

Dette er en underside til: <http://www.oz1dis.dk/>

## **Desværre virker det ikke som om alle Computerbrugere forstår problemet : uvidenhed er farligt.**

Tja - folk købet en PC, og efter et par dages tid ved tastaturet, så føler de sig fulbefaren til at udforske verden.

Mest af alt tror jeg de skal være glade for en del andre har gjort en stor del af arbejdet for dem, der findes ikke mange nye pc'er uden de leveres med en eller anden Internetsecurity pakke, så brugerne som skal ud og se hele verden via deres PC, trods alt burde være nogenlunde sikret.

Desværre - så viser ikke bare mine check, at folk stadig tror en alm antivirus, + en firewall og måske endelig en spyware remover, så er ens PC sikret.

Tja - det var udmærket engang, men ikke i dagens Danmark.  
Her er det som var ok i 2006 - noget der idag er tudsegammelt når vi snakker om PC'er på internettet.

Det sidste års tid er truslerne ikke kun kommet via email mv - men især når vi browser og surfer i vores udforskning af internettet.

Tænk bare på hvor tit man bruger google til at finde et eller andet - og næsten ukritisk klikker på de links som Google har fundet.

Kan det da være farligt?????

Ja - i allerhøjeste grad - især hvis man ikke har opdateret sin pc, ikke bare sit styresystem ( måske XP ) men sandelig også alle de hjælpe programmer som adobe reader, adobe flash, adobe shockwave, en række aktive X, java i mange afskygninger samt alle de andre ting som dem der laver hjemmesider kan finde på vi skal anvende.

Her er det at en fornuftig omgang med sikkerhed på ens pc, starter med at man installere en fuld Internet security pakke for så svarer det da til at man har fået en regnfrakke på, så ikke alt vand gennembløder ens tøj.

Når man så har haft gang i et eller andet der kræver installation af et aktivtx eller lignende, - så skal man huske at lukke hullet det efterlader når man er fædig med det som krævede dette hul..  
Hvis ikke gør det, så svarer det til at man lader døre og vinduer stå åben når man bevæger sig ud i hård storm og høj sø, hvorved en masse vand kan komme ind og ødelægge en masse inventar og lign.  
Bliver "båden fyldt over et vist punkt, så mister den sødygtighed" - og så opstår den situation hvor man skal reddes..

Redningen kan være en bedre form for scanner end den antivirus man startede med, som kan klare at få alt det som ikke hører til fjernet fra ens pc - og straks tror man at nu er ens pc klar igen til at man kan fortsætte rejsen..  
Men de fleste online scannere - de installere et ny aktive X - tilpasset netop det at have fuld adgang til hele pc'en så hvis man ikke husker at lukke dette hul efter brug, tja - så er man endnu dårligere stillet.

Så for at kopiere lidt mere fra Søsporten... kun en tåbe frygter ikke Internettet, og så spørger jeg - er det dig????

Uvidenhed om hvad der skal til for at have en sikker pc - tja det er nok den største fare..  
Brug idet mindste en opdateret version af Secunia's PCI - den findes i release candidate 3 nu - og hvis en tidligere version viste man havde en fuld sikret pc, så afslører den nyeste PCI nyle huller.. men desværre - den kan ikke selv opdatere sig selv..

Nå men vanen tro så er her et par historier som i bør læse..

# Webtrafik er farligere end e-mails

[Datakriminalitet](#), [Overvågning](#), [Sikkerhed](#)

Falske websites er efterhånden en større trussel end virusbefængte e-mails. Sikkerhedsfirma mener at spamfiltre og antivirus giver falsk tryghed.



Af [Karim Pedersen](#)

mandag 7. juli 2008, 11:30

It-sikkerheden er i højere grad truet af medarbejdernes internetadfærd end af virusbefængte e-mails. Det mener sikkerhedsleverandøren Websense, som samtidig konstaterer at spamfiltre, firewalls og antivirus giver falsk tryghed. I stedet er det nødvendigt at blokere helt for adgangen til sites, der truer sikkerheden.

Ifølge Websense er en tredjedel af alle underholdningssites på nettet fyldt med malware. For at kunne læse informationerne eller se billederne på sitet bedes man downloade en lille fil. Som tak kvitteres med skadelige kode.

»Ifølge Forrester Research sker 80 pct. af al datalækage fra virksomheder på grund af utilsigtet, men uhensigtsmæssig brugeradfærd. Derfor er det ikke tilstrækkeligt at indføre regler for god internet- og mailsik, for i langt de fleste tilfælde har medarbejderne ikke en chance for at vide, hvor usikkerhederne opstår,« siger Kim René Jensen, der er territory manager i Websense, Danmark.

Han tilføjer at de mange web 2.0 tjenester har gjort problemet endnu værre. Populære websites som Facebook, MySpace, iGoogle og Microsofts live.com importerer et hav af små applikationer alle steder fra, bl.a. underholdende tests, som brugerne flittigt downloader og sender videre.

»Som bruger har man ingen chance for at vide, hvor applikationerne stammer fra, og hvad deres ærinde i virkeligheden er,« siger Kim René Jensen.

Hverken firewalls eller antivirus kan beskytte tilstrækkeligt mod denne form for trusler, mener firmaet, som selv sælger beskyttelses-programmer.

»Nøjagtig som dengang København endnu var en befæstet by, og fire byporte udgjorde indgangene til byen. Voldene og murene omkring byen kunne holde en del røvere væk på samme måde som antispamprogrammer kan holde mailboksen fri for indbrudstyre. Men uden vogtere ved byens fire byporte ville der være fri passage ved hovedindgangen,« siger Kim René Jensen.

