdeles pågang på universitetets tidstjener fra denne typen enheter. Prosessen rundt synkronisering av tid er lite synlig for en vanlig bruker, som neppe vet hvordan ruteren setter tid og har liten grunn til å sjekke oppdateringer. Problemet kan således ikke løses med rene tekniske grep. Universitetet, som fremdeles må forvente mange NTP-forespørsler grunnet statisk ruterkonfigurasjon, samarbeider både med leverandør og nettoperatør for å håndtere dette på best mulig måte [61].

7.2.4 Avhengigheter

En bedrift eller større organisasjon kan velge å sette opp egne stratum 1-maskiner med referanseklokker, for så å spre tiden til nettverksutstyr og andre klienter internt. Alternativt kan offentlig tilgjengelige tidstjenere på Internett benyttes.

Det er vanskelig for driftspersonellet til en åpent tilgjengelig tidstjener å vite hvem som benytter seg av tjenesten og hvorfor den benyttes, da brukerne sjeldent har behov for direkte kontakt. NIST beskriver likevel typiske kunder av deres tidstjenester på Internett [44]. Systemene som synkroniseres inkluderer systemer for elektronisk handel og tidsstempling av transaksjoner, systemer for autentisering og validering, distribuerte databasesystemer, distribuerte loggsystemer, mer spesielle maskinvaresystemer som parkeringsbillettsystemer og tidsstemplingssystemer for ansatte, samt kontor- eller hjemmemaskiner for individuelle brukere som ønsker korrekt tid. I hvilken grad disse også har egne referanseklokker for redundans er ikke kjent.

Tidsforskjellen mellom synkroniserte tidstjenere varierer med nettverkslast og andre faktorer, men for deres tjenere estimerer NIST at forskjellen ligger på rundt 5 millisekunder, og en klient med god

[53] Av 175,000 maskiner var 729 i “peer”-forhold og 157 hadde valgt dårlig klokke for synkronisering.

forbindelse kan bli synkronisert med denne usikkerheten. En klient med dårlig nettverksforbindelse kan få en mye større tidsforskyvning, med en usikkerhet på mer enn ett sekund [44].

Lite er kjent om ulike systemers avhengigheter av korrekt tid. Det er lett å liste opp systemer som benytter tid i kjerneområder, som for eksempel systemer for autentisering og adgangskontroll, tillitshåndtering (PKI), backup, regnskap, databaser og filsystemer. I hvilken grad disse eller andre systemer er avhengige av tid på ukjente måter er det verre å svare på. Det er ikke lett å se et systems avhengighet av korrekt tid, likeledes er det lite data om hvor lett eller vanskelig det er å gjennomføre praktiske angrep indirekte via tidshåndteringstjenesten for å manipulere ulike systemer.

En åpenbar avhengighet av korrekt tid er ved ulike former for loggføring, noe som understøttes av samtaler med ISP-er. Synkronisert tid er viktig for å kunne sammenstille informasjon fra flere kilder, for eksempel ulike loggfiler ved rekonstruksjon av hendelsesforløp. Uten synkronisert tid er det vanskelig å få oversikt over hendelsesforløpet, spesielt med tanke på juridiske krav til bevis ved påtale.

7.2.5 Oppsummering

For den vanlige hjemmebruker er tidstjenesten en mindre kritisk tjeneste, og frafall av tjenesten kan i en rekke tilfeller gå uoppdaget over lengre tid, om den i det hele tatt benyttes. En rekke tyngre brukere benytter seg også av offentlig tilgjengelig tidstjenere, ofte for å synkronisere tid i sine produksjonssystemer. Det er usikkert hvor dramatisk et frafall av tidstjenesten vil være for disse og hvor lang tid som eventuelt må gå før det blir kritisk. Trolig vil kun systemer med store krav til korrekt tid bli direkte forstyrret, da lokal klokke neppe vil drive langt innen tjenerne kommer opp igjen. Muligheten for lokale referanseklokker uten koblinger mot Internett gjør også at kritiske systemer kan være uavhengige av tid fra Internett, i alle fall i direkte forstand. Indirekte avhengigheter via andre systemer er vanskeligere å avklare.

Det er også usikkerhet om systemer som benytter tidstjenesten er åpne for manipulasjon via denne, og hva slags konsekvenser villet endring av tid vil ha.

8 Kommunikasjonsinfrastrukturen

En sentral funksjon i Internett er kommunikasjonsinfrastrukturen. Denne står fundamentalt for transport av informasjon i form av IP-pakker mellom alle brukerne av Internett. Man kan si at denne delen av Internett avgrenses oppover til og med lag 3 i OSI-stakken. Fysisk og logisk er dette et svært sammensatt nettverk med utbredelse over hele verden.

Dette nettverket kan innledningsvis deles inn i to hovednivåer. Det øverste nivået består av en rekke mindre nettverk kalt autonome system (AS) knyttet sammen av rutere. Det laveste nivået består av transport- og aksessnett (se 8.2) som fysisk knytter ruterne i AS-ene sammen. Et AS er et nettverk med en klart definert rutingpolicy som registreres hos IANA. Kravet om en rutingpolicy er helt nødvendig for å få registrert et AS, som beskrevet i retningslinjer for opprettelse, valg og registrering av et AS i RFC 1930 [34]. Her beskrives et AS som *"the unit of routing policy in the modern world of exterior routing"*.

En tilbyder av internettjenester (ISP) vil normalt basere sitt tjenestetilbud på et nettverksdomene bestående av ett eller flere sammenknyttede AS-er. Også virksomheter som ikke tilbyr offentlige internettjenester vil kunne ha sin del av nettet organisert som et AS. Eksempel på sistenevnte er Oslo Børs og Elkem. Et AS kan ha svært varierende størrelse, og nettstrukturen i et lite AS vil kunne være svært forskjellig fra den i et stort AS.

Hvert enkelt av disse AS-ene består videre av lagdelte kommunikasjonsnettverk, som fysisk binder sammen brukere eller kunder i det aktuelle geografiske interesseområdet. Størrelsen og geografisk utbredelse av disse kommunikasjonsnettverkene er helt avhengig av markedsmessige forhold som brukervolum og anvendelse. De ulike aktørene vil knytte sin del av Internett (nettdomene) til det øvrige Internett gjennom i hovedsak to måter, enten via tilknytning til et offentlig sammenknyttingspunkt (IXP[54]) eller gjennom en direkte privat forbindelse (private peer) til en annen aktørs nett. Hvilke slike aktører det er naturlig å knytte seg opp mot vil i stor grad være et økonomisk spørsmål. Disse kan være både konkurrenter og samarbeidspartnere.

I den videre beskrivelsen i dette kapitlet rettes det fokus mot ISP-er "av en viss størrelse". Typiske aktører i Norge vil være Telenor, NextGenTel, Tele2 og BaneTele. Også UNINETT på universitetssiden innehar et betydelig nett. I en åpen publikasjon er det ikke mulig å gå konkret inn på detaljer rundt disse virksomhetenes nett og operasjon, i den grad dette måtte være kjent for prosjektet. Grunnlaget for beskrivelsen i dette kapitlet bygger dels på informasjon innhentet gjennom lengre tids kontakt med enkelte av operatørene og dels i åpen informasjon rundt høynivå design av nettverk (HLD).

[54] Internet eXchange Point.

8.1 Overføringslaget

Overføringslaget består fundamentalt av et nett med rutere som gjennom logiske eller fysiske forbindelser knytter sammen ulike geografiske entiteter. En eller flere rutere utgjør ett nettelement og er lokalisert i såkalte "Points of Presence" (POP). Disse POP-ene har ofte en intern struktur med sammenknytning av flere rutere. Ruterne innen en POP kan ha enn viss fysisk spredning, for eksempel til to forskjellige bygninger innen en bedrifts område, eller i to forskjellige bydeler i en by. Karakteristisk er at knytningen internt mellom ruterne innen en POP er svært robust.

Den viktigste egenskapen til overføringslaget er tjenesten for overføring av informasjon som datagrammer (IP-pakker). Ruterne inneholder ulike funksjoner for å kunne transportere slike informasjonspakker mellom brukere, der rutingfunksjoner og rutingprotokoller er de mest sentrale (se kapittel 9.2). Tjenestekvalitet eller "Quality of Service" (QoS) utgjør en viktig egenskap ved overføringstjenesten og er karakterisert ved forsinkelse, tilgjengelighet, prioritet og så videre. Ulike anvendelser, som for eksempel tale, e-post og video, vil ha ulike krav til tjenestekvalitet. Med økende behov for slike tjenester er det et stadig sterkere behov for mekanismer i tjenestenettet som støtter differensiert tjenestekvalitet.

8.2 Transportnettet

Transportnettet består av nettverksnoder og -forbindelser i kommunikasjonsinfrastrukturen som sørger for den fysiske transporten av informasjonspakkene mellom ruterne i POP-ene i overføringslaget. Transportnettet er i tillegg til å være bærer for informasjonspakkene mellom ruterne i overføringslaget i Internett, samtidig også bærer for andre tilsvarende typer tjenestenett, for eksempel mobiltelefoni- og bedriftsdatanett. De ulike anvendelsene bruker samme ressurser i transportnettet gjennom multipleksingsteknikker i tid og rom. Multipleksing er kort forklart at ulike informasjonsstrømmer mates inn i én informasjonsstrøm. Transportnettet med sine fysiske forbindelser og logiske multipleksede forbindelser utgjør dermed et eget nettverk i flere nivåer. Transportnettet vil kunne ha en annen struktur og utbredelse enn nettverket i overføringslaget. Ofte vil det være kunde-leverandør-relasjon mellom operatører på overføringslaget og operatør-operatør-relasjon i transportnettet. En vil også ofte se at flere operatører av transportnett leverer tjenester til ett og samme overføringslag i et AS. Dette kan ha årsak i ønske om økt robusthet gjennom økt redundans i viktige deler av nettet, eller at ulike aktører har forskjellig tjenestetilbud i ulike geografiske områder.

Transportnettet utgjør dermed den fysiske forutsetningen for all elektronisk kommunikasjon. Den enkelte kommunikasjonsforbindelsen har derfor typisk høy kapasitet, og er i dag de fleste steder basert på optisk fiberkabel. Fiberkabler vil kunne inneholde flere hundre fiberpar, der hver av fiberparene i et bølgelengdemultiplekset system (WDM[55]) har potensiale for toveis overføring av flere terabits/s. Typiske overføringsrater fra fiberbaserte transportnett levert til overføringslaget i Internett vil i dag være i størrelsesorden fra 155 og 622 Mbit/s, opp til 2,5 og 10 Gbits/s.

[55] Wavelength Division Multiplexing.

Radioforbindelser i transportnettet benyttes primært i forbindelse med radiolinjesystemer og satellittsystemer. Disse systemene vil ikke kunne tilby like gode overføringsrater, og er derfor nå mest benyttet i områder der befolkningstetthet eller geografiske forhold gjør at utrulling av fiberkabler ikke er lønnsomt. For radiolinjesystemer er det i offentlige nett i dag vanlig med overføringskapasitet i et multippel av 155 Mbit/s. Metallisk kabel er i dag i svært liten grad benyttet i transportnett.

Utviklingen innen transportnetteknologi har gått fra at transportnett tilbyr rene punkt-til-punkt-forbindelser basert på det plesiosynkrone multiplekshierarki (PDH), til sammensatte logiske nettstrukturer med flere veier og dermed også innlagt redundans (reserveveier). Ringstrukturer basert på det synkrone digitale multiplekshierarkiet (SDH) er et tidlig eksempel, mens man nå i tettbefolkede områder går mot transportnett med maskestruktur basert på fiber med bølgelengdemultipleksing og med tiden også optisk svitsjing [86].

Med dette går utviklingen mot mer komplekse nettstrukturer også i transportnettet, som derigjennom også kan tilby ulike former for redundans for de som kjøper transportnettjenester. Det vil si at en ISP i prinsippet kan kjøpe redundans mellom to rutere gjennom tjenester i transportnettet. Dette kan i utgangspunktet sees på som komplementært eller som alternativ til redundans på et logisk nivå i overføringsnettet.

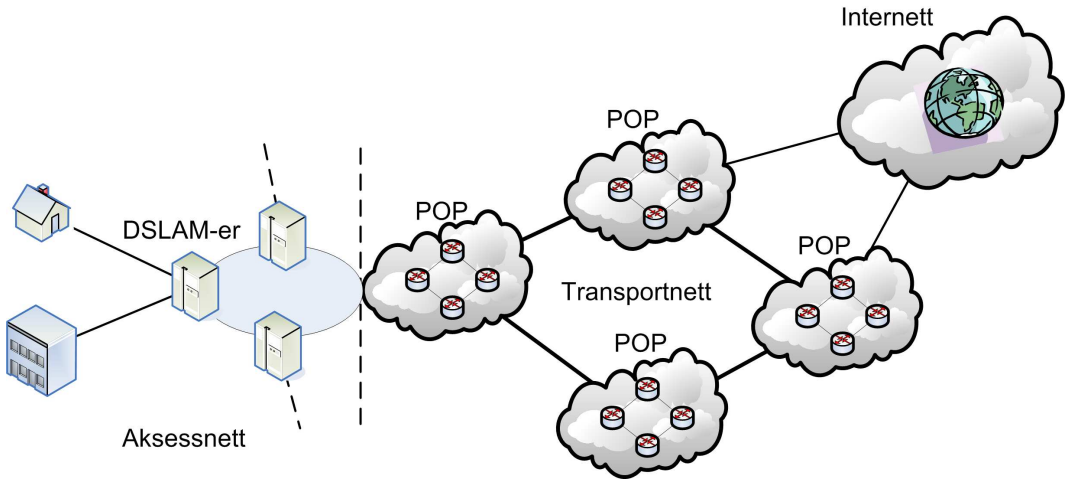
Imidlertid er det viktig å understreke at antall veier i fysisk transportnivå er svært begrenset. Å legge fiberkabler er relativt kostbart, og slike kabler blir da også ofte ført langs annen offentlig infrastruktur som veier, jernbane eller kraftledninger. Tilsynelatende uavhengige leverandører av transportnettjenester kan også ofte ha sine forbindelser i kabler i samme kabeltrase, og endog også i samme fysiske kabel. Som eksempel på utbredelse er det i [39] vist Telenors fiberbaserte stamnett i Norge. En karakteristisk egenskap med dette nettet er at det mange steder inneholder relativt få alternative fysiske veier, særlig i Nord-Norge. Dette har stor betydning for den fysiske robusthet det er mulig å realisere i ulike tjenestenett, deriblant Internett.

For øvrig vises det til “Sårbarhet i offentlig telekommunikasjon” [59] og “Analyse av sårbarhetsregulerende tiltak innen telekommunikasjon” [30] for mer inngående beskrivelse av transportnettet.

8.3 Aksessnettet

Aksessnettet står for tilknytningen av den enkelte brukeren til nærmeste tjenestenode/POP i sin ISPs nettverk. I dette ligger en aggregering av de ulike brukernes kommunikasjonsbehov som er tilknyttet nettet. Aksessnettet står dermed også for tilknytningen av den enkelte brukeren til transportnettet, som vist i figur 8.1 på neste side. Aksessnettet er vanligvis ikke definert som del av transportnettet, selv om den har tilnærmet samme funksjon i protokollstakken.

Karakteristisk for aksessnettet er at teknologiene på det overliggende logiske nivået, for eksempel Ethernet, er svært knyttet til teknologien i den fysiske overføringskanalen. I aksessnettet realiseres overføringskapasitet i forhold til det enkeltbrukeren har behov for og den teknologien som måtte



Figur 8.1: Tilknytning til POP.

være tilgjengelig i forhold til dennes fysiske plassering i forhold til nettet. Mangfoldet av teknologier er stort. Eksempelvis vil en bruker med behov for lav overføringskapasitet kunne knytte seg opp mot Internett gjennom en offentlig levert ISDN-tjeneste. Her benyttes en eller flere tradisjonelle digitale telefonikanaler til å knytte brukeren inn i nettet. Ulempen med denne metoden er imidlertid lav overføringskapasitet og både kostbar og stivbeint oppkobling og nedkobling av forbindelse.

I den andre enden av ytelsesspekteret vil typisk en stor bedrift kunne ha sin egen fysiske fiber-tilknytning til Internett. Også privatabonnenter blir i økende utstrekning tilknyttet optiske fiberkabler og gjennom det tilbudt "triple-play", det vil si kabel-TV-, internett- og telefonitjeneste i ett integrert abonnement.

Mest vanlig i dag er DSL-teknologier (Digital Subscriber Line), der man gjennom avanserte digitale linjekodingsteknikker kan overføre relativt store mengder informasjon over eksisterende kobber-basert parkabel. Dette kan være samme parkabel som i dag kun benyttes til telefoni. Avhengig av kabelkvalitet og lengde på kabel mellom sluttbrukeren og nærmeste offentlige EKOM-punkt, kan man i dag oppnå en kapasitet på i størrelsesorden 10 - 20 Megabit/s. Mest vanlig i dag er Asymmetric DSL (ADSL). Fysisk er det i aksessdelen av nettet utplassert såkalte DSLAM-er (Digital Subscriber Line Access Multiplexer), som i praksis tilbyr en multiplekserfunksjon. I figur 8.1 er brukerens tilknytning til en ISPs POP gjennom bruk av DSL i aksessnettet skissert.

Radiobasert brukeraksess er også i ferd med å bli utbredt, der Worldwide Interoperability for Microwave Access (WiMax[56]) er eksempel på en standard som er i ferd med å få stor utbredelse. Med en enkel antenne på husveggen og en mottaker vil man kunne få ytelse opp mot noen Mbits/s. Dette utstyret er også i ferd med å bli rimelig og vil ofte ha marked der tradisjonelle DSL-teknologier ikke er mulig, men kan også være en direkte konkurrent til kabelbaserte xDSL-teknologier.

[56] `http://wimaxforum.org`

Uansett teknologi vil normalt nettstrukturen i den ytterste delen av aksessnettet ha en relativt ren stjernestruktur, men i enkelte tilfeller også kunne ha et innslag av trestruktur. Der kabel-TV-nett benyttes som aksessteknologi til Internett, har man ofte en ren tre-struktur. Aksessnettet har dermed en struktur som er helt ulikt transportnettet, som tidligere nevnt normalt tilbyr flere mulige veier mellom to vilkårlige geografiske punkt.

Den enkelte brukeren vil dermed normalt ha kun én fysisk og logisk tilknytning til Internett. Har brukeren behov for større robusthet gjennom redundans, kan denne ved kjøp av en tilleggstjeneste velge å knytte seg opp med flere fysiske og/eller logiske forbindelser gjennom aksessnettet til en ISPs nettverk. Innehar en bruker eget AS vil den også kunne ha alternative fysiske og logiske tilknytninger til flere alternative ISP-ers internettjenester.

Til slutt kan det også nevnes at mobile tjenester som GSM/GPRS, UMTS og 4. generasjons mobil-tjenester blir stadig mer egnet som tilknytningsmetode til Internett.

