Innholdsfortegnelse

..... 6

1 Datasikkerhet 6

1.1 Hva er datasikkerhet? 6

1.2 Hvorfor er datasikkerhet viktig? 6

1.5 Sikkerhetssjekk for bedrifter 7

1.4 Ikke glem din Facebook konto og ditt nettbrett og smarttelefon som er blitt hackernes nye favoritter 7

2 Sikkerhetstrusler 7

2.1 Datavirus 7

2.1.1 Hva er et datavirus og hvorfor heter det virus? 7

2.1.2 Hvordan spres datavirusene? 7

2.1.3 Hvorfor er virus farlige? 8

2.1.4 Hvilke virustyper finnes? 8

2.1.5 Hva er et virusbibliotek? 9

2.1.6 Hva er hoax-virus? 9

2.1.7 Hva er muterende virus? 10

2.1.8 Hva er en Patch? 10

2.2 Malware 10

2.2.1 Hva er malware? 10

2.2.2 Keylogger 10

2.2.3 Skremselsprogram (Scareware) 11

2.2.4 Adware 11

2.2.5 Rootkits 11

2.3 Orm 12

2.4 Trojaner (trojansk hest) 13

2.4.1 Hvordan smitter trojanske hester min maskin? 13

2.4.2 Hvem angriper trojanske hester? 13

2.4.3 Hvilken skade kan en trojansk hest gjøre? 14

2.5 DDoS angrep 15

2.5.1 Definisjon 15

2.5.2 Slik ser et DDoS angrep ut 16

2.5.3 Metoder for angrep 16

2.5.4 Typer DDoS Angrep 16

2.5.5 Hvordan kan du beskytte deg mot DDoS angrep? 18

2.5.6 Brannmurer 18

2.5.7 Switches 18

2.5.8 Rutere 18

2.5.9 Applikasjonsserver for bredebåndstyring foran server parken 19

2.5.10 IPS forebygging 19

2.5.11 DDS baserte forsvar 19

2.5.12 Blackholing og sinkholing 19

2.5.13 Rene rør 19

2.6 Bakdør 20

2.7 botnet, også kalt Zombies 20

2.7.1 Hva er en bot? 20

2.7.2 Hvordan en bot fungerer? 21

2.7.4 Hvordan brukes et botnet til kriminelle handlinger? 22
2.7.5 Types of attacks 23

2.8 Brute Force 23

3 De vanligste sikkerhetshullene 24

3.1 Dårlig passord 24

3.2 Ikke oppdatert utstyr og programvare 24

3.3 Manglende virusprogram 24

3.4 Manglende brannmur 25

3.5 Åpen linje/kommunikasjon 25

3.6 Manglende sunn fornuft 25

3.7 Passordregler 25
3.7.1 Dette er passordene hackere prøver seg med 26
3.7.2 Hvordan velge gode passord? 27
3.7.3 Benytt minst åtte bokstaver i ditt passord 27
3.7.4 Benytt både små og store bokstaver 28
3.7.5 Lag en enkel huskeregel 28
3.7.6 Bytt ut bokstaver med tall 28
3.7.7 Ikke bruk ord som finnes i en ordbok eller på et språk. 28
3.7.8 Ikke bruk passord basert på personlig informasjon 29
3.7.9 Velg et vanlig ord + årstall + første stavelse av tjenesten 29
3.7.11 Ikke bruk det samme passordet overalt 30
3.7.12 Bytt passord ved jevne mellomrom 30
3.7.13 Husk at folk er forutsigbare – det samme er du 30
3.7.14 Ikke benytt «husk passord funksjonen» som ofte tilbys 31
3.7.15 Pass godt på ditt passord 31
3.7.16 Ingenting er helt sikkert 31

3.8 Surfe-regler på Internett 32
3.8.1 Dette er (som regel) ikke farlig 32
3.8.2 Dette KAN være risikabelt 32
3.8.3 Dette ER risikabelt 32
3.8.4 Grunnregler 33

3.9 E-postregler for sikker epost 34
3.9.1 Bruk hue 34

3.10 Slik beskytter du deg mot spam 35
3.10.1 Bruk flere e-postadresser ! 35
3.10.2 Hver kreativ i valg av e-postadresse 35
3.10.3 Bytt e-post adresse jevnlig 35
3.10.4 Skru av auto-svar, feriemeldinger og sykemeldinger 36
3.10.5 Ikke legg din e-post adresse på egne nettsider i klartekst 36
3.10.6 Skru av HTML-visning 36
3.10.7 Skru av bilde- og forhåndsvisning 36
3.10.8 Bruk alltid en oppdatert versjon av din nettleser og e-postprogram 37
3.10.9 Sørg for at du har et skikkelig spamfilter på både server og klientnivå 37
3.10.10 Sjekk hvilke RBL-filtre ditt spamfilter er satt opp mot 37
3.10.11 Opprett en SPF-record i sone-filen til ditt domenenavn 38
3.10.12 Hver forsiktig med å angi e-postadressen din på Internett. 38
3.10.13 Ikke åpn mistenkelig e-post eller e-post fra ukjente avsendere 38
3.10.14 Svar aldri på spam! 38
3.10.15 Klikk aldri på en URL eller nettadresse i en spammelding 38
3.10.16 Vær kritisk til «unsubribe» funksjonen i spam fra ukjent 39

3.10.17 Prøv aldre et anti-spam nettsted 39

4 Brannmur 40

4.1 Funksjon 40

4.2 Personlig brannmur 40

4.3 Trusler 41

4.4 Typer av brannmurer 41

4.5 Virkemåte 41
4.5.1 Applikasjonsfokusert 41
4.5.2 Trafikkfokusert 41

4.6 Installasjon 41

4.7 Bruk 42
4.7.1 Applikasjonsfokuserte 42
4.7.2 Trafikkfokuserte 42

4.8 Logger 43

4.9 Mer bistand 43

5 Sikring av trådløse nettverk (WI-FI) 43

5.1 WEP – den store synderen 43

5.2 WPA – krypteringen er ikke sterkere enn passordet 43

5.3 WPS – den skjulte sårbarheten 44

5.4 Å skjule nettverket er ingen god løsning 45

5.5 Logg inn på ruterens administrasjonsgrensesnitt 45

5.6 Oppdater firmware (operativsystemet) 45

5.7 Bytt til et unikt nettverknavn 46

5.8 Ikke skjul nettverknavnet 46

5.9 Ikke bruk WEP eller WPS 46

5.10 Bruk WPA2 med AES-kryptering 46

5.11 Bruk et godt passord på det trådløse nettverket 46

5.12 ..og på ruterens konfigurasjonsside 46

5.13 Slå av fjernadministrasjon 47

5.14 MAC-filtrering er ikke tilstrekkelig 47

5.15 Trenger du UPnP? 47

5.16 En bedre DNS? 47

5.17 Sjekk tilkoblede enheter 48

6 Sikring av datamaskiner 48

6.1 Hver forsiktig med Windows og Android 48

6.2 Skaff deg en personlig brannmur 48

6.3 Skaff deg et anti-virus program 49

6.4 Steng alle åpne porter på datamaskinen 49

6.5 Hold maskinen og programmene oppdatert 49

6.6 Passord beskytt sensitive filer og mapper *49*

7 Sikring av mobiltelefon og nettbrett **50**

7.1 Mobiltelefoner og nettbrett må håndteres på samme måte som datamaskiner *51*

8 SSL | Secure Sockets Layer **51**

8.1 Trygg overføring av data og transaksjoner! *51*

8.2 Sikkerheten avgjøres av krypteringsalgoritmen *51*

8.3 Hvorfor SSL? *51*

8.4 Bruksområder for SSL *52*

8.5 Kryptering over TCP/IP – nivået *52*

8.6 Hva er TCL (Transport Layer Security)? *53*

8.7 Krypterte porter *53*

8.8 Nettlesergjenkjennelse *54*

8.9 Transaksjonsforsikring *54*

8.10 Utstedes av et sertifiseringorgan *54*

8.11 Hvordan ser jeg at en nettside bruker SSL? *54*

8.12 Anbefaling *54*

9 Sikkerhetskopiering **55**

9.1 Hva kan skje med lagret informasjon *55*

9.2 Hvilke informasjoner skal sikres *55*

9.3 Gode vaner er viktig *55*

9.4 Typer sikkerhetskopi *55*

9.5 Intern oppbevaring *55*

9.6 Ekstern oppbevaring *56*

9.7 Typer av lagringsmedia *56*

9.7.1 CD og DVD 56

9.7.2 Minnepinner 56

9.7.3 Ekstern harddisk 56

9.7.4 Datatape/ kassett 56

9.7.5 Online tjenester 56

10 Hva må du huske på når du kaster din PC, Mac, kamera eller mobil? **57**

10.1 Husk å slett all sensitiv informasjon *57*

10.2 Det holder ikke å bare trykke på «Delete» *57*

10.3 Sjekkliste: *57*

10.3.1 PC 57

10.3.2 Mobiltelefon 58

10.3.3 Digitalkamera 58

10.4 Ansvar for sikker sletting *58*

11 Hvem står juridisk ansvarlig for sikringen og innholdet i nettskyen? **59**

11.1 Virksomheten er juridisk ansvarlig *59*

11.2 Hvilket ansvar har nettsky leverandøren? *59*
11.3 Risikovurdering og informasjonssikkerhet *59*
11.4 Informasjonsplikt *60*
11.5 Særlige problemstillinger *60*
11.6 Det gjelder å holde tunga rett i munnen *61*
11.7 Sjekkliste *61*
11.8 Noen banale sikkerhetsregler *61*

1 Datasikkerhet

1.1 Hva er datasikkerhet?

Datasikkerhet er et begrep som går ut på å beskytte data (filer, informasjon m.m.) mot uautorisert tilgang, sørge for at vi ikke mister noe data, hindre at andre får kjennskap til data eller at data blir endret.

Datasikkerhet er et fagområde som er knyttet til:

- **Konfidensialitet**: Å sikre at informasjon og informasjonssystemer bare er tilgjengelig for de som skal ha tilgang.
- **Integritet**: Å sikre at informasjon og informasjonssystemer er korrekte, gyldige og fullstendige.
- **Tilgjengelig**: Å sikre at informasjon og informasjonssystemer er tilgjengelig innenfor de tilgjengelighetskrav som er satt.

  Hensikten er å iverksette relevante, tilstrekkelige og effektive tiltak slik at forretningsprosessene har tilgang til informasjon med ønsket grad av sikkerhet.

  Relevante og kjente internasjonale standarder for informasjonssikkerhet er ISO/IEC 27000-serien og ISF Standard of Good Practice.

1.2 Hvorfor er datasikkerhet viktig?

Antall hackerangrep har de siste årene omtrent blitt doblet fra år til år. Samtidig viser survey at Nordmenn er generelt for naive når det gjelder datasikkerhet og de har for dårlige IT-systemer til å beskytte seg. Dette til tross for at det er over 40 år siden det første dataviruset kom. Folk flest har ennå ikke skjønt at det er farligere å surfe på Google enn å besøke porno nettsteder.

Allerede i 2011 ble det dokumentert at 820 nordmenn ble rammet av nettkriminalitet hvert minutt, uten at dette har gjort noe med Nordmenns holdning til datasikkerheten. Avstanden mellom trussel og sikkerhetstiltak blir stadig større!

Alle kan hackes, og sannsynligvis er du blitt hacket minst en gang allerede. Spørsmålet er derfor: **– Hva kan du gjøre for å beskytte deg?**

Når vi vet at antall kyberangrep og alvorlighetsgraden i dem stadig øker, er det skremmende å se at nordmenn flest ikke tar datasikkerheten på alvor. I 2014 var 1 av 4 PC er fortsatt uten et aktivt anti-virus program, selve forutsetningen for å kunne beskytte nettverket og maskinen mot datainnbrudd.

1.3 Hvor godt har du sikret ditt nettverk, og din datamaskin, nettbrett og mobil?

Situasjonen i næringslivet er ikke bedre. I 2013 ble 1 av 3 datamaskiner kastes rett på dynga uten at sensitive data og bedriftshemmeligheter på harddisken var slettet først. Dette sier bare litt om hvor lite beviste nordmenn er på datasikkerhet og hvor lite alvorlig de tar dette spørsmålet.

Datasikkerhet

Hvordan er det med deg? Tar du datasikkerhet på alvor og hva har du selv gjort for å sikre ditt nettverk, datamaskiner, nettbrett og smarttelefoner mot kyberangrep og datainnbrudd?

Når vi snakker om datasikkerhet tenker folk flest umiddelbart på sine nettverk, servere, PCer og Macer. Å sikre disse er selvfølgelig viktig, men å sikre disse enhetene er ikke nok. Hackernes nye favoritter er sosiale medier og smarttelefonene. Disse er på langt nær like godt beskyttede som nettverkene til næringslivet og de millioner av datamaskiner i de tusen hjem.

1.5 Sikkerhetssjekk for bedrifter

NorSIS har laget en Sikkerhetssjekk som gir deg muligheten til å sjekke hvilke sikringstiltak din virksomhet har iverksatt innen informasjonssikkerhet. Formålet med Sikkerhetssjekken er at du lett og raskt kan gjennomgå en liste av viktige sikringstiltak og få en oversikt over hvilke tiltak virksomheten har implementert og hva den mangler. Du kan velge mellom to nivåer av Sikkerhetssjekken. Du må selv vurdere hvilket nivå du skal velge, og dersom din virksomhet er svært avhengig av IT eller behandler konfidensiell informasjon bør du vurdere om du trenger flere sikringstiltak. Dersom du har høye sikkerhetsbehov, bør du forholde deg til informasjonssikkerhetsstandarden og kravene satt i ISO 27002.

1.4 Ikke glem din Facebook konto og ditt nettbrett og smarttelefon som er blitt hackernes nye favoritter

2 Sikkerhetstrusler

2.1 Datavirus

2.1.1 Hva er et datavirus og hvorfor heter det virus?

Datavirus er små dataprogrammer som spres til PC-er, Mac-er, nettbrett, smarttelefoner og servere, uten at eierne eller brukerne ønsker det.

For at det skal kalles et virus må det ha evnen til å reprodusere seg for videre spredning fra en infisert maskin og til andre maskiner.

Datavirus kan være alt fra harmløse men irriterende og til svært destruktive og farlige.

Selv om det er over 40 år siden det første dataviruset kom, hadde fortsatt 1 av 4 PC-er ikke et anti-virus program i 2014 som virker. Det virker dermed som om folk ikke forstår risikoen med disse virusene. Jeg har derfor skrevet denne artikkelen for å gjøre deg oppmerksom på faren og hvilke ulike former for datavirus som finnes.

2.1.2 Hvordan spres datavirusene?

Viruset i seg selv er laget for å reprodusere seg, dvs. lage en kopi av seg selv for å sende videre, og bruke en eller annen form for kommunikasjon – vanligvis et e-postprogram – til å spre seg videre. Ofte brukes adresseboken i e-postprogrammet ditt som utgangspunkt for å finne nye potensielle ofre for smitte, og det er ganske ”smart” av viruset; da vår dine kjente det de tror er en e-post fra deg, og den åpner de vel i god tro..?

Grunnlaget for første spredning av nye virus er ofte en automatisk innsamling av e-postadresser fra Internett, adressene er som kjent lett å finne ved at man søker på strenger med @ inni. Hvis du sprer e-postadressen din på nettet ukritisk, øker sjansen for at du blir mottaker av virus, og dette bør du tenke på når du videresender kjedebrev, deltar i debatter (web eller news) eller bruker andre Internettjenester. Et lite triks som jeg selv (ikke ofte nok...) bruker er å endre e-postadressen fra 'redaksjonen@iktnytt.no' til 'post-alfakrøll-iktnytt.no. Dermed vil de som ønsker det kunne forstå hva som er e-postadressen, mens automatiske søkeprogrammer ikke finner den fullt så enkelt.

Tidligere var e-post den vanligste måten å spre virus på, men de fleste ISPèr har i dag installert gode virusprogrammer på mailserverne sine som stopper de fleste av disse virusene før du mottar dem. Et større problem er de virusene som spres via nettsidene du besøker med din PC, Mac, nettbrett eller smarttelefon.

Hver spesielt oppmerksom på at de vanligste viruskildene på Internett i dag er:

- **fildelingsprogrammene (torrents)**
- **alle former for nedlastning av filmer, musikk, dokumenter, porno og lignende. Det er ingenting som er gratis. Spesielt ikke på Internett.**
- **gratisprogrammene du laster ned**
- **diskusjonsforumer og chatte-tjenester**
- **pornografiske og erotiske sider**
- **deltagelse i sosiale medier som f.eks. Facebook**

Datavirus sprer seg typisk over flere faser. Merk at det er variasjon i mønsteret fra datavirus til datavirus:

- **En infisert datafil blir lasted ned eller kopiert til en uinfisert maskin.**
- **Datafilen eksekveres så snart filen finnes på den uinfiserte maskinens harddisk**
- **Viruset aktiveres og kopierer seg inn i nye vertsfiler.**
- **Denne vertsfilen kopieres til en ny maskin osv**

2.1.3 Hvorfor er virus farlige?

Det er ikke nødvendigvis slik at virus er farlige i det hele tatt, men mange av dem er det og skaper til dels store problemer for eier og brukere av PC-er og servere. Problemene kan være alt fra å irritere brukerne gjennom å vise f.eks. ønskede politiske budskap på PC-en hver gang du starter opp, til å manipulere operativsystemet (f.eks. Windows) og ta kontroll over PC-en og bruke denne til å utføre kriminelle handlinger.

Vi skiller gjerne mellom "ufarlige" og "destruktive" virus, og det er de destruktive som ofte utgjør et problem. De mest "vellykkede" virusene har påført verdenssamfunnet kostnader i milliardklassen.

2.1.4 Hvilke virustyper finnes?

Helt siden PC-ens barndom har det blitt laget nye typer virus, og innenfor hver type finnes det mange ulike varianter. En måte å dele virus inn på kan være som følgende:

Eksekverbare (kjørbare) filer, dvs. filer med etternavnet .com (må ikke forveksles med Internettsider) eller .exe. Slike virus var vanlige tidlig på 80-tallet og gjemte seg inne i slike filer med kjente navn. Dermed var det vanskelig å oppdage dem, vanligvis greide vi å finne dem ved å sjekke størrelsen på de mest kjente filene; hvis "din versjon" av en kjent exe-fil var større enn den skulle ha vært, var det ofte et tegn på virus.

Boot-sector-virus: Dette er virus som hadde evnen til å legge seg i diskenes (eller diskettenes) boot-sector, dvs. der maskinene starter å lese før operativsystemet lastes inn. Disse virusene greide ofte å slå av virusbeskyttelsen slik at de ikke ble oppdaget.

Makrovirus: Dette er virus som utnytter de makrospråkene som mange brukerapplikasjoner etter hvert fikk. En makro er en samling tastaturtrykk som utføres automatisk, en vanlig måte å automatisere ulike oppgaver på. Etter hvert som makrospråkene ble svært avansert, som f.eks. Microsoft VBA (Visual Basic for Applications), ble det også mulig å skrive avanserte virus og spre dem som makroer. En vanlig måte å gjøre dette på var å infisere den globale dokumentmalen (i MS Word heter denne "normal.dot") slik at alle nye filer var smittet allerede fra starten, og makroene var vanligvis auto-makroer som starter automatisk når f.eks. filen åpnes. For å stoppe dette problemet innførte mange bedrifter forbud mot, og automatisk fjerning av, makroer, til stor fortvilelse for de av oss som laget "nyttige" makroer. Nå har problemet blitt litt nedtonet og de fleste applikasjoner gir nå en advarsel hvis det er en makro i filen som åpnes.

Skript-virus. Dette er en videreutvikling av makrovirus som utnytter de skriptmulighetene som brukes f.eks. ved innlogging på nettsider o.a. Skriptene er enkle ASCII-baserte filer skrevet i f.eks. VBS (Visual Basic Script) eller JavaScript. Skript-virus kan angripe alle typer applikasjoner som tillater kjøring av slike skript, og de fleste script-virus har angrepet e-postapplikasjoner som MS Outlook og Outlook Express.

Internett-ormer (eller bare ormer): Dette er virus som spres gjennom ulike former for kommunikasjon over Internett, mest brukt er e-post. Introduksjonen av Internett som et tilbud til alle, ga virusprodusentene et svært godt og effektivt grunnlag for spredning av virusene sine.

