MacInfo
datasikkerhet

revidert aug 2010

hvorfor bør jeg være opptatt av data-sikkerhet?

Vi bruker datamaskiner hjemme og på jobb til alt mellom himmel og jord, fra nettbank til chatting. Selv om du mener det du selv holder på med ikke akkurat kvalifiserer til «Ultra Top Secret», så har du antageligvis ikke lyst til at fremmede skal lese e-mailen din, bruke din datamaskin til å angripe andre systemer, sende falsk e-mail fra din maskin, eller sjekke personlig informasjon, som f.eks. kontoutskrifter, som du har lagret på din harddisk.

Selv om du mener å ha sikret eget datanett-verk på beste måte, med løsninger som anti-virus, sikkerhetskopiering og brannmur, viser undersøkelser ute i verden at sensitiv infor-masjon som havner på avveie, ofte stammer fra bærbare datamaskiner og/eller hjemme-PC-løsninger med mangelfull sikkerhet.

Så særlig for deg som er hjemme- eller mobil databruker, er det viktig å være klar over hvor utsatt du kan være. Den følgende oversikt håper jeg kan bidra til økt forståelse og sikkerhet for deg selv, og derved en tørrere og bedre følelse for oss alle.

Inntrengere (også kalt *hackers*, *angripere* eller *crackers*) bryr seg ikke nødvendigvis om din identitet i seg selv. Men ved å få kontroll over din datamaskin kan de bruke den som base for å utføre angrep på andre datasystemer.

hvem vil bry seg med å bryte seg inn hos lille meg?

Ved å ha kontroll over din datamaskin kan de skjule sin egen identitet på nettet når de an-griper høyprofil datasystemer som stat, det militære og finansinstitusjoner. Så selv om du bare bruker datamaskinen hjemme «for spill til ungene» eller e-mail til tanter og onkler, kan du fortsatt være et interessant mål.


Nordmann (20) tok kontroll over 36 000 PCer

Gigantisk botnett.

På sporet etter DDOS-angrep

fra iT-avisen 18. april 2008

Inntrengere er kontinuerlig på jakt efter svakheter i eksisterende datasystemer (såkalte «hull»). Jo mer komplekse våre datasystemer blir, desto vanskeligere blir det å sjekke fullstendig alt og alle overalt mot alt. Det er derfor opp til deg som ansvarlig databruker å følge med på de siste sikkerhetsoppdateringene, og å få disse på plass. På din Mac får du automatisk beskjed om disse via *Sikkerhetsoppdatering*, og det er bare å si ja, takk.

http://www.

hvor lett er det å få adgang til min datamaskin?

Endel software har som standard innstillinger (default settings) som gir andre brukere tilgang til din maskin, hvis du ikke selv skifter oppsett. Windows har dessverre meget av dette, med flere åpne porter som standardinnstillinger. Eksemplene inkluderer chatteprogrammer som som lar utenforstående utføre kommandoer på din maskin, eller nettlesere som kan tillate noen å plasere skadelige programvare på din datamaskin, og som aktiveres når du klikker på dem.
Derfor er ord som *brannmur* og *viruskontroll* nøkkelord i datasikkerhet.

hva gjør en firewall...

En **firewall** (eller brannmur) i det virkelige liv skal hindre hindre brann i å spre seg videre til andre bygninger eller deler av bygninger. Innenfor datasikkerhet er firewall et system eller gruppe systemer som oppretter og vedlikeholder adgangskontroll mellom to nettverk.

Det er to hovedtyper: *Software firewall*: programvare installert på enkelt datamaskin, eller *Network firewall*: som er dedikert utstyr som sikrer flere datamaskiner i et nettverk. Begge typer gir brukeren muligheter for å definere tilgangsnivåer og adgangsrutiner til den eller de maskiner de beskytter.

virus og **spam**: temaet blir stadig viet stor oppmerksomhet i media, og PC-brukere er dessverre *svært* utsatt. Du skal ikke ha en PC lenge på nettet før det baller på seg med all slags styggedom.

Virus er lykkeligvis et *ikke-eksisterende* problem for Mac-brukere. Til nå har ikke et eneste virus for Mac dukket opp — og heller ingen Windows-lignende flom av spyware (nedlastede programmer som gjør ting bak ryggen din). *Faktisk finnes ingen Mac virus eller spyware.*

Men, men: efter at Mac nå også kan kjøre Windows, enten med *Boot Camp* eller med *Parallels*, må også Mac-brukere ta denne problematikken inn over seg, hvis de planlegger å kjøre dobbelt. Riktignok ikke fullt så belastende som for rene WIN-brukere, siden eventuelle angrep bare berører Windowsdelen.
[*les mer på macbasics.no > MacTips #33*]

hva er brannmur?