9 Overføringslaget

Overføringslaget utgjør et sammenkoblet nett med IP-rutere, som tilsammen muliggjør kommunikasjon av IP-pakker mellom geografisk atskilte datamaskiner. Ruterne kan forenklet deles inn i to forskjellige kategorier, de som ruter IP-pakker internt i et AS og de som ruter IP-pakker mellom AS-er. Et viktig prinsipp for ruting i Internett er at en gitt datapakke alltid skal ha minimum to veier videre fra en gitt ruter. Dette er svært viktig i forhold til Internetts robusthet, men er på ingen måte påkrevd.

For brukere med trafikk som flyter innenfor en ISPs nettdomene, som kan bestå av ett eller flere AS-er, vil robusthet være en funksjon av ISP-ens nett- og sikkerhetsarkitektur. Med en gang informasjon skal flyte på tvers av flere ISP-ers AS-er, vil spørsmålet om robusthet bli betydelig mer sammensatt. Man er da avhengig av hvordan nettstrukturen i alle involverte AS-er som inngår i et kommunikasjonsbehov er bygget opp.

Ett viktig ledd i dette er hvordan samtrafikk mellom de ulike AS-ene er realisert fysisk og funksjonelt. Samtrafikk vil være realisert gjennom en direkte forbindelse mellom to AS-er (peer), gjennom et offentlig samtrafikkpunkt eller begge deler. Den fysiske og logiske forbindelsen vil normalt være basert på en teknisk løsning med sammenkobling av to AS-er og en kommersiell avtale mellom partene. Rutingfunksjonen mellom AS-er bygger dessuten på en rutingpolicy.

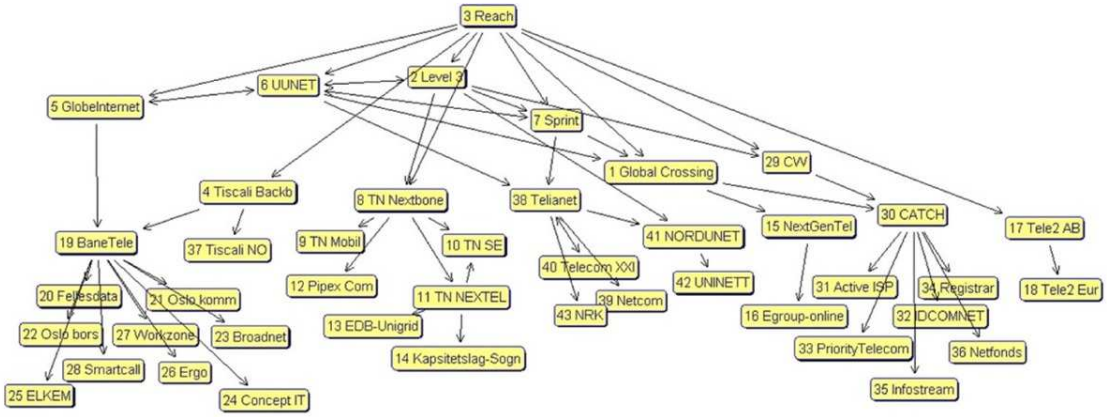
De fleste land har ett eller flere offentlige samtrafikkpunkt. I Norge er de to mest kjente punktene NIX1 og NIX2[57] plassert i Oslo, som driftes av Universitetet i Oslo (USIT). Per i dag er ca 60 virksomheters AS-er tilknyttet NIX1 og i underkant av 20 av disse har også tilknytning til NIX2. Mange av disse samtrafikkpartnerne er tradisjonelle ISP-er, men en finner også rene innholdsleverandører så vel som sluttbrukere blant disse. Som det går frem av brukerantallet er NIX1 det største av disse to samtrafikkpunktene. NIX2 er etablert som et selvstendig samtrafikkpunkt frikoblet fra NIX1, og betyr dermed økt redundans for de som bruker begge. Om NIX2 benyttes for lastdeling eller kun som standby redundans er det opp til peeringpartnerne å avgjøre innbyrdes.

Direkte forbindelser (peer) mellom aktører er det andre alternativet for samtrafikk. Disse etableres ut fra kommersielle behov. Det antas at de fleste av de store kommersielle ISP-ene i Norge har slike forbindelser seg i mellom. I tillegg vil de største aktørene også ha slike forbindelser mot større internasjonale ISP-er. I figur 9.1 på neste side er det vist et eksempel på relasjoner mellom en del nasjonale AS-er, på et gitt tidspunkt i 2005 sett fra Reach[58]. Oversikten er fremskaffet ved gjennomgang av offentlig tilgjengelige BGP-tabeller. Denne viser ikke horisontale forbindelser (peering).

Avhengig av overføringsbehovet vil det i en rekke tilfeller også være nødvendig å formidle transitttrafikk gjennom AS-er. Slik trafikk vil være tilfelle når to AS-er med et kommunikasjonsbehov ikke har mulighet for innbyrdes sammenknytning gjennom private peeringforbindelser eller offentlige samtrafikkpunkter.

[57] `www.nix.no`.

[58] Reach er en stor ISP med base i Hong Kong.



Figur 9.1: Eksempel på relasjoner mellom AS-er på ett tidspunkt i 2005 sett fra Reach, fremskaffet ved gjennomgang av offentlig tilgjengelige BGP-tabeller. Reflekterer ikke NIX-tilknytninger eller private forbindelser.

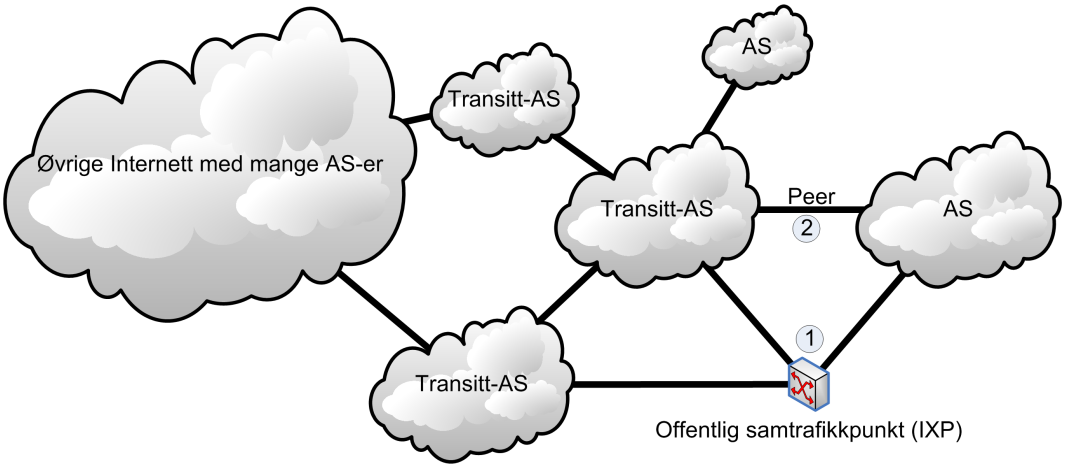
I figur 9.2 på neste side er det vist et eksempel på fem AS-ers sammenkobling med hverandre og resten av Internett. Tre AS-er er direkte knyttet til et offentlig samtrafikkpunkt (1), og disse har også flere private peeringavtaler seg imellom (2). Dette er ofte nødvendig da offentlige samtrafikkpunkt normalt vil stille krav om at tilkoblede AS-er skal ha en alternativ vei til Internett. Flere av AS-ene fungerer også som transitt-AS-er som videreformidler trafikk for andre AS-er.

Historisk sett har det vært mange fortellinger om trafikk som går lange avstander gjennom mange nett i mange land før den kommer tilbake til for eksempel samme by. Det har også versert historier om offentlige samtrafikkpunkts store betydning, supplert med historier om hvor dårlig disse har vært sikret fysisk og i forhold til nødstrøm og så videre.

I samtale med flere operatører har vi imidlertid dannet oss en oppfatning av at mye av den tunge trafikken i Internett i dag går gjennom samtrafikk over private forbindelser. De ulike mulighetene for samtrafikktrafikk som foreligger må uansett anses å innebære en styrking av robustheten i Internett. En utfordring i den sammenhengen er imidlertid at inter-AS-ruting i Internett er en svært kompetansekrevende disiplin, som setter store krav til kompetanse hos hver aktør for å oppnå robust informasjonsflyt i Internett. Kommersielle grunner tilsier at i hvert fall de store aktørene vil måtte ha slik kompetanse. IP-protokollen og inter-AS-ruting er for øvrig nærmere beskrevet i påfølgende delkapitler.

9.1 Internettprotokoller

I forhold til overføringslaget er Internett et nett for å rute datapakker/datagrammer tilhørende IP-protokollen. Kahn og Cerf utviklet IP-protokollen på slutten av 1970-tallet, og den er utvilsomt den



Figur 9.2: Et lite sett med AS-er koblet sammen ved private peeringavtaler og gjennom et offentlig samtrafikkpunkt.

mest brukte nettverksprotokollen i dagens nettverk. Forenklet tilbyr IP-protokollen et adresseringssystem for å identifisere og nå alle maskiner i nettet, samt en forbindelsesløs "best effort" levering av datapakker. Enhver datapakke er utstyrt med en destinasjons- og avsenderadresse, og datapakker tilhørende samme dataoverføring kan gå flere forskjellige veier for å nå destinasjonen. IP-protokollen gir ingen garantier for at IP-pakkene når destinasjonen, derav "best effort".

IP frakter stort sett protokollene User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), Transmission Control Protocol (TCP) eller IP Security (IPSec), som igjen frakter applikasjonsprotokoller. UDP er en forbindelsesløs protokoll som tilbyr sjekksum av data og multipleksing til riktig applikasjon. UDP gir ingen garanti for at UDP-pakkene når mottakende applikasjon, og det er relativt enkelt å opprette falske UDP-pakker som mottaker godtar ved blant annet å forfalske IP-avsenderadresser. TCP er en forbindelsesorientert protokoll som tilbyr sjekksum og multipleksing til riktig applikasjon, som garantert sender alle data i riktig rekkefølge til applikasjonen. Ved bruk av TCP er det betraktelig vanskeligere å opprette falske TCP-pakker med blant annet forfalsket IP-avsenderadresse, da blant annet TCP-sekvensnummerne må være riktige. På en annen side kan en angriper terminere TCP-forbindelser, hvis han har nok kjennskap om kommunikasjonsegenskapene til endepunktene (TCP-RST)[59]. Legg merke til at TCP er vesentlig mer kompleks og ressurskrevende enn UDP. Derfor er det bedre å benytte UDP i blant annet multimediaapplikasjoner med strenge krav til sanntid. ICMP er en kontrollprotokoll for IP, og benyttes blant annet til signalisering av tilgjengelighet og til feilsøking. IPSec er i stor grad teknologien som benyttes for å realisere kryptografisk beskyttede virtuelle private nettverk (VPN) over Internett.

IP-protokollen tillater at avsenderadressen settes til hva som helst av den som sender IP-pakken, noe som gjerne gjøres i forbindelse med tilgjengelighetsangrep. Mottakeren av en slik pakke vil

[59] Ved å sende mange TCP-RST (reset) meldinger, vil man hvis sekvensnummeret er riktig kunne ta ned TCP-sesjonen. Sannsynligheten for å gjette riktig sekvensummer er avhengig av båndbredden og TCP-vindusstørrelsen til målet.

ikke vite hvem avsenderen er og vil heller ikke være i stand til å filtrere bort trafikken på en effektiv og sikker måte, da avsenderen bare kan velge en ny avsenderadresse i neste omgang. Denne type forfalskning refereres ofte til som spoofing, og er noe som i flere tilfeller kan filtreres vekk i ruterne på veien mellom avsender og mottaker. RFC 2827 beskriver en beste-praksis for slik filtrering, og RFC 3704 gir en oppdatering, spesielt for nettverk tilknyttet flere nettverksleverandører.

I et forsøk på å avdekke i hvilken grad spoofing er mulig, utviklet ANA Spoofer Project[60] ved MIT programvare for å kartlegge mulighetene for spoofing. I skrivende stund pågår prosjektet fortsatt, og baserer seg på at personer over hele verden laster ned og kjører programvaren fra egen maskin. Programvaren forsøker å spoofe med utvalgte IP-adresser mot prosjektets maskin, og over tusen personer har bidratt i prosjektet. Per januar 2007 kan man forvente at det fra en tilfeldig IP-adresse er mulig å spoofe omtrent 20% av IP-adressene på Internett. Dette indikerer en forholdsvis utstrakt bruk av filtrering på IP-avsenderadresser.

Svakheter og sårbarheter i protokollene UDP, TCP og ICMP, er i hovedsak følger fra svakheter i IP-protokollen. Det er ikke kjent noen egne svakheter som medfører at UDP, TCP og ICMP bør behandles separat i forhold til sårbarheter på overføringslaget til Internett. Det fokuseres derfor kun på rutingen av IP-pakker i dette kapittelet.

9.2 Ruting av trafikk mellom internettilbydere

Ruting av trafikk mellom AS-er realiseres i dag av protokollen Border Gateway Protocol (BGP) [64]. Hver aktive BGP-ruter på Internett inneholder ”veiruter” til et sett av IP-adresser/nett, hvor en rute er definert som et sett av AS-er. I 2002 inneholdt hver BGP-ruter i overkant av 70.000 ruter [9]. I skrivende inneholder de i underkant av 200.000 ruter [65].

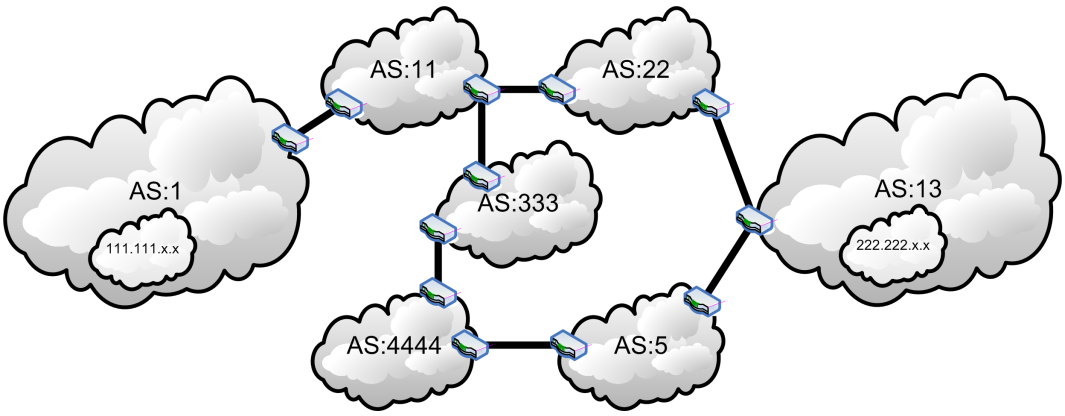
Hver aktive BGP-ruter er satt opp med BGP-sesjoner til andre BGP-rutere i eget og/eller andre AS-er. En BGP-sesjon er realisert over en TCP-forbindelse. Når BGP-ruterne tilhørende samme AS kommuniserer kalles det intern-BGP, og når BGP-rutere tilhørende forskjellige AS-er kommuniserer kalles det ekstern-BGP. Naboer i BGP er definert som alle eksterne BGP-rutere en gitt BGP-ruter har/skal ha BGP-sesjon med. Denne sesjonen kalles ofte for peering.

For at maskiner i IP-nettet 111.111.x.x. i AS:1 i figur 9.3 på neste side skal kunne kommunisere med maskiner i nettet 222.222.x.x i AS:13, kan pakkene sendes gjennom rutene/AS-ene (11, 22, 13) eller (11, 333, 4444, 5,13). Det eksisterer altså to forskjellige ruter mellom IP-nettene. Valg av rute er avhengig av AS-ene sine policyer og hvilken rute som antas som ”raskest”.

9.2.1 Policy for ruting

BGP handler mye om policy for ruting mellom AS-er, og policy er for det meste motivert av politikk, sikkerhet og økonomi.

[60] `http://spoofer.csail.mit.edu`



Figur 9.3: Eksempel på BGP-arkitektur.

Policyer er økonomisk motivert i form av samtrafikkavtaler mellom AS-er. Dette kalles Service Level Agreements (SLA-er), hvor nivået/kvaliteten på tjenesten konkretiseres. Et gitt AS tar seg gjerne betalt for at andre AS-er skal få lov til å sende trafikk gjennom det. Dette må settes som policy i AS-et sine BGP-rutere, og blir med andre ord en realisering av et kundeforhold mellom to AS-er.

BGP gir også mulighet for å forkaste/filtrere ut alle ruter som starter med eller inneholder visse AS-er, samt filtrere ut ruter basert på destinasjon. Denne filtreringen vil typisk være motivert av politikk og sikkerhet. For eksempel kan det velges ikke å formidle at en gitt BGP-ruter har en rute til et gitt IP-nett, eller det velges ikke å rute trafikk til en gitt organisasjon/land gjennom dette AS-et. Et AS kan også velge for eksempel ikke å rute pakker mellom to utenlandske AS-er, selv om den korteste ruten er via dette AS-et.

9.2.2 Valg av rute

Som vist i figur 9.3 kan det eksistere flere mulige ruter mellom to IP-nett, og ved siden av interne rutingstrategier i AS-ene, må hver BGP-ruter velge hvilken rute den vil benytte. Som hjelpemiddel har BGP-rutere mulighet for å vekte forskjellige ruter. Ved siden av vektingen kan det angis hvilken BGP-ruter man vil andre AS-er skal nå ditt AS gjennom, samt settes opp regler om antall AS-er i hver rute[61].

Resultatet av policy, vektingen og andre regler, gir hvilken rute som blir plassert i rutetabellen til den gitte BGP-ruteren. Når BGP-ruteren mottar en IP-pakke med en gitt IP-destinasjonsadresse, slår den opp i sin egen rutetabell og videresender datapakken til neste AS i ruten.

Legg merke til at ruteinformasjon i BGP også må formidles inn til ruterne internt i et AS. Dette diskuteres ikke videre i denne rapporten.

[61] Typisk en regel om at jo færre AS-er, jo bedre.

9.2.3 Formidling av ruter

Forenklet inneholder BGP-rutere tre forskjellige tabeller kalt Inn, Policy og Ut. Inn-tabellen inneholder all ruteinformasjon den har fått inn fra sine naboer og Ut-tabellen inneholder all ruteinformasjon den har formidlet til sine naboer. Policy-tabellen inneholder et sett av regler for realisering av AS-et sin policy.

Når et AS ønsker å annonsere/formidle at man kan nå et IP-nett via dette AS-et, distribueres denne informasjonen til alle BGP-naboer, som igjen kan formidle informasjonen videre. Denne formidlingen av informasjon til alle BGP-naboer kalles ”flooding”, og hvordan denne formidlingen håndteres videre er avhengig av policyen i hver enkelt BGP-ruter denne ruten formidles videre til.

Tilsvarende som det formidles hvilke ruter som er nye, vil det også formidles tilbakekalling av ruter. En rute kan tilbakekalles på grunn av for eksempel feil i et nettverkskort på en intern ruter.