2.1.5 Hva er et virusbibliotek?

Et virusbibliotek er en oversikt over alle kjente virus som virusjegerne har funnet. Dette biblioteket inneholder bestemte egenskaper – også kalt signatur – for hvert enkelt virus som gjør det mulig å søke etter dette på en harddisk. Når virusjegerne finner et nytt virus, oppdateres virusbiblioteket, og da må brukerne av antivirusprogrammet oppdatere sitt bibliotek for at programmet kan finne ut om du er infisert.

2.1.6 Hva er hoax-virus?

Hoax betyr bløff eller spøk og brukes om falske advarsler om virus. Slike hoax-virus spres gjennom ukritisk videresending av e-post. Du kan bidra til å hindre dette ved aldri å videresende slike advarsler hvis du ikke har mulighet til å sjekke dem først. En enkel måte å sjekke på er å gå til hjemmesiden for en av de store antivirusleverandørene; finner du ikke noe om det aktuelle viruset der, er det sannsynlig en hoax.

Et slikt hoax-virus kan være alvorlig nok fordi spredningen av e-post på denne måten hindrer normal bruk av e-postsystemet (Denial of Service) og fordi folk blir alarmert og setter i verk tiltak uten at det er grunn til det.

Bruken av hoax-virus bygger på folks frykt for virus og vilje til å spre informasjon om farlige virus til venner og bekjente.

Kjennetegn på et hoax-virus kan være at de ofte gir skinn av at det haster å varsle andre og de oppgir gjerne store kjente firma som referanse (sjekk på firmaets hjemmeside). Det beste du kan gjøre er å videresende (eller varsle) driftspersonalet, men ikke videresende det til alle du kjenner!

2.1.7 Hva er muterende virus?

Et muterende virus er et virus som har den egenskapen at det kan lage kopier av seg selv som endres mer eller mindre fra gang til gang. Dermed endres også de karakteristikkene eller signaturen som virusjegerne bruker for å detektere virus. Dette er avanserte virus som kan være svært skadelige, og det er svært kompetente programmerere som står bak slike virus.

2.1.8 Hva er en Patch?

En patch er det samme som en ”bot” som brukes for å tette et sikkerhetshull i en operativplattform eller en applikasjon. Når slike hull oppdages lager leverandøren (f.eks. Microsoft) en liten programsnutt som tetter akkurat dette hullet. Slike patch-er må du som bruker laste ned og installere snarest mulig for å være sikker på at ikke et virus skal utnytte akkurat dette sikkerhetshullet.

2.2 Malware

Innenfor sikkerhet finnes det en mengde ord og uttrykk du bør være klar over for å forstå det som blir skrevet. På denne siden har jeg samlet en kort forklaring av de viktigste generelle begrepene.

2.2.1 Hva er malware?

Malware står for ***malicious software***, eller ***ondsinnet programvare***. Dette er en samlebetegnelse for all programvare som kommer seg inn på maskinen din uten av du vil det og gjør skade av ett eller annet slag: spionvare, ormer, virus, trojanske hester etc. Folk flest kaller alt for virus, selv om virus ikke spenner over alt av ondsinnet programvare.

2.2.2 Keylogger

Keylogger er et verktøy for å avlytte tastetrykk og informasjon om hva brukeren foretar seg på en datamaskin. Verktøyet kan bestå av programvare eller en elektronisk enhet som f.eks. kan kobles mellom tastatur og datamaskin. Keyloggeren loggfører tastetrykk, og evt. annen informasjon som skjermbilder, for så å overlate disse til en tredjepart.

Enkelte varianter av spyware er keyloggere som er i stand til å fange opp brukerens skjermbilder og tastetrykk. Det hevdes at det bare i USA har blitt stjålet 24 milliarder dollar

på denne måten. Keyloggere kan altså la skurken komme i besittelse av ditt kontonummer, pinkode, osv.

Politimyndigheter benyttet slike verktøy i enkelte tilfeller der den mistenkte har vært i besittelse av kryptert informasjon. Ved å avlytte tastetrykkene har de kommet frem til passord slik at informasjonen kan dekrypteres.

2.2.3 Skremselsprogram (Scareware)

Et skremselsprogram, eller *scareware*, holder pc-en din som gissel. Det vil prøve å få tak i kredittkortinformasjon for å rense pc-en din for ondsinnet programvare. Selv om den selv er ondsinnet! Slike programmer gir seg ut for å være anti-virus-programmer eller lignende.

2.2.4 Adware

Adware (av **Ad**vertising soft**ware**) er en økonomisk modell som skal sikre produsent av et dataprogram inntekter. Bruker inngår ved installasjon av programmet en avtale med produsent som gir denne rett til å publisere reklame – som regel begrenset til den tid programmet er i bruk. Begrepet grenser inn mot shareware og freeware.

Adware omtales ofte i samme åndedrag og blir ofte blandet sammen med spyware. Grunnen er delvis at enkelte av de samme mekanismene er tilstede og delvis medias manglende faglige forståelse og ønske om å skape nyheter.

Adware-program skal ha en lisensavtale som brukeren skal godta for å kunne bruke programmet. Denne avtalen vil inneholde vilkår som gir leverandøren rett til å distribuere reklame til brukeren. Denne distribusjonen vil i mange tilfeller være rettet, ved at programmet rapporterer tilbake hvilke sider på Internett en bruker besøker. Informasjonen er vanligvis anonym, men knyttet til for eksempel lisensnummeret på programvaren. Dette er normalt det elementet av spyware som adware inneholder.

Det finnes egne skannere for å finne og fjerne adware. Disse er gjerne utviklet på bakgrunn av brukeres bekymring for *spyware*. Dette har generert rettssaker mellom produsenter av adware og skanner-utviklerne. I tillegg vil ofte disse skannerne medføre at adware- programmene ikke lenger fungerer.

2.2.5 Rootkits

Så snart du har fått installert et virus, orm eller trojaner på maskinen vil programmet prøve å gjemme seg slik at det ikke blir oppdaget av maskinens anti-virus og anti-spyware programmer. Gjennom å bruke teknikker som kalles for *rootkits* klarer de å endre operativsystemets innstillinger slik at de blir «usynlig» tjenester som kjører i bakgrunnen og som ikke vises på noen monitorer i systemet. Dette gjør det nærmest mulig å oppdage og utrydde dem.

2.3 Orm

Innenfor datasikkerhet dukker begrepet «orm» og «ormer» opp ved jevne mellomrom, men hva er egentlig en orm?

Ormer er en spesialkategori av virus. En variant av virus er som ikke trenger noen vert for spredning. Ormer har selv de mekanismer som kreves for spredning, men opptrer og ødelegger for øvrig på samme måte som virus. Innebygde mekanismer sørger for å spre ormen videre ved å sende e-post med et infisert vedlegg fra datamaskinen ormen har infisert – uten hjelp fra noen. I tillegg til reproduksjon, kan både virus og ormer ha andre funksjoner.

Mange ormer som har blitt opprettet er laget kun for å spre seg, og ikke forsøke å endre systemene de passerer gjennom. Men som Morris-ormen og Mydoom viste, kan selv disse «*nyttelast gratis*» ormer forårsake store forstyrrelser ved å øke nettverkstrafikk og andre utilsiktede effekter. En «*nyttelast*» er koden i ormen designet for å gjøre mer enn å spre ormen videre. Ormen kan ha som oppgav å slette filer på harddisken og alle

andre lagringsmedia som finnes i maskinen eller som settes inn i maskinen senere. Andre ormer som f.eks ExploreZip ormen kryptere filer i en cryptoviral utpressing angrep, eller sende dokumenter via e-post. En veldig vanlig nyttelast for ormer er å installere en bakdør i den infiserte datamaskinen for å tillate etablering av en «zombie»-datamaskin under kontroll av ormen forfatteren. Slike ormer kan være tidsbomber som går av på en gitt tid, eller **logiske bomber** som går av under en gitt forutsetning eller handling.

Ormer benyttes ofte til å avlytte brukeres passord og for å skaffe kontroll, og ta over maskinen. Ofte spres de gjennom e-post, og sender seg selv videre til alle på adresselista i e-postprogrammet.

Det minste kjente dataviruset er på 13 bytes. Det største kjente viruset er på over 2,84 Terabytes. Viruset ble formet under feilprogrammering av programvare i datahovedbasen NKPA, Florida.

De fleste ormer begynner som e-postvedlegg som infiserer en datamaskin når de blir åpnet. Ormen søker gjennom den infiserte datamaskinen etter filer, for eksempel adressebøker eller midlertidige nettsider som inneholder e-postadresser. Ormen bruker adressene for å sende ut infisert e-post og forfalsker (engelsk: to spoof) ofte Fra-adressen i disse e-postmeldingene, slik at de infiserte meldingene ser ut som de kommer fra noen som mottakeren kjenner. Ormen sprer seg deretter automatisk gjennom e-post, nettverk eller sikkerhetsproblemer i operativsystemer, og overbelaster ofte disse systemene før noen avslører årsaken.

Ormer er ikke alltid destruktive for datamaskiner, men de forårsaker vanligvis problemer med ytelse og stabilitet for datamaskiner og nettverk.

Ormer sprer seg gjennom sikkerhetshull i maskinen din. De kan spre seg fra pc til pc over nettverket selv om du ikke sitter ved pc-en. Slik ondsinnet programvare kan spre seg meget raskt og benytter kjente sikkerhetshull i datamaskiner som ikke er oppdatert! Spredningen skjer ofte så fort at de kan overbelaste virksomhetens nettverk eller e-postserver.

2.4 Trojaner (trojansk hest)

En trojanske hest eller **trojaner** er et uønsket tilleggsprogram i form av en fil som utfører uønskede handlinger på din datamaskin, nettbrett eller smarttelefon.

Trojanere kjennetegnes av å være et noe det ikke er. F.eks. et lite program som skal sjekke datamaskinen din for feil eller virus, oppdatere en driver eller ber deg bli med på noe morsomt bare ved å klikke på et bilde eller lignende. Så snart du har gjort det, er maskinen din smittet.

Navnet stammer fra fortellingen om da byen Troja ble nedkjempet ved at angriperne skjulte seg i det som senere har blitt kalt en trojanske hest. Navnet har det fått fordi trojaneren ofte gjemmer seg inni andre programmer du installerer på din maskin. Akkurat som i historien om kampen om «Troja» i gresk mytologi.

Trojanere er et slags virus som er forkledd som nyttige eller morsomme filer eller programmer og som starter når brukeren åpner eller starter det han tror er et ufarlig program eller en fil. Slike programmer kan virkelig gjøre stor skade.

2.4.1 Hvordan smitter trojanske hester min maskin?

Trojanere er en type malware som i motsetning til datavirus krever at mottageren på en eller annen måte starter programmet. De vanligste måtene en trojaner får tilgang til din maskin på er gjennom en av følgende fremgangsmåter:

- Du laster ned et gratis program fra Internett eller fra en CD-ROM eller DVD plate som utgir seg for å være et nytte program du har bruk for. Gjerne en gratis «trial» versjon av en anti-virus program, skjermbeskytter eller lignende. Inni denne gratis pakken ligger det gjemt en fil (trojaner) som blir installert og aktivisert samtidig.
- Du laster ned og installerer et tillegg til et annet program du allerede har, f.eks. en plug-ins til WordPress eller Joomla!. Det du ikke vet er at det samtidig ligger en trojaner gjemt i pakken som installeres og aktiviseres samtidig.
- Du laster ned piratkopi av en film eller musikk fil fra en Torrent nettverk. Det du ikke vet er at du samtidig laster ned en trojaner som blir aktivisert i det øyeblikket du starter filmen eller MP3 filen.
- Du klikker på et bilde i en nettside, på Facebook eller et annet nettsted. For å friste deg til å klikke på dette bilde sier de f.eks. «Sjekk hva dine venner mener om dette» eller lignende. Så snart du klikker på bilde eller linken blir maskinen din smittet av en trojansk hest.
- Du mottar en e-postmelding med et fil-vedlegg som du blir bedt om å åpne. Så snart du åpner fil-vedlegget, f.eks. en bildefil eller pdf-dokument, smittes maskinen din samtidig av en trojansk hest.

2.4.2 Hvem angriper trojanske hester?

Trojanerne angriper alle datamaskiner, enten det er snakk om Windows, Mac eller Linux baserte maskiner. Dernest angriper de alle typer nettbrett og alle smarttelefoner som bruker Android eller IPhone operativsystem. I praksis kan dermed alle bli smittet av en trojaner.

2.4.3 Hvilken skade kan en trojansk hest gjøre?

Har maskinen din blitt infisert av en trojaner er det ingen begrensninger for hvilke skader den kan gjøre på din maskin.

Hensikten med en trojaner er ofte å stjele informasjon fra deg, legge opp filer som andre kan hente, eller bruke din maskin som utgangspunkt for angrep mot andre datamaskiner (som en del av et**botnet**).

En type trojaner som utfører en handling på et forhåndsbestemt tidspunkt kalles en **logisk bombe**.

Ofte inneholder Trojanske hester spionprogramvare, men de kan også inneholde virus som starter å spre seg etter nedlasting.

For kort tid siden ble det oppdaget en trojaner som ble spredt til flere hundre tusen norske datamaskiner og som prøvde å ta kontroll over påloggingen til norske nettbanker, for så i verste fall, utføre banktransaksjoner i andres navn.

En annen trojaner ble for kort tid siden oppdaget i en av annonsene til Teknisk Ukeblad. Ved å klikke på bilde ble du redirectet til en annen side som forventet, men annonsen startet samtidig nedlastningen av en .jar-filen (Java fil) til din datamaskin. Så snart filen er lastet ned vil den prøve å kjøre et program i bakgrunnen. Programmet er en versjon av Citadel- og Zeus-trojanerne, som er programmert til å ligge i bakgrunnen og registrere tastetrykk, lagre passord og informasjon, samt ta skjermbilder. Informasjonen som trojaneren finner sendes så tilbake til hackeren som kontrollerer botnettet som maskinen din er blitt en del av.

Appel fikk tidligere i år smittet 600.000 Mac maskiner med en trojaner som viste ondsinnede annonser på de infiserte maskinene. Her var intensjonen til bakmennene å tjene penger på alle som klikke på dem (paid per click).

Den form for trojanere folk flest kommer borti er trojanere som scanner adressebøkene og innboksen din etter mailadresseret som sendes tilbake til hackeren som kontrollerer botnettet du er en del av. Deretter bruker de maskinen din til å sende ut sine spammeldinger fra din maskin og via din Internett leverandør sine Internett linjer, helt gratis og uten fare for å bli oppdaget. Alt peker tilbake til deg og ikke dem.

En trend i år har vært å bygge opp et botnet ved hjelp av trojanere som kan benyttes i forbindelse med et «DDoS angrep» eller et «Brute-Force»-angrep mot en server. Bare i år har vi skrevet om «Historiens største hackerangrep på Internett», «WordPress og Joomla utsatt for brute-force angrep», «OnNet sin serverpark er angrepet av et stort «brute force» angrep. Dessverre er det heller ingenting som tyder på at denne trenden vil stoppe.

Som regel åpner en trojaner også en «**bakdør**» på datamaskinen, slik at den som laget trojaneren i teorien kan ta kontroll over datamaskinen og komme tilbake til den igjen selv om du skulle avdekke trojaneren og klare å fjerne den. Har du først fått en trojaner på

maskinen din, er det ikke sikkert at du klarer å bli kvitt den uten å foreta en formatering av harddisken og sette maskinen opp på nytt igjen.

Trojanere sprer seg vanligvis ikke selv, de spres av virus, ormer eller programmer som lastes ned etter at trojaneren har blitt installert og aktivisert på din datamaskin, nettbrett eller mobiltelefon. Deretter spres koden seg og legge seg inn som en del av koden til operativsystemet ditt, slik at hackerne som har laget trojaneren kan skaffe seg tilgang til din maskin, nettbrett eller mobilen din hver gang den er online, uten at du selv merker det.

Trojanerne blir stadig mer avanserte for å gjøre det vanskelig å oppdage dem og de blir i stand til gjøre stadig mer avanserte ting. Foruten at de legger seg inn i registry filen for Windows, scanner de etter installert anti-virus programmer og andre programmer som er installert for å avdekke spyware. Disse blir så deaktivisert av trojaneren, samtidig som de gjør det umulig for deg å oppdatere disse programmene. Alt for å unngå at du skal klare å finne og fjerne trojaneren på din maskin.

2.5 DDoS angrep

I den senere tid har vi hørt om begrepet DDoS angrep på banker, mediehus, datasentre og andre viktige samfunnsmål, men hva er egentlig et DDoS angrep. I denne artikkelen ser jeg litt nærmere på akkurat dette.

2.5.1 Definisjon

La oss starte med å definere de to viktigste begrepene her:

- **Distribuert angrep** (*Denial-of-Service) er det samme som et **DoS angrep.***
- **Distribuert tjenestenekt** (*Distributed Denial-of-Service) er det samme som*

  *et **DDoS angrep***).

  Begrepene brukes innen Informasjons- og IT-sikkerhet til å beskrive et angrep hvor noen prøver å hindre andre å få tilgang til en tjeneste, ressurs eller lignende. Dette gjøres normalt ved å sende uendelig mange pakker til en og samme server/IP-adresse gjennom et **botnet** med det mål å overbelaste servernes kapasitet, slik at serveren og dens tjenester blir **utilgjengelige for brukerne**.

  Med **botnet** menes en gruppe av datamaskiner (også kalt "**zombies**") som er blitt smittet av malware for å utføre ulike oppgaver for eieren av botnettet. Botnettet kontrolleres gjennom å sende instruksjoner til nettets zombies fra en eller flere **Command & Control (C&C) servere**.

  Et vellykket DDoS angrep fører til at tjenesten, f.eks. en server, datasenter, switch/router e.l. **blir utilgjengelig** for dem som skal ha tak i dem.

Tjenestenektangrep har vokst til å bli et problem på Internett, særlig distribuerte varianter (*Distributed DoS, DDoS*), hvor flere «slave»-maskiner brukes til å angripe en eller flere maskiner via nettverket. Alle disse maskinene samlet vil ha større båndbredde enn offeret, noe som utnyttes til å sende så mye data til offeret at legitim trafikk ikke vil komme igjennom.

Et tjenestenektangrep må ikke nødvendigvis utføres via et nettverk. Det er mulig å lage programmer som ikke gjør annet enn å kopiere seg selv. Etter kort tid vil prosessoren bli overarbeidet og systemet vil stoppe. Dette er i såfall et DoS angrep og ikke et DDoS angrep.

2.5.2 Slik ser et DDoS angrep ut

Ludovic Fauvet fra VideoLAN har via visualiseringsverktøyet Logstalgia laget en grafisk framstilling av forespørsler mellom besøkende PC-er og en gitt server.

Det endelige resultat ser ut som det klassiske arkadespillet Pong – bare i en litt mer overdådig variant.

Mens vanlige logger viser en jevn flyt av forespørsler, er DDoS-angrep nokså annerledes. Her er «besøket» så målrettet og intenst at det nesten ser ut som mottakeren tar fyr.

2.5.3 Metoder for angrep

Det finnes tre hovedmetoder for å utføre et tjenestenektangrep:

- **Volum Bassert Angrep** – inkluderer UDP floods, ICMP floods, og andre spoofed-pakkestrømmer. Målet er å bruke så store ressurser at systemet går ned, Vi tenker da på ressurer som båndbredde, minne, harddiskplass eller prosessortid til en server (offer). Slike angrep måles i bits per sekund (Bps).
- **Protocol Angrep** – inkluderer SYN floods, fragmented pakke agrep, Ping of Death, Smurf DDoS og ligende teknikker. Slike typer angrep angriper en servers ressurser, en brannmur eller ligende.
- **Application Layer Angrep** – inkluderer Slowloris, Zero-day DDoS angrep, DDoS angrep som angriper Apache, Windows eller OpenBSD sårbarheter. Målet med slike angrep er å krasje hele seerveren og slike angrep målet i forespørsler per sekund.