# Online virusscanner gennemhuller Internet Explorer

En sårbarhed i ActiveX-plugin'en Panda ActiveScan gør Internet Explorer sårbar overfor et bufferoverflow-baseret angreb, lige som det også er muligt for ondsindede personer at installere cab-filer på klienten.

Af [Jakob Møllerhøj](#), mandag 07. jul 2008 kl. 13:40

EMNER: [Datakriminalitet](#) [Sikkerhedshuller](#) [Sikkerhedssoftware](#) [Browsere](#)

Så er den gal igen med en ActiveX-komponent i Internet Explorer.

Som udgangspunkt er det meningen, at antivirus-produkter skal gøre pc'en mere sikker. Men nu oplyser sikkerhedsvirksomheden CSIS, at der er fundet flere sikkerhedshuller med antivirus-produktet Panda ActiveScan 2.0, som gør det muligt at eksekvere ondsindet kode på klient-maskinen.

Panda ActiveScan er en ActiveX-komponent, der bliver installeret hos Internet Explorer-brugere, når de besøger Pandas [hjemmeside](#) for at online-scane deres [computer](#) for vira. Sikkerhedshullet i komponenten gør det både muligt at køre kode på klienten via et bufferoverflowbaseret-angreb, og så er det også muligt at installere såkaldte cab-filer på klientmaskinen.

»Cab-filer er egentlig et Microsoft-format, som i princippet er binært. Det vil sige, at den kan indeholde installationsopgaver, og den kan indeholde programkode, der automatisk installerer en bagdør på systemet. Det er den ene. Den anden er, at der er et bufferoverflow i den selv samme ActiveX-komponent, som gør det muligt at køre kommandoer direkte på systemet,« siger Peter Kruse fra CSIS til Version2.dk.

Desuden oplyser han, at CSIS endnu ikke har registreret, at sårbarhederne er blevet udnyttet i praksis, men Peter Kruse er dog ikke i tvivl om, at det kan lade sig gøre.

Den skadelige ActiveX-komponent kan identificeres ud fra følgende CLSID:  
41524153-46FB-488C-8E53-7624AB83C46F.

Panda har nu lukket hullerne i komponenten, hvilket betyder, at brugere, der besøger Panda igen for at blive scannet, får den opdaterede version installeret. Det er også muligt at blokere for den farlige udgave af ActiveScan ved at sætte en killbit for CLSID'et, hvilket er beskrevet i nedenstående link.

Endeligt er det muligt at sikre sig ved at deaktivere active scripting i Internet Explorer for websider, man ikke har eksplicit tillid til

# Vrede mænd

Af [Kåre Kjelstrøm](#), mandag 07. jul 2008 kl. 12:00

EMNER: [Backup Hacking](#) [Sikkerhedshuller](#) [Webapplikationer](#)

Der dumpede en email ind i min mailbox for et par dage siden fra en af mine kolleger med den dramatiske titel "Vapor Trails - Hacked !". I mailen var en kort tekst, der fortalte at min gamle blog <http://www.vaportrail.dk> var blevet hacket af vrede mænd.

I mailen var også et screenshot af det ulykkelige site, hvor hver eneste af mine +50 blogentries var blevet overskrevet med teksten "Stop your fitna & propaganda against ISLAM. Why we are here? because, to show you, that TRUTH can not be ignore & ISLAM is the TRUTH". Jeg var blevet ramt af et "[defacement](#)" angreb.


Jeg loggede straks på sitets web baserede administrationsmodul og kunne konstatere at mit gamle password fint virkede, at alt så normalt ud bortset fra at hver evig eneste felt og titel i den tabel der indeholder blog-posts var blevet overskrevet.

Siden jeg begyndte at skrive på Version2 har jeg ikke brugt den gamle blog, men blot ladet den være. Sitet kører [Wordpress](#) og på det tidspunkt i en version fra december 2006, hvilket i Internettet betyder at den var tudsegammel. En hurtig søgning på "sql injection wordpress" afslørede da også at den slags problemer åbenbart til stadighed finder vej ind i produktet omend de bliver patchet løbende.

Efter en halv times arbejde havde jeg fået rådet bod på problemet, patchet Wordpress og genetableret databasen med den nyeste backup jeg havde til rådighed. Desværre var forsidens nyeste entry efterfølgende fra februar 2006, sidste gang jeg tog backup.

Nu var jeg pludselig en anelse svedt ved tanken om at 20 måneders skriblerier var tabt for altid og tog en tre-fire ture rundt i stuen i koncentriske cirkler før det pludselig slog mig: Google har en cache. Cachen udgør et snapshot. Cachen indeholder måske den gamle forside!

Og ganske rigtigt. Google havde været så elskværdige at gemme alle mine entries fra 2007 samt af uvisse årsager den fra april 2006, så nu er jeg nede på at mangle i omegnen af 7-8 indlæg. Hvis

nogen mod forventning skulle ligge inde med dem er der en dusør 

Der er i hvert fald et par moraler i denne anekdote fra det virkelige liv:

- 1) Der er vrede mænd derude, som åbenbart bruger tid på at finde sårbarheder i open source software. Truslen er reel.
- 2) Hvis du vil mindske risikoen for hacking, defacement etc. er det en god idé at holde dit website software opdateret med nye sikkerhedspatches - også selv om du ikke bruger det mere.
- 3) Skulle uheldet alligevel være ude er det rart at have en rimelig frisk backup af site software, databaser, etc.

Så kan jeg lære det!