9.3 Sårbarheter i rutingen mellom internettilbydere

I den nasjonale strategien for å sikre Internett, fra Department for Homeland Security i USA, pekes IP, DNS og BGP ut som protokollene det bør fokuseres på for å få et mer robust Internett [19]. Hovedbekymringen er godt organiserte angrep fra aktører med høy kapasitet. BGP blir her vurdert som den største sårbarheten i tilfelle storskala angrep mot Internett. Internetts videre funksjonalitet og sikkerhet er i følge den amerikanske nasjonale strategien helt avhengig av en mer robust versjon av BGP.

I denne seksjonen vurderes fysiske, logiske og sosiale sårbarheter og avhengigheter i forbindelse med rutingen mellom AS-er. Som en konsekvens av sårbarhetene i BGP, krever siste versjon av BGP-spesifikasjonen at alle BGP-implementasjoner skal ha støtte for autentiseringsmekanismene spesifisert i TCPMD5 [35] [55]. TCPMD5 baserer seg på at to BPG-naboer deler en felles hemmelig nøkkel, og at alle TCP-pakker som utveksles mellom dem er signert basert på innhold og nøkkelen. Dette fungerer som en integritetssikring av kommunikasjonen mellom to BGP-naboer, men garanterer på ingen måte at innholdet i BPG-meldingen er korrekt. I hvor stor grad TCPMD5 benyttes, vites ikke.

9.3.1 Fysiske sårbarheter

Fysiske angrep mot offentlige samtrafikkpunkter, som NIX1 og NIX2 har lenge vært sett på som svært kritisk for Internett i Norge. Etter samtaler med internettilbydere og studier av deres internettarkitektur, kan det virke som om offentlige samtrafikkpunkter er av mindre betydning for robustheten til Internett i Norge. Det ser ut som om de fleste nasjonale seriøse internettilbydere har etablert samtrafikkavtaler med flere forskjellige AS-er, både nasjonalt og internasjonalt. Dette er både transittavtaler med store AS-er som AT&T, Level 3 og Global Crossing, og peeringavtaler med de internettilbyderne som har mye trafikk mellom seg. Fysiske angrep mot samtrafikkspunktene vil dermed

kunne spolere mye av den potensielt rimeligere peeringtrafikken mellom norske internettilbydere, men trafikken vil nok raskt rutes om til de potensielt dyrere transittrutene og på denne måten allikevel nå mottakerne.

Selv om man på overføringslaget har mye redundans, vil det fortsatt kunne være mye av trafikken som går over de samme fysiske kablene. For Norge og særlig utenfor østlandsområdet, er det ofte få leverandører av transportnett. Det begrenser seg ofte til Telenor, BaneTele og lokale aktører som kraftlag. En togavsporing vil i så fall kunne føre til at både den billige peeringtrafikken og den dyre transittrafikken blir stoppet på grunn av kabelbruddet.

9.3.2 Logiske sårbarheter

BGP er en distribuert protokoll som kjøres på over 100.000 rutere på Internett [11]. Det er derfor mange rutere å velge mellom for et angrep mot BGP og Internett. Siden ethvert AS er indirekte knyttet til alle andre AS-er, vil angrep mot BGP et sted på Internett også kunne få store konsekvenser helt andre steder på Internett. I følge Murphy sin sårbarhetsanalyse av BGP, har protokollen noen fundamentale sårbarheter [55]. Disse inkluderer:

1. BGP beskytter ikke mot eventuelle endringer av ruteformidlinger (integritet)
2. BGP sjekker ikke at ruteformidlingen faktisk er en ny formidling, og ikke en gammel som blir avspilt i nettverket på nytt
3. BGP benytter ikke autentisering ved ruteformidling
4. BGP verifiserer ikke om det gitte AS-et får lov til å formidle disse IP-adressene
5. BGP verifiserer ikke ektheten til AS-ene i en rute

Sårbarhet nummer 1 går på at ruteformidlinger kan endres uautorisert underveis av en BGP-ruter. Sårbarhet nummer 2 går på at gamle ruteformidlinger kan lagres og sendes senere, dette kalles ofte repetisjonsangrep (replayangrep). Sårbarhet nummer 3 går på at det påståtte opphavet til en formidling kan være falskt. Sårbarhet nummer 4 går på at hvem som helst kan formidle at de har en vei til hvilke som helst IP-adresse. Sårbarhet nummer 5 går på at det ikke er noen sjekk for å verifisere at AS-ene i en rute er ekte.

Det eksisterer flere eksempler på sårbarhet nummer 4, hvor AS-er har formidlet at de har rute til angitte deler av Internett, selv om de ikke har det. Dette refereres ofte til som å skape svarte hull på Internett, i og med at store mengder trafikk rutes feil. I april 1997 formidlet en feilkonfigurert ruter tilhørende et lite AS i Virgina i USA at den hadde en optimal rute til hele resten av Internett [11]. Konsekvensen av dette var at mye av internettrafikken ble rutet mot AS-et, og store deler Internett var ”nede” i to timer. Svarte hull kan være meget vanskelige for offer-AS-ene å diagnostisere og rette opp [11]. Dette handler om et AS som har formidlet en potensiell kortere vei til offer-AS-et til resten av Internett. Offer-AS-et må dermed sørge for at denne feilinformasjonen blir fjernet fra

alle andre AS-er som velger den falske ruten. I tillegg vil den ”kaprede trafikken” kunne overbelaste ruterne den nå feilaktig er satt opp til å traversere. Disse ruterne kan så stoppe opp, og man får skapt kaskader av feil over potensielt store deler av Internett.

Feil har også ført til at trafikk mellom to destinasjoner unødvendig rutes via tredjepart. I følge Butler et.al har det vært rapportert om at trafikk mellom USA og London unødvendig har gått via Israel [11]. Et AS kan blant annet få til unødvendig ruting, hvis AS-et modifiserer ruteformidlingene fra andre AS-er før de videreformidles (sårbarhet nummer 1).

9.3.3 Sosiale sårbarheter

En av de kanskje mest alvorlige sårbarheter for Internett er uenigheter mellom sentrale AS-er. Hvis for eksempel to store AS-er velger å avslutte ethvert samarbeid, vil dette kunne få store konsekvenser for Internett. Nettopp dette skjedde i oktober 2005, da AS-et Level 3 ikke lenger ville ha samtrafikk med AS-et Cogent Communications. Dette førte til at kunder hos Cogent ikke kunne nå kunder hos Level 3, og omvendt. Dette varte i nesten en måned, før Level 3 og Cogent ble enige om vilkårene for samtrafikk mellom hverandre.

I en studie om feilkonfigurasjoner av BGP-rutere, viser det seg at mellom 0,2-1,0% av de daglige annonserte endringene i BPG-rutingtabellen skyldes feilkonfigurasjon [45]. Studien viser også at nesten 3 av 4 annonserte nye IP-prefikser skyldes feilkonfigurasjon. Allikevel viser studien at endringene i liten grad fører til tap av konnektivitet for sluttbrukerne. Feilkonfigurasjonene skyldes i stor grad menneskelig feil, og studien etterlyser bedre verktøy for konfigurasjon av BGP.

Dette viser at feilinformasjon til stadighet introduseres i BGP, men at dette sjelden får store konsekvenser. Merk at dette ikke nødvendigvis betyr at rettede angrep ikke får store konsekvenser for deler av Internett. Historien har vist at noen feilkonfigurasjoner har fått store konsekvenser.

Litteraturen på området og samtaler med internettilbydere har gitt et inntrykk av at de aller fleste seriøse aktører kjører BGP-sesjoner med sine samtrafikkpartnere over egne linjer, som for eksempel leide forbindelser. På denne måten skilles data- og kontrolltrafikk. Dette gir en lav sannsynlighet for å kunne kompromittere eller avlytte selve BGP-sesjonen direkte, men BGP-ruterne kan ha andre tjenester åpne mot Internett, slik som for eksempel SSH og Telnet eller HTTP og SNMP. En sårbarhet i disse tjenestene vil i så fall kunne gi en angriper muligheten til å overta BGP-ruteren, og på den måten sende ut falsk rutinginformasjon fra den overtatte ruteren.

I et forsøk på å kartlegge BGP-rutere på Internett i 2003, portskannet Convery og Franz fra Cisco i overkant av 115.000 mulige BGP-rutere over Internett [17]. Etter skannet forsøkte de å sette opp en forbindelse med tjenestene BGP, HTTP, Telnet og SSH på BGP-ruterne. Omtrent 4% av ruterne tillot å sette opp en TCP-forbindelse til BGP. Dette betyr ikke at 4% av ruterne tillater hvem som helst å kommunisere BGP med ruteren, men det viser at BGP-ruteren ikke er satt opp med filtrering på IP-adresser. Verre var kanskje resultatet om at omtrent 14% av ruterne tillot å sette opp en forbindelse til en av tjenestene Telnet, HTTP eller SSH. En angriper vil kunne utføre mye skade ved å overta en

BGP-ruter via disse tjenestene og formidle falsk ruteinformasjon. Det er derfor like viktig å sikre Telnet, SSH, SNMP og HTTP, som BGP. Undersøkelsen viser også kraftige variasjoner fra land til land når det gjelder hvor godt BGP-ruterne er sikret i forhold til å sette opp TCP-forbindelser mot de angitte tjenestene. For eksempel tillot 73% av BGP-ruterne på Bahamas en eller flere TCP-forbindelser til tjenestene, mens bare 5% av Spania sine BGP-rutere tillot det samme.

9.3.4 Avhengigheter

BGP-sesjonen mellom to BGP-rutere sender periodisk keep-alive meldinger til hverandre, slik at den underliggende TCP-forbindelsen ikke kobles ned. Samtidig vil keep-alive meldingene kunne detektere om BGP-naboen går ned. Hvis BGP-sesjonen termineres vil den settes opp igjen, og de to involverte BGP-ruterne må utveksle all ruteinformasjon på nytt [64]. BGP-rutingtabellen tilhørende AS-et REACH var per 1. oktober 2006 på omtrent 16Mbyte[62], og et angrep som stadig terminerer BGP-sesjoner vil skape mye trafikk på linken mellom ruterne. Dette vil kunne føre til en tregere ruting av pakker eller i verste fall et tilgjenglighetsangrep.

Når en BGP-sesjon termineres, vil alle ruter annonsert gjennom sesjonen måtte tilbaketrekkes. Dette betyr at andre BGP-rutere på Internett må sette opp/regne ut nye ruter [85]. Når så BGP-sesjonen settes opp igjen, blir alle rutene annonsert på nytt. Dette fører igjen til mye utregning på andre BGP-rutere. Hyppige tilbaketrekkinger og reformidlinger av de samme rutene kalles ofte “flaps”. De aller fleste BGP-rutere er satt opp med en mekanisme for å holde tilbake formidlinger og tilbaketrekkinger av ruter, inntil ruteren har nådd et visst nivå av stabilitet. Mekanismen kalles “route flap damping” [83].

Flere AS-er legger ut sine dynamiske BGP-tabeller på Internett, slik at hvem som helst kan søke i dem og få ut informasjon om hvordan Internett ser ut sett i fra det gitte AS-et. Reach Network (AS4637) legger daglig ut sin BGP-tabell [65]. Ved å søke på denne siden vil man kunne bygge opp arkitekturen for Internett, sett fra Reach. Tidlig i 2005 så deler av den norske internettarkitekturen ut som vist i figur 9.1. Figuren viser hvilke AS-er som var koblet sammen på dette tidspunktet, sett fra Reach. Oslo Børs vises koblet til BaneTele, som igjen er koblet til Globeinternett og Tiscali. BGP-rutetabeller avdekker med andre ord hvem som har samtrafikkavtaler med hvem, men den gir ikke hele sannheten. Den viser ikke lokale samtrafikkavtaler som omfatter trafikk internt mellom AS-ene, og som da naturlig ikke annonseres ut på Internett.

9.3.5 Oppsummering

Per 2007 eksisterte det over 20.000 AS-er [65] og alle disse kan være kilde til feilene/angrepene beskrevet i dette kapittelet. Allikevel har det i følge Murphy og Montgomery til dags dato ikke vært vellykkede alvorlige rettede angrep mot rutingen på Internett [54].

[62] `http://bgp.potaroo.net/as4637/bgptable.txt`

Hvor sårbart Internett er ovenfor angrep mot BGP, avhenger av AS-er sine policyer og filtreringsmekanismer. Basert på Murphy sine skisserte svakheter i BGP, antas det at et ”ondt” AS kan få til angrep med alvorlige konsekvenser for deler av Internett, selv om BPG-naboer benytter TCPMD5 [35]. Butler et al. støtter denne teorien, ved å vise til flere alvorlige hendelser grunnet menneskelige feil gjort av administratorer i forskjellige AS-er gjennom tidene.

Angrepene og feilene antas allikevel i stor grad å kunne bli rettet innen rimelig tid av kompetente operatører. Godt planlagte og rettede angrep mot BGP kan med andre ord få dramatiske konsekvenser for deler av Internett, men trolig bare for en begrenset tidsperiode.

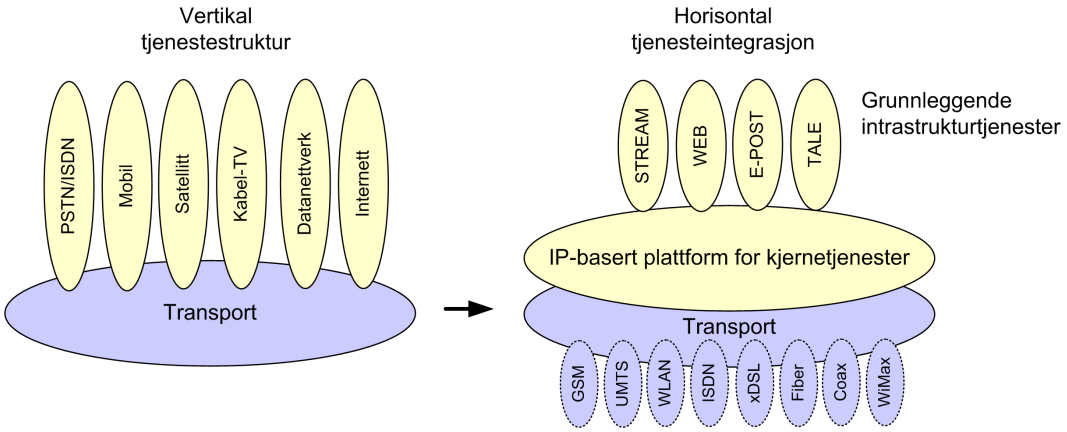
På samme måte vil angrep mot ett eller flere viktige punkt i Internetts fysiske infrastruktur antas å kunne få effekt. Hvor stor effekt vil imidlertid være avhengig av om man har angrepet det ”rette” punktet. Det anses ikke uten videre som trivielt for en utenforstående å finne slike punkt.

10 Nettverksarkitektur for internettilbydere

Kommunikasjonsinfrastrukturen som danner basis for et AS er designet med en nettverksstruktur som gjør det egnet til å overføre IP-pakker med gitt kvalitet mest mulig kosteffektivt. Viktige egenskaper i så måte er driftbarhet, fleksibilitet, skalerbarhet, kvalitet og robusthet. Størrelsen på denne nettstrukturen vil variere med størrelsen på operatør (ISP), som igjen er en funksjon av geografisk interesseområde og kundegrunnlag (trafikkvolum). I denne rapporten er oppbygging av nettstruktur ikke et sentralt tema. For å få en basal oppfatning av hvilken relasjon det er mellom slik nettstruktur og robusthet, er det likevel naturlig med en relativt overflatisk beskrivelse av hvordan denne er bygget opp.

Man kan hevde at slike nett i større eller mindre grad har vært bygget opp ut fra en bottom-up strategi. Ruteren, som hovedkomponent i overføringsnettet, har blitt fysisk utplassert der det har vært funksjonelt og markedsmessig grunnlag og tilknyttet andre rutere i nettverket ut fra løpende behov. Dette nettet har dermed vært bygget ut med rutere og forbindelser med basis i et økende behov. Behov for tjenestefunksjonalitet har også blitt bygget ut parallelt. Hensyn til robusthet i fysisk struktur i Internett har neppe vært det mest fremtredende designkriterium tidlig i denne utviklingen.

I løpet av de siste årene har det imidlertid inntruffet to viktige endringer som påvirker den fysiske nettinfrastrukturen i Internett. Den første er at tjenester fra internettbaserte infrastrukturer har fått en mye større betydning for mange brukere. E-handel er et eksempel på en av anvendelsene som påvirker dette. Tilgjengelighet til internettbaserte tjenester har blitt kritisk for mange brukere. Behovene for robusthet og kvalitet i tjenesteproduksjon blir dermed stadig viktigere.



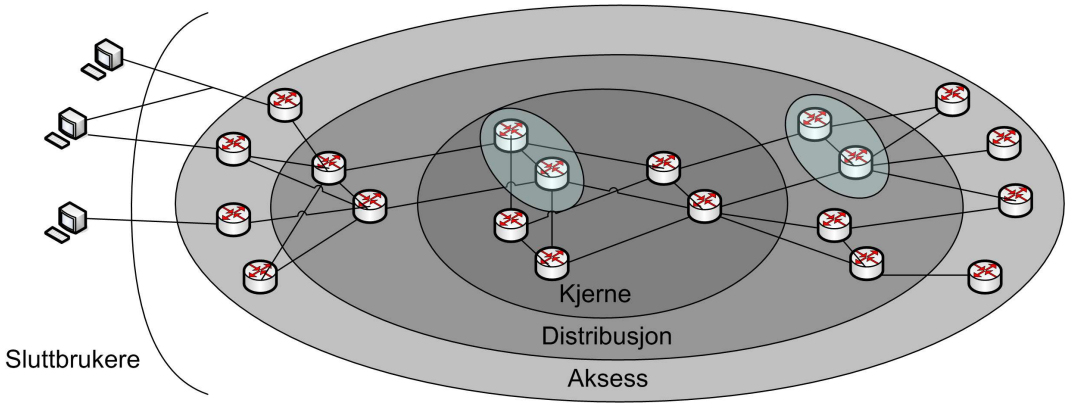
Figur 10.1: Migrering til felles IP-plattform. Basert på Bjørn Netland, "Telenors nye IP-nett"[57].

Den andre endringen går på utviklingen innen tradisjonell telekommunikasjon. Denne går mot å migrere tidligere separate tjenestespesifikke nett og plattformer til ett tjenesteintegrert nettverk med IP som teknologiplattform, som vist i figur 10.1. IP-teknologi vil med dette utgjøre en felles plattform på overføringslaget for alle elektroniske kommunikasjonstjenester som produseres, inklu-

dert operatørens del av Internett. Basis tjenesteplattform i et slikt integrert nett vil tilby fire fundamentale tjenestetyper med ulike egenskaper og krav til tjenestekvalitet: Web (browsing), tale, "mail" og "stream". Denne integrerte tjenesteplattformen får direkte innflytelse på nettstrukturens egenskaper og den robusthet denne innehar. Selskaper som British Telecom[63], Telenor og andre EKOM-operatører er i full gang med å overføre sin tjenesteplattform til dette konseptet. Det ligger også i konseptet at kunder tilbys ulike tjenesteegenskaper og ulik kvalitet ut fra behov og betalingsvilje.