2.5.4 Typer DDoS Angrep

Some specific and particularly popular and dangerous types of DDoS attacks include:

- **UDP Flood** – utnytter User Datagram Protocol (UDP), en session løs nettverksprotokoll. Denne typen angrep gjennomføres ved å sende en flom av UDP pakker til tilfeldige porter på en ekstern vert. Gjør at vert maskinen gjentatte ganger vil sjekke og lytte til denne porten, og (når ingen programmer er funnet) svar med en ICMP Destination Unreachable pakke. Denne prosessen safter vertsressurser, og kan til slutt føre til utilgjengelighet.
- **ICMP (ping) Flood** – tilsvarer i prinsippet et UDP flom angrep, men her overvelder man vert serveren med flom av ICMP Echo Request (ping) pakker. Pakker som krever at vert serveren sender et svar tilbake til dem. Når antall forespørsler med slike pakker

mot en av serverens porter, blir til slutt belastningen så stor at det går ut over ytelsen eller krasjer hele serveren. Dette er **den vanligste formen for DDoS angrep**.

- **SYN Flood** – En SYN flom DDoS angrep utnytter en kjent svakhet i TCP forbindelsen («tre-veis håndtrykk»), hvor en SYN forespørsel kommer for å starte en TCP forbindelse med en vert, som må besvare med en SYN-ACK respons, før det avsluttes med en ACK svar fra anmoderen. I et SYN flom angrep sender anmoder flere SYN forespørsler, men når verten svarer med en SYN-ACK svar for de ikke svar eller svaret blir sendt til en falsk IP-adresse. Uansett, fortsetter vertssystemet for å vente på bekreftelse for hver av forespørslene, bindende ressurser inntil ingen nye forbindelser kan utføres, og som til slutt resulterer i sperring av tjeneste.
- **Ping of Death** – en ping of death («POD») angrep innebærer at angriperen sende flere misdannede eller skadelig ping til en datamaskin. Den maksimale pakkelengde på en IP-pakke (inkludert header) er 65 535 byte. Imidlertid stiller Data Link Layer vanligvis grenser for maksimal rammestørrelse – for eksempel 1500 bytes over et Ethernet-nettverk. I dette tilfellet er en stor IP-pakke splittet på tvers av flere IP-pakker (kjent som fragmenter), og at mottakeren vert reassembles IP-fragmenter inn i den komplette pakke. I en Ping of Death scenario, etter ondsinnet manipulering av fragment innhold, ender mottakeren opp med en IP- pakke som er større enn 65 535 byte når settes sammen. Dette kan overløp minnebuffere avsatt til pakken, forårsaker denial of service for legitime pakker.
- **Slowloris** – spesielt farlig for verter som kjører Apache, dhttpd, Tomcat og GoAhead WebServer. Slowloris er et svært målrettede angrep, med det mål å ta ned en eller annen server, uten å påvirke andre andre tjenester eller porter på målet nettverket. Slowloris gjør dette ved å holde så mange forbindelser til målet webserver åpen så lenge som mulig. Det oppnår dette ved å skape forbindelser til målet server, men sender bare en delvis forespørsel. Slowloris sender stadig flere HTTP-hoder, men aldri fullfører en forespørsel. Den målrettede serveren holder hver av disse falske tilkoblinger åpne. Dette flyter til slutt den maksimale samtidige forbindelsen bassenget, og fører til fornektelse av ekstra tilkoblinger fra legitime kunder.
- **Zero-day DDoS – «Zero-day**» er rett og slett ukjent eller nye angrep, som utnytter sårbarheter som ingen patch ennå fanger opp. Begrepet er velkjent i hacker samfunnet, og handel med Zero-day sårbarheter som kan brukes i angrep har blitt en populær aktivitet.

DDoS-angrep er raskt blitt den mest utbredte typer angrep. Disse formene for angrep har vokst raskt de siste årene, både i antall og volum, ifølge en fersk markedsundersøkelse. Trenden går mot kortere angrep, men med større pakke-per-sekund (volum angrep). I løpet av Q4-2011, fant en undersøkelse 45% flere DDoS angrep i forhold til den parallelle periode i 2010, og over dobbelt så mange angrep observert under Q3-2011.

I gjennomsnitt benyttet hvert av angrepene som ble målt en båndbredde på 5,2 g bps, som er 148% høyere enn forrige kvartal.

Et ping-angrep er basert på å sende et stort antall ping-pakker til et mål. Har angriperen større båndbredde enn målet vil målet etter hvert ikke greie å ta imot flere pakker. Båndbredden blir sprengt.

Et nuke-angrep sender en pakke, som oftest ICMP, som er fragmentert. Pakken utnytter en programvarefeil i operativsystemet og maskinen vil krasje. Dette er også kjent som «Dødens ping».

2.5.5 Hvordan kan du beskytte deg mot DDoS angrep?

For å unngå «Denial of Service-angrep» bruker man normalt en metodetriangulering. En kombinasjon av angrep gjenkjenning, trafikk klassifisering og respons verktøy, med formål å blokkere trafikk som de identifiserer som illegitim og tillate trafikk at de identifiserer seg som legitime. En liste over forebygging og respons verktøy er gitt nedenfor:

2.5.6 Brannmurer

Brannmurer kan settes opp til å ha enkle regler slik å tillate eller nekte protokoller, porter eller IP-adresser. I tilfelle av et enkelt angrep fra et lite antall uvanlige IP-adresser for eksempel, kan man sette opp en enkel regel for å slippe all innkommende trafikk fra disse hackere.

Mer komplekse angrep vil imidlertid være vanskelig å blokkere med enkle regler: for eksempel hvis det er et pågående angrep på port 80 (web service), er det ikke mulig å slippe all innkommende trafikk på denne porten fordi dette vil hindre at serveren fra serverer legitim trafikk. I tillegg kan brannmurer være for dypt i nettverkshierarkiet. Rutere kan bli påvirket før trafikken kommer til brannmuren. Likevel kan brannmurer effektivt hindre brukere fra å lansere enkle flom type angrep fra maskiner bak brannmuren.

Noen tilstandsløse brannmurer, som OpenBSD PF pakkefilteret, kan fungere som en proxy for tilkoblinger: håndtrykk er validert (med klienten) i stedet for bare å videresende pakken til bestemmelsesstedet. Den er tilgjengelig for andre BSDene også. I den sammenheng er det som kalles «synproxy».

2.5.7 Switches

De fleste switches har noen hastighetsbegrensende og ACL evne. Noen svitsjer gir automatisk og/eller system-wide hastighetsbegrensende, traffic shaping, forsinket binding (TCP spleising), deep packet inspection og Bogon filtrering (falske IP-filtrering) for å oppdage og avhjelpe denial of service angrep gjennom automatisk sats filtrering og WAN Link failover og balansering.

Disse ordningene vil fungere så lenge DoS angrep er noe som kan forebygges ved å bruke dem. For eksempel SYN flom kan forebygges ved hjelp av forsinket binding eller TCP spleising. Tilsvarende innhold basert DoS kan forebygges ved hjelp av Deep Packet Inspection. Angrep stammer fra mørke adresser eller gå til mørke adresser kan forebygges ved hjelp av Bogon filtrering. Automatiske rente filtrering kan fungere så lenge du har satt rente-terskler riktig og granularly. Wan-link failover vil fungere så lenge begge linkene har DoS/DDoS forebygging mekanismen.

2.5.8 Rutere

I likhet med svitsjer, har ruterne noen hastighetsbegrensende og ACL evner som må settes opp manuelt på routeren. De fleste rutere kan i dag lett bli overbelastet under et DDoS angrep. Cisco IOS har funksjoner som hindrer flom i sine brannmurer som plasseres før serverparken.

2.5.9 Applikasjonsserver for bredebåndstyring foran server parken

En applikasjonserver menes en «boks» med innebygd hardware og software som er plassert på nettverket før trafikken når serverne. De brukes på nettverk i forbindelse med rutere og svitsjer. Boksen analyserer alle datapakker som kommer utenfra, identifiserer innholdet i dem og prioriterer dem etter farlighetsgrad før pakkene leveres videre til serveren. Boksen kan strupe båndbredden til enkelte IP-adresser/klasser, enkelt domener o.l. slik at de ikke får anledning til å spise opp all kapasiteten på nettverket.

2.5.10 IPS forebygging

Inntrenging forebygging systemer (IPS) er effektive hvis angrepene har signaturer forbundet med dem. Imidlertid går trenden mot å sende DDoS angrep med et lovelig innhold, men de har dårlige hensikter, og da er jo hele systemet verdiløst.

Husk også at inntrenging-forebygging systemer som fungerer godt på innholdsanalyser ikke kan blokkere atferd-baserte DoS-angrep. En **ASIC baserte IPS** kan oppdage og blokkere denial of service angrep bedre fordi de har tilgang til informasjon om bruk av prosessorkraft, båndbredde og minnne i sine analyser av angrepene og fungerer som en automatisk sikring av hele nettverket til serverparken.

En **rente-baserte IPS (RBIPS)** analyserer trafikken kontinuerlig og overvåker trafikken mønsteret for å finne ut om trafikken er normal eller ikke. Systemet lar den legitime trafikken passere, mens de blokkerer trafikk knyttet til DDoS angrep.

2.5.11 DDS baserte forsvar

Mer fokusert på problemet enn IPS, er et DoS Defense System (DDS). De er i stand til å blokkere innhold som stammer fra et DoS-angrep, samtidig som lovelig innhold slipper igjennom. En DDS kan også ta begge protokollen angrep (for eksempel Teardrop og Ping of death) og rente-baserte angrep (for eksempel ICMP flom og SYN flom).

Som IPS, kan et spesialbygd system, som for eksempel den velkjente Radware defensepro, oppdage og blokkere denial of service angrep på mye nærmere linjehastighet enn en programvarebasert system.

2.5.12 Blackholing og sinkholing

Med blackholing, blir all trafikk til angrepet DNS eller IP-adressen sendes til et «sort hull» (null grensesnitt eller en ikke-eksisterende server). For å være mer effektive og unngå å påvirke nettverkstilkobling, kan det bli styrt av ISP.

Sinkholing ruter trafikk til en gyldig IP-adresse som analyserer trafikken og avviser dårlige pakker. Sinkholing er ikke effektivt for de fleste alvorlige angrep.

2.5.13 Rene rør

All trafikk går gjennom en «rengjøring senter» eller et «skrubbing center» via ulike metoder som proxyer, tunneler eller til og med direkte kretser, som skiller «dårlig» trafikk (DDoS og også andre vanlige Internett-angrep) og bare sender god trafikk utover til serveren. Tilbyderen

må sentral tilkobling til Internett for å håndtere denne type tjeneste med mindre de måtte være plassert innenfor samme anlegget som «rengjøring senter» eller «skrubbing center». Prolexic, Tata Communications AT & T og Verisign er eksempler på tilbydere av denne tjenesten.

2.6 Bakdør

De fleste virus, ormer og trojanere du vil få på din maskin, vil prøve å lage en bakdør på ditt system som de kan bruke sendere for å komme inn igjen hvis de skulle bli avslørt og fjernet.

En bakdør er en ubeskyttet og ukjent åpning inn i et datasystem, laget av hackere gjennom bruk av en orm eller trojaner. Dersom et virus får laget en slik bakdør kan hackeren senere når han ønsker det gå inn og ta kontrollen av din PC, nettbrett og mobiltelefon og bruke den til ødeleggende eller kriminelle aktiviteter.

Ofte er det svakheter i operativplattformen (f.eks. Windows) som gjør det mulig å lage slike bakdører. Et annet kjennetegn ved en bakdør er at den er laget slik at den kan bypasse systemets normale authentication prosedyrer.

En annen type bakdører er de åpen «bakdørebe». En «åpen bakdør» er en udokumentert måte å innhente tilgang til et program, nettjeneste eller it-system, og er skrevet av programmereren av koden til programmet. Dette kan være gjort bevisst for å kunne gå inn senere for å rette noe hvis alt annet skulle skjære seg, eller på grunn av manglende kunnskaper hos programmereren.

En måte å utnytte en slik bakdør på kan være å laste ned uønsket materiale, f.eks. barnepornografi, og lagre det på harddisken uten at brukeren vet om det. I England var det nylig en barnepornosak der tiltalte gikk fri fordi han påstod at bildene som var funnet på hans PC var plantet der av andre, og ingen kunne motbevise dette.

2.7 botnet, også kalt Zombies

De siste årene har ulovlige botnett blitt kommersielle. Den som ønsker å sende ut uønsket reklame i stor skala eller angripe en nettressurs kan leie et allerede eksisterende botnett på det svarte markedet, på time- eller døgnbasis. Bots er i dag blitt en av de mest sofistikerte og mest populære former for Internettkriminalitet.

2.7.1 Hva er en bot?

En «**bot**» er en type ondsinnet kode som lar angriperen ta kontrollen over en datamaskin. De er også kjent som «**webroboter**» og de inngår som regel i et nettverk av infiserte maskiner, også kalt «**botnett**«, som er skapt av infiserte maskinen fra hele verden.

Siden en botinfisert datamaskin er underkastet sin mester, er det mange mennesker som kaller slike maskiner for «**zombier**«. De kriminelle som kontrollerer disse kalles **bothyrder** eller **botmestere**.

Noen botnett kan bestå av noen hundre eller noen tusen datamaskiner, men andre har både ti- og hundretusen «zombier» til sin disposisjon. Mange av disse datamaskinene er infiserte uten

at eieren vet om det. Noen mulige symptomer? En bot kan få datamaskinen til å gå saktere, vise merkelige meldinger eller helt enkelt krasje.

2.7.2 Hvordan en bot fungerer?

Et **botnett** er et nettverk av datamaskiner som er blitt infisert av et datavirus eller trojanske hester. Disse maskinene kobler seg til en eller flere sentrale styrende noder der de får tildelt oppgaver. Oppgavene kan være å søke gjennom web-sider etter e-postadresser, sende ut uønsket søppelpost (spam) eller å utføre tjenestenektangrep mot utvalgte mål på internett. Et botnett kan bestå av tusentalls datamaskiner, ofte kalt **zombier**, spredd over hele verden og med eiere som ikke vet at maskinene er infiserte.

En botnet (også kjent som en zombie hær) er en rekke Internett-datamaskiner som, selv om deres eiere er klar over det, har blitt satt opp til å videresende sendinger (inkludert spam eller virus) til andre datamaskiner på Internett. Enhver slik datamaskin er referert til som en zombie – i praksis en datamaskin «robot» eller «bot» som serverer ønskene til noen mester spam eller virus opphavsmann. De fleste datamaskiner kompromittert på denne måten er hjemme-baserte. Ifølge en rapport fra russisk-baserte Kaspersky Labs, botnets – ikke spam, virus eller ormer – i dag utgjør den største trusselen til Internett. En rapport fra Symantec kom til en lignende konklusjon.

Datamaskiner som er rekuperert å tjenestegjøre i en zombie hær er ofte de som eiere ikke klarer å gi effektive brannmurer og andre sikringstiltak. Stadig flere hjemmebrukere har høy hastighet tilkoblinger for datamaskiner som kan være mangelfullt beskyttet. En zombie eller bot er ofte skapt gjennom en Internett-porten som har stått åpent og der en liten Trojaner kan stå for fremtidig aktivering. På et bestemt tidspunkt, kan zombiearmé «controller» slippe løs effektene av hæren ved å sende en enkel kommando, muligens fra en Internet Relay Channel (IRC) nettsted.

Datamaskinene som danner et botnet kan programmeres til å omdirigere sendingene til en bestemt datamaskin, for eksempel et webområde som kan være stengt av å måtte håndtere for mye trafikk – et distribuert denial-of-service (DDoS) angrep – eller, i av spam fordeling, til mange datamaskiner. Motivasjonen for en zombie master som skaper et DDoS angrep kan være å lamme en konkurrent. Motivasjonen for en zombie mester sende spam er i penger å hente. Begge er avhengige av ubeskyttede datamaskiner som kan gjøres om til zombier.

En botnet refererer til en type bot kjører på en IRC-nettverk som har blitt opprettet med en trojaner. Når en infisert datamaskin er på Internett kan boten starte opp en IRC-klient og koble til en IRC server. Den trojanske vil også ha blitt kodet til å gjøre bot delta i et bestemt praterom når den er tilkoblet. Flere bots kan deretter bli med i en kanaler og den personen som har gjort dem kan nå spam IRC chatterom, lansere et stort antall Denial of Service-angrep mot IRC-servere som forårsaker dem til å gå ned.

2.7.3 Hvilken skade kan et botnet gjøre?

Når en bot har overtatt en datamaskin kan den utføre mange automatiske oppgaver, inkludert følgende;

Sende

De sender
– spam
– virus
– spionprogrammer

Stjele

De stjeler personlig og privat informasjon og kommuniserer denne informasjonen til sin mester:

– kredittkortnummer – kontoutdrag
– annen sensitiv og personlig informasjon

DoS (Denial of Service)

Lanserer DoS-angrep mot spesielle mål. Kriminelle presser penger fra eiere av websider mot at eieren får tilbake kontrollen av siden.Ofte er målgruppen private datamaskinbrukere, helt enket som spenning for bothyrderen.

«Clickfraud»

Bedragere bruker bot til å skape webbasert reklamefakturering ved automatiske klikk på Internettannonser.

2.7.4 Hvordan brukes et botnet til kriminelle handlinger?

Under finner du en illustrasjon som prøver å vise hvordan et botnet oppstår og brukes til å sende utepost spam.

Slik virker et botnet som er opprettet for å sende ut spam:

1. Eieren av botnetet starter med å sende ut virus og ormer gjennom ulike kanaler – epost spam, Facebook gimmics, konkurranser på store nettsteder, gamle bakdører de har opprettet tidligere m.m. De infiserte maskinene bliessr så omkonfigurert av trojaneren slik at det ikke skal være lett for anti-virus programmer å oppdaget dem. Mange slår faktisk av hele anti-virus programmet eller i det minste fjerner muligheten til å oppdater anti-virusprogrammet. Normalt gjør de også prosessene som kjører i bakgrunnen usynlige i alle overvåkningsverktøy, f.eks. Task Manager i Windows.
2. *Den infiserte maskinen logger seg inn på en* C&C server og er nå klar til å motta kommandoer fra eieren av botnettet,
3. En spammer kjøper tilgang til botnettet fra en annen operatør for å sende ut spam via botnettet
4. Eieren av botnettet sender nå 2 filer til zombiene som står og venter på neste oppgave. Den første inneholder teksten og bildene i epostmeldingen som skal sendes ut. Den andre inneholder komma separert liste over alle epostadressene som meldingen skal sendes til. Så snart filene er lastet opp til zombien starter den å

sende ut disse epostmeldingene i bakgrunnen uten at eieren av maskinen merker noe som helst. Zoombiene bruker de standard innstillingene som finnes på ditt skrivebord til å sende ut disse spam meldingene via din SMTP-tjeneste.

2.7.5 Types of attacks

- Botnet brukes alltid i et **DDoS angrep**, Jo større båndbreddekraft dette botnettet har, jo flere C-klasser det er delt på og jo nærmere offeret de er, jo større gjennomslagskraft har de. Et kraftig botnet kan stoppe alle typer tjenester på en server, f.eks. webserveren, databaseserveren,inngående og utgående epost, innlogging til tjenester, telefonlinjer, datalinjer o.l.
- Botnet brukes også ofte til å spre Adware reklame gjennom å erstadvertises a commercial offering actively and without the user's permission or awareness, for example by replacing banner ads on web pages atte bannere og ads på alle nettsteder du besøker.
- Botnet brukes også ofte til spredning av Spyware som skal samle inn sensitiv informasjon om deg. F.eks. personnummer, fødselsnummer, adresse, postnr og sted, land, bankkonto nummer, pinkode, utløpsdato, sikkerhetskode, brukernavn og passord til ulike tjenester o.l. informasjon.
- Botnet brukes i stor utstrekning til utsendelse av **SPAM**, slik som beskrevet over.
- Klikk svindel vil si at et botnet brukes til å besøke ulike nettsteder uten at eieren er

  klar over det. Alt skjer i bakgrunnen for å generere falsk trafikk til et nettsted for

  økonomisk vinning gjennom annonseinntekter e.l.

- Fast flux er en DNS teknikk som botnet bruker for å skule phishing og malware

  leveranser bak en falsk front til en annen nettside.

- Brute-force angrep på tjenester som f.eks. FTP, SMTP and SSH.
- Ormer. Rekruttering av flere zombier til botnettet.
- ScarmeWare er skremselsforsøk hvor maskinen blir kapret og blir utsatt for

  utpressing av ulik slag.