Innen datasikkerhet er en brannmur (eng.: firewall) et system eller gruppe systemer som oppretter og vedlikeholder adgangskontroll mellom to nettverk.

De fleste firewall opplegg for hjemmebruk kommer med forhåndsdefinerte sikkerhetsalternativer som det kan velges mellom.

Mac OS X *har egen innebygget firewall, og ekstra sikring gjennom File Vault.*
[>MacTips #73]

Apples FileVault

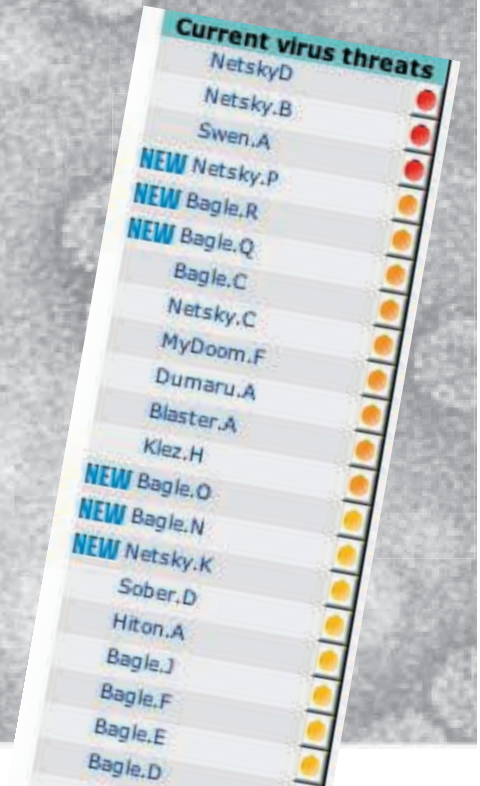
hva er virus...

virus: dette er fremmede programmer som skader eller ødelegger disketter, harddisker osv.; utviklet og sendt ut av datafreaker med dårlig moral. Ofte for moro skyld, og med relativt uskyldige resultater, men også skikkelig ondsinnede ting, som kan ødelegge hele datanett, lamme institusjoner og bedrifter, osv.

Grunnen til at dette kalles virus, er nettopp at du kan bli smittet uten å vite om det, og du kan også *selv* være smittebærer, uten å vite om det.
Dette gjør også at advarslene får et visst preg av meldinger fra Helsedirektoratet:
Vær kritisk til hva du putter inn i Mac-en din! Gå til kontroll regelmessig! La ikke fremmede tukle med Mac-en din! ...

Noen virus kan ligge skjult i systemet i lang tid uten at du merker noe, for så plutselig å slå til med blank skjerm, tom harddisk, osv. Andre kan gradvis bruke opp datakraften i systemet, ved at de tvinger maskinen til å reprodusere viruset, noe som merkes ved at maskinen og programmene efterhvert går langsommere o g l a n g s o m m e r e ...

Virus overføres som hovedsakelig som vedlegg til e-mail, men kan også følge spam. Og mailadressene henter både spammere og virusprodusenter fra adresseboken din (eller den til en som har deg i *sin* adressebok, og som ikke er like flink som deg til å passe på).



spyware er programvare som overvåker PC-en og stjeler informasjon fra den. Spyware kan overvåke og sende inn rapporter om dine surfevaner. Spyware kan også, dog langt sjeldnere, stjele sensitiv informasjon som brukernavn, passord og kredittkortnummer. Og den kan installere en rekke andre uønskede programmer.

adware er programvare som er spesielt laget for å pøse på med reklame når du surfer på nettet. Ofte registrerer Adware også dine surfevaner, men grenser da opp til spyware. Grensen mellom spyware og adware er smal, og mange programmer er kombinasjoner av disse to.

Nifse greier..

hvordan virker antivirus programvare?

Antivirus programvare settes opp på forskjellige måter, men felles for dem alle er at de ser efter mønstre i filer som indikerer mulig tilstedeværelse av et kjent virus. Antivirusprogrammet vet hva det skal lete efter ved hjelp av virus profiler. Nye virus oppdages daglig. Skal du ha et effektivt antivirusprogram, er det derfor ekstremt viktig at det er oppdatert med de siste virusprofiler.

På macbasics.no > machjelp finner du linker gode antivirus program, som f.eks. **AVG Antivirus** *eller* **Avast Antivirus.** *Et av de enkleste og rimeligste er ironisk nok Microsofts* **OneCare Live.**

hva er ondsinnede scripts?