10.1 Nettverksstruktur for integrert tjenesteplattform

Som basis for denne integrerte tjenesteplattformen realiseres ofte hver ISPs nettstruktur som en trelagsmodell: Kjernelag, distribusjonslag og aksesslag. Disse tre lagene har grunnleggende forskjellige roller i formidling av de fire hovedtypene trafikk nevnt ovenfor. Se figur 10.2.



Figur 10.2: Arktitekturmodell for en ISP.

Aksesslaget knytter opp brukerne til det øvrige nettverket. Aksesslagets viktigste funksjon er å samle og aggregere informasjonen fra mange brukerforbindelser. Aksesslaget er dermed ikke synonymt med aksessnettet. Aksessnettet kan sees på som underliggende infrastruktur for (deler av) aksesslaget. Distribusjonslaget står for formidling av trafikk mellom ulike noder i aksesslaget. Dette skiller også mellom lokal trafikk og trafikk videre inn i nettverket. Tjenesteplattformer og sikkerhetsfunksjoner vil logisk knyttes opp mot aksess- og distribusjonslaget. Distribusjonslaget vil typisk være avhengig av forbindelser i transportnettet.

Mens aksesslaget og distribusjonslaget står for aggregering av trafikk og all tjenestehåndtering, er kjernelagets eneste rolle å formidle store mengder IP-trafikk effektivt. Typisk for designet av kjernelaget er enkelthet. Kjernelaget er avhengig av høyhastighetsforbindelser i transportnettet.

Karakteristisk for realiseringen av denne trelagsmodellen er at denne tar utgangspunkt i en helhetlig arkitekturtilnærming med integrert tjenesteleveranse i fokus. I dette realiseres krav om mest mulig

[63] `http://www.btplc.com/21CN/`

enkelhet i nettets oppbygging. Også mest mulig standardisering på få teknologier ligger på sett og vis implisitt i dette. Som eksempel søker man raskest mulig å fase ut teknologier som ATM og SDH, til fordel for IP og WDM. En målsetting for utviklingen av ett slikt tjenesteintegrert nett kan typisk være: *"Gradvis overgang til en felles IP-basert plattform for alle anvendelser og aksessformer som gir forenklet operasjon og drift. Eksisterende nett og løsninger vil bli faset ut.*" [57].

Mens man i tidligere nett hadde større strukturer i kjernen av nettet, ofte med mange noder spredt geografisk, går man nå mot ett rendyrket enkelt kjernenett som kun har funksjonalitet fra kjernelaget i modellen. Antall noder i et moderne kjernelag er få. I et "lite land"-kontekst vil typisk tre til seks POP-er være typisk.

Siden kjernelaget, som termen også indikerer, utgjør den delen av nettet som alle er "mest" avhengig av, har denne ofte en mer robust struktur enn den øvrige nettstrukturen, med redundans både i noder (rutere) og i forbindelser. Man vil unngå såkalte Single Point of Failure (SPOF-er), og man er generelt opptatt av at redundans i forbindelsesveiene mellom POP-er i størst mulig grad er fysisk og ikke bare logisk separert. Så langt det er mulig vil de største operatørene også søke å oppnå fysiske maskestrukturer i kjernelaget, men begrenset tilgang til transportnettjenester mange steder vil begrense denne muligheten. Det kan antas at de minste aktørene har en mer sentralisert struktur.

Samlet sett vil et slikt integrert tjenestedesign være med på å styrke internettype EKOM-tjenester. Disse får plass på samme plattform som alle andre typer EKOM-tjenester på en helhetlig og robust måte. På en nettverksplattform oppbygget etter en helhetlig arkitektur er det mulig å integrere sikkerhetsfunksjoner som styrker nettets robusthet.

10.2 Sårbarheter i nettverksstrukturen

Det vil føre for langt å gå inn i en full analyse av sårbarhet i den fysiske strukturen i kommunikasjonsinfrastrukturen for ISP-er. Til dette har vi heller ikke tilstrekkelig datagrunnlag. Dette begrenses derfor til kun å være en vurdering ut fra det begrensede bildet vi har bygget opp gjennom innhenting av skriftlig dokumentasjon og samtaler med aktører. Dette materialet er i betydelig grad innhentet som bedriftskonfidensiell informasjon. Denne vurderingen bygger også på tidligere sårbarhetsanalyse av nasjonale offentlige telenett i BAS2 [59].

Beskrivelsen gjøres ut fra logikken om at svikt i enkeltpunkter eller forbindelser i infrastrukturen vil kunne medføre svikt i tjenesteplattform, og ende opp i at en eller flere tjenester faller fra. Det legges dermed hovedvekt på tilgjengelighetsaspektet.

10.2.1 Fysiske sårbarheter

Det enkleste vil trolig være å sette en eller flere noder ut av spill ved å ødelegge kommunikasjonsnoden selv eller de forbindelsesveiene som knytter noden til resten av nettet og andre nettjenester. Dette kan skje gjennom fysisk ødeleggelse av bygningsmasse eller utstyr. Også elektroniske angrep

i form av High Power Microwave (HPM) eller Electro Magnetic Pulse (EMP) kan nyttes for å skade eller funksjonsforstyrre elektronisk utstyr. Dette sistnevnte har lenge vært grunnlag for bekymring i enkelte fagmiljøer.

De mest sentrale komponentene i kommunikasjonsinfrastrukturen i de største aktørenes nettdomener antas å være relativt godt fysisk beskyttet i bygninger eller fjellanlegg. I moderne nettstrukturer som beskrevet ovenfor ligger det også relativt mye innebygget redundans. Skade på en vilkårlig installasjon i et nett vil derfor i utgangspunktet normalt kunne antas å ha liten innvirkning på tjenesteproduksjon. Spørsmålet er imidlertid svært sammensatt og er blant annet avhengig av faktorer som:

- Hvilken geografisk struktur med rutere (POP-er) og forbindelser den enkelte operatør faktisk har i sitt nettdomene. Dette vil blant annet være avhengig av hvor mange kunder en operatør har og hvilken geografisk fordeling disse strekker seg ut over.
- Hvilke typer brukere en operatør har rettet virksomheten inn mot, i hovedsak bedrift- eller privatmarkedet. Dette vurderes normalt å si noe om hvilken styrke man bygger inn i nettets struktur ut fra risikotilnærming i forhold til kundeprofil.
- Hvilken fysisk og logisk samtrafikkløsning som er valgt for tilknytning til resten av Internett. Dette har betydning for anvendelser der trafikk går på tvers av flere aktørers AS-er.

Det er i tillegg viktig å understreke at sårbarhet i slike flerlags nettstrukturer er svært dynamisk. I tillegg til at strukturene i seg selv er komplekse er de også ofte dynamisk i forhold til sin oppbygging. En liten endring i struktur på ett tidspunkt kan ha stor betydning for de konsekvenser som oppstår ved en eller flere tilstander av svikt i nettverket. Med hensyn til sårbarhet utgjør dette både en styrke og en svakhet. Det vurderes å kreve relativt stor innsats for en angriper å finne ut med sikkerhet hvilke konsekvenser ett angrep mot nettet vil føre til i forhold til nettets totale ytelse og tjenesteproduksjon. Et gitt angrep kan forårsake en tilstand som gir alt fra store tjenesteutfall til knapt merkbare effekter. Sett fra systemeiers synsvinkel er slik kompleksitet også en svakhet. Man vet aldri helt sikkert hva mange mulige feiltilstander i nettet kan føre til av konsekvenser for tjenesteproduksjon.

Det må også understrekes at det mange steder er begrensede muligheter for å oppnå fysisk redundans i transportnett og aksessnett. Redundans i aksessnett er i hovedsak et ansvar for brukeren, ikke for tjenesteleverandøren.

10.2.2 Logiske sårbarheter

De fleste komponenter i overføringslaget og underliggende aksess- og transportnett bygger på åpne standarder og kan angripes logisk. På samme måte som gjennom fysiske angrep vil man kunne sette en komponent ut av drift for en periode med konsekvens for nettstrukturen, for eksempel

ved at porter i en ruter deaktiveres. Mer sammensatte angrep mot strukturen, for eksempel mot rutingfunksjonen eller adresseringsfunksjonen, er også mulige (kapittel 9.2).

I tre-lagsmodellen for nettverksarkitektur, som vist i figur 10.2, består nettet egentlig av et privat IP-basert ruternett. Operatørene hevder at det gjennom denne lagdelte arkitekturen vil være enklere enn i tidligere strukturer å beskytte vitale deler av nettstrukturen med teknologier som for eksempel brannmurer. Denne modellen innebærer også en enklere struktur, som igjen fører til forenklet operasjon av nettverket. Nettstrukturen er imidlertid, som andre typer arkitekturer, svært sårbar overfor angrep gjennom tilhørende drifts- og styringssystemer, som diskuteres i kapittel 11. En kombinasjon av fysiske og logiske virkemidler vil kunne være svært virkningsfullt.

10.2.3 Sosiale sårbarheter

Som nevnt ovenfor er det sentraliserte drifts- og styringssystemet pekt på som en kritsik ressurs i et moderne kommunikasjonsnett. På samme måte er personellet som står for operasjonen av systemet svært viktig for dets tjenesteproduksjon. Dette gjelder først og fremst i forhold til personellets kompetanse. Det er imidlertid også nærliggende å tenke seg at ulike typer negativ påvirkning fra utenforstående mot dette driftspersonellet kan utgjøre en betydelig trussel mot systemet.

10.2.4 Avhengigheter

Det fysiske nettet, både på overføringslaget og underliggende lag, er svært avhengig av sikker kraftforsyning. I det tradisjonelle telefoninettet er det bygget inn mye nødstrømskapasitet. I mer moderne nett, som for eksempel mobiltelefoninettene, er det mange steder i nettet lite eller til og med ingen innebygget nødstrømskapasitet. I Norge har det historisk vært svært stabil kraftforsyning. I utviklingen av nye nettstrukturer av store og små aktører vil kraftforsyning være en kritisk faktor.

11 Aktørenes drift og styring av nett og tjenester

Dagens nett og tjenester, tilhørende for eksempel internettilbydere, transportnettilbydere og organisasjoner med kritisk infrastruktur, er typisk satt sammen av mange ulike komponenter fra flere forskjellige leverandører. Komponentene inkluderer blant annet multipleksere, svitsjer, rutere og tjenere, og alle komponentene er underlagt drift og styring. Organisasjonene må med andre ord drive drift og styring av komponenter i transportnettet, av overføringslaget, av fundamentale tjenester og av tjenester på applikasjonslaget.

Vanligvis vil ikke drift og styring av de forskjellige nivåene være integrert i ett system, men snarere vil det eksistere flere adskilte drifts- og styringssystemer for realiseringen av nettene og tjenestene. I tillegg vil det ofte være forskjellige aktører som drifter og styrer de forskjellige nivåene, noe som krever godt samarbeid ved endringer. Grunnen til dette er at endringer på et nivå kan få utilsiktede effekter på andre nivåer. Hvis for eksempel det gjøres endringer i tjenestedistribusjonen, vil dette kunne påvirke valg av ruter i overføringslaget.

Til forskjell fra tradisjonelle telenett hvor signalisering, kontroll og drift er atskilt fra tale- og datatrafikken, skiller ikke IP-nett på data-, signaliserings-, kontroll- og driftstrafikk. Eksempelvis kan datatrafikk være web, e-post eller filoverføring, signaliseringstrafikk kan være oppsett av TCP-forbindeler, kontrolltrafikk vil typisk være ICMP og driftstrafikk kan være SNMP. Sammenblandingen av trafikk fører til at alle i prinsippet har tilgang til å gjøre angrepsforsøk mot kritiske funksjoner.

11.1 Kompleksitet og krav til kompetanse

Det eksisterer standardiserte informasjonsmodeller, kommunikasjonsprotokoller og funksjonalitet som skal dekke drift- og styringsfunksjonen for hele eller deler av nettene og tjenestene. Det internasjonale arbeidet med utvikling og standardisering av arkitekturer for drift og styring av kommunikasjonsnett er svært omfattende.

Dette betyr at ikke bare nettene og tjenestene er teknologisk komplekse, men at drift og styringen av dem også er meget komplekst. Dette setter helt andre krav til operatørene som skal utføre den daglige driften og styringen av nettene og tjenestene, i forhold til den daglige driften og styringen av de gamle telenettene. Dagens internettilbydere må ha meget kompetente personer på vakt 24 timer i døgnet, hele året. For eksempel krever endringer i ekstern ruting med andre internettilbydere god kjennskap til protokollen BGP, som svært få personer har kunnskap til å endre i sanntid. Kravet til endringer kan komme når som helst, for eksempel som en konsekvens av feil hos andre internettilbydere, og kompetansen må derfor være tilgjengelig hele tiden.

Nye tjenester impliserer også at kunder skal kunne håndtere visse parametere for egen trafikk. Dette inkluderer blant annet krav til prioritet, båndbredde, forsinkelse og varians i multimediatrafikk. Denne tendensen vil sannsynligvis forsterkes, noe som fører til at drift- og styringssystemene ikke

bare skal håndtere en teknologisk kompleksitet, men i økende grad også en administrativt og juridisk kompleksitet.

11.2 Migrering mot IP-baserte nett

En trend i dagens nett er at de migreres mot IP, som beskrevet i kapittel 10. Dette betyr at alle tjenester, som for eksempel telefoni, ønskes kjørt over IP. Dette fører til at det gjerne eksisterer flere logisk adskilte IP-nett, som hver for seg frakter forskjellige typer trafikk. Med andre ord ønsker man å kjøre all trafikk over samme IP-nett, men av sikkerhetsmessige årsaker ønsker man fortsatt å skille logisk på forskjellige typer trafikk.

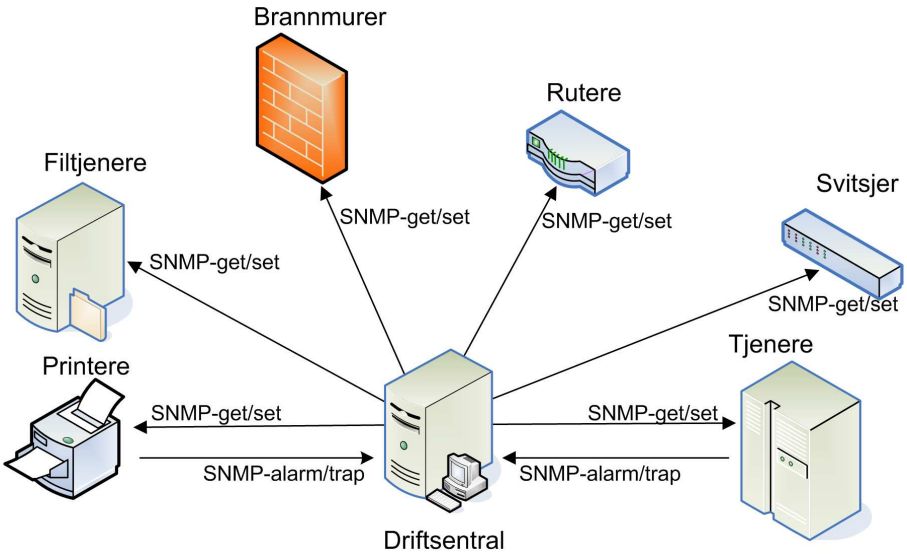
Multiprotocol Label Switching (MPLS) er en mekanisme som benyttes til å sette opp flere logiske eller virtuelle IP-nett over det samme IP-nettet. For eksempel kan det settes opp et virtuelt IP-nett for drift og styring, et for kontroll av kritiske SCADA-systemer, et for administrasjons- og kontorfunksjoner og et for eksterne kunder. I prinsippet vil da alle IP-pakkene gå i det samme IP-nettet, men MPLS merker de forskjellige IP-pakkene etter hvilken type trafikk de tilhører, og pakkene behandles i hver ruter etter det. Som beskrevet i kapittel 12.3 er det også mulig å benytte virtuelle private nettverk (VPN) for å logisk separere nett.

Bruken av flere forskjellige logiske IP-nett vil naturlig føre til et komplekst IP-nett, ikke minst i forbindelse med drift og styring av alle IP-nettene, og koordineringen av dette. Allikevel vil nok muligheten for integrert drift gi en totalt bedre drift i forhold til de tidligere mange separate drifts-systemene.

11.3 Drift og styring av IP-baserte nett

I dagens IP-baserte nettverk er det vanlig å benytte protokollen Simple Network Management Protocol (SNMP), for utveksling av drifts- og styringsinformasjon mellom driftssentraler og nett-verksenheter. Driftssentraler vil periodisk hente ut informasjon og eventuelt konfigurere nettverks-enhetene. Dette gjøres ved at driftssentralen sender en SNMP-forespørsel til nettverksenheten for å få rapportert eller endret en egenskap på nettverksenheten. Nettverksenheten sender deretter svar tilbake til driftssentralen med egenskapen som driftssentralen ville lese eller ha endret. Det er også mulig for nettverksenheten å sende meldinger/alarmer uoppfordret til driftssentralen. Figur 11.1 viser et eksempel på hvordan en driftssentral kan drifte og styre komponenter i eget nettverk, ved å sende SNMP-forespørsler. I tillegg kan driftssentralen motta alarmer fra komponentene, som gjerne kalles traps.

Drift og styring kan foregå over Internett, over dedikerte linjer slik som for eksempel et eget IP-nett eller via et modem koblet til en ruter [9]. Dermed kan for eksempel ruteren ringes opp og driftes over telenettet, noe som er særlig nyttig når driftssentralen ikke får kontakt med ruteren over Internett. Driftssentralene kan lokaliseres hvor som helst i nettverket, og de må kunne fritt kommunisere



Figur 11.1: Drift og styring i IP-baserte nettverk ved hjelp av SNMP.

med enhetene de skal drifte. Det varierer hvorvidt organisasjoner velger å drifte over egne nett helt frakoblet fra Internett eller om driftingen skjer over Internett.

Et eksempel på nettverksenheter som overvåkes ved hjelp av SNMP, er samtrafikkpunktene NIX1 og NIX2[64] i Norge. Disse overvåkes ved hjelp av gratisprogrammet Multi Router Traffic Grapher[65] (MRTG). MRTG benytter SNMP for å hente ut informasjon fra svitsjene som realiserer NIX-ene. En akkumulert trafikkstatistikk for alle internettilbydere tilknyttet NIX-ene er offentlig tilgjengelig på NIX sine hjemmesider[66].

11.4 Sårbarheter i drift og styring av IP-baserte nett

Angrep på drift- og styringssystemet vil kunne gi en angriper fullstendig kontroll over en organisasjon sitt nett. I denne seksjonen diskuteres sikkerheten i SNMP, som i første rekke benyttes for overvåking av IP-baserte nettverk. SNMP har også støtte for konfigurering av nettverksutstyr, men det er mer vanlig å bruke Telnet og/eller web til dette. Litt forenklet er denne SNMP-funksjonaliteten adskilt med passord, ett for overvåking og ett for konfigurasjon av nettverksenheter. For drift og vedlikehold av enheter på hjemmemarkedet, som trådløse rutere og liknende, brukes ofte web.