2.8 Brute Force

«**Brute-force**» angrep er en samlebetegnelse for angrep mot et nettsted eller server gjennom å tippe brukernavnet og passordet til innloggingen til nettstedets eller serverens kontrollpanel, ftp-konto eller begge deler. Fortrinnsvis er de ute etter å finne brukernavnet og passordet til en bruker som har administrator rettigheter.

Så snart de lykkes å tippe riktig brukernavn og passord har de full tilgang til nettstedets eller serverens ressurser. Av denne grunn er det ekstremt viktig at du benytter et komplekst passord som det ikke er lett å tippe. IKTnytt.no anbefaler at du følger disse passordreglene.

Den enkleste form for brute-force angrep er angrep fra en datamaskin som systematisk prøver å tippe brukernavnet og passordet. De starter med de vanligste administrator brukernavnene – root, admin og administrator og starter et script som starter med a, før de fortsetter A, ab, Ab,

abc osv. Slik fortsetter de helt til de har klart å tippe korrekt passord gjennom å forsøke alle tenkelige kombinasjoner.

Hvor lang tid det tar å tippe ditt brukernavn og passord er avhengig av hvor kompleks ditt passord er. Jeg anbefaler at du bruker et passord på minimum 8 tegn, hvor du kombinerer store og små bokstaver, med tall og minst ett spesialtegn, f.eks. @,+,* eller ? Dette gjør det svært vanskelig å tippe ditt passord.

De fleste host- og webmastere har satt på en «brute force» beskyttelse på sin innloggingside, slik at alle som tipper feil brukernavn og/eller passord blir blokkert for nye påloggingsforsøk for en periode når de f.eks. har nådd 5 mislykkede påloggingsforsøk.

Et brute-force-angrep fra kun en maskin er dermed ikke så farlig, så lenge du har et kompleks passord. De blir blokkert ute etter 5 mislykkede påloggingsforøk og må kanskje vente 15 minutter til 6 timer før de kan prøve å logge på igjen.

Langt farligere blir det når serveren eller nettstedet blir angrepet av et stort botnet med flere hundre tusen maskiner som angriper serveren eller nettstedet samtidig og begynner å tippe passord. Når den første blir blokkert fortsetter bare neste maskin, og når alle maskinene er blokkert, kan de som ble blokkert først fortsette å forsøke å logge inn siden deres karantene nå har løpt ut. På denne måten kan de knekke de mest avanserte passord i løpet av få timer.

3 De vanligste sikkerhetshullene

Etter å ha jobbet med sikkerhet i 25 år og lest hundrevis av studier om datasikkerhet kan de vanligste sikkerhetshullene i privatpersoners og småbedrifters datasikkerhet oppsummeres i følgende sikkerhetshull.

3.1 Dårlig passord

Dårlig passord er den vanligste årsaken til at du blir utsatt for et datainnbrudd. Med dårlig passord menes et passord på under 8 tegn og/eller som er lett å tippe, f.eks. et ord i en ordliste. Gå ikke i denne generalfellen. Bruk alltid et komplekst passord og følg passordreglene vi gir i en egen artikkel senere i denne artikkelserien.

3.2 Ikke oppdatert utstyr og programvare

Etter dårlige passord er utstyr og programvare som ikke er oppdatert det største sikkerhetshullet i folks datasikkerhet. Sørg derfor at alt utstyr og alle programmer du benytter er oppdatert med siste versjon fra produsenten. Lag gode rutiner for å sørge for at dette blir gjort jevnlig, f.eks. ukentlig.

3.3 Manglende virusprogram

1 av 4 datamaskiner mangler fortsatt et virusprogram eller har et utgått virusprogram. Dette blir omtrent som å gå på jobben uten å låse ytterdøra. Installer først som sist et virusprogram på alle maskiner og sørg for at de er oppdatert med de siste filene. Disse filene oppdateres normalt 1 gang i timen.

3.4 Manglende brannmur

Å ikke ha en personlig brannmur og en nettverksbrannmur på LAN nettverket er nesten like ille som å ikke ha et aktivt antivirus program, da hvem som helst kan gå til alle ressurser og områder som ikke er passordbeskyttet. Begrens folks tilgang til ditt utstyr og nettverk gjennom å sette opp en brannmur. Noe vi vil gå igjennom i en egen artikkel.

3.5 Åpen linje/kommunikasjon

Send aldri sensitive informasjon, f.eks. brukernavn, passord, kortinformasjon, fødelsdato, telefonnummer, adresse o.l. på en åpen linje. Sørg for at all slik kommunikasjon skjer på en kryptert linje som bruker et godkjent SSL-sertifikat. Gjør du ikke dette kan hvem som helst sette opp en lyttepost og ta en kopi av all informasjonen som sendes frem og tilbake på linjen.

3.6 Manglende sunn fornuft

Ser vi bort i fra disse forholdene kan den største svakheten i folks datasikkerhet oppsummeres i tre ord: - **Manglende sunn fornuft**.

3.7 Passordregler

8 av 10 passord kan knekkes i løpet av kort tid. Det er derfor essensielt viktig at du har et sikkert passord som ikke kan knekkes enkelt. Her lærer du hvordan du lager et «*idiotsikkert*» passord.

I et eksperiment utført av teknologinettstedet Ars Technica hacket en av verdens fremste passordknekkere 82 prosent av 16.000 passord i løpet av én time.

Konsekvensene av elendige rutiner hører vi om daglig. Et eksempel er er en melding som ble sendt ut fra nyhetsbyrået AP sin twitterkonto ble om at president Barack Obama var såret etter to eksplosjoner i Det hvite hus. Kontoen var hacket som følge av dårlige passordrutiner, og den oppsiktsvekkende meldingen senket børsene med 800 milliarder kroner.

Norsis og Høgskolen i Gjøvik gjennomførte i desember 2012 en passordundersøkelse i Norge. Der fant de ut følgende om nordmenns bruk av passord:

– Gjennomsnittlig antall private passord: 17
– Gjennomsnittlig antall jobbpassord: 8
– Snittlengde på passord: 8 tegn
– 31 % deler passord med sin partner/ektefelle
– På spørsmål om hva som er et godt passord, svarer de fleste «en blanding av tegn

og bokstaver»

Nå som du vet dette, kan vi gå videre og se på de passordene hackerne først prøver seg med, og som du av den grunn må holde deg unna.

3.7.1 Dette er passordene hackere prøver seg med

I forbindelse med en analyse av hvordan Internet-ormen «*Morto*» smitter andre datamaskiner, har Sikkerhetsselskapet F-Secure avdekket av hackerne benytter seg en liste på 30 vanlige passord for å bryte seg inn på andre systemer. Listen med disse 30 passordene ga dem tilgang til over 50.000 datamaskiner.

Vi må derfor igjen advare våre lesere mot å bruke «*svake*» passord som er enkle å gjette seg til. Styr også unna passord som dannes gjennom et naturlig tastemønster på tastaturet – og da spesielt keypaden.

Passord listen Morto brukte er følgende passord:

- admin
- password
- server
- test
- user
- pass
- letmein
- 1234qwer
- 1q2w3e
- 1qaz2wsx
- aaa
- abc123
- abcd1234
- admin123
- 111
- 123
- 369
- 1111
- 12345
- 111111
- 123123
- 123321
- 123456
- 654321
- 666666
- 888888
- 1234567
- 12345678
- 123456789
- 1234567890

En undersøkelse fra 2007 gjennomført av inTechnology viser at mange av de samme ordene går igjen på begge listene.

1. password
2. 123456
3. qwerty
4. abc123
5. letmein
6. monkey
7. myspace1
8. password1
9. link182
10. [ditt fornavn]

Nå som du vet alt dette, kan vi gå videre og se på hvordan du bør gå frem for å velge et trygt passord.

3.7.2 Hvordan velge gode passord?

Styr unna passord som er enkle å tippe og passord som er en naturlig tastekombinasjon på keybordet, men selv dette er ikke nok. Det finnes 1000-vis av små programmer ute på nettet som «*bruker ren makt*«, også kalt «brute force», for å finne ut passordet ditt. Disse programmene begynner ofte å gjette seg frem til passord med å prøve seg på alle mulige ord i ordboka. Finnes ordet i en ordbok, så kan et passord være knekt på bare noen tideler av et sekund.

Er passordet ditt litt mer komplisert, fortsetter gjerne programmene med å gjette seg frem med alle tenkelige bokstavkombinasjoner.

Knekkes i løpet av en sang...

Hvis du bruker et passord på fem bokstaver med bare små bokstaver, så er drøyt 20 millioner kombinasjonsmuligheter.

Det høres kanskje betryggende ut, men en moderne datamaskin kan teste utrolig mange kombinasjoner per sekund. Antar vi at et program kan teste 100.000 kombinasjonsmuligheter i sekundet, noe som ikke vil være noe problem, er passordet knekt på litt over tre minutter. Passordet ditt er altså tilgjengelig for kriminelle før de har hørt ferdig Britney Spears' «*I'm a slave 4 you*»...

3.7.3 Benytt minst åtte bokstaver i ditt passord

Det er derfor viktig å bruke passord på minimum åtte bokstaver, og passordet bør fortrinnsvis inneholde både store og små bokstaver, i tillegg til tall og spesialtegn.

Årsaken er ganske enkel: La oss si at du har et ord på åtte bokstaver. I tabellene under viser vi hvor mange kombinasjonsmuligheter du har med bare små bokstaver, små og store bokstaver, små og store bokstaver samt tall – og antall muligheter med alle tenkelige spesialtegn.

Tegn inkludert	Tegn i passordet	Kombinasjons-muligheter
Små bokstaver (antatt 29)	**5**	**20,5 millioner**
Små bokstaver (antatt 29)	**8**	**500 millioner**
Små og store bokstaver (58)	**8**	**128 bilioner**
Små, store og tall (68)	**8**	**457 bilioner**
Små, store, tall og spesialtegn *(antatt 96 – antall spesialtegn tilgjengelig kan varierer betydelig)*	**8**	**7200 billioner**

Som en raskt kan se ut ifra denne tabellen, så øker antallet potensielle kombinasjonsmuligheter enormt hvis du legger inn spesialtegn.

3.7.4 Benytt både små og store bokstaver

Problemet med både store bokstaver, tall og spesialtegn er derimot at det ofte ikke er så enkelt å huske. Det er enklere å huske «*pusekatt*» enn «*4j#fK0Iu*» selv om det er like mange tegn.

3.7.5 Lag en enkel huskeregel

Skaff deg et vanskelig passord som du likevel er lett å huske gjennom en enkel huskeregel. Du kan f.eks. ta et sitat eller setning fra din favoritt sang, og plukke ut den første bokstaven i hvert ord som ditt passord.

La oss for eksempel si at du er kristen. Da vil følgende setning være enkel: «*For så høyt har Gud elsket verden, at han ga sin Sønn*»

I et passord vil det kunne se slik ut: «*FshhGev,ahgsS*»

Der har du skapt et passord på 14 tegn som er utrolig vanskelig å gjette seg til, men enkelt å huske, som både har store og små bokstaver, i tillegg til et spesialtegn. Tall kan du enkelt legge inn hvis setningen du benytter seg også benytter seg av et eller annet tall.

3.7.6 Bytt ut bokstaver med tall

En annen mulighet er å ta et naturlig ord som er enkelt og huske, for så bytte ut alle bokstaver som ligner på tall med dette tallet. La oss si at du i dag bruker passordet: «*HEMSEDAL*«. Dette passordet kan omskrives til følgende passord:

Vi har her bare byttet ut bokstaven E med tallet 3, mens bokstaven L har blitt erstattet med tallet 1. Ved så å starte passordet med STOR bokstav, og deretter skrive alle de andre med bare små bokstaver, har vi nå fått et passord som er vanskelig å knekke, men lett å huske.

3.7.7 Ikke bruk ord som finnes i en ordbok eller på et språk.

Siden hackerne benytter seg av tilgjengelige ordbøker på ulike språk i sine «brute force» angrep, bør du holde deg unna vanlige ord som finnes i en ordbok – uansett språk.

3.7.8 Ikke bruk passord basert på personlig informasjon

Foruten alle tilgjengelige ordbøker, samler hackere ofte inn bakgrunnsinformasjon om objektet de skal angripe. Jo mer de ønsker å bryte seg inn, jo mer tid bruker de på å samle inn nødvendig bagrunnsinformasjon om deg og objektet de skal bryte seg inn i. Hackere samler inn alt fra tilgjengelig informasjon fra Facebook og andre sosislae medier, dine nettsider, offentlig informasjon om deg og objektet som skal hackes (f.eks. adresse, postnummer, telefonnummer m.m.).

Benytt derfor ikke slik informasjon som utgangspunkt for ditt passord.

3.7.9 Velg et vanlig ord + årstall + første stavelse av tjenesten

Nettstedet CorvusConsulting har en litt annen holdning til hvordan du potensielt kan skape et unikt passord til hvert eneste sted du registrerer deg:

Velg først ut et helt normalt ord, fortrinnsvis ikke på engelsk. Fortsette så med et årstall som har stor betydning for deg, men ikke din bursdag, og avslutt med den første stavelsen av tjenesten du skal registerer deg.

For eksempel kan det da være «*brostein1994goo*». Dette er altså et normalt ord, årstallet for OL på Lillehammer, og den første stavelsen av Google.

Et lignende passord kan være «*brostein1994wi*» på Wikipedia. **3.7.10 Lag naturlige spesialtegn**

Vil du gjøre det enda sikrere kan du for eksempel velge å markere starten av hver stavelse med stor bokstav, og andre halvdelen av årstallet med spesialtegnet som tilsvarer symbolet på tastaturet.

Det første passordet ditt vil da se slik ut: «*BroStein19)¤Goo*»

Her har du et passord på 15 tegn som er veldig enkelt å huske, men som samtidig være uoverkommelig å knekke med de fleste datamaskiner. Regner vi med at du har tilgang til 96 forskjellige tegn med bokstaver, tall og spesialtegn, så er det snakk om over *540.000 billioner billioner* kombinasjonsmuligheter (96^15).

Dette passordet gjør at hvis du mister passordet ditt for én tjeneste, så vil du fortsatt ha hemmeligheten din intakt for andre nettsteder. Ulempen er at det er enkelt å avsløre hvis noen først finner frem til mønsteret ditt. Det er likevel betydelig sikrere enn alle standardpassord som folk flest gjerne benytter seg av.

3.7.11 Ikke bruk det samme passordet overalt

– *Gjenbruk av passord bør man unngå. Det er greit på tjenester man ikke bruker så ofte, men hyppig brukte nettjenester bør ha et unikt passord*, sier sikkerhetsekspert Per Thorsheim til DN.no.

– *Noen passord bruker man sjelden. Da er det faktisk bedre å skrive ned passordene sine på et papir, fremfor å bruke det samme passordet på ulike tjenester*, sier Thorsheim.

Her får Thorsheim støtte av en av de fremste sikkerhetsguruene i verden, Bruce Schneier, som har utgitt et titalls bøker om kryptografi.

Schneier mener folk stort sett er flinke til å ta vare på det som har en verdi, for eksempel penger eller kredittkort i lommeboken, og at det derfor ikke er noe i veien for å oppbevare et papir med passord.

Det ideelle er å lage et unikt passord for hver nettjeneste. E-postkontoer er spesielt utsatt for målrettede angrep, så her bør du ha spesielt gode passord.

3.7.12 Bytt passord ved jevne mellomrom

Siden hackere samler inn bakgrunnsinformasjon om hva som skal hackes, og siden «brute force» er en vanlig innbruddsteknikk gjelder det å bytte passord ved jevne mellomrom slik at de ikke får tid til å teste alle mulige kombinasjoner før passordet byttes igjen. Spesielt viktig er det at du bytter passord hvis du har mistanke om at ditt passord kan ha kommet på avveie.

Hver samtidig klar over at hackere ofte setter opp «*lytteposter*» som prøver å snappe opp all informasjon inn og ut av en server. Kobler du deg opp på din mailkonto, ftp-konto eller FrontPage konto på en usikret sone, kan hackere meget enkelt snappe opp ditt brukernavn og passord. Deretter kommer de seg inn på dine kontoer og kan begynne å gjøre skade. Bytt av denne grunn dine passord ved jevne mellomrom.

3.7.13 Husk at folk er forutsigbare – det samme er du

Et stort problem er at folk har en tendens til å gjøre det enkelt for seg selv ved å bake inn navn eller lesbare ord i passordet, samt slenge på tall på slutten, noe som gjør det langt enklere for hackerne å knekke; for eksempel: «Hege1979».

– *Statistikken viser at folk vil bruke et ord eller navn i passordet sitt, første bokstav har stor bokstav, og gjerne noen tall eller årstall på slutten. På nettsider hvor det ikke stilles krav til kompleksitet, så skriver folk gjerne alt med små bokstaver og siffer på slutten*, sier sikkerhetsekspert Thorsheim.

Thorsheim har følgende råd til deg som trenger et godt passord som er enkelt å huske: La passordet være en setning som du at du klarer å huske.

Eksempel på et trygt passord som er enkelt å huske:

• ***«Barna mine er 4 og 7 år gamle. Barna mine heter Kjetil og Lisa»***
Lengden på passordet trumfer alt annet i dette tilfellet – med så mange tegn tar det lang tid

å knekke passordet.

3.7.14 Ikke benytt «husk passord funksjonen» som ofte tilbys

Mange programmer tilbyr deg å «huske» passordet ditt til neste gang du logger inn, men slike programmer har ulike nivåer av sikkerhet når det gjelder å beskytte passordet. Noen lagrer denne typen informasjon i klartekst i en fil på datamaskinen din. Det betyr at hvem som helst som har tilgang til din datamaskin kan finne passordene og bruke disse videre. Derfor må du aldri benytte «huske-funksjonen» når du bruker en offentlig tilgjengelig datamaskin, for eksempel på biblioteket, internettkafeer eller en som brukes av flere der du jobber. Dessuten, på slike maskiner som brukes av flere, må du alltid huske å logge ut, iallfall lukke alle nettleservinduene, da enkelte programmer «husker» passord selv om du ikke spesifikt har bedt om det.

3.7.15 Pass godt på ditt passord

Ikke fortell passordet til noen og ikke skriv det opp på en lapp som du legger på kontoret, pulten eller fester til skjermen.

3.7.16 Ingenting er helt sikkert

Hardbarkede sikkerhetsfantaster vil påpeke at ingen av disse løsningene er helt sikre. På mange nettsteder så lagres passordet ditt i klartekst slik at bakmennene kan gå inn i systemene sine og se passordet ditt. Dette gjelder blant annet alle tjenester som gir deg muligheten til å få tilsendt passordet ditt i klartekst på mail. Det kan derfor være veldig fornuftig å bruke forskjellige passord på forskjellige tjenester.

Den løsningen mange derfor bruker er å ha forskjellige nivåer av passord. På helt meningsløse tjenester kan en registrere seg med et helt generisk passord som det ikke betyr noe om noen får tak i. Og så kan du lage deg 3-4 nivåer oppover med viktigere passord som blir vanskeligere og vanskeligere.

For eksempel kan passordet ditt på en gratistjeneste du ikke bryr deg om, men må registrere deg for å få tilgang til, bare være «vissvass», mens Facebook og E-posten din bør ha mer infløkte passord som vi har vært inne på.

De mest hardbakrede vil likevel foretrekker å bruke lange og unike passord på dusinvis av tegn, men for folk flest er det å være litt velparanoid.

3.8 Surfe-regler på Internett

Det beste sikkerhetsrådet vi kan gi deg er dette:

Bruk sunn fornuft og følg noen enkle surfe-regler for å beskytte deg selv mot malware og uønskede hackerangrep.

La meg starte med noen kjøreregler for hva som er farlig, litt farlig og ufarlig å gjøre når du surfer rundt på nettet.

