Sikkerhed på din private Computer.

Sikkerhed er ikke kun et spørgsmål om at have en firewall, mange andre ting kan gøres for at forbedre sikkerheden. Ofte er det et spørgsmål om at tænke sig om, og det kan faktisk gøres helt gratis hvis du vil

Skrevet den **03. Feb 2009** af **bufferzone** I kategorien **Sikkerhed / Generelt** | ★★★☆☆

Sikkerhed på din private Computer.

Sikkerhed på din computer kan sammenlignes med sikkerheden i et hus. Ligesom det ikke er nok at sætte alarm på hoveddøren, er en firewall heller ikke nok til at stoppe indtrængen i din PC. Nedenstående artikel er et bud på hvilke ting du bør kikke på, hvad du bør gøre, og hvor du kan finde relevante oplysninger og software.

1. Opdatering af alt. og jeg mener alt.

Når en hacker trænger ind i et system, gør han det normalt gennem huller systemet. Alt software har huller og sårbarheder, disse bliver fundet og lukket som tiden går af producenter og af hackere, men det er dig der skal sørge for at opdateringer de enkelte producenter udgiver, bliver kørt ud på dit system. Windows update er en rigtig god ting, og du bør altid sørge for at gennemføre total update af dit styrersystem før du tilslutter din maskine til nettet (Hvis du gør windows update personlig, kan du hente updateringerne ned på din maskine, så de efterfølgende kan indlæses f.eks. fra CD, uden at du først skal på nettet).
Et fuldt updated system er ikke blot mere sikkert i forhold til hackere, du slipper også for en masse forskellige orme, hvoraf de nyeste er begyndt at sprede sig via huller i dit system. Orme som Nimda, Code Red, Sorbig og Blaster er gode eksempler på orme der spredes via sårbarheder og huller. Også 2005 vil bliver et år med forskellige orme og andre mere eller mindre underholdende ting, så det er mere vigtigt end nogensinde at holde sin maskine opdateret.

Når dit styresystem er opdateret, skal du huske dine andre programmer. Officepakker kan opdateres nogenlunde ligesom Windows update. Du finder et faneblad med Office Update på siden for Windows update. For de programmer der ikke leveres af Microsoft, er du nødt til at holde dig orienteret på de enkelte producenters hjemmesider. Gør det til en fast rutine at kikke forbi jævnligt, hvis du ikke kan tilmelde dig et nyhedsbrev, der melder om nye opdateringer.

2. Fornuftige valg af software, især fravalg.

Hullerne findes i de enkelte programmer, det er således logisk at jo flere programmer du har installeret, jo flere potentielle huller har du. Dette betyder at du altid bør tænke dig om, før du installere programmer, installer kun de programmer du har brug for, og holder du op med at anvende et program, så afinstaller det.
For nogle typer programmer er det særlig vigtigt at tænke sig om, da disse programmer giver en hacker ekstra muligheder. Alle kommunikations programmer, f.eks. ICQ, Messenger, Pow Wow og Skype åbner nogle muligheder ud mod nettet. Det er de jo nødt til for at kunne virke som de skal. Samtidig er du nødt til at åbne for de relevante porte i din firewall for at dine kommunikationsprogrammer kan komme ud på nettet, og programmerne annoncere typisk din tilstedeværelse. Alt sammen en dårlig ide i forhold til hackerne.
Alle former for servere, især FTP-, Web- og Mail-servere, udgør et problem. En servers opgave er netop at give services til andre, og dette gør at de ofte kan udnyttes til uhensigtsmæssige ting. Faktisk sker de

fleste indbrud på nettet gennem disse tre servertyper. Hvis du absolut vil have en eller flere af disse servertyper kørende, så placer dem i DMZ (Demilitariseret Zone, læs mere om dette i en kommende artikel).
Fjern administrations programmer som VNC, PCAnywere og Damewere udgør altid et problem, fjernadministration er jo netop hvad en hacker ønsker at udføre, og har du allerede placeret værktøjer han kan anvende, gør du livet meget lettere for ham.
Alle former for p2p programmer udgør også en risiko, dels deler du dine ressourcer ud til andre, med fare for at du kommer til at dele for meget ud, dels bruges disse programmer til at hente ting ned på din maskine, ting der potentielt er farlige, og endelig annoncere de aktivt din tilstedeværelse på netter.