[64] http://www.nix.no
[65] http://www.mrtg.no
[66] http://mrtg.uio.no/mrtg/nix/

11.4.1 Fysiske sårbarheter

For drift og styring av komplekse nett og tjenester, blir driftssentralene raskt viktige områder å sikre fysisk. Trenden er at drifts- og styringsfunksjoner sentraliseres til fysisk få lokasjoner, noe som i enda større grad setter store krav til fysisk sikkerhet. Dette inkluderer blant annet tilgangskontroll og akkreditering, fysisk lokasjon i forbindelse med sabotasje og uhell, nødstrømsløsninger, samt fysisk redundans i datamaskiner, datanett og transmisjonslinjer.

En driftssentral bør implementere både fysisk og logisk redundans. I forbindelse med redundans bestilles det gjerne IP-tilgang fra flere internettilbydere, med antagelse om at dette vil gi god redundans. I praksis kan dette vise seg å gi falsk trygghet, da internettilbyderne kan leie transmisjonslinjer fra den samme transportnettilbyderen. Med andre ord vil ett kabelbrudd kunne ta ned IP-tilgangen til begge internettilbyderne samtidig, og driftssentralen blir satt ut av spill.

11.4.2 Logiske sårbarheter

Logisk sikkerhet i drift og styring av IP-baserte nett, er i utgangspunktet basert på aksess til tjenestene (brannmursettinger) og aksess til SNMP/telnet/webagenten via kjennskap til passordene. Nettverkskomponentene settes ofte opp med aksesslister over hvilke IP-adresser som får lov til å drifte denne enheten. Siden SNMP kjøres over UDP, kan IP-avsenderadressen settes til hva som helst (spoofes), og angriperen kommer seg forbi aksesslisten på den måten.

En annen sikkerhetsmekanisme er å redusere antall ruterhopp en IP-pakke fra nettverksenheten kan transporteres. For eksempel vil da svaret på en SNMP-forespørsel kunne nå driftssentralen (3 ruterhopp unna), men ikke en angriper i Asia (11 ruterhopp unna). Dette vil til en viss grad øke konfidensialitetsbeskyttelsen av nettverksenhetene, men i liten grad øke integritetsbeskyttelsen. En angriper kan fortsatt sende og aktivere konfigurasjonsendringene ved hjelp av SNMP, men vil ikke få tilbake et svar om suksess eller feil.

SNMP vil som alle andre tjenester kunne inneholde logiske feil, som lar seg utnytte av en angriper. I februar 2002 publiserte finske forskere fra Universitetet i Oulu et verktøy for å teste sårbarheter i implementasjonene/realiseringene av SNMP-tjenesten til leverandører av driftssentraler og nettverksenheter [29]. Det viste seg at så å si alt utstyr fra alle leverandører var sårbare for en eller flere av testene i dette verktøyet. Dette offentlig tilgjengelige verktøyet inneholder 29.516 forskjellige tester mot nettverksenheter og 24.100 forskjellige tester mot driftssentraler. Sårbarhetene i de forskjellige realiseringene av SNMP vil i ytterste konsekvens kunne gi en angriper mulighet til å overta og kontrollere driftssentraler og nettverksenheter. Disse sårbarhetene var såpass alvorlige at de fleste leverandørene har lagt ned mye arbeid i å ordne problemene i egne produkter.

11.4.3 Sosiale sårbarheter

Krav til kompetanse 24 timer i døgnet hele året, gir naturlig sosiale sårbarheter en viktig rolle innen sikkerhet i drifts- og styringssystemer. Ikke bare må kompetansen være til stede, men organisasjonene må også ha systemer og rutiner for å kunne håndtere det dynamiske systemet i sanntid. En menneskelig feil kan få store økonomiske konsekvenser, både for organisasjonen og dens kunder.

Teknologisk sett vil en angriper ved tilgang til SNMP-tjenesten, og med antagelse om at den ikke inneholder logiske sårbarheter, måtte ha kjennskap til SNMP-lesepassordet for overvåkning av egenskaper og SNMP-skrivepassordet for konfigurasjon av egenskaper. SNMP-passordene kalles også community strings, og de vil kunne gå i klartekst over nettverket. Dette gjelder for SNMP versjon 1 og 2, mens SNMP versjon 3 støtter kryptering og signering av SNMP-trafikken. SNMP-trafikken kan også sikres ved å benytte sikre tunneler (VPN).

I følge SANS er det mange som ikke bryr seg om å bytte SNMP-passord, og ofte benyttes passordene satt av leverandørene av nettverksenhetene [71]. En angriper med passordet for konfigurasjon og oversikt over hvilke IP-adresser som får lov å drifte enheten, kan få endret mange parametere på nettverksenheten. Han kan for eksempel skru av utvalgte nettverkskort eller rute trafikken feil. På denne måten kan deler av en organisasjon isoleres fra Internett.

11.4.4 Avhengigheter

En konsekvens av den stadig økende kompleksiteten i nett og tjenester, med tilhørende krav til kompetanse, fører til at mange organisasjoner velger å outsource forskjellige IKT-funksjoner. Hvis en organisasjon velger å outsource drift og styring av utvalgte nivåer, bør den sette strenge krav til fysisk og logisk sikkerhet hos bedriften som overtar oppgaven.

Outsourcing over landegrenser kan også føre til at viktige deler av norsk kritisk infrastruktur blir underlagt områder utenfor norsk jurisdiksjon.

11.4.5 Oppsummering

En angriper med kontroll over drift- og styringssystemet til en organisasjon har også kontroll over organisasjonens nettverk. Hvorvidt dette kan ha konsekvenser for Internett avhenger i stor grad av organisasjonens rolle på Internett. Hvis for eksempel drift- og styringssystemet til en stor leverandør av tjenestedistribusjon kompromitteres, kan dette i verste fall få deler av Internett til å kollapse med hensyn på båndbreddebruk. Hvis drift- og styringssystemet til en liten ISP uten transittruting angripes vil dette opplagt kunne gå utover ISP-ens kunder, men det kan også få store konsekvenser for rutingen på deler av Internett, som beskrevet i kapittel 9.3.1.

12 Sikkerhetslaget

I dette kapitlet fokuseres det på sikkerhetstjenester og -protokoller på Internett, relatert til referansemodellen presentert i kapittel 4.1. Noen av tjenestene og protokollene vil være integrerte i de horisontale og vertikale lagene i modellen. Dette inkluderer blant annet sikring av e-post, sikring av web, sikring av navneoppslag, sikring av drift og vedlikehold, samt bruk av virtuelle private nettverk (VPN). Andre tjenester, slik som for eksempel tillitshåndtering/PKI, er ikke integrert i lagene, men er egne autonome systemer.

12.1 Sikkerhet på applikasjonslaget

Secure Shell (SSH) er et sett av protokoller for å konfidensialitets- og integritetssikre applikasjonsdata, og benytter offentlig nøkkelkryptografi/tillitshåndtering til å autentisere eksterne datamaskiner og eventuelt brukere. SSH benyttes vanligvis til å logge inn på eksterne datamaskiner, uten at brukernavn, passord og annet innhold går i klartekst. SSH tilbyr også tunnelering av andre protokoller, slik at disse blir underlagt sikkerheten i SSH.

Secure/Mulitpurpose Internet Mail Extensions (S/MIME) er en standard for å kryptere og signere e-post. MIME er et format for e-post, som tillater å skrive andre tegn enn US-ASCII og inkludere vedlegg av forskjellige formater i e-posten. S/MIME benytter tillitshåndtering med offentlig nøkkelkryptografi for å signere og kryptere e-post, samt for å verifisere signaturer og dekryptere e-post. De fleste e-postklienter støtter S/MIME, og den gir ende-til-ende sikring. Dette betyr at e-posten sikres mellom e-postklientene, og enhver sikkerhetsmekanisme mellom disse vil ikke få innsyn i e-posten. Dette gjelder for blant annet SPAM-filtre og antivirusprogramvare som leter etter ondsinnet programvare.

Pretty Good Privacy (PGP) var opprinnelig et program og en tillitshåndteringsmodell for kryptografisk beskyttelse og autentisering av data. PGP ble første gang implementert i 1991 av Phil Zimmermann, og var den gang benyttet til å beskytte innholdet i e-post. I dag er PGP en aktiv internettstandard under navnet OpenPGP, som har et vidt spekter av mulige bruksområder for å beskytte og autentisere data. PGP er basert på offentlig nøkkelkryptografi, hvor dine offentlige nøkler signeres av andre personer som stoler på deg og hvor du igjen kan signere andres nøkler. Således kan en danne et nettverk av tillit i en flat struktur fremfor i en hierarkisk struktur, som beskrevet i kapittel 12.5. PGP egner seg på grunn av dette best for tillitshåndtering i mindre grupper.

Sender Policy Framework (SPF) er en metode for å identifisere e-post med forfalsket returadresse[67], noe som ofte benyttes i spam. SPF baserer seg på at navnetjeneren til et domene angir hvilke datamaskiner som får lov til å sende ut e-post på vegne av domenet. For eksempel kan FFI angi i sin navnetjener at kun IP-adressen 10.20.30.40 får lov til å sende ut e-post fra ffi.no. En e-post som hevder å være fra FFI må derfor være sendt fra 10.20.30.40, og dette kan enkelt sjekkes av

[67] SMTP MAIL FROM/Return-Path.

mottakeren med et navneoppslag hos navnetjeneren til ffi.no. I en undersøkelse[68] utført av Measurement Factory i august 2006, viser det seg at anslagsvis 5% av navnetjenerne på Internett har støtte for SPF. Legg merke til at SPF kun er en metode for å la mottakere oppdage at ffi.no er misbrukt i en forfalsket e-post.

DomainKeys er et autentiseringssystem for e-post, utviklet av Yahoo!. Hensikten med DomainKeys er å kunne verifisere domenet til en e-postsender og tilby integritetssikring av e-posten. En e-posttjener som benytter DomainKeys signerer all utgående e-post, noe Yahoo! har gjort siden 2004. Signaturen til en e-post kan verifiseres ved hjelp av domenets offentlige nøkkel, som kan hentes ved hjelp av navneoppslag.

Transport Layer Security (TLS) og dens forgjenger Secure Sockets Layer (SSL), er protokoller for å autentisere endepunkter og utføre konfidensialitetssikring av overliggende protokoller. TLS/SSL baserer seg på tillitshåndtering med offentlig nøkkelkryptografi, og benyttes i stor grad for å sikre webtrafikk/HTTP i form av HTTPS. TLS/SSL er med andre ord protokollen som benyttes for sikring av kommunikasjonen ved bruk av nettbanker og nettbutikker på Internett.

Legg merke til at SSH, S/MIME, SSL og TLS i stor grad baserer seg på tillitshåndtering, som beskrives i kapittel 12.5. SPF og DomainKeys baserer seg på DNS.

12.2 Sikring av de fundamentale tjenestene

Domain Name System Security Extensions (DNSSec) er en protokoll for å beskytte klienter mot falske svar på navneoppslag, i form av å tilby integritetssikring og autentiserte svar. Dette gjøres ved at alle svar fra en navnetjener som støtter DNSSec er signerte. Mottaker av det signerte svaret kan verifisere signaturen ved hjelp av den offentlige nøkkelen i navnetjenerens sertifikat. Dette sertifikatet kan igjen verifiseres med en nøkkel fra et overliggende domene, slik at for `example.com` vil com-domenets offentlige nøkkel kunne verifisere `example.com` sitt sertifikat mens rot-tjenerens offentlige nøkkel vil kunne verifisere com-domenet sitt sertifikat.

På denne måten vil DNSSec kunne bli et globalt hierakisk tilitshåndteringssystem med for eksempel ICANN/USA som rotsertifikatutsteder (se kapittel 4.3.1 og 12.5). I praksis har derimot dette vist seg vanskelig å få til, blant annet på grunn av politiske føringer i forhold til hvem som stoler på hvem. I tillegg var nøkkelutveksling mellom navnetjenere vanskelig i den første utgaven av standarden. Dette ble endret i en utgave som kom i 2004, men også i denne pågår det endringer som trolig er nødvendige for å den allment akseptert.

En innføring av DNSSec vil føre til mer trafikkmengde per oppslag, noe som vil gjøre DDoS-forsterkningsangrep som beskrevet i avsnitt 7.1.2 enda mer effektive. Behovet for kryptografiske beregninger for hvert oppslag kan også tenkes brukt i ulike tjenestenektsammenhenger.

[68] `http://dns.measurement-factory.com/surveys/200608.html`

Alt dette har ført til at utrullingen av DNSSec har tatt mye lenger tid enn forventet. I følge en undersøkelse[69] utført av Measurement Factory i august 2006, støtter omtrent 1 av 100.000 navnetjenere i net- og com-domenene DNSSec. Undersøkelsen påpeker likevel at disse tallene trolig underrepresenterer global utbredelse. Enkelte europeiske toppnivådomener oppforderer aktivt til bruk av DNSSec, og blant annet er det svenske toppdomenet (se) og flere av RIPE NCC sine reversoppslag (under `in-addr.arpa`) signert.

For sikker distribusjon av tid, baserer NTP seg på såkalte sikre grupper. En sikker gruppe består av et sett av datamaskiner som deler en hemmelig verdi, kalt gruppenøkkel (K). Forenklet vil en NTP-tjener basert på K signere NTP-pakkene den sender til en NTP-klient, og således tilby autentiserte og integritetssikrede tidsstempler. For at NTP-klienten skal kunne verifisere NTP-pakkene, må den på forhånd ha fått tilgang til K. NTP-klienten er med andre ord medlem i den sikre gruppen. Legg merke til at sikker distribusjon av tid ikke baserer seg på utenforstående tillitshåndteringssystemer. Grunnen til dette er at tillitshåndteringssystemer er avhengig av korrekt tid, i forhold til blant annet gyldigheten av sertifikater og nøkler.

I terorien kunne både DNS og NTP sikres ved hjelp av virtuelle private nettverk (VPN) som IPSec, beskrevet i kapittel 12.3. I praksis ville dette vært svært ressurskrevende, da både NTP og DNS potensielt har svært mange forskjellige klienter. Ved bruk av IPSec måtte NTP- og DNS-tjeneren håndtert tilstandsinformasjon om hver ”samtidige” klient, noe som hadde krevd mye ressurser.

12.3 Sikkerhet på overføringslaget

Secure BGP[70] (S-BGP) er en foreslått arkitektur for å sikre BGP-trafikk på Internett. S-BGP baserer seg på et tillitshåndteringssystem som tilbyr autentisering av eierskap på IP-blokker og AS-nummer, autentisering av identiteten til et AS, samt autentisering av BGP-rutere i forhold til å kunne representere et AS. Det foreslåtte tillitshåndteringssystemet baserer seg på ICANN og de fem RIR-ene som root CA-er (se kapittel 4.3.1 og 12.5), og det er i skrivende stund mye arbeid som gjenstår for å realisere systemet.

Et virtuelt privat nettverk (VPN) er en fellesbetegnelse på et eget nett realisert virtuelt over et annet nett. Nettet kalles virtuelt fordi det fysisk ikke er et eget nett, og det kalles privat fordi man må gis aksess for å bruke det. For eksempel kan en bedrift sette opp krypterte tunneler mellom alle sine avdelingskontorer over Internett. All trafikk som sendes gjennom disse krypterte tunnelene er da en del av VPN-et. De krypterte tunnelene kan realiseres ved hjelp av for eksempel IP Security (IPSec), SSL eller SSH.

Som beskrevet i kapittel 11.2, er det en trend i dagens nettverk at de migrerer mot IP. Fremfor å ha egen nett for forskjellige tjenester, lager man flere VPN-er over det samme IP-nettet. For dette er det vanlig å benytte Multiprotocol Label Switching (MPLS). Ved bruk av MPLS merkes datapakkene

[69] `http://dns.measurement-factory.com/surveys/200608.html`
[70] `http://www.ir.bbn.com/sbgp/`

med hvilket VPN de tilhører, og nettverksutstyret sørger for at de rutes inn i riktig VPN. Legg merke til at MPLS ikke tilbyr konfidensialitets- eller integritetssikring, slik som IPSec og SSH. En leverandør som tilbyr VPN tilbyr derfor ikke nødvendigvis kryptering av trafikken.

En brannmur har til hensikt å analysere og filtrere trafikk mellom nettverk. Dagens datamaskiner kommer også med personlige brannmurer, som analyserer og filtrerer trafikken inn og ut til den gitte datamaskinen basert på personlige innstillinger. De enkleste brannmurene analyserer og filtrerer på overføringslaget, og kalles ofte pakkefiltre. Mer avanserte brannmurer analyserer og filtrer også på applikasjonslaget, ved for eksempel å kaste pakker som inneholder feilformaterte HTTP-felter. De aller fleste organisasjoner benytter brannmurer, og siden moderne operativsystemer i større grad har kommet med personlige brannmurer, har også disse blitt vanlige.

12.4 Sikker drift og styring

I denne rapporten har det blitt fokusert på drift og styring av IP-nettverk, ved hjelp av protokollen Simple Network Management Protocol (SNMP). Versjon 3 av SNMP er en kompleks protokoll som gir støtte for autentisering, integritets- og konfidensialitetsikring av SNMP-trafikken. SNMPv3 baserer seg på forskjellige brukere med passord for autentisering, samt bruk av forskjellige grupper for aksesskontroll. Alternativt til å benytte SNMPv3 for å sikre SNMP-trafikken, kan man også benytte SNMP versjon 1 og 2 over IPSec.

12.5 Tillitshåndtering, fundamentet for sikker elektronisk kommunikasjon

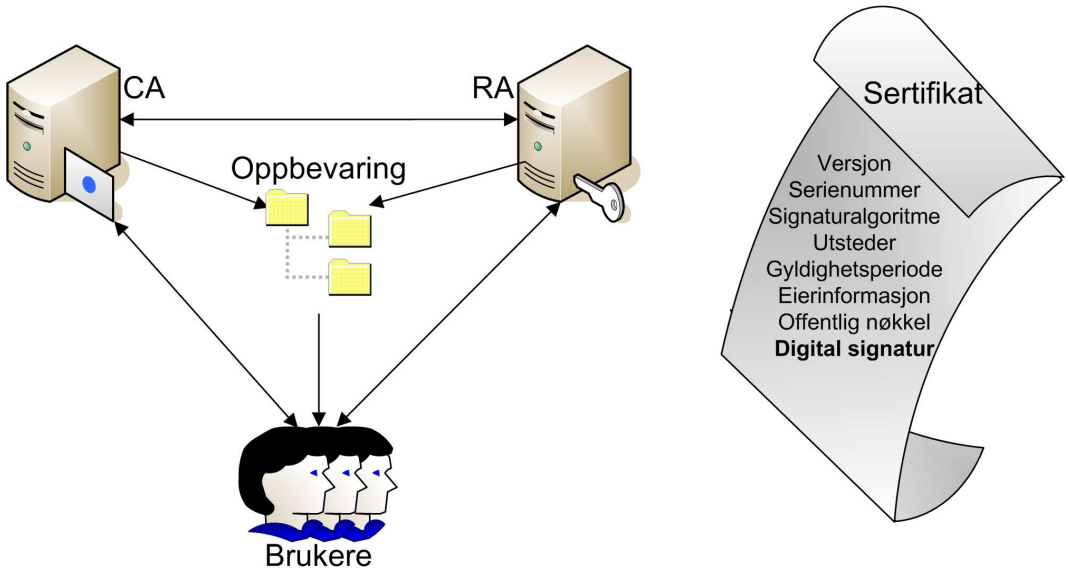
Systemer for tillitshåndtering er helt nødvendig for tjenester som blant annet nettbank, e-handel og sikker elektronisk kommunikasjon med og i offentlig sektor. Sikring av webforbindelser mellom kunder og nettbanker/nettbutikker, gjøres i stor grad ved hjelp av protokollene TLS eller SSL. Disse protokollene er beskrevet i kapittel 12.1, og refereres gjerne til som sikker HTTP (HTTPS). TLS/SSL i forhold til HTTPS baserer seg på et godt utbredt tillitshåndteringssystem, hvor det er tjenerne som autentiseres. Bakgrunnen for suksessen til dette systemet er at operativsystemer og nettlesere leveres med sertifikater/CA-er man stoler på. Denne ”ferdiglagde” enveistilliten kan brukerne endre, men dette gjøres nok av de færreste. Dette fører til at klienter enkelt kan få autentisert tjenester på Internett, men det er svært langt igjen til at tjenester også kan få autentisert klienter ved hjelp av samme tillitshåndteringssystem (toveistillit). Grunnene til dette er blant annet problemet med hvilken annen informasjon som må inkluderes i sertifikater for å kunne skille mellom enkeltpersoner, samt at man ikke stoler på klientmaskinenes sikkerhet.