3.8.1 Dette er (som regel) ikke farlig

- Å gå til en webside, se på innholdet, klikke i menyer og navigere rundt
- Følge koblinger og linker på sosiale medier som fører deg til andre etablerte, kjente nettsteder eller medier
- Opprette brukerkontoer og personprofiler på nettsteder og sosiale medier
- Kjøpe varer og tjenester på nett med online betaling via sikre betalingskanaler
- Kommentere på blogger eller delta i kjente, etablerte diskusjonsfora

3.8.2 Dette KAN være risikabelt

- Å besøke "lugubre", lite kjente nettsteder med tvilsomt innhold
- Følge linker på nett eller sosiale medier som tilbyr noe som virker for godt til å være sant
- Klikke ukritisk på linker du får på mail og chat fra venner. Syns du linken virker snodig Spør!
- Fortsette å navigere rundt på en nettside som har et helt annet innhold enn den opprinnelige linken skulle tilsi
- Installere lite kjente / helt ukjente gratisprogrammer du finner på nett

3.8.3 Dette ER risikabelt

- Å surfe jevnlig på risikable webområder (f.eks pornografiske nettsider)
- Akseptere venneforespørsler fra totalt ukjente personer i sosiale medier uten å gjøre en liten research på dem først
- Svare på mail eller chat-meldinger fra personer du absolutt ikke kjenner, spesielt hvis dere heller ikke har noe felles nettverk
- Ukritisk installere alle tillegg og gratisprogrammer du dumper over på internett
- Gi informasjon om dine brukernavn og passord via meldingsfunksjoner i sosiale medier
- Ukritisk gi forskjellige applikasjoner tilgang til dine personopplysninger på f.eks facebook
- Tillate nedlasting og "kjøring" eller installering av .exe-filer fra nettet, uten at du er sikker på hva slags program det er snakk om
- Lagre .zip-filer på din maskin uten å være sikker på hva disse filene inneholder

3.8.4 Grunnregler

Dernest gjelder det å følge disse grunnreglene for å unngå spyware, trojanere, virus og annen malware:

- **Ikke klikk på lenker inni pop-up-vinduer**. Fordi pop-up-vinduer ofte er relatert til spyware, kan det hende at et klikk på slike vinduer fører til at spyware installeres på datamaskinen din. For å lukke et slikt vindu må du ikke trykke på krysset øverst i høyre hjørne av selve vinduet eller klikke på ”Lukk”-knapp inni vinduet. Bruk ALT + F4 istedenfor.
- **Velg ”Nei” når du får uventede spørsmål om et eller annet**. Vær varsom med uventede dialogbokser som spør om du ønsker å kjøre et gitt program eller gjøre noe annet du ikke selv har valgt å gjøre. Velg alltid ”Nei” eller ”Cancel”, eller lukk dialogboksen ved å trykke på krysset øverst i høyre hjørne av selve vinduet. Aller helst bør du velge ALT + F4.
- **Vær varsom med gratis nedlastbar programvare**. Det er mange nettsteder som tilbyr tilpassede verktøylinjer eller andre finesser som virker fristende på brukerne. Ikke last ned programmer som du ikke stoler på, og vær klar over at det kan hende at du utsetter datamaskinen din for spyware dersom du laster de ned (gratis programvare er i dag en av de vanligste måtene å spre spyware på).
- **Ikke følg lenker i e-post som later til å tilby programmer mot spyware**. Akkurat som e-postvirus, kan det hende at lenkene har en annen hensikt, nemlig å installere akkurat den typen spyware som de hevder å skulle beskytte mot.
- **Styr unna fildelingsprogrammer**. Ingenting er gratis her i livet. Programvare og filer som deles gjennom fildelingsprogrammer er som regel infisert av en aller annen form for maleware.
- **Ikke klikk på ukjente PDF-dokumenter**. Adobe advarer mot et sikkerhetshull i deres Acrobat Reader som hackere har utnyttet til å skaffe seg sensitiv informasjon på din maskin.

  Sett innstillingene i nettleseren din til å begrense pop-up-vinduer og informasjonskapsler (eng: cookies). Pop-up-vinduer er ofte generert av scripting eller aktivt innhold. Det å tilpasse innstillingene i nettleseren til å hindre dette, kan redusere antall pop-up-vinduer som dukker opp. Noen nettlesere tilbyr muligheten for å blokkere pop-up-vinduer. Enkelte typer informasjonskapsler kan sees på som spyware fordi de avslører informasjon om hvilke nettsider du har besøkt. Du kan tilpasse dine personlige innstillinger til bare å tillate informasjonskapsler for nettsider som du faktisk besøker.Deretter må du sørge for å holde dette anti-spyware programmet oppdatert. Gjør du ikke det, kan du heller ikke forvente at det beskytter deg mot disse typer angrep.

3.9 E-postregler for sikker epost

Her finner du en rekke praktiske råd og tips for å unngå spam eller bli utsatt for epost svindel

3.9.1 Bruk hue

Dette er kanskje det viktigste rådet jeg kan gi. La meg ta et eksempel:

– Rimer tittel og tema på en epost med vedkommende som sendte den?

Veldig ofte får man virus fordi venner har fått sin epostkonto hacket. Jeg sparte meg selv for «*I Love You-viruset*» fordi jeg fikk e-posten med viruset til sendt av min eks, og er det noe jeg vet veldig godt så er det at hun ikke elsker meg.

Bruk hue. Hver alltid forsiktig. Ta aldri noen sjanser når det gjelder sikkerheten. En liten glipp fra din side, er alt de venter på for å hacke deg.

Følg råd gjelder for epost:

- **Ikke åpn epostmeldinger fra ukjente** og hvis du gjør det, ikke svar på meldingen før du har sjekket alle punktene under.
- **Vær tvilsom til utenlandske e-postmeldinger**. Sjekk alltid avsenderes e-postadresse. Scandinaviske selskaper har domenenavn som slutter på .no, .se og .dk. Ingen bruker .ru, .it, .es og ligende endelser. Foreta et whois oppslag av domenenavnet til avsenderen for å finne ut hvem som eier domene og hvor eieren kommer fra.
- **Se etter om teksten kunne faktisk vært skrevet av en nordmann, og ikke en oversettingsmoto**r. Svindlerne er som regel utlendinger som oversetter teksten til norsk via Google oversettelsesservice e.l. Se etter gramatiske feil.
- **Aldri, aldri oppgi sensitiv informasjon som personnummer, passnummer, passord, kredittopplysninger osv**. Banker (eller andre offentlige bedrifter) vil aldri spørre deg etter slik informasjon, spesielt ikke gjennom epost.
- **Se etter typiske trekk i e-posten som kan peke mot at den er masseprodusert** (bilder, tekst, linker osv).
- **Foreta et Googlesøk etter avsenderens navn, domenenavn og e-postadresse**. Det kan hende du ikke finner noe interessant, men det kan redde deg fra å bli svindlet.
- **Krev forhåndsbetaling hvis du selger noe**. Ikke stol på penger som er satt på «vent» gjennom tjenester som f. eks Paypal (svindleren kan angre kjøpet, og få pengene sine tilbake — etter at du allerede har sendt varen)
- **Det skader ikke å ringe personen, istedenfor og ikke bare bruke epost som eneste kommunikasjonsmiddel**. Aldri inngå avtaler e.l. med mennesker som ikke oppgir sitt telefonnummer og adresse.
- **Er ting for godt til å være sant, er det som regel det.**
- **Vær kritisk**

3.10 Slik beskytter du deg mot spam

Selv om antall -postmeldinger som inneholdt **spam**, det vil si**uønsket s-post**, sank i fjor, er fortsatt **8 av 10 e-postmeldinger**som sendes på Internett spam.

Unsket e-post, ogsp kalt spam, er dermed fortsatt et stor problem for folk flest. Spørsmålet er derfor:

– Hva kan du selv gjøre for å beskytte det mot spam og e-postsvindel?

Det finnes mye du selv kan gjøre for å beskytte deg mot dette. Jeg har i denne artikkelen delt opp tiltakene i to grupper:

1. Tekniske tiltak mot spam
2. Brukerråd for å unngå spam

Følger du rådene vi gir på denne siden kan vi garantere at du ikke vil slite med masse SPAM i fremtiden.

3.10.1 Bruk flere e-postadresser !

Skaff deg først som sist minst to e-postadresser. En «SPAM-adresse» som du oppgir når du surfer rundt på Internett, deltar i diskusjonsforum og registrerer deg for å få tilgang til ulike tjenester, og en annen spam-fri adresse som du bruker i din kommunikasjon med kunder, forretningsforbindelser, venner, bekjente og andre som du ønsker skal ha e-postadressen din. Å tro du kan oppnå en spam-fri hverdag uten å gjøre dette, er dessverre utopi!

3.10.2 Hver kreativ i valg av e-postadresse

Mange spammere prøver å gjette seg frem til din e-postadresse. De sender derfor en mail til alle vanlige adresser, deriblant: post@domenenavn.com, postmaster@domenenavn.com, webmaster@domenenavn.com, info@domenenavn.com, firmapost@domenenavn.com, help@domenenavn.com, firma@domenenavn.com og support@domenenavn.com. Hver derfor kreativ i valg av e-postadresse, så slipper du mange spam mail.

De mest utsatte e-postadressene er de korte, dvs. de med mindre enn 6 bokstaver.

3.10.3 Bytt e-post adresse jevnlig

Bytter du din e-postadresse jevnlig får du heller ikke SPAM. Vanskeligere er det ikke. Imidlertid er dette dette noe de flest ikke ønsker å gjøre, da det er slitsomt å oppdatere alle sine kontakter med en ny e-post adresse og få dem til å huske den. Å bytte e-postadresse for ofte er derfor en dårlig løsning for de fleste.

3.10.4 Skru av auto-svar, feriemeldinger og sykemeldinger

Ikke bruk «feriemelding» eller andre former for «auto-responder». Det gjør bare at senderen får et svar fra deg, og dermed vet spammerne at adressen er gyldig Det gjør at de bare vil fortsette å sende deg flere meldinger. Styr unna dette.

3.10.5 Ikke legg din e-post adresse på egne nettsider i klartekst

Hackere og spammere skanner Internett og alle nettsidene de finner for e-postadresser. Adressene de finner legger de inn i en database som de senere bruker til å sende ut spam eller bruker som en del av sitt kyberangrep mot et kybermål. Legger du ut din e- postadresse på egne eller andres hjemmesider, blogger e.l. er du garantert å motta spam før eller senere i stadig større grad. Rådet er derfor:

– Ikke legg ut din e-postadresse i klartekst

Ønsker du å legge ut din e-postadresse på egne nettsider, i en blogg e.l. bør du ikke legge ut e-postadressen i klar test. Det vil si som vanlig bokstaver. Legg heller ut e-postadressen som et bilde eller krypter e-postadressen til et «ikke-leselig» format for søke-robotene. Dette hindrer at noen kan bruke et «harvest» program til å finne e-postadressen din ved å skannet nettet.

Det finnes flere måter å kryptere din e-postadresse til et uleselig format for harvest programmer. De to vanligste måtene er:

Skriv adressen på en kryptisk måte

Skriv for eksempel navn@online punktum no istedet for navn@online.no, eller på en annen måte unngå å skrive adressen korrekt.

Bruk ASCII-koder

Eksemplet navn@online.no ser slik ut med ASCII-koder (tegnene skal være på én linje uten mellomrom):

- navn@
- online
- Du finner en komplett liste over ASCII-koder på Windows.no.

3.10.6 Skru av HTML-visning

Det anbefales å vise e-post som ren tekst (plain text), og dermed deaktivere HTML- visning. Da unngår du å bli rammet av såkalte web bugs som sjekker om adressen er gyldig og at du faktisk har lest e-posten.

3.10.7 Skru av bilde- og forhåndsvisning

Ønsker du å beholde HTML-visning, bør du deaktivere visning av billedlenker. Skru også av forhåndsvisning av e-post, slik at du kan slette mistenkelige meldinger uten å åpne dem.

De fleste spam meldinger inneholder et usynelig bilde. Så snart e-posten blir åpnet, blir bildet automatisk lastet ned fra spammerens server og de får dermed en bekreftelse på at e-postadressen er aktiv. Derfor bør du skru av denne funksjonen. Last heller ned bildet manuelt etter at e-posten er åpnet og du ønsker å lese hele meldingen.

3.10.8 Bruk alltid en oppdatert versjon av din nettleser og e-postprogram

Hold operativsystemet, e-postprogrammet, nettleseren, virusprogrammet og brannmuren på din pc/mac alltid oppdatert med den siste versjonen. Unnlater du å lage gode rutiner for å holde disse programmene oppdaterte til enhver tid får du ikke bare mer spam, men du utsetter deg selv og dine systemer for en stor sikkerhetsrisiko.

3.10.9 Sørg for at du har et skikkelig spamfilter på både server og klientnivå

Et spamfilter sorterer bort uønskede meldinger og sparer deg dermed for masse spam. Ta kontakt med din e-postleverandør og hør om hvilke spamfilter de tilbyr på din e-postkonto og hvor du finner konfigurasjonsmulighetene til dette spamfilteret. Som regel gjøres dette som en del av kontrollpanelet (f.eks. cPanel) til webhotellet ditt. Tilbyr ikke leverandøren et av de mest kjente anti-spam filtrene bør du bytte leverandør.

Disse spamfiltrene på servernivå som sjekker innkommen e-post for spam før de kommer til din innboks, fjerner normalt rundt 60% av all spam som sendes. Ønsker du en høyere beskyttelse på servernivå, må du skaffe deg en brannmur som står foran mailserveren og som sjekker all innkommen e-post for spam, virus og malware før meldingen leveres til mailserveren du benytter. Her finnes det mange systemer å velge mellom, men de fleste koster noen tusen per år. OnNet sin Barracuda Spamfirewall er en rimelig løsning som stopper 99,9% av alle virus og malware som sendes via e-post og minimum 85% av all spam som sendes til kr. 19/mnd.

Laster du ned e-posten til et lokalt e-postprogram som du benytter til å lese e-posten med, f.eks. Outlook, bør du i tillegg installere et spamfilter på din datamaskin som sjekker all mail før den blir levert til innboksen på din maskin. Du får dermed en dobbel beskyttelse, og dette spamfilteret vil sikkert klare å fange opp noen av de meldingene spamfilteret på servernivå ikke klarte å stoppe.

Mange anti-virus programmer har denne funksjonen innebygd som en del av programvaren. Sjekk derfor først med ditt anti-virus program for å se hvilke muligheter som finnes der. Sjekk innstillingene og sørg for at det er aktivt.

Vær oppmerksom på at spamfiltre også kan sortere bort ønsket e-post til en egen mappe, gjerne kalt Søppelpost eller Uønsket e-post. Du bør derfor ha mulighet til å titte gjennom utsorterte meldinger, før de slettes for godt.

3.10.10 Sjekk hvilke RBL-filtre ditt spamfilter er satt opp mot

RBK filtre som lages av de store anti-spam organisasjonene på Internett og inneholder oversikt over alle kjente avsendere av spam. Disse RBL-filtrene benyttes av spamfiltre på både server- og klientnivå til å sjekke om meldingen er spam eller ikke. **Les mer om hva RBL-filtre er og hvilke filtre som kan anbefales**.

3.10.11 Opprett en SPF-record i sone-filen til ditt domenenavn

Ved å opprette en SPF-record som forteller hvilke mailserer som har lov å sende e-post fra din mailadresse, gjør du det vanskelig for spammere å forfalske din avsenderadresse. Dvs. utgis seg for å være deg til andre. Tiltaket reduserer også antall spam meldinger, da svært mange spammere bruker ditt domene eller din e-postadresse som avsender adresse for å lure ditt spamfilter som ofte er satt opp til å godta all epost fra deg selv eller ditt domene (organisasjon). **Les mer om hva en SPF-record er og hvordan denne recorden settes opp**.

3.10.12 Hver forsiktig med å angi e-postadressen din på Internett.

En e-post adresse som spammere ikke finnert, får heller ikke spam eller i veldig liten grad. Dette viser erfaringer helt klart. Det er derfor viktig å sørge for å ikke bruke adressen til diverse registreringer på Internett.

Hver forsiktig med å fylle ut online skjemaer som ber om din e-postadresse. Ikke gi din e-postadresse til et nettsted, med mindre du virkelig ønsker å gi dem din e-postadresse. Sjekk hvordan de har tenkt å benytte den og forsikr deg om at den ikke blir distribuert til andre eller brukt til andre formål en det du har gitt tillatelse for. Her syndes det mye, men hver her klar over at svært mange selger og bytter mailinglister seg imellom. Og skulle du tro noe annet; – Dette gjelder ikke bare utenlandske nettsteder. De norske er ikke noe bedre! De som sender ut spam, har funnet e-postadressen din et sted.

I forbindelse med e-postlister og annen publisering av din adresse på Internett, må du vurdere muligheten til senere å slette adressen og eventuelle andre personopplysninger.

3.10.13 Ikke åpn mistenkelig e-post eller e-post fra ukjente avsendere

Ikke åpn mistenkelig e-post. Slett all mistenkelig e-post. Bruk heller ikke funksjonen for forhåndsvisning av e-post. Dette kan medføre at spammerne for en tilbakemelding via e-postklienten din at e-postkontoen er i bruk.

3.10.14 Svar aldri på spam!

Dette bør du ikke gjøre, fordi da bekrefter du at din e-post adresse er gyldig. Resultatet blir da bar en øking i antall spam meldinger fra dem og deres nettverk.

3.10.15 Klikk aldri på en URL eller nettadresse i en spammelding

Dette bekrefter bare at e-postadressen din er aktiv og brukes til avsenderen, og du kan risikere å få mer spam. Kopier heller linken og lim den inn i nettleservinduet ditt, hvis du tror det er informasjon du er interessert i.

Dette er også relevant om det ser ut som om mailen kommer fra eBay, nettbanken din eller andre sider du stoler på. Spammere er veldig glad i å lage forfalskede e-post. Sjansen er stor for at du blir utsatt for et svindelforsøk.

Spam er en av de enkleste måtene folk med skumle hensikter får tilgang til din maskin på. Ved å sende deg en e-post som kan virke interessant, relevant, forlokkende, spennende, eller humoristisk får de deg til å åpne mailen.

Dessverre kan ett klikk ofte være nok til å slippe uvedkommende inn på maskinen din. Her er noen av de vanligste truslene du utsetter deg selv for ved å åpne spam:

- **Trojanske hester.** Disse filene ligger skjult i e-postvedlegg. Når de åpnes, installerer de ondsinnet kode, vanligvis spionprogrammer eller virus – designet for å stjele eller ødelegge data på PC-en.
- **Zombier**. Denne typen skadeprogrammer kommer også i e-postvedlegg, men gjør datamaskinen din om til en server som sender ut spam til andre PC-er.
- **Nettfiskere og vishere.** Nettfiskere (kjent som phishing) sender e-post som gir seg ut for å være meldinger fra legitime finansselskaper eller andre bedrifter som du bruker. E-post fra nettfiskere vil be deg gå til et falskt eller imitert webområde for å oppgi kredittkortnummeret eller kontrollere passordet ditt. Vishere vil be deg ringe dem med samme opplysninger. Husk at seriøse virksomheter aldri vil be om disse tingene via e-post.
- **Ren svindel.** Du har ikke vunnet et lotteri i Tyrkia, heller ikke ble du valgt spesielt av kona til en avdød president i Afrika for å motta 10 millioner dollar for å la henne bruke bankkontoen din. Ikke bli skuffet. Hvis et tilbud er for godt til å være sant, er det antageligvis det.

3.10.16 Vær kritisk til «unsubribe» funksjonen i spam fra ukjent

Følg aldri meldingens instruksjoner om å svare med ordet «fjern» eller «remove» fra utenlandske avsendere, med mindre du stoler på firmaet som sendte e-posten.

Dette gjør spammerne for å få deg til å reagere på e-posten og det vil fortelle avsenderen at kontoen din er aktiv og at du tar imot post, noe som øker verdien av adressen din. Hvis du svarer risikerer du at adressen din settes på enda flere lister, og du får mer spam.

Norske avsendere kan forfølges rettslig i Norge og kan enkelt klages inn til Forbrukerombudet. Avmeldingsfunksjonene fra disse avsenderne er derfor normalt trygge å bruke, og er å anbefale som første steg.

3.10.17 Prøv aldre et anti-spam nettsted

Registrer deg aldri på sider som lover å fjerne navnet ditt fra spam-lister. Selv om disse sidene som regel er lovlydige, er de adressesamlere. De lovlige sidene blir utnyttet av og eies av spammere. Hvis du registrerer deg, bekrefter du at adressen din er aktiv.