Du kan utsette deg for ondsinnede scripts når du:

☛ *følger linker på websider, i e-mail eller i newsgroups når du ikke vet hva de linker til.*

☛ *hvis du bruker interaktive skjema på en uredelig website.*

☛ *følger online diskusjonsgrupper, forums, eller andre dynamisk genererte sider hvor brukerne kan sende tekst med HTML tags.*

hva er spam...

spam (eller junk-mail) defineres som all uønsket e-mail, som dropper uoppfordret i innboksen din, med tilbud om alt fra Viagra til billige lån. Spamming er masseutsendelser av slik mail, ofte til millioner av e-mail adresser samtidig. Spam og spamming er ikke direkte skadelig for din datamaskin, men irriterer i større eller mindre grad.

Den belaster imidlertid system, nettverk og mailservere omkring i verden. Spam og spamming kan sammenlignes med ubedt reklame (junk-mail) i postkassen hjemme. Spammerne støvsuger kontinuerlig på nettet efter aktive e-mailadresser (se ovenfor om Spyware).

De som regner på slikt sier at 40-50% av all e-mail i verden er spam (noen sier enda mer, opp til 70%) og tendensen er sterkt økende.

Spammerne bruker alle midler, også ulovlige, med stjålne identiteter osv., for å samle e-mail adresser. Egne søkeprogram (Spyware) ligger konstant ute på nettet og tråler efter gyldige e-mail adresser på alt fra nettsider til chatrooms og diskusjonsgrupper. *Spyware* og *Adware*, eller spionprogrammer og skjulte uønskede reklameprogrammer, har blitt et stadig større problem for PC-brukerne. Plagen har blitt så stor at en ny lov vedtatt i USA gjør det straffbart å spre slike programmer.

De svært irriterende og potensielt skadelige programmene er ofte umulig å oppdage for vanlige PC-brukere.

visste du?...

Opprinnelsen til navnet Spam er ganske spesiell: dert er opprinnelig navnet på det første hermetiske fabrikkfremstilte skinkeprodukt (SPiced hAM), tilsvarende vår «skinkeboks», meget brukt i det militære, og udødeliggjort gjennom en Monty Python sketsj hvor vikingene roper Spam, Spam stadig høyere og høyere, for å overdøve all annen konversasjon.

MacInfo

10 gode råd om datasikkerhet

1 invitér ikke ukjente med hjem...

Vær kritisk til hvordan datamaskinen din er konfigurert før du kobler den opp mot Internet. Det er spesielt viktig at du er oppmerksom på delte mapper/-ressurser. Du ønsker neppe å vise dine private data til hele Internettsamfunnet, noe som imidlertid kan skje dersom du deler dataene dine uforsvarlig. Ikke slå på fildeling hvis du ikke er helt sikker, og iallefall bruk passordbeskyttelse når du logger deg på.

Dette er et av de største sikkerhetshullene i Windows, og et som inntrengerne ofte benytter seg av. Slå av maskinen når den ikke er i bruk.

2 bruk et godkjent renholdsbyrå...

Installasjon av antivirusprogram er et elementært sikkerhetstiltak (gjelder PC-delen hvis du kjører dobbelt på din Mac). Sjekk din konfigurasjon, og at du vet hva den stopper av uhumskheter. Og ikke minst, sørg for all del også å oppdatere antivirusprogrammet regelmessig.

3 oppdater operativsystemet fortløpende...

Operativsystemet (OS) er kjernen til alt som foregår i datamaskinen din. Intet OS er 100% feilfritt, og virusmakerne utnytter alle feil de finner i programkoden. Microsoft og deres mailprogram (Outlook/ Entourage) har vært, og er, skikkelig utsatt her, og Microsoft sender jevnlig ut Security Updates som skal tette slike hull. Mac OS er som sagt pr. dato lykkelig fri for slikt, men her også oppdages ting. Derfor, også på Mac: sjekk Programvareoppdatering (Software Update) jevnlig, og si ja til det du får der.

4 ikke stol blindt på postvesenet...

Bruk sunn fornuft (og vær skeptisk). Kjenner du avsenderen?
Har emnefeltet (subject) et fornuftig tema?
Sjekk hvorhen i verden Internettkoblingen (linken) i e-mailen sender deg.
Slett e-mail med vedlegg som virker mistenkelige.

Åpne aldri, *aldri* vedleggene i mistenkelig e-mail (NB! Mac-en spør deg alltid først!).
Får du mail fra avsendere som *nia_tfc@yahoo.com*, med emne "hi" og tekst "Please read the "VirusWarning.txt" attachment(s) for more information", – *så ikke gjør det*.

...visste du?

at over 50% av nett-trafikken er spamming, og at tendensen er økende?

Når det bare koster 800 dollar å få kjøpt 15 millioner gyldige e-mail adresser, og samme melding så kan sendes til alle disse med et tastetrykk, får man et inntrykk av problemet...