I tillegg til sikring av webforbindelser, baserer mange av forslagene vedrørende sikring av viktige tjenester på Internett seg på tillitshåndtering. Dette inkluderer blant annet sikkert navneoppslag (DNS), sikker distribusjon av tid (NTP), sikker drift og styring (SNMP) og virtuelle private nettverk (VPN/IPSec).

Prinsippet for tillitshåndtering er at to ukjente parter kan stole på hverandres identitet, ved at begge stoler på en felles tredjepart som går god for identitetene. Det mest brukte konseptet for tillitshåndtering kalles Public Key Infrastructure (PKI), som er en infrastruktur som legger til rette for at brukere, datamaskiner og applikasjoner skal kunne verifisere offentlige kryptografiske nøkler. I Norge arbeides det i skrivende stund med å opprette en offentlig nasjonal PKI-infrastruktur.

Komponentene i et PKI-system inkluderer, som vist i figur 12.1, et oppbevaringssted for gyldige og annullerte sertifikater, forskjellige typer og nivåer av sertifikatutstedere (Certificate Authorities (CA)), en eller flere registratorer (Registration Authorities (RA)), og et sett av PKI-brukere. Pilene i figuren illustrerer informasjonsflyten mellom komponentene. For eksempel vil PKI-brukere hente sertifikater og annulleringslister fra oppbevaringsstedene, men oppbevaringsstedene henter ingen informasjon direkte fra PKI-brukerne.

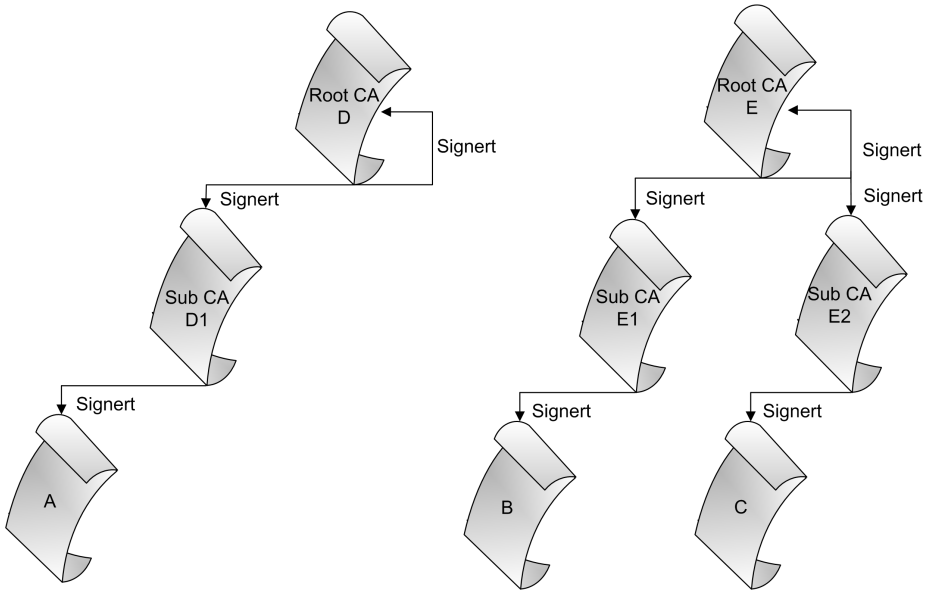
Oppgaven til en CA er å utstede sertifikater og annulleringslister. RA sin oppgave er å verifisere at PKI-brukerne kan få sertifikatene de har spurt om. Dersom man stoler på en CA, betyr det at man stoler på policyen til PKI-systemet, som CA-en er en del av. Politikken inneholder blant annet krav og regler for utstedelse og annullering av sertifikater.



Figur 12.1: PKI-arkitekturen.

Når en PKI-bruker ønsker å få utstedt et sertifikat, må brukeren først autentisere seg ovenfor RA, som da kan gå god for identiteten til brukeren. RA sørger også for at det kun utstedes sertifikater for oppgaver brukeren er autorisert for. Nøkkelgeneratoren genererer, avhengig av en spesifikasjon, en offentlig og en privat nøkkel, og informasjon om identiteten til enheten, den offentlige nøkkelen og annen relevant informasjon signeres på CA-en, med CA-en sin private nøkkel. Den signerte informasjonen og signaturen utgjør et sertifikat, og CA publiserer sertifikatet til et oppbevaringssted. Denne prosessen krever naturlig et tillitsforhold mellom RA og CA.

Valg av PKI-modell i forhold til hvem som stoler på hvem og hvor sertifikater publiseres, har sine fordeler og ulemper. En CA signerer et sertifikat som den utsteder med egen privat nøkkel. CA-en sin offentlige nøkkel er innpakket i et eget sertifikat, signert av en annen CA eller CA-en selv. På denne måten opprettes kjeder/hierarkier av signerte sertifikater, som vist i figur 12.2. En CA som signerer sitt eget sertifikat kalles en root CA, og en CA som har sitt sertifikat signert av en annen CA kalles en sub/mellomliggende CA. På toppen av kjeden vil det altså befinne seg et root CA sertifikat, som root CA-en har signert selv.



Figur 12.2: Kjede av signerte sertifikater.

Når bruker A mottar et sertifikat fra bruker B vil det ikke alltid være slik at A lokalt har sertifikatet til CA-en som signerte sertifikatet til B (Sub CA E1) i figur 12.2, samt at A eksplisitt stoler på denne CA-en. For at A skal kunne stole på og verifisere gyldigheten til sertifikatet til B, må A hente inn en kjede av sertifikater tilhørende CA-er (Root CA-E sertifikatet og Sub CA E1 sertifikatet). Hvert sertifikat i kjeden verifiseres ved hjelp av overliggende CA i kjeden sin offentlige nøkkel.

Merk at organisasjoner gjerne setter opp interne PKI-systemer. I slike tilfeller vil hele PKI-infrastrukturen være under organisasjonens kontroll, og i større grad være beskyttet mot angrep fra Internett. Det er heller ikke uvanlig at root CA-er ikke er koblet til Internett, da kompromittering av disse vil ødelegge tilliten i de underliggende hierarkiene.

12.6 Sårbarheter innen tillitshåndtering

En sikker nasjonal bruk av tjenester på Internett og sikring av forskjellige protokoller på Internett, baserer seg i stor grad på tillitshåndteringssystemer. Dette fører til en stor avhengighet av tillitshåndteringssystemer, og det bør derfor vurderes hvilken konsekvens forskjellige sårbarheter i tillits-

håndteringssystemer vil kunne ha for anvendelsen av Internett. I dette kapittelet vil PKI-systemer vurderes i forhold til avhengigheter, samt fysiske, logiske og sosiale sårbarheter.

I tillegg til de fundamentale funksjonene CA, RA, samt oppbevaringssteder for sertifikater, annulleringslister og nøkler, må et PKI-system tilby andre viktige funksjoner og sikkerhetsmekanismer. Dette inkluderer blant annet støtte for sikkerhetskopiering og gjenoppretting av nøkler, eksportering av private nøkler og sertifikater, ikke-fornektelse, automatisk oppdatering av nøkkelpar og sertifikater, støtte for nøkkelhistorikk, støtte for kryssertifisering, integrasjon med gammel programvare og støtte for bruk av åpne standarder [84].

Det ligger mange utfordringer i forbindelse med konfigurasjon av funksjonene og sikkerhetsmekanismene i PKI-systemet. For eksempel bør nøkler for digital signering aldri sikkerhetskopieres eller kunne gjenopprettes. Dette fordi et viktig krav til digital signering er at det kun skal være brukeren som har tilgang til den private nøkkelen. Nøkler for konfidensialitetsikring bør imidlertid sikkerhetskopieres og kunne gjenopprettes. Dette for å blant annet kunne lese gammel kryptert e-post. Dette argumenterer for bruken av ”et sertifikat for kryptering” og ”et sertifikat for signering”, noe som naturlig gjør systemet mer komplekst.

Dette illustrerer hvor vanskelig det kan være å designe, konfigurere og bruke PKI-systemer, samt at PKI-systemer i seg selv ofte blir store og komplekse. PKI-systemer har med andre ord alle forutsetninger for å inneholde sårbarheter, på lik linje med alle andre komplekse systemer.

12.6.1 Fysiske sårbarheter

Fysiske sårbarheter omfatter fysiske aspekter slik som materiell, geografisk plassering og fysisk redundans. Angrep som benytter seg av primært fysiske virkemidler faller i denne kategorien. I forhold til PKI omfatter dette fysiske sårbarheter i forhold til minimum CA, RA og oppbevaringsstedene for sertifikater, annulleringslister og nøkler.

I forbindelse med offentlig PKI, er prosessene rundt sertifikathåndtering regulert av esignaturloven [22]. Her settes det strenge krav til sertifikatutstedere om å administrere virksomheten på en forsvarlig måte i forhold til å tilby sikre, pålitelige og velfungerende sertifikattjenester. Post- og teletilsynet (PT) utøver tilsyn ovenfor sertifikatutstederne i forhold til loven.

Med bakgrunn esignaturloven og tilsyn fra PT, antas det at den fysiske sikkerheten er ivaretatt på en forsvarlig måte, gjennom blant annet fysisk redundans.

12.6.2 Logiske sårbarheter

I dette kapittelet sees det på sårbarheter i det logiske domenet, som stort sett omfatter sårbarheter i programvare, konfigurasjon og design. Det vil ikke bli sett på viktige sikkerhetstiltak[71] for å sikre

[71] Tolkes som påkrevet av esignaturloven.

PKI-programvaren ved hjelp av for eksempel brannmurer, antivirusprogramvare og installasjon av sikkerhetsoppdateringer.

Et sertifikat er en binding mellom en offentlig nøkkel og et navn. For bedrifter vil kanskje alle ha forskjellige navn, eller at ansatte med like navn har forskjellige roller, slik at andre kan skille hvem som er hvem. For store nasjonale PKI-systemer vil mange ha de samme navnene, og annen informasjon må benyttes for å skille disse fra hverandre. En mulighet er å inkludere personnummeret i sertifikatet, men dette vil kunne øke sannsynligheten for identitetstyveri. Sertifikatene skal jo være elektronisk tilgjengelig for alle på Internett. Hvilken annen informasjon som da må inkluderes i sertifikater for å kunne skille mellom blant annet de 820 mennene som heter Jan Johansen og alle de 647 kvinnene som heter Anne Hansen [78], forblir et problem avhengig av hvordan systemene er tenkt benyttet. Legg merke til at dette er lagt under logiske sårbarheter, da dette omfatter PKI-systemets egenskaper i det logiske domenet.

En viktig del av PKI er kontrollen av sertifikater i forbindelse med at sertifikater kan være annullerte. Alle sertifikater bør inneholde en referanse til et oppbevaringssted over annullerte sertifikater, utstedt av den gitte CA-en. Listen over annullerte sertifikater kan for eksempel hentes ved hjelp av protokollen HTTP[72], noe som betyr at annulleringslisten publiseres fra en webtjener. Det er selvsagt viktig at denne webtjeneren sikres på en best mulig måte, men kompromittering av webtjeneren vil mest sannsynlig ikke føre til kompromittering av annulleringslistene, da disse listene er signerte.

Når en PKI-bruker mottar en annens part sertifikat, bør annulleringslisten til utsteder av sertifikatet konsulteres. Det er vanlig å la PKI-systemet lagre/cache annulleringslister lokalt og benytte disse basert på en gyldighetsperiode på for eksempel 2 dager. Når gyldighetsperioden går ut, hentes annulleringslisten på nytt fra oppbevaringsstedet. Lokal caching av annulleringslister er fornuftig i forhold til den påkjenning det ville vært for nettverket og datamaskinen med annulleringslisten, hvis listen skulle konsulteres hver gang noen benyttet et sertifikat. På en annen side vil det da alltid være en tidsperiode hvor et annullert sertifikat godtas.

12.6.3 Sosiale sårbarheter

Sosiale sårbarheter dekker det menneskelige engasjement i sikkerhetsprosessen. Det fokuseres med andre ord på hvilken måte mennesker kan introdusere sårbarheter i PKI-systemet.

Et viktig valg er hvem som skal ha autoritet til å binde navn, nøkkel og andre opplysninger om en person til et sertifikat. I kravspesifikasjonen for PKI i offentlig sektor settes det krav om at en leverandør skal tilby både en CA- og RA-tjeneste. Prosessen med å utstede sertifikater håndteres dermed av leverandøren, som derfor må ha tilgang til en infrastruktur for dette. Noen sertifikater kan sendes i posten, mens andre krever personlig oppmøte [52]. Ved personlig oppmøte må mottaker bevise sin identitet ved for eksempel å vise frem passet.

[72] For eksempel `http://crl.microsoft.com/pki/crl/products/microsoftrootcert.crl` og `http://crl.verisign.com/pca1.1.1.crl`.

I 2001 utga noen seg for å være fra Microsoft, og lurte VeriSign til å utstede to sertifikater til dem [82]. Svindlerne fikk med andre ord Verisign til å gå god for at de representerte Microsoft, og sertifikatene kunne benyttes til å signere programmer. Programmer signert med disse sertifikatene ville for brukerne sett ut som programmene var fra Microsoft, og basert på dette ville brukerne valgt å kjøre/ikke kjøre programmene. I dette tilfellet var det RA-funksjonen til VeriSign som sviktet, noe som er svært alvorlig.

12.6.4 Avhengigheter

Avhengigheter omhandler koblinger til andre systemer, personer eller organisasjoner utenfor egen kontroll. I denne rapporten har det blitt sett på sårbarheter i forhold til referansemodellen presentert i kapittel 4.1, og PKI-systemer er som andre systemer på Internett avhengig av transportnettet, overføringslaget og fundamentale tjenester.

Et PKI-system er avhengig av korrekt tid ved utstedelse av sertifikater og for å kunne avgjøre gyldigheten av sertifikater og annulleringslister. Dette indikerer en sterk avhengighet til tjenesten for distribusjon av tid, som beskrevet i kapittel 7.2.

Vanligvis oppgis lokasjonene til annulleringslistene i form av domenenavn, slik som for eksempel http://crl.verisign.com/pca1.1.1.crl. PKI-brukerne er med andre ord helt avhengig av en fungerende navnetjeneste for å kunne sjekke gyldigheten av sertifikater.

Lokasjonen til tjenestene CA, RA og oppbevaringsstedene for sertifikater og annulleringslister, må være tilgjengelige over Internett. Som for alle andre tjenester, vil feil eller angrep på overføringslaget kunne føre til at disse tjenestene blir utilgjengelige. Dette kan for eksempel skje hvis PKI-tjenestene plassers på samme IP-subnett og en vilkårlig internettilbyder annonserer feilaktig en rute til subnettet via BGP. For å sikre seg mot dette kan PKI-systemet ta i bruk tjenestedistribusjon, som beskrevet i kapittel 6.3.

Bedrifter setter gjerne opp i utgangspunktet interne PKI-systemer, men disse kan for fremtiden ønskes inn i større PKI-regimer. Dette er en utfordring hvis bedriftens PKI-system er basert på en egen root CA. Enten må alle eksterne i forhold til bedriften eksplisitt stole på sertifikatet til root CA-en i bedriften, eller så må bedriften bygge opp PKI-systemet sitt på nytt og bruke en mer kjent root CA. Med kjent menes her en root CA andre allerede stoler på i for eksempel sine weblesere. Alternativt kan man benytte kryssertifisering mellom bedrifter.

Kryssertifisering i PKI-systemer er å opprette tillit mellom hierarkier av tillit/sertifikatkjeder. For eksempel kan root CA A kryssertifisere root CA B, ved å utstede et kryssertifikat til B. Etter dette vil alle brukere som stoler på A også stole på alle brukere og CA-er under B, men ikke omvendt. På denne måten vil det kunne bygges komplekse ”horisontale” tillitsnettverk mellom de ”vertikale” tilitshierarkiene. Et problem med kryssertifisering er kjennskapen til hvem som har kryssertifisert hvem. Dette krever en global katalog med oversikt over kryssertifiseringene. Hvis realiseringen av en slik global katalog er vanskelig, må eventuelt hver datamaskin/bruker lokalt ha lagret listen over

kryssertifiseringer. Det kontraktmessige ved kryssertifisering kan også være problematisk. I tilfellet over vil en bruker av CA A sine tjenester ha inngått en avtale med CA A om sikkerhetsnivå og tjenestekvalitet, men vil ikke ha et avtalemessig forhold til CA B. Slike kontraktsløse avhengigheter oppstår uansett når en kontakter en tilfeldig part og stoler på dennes CA. Dette er for eksempel den vanlige bruken av PKI til HTTPS på Internett, der en stoler på webleserens innebygde rotnøkler.

12.6.5 Oppsummering

En gjenganger i arbeidet har vært at de fleste sårbare protokoller tilhørende internettinfrastrukturen har blitt foreslått sikret ved hjelp av tillitshåndtering/PKI-modeller. Dette inkluderer blant annet sikkert navneoppslag, sikker drift og styring, sikker BGP og virtuelle private nettverk (VPN/IPSec).

Sikring av protokollene skaper dermed en stor avhengighet til tillitshåndteringssystemer, som det kan være vanskelig å realisere grunnet blant annet politiske føringer vedrørende hvem man kan stole på. Tillitshåndteringssystemer krever at sikkerheten er ivaretatt på maskinene som håndterer de private nøklene. For autentisering av klienter krever dette at klientmaskinene ikke er kompromitterte, et problem tillitshåndteringssystemer ikke kan løse.