4 Brannmur

For å sørge for at ingen utenforstående får tilgang til virksomhetens nettverk, servere og datamaskiner, må man ha en fysisk nettverks brannmur som står mellom Internett forbindelsen til virksomheten og LAN-nettverket på innsiden.

I datateknikk er en **brannmur**, eller *firewall* som det heter på engelsk: ***"maskinvare og/eller programvare som beskytter datanett mot uønsket***

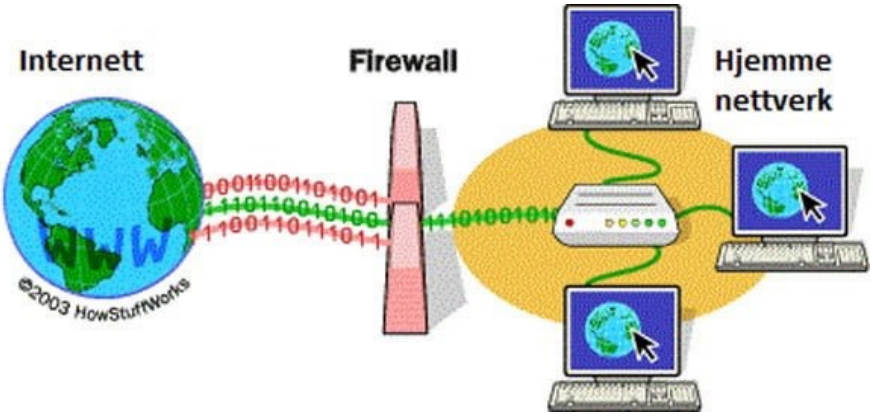
kommunikasjon".

Eksempel på slik uønsket kommunikasjon kan være hackere som trenger inn i datanett koplet til internett.

4.1 Funksjon

Brannmuren sin oppgave er å kontrollere trafikk mellom datanettverk med ulike tillits-forhold. Typiske eksempel er Internet som er ei sone uten tillit, og et internt nettverk som er (og skal være) en sone med høy tillit. Målet er å tilby kontrollerte grensesnitt mellom soner med ulike tillitsforhold ved å påtvinge en sikkerhets-politikk og tilkoblingsmodell. En sone med et mellomliggende tillitsnivå, plassert mellom Internett og det pålitelige interne nettverket blir ofte referert til et perimeter-nettverk eller DMZ (DeMilitarized Zone).

Riktig konfigurasjon av brannmurer krever gode evner hos system-administratoren. Det krever betydelig forståelse for nettverks-protokoller og datasikkerhet. Små feilgrep kan gjøre en brannmur verdiløs som sikkerhetsverktøy. Standard sikkerhetsrutiner foreskriver et «default-deny» (avslå dersom ikke annet er spesifisert) regelsett for brannmuren.



4.2 Personlig brannmur

En personlig brannmur
er et program som beskytter datamaskinen mot angrep fra Internett. Den kan ikke beskytte mot alle typer angrep, men er et av de grunnleggende og nødvendige sikringstiltakene. I virksomheter, som bør ha en nettverksbrannmur, bør alle bærbare maskiner ha en personlig brannmur installert. På hjemmenettverk bør alle datamaskiner ha personlig brannmur installert.

4.3 Trusler

Personlig brannmur gir god beskyttelse mot kartlegging av maskinen, automatiserte angrep og ormer. De fleste personlige brannmurer inneholder ofte også ekstra funksjonalitet som kan øke beskyttelsen mot spam, virus, spyware, phising og andre former for uønskede hendelser. Hvor mye og hvor godt den beskytter mot slike trusler, varierer mye mellom de ulike variantene av personlige brannmurer.

4.4 Typer av brannmurer

Alle de vanlige operativsystemene har i dag brannmurfunksjonalitet inkludert. Linux inneholder iptables, Mac OS X har ipfw, og Windows XP har Windows-brannmur. Alle disse kan gi god beskyttelse mot ulike former for angrep. De inneholder ikke mye ekstrafunksjonalitet for ytterligere beskyttelse, men gir en god og nødvendig basisbeskyttelse. Det finnes også mange personlige brannmurer som kan lastes ned gratis eller kjøpes. Felles for disse er at de tilbyr utvidet eller forbedret funksjonalitet enn de som følger standard med operativsystemet. For Linux og Mac OS X er det stor sett snakk om verktøy som gjør det enklere å administrere den innebygde brannmuren.

4.5 Virkemåte

Det finnes to hovedtyper av personlige brannmurer. **Applikasjons- og trafikkfokuserte**.

4.5.1 Applikasjonsfokusert

Disse styrer tilgang ut på Internett basert på hvilken applikasjon som prøver å nå nettet. Normalt lager de seg en signatur av alle applikasjoner som har fått lov til å gå på nett for å enkelt kunne se om disse endres. Inngående trafikk kan også styres til spesifikke applikasjoner og ikke bare på portnumre.

4.5.2 Trafikkfokusert

Disse styrer tilgang kun basert på IP-adresser og portnumre. De gir samme type beskyttelse som en nettverksbrannmur, men bare for en enkelt datamaskin. For brukere med erfaring fra nettverksbrannmurer vil det være enkelt å sette seg inn i bruken av disse.

Begge typer er effektive sikkerhetsverktøy. De applikasjonsfokuserte gir noe mer sikkerhet, da de i tillegg til å filtrere trafikken også kan oppdage at applikasjoner blir endret.

4.6 Installasjon

Hvis en bruker de medfølgende personlige brannmurene, er det bare å ta den i bruk. Nøyaktig informasjon om hvordan dette gjøres finnes i medfølgende dokumentasjon eller i hjelpesystemet. Ofte kan en også finne utførlige veiledninger på nettet om disse brannmurene.

Hvis en i stedet velger å bruke en annen personlig brannmur enn den som følger med operativsystemet, så bør en følge installasjonsveiledningen nøye.

4.7 Bruk

I daglig bruk er det forskjell på hvordan brukeren må forholde seg til den personlige brannmuren avhengig av om den er applikasjons- eller trafikkfokusert.

4.7.1 Applikasjonsfokuserte

De fleste av denne typen er såkalt selvlærende. Det vil si at første gang en applikasjon prøver å gå på nett så vil en få spørsmål om en vil tillate dette eller ikke. Innholdet i dialogboksen som kommer opp kan være forvirrende og vanskelig å forstå. For å hjelpe brukerne med dette har de personlige brannmurene ofte ferdige regler som åpner for de vanligste nettlesere og e-postklienter. De har også ofte muligheten for å klikke på en link for å få mer informasjon om applikasjonen det gjelder.

En ting som kan forvirre er applikasjoner som kjører i en virtuell maskin eller i et større rammeverk. Da vil en ofte få spørsmål om en tillater at den virtuelle maskinen eller rammeverket skal få tilgang til nett i stedet for applikasjonen en startet. En tommelfingerregel som normalt gjelder er at hvis dialogboksen kommer opp rett etter du har prøvd å starte et program, så er det som regel det programmet det gjelder. Denne tommelfingerregelen er ikke 100 % vanntett, men vil i de fleste tilfeller fungere godt nok.

Rett etter installasjon vil du ofte få mange spørsmål om applikasjoner som skal på nett uten at du har startet dem selv. Dette er programmer som startes automatisk av operativsystemet. Etter kort tid vil dette bli redusert drastisk. Da kan du bli mer skeptisk til programmer som uten at du har bedt om det prøver å gå på nett.

Noen applikasjoner oppdaterer seg meget hyppig. Antivirusløsninger er et vanlig eksempel på dette. Slike programmer vil medføre at en må gi tillatelse til å gå på nett etter hver endring. Mange vil synes dette er plagsomt, derfor har mange applikasjonsfokuserte personlige brannmurer funksjonalitet som kan gi tillatelse til å gå på nett basert på katalog og filnavn i stedet for selve signaturen til applikasjonen. Dette gir en noe lavere beskyttelse enn bruk av signaturer, men gir mindre bryderi med dialogbokser.

4.7.2 Trafikkfokuserte

Disse vil utføre jobben sin i bakgrunnen. I stedet er du nødt til å på forhånd ha definert de nødvendige reglene for det du skal ha tilgang til. Denne jobben kan ta noe tid og kan også virke vanskelig i begynnelsen. Når denne jobben først er gjort så vil en slik personlig brannmur kreve lite oppfølging utenom loggen.

For å få tilsvarende beskyttelse av applikasjonene som de applikasjonsfokuserte gir, bør en vurdere ulike verktøy for å oppdage endringer av applikasjoner. Det finnes mange slike verktøy på markedet. Det finnes også flere gode gratisversjoner for dette.
Virksomheter som skal administrere mange personlige brannmurer bør vurdere en løsning med god støtte for sentralisert kontroll og administrasjon.

4.8 Logger

I daglig bruk vil de to ulike hovedtypene av personlige brannmurer oppføre seg noe forskjellig. Felles for begge er at logger bør følges opp jevnlig. På den måten vil en etter hvert lære seg hva som er normal trafikk og støy i loggen, slik at en i stedet kan fokusere på de alvorlige avvikene.

4.9 Mer bistand

Det kan være vanskelig å vite om en har installert og konfigurert en personlig brannmur riktig. På nettet finnes det mange verktøy som kan hjelpe deg til å teste dette. De viktigste er:

- Leaktest sjekker om brannmuren tillater en ukjent applikasjon å gå på nett.
- Shields UP! kjører en såkalt portskanning for å se om maskinen er synlig utenfra.
- Symantec Security Check som sjekker den personlige brannmuren og Virus detection kan sjekke etter virusinfeksjoner.

5 Sikring av trådløse nettverk (WI-FI)

Trådløse nettverk har mange fordeler, da de ikke trenger kabler, samtidig som signalene går igjennom både vegger, tak og gulv. Trådløse nettverk tas derfor i bruk på stadig flere steder, både privat, på jobben og offentlige steder.

Problemet med trådløse nettverk, også kalt **WI-FI**, er at det er relativt enkelt å bryte seg inn på trådløse nettverk. Et WEP angrep tar bare minutter, et WPS-angrep kan være unnagjort på en formiddag, mens et svært omfattende angrep på WPA med ordbok kan gjøres på én uke, hvis angriperen har et par gode skjermkort tilgjengelig.

Det eneste angriperne trenger å gjøre er å laste ned noen programvarer og bruksanvisninger fra Internett, før de starter angrepet mot ditt trådløse nettverk.

La oss først se på de 3 sikkerhetstandardene som gjelder for trådløse (WI-FI) nettverk, før vi kommer nærmere inn på hvordan du bør gå frem for å sette opp din ruter på en sikrest mulig måte.

5.1 WEP – den store synderen

Wired Equivalent Privacy (WEP) var den første sikkerhetsstandarden for trådløse nettverk som kom. Standarden kom i 1999, men er i dag å anse som en svært usikker krypteringteknologi. Krypteringen kan i dag knekkes på svært kort tid, faktisk på minutter.

Bruk derfor ALDRI WEB kryptering av ditt trådløse nettverk.

5.2 WPA – krypteringen er ikke sterkere enn passordet

For å bøte på problemet WEP skapte, kom **Wi-Fi Protected Access (WPA)** i 2003. Sikkerhetstandarden WPA har i dag ingen kjente sikkerhetshull for å knekke

nettverkpassordet til WPA-krypterte nettverk. Etterfølgeren WPA2 har dessuten gjort standarden enda sikrere.

Til tross for at krypteringen regnes som sikker, er det mulig å knekke passordet. Hackere kan f.eks. sette opp en lyttepost for å prøve å snappe opp samhandlingen mellom datamaskinen og nettverkruteren når en annen datamaskin kobler seg til WPA nettverket ditt.

Den interessante delen av denne samhandlingen kalles en handshake, og er prosessen som går ut på å verifisere om en datamaskin er en gyldig bruker av WPA-nettverket eller ikke. Påloggingen skjer ved at sikkerhetsstandarden regner seg frem til en unik nøkkel, Denne nøkkelen kalles **Pairwise Master Key (PMK)**, og er basert på nettverkets navn og et selvvalgt passord.

En eventuell hacker vil prøve å fange opp håndtrykket mellom datamaskinen og ruteren, for å deretter generere en haug med nøkler ut i fra nettverknavnet og en liste med vanlige passord. Til slutt kan han teste disse nøklene mot håndtrykket for å sjekke om listen inneholdt rett passord til nettverket. Det er også mulig å gå systematisk til verks, ved å teste ethvert mulige passord. Dette kalles for et **«brute-force»-angrep**.

Har du et svakt passord, et passord som finnes i ordlister, eller et som hackeren selv kan generere ut ifra informasjon som adresse, navn og telefonnummer, har du et nettverk som er sårbart for ytre inntrengere. Her gjelder regelen: **– Jo lengre passordet er, jo vanskeligere er det å knekke det**.

Å kalkulere slike nøkler krever stor datakraft, og var tidligere en fremgangsmåte som var lite brukt. I dag har datakraften til PCèr og da spesielt skjermkortene blitt så stor at det i dag er fult mulig å knekke passord på kun 5 bokstaver på relativt kort tid.

5.3 WPS – den skjulte sårbarheten

Wi-Fi Protected Setup (WPS) er den siste sikkerhetsstandarden for trådløse nett og kom for å gjøre det enklere og tryggere for ukyndige å koble enheter til et trådløst nettverk. Standarden gjorde det mulig å få tilgang til et trådløst nettverk ved å kun oppgi en 8-sifret kode som var klistret på selve ruteren.

I desember 2011 ble det imidlertid funnet en grov usikkerhet i standarden, som gjør det mulig å sjekke om de første fire sifrene i koden er korrekt, uavhengig av om resten av koden er korrekt. Denne designfeilen i WPS-protokollen gjør det praktisk mulig å bruke et såkalt "brute force"-angrep for å knekke den åttesifrene PIN-koden. Når ruteren får feil PIN-kode viser det seg nemlig at den gir beskjed tilbake om de fire første snifferne er riktige

Som om dette ikke var nok, slenger ruteren samtidig ut informasjon om det siste tallet i koden som brukes som et kontrollsiffer er riktig eller galt. Dette kontrollsifferet blir regnet ut ved hjelp av de syv foregående sifrene. I praksis ble dermed den 8-sifrene koden redusert til to koder på fire og tre siffer, som reduserer antall mulige nøkler fra 100 000 000 til 11 000.

Når dette kombineres med at mange rutere ikke blokkerer klienter som gjør vedvarende tilkobling forsøk med feil PIN-kode, kan uvedkommende med lysten og kunnskapen komme seg inn i et slikt nettverk på noen få timer. Angreptiden varierer ut i fra rutermodell og

avstand fra nettverket, men svært få rutermodeller er sikret mot sårbarheten. Et gjennomsnittlig angrep tar gjerne rundt 4-5 timer, så med andre ord er heller ikke WPS en fullgod løsning i seg selv.

5.4 Å skjule nettverket er ingen god løsning

Innbruddprosessen i en WPA-kryptering avhenger som tidligere nevnt ikke av rutermodell, men av nettverknavnet. Noen trådløse rutere tilbyr muligheten til å skjule nettverknavnet, slik at det ikke blir synlig i listen over nettverk i nærheten av deg. Da må du manuelt skrive inn nettverknavnet på enheten som skal kobles til. Det kan ved første øyekast virke som en god løsning, men den har flere klare ulemper.

Dette er mindre gjennomtenkt funksjon, da det medfører at alle tilkoblede enheter – og enheter som tidligere har vært tilkoblet og som for øyeblikket ikke er tilkoblet noen nettverk – sender ut nettverknavnet i alle retninger, enten de befinner seg hjemme eller på flyplassen.

I stedet for at én enkelt enhet, ruteren, kringkaster nettverknavnet har nå alle tilkoblede laptoper, mobiler, og nettbrett fått denne oppgaven. Navnet er fortsatt skjult for det nakne øyet, men enhver programvare som søker etter nettverk vil plukke opp både nettverket og dets navn.

5.5 Logg inn på ruterens administrasjonsgrensesnitt

For å kunne sette opp ruteren, må du først logge på ruterens administrasjons – grensesnittet.

Ruteren vil normalt være satt opp med ip-adressen 192.168.0.1 , 192.168.1.1 eller 10.0.0.1 . Dette vil framkomme av dokumentasjonen.

For å få kontakt med ruteren åpner du en nettleser (f.eks. Chrome eller Firefox) og skriver ip-adressen til ruteren. F.eks. http://192.168.0.1. Logg så inn med det brukernavnet og passordet som du finner i dokumentasjonen til ruteren.

En alternativ løsning vil være å kjøre kommandoen **ipconfig /all** fra kommandolinjen. Denne kommandoen vil liste ut tilkobling informasjon for alle nettverks forbindelsene til pc-en. For forbindelsen som benyttes til ruteren skal man se etter «***Default gateway***«-ip- adressen.

5.6 Oppdater firmware (operativsystemet)

Det første du bør gjøre når du er inne, er å oppdatere ruterens firmware (operativsystem), slik at du er sikker på at du bruker den nyeste versjonen av programvaren til ruteren. Noen har innebygde funksjoner for å gjøre dette, mens andre krever at du besøker en nettside.

5.7 Bytt til et unikt nettverknavn

Bruker du et standard nettverknavn (SSID) som «dlink» eller «linksys» bør du skifte til noe som er unikt.

Årsaken til dette skyldes at hackere som ønsker å bryte seg inn på ditt trådløse nettverk vil benytte lister med ferdige nøkkelsamlinger som kan testes på kjente nettverknavn som f.eks. dlink og linksys. Skift derfor nettverknavnet til noe unikt.

5.8 Ikke skjul nettverknavnet

Dette er en dårlig ide, da navnet egentlig ikke blir skjult. Å prøve å skjule nettverknavnet skaper bare mer jobb for deg hver gang du skal koble til en enhet, uten at sikkerheten øker.

5.9 Ikke bruk WEP eller WPS

WEP og WPS er som vi har vært inn på tidligere ikke å anse som en sikker protokoll og bør derfor ikke brukes.Spesielt ikke WEP.

5.10 Bruk WPA2 med AES-kryptering

Velg den nyeste krypteringen som er tilgjengelig. Velg WPA2 med AES eller TKIP kryptering.

5.11 Bruk et godt passord på det trådløse nettverket

Nettverks passordet er systemets svakeste ledd. Sørg derfor for å velge et trygt passord til ditt trådløse nettverk.

Når det gjelder nettverks passordet til ditt trådløse nett er det bedre å lage et langt og vanskelig passord som skrives ned på en lapp som festes på ruteren, enn et enkelt passord som er lett å huske.

En kjent, og forholdsvis grei metode, er å velge et langt passord som er lett å huske. Det er antageligvis svært få hackere som har ordlister omfattende nok til å inneholde «MinHUNDheterROCKY3».

Husk i denne sammenheng at passordet blir mye sterkere om du benytter deg av norske bokstaver som æ, ø og å, sammen med både tegn og tall. Skal du lage et passord sammensatt av ord, bør det inneholde dialektuttrykk som ikke finnes i ordbøker, og det bør helst være ganske langt.

5.12 ..og på ruterens konfigurasjonsside

For å være på den sikre siden bør du også sette et nytt passord for å få tilgang til ruterens konfigurasjonsside. Ikke bruk det samme passordet her som for påloggingen til nettverket. Bruk heller ikke et passord som er enkelt å gjette. La aldri ruteren bli stående med standard passordet fra produsenten, da dette er det samme som å la døra stå åpen.

5.13 Slå av fjernadministrasjon

Noen rutere støtter konfigurasjon over internett. Denne funksjonen pleier å være avslått som standardvalg, men det kan være lurt å sjekke at denne er av.

5.14 MAC-filtrering er ikke tilstrekkelig

Hver eneste nettverkenhet, det være en mobiltelefon, nettbrett eller nettverkskort, har en unik MAC-adresse knyttet til seg. Denne brukes blant annet av ruteren for å holde styr på hvilke enheter som er hvilke.

I mange rutere har du muligheten til å lage en liste over MAC-adresser som er godkjent til å koble til nettverket. Vi anbefaler ikke å slå på denne funksjonen, da det er en triviell sak å omgå denne sperren. MAC-filtrering vil bare gjøre det mer tungvindt for deg, uten å virke som en sperre mot en eventuell innbryter.