Alternative valg af programmer
Ofte kan du hjælpe dig selv ved at vælge anternative programmer til at løse forskellige opgaver. F.eks. bruger mange Internet Explore til at browse nettet med og denne browser gør da også dette godt. Desværre er der en lang række sikkerhedsproblemer med flere af Microsofts produkter, der betyder at du kan/bør vælge andre mere sikre produkter. Selv bruger jeg Firefox som browser og thunderbird som mail klient. Disse to alternativer fjerner en lang række sikkerhedsproblemer, uden at jeg savner funktionalitet. Overvej altid alternativer til det software du anvender, der er ogte sikre muligheder

3. Sikker konfiguration.

Sikker konfiguration af windowsmaskiner er et helt kapitel for sig selv. Microsoft levere standard windows med alt slået til og alle muligheder åbne for en hver. Dette betyder at du kan gøre rigtig meget for at sikre din maskine. For en fuld beskrivelse, se de meget gode vejledninger på http://www.nsa.org og http://www.microsoft.com/security Nogle enkelte ting kan du dog gøre som minimum:

- disabel Gæste accounten
- omdøb administrator accounten
- brug NTFS filsystemet på alle dine diske
- Bruge stærke passwords (mere end 10 tegn, både store og små bogstaver, tal og specialtegn)
- Meget meget mere, se de store vejledninger for inspiration.

4. Firewall.

Alle bør anvende en firewall, helst en ordentlig/rigtig firewall (her er vi ude i definitions problemer, men jeg taler om f.eks. en Cisco Pix, en Linux Netfilter box eller Symantec's Velociraptor) eller en personlig firewall hvis du er en privat bruger uden specielle sikkerheds behov. Sørg for at holde din firewall opdateret, hvilken firewall du vælger er ikke så vigtigt, bare du har alle punkter med i denne liste. Jeg vil anbefale at du kikker på Sygates personlige firewall, den er certificeret og gratis se http://www.sygate.com, og har du ikke noget i mod at betale lidt bør du kikke på BitGuard fra danske Callisoft (hedder Netop Desktop Firewall i dag). Denne firewall anvender en spændende teknologi og giver god sikkerhed, se http://www.danwaresecurity.com/.

5. Antivirus.

Virus bruges også af hackere til at komme ind på din maskine. Der findes forskellige vira der indlægger bagdøre på dit system, ligesom vira melder tilbage om systemer der har huller der kan udnyttes. En god fuldt opdateret virusscanner er en vigtig del at din sikkerhed, her bør du aldrig gå på kompromis. Du kan f.eks. anvende AVG, der kan downloades gratis her. http://www.grisoft.com/us/us_dwnl_free.php og der findes også mange gode købe Antivirus software, fra Mcafee, Norton, Panda og flere andre

6. Spyware/adware.

Spyware og ad ware er også et problem i forhold til din sikkerhed. Dels kan disse udnyttes til ting du ikke

er interesseret i og dels annoncere de din tilstedeværelse på nettet, hvilket du heller ikke er interesseret I. På http://www.spywarefri.dk kan du læse en masse om forskelligt software der beskytter dig og du kan få hjælp til at fjerne det du allerede har fået. Kik på programmerne Ad Aware og Spybot.

7. Logfiler og IDS.

Mange mennesker kikker aldrig i deres logfiler, hverken de "almindelige" logfiler, deres firewall logfiler, deres webserver logfiler eller andre logfiler der findes på deres computer. Dette er ekstremt dumt, da det giver enhver hacker god tid til at komme ind på computeren. Kontroller dine logfiler regelmæssigt og spørg, f.eks. på eksperten, hvis der er ting du synes ser underlige ud. Det er dine log filer der skal give dig de første advarsler når derer noget i gang. Du kan bruge et Intrution Detection System til at overvåge dit system for dig. Et IDS holder øje med dine logfiler samt med den trafik der køre på dit netværk, og giver dig en melding hvis der foregår noget systemet genkender som noget skidt, dette kunne f.eks. være en portscanning eller en sårbarhedsscanning med kendte værktøjer, eller andre former for exploits der køres af mod dit system. Et godt Gratis IDS system er Snort, der fås til både windows og Linux, se http;//www.snort.org.
Se også på Microsoft Log Parser, der er et lille program du kan downloade på microsofts hjemmeside. Den kan hjælpe dig med at udtrække det relevante for MS logfiler

8. Opfør dig ordentligt.

Mange dumme ting sker fordi en bruger opfører sig dumt.
Tænk dig om når du åbner e-mail, åben f.eks. aldrig vedhæftede filer fra folk du ikke kender, og åben aldrig vedhæftede filer at typen exe, com, bat, pl, eller andet format du ikke er helt sikker på hvad er. Modtager du den slags, så skriv tilbage til afsenderen og spørg om det er korrekt at du skal have denne mail, og hvad den vedhæftede fil er for noget.
Tænk dig om når du installere programmer, mange af de gratis programmer du kan downloade fra nettet eller får med gratis når du køber computerblade, indeholder spy ware, ad ware og bagdøre. Undlad at installere dette på internetmaskiner, lad helst helt være med at installere den slags.