13 Helhetsvurdering

I de siste årene har Internett blitt en svært viktig del av samfunnet, både som et kommunikasjonsmedium og som en plattform for stadig mer avanserte tjenester. Internett har blitt en viktig integrert del av mange virksomheters forretningsmodell, også de som anses å være samfunnskritiske. Private brukere har på samme måte i stor grad gjort seg avhengige av ulike typer internettjenester.

I denne rapporten fremkommer ingen entydig konklusjon på vår vurdering av sårbarheter i Internett. Vi har følgende hovedvurderinger:

- Internett blir en stadig viktigere infrastruktur for formidling av informasjon i samfunnet
- Internett har i utgangspunktet en robust arkitektur, i den forstand at informasjonens vei gjennom nettverket kan endres dynamisk ved frafall av noder eller forbindelser
- Den grunnleggende sikkerhetsmodellen for Internett tok imidlertid ikke høyde for ondsinnede handlinger på samme nettverk
- Antall publiserte sårbarheter i programvare som er tilknyttet eller er en del av Internett øker
- Strukturen i Internett er i økende grad svært kompleks og dynamisk
- Det er meget vanskelig å oppnå en robust teknisk infrastruktur i Internett som er motstandsdyktig overfor mange typer ondsinnede handlinger
- Robustheten i Internett overfor utilsiktede feiltilstander og ondsinnede aktiviteter vil i betydelig grad være avhengig av robust hendelseshåndtering i sanntid, basert på høyt kompetent personell på 24/7-basis

Denne rapporten dokumenterer vår sårbarhetsvurdering av Internett. Vi har forsøkt i størst mulig grad å avgrense denne til den norske delen av Internett. Dette har ikke uten videre vært en hensiktsmessig avgrensing. Internett består i dag av eier-, operatør-, tjeneste- og nettverksstrukturer på tvers av og uavhengig av nasjonale grenser.

I arbeidet har det blitt utviklet en referansemodell for Internett, presentert i kapittel 4.1. Modellen er teknologifokusert og deler Internett inn i horisontale og vertikale lag, hvorpå de forskjellige lagene sårbarhetsvurderes hver for seg. Det er lagt størst vekt på å gjøre en sårbarhetsvurdering av internettinfrastrukturen som er felles for de fleste tjenester, fremfor å vurdere sårbarheter som

rammer brukerne direkte i form av blant annet virus, trojanere, bakdører, uønsket e-post, kartlegging og overvåkning.

En viktig bakenforliggende årsak til sårbarhetene i Internett er det naturlige fokus på egne hensyn fremfor fellesskapets beste. Dette fører til et fokus på økonomiske hensyn fremfor oppfyllelse av et ansvar som ikke er understøttet av positive eller negative insentiver. Global informasjonssikkerhet er på mange måter et felles gode som lider under dette prinsippet når et eventuelt bidrag føles større enn det direkte utbyttet. Dette kan også føre til ansvarsfraskrivelse som en del av en virksomhets forretningsmodell, noe som er svært tydelig innenfor programvareindustrien, gjennom blant annet lisenshåndtering. Regulering på dette området, både i global og nasjonal kontekst, kan være svært problematisk.

Vår sårbarhetsvurdering er svært sammensatt, og det fremkommer ingen entydig konklusjon. På den ene siden viser våre funn at Internett er sårbart for mange ulike angrep på de forskjellige lagene i referansemodellen, i form av utnyttelse av avhengigheter og fysiske, logiske og sosiale sårbarheter. Mange av disse sårbarhetene er velpubliserte, samtidig som det også kontinuerlig gjennomføres tiltak i infrastrukturen for å redusere disse. Eksempler på slike sårbarheter ligger i viktige funksjoner som ruting (BGP) og navnetjeneste (DNS). På den annen side er det til tross for disse mer eller mindre kjente sårbarhetene ikke dokumentert angrep mot Internett med omfattende konsekvenser i tid og omfang. Spørsmålet man da må stille seg er hvorfor ingen til nå har utført svært alvorlige angrep mot internettinfrastrukturen siden den tilsynelatende er så sårbar. Et mulig svar er at de som har kapasitet til å utføre angrepet selv er avhengige av Internett. Et annet svar er at Internett, tross sine mange enkeltsårbarheter, virkelig er en robust infrastruktur.

Vi har tro på begge svar, og antar at en viktig grunn til denne tilsynelatende robustheten er den høye kompleksiteten og dynamikken som ligger i Internett. For eksempel er det sterke innebygde funksjoner for å rute IP-pakker automatisk alternative veier ved feil eller angrep. Viktige tjenestefunksjoner utstyres med redundans i eget nett, og i samtrafikk med andre internettilbydere. Denne kompleksiteten og dynamikken fører imidlertid til at drift av Internett sett fra hver operatørs ståsted er blitt et håndverk, der det kreves tilgang til svært høy kompetanse på døgnkontinuerlig basis.

Dette siste er antagelig den viktigste faktoren for at Internett i dag tross alt har utviklet seg til å bli en i hvert fall tilsynelatende robust og tilpasningsdyktig struktur. Imidlertid er det ikke sannsynlig at det i en så vidt kompleks struktur som Internett kan unngås svikt som følge av angrep eller feilfunksjoner. Det viktigste tiltaket for å redusere konsekvensene av slik svikt er rask tilgang på "håndverkere" som sørger for å redusere skade og skadeomfang, og deretter reetablerer tjenestetilbudet til sluttbrukerne.

Én sentral faktor i sårbarheten av Internett er den grunnleggende og i stor grad fysiske kommunikasjonsinfrastrukturen. Denne utgjør basis for alle internettjenester. Det er en klar trend at dagens nettverk og tjenester for elektronisk kommunikasjon (EKOM) migreres mot bruk av IP-teknologi. Dette innebærer at alle tidligere separat produserte EKOM-tjenester legges over på en felles IP-basert plattform, blant annet tradisjonell telefoni, kabel-TV, internettjenester og mobiltelefoni. IP-

teknologien er dermed i ferd med å bli en felles plattform for alle EKOM-tjenester som produseres, noe som får direkte innflytelse på nettinfrastrukturens egenskaper og dens robusthet. Dette anses å få betydelig positiv betydning for robustheten til tjenestene, ved at i hvert fall de større operatørene baserer alle sine tjenester på en felles robust nettverksplattform. En slik felles plattform kan selvfølgelig også innebære sårbarheter, men det er vår vurdering at nettoeffekten er klart positiv.

Vi har dermed en relativt åpen konklusjon på vår sårbarhetsvurdering. Det er ikke vanskelig å finne delområder innen internettinfrastrukturen der det kan argumenteres for behov for økt sikkerhet. Løsninger for sikkerhet bør imidlertid implementeres på en balansert og helhetlig måte for å gi effekt. For hver operatør ligger det store utfordringer i dette. Hever man så dette spørsmålet opp til nasjonalt nivå med ønske om å etablere et nasjonalt sikkerhetsregime for Internett i Norge, øker utfordringen ytterligere. En metodisk forankret tilnærming som gir et balansert og helhetlig sikkerhetsregime på nasjonalt nivå vil være svært vanskelig i seg selv.

Etterord

Refleksjoner rundt tiltak og mulig regulering for å oppnå robusthet i Internett

Gjennom arbeidet med denne rapporten har vi både observert og deltatt i mange interessante diskusjoner vedrørende mulige tiltak for å sikre Internett bedre. Enkelte viser stor iver og tro på at man gjennom nasjonale offentlige reguleringer og tiltak kan gjøre Internett mer robust, gjennom anvendelse av tiltak i grenselandet mellom jus og teknologi. I den andre enden finner man en ren markedstilnærming til sikkerhet, som i hovedsak går på at aktørene innen Internett selv vil gjøre jobben, og at de som ikke er gode nok på sikkerhet vil svikte og falle fra.

Et sentralt spørsmål er dermed om en nasjonal eller global reguleringslinje i forhold til sikkerhet har noe for seg. Det må forutsettes at den enkelte operatør har et godt nivå av sikkerhet innebygd i sitt tilbud tilpasset sine kunders behov. Hva som er godt nok i en nasjonal kontekst er likevel et ubesvart spørsmål. Selv om det ikke var noen opprinnelig målsetting for denne rapporten å svare på dette spørsmålet, gis det avslutningsvis noen betraktninger rundt dette.

Vår vurdering er at Internett i liten grad lar seg regulere på et globalt nivå. Grunnen til dette er at Internett eies og kontrolleres av mange aktører i et svært mangfoldig fellesskap. Det er i dag mer enn 20 000 registrerte autonome systemer (AS). Mange av disse aktørene driver ikke sin virksomhet etter kommersielle prinsipper. Nettet kjennetegnes da også i dag nettopp av en svært liten grad av overordnet global styring. Det er vanskelig å se for seg noe annet enn at global styring i stor grad vil måtte være konsensuspreget, og dermed dreie seg om svært “enkle” og langsiktige forhold.

Det kan imidlertid hevdes at det vil være enkelt å realisere et reguleringsregime nasjonalt, slik som det blant annet hevdes at det gjøres i Kina. Da er det viktig å legge til at reguleringen i Kina så langt vi har kjennskap til er knyttet til innholdskontroll, noe som må forutsettes å være uaktuelt i Norge. Innholdsregulering er også en betydelig enklere og mindre kostbar form for regulering enn å regulere sikkerhet og robusthet.

De reguleringene man eventuelt kunne tenke seg i en norsk nasjonal kontekst kan for eksempel dreie seg om krav til grunnleggende redundans i ulike deler av nettinfrastrukturen til “viktige” tjenesteleverandører. Dette kan også dreie seg om ulike former for fysisk beskyttelse av viktige infrastrukturelementer i nettet. I BAS2-prosjektet, som nettopp hadde telesikkerhet og -beredskap som tema, ble det i 1999 foreslått en rekke ulike tiltak, der disse to eksemplene inngikk i et større regime. Det foreslåtte regimet ble senere forankret i Stortingsmelding 47 (2001-2001) [70].

Forslagene fra BAS2 ble fremlagt for ca åtte år siden. Siden da har svært få av de konkrete forslagene om tiltak blitt gjennomført, av mange årsaker. Som Riksrevisjonens gjennomgang av arbeidet med IKT-sikkerhet [66] viser er dette delvis et resultat av norsk forvaltningsskikk. Det kan legges til at sakshåndtering tar tid i forvaltningen, og det er mange argumenter for at det bør ta tid. I tillegg kommer ikke minst at forhold som teknologiske forutsetninger, markedsutvikling og sikkerhetspolitisk har situasjon endret seg betydelig i løpet av disse åtte årene. Forutsetningene for et nasjonalt

sikkerhetsregime innen EKOM har dermed endret seg ganske dramatisk parallelt med dette. Mange av tiltakene som ble foreslått av BAS2-prosjektet er det antagelig heller ikke lenger hensiktsmessig å innføre. Globaliseringen på både operatør- og nettnivå gjør at flere av tiltakene trolig ikke lenger er mulig å gjennomføre. Det nasjonale handlingsrommet til å innføre en rekke typer tiltak med formål å redusere sårbarhet anses i løpet av disse åtte årene å være sterkt redusert. Utviklingen innen Internett har gitt betydelige bidrag til denne utviklingen.

Det neste spørsmålet vil da være hva som bør være Statens og samfunnets rolle innenfor sikkerhet av en for samfunnet nasjonalt viktig infrastruktur som EKOM og Internett. Denne rapporten har ikke som målsetting å gi et konkret svar på dette. Basert på tidligere erfaring fra BAS-prosjektene, oppdatert med erfaringene med arbeidet med internettrapporten, har vi likevel noen synspunkter.

Å gjøre kommersielle EKOM- og internettjenester til robuste tjenester, som med en viss grad av sikkerhet skal kunne benyttes av samfunnet også under større påkjenninger, anses ikke lenger som realistisk. Sikkerhet i slike tjenester må i all vesentlighet baseres på relasjonen mellom kunde og tjenesteleverandør. Ikke fordi dette nødvendigvis er ideelt for samfunnet, men fordi det i praksis ikke er alternativer til denne tilnærmingen. En konsekvens av dette er at det bør utvises stor forsiktighet med å etablere tekniske og organisatoriske sårbarhetsreduserende tiltak basert på en myndighets-regulering med målsetting om økt nasjonal sikkerhet. Likevel vurderes det å være enkelte typer tiltak som relativt kosteffektivt kan være med på å styrke robusthet når EKOM-tjenester utsettes for negativ påvirkning.

Et sentralt spørsmål for å avklare nødvendige tiltak er hvilket sikkerhetsnivå man bør kunne oppnå og hvilken hensikt dette skal ha for samfunnet. Dette krever i første omgang en metodisk og ikke minst sporbar prosess. Dette krever igjen betydelig kunnskap om EKOM hos myndighetene. Til en hver tid oppdatert kunnskap om teknologi og marked vil være en avgjørende forutsetning, selv for et enkelt reguleringsregime. Derfor er det svært viktig at det forankres god kontakt mellom myndigheter og operatører. Det er naturlig at et myndighetsorgan har dette ansvaret. Det er imidlertid viktig å merke seg de naturlige begrensninger som vil måtte ligge i en slik kontakt, gitt virksom-hetenes klare kommersielle føringer.

Deretter må det vurderes hvilke typer tiltak det vil være mulig å gjennomføre i et globalisert og kommersielt basert sikkerhetsregime. Med et så lavt ambisjonsnivå som her er indikert, og som ligger langt under det som er foreslått i Stortingsmelding 47, synes det hensiktsmessig å dele tiltakene inn i to hovedområder. Det første dreier seg om kompetanseutvikling og informasjon knyttet til anvendelsen av EKOM-tjenester, mens det andre dreier seg om samfunnsmessig beredskap i forhold til omfattende svikt i EKOM- og internettjenester i tid og omfang.

Et myndighetsengasjement på det første området kan være å bidra til at relevant informasjon om sikkerhet flyter mellom EKOM-operatørene og deres kunder, og at det etableres hensiktsmessige kundeavtaler dem i mellom. Herunder kommer også å utvikle bred informasjon om sikkerhet til ulike typer kundegrupper, for eksempel i form av “best practices”. Hensikten med dette er at en kunde i størst mulig grad skal vite om hvilken grad av sikkerhet en EKOM-tjeneste innehar. Dette

for å kunne forstå den risikoøkning egen virksomhet påføres som følge av EKOM-anvendelsen. Det er svært viktig at det offentlige som kunde av EKOM-tjenester blir foregangsvirksomheter på dette området. Inntrykk samlet inn gjennom BAS-prosjektene over tid har vist at offentlige kunder ofte har vært svake i denne sammenheng. Mange av disse har nok en innstilling om at dette er sektoransvaret til "et annet offentlig organ". EKOM-tjenester skal som følge av dette sektoransvaret i utgangspunktet være robuste, og "er dermed ikke vår sak". Da bestiller man de tjenestene som er rimeligst, uten hensyn til sikkerhet.

Et myndighetsengasjement på det andre hovedområdet vil dreie seg om å bistå aktørene i markedet med å redusere konsekvensen av svikt i tjenesteproduksjon. Dette kan dreie seg om tilsyn med at beredskapsplaner utvikles og følges ut fra en minimumsstandard. Dette kan også bestå av å arrangere faglig samarbeid mellom konkurrerende aktører på området, og arrangere ulike typer samøvelser for å øve på beredskapsutfordringer.

Vår vurdering er at det fremdeles er viktig at myndighetene har et ansvar for utviklingen innen sikkerhet og robusthet i EKOM-tjenester. Man bør imidlertid dempe ambisjonsnivået som ble gitt av Stortingsmelding 47 til å omfatte en grad av tilrettelegging i markedet, basert på et minimum av tilsyn av sikkerhet i offentlig tjenesteproduksjon. Det advares på det sterkeste mot et urealistisk symbolsk preget ambisjonsnivå, som vil gi brukerne i markedet en falsk forventning om nivået av sikkerhet i EKOM og Internettjenester.

A Forkortelser

ADSL	Asymmetric DSL
APOP	Authenticated POP
ARPA	Advanced Research Project Agency
AS	Autonomt System
ASCII	American Standard Code for Information Interchange
BAS	Beskyttelse av samfunnet
BIND	Berkeley Internet Name Domain
BOT	Robot
CA	Certificate Authorities
CDI	Content internetworking
CERT	Computer Emergency Response Team
CSI	Computer Security Institute
DNS	Domain Name System
DNSSec	DNS Security
DOD	Department of Defence
DOS	Denial of Service
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
EK	Elektronisk krigføring
EKOM	Elektronisk kommunikasjon
EMP	Electro Magnetic Pulse
ENUM	Telephone Number Mapping
FTP	File Transfer Protocol
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communication
HLD	High Level Design
HPM	High Power Microwave
HTML	Hypertext Markup Language
HTTP	Hypertext Transport Protocol
HTTPS	HTTP Secure
IAB	Internet Architecture Board
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICMP	Internet Control Message Protocol
IDN	International Domain Names
IDS	Inntrengningsdeteksjonssystemer
IETF	Internet Engineering Task Force
IKT	Informasjons- og kommunikasjonsteknologi

IMAP	Internet Message Access Protocol
INI	Informasjonsinfrastruktur
IP	Internet Protocol
IPSec	IP Security
IRC	Internet Relay Chat
ISC	Internet Software Consortium
ISDN	Integrated Services Digital Network
ISOC	Internet Society
ISP	Internet Service Provider
IXP	Internet eXchange Point
LAN	Local Area Network
MAC	Media Access Control
MD5	Message Digest algorithm 5
MDA	Message Delivery Agent
MIME	Multipurpose Internet Mail Extensions
MOU	Memorandum of Understanding
MPLS	Multiprotocol Label Switching
MRTG	Multi Router Traffic Grapher
MTA	Message Transfer Agent
MX	Mail eXchange
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NIX	Norwegian Internet eXchange
NORSIS	Norsk senter for informasjonssikring
NSM	Nasjonal sikkerhetsmyndighet
NTP	Network Time Protocol
OSI	Open Systems Interconnection
P2P	Peer to Peer
PDH	Plesiochronous Digital Hierarchy
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
POP	Post Office Protocol
POP(2)	Points of Presence
PT	Post og teletilsynet
QOS	Quality of Service
RA	Registration Authorities
RFC	Request for Comments
RFID	Radio Frequency Identification
RIPE NCC	Réseaux IP Européens Network Coordination Centre

RIR	Regional Internet Registries
ROS	Risiko og sårbarhet
S/MIME	Secure MIME
SANS	SysAdmin Audit Networking and Security
SCADA	Supervisory Control And Data Acquisition
SDH	Synchronous Digital Hierarchy
SIS	Senter for informasjonssikkerhet
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SPF	Sender Policy Framework
SPOF	Single Point of Failure
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunication System
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USIT	Universitetets senter for informasjonsteknologi
USNO	US Naval Observatory
VDI	Varslingssystem for digital infrastruktur
VOIP	Voice over IP
VPN	Virtual Private Network
WDM	Wavelength Division Multiplexing
WIMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless LAN
WWW	World Wide Web
XSS	Cross Site Scripting

B Begreper

Advanced Research Projects Agency (ARPA), virksomhet innenfor det amerikanske forsvarsdepartementet, som har ansvaret for å utvikle ny teknologi til militær bruk. ARPA byttet navn

til Defence ARPA (DARPA) i 1972, tilbake til ARPA i 1993 og tilbake til DARPA igjen i 1996.