5.15 Trenger du UPnP?

UPnP er en teknologi der tjenester/programmer/enheter kan sende konfigurasjons ønsker til ruteren. Dette er en vanlig løsning å benytte når ruteren skal settes opp til å kunne ta i mot trafikk som er initialisert utenfra. For eksempel hvis du bruker ip-telefoni/ip-telefoni- adapter vil den normalt sett sende en forespørsel via UPnP for å få åpnet porten den trenger å motta samtaler.

En annen vanlig bruk av UPnP hos mange er bittorrent-klienter, hvor bedre ytelse oppnås hvis man enten manuelt setter opp en port for klienten eller at den får gjort dette via UPnP. Noen spill vil også kunne utnytte UPnP for automatisk oppsett i forhold til nettspilling.

UPnP gir imidlertid en del sikkerhetsmessige utfordringer. Det vi blant annet ser er at en del har skrivere, overvåkningskameraer og NAS-lagringsenheter som har eksponert seg mot nettet via UPnP, og det uten at man nødvendigvis i praksis bruker de tjenestene som har blitt eksponert. Dessuten finnes det mange eksempler på malware/virus som har utnyttet UPnP.

Tidligere var det mange rutere som ble levert med UPnP deaktivert, men etter hvert er det blitt vanlig at dette er aktivert som standard. Bakgrunnen for dette kan nok ha vært klager om at for eksempel bittorrent var tregt for mange eller at andre rutere kanskje var «bedre» fordi en del tjenester fungerte uten at man trengte å gjøre noe som helst.

Alternativet til UPnP blir at man må gjøre manuelle portinnstillinger/NAT-innstillinger på ruteren for en del tjenester. For svært mange er det ikke tjenester i bruk som vil kreve noe spesiell konfigurasjon av ruteren, og UPnP kan da godt deaktiveres.

5.16 En bedre DNS?

DNS står for Domain Name System og er tjenesten som på internett gjør koblingene mellom domenenavn og ip-adressene til serverne. Normalt sett har internettleverandøren en egen DNS-tjener og ruteren blir i utgangspunktet satt opp til å bruke denne.

Gjennom tjenester som OpenDNS kan man få forbedringer i forhold til sikkerhet for alle enhetene koblet på nettverket. Gjennom en OpenDNS-konto kan man for eksempel velge at

sider som er kjent for å inneholde pornografi, piratkopiert programvare, vold, phisingforsøk og mer til blokkeres.

Aktører som D-Link og Netgear har valg i administrasjons grensesnittet for å ta i bruk OpenDNS. På andre rutere må man sette opp en konto hos OpenDNS og mer manuelt sette opp DNS-ip-adressen i ruteradministrasjonen.

5.17 Sjekk tilkoblede enheter

Mistenker du at noen er tilkoblet nettverket ditt? De fleste rutere har en oversikt over enheter som er tilkoblet og som har vært tilkoblet. Vær oppmerksom på at en inntrenger på nettverket som også har tilgang til ruterens administrasjon, kan slette denne informasjonen. Informasjonen kan også være tildels vanskelig å dekode.

I ruter oppsettet vil det i utgangspunktet stå MAC-adressen til enheter som har vært tilkoblet. Enhver enhet (mobiltelefon, pc, nettbrett og så videre) vil ha hver sin unike MAC-adresse. Riktignok kan MAC-adressen forfalskes.

I tillegg til MAC-adressen vil det stå hvilke ip-adresser enhetene har, samt i noen tilfeller også et enhetsnavn som vil gjøre det enklere å identifisere enheten.

En del sikkerhetsprogrammer vil også gi varsler når nye pc-er eller andre enheter blir koblet til lokalnettverket. En del rutere har også funksjonalitet for å overvåre sanntidstrafikk.

Det finnes også flere gratis overvåkningsprogrammer du kan laste ned for å sjekke hvem som er på nettet ditt.

6 Sikring av datamaskiner

Rådene du finner på denne siden gjelder for både PC og Mac og er de mest banale sikkerhetsrådene for å sikre din maskin mot datainnbrudd.

6.1 Hver forsiktig med Windows og Android

Du reduserer risikoen 90% hvis du velger et annet operativsystem enn Windows for PC og Android for mobile enheter. Windows og Android er i dag det dominerende operativsystemet, noe som gjør systemet mer attraktivt for hackere enn Mac, Linux og iOS som har en relativt liten markedsandel.

6.2 Skaff deg en personlig brannmur

En brannmur er den beste beskyttelsen mot uønskede angrep. Den beste beskyttelsen gir hardwarebaserte brannmurer, men har du ikke råd til dette kommer du langt med en softwarbasert brannmur. Faktisk så trenger du begge deler, spesielt hvis vi snakker om bærbart utstyr.

6.3 Skaff deg et anti-virus program

1 av 4 PCer har IKKE et aktivt anti-virus program. Dette er skremmende. Når brannmuren er på plass, er **neste obligatoriske oppgave** å installere et skikkelig anti-virus program som sjekker maskinen for virus, trojanere, ormer og annen malware som du kommer over når du installerer programmer, surfer på nettet og laster ned og leser epost.

6.4 Steng alle åpne porter på datamaskinen

Hackere, ormer og virus kommer seg inn på maskinen din ved at de finner en åpen port på maskinen din som de klarer å bruke til å komme seg inn. Ønsker du å holde hackere, ormer o.l. unna dine systemer gjelder det dermed å stenge alle porter du ikke bruker.

6.5 Hold maskinen og programmene oppdatert

Det oppdages hele tiden nye sikkerhetshull, spesielt i Windows. Det gjelder derfor å kjøre **Windows Update** ved jevne mellomrom, f.eks. en gang hver 14 dag. Sett Windows til å laste ned og installere disse oppdateringene automatisk. Det samme gjelder ditt anti- virus program og Office-pakken som også trenger konstant oppdatering. Glem heller ikke andre teknologier du måtte ha installert på maskinen, f.eks. Java og Flash.

6.6 Passord beskytt sensitive filer og mapper

Sett et trygt passord på sensitive filer og mapper du har på din maskin. Dette kan normalt gjøres raskt og enkelt, enten du er på ditt nettsted eller lokale datamaskin. Benytt aldri det samme passordet her som gjelder for for andre områder eller tjenester på samme maskin eller nettsted. Da faller hele hensikten bort. Meningen er at dette skal være en dobbel beskyttelse mot tyveri av sensitiv informasjon.

7 Sikring av mobiltelefon og nettbrett

Dagens mobiltelefoner kan sammenlignes med små datamaskiner. De inneholder ofte mye av den samme informasjonen som du finne på din PC. Det er derfor like viktig, om ikke viktigere å sikre mobiltelefonen.

• **Slå på apparat lås**
o Dette er ikke det samme som PIN-kode som kun låser SIM-kortet.

Apparat låsen kan sammenlignes med en skjermsparer med passord. Denne settes normalt til å slå seg på etter en gitt tid med inaktivitet. Normalt finner man dette valget under innstillinger og sikkerhet.

• **Pinkode**
o Slå på pinkode. PIN koden kreves hver gang telefonen startes på nytt. Om

du bytter SIM kort kan du benytte en telefon som kun har pinkode, men ingen andre sikkerhetsløsninger aktivert. Hvordan du aktiverer pinkoden varierer fra telefon til telefon, men normalt finner man dette valget under innstillinger og sikkerhet.

• **Installere et sporings program**
o Det finnes flere programmer som både kan lokalisere telefonen, fjernslette

innholdet samt at en alarm kan aktiveres. Noen forslag: Lookout Mobile Security for Android og Find My iPhone for IPhone/iPad/iPod. Det finnes flere slike løsninger. Noen av disse koster litt penger, men dette kan være en rimelig forsikring.

• **Krypter innholdet på telefon og minnekort**
o Om du skulle være så uheldig å miste eller få stjålet telefonen, er det

viktigste at innholdet ikke blir tilgjengelig for andre. Dette unngår du ved å kryptere viktig/sensitiv informasjon. De fleste javabaserte telefoner kan benytte f.eks. SafeCase. Sjekk med leverandør, produsent eller operatør.

• **Ta sikkerhetskopi av innholdet**
o Det er ulike måter å ta sikkerhetskopi av telefonen avhengig av hva slags

mobiltelefon du har. Sjekk nettsiden til din operatør om de har egen

programvare slik at du kan ta sikkerhetskopiene selv.

• **Registrer telefonene IMEI nr. på en trygg plass**
o Dette er mobiltelefonens unike identifikasjonsnummer. Du finner det oftest

under batteriet i telefonen eller på esken telefonen kommer i. Du får det frem på mobiltelefonen ved å taste *#06#. Med dette nummeret kan du melde fra til operatøren din og få sperret telefonen om den blir stjålet.

• **Remote Device Management**
o For bedriftsmarkedet finnes det egne løsninger der én eller flere i bedriften

kan administrere mobiltelefonene til alle de ansatte uten å få tilgang til

7.1 Mobiltelefoner og nettbrett må håndteres på samme måte som datamaskiner

selve til innholdet. Disse systemene kan låse telefoner som er stjålet, ta backup, fjernslette innhold eller endre konfigurasjoner.

Ta like godt vare på telefonen din som datamaskinen og eventuelt nettbrettet.
Disse er alle datamaskiner med ulik formfaktor som inneholder viktig informasjon som ikke skal deles med andre. Husk at det er informasjonen som er verdien din!

8 SSL | Secure Sockets Layer

8.1 Trygg overføring av data og transaksjoner!

Secure Sockets Layer, **SSL**, er en protokoll som tillater autentisering mellom en klient (maskin/mobil) og en tjener (server) for å opprette en autentisert og kryptert tilkobling. Eller som vi sier på god norsk:

«***En sikker tilkobling mellom to datamaskiner, hvor det er umulig for hackere og andre uvedkommende å snappe opp informasjonen som sendes mellom disse to datamaskinene»*.**

SSL protokollen brukes for å opprette en sikker kobling mellom en server og en klient (din datamaskin/pad/mobil).

Ved at linjen mellom A og B blir kryptert er det ikke mulig for uvedkommende å sette opp en «*lyttepost*» på linjen som tar en kopi av informasjonen som sendes mellom serveren og tjeneren (din maskin/mobil. SSL brukes derfor alltid i forbindelse med korttransaksjoner, innlogging til nettbanker og annen overføring av sensitiv informasjon.

8.2 Sikkerheten avgjøres av krypteringsalgoritmen

Hvor godt denne linjen blir kryptert er avhengig av krypteringsalgoritmen som brukes. Jo høyere kryptering, jo vanskeligere er det for hackere å knekke krypteringen av dataene. Den høyeste krypteringen er idag 256-bit kryptering gjennom SHA-256 algoritmen. Av den grunn bygger alle SSL-sertifikatene OnNet selger på 256/128 bits SHA-256 kryptering.

8.3 Hvorfor SSL?

SSL tillater sensitiv informasjon som kredittkort informasjon, personnumre og passord til å bli overført på Internett på en trygg måte.

Gjennom å installere et SSL sertifikat på ditt nettsted viser du alle kunder og brukere som besøker nettstedet ditt at dette er et seriøst og trygt nettsted, hvor ikke noe informasjon kan bli stjålet av uvedkommende. Noe som blir stadig viktigere for å få kundenes tillit.

Facebook andre sosiale medier har også begynt å kreve at nettstedet har et SSL sertifikat for å kunne utveksle informasjon med det sosiale mediet via et API-grensesnitt e.l. Det samme gjelder nettsteder som ønsker å implementere en betalingløsning.

8.4 Bruksområder for SSL

SSL-sertifikat brukes hovedsakelig til å kryptere følgende typer linjer og kommunikasjon mellom en server og klient:

- **Nettsider** – Alle trafikk til ett nettsted kan omdirigeres til et SSL-sertifikat som krypter all kommunikasjon mellom nettstedet og de som besøker nettstedet via HTML-protokollen. Noe som er svært viktig for å sørge for at kortinformasjon, brukernavn, passord og andre sensitive opplysninger ikke kommer på avveie.
- **Epost** – Ved å kryptere kommunikasjonen over POP3, IMAP og SMTP protokollen til et SSL-sertifikat kan man sikre seg mot at andre klarer å snappe opp sensitiv informasjon som sendes på mail.
- **FTP** – Ved å kryptere kommunikasjonen over FTP-protokollen kan man sikre seg mot at ingen klarer å snappe opp filer som lastes opp eller ned mellom en server og bruker.

  SSL-sertifikatet viser nettbrukeren hvilket selskap som eier domenet. Før dette kan skje må eierskapet være validert og bekreftet av en betrodd tredjepart (sertifiseringsautoritet CA), for å være gyldig.

  Om et SSL-sertifikat er gyldig kan surferne på Internett enkelt se i sin nettleser. Er SSL- sertifikatet gyldig vil du se en hengelås i adressefeltet til nettleseren. I tillegg kan du se at nettsiden benytter SSL ved å se på URLen. Den begynner med med https:// i adressefeltet i stedet for http://.

8.5 Kryptering over TCP/IP – nivået

SSL kjører over TCP/IP-nivået, men under HTTP, LDAP, IMAP, NNTP, og andre nettverksprotokoller som kjører på et høyere nivå.

Den nyere Internet Engineering Task Force (IETF)-standarden Transport Layer Security (TLS) er også basert på SSL.

Hvordan «handshaket» er mellom klienten (deg) og serveren skjer for å etablere en trygg, kryptert linje ved hjelp av et SSL-sertifikat er vist i illustrasjonen til høyre.

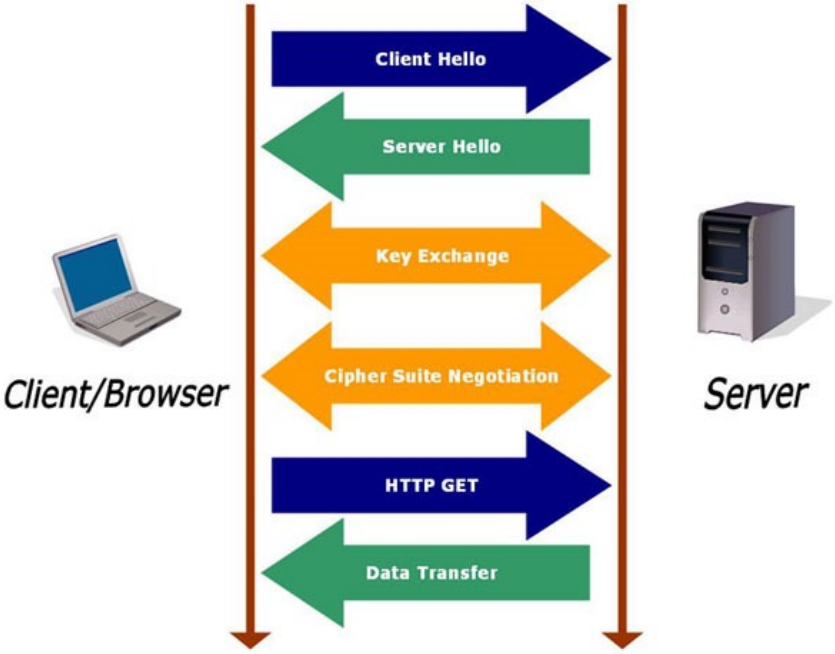
Krypteringen skjer ved at tjenermaskinen (serveren/nettstedet) har en krypteringsnøkkel med to passord. Det ene kan bare brukes til å kryptere innholdet og kan derfor gis ut til alle (**offentlig nøkkel**). Den andre kan brukes til å dekryptere innholdet og må selvsagt bare være kjent for eieren (**privat nøkkel**).

Når SSL brukes f.eks for å lese e-post så sender tjenermaskinen det offentlige passordet til brukermaskinen uten at brukeren av brukermaskinen trenger å vite om dette. Dette passordet (krypteringsnøkkelen) bruker så brukermaskinen til å lage meldingen uleselig (kryptert) for tredjeparter som ikke kjenner dekrypterings passordet (nøkkelen). Deretter sendes meldingen over nettet til tjenermaskinen. Tjenermaskinen mottar meldingen og dekrypterer den ved hjelp

av sitt hemmelige passord (krypteringsnøkkel), og leverer meldingen videre inn i sitt lokale system. Dermed vil ingen mellom bruker og tjener kunne avlytte kommunikasjonen.

I denne sammenheng er det viktig å merke seg at det er kommunikasjonskanalen (linjen) som er kryptert, og ikke selve budskapet (dataene). Ønsker du maksimal sikkerhet mot uautorisert adgang bør også dataene som sendes og lagres krypteres.

8.6 Hva er TCL (Transport Layer Security)?



TLS står for **Transport Layer Security**, og er en nyere versjon av SSL, med mindre justeringer. Brukes bl.a. til å kryptere linjer som brukes til å sende/motta epost og filer.

8.7 Krypterte porter

For å sikre en sikker kryptert tilkobling mellom serveren og brukeren skjer selve krypteringen ved at brukerne blir sendt til helt andre porter enn de åpne standardene bruker. Den åpne HTML standarden for nettsider bruker f.eks. port 80, mens HTMLS standarden bruker port 443. Under finner du oversikt over hvilke porter som normalt brukes.

HTML protokollen:

- Åpen – Port: 80 SSL – Port: 443

FTP protokollen:

- Åpen – Port: 20 SSL – Port: 21

POP3 protokollen:

- Åpen – Port: 110 SSL – Port: 995

SMTP protokollen:

- Åpen – Port: 25 SSL – Port: 465

IMAP protokollen:

- Åpen – Port: 143 SSL – Port: 993

8.8 Nettlesergjenkjennelse

Dersom et SSL-sertifikat ikke gjenkjennes av brukerens nettleser, vil brukeren få et varsel om at nettsiden ikke er trygg. Dette er selvsagt til stor ulempe for eieren av nettsiden som kan miste verdifulle brukere. Hvor stor andel av nettleserne som har forhåndsinstallert roten til de ulike SSL sertifikatene varierer en god del. Et godt sertifikat har minst 99 % nettlesergjenkjennelse.

8.9 Transaksjonsforsikring

SSL sertifikater ivaretar i hovedsak to funksjoner; sikker kryptering av informasjon og identifisering av eier av websiden. Transaksjonsforsikringen er ment å være nettbrukerens økonomiske garanti for at krypteringen ikke blir brutt under sesjonen og at informasjonen i sertifikatet er korrekt. Ved valg av forsikringsbeløp i sertifikatet må man ta stilling til hvilke økonomiske konsekvenser det vil ha dersom utvekslet informasjon kommer til feil mottaker eller blir tappet. Transaksjonsforsikring vil være med på å dekke økonomiske krav fra brukere som har blitt påført tap som et resultat av å ha blitt tappet for informasjon under en kryptert sesjon på din nettside.

8.10 Utstedes av et sertifiseringorgan

SSL sertifikater blir verifisert gjennom en tillitskjede. Tillitsankeret for SSL sertifikatet er rotleverandøren (Root Certificate Authority eller CA). Dersom rotleverandøren er kjent for brukeren er det større sannsynlighet for at vedkommende tar i bruk de tjenestene som websiden tilbyr, enn om det er en ukjent rotleverandør. Årsaken er at brukeren vil anse det som mindre sannsynlig at dette er et svindelforsøk fordi vedkommende stoler på rotleverandøren. Velg derfor sertifikater med mest mulig kjent og tiltrodd rotleverandør. Et godt eksempel på en velkjent rotleverandør er Verisign.

8.11 Hvordan ser jeg at en nettside bruker SSL?

Normalt skjer all kommunikasjon mellom en webserver og en besøkende av din nettside på den åpne HTML-standarden. Dvs. via en adresse som starter med http://.

Skjer kommunikasjonen på en sikker linje starter nettadressen med https://.

I tillegg vil du normalt få et symbol i nettleseren din som forteller at dette er et SSL- beskyttet område. De dyreste SSL-sertifikatene gir i tillegg en «grønn sidebar» med firmanavnet og ett stort grønt felt som en del av nettadressen for å vise at nettstedet benytter et SSL-sertifikat.

8.12 Anbefaling

Vi anbefaler at du alltid bruker SSL protokollen på nettsider som inneholder sensitiv informasjon eller informasjon som du er redd for at andre kan snappe opp via en lyttepost på linjen din. Klassiske eksempler er innloggingssider til brukerne dine.

9 Sikkerhetskopiering

9.1 Hva kan skje med lagret informasjon

Informasjon eller data lagres på datamaskinens harddisk. Det er mye som kan skje med informasjonen du har lagret. Du eller andre kan utilsiktet slette eller endre den. Selv om du oppdager det i det du har trykket ENTER er skaden gjort og mange timers arbeid er borte.