9. Spørg og spørg igen.

Brug eksperten, spywarefri og andre fora til at spørge hvis du føler dig usikker. Spørg hellere en gang for meget end en gang for lidt. Tænk dig om hvordan du spørger, der er ingen grund til at offentlig gøre konfigurationsdata, tilstedeværelsen af sårbarheder og bagdøre på dit system og passwords til dette og hint.

Hvis du har spørgsmål og/eller kommentarer, er du selvfølgelig velkommen til at bruge eksperten, ligesom du altid kan kontakte mig på kim@bufferzone.dk

Kommentar af karsten_larsen d. 27. Jan 2004 | 1

Fin artikel - giver et godt overblik med handlemuligheder

Kommentar af hschak d. 04. Feb 2004 | 2

En Rigtig god artikel. Og lige som de andres mening burde den bruges af Alle.

Kommentar af athlon-pascal d. 15. Jan 2004 | 3

Super artikel :o)

Kommentar af ducks d. 20. Jan 2004 | 4

Som fremsej siger, gid flere ville bruge dem, men mange synes desværre det er for besværligt og nogen er fuldstændig ligeglade.

Kommentar af blackadder d. 05. Aug 2004 | 5

Velskrevet artikel. Gode råd.

Kommentar af triple-x d. 01. Jul 2004 | 6

god artikel, dog synes jeg at punkt 7. logfiler og IDS, det er jo ikke fordi folk ikke har lyst til at kigge i disse log, men tvivler på der er ret mange der ved hvilke logs man skal kigge i hvor de ligger og hvad det betyder det der står i dem.
Ellers utrolig dejlig artikel, men plejer dine artikler og svar også at være

Kommentar af barbarbo d. 14. Jan 2004 | 7

Rigtig god artikel, Bredere perspektiv end man er vandt til. Gode råd

Kommentar af nicidem d. 18. Feb 2004 | 8

Kommentar af jochrisyogi d. 06. Feb 2004 | 9

Endelig en artikel skrevet for almindelige folk, med mange fine råd.

Kommentar af fromsej d. 12. Jan 2004 | 10

Udmærkede tips, gid flere ville bruge dem.

Kommentar af ravsted_dk d. 26. Jan 2004 | 11

Kommentar af morty d. 15. Jan 2004 | 12

Kommentar af sqren d. 22. May 2004 | 13

Rigtig god artikel, men kan ikke lade være med at drille hehe...:
"Windows update er en rigtig god ting, og du bør altid sørge for at gennemføre total update af dit styrersystem før du tilslutter din maskine til nettet."
Ved ikke hvordan du vil opdaterer totalt FØR du er tilsluttet til nettet... ;)

Kommentar af arlet d. 12. Jan 2004 | 14

Kommentar af serverservice d. 21. May 2005 | 15

godt sammenkog omkring sikkerhed på en pc og synes de vigtige ting er med + lidt ekstra - vil se lidt mere på hvad IDS kan i fremtiden.

Kommentar af fieklokke d. 31. Jan 2004 | 16

Kommentar af baxos d. 09. Aug 2004 | 17

Meget nice!

Kommentar af knighten d. 20. Jan 2004 | 18

Rigtig godt - på et niveau så alle forstår.

Kommentar af scramer d. 15. Jan 2004 | 19

Fin artikel

Kommentar af draco999 d. 09. Feb 2004 | 20

ok artikel

Kommentar af chodeof72 d. 05. Apr 2004 | 21

;-P

Kommentar af karsberg d. 16. Oct 2004 | 22

Kommentar af j_mortensen d. 27. Mar 2004 | 23

Kommentar af sorenbs d. 11. Jan 2005 | 24

Kommentar af bjarne003 d. 29. Aug 2004 | 25

"Modtager du den slags, så skriv tilbage til afsenderen og spørg om det er korrekt at du skal have denne mail, og hvad den vedhæftede fil er for noget."
Det skulle måske lige nævnes, at det ikke altid er en god ide. Mange vedhæftede filer kommer sammen med spam. Skriver du tilbage på en spam-mail, ved spammeren at mail-adressen er aktiv, og så får man bare endnu flere uønskede mails.

Kommentar af i865 d. 17. Oct 2004 | 26

En artikel, som den alm. pc bruger bør have som bilag til sin pc manual!

Kommentar af visualdeveloper d. 19. Dec 2004 | 27

ok

Kommentar af maijen d. 05. Feb 2005 | 28

Rigtig god artikel...

Kommentar af mtj111 d. 19. Feb 2006 | 29

Tjah... Måske lidt for generel; jeg kunne godt bruge nogle flere uddybelser og ikke mindst en lille vejledning til nogle småting...

Kommentar af mo-od d. 29. Mar 2005 | 30

Kommentar af st3ff d. 07. Mar 2006 | 31

God artikel

Kommentar af phpzer0 d. 28. May 2006 | 32

Rigtig od artikel!