Autentisering, prosessen for å bevise at en enhet (bruker, applikasjon eller datamaskin), er det som den utgir seg for å være.

Autonomt System (AS), en organisasjon som har registrert en klart definert policy i forhold til ruting av IP-pakker på Internett hos IANA.

Cache, lagring av informasjon annet sted enn kilden, og gjerne med en gyldighetsperiode. Cachen vil således avlaste informasjonskilden, da informasjonen hentes fra cachen fremfor kilden, hvis man er innenfor gyldighetsperioden.

Identitetstyveri, bruk av andres/falske identitetspapirer for å utgi seg for å være en annen person.

Inntrengingsdeteksjonssystem (IDS), forsøker å identifisere datainnbrudd ved å se på nettverkstrafikk eller datamaskiners oppførsel.

Integritet, forhindring av uautorisert modifikasjon av informasjon.

Internet Assigned Numbers Authority (IANA), enheten som overvåker global IP-adresseallokering, styrer DNS-rootsonen og tildeler identifikatorer (protokollnumre) til forskjellige protokoller . Opereres i skrivende stund av ICANN.

Internet Corporation for Assigned Names and Numbers (ICANN), ikke-profitt virksomhet opprettet 18. september 1998, for å håndtere IANA-funksjonen på Internett for amerikanske myndigheter.

Internet Engineering Task Force (IETF), arbeider med å utvikle og ”markedsføre” standarder på Internett. IETF er oppdelt i mange arbeidsgrupper, og mye av arbeidet foregår via e-postlister. IETF håndterer de mange Request for Comments (RFC-ene), og IETF egen misjon kan leses i RFC 3935.

Internettinfrastrukturen, alle lagene i referansemodellen presentert i kapittel 4.1. Lagene inkluderer transportlaget, overføringslaget, fundamentale tjenester, tjenestedistribusjon og applikasjonslaget.

Kommunikasjonsinfrastruktur, lagene som er nødvendige for å frakte IP-pakker fra kilde til destinasjon. I referansemodellen for Internett i kapittel 4.1, er dette overføringslaget og transportnettet.

Kommunikasjonssystem, samling av nettverksutstyr og annet utstyr, i form av maskinvare og programvare, som tilsammen tillater brukere eller maskiner å kommunisere med hverandre.

Konfidensialitet, forhindring av uautorisert avsløring av informasjon.

Local Area Network (LAN), nettverk som dekker et lokalt område som en bedrift, avdeling eller et hjem.

Nyhetsgruppe, en form for e-postgruppe hvor et gitt tema diskuteres i form av å sende til og lese e-post fra gruppen. Egen nyhetsleserklient, for eksempel Outlook Express, holder orden på hvilke e-post man har lest tilhørende en gruppe. Det eksisterer svært mange forskjellige grupper, alle med hvert sitt tema.

Open Systems Interconnection (OSI)-modellen, lagdelt modell for kommunikasjon mellom datamaskiner. Hvert lag benytter kun tjenestene tilbudt av laget under.

Risiko, kombinasjon av sannsynlighet og konsekvens for en gitt uønsket hendelse.

Risiko- og sårbarhetsanalyse (ROS)-analyse, prosess for å kartlegge og dokumentere risiko forbundet med et gitt system. Vanligvis ligger en sårbarhetsanalyse av systemet til grunn for å utlede risiko.

Ruter, nettverksenhet som videresender datapakker mellom nettverk. Denne prosessen kalles ruting, og foregår på lag 3 i OSI-modellen (IP-laget).

Sertifikat, informasjon om en enhets identitet og enhetens offentlige nøkkel, signert med utsteder av sertifikatet sin private nøkkel.

Signatur, informasjon generert ved hjelp av en hashfunksjon, en asymmetrisk krypteringsalgoritme, og en privat nøkkel.

Sikkerhetsmekanisme, en mekanisme for å understøtte en del av sikkerhetspolicyen. For eksempel en brannmur for å hindre eksterne tilgang til interne datasystemer og antivirusprogramvare for å håndtere virus.

Sikkerhetspolicy, et sett av regler og føringer for å opprettholde et sikkerhetsnivå og for å kunne håndtere sikkerhetshendelser.

Social Engineering, tilegne seg konfidensiell informasjon ved å manipulere personer.

Supervisory Control And Data Acquisition (SCADA), benyttes som betegnelse på et sentralstyrt datasystem for overvåkning og kontroll av gjerne distribuerte prosessnett.

Svitsj, nettverksenhet som videresender datapakker i forhold til lag 2 adresser i OSI-modellen (Ethernet).

Søkemotor, samler inn og indekserer sider på Internett. Forskjellige søkemotorer har ulike strategier for å presentere og rangere sidene opp mot søket som gis.

Tilgjengelighet, utstyr og data kan brukes av autoriserte enheter når disse har behov for det.

US American Standard Code for Information Interchange (US-ASCII), 128 utvalgte tegn, inkluderer blant annet ikke æ, ø og å.

Virtuelt privat nettverk (VPN), en fellesbetegnelse på et eget nett realisert over et annet nett. Nettet kalles virtuelt fordi det fysisk ikke er et eget nett, og det kalles privat fordi man må gis aksess for å bruke det.

Wide Area Network (WAN), nettverk som strekker seg over et stort geografisk område. Et WAN knytter sammen LAN.

Referanser

[1] Arbeidsgruppe oppnevnt av Justisministeren 1. juni 2006. Forebygging av internettrelaterte overgrep mot barn, 30. januar 2007.

[2] Aftenposten.no. Fikk 100.000 for smk.no, 3. mai 2006. http://www.aftenposten.no/nyheter/iriks/politikk/article1302379.ece. Besøkt 31.januar 2007.

[3] Akamai. http://www.akamai.com. Besøkt 15.januar 2007.

[4] Ross Anderson. Why Information Security is Hard - An Economic Perspective. University of Cambridge Computer Laboratory, 2001. http://www.cl.cam.ac.uk/~rja14/Papers/econ.pdf. Besøkt januar 2007.

[5] Anti Phishing Working Group. Phishing Activity Trends Report - December 2006 . http://www.antiphishing.org/reports/apwg_report_december_2006.pdf.

[6] Arbeids- og administrasjonsdepartementet. Strategi for IKT i offentlig sektor 2003-2005, 18. februar 2003.

[7] Nils Øyvind Audestad. Masteroppgave. Sårbarhetsvurdering av tidstjenesten NTP med fokus på tjenestenekt og integritetsangrep, 1. februar 2007.

[8] Steve Beattie, Seth Arnold, Crispin Cowan, Perry Wagle, Chris Wright og Adam Shostack. Timing the Application of Security Patches for Optimal Uptime. Proceeding of LISA '02: Sixteenth Systems Administration Conference, s 233-242, november 2002. http://www.usenix.org/events/lisa02/tech/full_papers/beattie/beattie.pdf.

[9] James Boney. Cisco IOS in a Nutshell. O'Reilly, januar 2002.

[10] Randy Bush, Daniel Karrenberg, Mark Kosters og Raymond Plzak. RFC 2870: Root Name Server Operational Requirements, juni 2000.

[11] Kevin Butler, Toni Farley, Patrick McDaniel og Jennifer Rexford. A Survey of BGP Security. ACM, april 2005.

[12] Eric Byres og Justin Lowe. The Myths and Facts behind Cyber Security Risks for Industrial Control Systems. VDE Congress Berlin, oktober 2004.

[13] CERT Coordination Center. CERT/CC Statistics 1988-2006. http://www.cert.org/stats/cert_stats.html. Besøkt februar 2007.

[14] Comendo. Annual Security Report 2006. http://www.comendo.dk.

[15] ICANN Security Stability Adisory Committee. SSAC Advisory SAC008, DNS Distributed Denial of Service (DDoS) Attacks, mars 2006. http://www.icann.org/committees/security/dns-ddos-advisory-31mar06.pdf.

[16] Computerworld. Akamai now says it was targeted by DDoS attack, 16. juni 2004. http://www.computerworld.com/securitytopics/security/story/0,10801,93862,00.html. Besøkt 12.desember 2006.

[17] Sean Convery og Matthew Franz. BGP Vulnerability Testing - Separating Fact from FUD v1.00. NANOG 28, juni 2003. http://www.nanog.org/mtg-0306/pdf/franz.pdf.

[18] Cooperative Domain Name System. A Survey of DNS Security: Most Vulnerable and Valuable Assets. Computer Science Department, Cornell University. http://www.cs.cornell.edu/people/egs/beehive/dnssurvey.html.

[19] Department of Homeland Security. The National Strategy to Secure Cyberspace, februar 2003. http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf.

[20] Domain Health Surveys. Men & Mice, 1998-2003.

[21] Ekomloven. Lov om elektronisk kommunikasjon, 2003. http://www.lovdata.no/all/tl-20030704-083-001.html.

[22] Esignaturloven. Lov om elektronisk signatur, januar 2005. http://www.lovdata.no/all/hl-20010615-081.html.

[23] Forsvarets forskningsinstitutt. Beskyttelse av samfunnet (BAS)-prosjektene, 1994-2006.

[24] David Geer. Malicious Bots Threaten Network Security. IEEE Computer, vol 38, nr 1, s 18-20, januar 2005.

[25] Jack Goldsmith og Tim Wu. Who Controls the Internet? Illusions of a Borderless World. Oxford University Press, 2006.

[26] Lawrence Gordon, Martin Loeb, William Lucyshyn og Robert Richardson. CSI/FBI Computer Crime and Security Survey, 9. årgang, 2004.

[27] Luis Grangeia. DNS Cache Snooping or Snooping the Cache for Fun and Profit, versjon 1.1, februar 2004. http://www.sysvalue.com/papers/DNS-Cache-Snooping/files/DNS_Cache_Snooping_1.1.pdf.

[28] Scott Granneman. Googling Up Passwords, mars 2004. http://www.securityfocus.com/columnists/224.

[29] Oulu University Secure Programming Group. PROTOS Test-Suite: c06-snmpv1. University of Oulu, Finland, februar 2002.

[30] Janne Merete Hagen, Kjell Olav Nystuen, Håvard Fridheim og Eirik Østby. Analyse av sårbarhetsreduserende tiltak innen telekommunikasjon, FFI/RAPPORT-99/00241, 1999. KONFIDENSIELT.

[31] Geir Hallingstad og Knut Eckstein. Cyber Defense Protection Methods. NATO Consultation, Command and Control Agency (NC3A), desember 2005.

[32] Gisle Hannemyr. Hva er Internett. Universitetsforlaget, 2005.

[33] Garrett Hardin. The Tragedy of the Commons. Science, New Series, vol 162, nr 3859, s 1243-1248, 1968.

[34] John Hawkinson og Tony Bates. Rfc 1930: Guidelines for creation, selection, and registration of an Autonomous System (AS).

[35] Andy Heffernan. RFC 2385: Protection of BGP Sessions via the TCP MD5 Signature Option, august 1998.

[36] ICANNN. Factsheet. Root server attack on 6 February 2007. `http://www.icann.org/announcements/factsheet-dns-attack-08mar07.pdf`. Besøkt 10. mars 2007.

[37] IETF. Open Pluggable Edge Services. `http://tools.ietf.org/wg/opes/`. Besøkt 15.januar 2007.

[38] Internetnews.com. Akamai Outage Raises DNS Questions, 16. juni 2004. `http://www.internetnews.com/security/article.php/3369371`. Besøkt 12. desember 2006.

[39] Harald Jansen. Building a fiber-optic network in Norway. Telektronikk 2.2005. `http://www.telenor.com/telektronikk/volumes/pdf/2.2005/Page\_102-108.pdf`.

[40] Dan Kaminsky. Doxpara research. `http://www.deluvian.doxpara.com`.

[41] Daniel Karrenberg. DNS Root Name Servers Frequently Asked Questions. ISOC Member Briefing #20, Internet Society, januar 2005.

[42] NSO/NSR ØKOKRIM/PDS og NORSIS. Mørketallsundersøkelsen 2006 it-sikkerhet og datakriminalitet, 2006. Draft.

[43] Krisberedskapsmyndigheten. Kartläggning av internetrelaterade hot. Fjärde kvartalet 2004, 2005. januar.

[44] Judah Levine, Michael Lombardi og Andrew Novick. NIST Computer Time Services: Internet Time Service (ITS), Automated Computer Time Service (ACTS), and time.gov Web Sites, mai 2002. `http://tf.nist.gov/timefreq/general/pdf/1551.pdf`.

[45] Ratul Mahajan, David Wetherall og Tom Anderson. Understanding BGP Misconfiguration. ACM SIGCOMM'02, 2002.

[46] Microsoft. MS04-028: Buffer Overrun in JPEG Processing (GDI+) Could Allow Code Execution. http://www.microsoft.com/technet/security/bulletin/ms04-028.mspx. Besøkt 7. mars 2007.

[47] David Mills. Proposed Authentication Enhancements for the Network Time Protocol Version 4, oktober 1996. http://www.ee.udel.edu/~mills/papers.html.

[48] David Mills. Computer Network Time Synchronization. Taylor & Francis CRC Press, 2006.

[49] David Mills. RFC 4330: Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI, januar 2006.

[50] David Mills, Judah Levine, Richard Schmidt og David Plonka. Coping with overload on the Network Time Protocol public servers, desember 2004. http://www.ee.udel.edu/~mills/papers.html.

[51] Nelson Minar. A Survey of the NTP Network, desember 1999. http://alumni.media.mit.edu/~nelson/research/ntp-survey99/.

[52] Moderniseringsdepartementet. Kravspesifikasjon for PKI i offentlig sektor, versjon 1.02, januar 2005.

[53] Ram Mohan. Amplified DNS Distributed Denial of Service (DDOS) Attacks and Mitigation. Presentasjon, ICANN Security and Stability Advisory Committee, New Delhi, India, 2006. http://www.cert-in.org.in/training/1stmay06/dotIN-DNS-DDoS.pdf.

[54] Doug Montgomery og Sandra Murphy. Toward Secure Routing Infrastructure. IEEE Security and Privacy, vol 4, nr 5, s 84-87, september-oktober 2006.

[55] Sandra Murphy. RFC 4272: BGP Security Vulnerabilities Analysis, januar 2006.

[56] Nasjonal sikkerhetsmyndighet. NorCERT - Månedsrapport, desember 2006, 17. januar 2007. http://www.nsm.stat.no/Documents/NorCERT/Microsoft\%20Word\%20-\%20NorCERT_maanedsrapport_12_dec_2006.pdf.

[57] Bjørn Netland. Telenors nye IP-nett. Telenor, 27. september 2005.

[58] Privat korrespondanse med NIST, 2006.

[59] Kjell Olav Nystuen. Sårbarhet i offentlig telekommunikasjon FFI/RAPPORT-98/02561, 2001. BEGRENSET.

[60] George Pallis og Athena Vakali. Insight and perspectives for content delivery networks. Communications of the ACM, vol 49, nr 1, s 101-106, januar 2006. http://doi.acm.org/10.1145/1107458.1107462.

[61] Dave Plonka. Flawed Routers Flood University of Wisconsin Internet Time Server. http://www.cs.wisc.edu/~plonka/netgear-sntp/.

[62] Justis og politidepartementet. Nou 2006:6 Når sikkerheten er viktigst, 2006. http://www.dep.np/filarkiv/277564/Nou062006-TS.pdf.

[63] President's Information Technology Advisory Committee. Report to the President. Cyber Security: A Crisis of Prioritization. National Coordination Office for Information Technology Research and Development, februar 2005.

[64] Yakov Rekhter og Tony Li. RFC 1771: A Border Gateway Protocol 4 (BGP-4), mars 1995.

[65] Classless Inter-Domain Routing (CIDR) Report. Statistikk og oppsummering AS4637 Reach. http://www.cidr-report.org.

[66] Riksrevisjonen. Riksrevisjonens undersøkelse av myndighetenes arbeid med å sikre IT-infrastruktur. Dokument 3:4 (2005-2006), 2005.

[67] RIPE NCC. List of Country Codes and RIRs, 2006. http://www.ripe.net/info/resource-admin/rir-areas.html.

[68] Peter Rybaczyk. Expert Network Time Protocol: An Experience in Time with NTP. Apress, 2005.

[69] J. H. Saltzer, D. P. Reed og D. D. Clark. End-to-end arguments in system design. ACM Transactions on Computer Systems, vol 2, nr 4, s 277-288, november 1984. http://doi.acm.org/10.1145/357401.357402.

[70] Samferdselsdepartement. Stortingsmelding 47 (2000-2001). Telesikkerhet og -beredskap i et telemarked med fri konkurranse, 2001.

[71] SANS/FBI. TOP 20 LIST, The Twenty Most Critical Internet Security Vulnerabilities, Version 5.0, oktober 2004.

[72] Stefan Saroiu, Krishna Gummadi, Richard Dunn, Steven Gribble og Henry Levy. An Analysis of Internet Content Delivery Systems. 5th Symposium on Operating Systems Design and Implementation (OSDI)'02.

[73] Bruce Schneier. Testimony and Statement for the Record: Hearing on Overview of the Cyber Problem, A Nation Dependent and Dealing with Risk. Subcommittee on Cybersecurity, Science and Research and Development, Committee on Homeland Security, United States House of Representatives, juni 2003.

[74] Senter for informasjonssikring (SIS). IKT-trusselbilde for Norge, oktober 2004.

[75] SITA. Airline IT Trends Survey 2006 Executive Summary, 2006.

[76] SITA. Passenger self-service survey - Highlights, 2006.

[77] Robert Slade. Dictionary of Information Security. Syngress, 2006.

[78] Statistisk sentralbyrå. Navnestatistikk 2004. http://www.ssb.no/navn. Besøkt februar 2005.

[79] Symantec. Symantec Internet Security Threat Report, Trends for January 06 - June 06, Volume X, september 2006. http://www.symantec.com/specprog/threatreport/ent-whitepaper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf.

[80] Symantec. Symantec Internet Security Threat Report, Trends for July 05 - December 05, Volume IX, mars 2006. http://eval.veritas.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_ix.pdf.

[81] The Honeynet Project & The Honeynet Research Alliance. Know Your Enemy - Trend Analysis, desember 2004. http://www.honeynet.org/papers/trends/life-linux.pdf.

[82] VeriSign Inc. Advisory from VeriSign Inc, januar 2001.

[83] Curtis Villamizal, Ravi Chandra og Ramesh Govindan. RFC 2439: BGP Route Flap Damping, 1998.

[84] Paul Wing og Brian O'Higgins. Using Public-Key Infrastructure for Security and Risk Management. IEEE Communications Magazine, vol 37, nr 9, s 71-73, september 1999.

[85] Xiao, Holly. BGP Security Issues and Countermeasures. MITRE Mission-Oriented Investigation and Experimentation program, Engineering Issues for an Adaptive Defense Network project, 2002.

[86] Evi Zouganeli. Optical networks: From point-to-point transmission to full network capabilities. Telektronikk 2.2005. http://www.telenor.com/telektronikk/volumes/pdf/2.2005/Page_003-019.pdf.