Datamaskinens lagringsmedium, harddisken, kan også gå i stykker. Etter hvert som disken blir eldre må man regne med at den kan feile. Forventet levetid på en vanlig harddisk er i dag 3-5 år. Når en disk feiler er det svært vanskelig å redde informasjonen på den, og noen ganger blir det svært dyrt. Det er derfor en god forsikring å ta vare på dataene flere steder før dette skjer.

9.2 Hvilke informasjoner skal sikres

Virksomheten må vurdere hvilke data som skal sikkerhetskopieres og hvor ofte. Eksempel på data det er viktig å huske er data for produksjonssystemer, kundeinformasjon, e-post, kalendere, kontakter, favoritter i nettleser og skrivebord. Du bør prioritere det som ikke kan reddes lett ved et tap. Husk å kopiere data for både servere, stasjonære og bærbare PC- er. Kritisk data kan også finnes på PDA-er, minnepinner og mobiltelefoner. Sørg også for å kopiere disse dataene, dersom de er viktig for din virksomhet.

9.3 Gode vaner er viktig

Ingen lagringsmetoder kan hjelpe deg dersom du aldri bruker dem. Sikkerhetskopiering er avhengig av at det lages rutiner og at det utpekes ansvarlige for jobben. Husk også ansvarlige i ferier og fravær. Hver virksomhet må bestemme seg for hvor ofte det tas sikkerhetskopi. Dette avhenger av hvordan dataene endrer seg og hvor kritiske de

er. Daglige eller ukentlige sikkerhetskopier er vanlig.

9.4 Typer sikkerhetskopi

Man kan ta full sikkerhetskopi eller inkrementell sikkerhetskopi av bare de data som er ny eller endret siden forrige sikkerhetskopi. Full sikkerhetskopi tar og lagrer unna alle data. En inkrementell sikkerhetskopi tar bare kopi av data som er nye eller endret siden forrige sikkerhetskopi. Periodisk bør det sørges for en full sikkerhetskopi av alle data. Dette styres av programvaren. Vanlige intervaller er daglig, ukentlig eller månedlig for full sikkerhetskopi. Valget gjøres ut fra hvor kritiske dataene er og hvor hurtig en må være i stand til å gjenopprette dem.

9.5 Intern oppbevaring

En sikkerhetskopi er lite verdt hvis den lagres sammen med originaldataene. Derfor må en sørge for at sikkerhetskopien oppbevares på en måte som gjør at den er bedre beskyttet en originaldataene. Mye av tanken bak sikkerhetskopiering er at selve datasystemet er for stort og dyrt å beskytte mot alle mulige fare som brann, flom og lignende. Derfor tar en vare på bare data på mer kompakte løsninger som tape, CD, DVD og så videre. Har virksomheten et brannsikret skap kan dette med fordel brukes til å lagre sikkerhetskopien i. Dette er ikke en fullgod løsning. Brannsikringen er laget med tanke på papir og ikke datamedium. Det finnes

egne kofferter og esker som kan brukes som tilleggssikring og som passer inn i de fleste brannsikre skap.

9.6 Ekstern oppbevaring

For de metodene som gir deg muligheten til å legge sikkerhetskopien et annet sted, bør en gjøre det for å sikre seg i tilfelle brann eller tyveri. Lagring kan skje hjemme i innlåst skap eller hos en annen virksomhet. En mye brukt løsning for mindre datamengder er en bankboks.

9.7 Typer av lagringsmedia

For små og mellomstore virksomheter er følgende lagringsmedier aktuelle å bruke.

9.7.1 CD og DVD

Viktig informasjon kan brennes fra datamaskinens disk og til CD eller DVD. Det forutsetter at maskinen har en CD- eller DVD-brenner eller at man kjøper en ekstern og kobler på datamaskinen. CD- og DVD-plater er billige og de fleste datamaskiner i dag har brenner. Løsningen er enkel og platene er lett å lagre. Platene har imidlertid relativt kort levetid og de har relativt liten lagringskapasitet.

9.7.2 Minnepinner

Viktig informasjon kan kopieres til USB minnepinner. De fleste datamaskiner har USB- port som pinnene kan settes i. Filer og mapper kan kopieres ved å dra de over eller de kan kopieres ved bruk av funksjonene «Kopier» og «Lim inn». Minnepinner er små og tar lite plass, men er også lett å miste. Ellers har de mange av de samme fordeler og ulemper som for CD og DVD.

9.7.3 Ekstern harddisk

Harddisker kan kjøpes separat og kobles til datamaskinen. Disse har like god kapasitet som interne harddisker og nye metoder for overføring gjør transporten av data rask og enkel. Flere eksterne harddisker kommer også med egne programmer for sikkerhetskopiering.

9.7.4 Datatape/ kassett

Tape eller tapekassetter er et godt alternativ for virksomheter som har noe større krav til sikkerhetskopiering. Tapene er laget spesielt for sikkerhetskopiering. En tape kan ta store mengder data, og er robust. Tape er en god løsning for å oppbevare sikkerhetskopier ulike steder, for eksempel i en bankboks. Det er imidlertid noe høy terskel å starte med tape. Tapedrevene er noe dyre og det er nødvendig med egne programmer for å ta sikkerhetskopi.

9.7.5 Online tjenester

Flere leverandører tilbyr lagring av data med overføring over Internett. Du betaler et firma for å lagre dine data hos dem. De gir deg tilgang gjennom en nettside eller et program. Hos noen bredbåndsleverandører følger et slik tilbud med i bredbåndspakken, og det finnes uavhengige leverandører. Dette kan gi tryggheten et seriøst firma kan tilby. De har lagringssystemer som

tåler det meste og lagrer dataene dine trygt. En slik løsning krever at man stiller krav til leverandøren, slik at man kan stole på sikkerhetskopieringen fungerer.

10 Hva må du huske på når du kaster din PC, Mac, kamera eller mobil?

10.1 Husk å slett all sensitiv informasjon

Flere undersøkelser viser at så vel bedrifter som privatpersoner ofte glemmer å slette all personlig og sensitiv informasjon som finnes på den PCen, MACen, PADen, kamera eller mobilen. Dette er en stor sikkerhetsrisiko siden survey viser at 1 av 3 mobiltelefoner inneholder sensitiv informasjon.

Resultatet blir da at du gir bort denne sårbare informasjonen «*søppelbilen*» som ofte skruer ut harddisken og minnekortet for å hente ut informasjonen på den. Hva skjer med informasjonen etter dette har du ingen kontroll over, og må derfor unngås for enhver pris.

Når du lagrer en fil, spesielt en stor fil, deles den opp og lagres i utstyrets lagringsenhet i mindre deler. Når du åpner filen, samler lagringsenheten bitene og rekonstruerer dem til en samlet fil.

10.2 Det holder ikke å bare trykke på «Delete»

Når du sletter en fil, forsvinner den opprinnelige koblingen mellom de delene som filen består av. Men de ulike delene blir igjen i lagringsenheten inntil de blir overskrevet av annen informasjon. Det betyr også at filen kan gjenopprettes. Programvare som kan gjenskape tapte eller slettede data er lett tilgjengelig og kan enkelt brukes til å rekonstruere opplysninger fra en lagringsenhet.

10.3 Sjekkliste:

Datatilsynet har laget følgende sjekkliste over hva du må huske på når du skal kaste en pc, mobil eller et digitalt kamera.

10.3.1 PC

Før du sletter innhold fra datamaskinens lagringsenhet bør du lagre filene dine på eksterne lagringsenheter, slik som på et CD-rom, en USB-penn eller en annen ekstern lagringsenhet.

Når du kvitter deg med PCen bør du ta ut lagringsenheten eller slett innholdet med spesial-programvare. Slik programvare er tilgjengelig på nett og varierer i pris og funksjonalitet:

- **noen sletter alt på lagrinsenheten, mens andre lar deg velge hva du vil slette**
- **noen overskriver og sletter fra lagringsenheten mange ganger, mens andre**

  overskriver bare en gang

  Du bør vurdere å bruke programvare som overskriver eller sletter fra lagringsenheten flere ganger. Slettet informasjon kan ellers gjenopprettes. Alternativt kan du fjerne lagringsenheten fra PCen og destruere denne.

10.3.2 Mobiltelefon

De fleste telefoner har flere lagringsenheter. Sørg for å slette data fra alle enheter, slik som fra:

- det innebygde internminnet
- minnekortet, dette er ofte lett å ta ut før du gir fra deg telefonen
- SIM-kortet (samme som for minnekortet)

10.3.3 Digitalkamera

Slik kan du gå fram

- ta ut minnekort fra kameraet og ta vare på det
- når du har fjernet minnekortet sjekker du om det fortsatt ligger bilder i kameraets

  internminnet

- slett eksisterende bilder og ta noen nye bilder med upersonlig motiv, slik at

  internminnet overskrives med disse bildene

10.4 Ansvar for sikker sletting

Som privatperson kan du selv bestemme om du tåler at opplysninger om deg selv kommer på avveier. Men vær oppmerksom på at du kan komme i erstatningsansvar dersom du lar andres opplysninger komme på avveier når du kvitter deg med eget utstyr.

Når det gjelder virksomheter og personer som bruker personopplysninger til andre formål enn rent private gjelder personopplysningsloven. Når utstyret til en virksomhet kastes eller gis videre, må lagringsmediene destrueres eller slettes slik at de ikke kan bli gjenopprettet. I slike tilfeller må virksomheten sikre at metodene som brukes for sletting er gode nok – vanlig sletting er utilstrekkelig.

11 Hvem står juridisk ansvarlig for sikringen og innholdet i nettskyen?

Hvem er det som står juridisk ansvarlig for nettskyen, konfigureringen, innholdet og bruken av den? Bedriften eller nettsky leverandøren?

Vi har her tatt utgangspunkt i Datatilsynets veiledning om bruk av nettsky-tjenester.

11.1 Virksomheten er juridisk ansvarlig

Datatilsynet sier at virksomheter som tar i bruk nettskytjenester selv er juridisk ansvarlig for nettskyen, og det er deres ansvar å sørge for at personopplysningene som finnes lagret i nettskyen behandles i tråd med personvernregelverket.

Her gjelder de samme reglene som for leverandører av elektroniske tjenester på Internett. og behandlingen av disse opplysningene defineres i personopplysningsloven § 2 nr. 2, sier Datatilsynet.

11.2 Hvilket ansvar har nettsky leverandøren?

Om nettsky leverandørens ansvar sier Datatlsynet følgende. Leverer en nettsky leverandør en tjeneste som kundene kan velge å ta i bruk som beehandlingsansvarlig, er nettsky leverandøren å anse som en databehandler. Datatilsynet anser derfor en leverandør av nettskytjenester som en databehandler, uavhengig av hvilken tjeneste som leveres.

En nettsky leverandør kan ikke behandle personopplysninger på annen måte enn det som er avtalt med kunden (bedriften) som eier dataene, jf. personopplysningsloven § 15. Nettsky leverandøren plikter i tillegg å gjennomføre sikringstiltak som følger av personopplysningsloven § 13 og forskriftens kapittel 2. En databehandleravtale fritar ikke bedriften som eier og bruker dataene for lovfestet juridisk ansvar.

Datatilsynet har laget en veileder om og eksempel på avtaleskisser for en slik databehandleravtale. I avtaleskissen og veilederen finner man minimumskravene som det forventes at en slik avtale innholder. Det kan være andre punkter som tilkommer selve avtalen, men det er avhengig av internkontrollen til bedriften som leier tjenesten. Noen slike punkter kan være; sikkerhetskopiering, sletting, tilgangstyring og segmentering av databaser.

11.3 Risikovurdering og informasjonssikkerhet

Bedriften som leier nettskyen, skal gjennomføre en risikovurdering for sin behandling av personopplysninger. Risikovurderingen må ses i sammenheng med etablerte akseptkriterier for risiko, og bedriften som leier nettskyen skal iverksette nødvendige tiltak for å oppnå en tilfredsstillende informasjonssikkerhet.

For å oppnå tilfredsstillende informasjonssikkerhet må bedriften som leier nettskyen kunne forvisse seg om at tjenesten som blir tatt i bruk møter de kravene som er fastlagt under arbeidet med akseptkriteriene og risikovurderingen. Vurderingen må tillegges større vekt når man går fra egen drift til nettskybaserte løsninger, siden personopplysningene vil ligge utenfor direkte kontroll til den som leier nettskyen. Spørsmålet blir: Hvordan skal bedriften som leier nettskyen forvisse seg at informasjonssikkerheten faktisk er tilfredsstillende?

Databehandleravtalen skal inneholde en del som omhandler informasjonssikkerhet, og det er viktig at den som leier nettskyen går grundig gjennom denne. Avtalen i seg selv er ingen forsikring for at leverandøren har en tilfredsstillendeinformasjons sikkerhet.

Personopplysningsforskriftens kapittel 2 om informasjonssikkerhet har en bestemmelse om sikkerhetsrevisjon:

"Sikkerhetsrevisjon av bruk av informasjonssystemet skal gjennomføres jevnlig. Sikkerhetsrevisjon skal omfatte vurdering av organisering, sikkerhetstiltak og bruk av kommunikasjonspartner og leverandører. Dersom sikkerhetsrevisjonen avdekker bruk av informasjonssystemet som ikke er forutsatt, skal dette behandles som avvik, jf. § 2-6. Resultatet fra sikkerhetsrevisjon skal dokumenteres."

Datatilsynet er derfor av den oppfatning at:

- bedriften som leier nettskyen må kunne legge frem dokumentasjon for informasjonssystemets utforming og sikkerhetsløsninger. Dette for at den som leier nettskyen kan forvisse seg om at løsningen har tilfredsstillende informasjonssikkerhet sett opp mot risikovurdering og akseptkriterier.
- nettsky leverandøren ikke kan endre informasjonssikkerhetstiltak uten at den som leier nettskyen er blitt informert skriftlig og har godkjent endringen.

11.4 Informasjonsplikt

Det følger av personopplysningsloven § 19 at den registrerte skal ha informasjon fra den som leier nettskyen om:

- navn og adresse på den som leier nettskyen,
- formålet med behandlingen,
- opplysningene vil bli utlevert, og eventuelt hvem som er mottaker,
- det er frivillig å gi fra seg opplysningene, og
- annet som gjør den, registrerte i stand til å bruke sine rettigheter etter

personopplysningsloven.

11.5 Særlige problemstillinger

Leverandører av nettskytjenester har i utgangspunktet noen fordeler i forhold til tradisjonelle leverandører av servertjenester. For eksempel kan nettskytjenestene gi mer fleksible og integrerte løsninger. Men slike fordeler fører også med seg noen særlige problemstillinger:

- **Sikkerhetskopiering/Speiling** – Hvordan fungerer dette? Overføres personopplysningene til et annet land for redundans, eksempelvis fra Irland til USA eller fra Tyskland til India? Er en slik redundans i henhold til de avtaler som er inngått? Hvordan behandles personopplysningene etter at de er overført?
- **Segmentering** – Datatilsynet har uttalt at den som leier nettskyens skal sørge for at personopplysninger ikke sammenblandes med opplysninger fra en annen behandlingsansvarlig. Hvordan vil dette bli håndtert?

- **Tilgangsstyring** – Hvem hos leverandøren har tilgang til personopplysningene som behandles? Er tilgangstyring i samsvar med lovpålagte krav og egen internkontroll? Se særlig avsnittet over om risikovurdering og informasjonssikkerhet.
- **Autorisert og uautorisert bruk** – Tar løsningen høyde for registrering av autorisert og uautorisert bruk i henhold til personopplysningsforskriften § 2-14
- **Dokumentasjon** – Er løsningen tilstrekkelig dokumentert med hensyn til kontroll fra offentlige myndigheter?
- **Overføring til tredjeland** – Personopplysninger kan ikke uten videre overføres til land utenfor EØS-sonen, men enkeltvise overføringer kan forhåndsgodkjennes av Datatilsynet. I tillegg er enkelte land godkjent av EU som trygge mottakerstater. Mer om overføring til utlandet.

11.6 Det gjelder å holde tunga rett i munnen

Som du skjønner av veiledningen over som jeg har kopiert rett fra Datatilsynets veiledning om bruk av nettsky tjenester er det mye å huske på for både nettsky leverandøren og du som bruker av nettskyen.

Jeg håper veiledningen over har gitt deg en ide om hva du må tenke på når du skal flytte noe av virksomhetens IT-infrastruktur ut i nettskyen, slik at du ikke kommer i juridiske problemer senere.

11.7 Sjekkliste

Datatilsynet sier at hvis du skal bruke nettbaserte lagringsløsninger bør du stille deg følgende spørsmål:

- Brukervilkår: Hva sier brukervilkårene? Bør jeg være bekymret for noen av dem? Forstår jeg vilkårene?
- Seriøsitet: Hvor seriøse fremstår tjenestetilbyderen? Kjenner jeg noen som kan gi med et råd om bruk av tjenesten er forsvarlig for formålet mitt?
- Sikkerhet: Hvordan ser det ut til at tjenesteleverandør har ivaretatt sikkerheten? Hvor enkel ser det ut til for uvedkommende å skaffe seg tilgang? Ser sikkerheten tilstrekklig ut i forhold til informasjonen jeg ønsker lagret? Søk gjerne råd hos andre som har greie på sikkerhet.
- Passord: Hvis tjenesteleverandør stiller krav til kvalitet på passordet er dette et godt tegn. Virker det som leverandør har ivaretatt dette på en god måte?
- Rettigheter: Hvilke rettigheter har jeg om all informasjonen jeg har lagret blir borte? Sies det noe om det i vilkårene? Har jeg en egen sikkerhetskopi?
- Lovgivning: Hvilket land er tjenesteleverandøren hjemmehørende i? Hvem kan hjelpe meg hvis noe skulle gå galt? Informasjonen på nettaserte løsninger kan i utgangspunktet være lagret hvor som helst i verden, og at andre regler kan gjelde i utlandet.

11.8 Noen banale sikkerhetsregler

Er du fersk på område og skal flytte deler av virksomheten IT-infrastruktur ut i en nettsky for første gang, anbefaler vi at du starter med å forsikre deg om følgende banale sikkerhetsregler som du bør følge som bruker av en nettsky for å unngå å datainnbrudd og problemer med Datatilsynet.

Datasikkerhet

SSL – Sørge for ende til ende kryptering. Alle data som sendes mellom nettskyen og deg som bruker må skje på en sikker linje (SSL), uansett om dataene overføres over Internett eller mobilnettet.

Avansert passord – All pålogging til nettskyen må skje med bruk av et avansert passord som består av over 10 tegn, har store og små bokstaver, pluss minst ett tall og spesialtegn.

Brute force protection – Pålogging serveren må ha en brannmur med brute force protection som f.eks. blokkerer er IP-adresse som har flere enn f.eks. 5 feil påloggingsforsøk.

Fil-kryptering – Foruten at selve linjen bør være kryptert, bør all sensitiv informasjon som sendes over Internett og lagres i nettskyen krypteres, slik at uvedkommende ikke kan åpne filen uten å kjenne krypteringnøkkelen.

Filrettigheter – Ingen fil-områder må under noen omstendigheter gis 777-rettigheter. Det vil si fulle skrive-lese rettigheter. Det gjør at hvem som helst kan laste opp og kjøre filer på nettskyen din. Noe som vil gi hackere tilgang til dataene dine i mange tilfeller.

Virus- og malware program – Serveren må ha et virus- og malware program som skanner alle filer som blir lastet opp og ned til nettskyen for virus, ormer, trojanere og annen malware.

Norske servere – Benytt aldri utenlandske nettsky servere. Ikke bare er dette ulovlig i mange sammenheng, men gjør også at du mister kontrollen og eierretten til dataene. Lagres dataene på amerikanske servere er det amerikansk lovgivning som gjelder for dataene dine og ikke norsk, jf. Snowden avsløringene.

Kryptert backup – Alle dataene som ligger i nettskyen bør det tas en backup av. Alle dataene i backupen bør komprimeres for å spare plass og krypteres for å gjøre det umulig for andre å åpne backupene uten krypteringnøklene. Backupen bør dessuten ligge lagret på en annen server eller i det miste på en annen partisjon.

Kilder: Kjetil Sander ++++