Da "the Buffalo Spammer" ble arrestert, efter flere års efterforskning, hadde han rukket å sende ut over 825 millioner uønskede e-mails, til adresser han hadde tilegnet seg på ulovlig vis.

MacTips datasikkerhet / Paal Ovrum © 2008/2010

Men slik virusmail kan også komme fra folk du kjenner, med riktig adresse, så igjen: sjekk vedleggene, og åpne aldri hvis det ikke er noe du vet du skal ha.

Har du et filter for søppelpost (junk-mailfilter/spam filter) slipper du unna mye rydde-arbeide. Apples eget mailprogram «Mail», har et intelligent Junk Mail filter, som efterhvert lærer seg hva du ikke liker.

“-anybody home?”

Svar aldri på oppfordringer som «kryss her for å melde deg av postlisten» som du får på uoppfordret mail; dette er bare en sneaky måte for å finne ut om «det er folk hjemme», slik at spammeren kan bruke adressen din.

5 sjekk at du har en god dørvakt

Datamaskinen din har mange «inngangsdører» (porter) for forskjellige oppgaver. Porter kan slippe inn uønskede elementer. Windows kommer med åpne porter som«default», ikke helt den beste løsningen…
En «brannmur» har som hovedoppgave å beskytte din datamaskin mot uønsket inntrengning via Internet.
Hva har du hjemme?

6 lås arkivskap med sensitiv informasjon…

Lagre dine konfidensielle data *sikkert*. Dette er spesielt viktig for bærbare maskiner som lett kan komme på avveie. Bruk passordfunksjonen for pålogging. Den beste løsningen er å benytte krypteringsverktøy som håndterer både mapper og enkeltfiler. Nye Mac OS X har dette innebygget.
Mobile Mac-ere bør også aktivere skjermsparer med passord.
[> *MacTips #73*]

7 ikke slipp inn hvem som helst…

Sjekk at nettleseren din alltid spør deg om du vil tillate «aktivt innhold». Mange nettsteder benytter script for å forbedre surfeopplevelsen. Dette kan være en sikkerhetsrisiko, da det innebærer at programkode kjøres på din egen maskin. Vær selektiv i forhold til hvilke nettsteder som får slik tilgang til din datamaskin.

8 vær kritisk med hvem du omgåes…

Ikke putt alt du får «gratis», i datamaskinen din. Lettbrente CDer kan lett bli dyre, når nissen har flyttet med på lasset!
Bruk originalvare. Programvare fra folk du ikke kjenner (*og* folk du kjenner!) kan inneholde trojanske hester…

MacTips datasikkerhet © Paal Ovrum © 2008/2010

9 fortell minst mulig om deg selv...

Gi aldri fra deg mer informasjon av personlig karakter enn absolutt nødvendig. Bruk gjerne en ekstra e-mail adresse til bruk ved ulike forespørsler. Bruk f.eks. jobb-adressen til dette, og ha din egen private for alt annet.

Svar aldri på oppfordringer som «kryss her for å melde deg av postlisten»; dette er bare en smart måte for å finne ut «om det er folk hjemme».

10 ta sikkerhetskopi av riktig informasjon...

Data kan bli slettet ved uhell (— Oops!), virus eller annen ondsinnet kode. Ta backup (sikkerhetskopi) av viktige data regelmessig. Viktige data er egenproduserte filer som du har brukt tid og krefter på å lage.
[>*MacTips #36*]

Programvare og andre systemfiler kan alltid reinstalleres dersom disse skulle bli ødelagt (men husk: da får du ikke med deg alle oppgraderingene du med stor flid har lastet ned). Spander et par ekstra CDer på backup, eller skaff deg en separat harddisk, hvis du har mye å ta vare på — og gled deg over automatisk sjelefred med Time Machine.
Evig eies kun det tapte!

Husker du hvordan det gikk med lille Rødhette?
Det er to typer mennesker i verden: de som har mistet data, – og de som kommer til å gjøre det.

følg disse reglene:

- *det er ingen skam å spørre om råd*
- *bruk antivirus programvare (– og oppdater den!);*
- *sjekk at du har brannmurbeskyttelse der du jobber;*
- *åpne aldri ukjente e-mail vedlegg;*
- *laste aldri inn programvare med ukjent opprinnelse;*
- *slå av "hidden filename extensions" (for PC);*
- *oppdater all program-vare jevnlig, også operativsystem;*
- *slå av datamaskinen når du ikke bruker den;*
- *slå av scripting i e-mail program;*
- *ta jevnlig backup;*
- *lag en full backup du kan benytte hvis din datamaskin blir ødelagt eller kompromittert (boot disk)*

MacTips datasikkerhet / Paal Ovrum © 2008/2010