

Denne underside kommer fra  
<http://www.oz1dis.dk/>



# Ekspertter: Afbryd ActiveX omgående

**Flere nye angreb via sårbare ActiveX-komponenter og et hav af angreb i 2007 får nu eksperter til at advare generelt mod Microsoft-komponenten ActiveX.**

Af [Jakob Møllerhøj](#), 6. februar 2008 kl. 10:40

Sikkerhedseksperter anbefaler nu, at man helt afbryder muligheden for afvikling af såkaldte ActiveX-komponenter, der er programmer, der kan køre via Microsofts Internet Explorer.

Baggrunden er en stribe af angreb, der udnytter huller i ActiveX-komponenter.

Alene i 2007 er der ifølge den danske sikkerhedsvirksomhed Secunia fundet 339 sårbarheder, som relaterer direkte til ActiveX-komponenter.

»Man får dem alle mulige steder fra, uden man nødvendigvis er vidende om, at de kommer ind på dit system. Så det er et voldsomt stort problem,« siger teknisk direktør Thomas Kristensen fra danske Secunia.

Senest kan amerikanske Computerworld fortælle om en række nye exploits fundet i ActiveX-komponenter brugt af brugere på Facebook og MySpace. Sårbarhederne gør det, som den slags har for vane, muligt for en hacker at overtage kontrollen med en klientcomputer. De nye huller har fået flere amerikanske sikkerhedseksperter til at anbefale brugere helt at afbryde alle ActiveX-controls.

## **Benytte højeste sikkerhedsniveau**

Thomas Kristensen mener også, der er grund til at passe på. Han opfordrer til, at brugerne som udgangspunkt benytter højeste sikkerhedsindstilling i Internet Explorer, hvilket forhindrer brug af ActiveX-komponenter i browseren.

»Selvom det kan være lidt irriterende, når man sidder og surfer, så bør man helt klart sætte den til, at man har den mest restriktive sikkerhedszone generelt, og at det er den indstilling, man surfer alle web-sites med. Web-sites, man har tillid til, som version2.dk, dem kan man gå ind og tilføje til en trusted zone,« siger sikkerhedseksperter.

### **Burde være sikker fra starten**

Thomas Kristensen erkender dog, at der skal en del til, før en bruger finder vej til sikkerhedsindstillingerne på Internet Explorer og aktivt ændrer på settings. Derfor ville han også ønske, at Microsoft som default havde sat Internet Explorer op til at køre med højeste sikkerhedsniveau.

Et af problemerne med ActiveX er ifølge Thomas Kristensen, når tredjepartsprogrammer inkluderer ActiveX-komponenter og registrerer dem som 'safe-for-scripting'. Dette bevirker i mange tilfælde, at ActiveX-komponenter, der ikke er designet til at blive kaldt igennem Internet Explorer, kan kaldes af alle web-sites.

### **Brug Firefox**

Sikkerhedseksperter nævner også en anden mulighed. Næmlig at køre med en kombination af browseren Firefox, der ikke som standard understøtter ActiveX og så benytte Internet Explorer, hvor det er nødvendigt.

»Det er også en mulighed at benytte Firefox, mens man surfer rundt, og så skifte til Internet Explorer, hvis det er nødvendigt for at en side fungerer ordentligt,« siger han.

Endeligt opfordrer Thomas Kristensen til at sætte Windows op med flere brugerkonti.

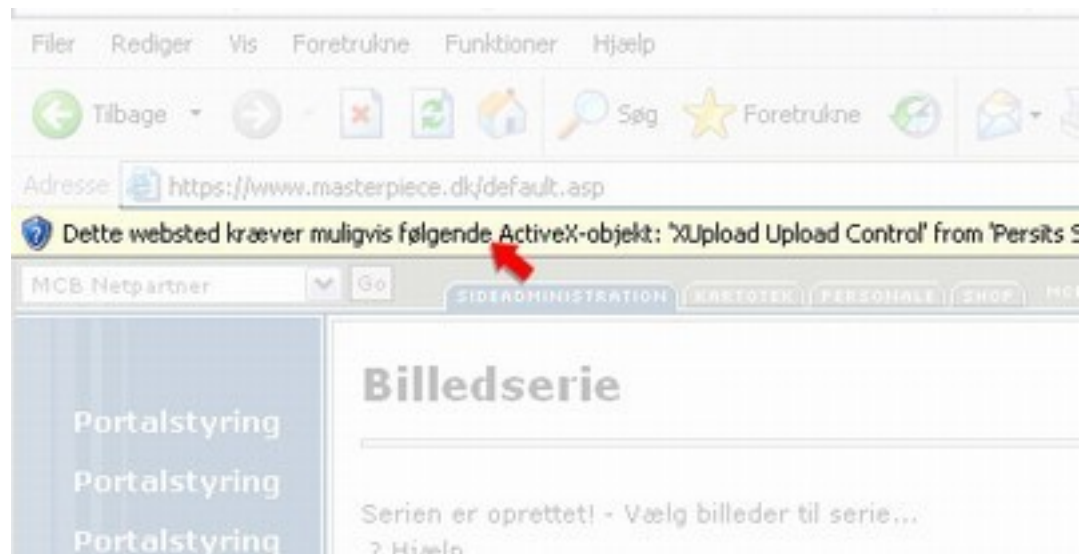
### **En restriktiv konto til internet-surfing og en anden konto til øvrigt computerbrug.**

---

[Se – de fleste kender vel aktive X på denne måde...](#)

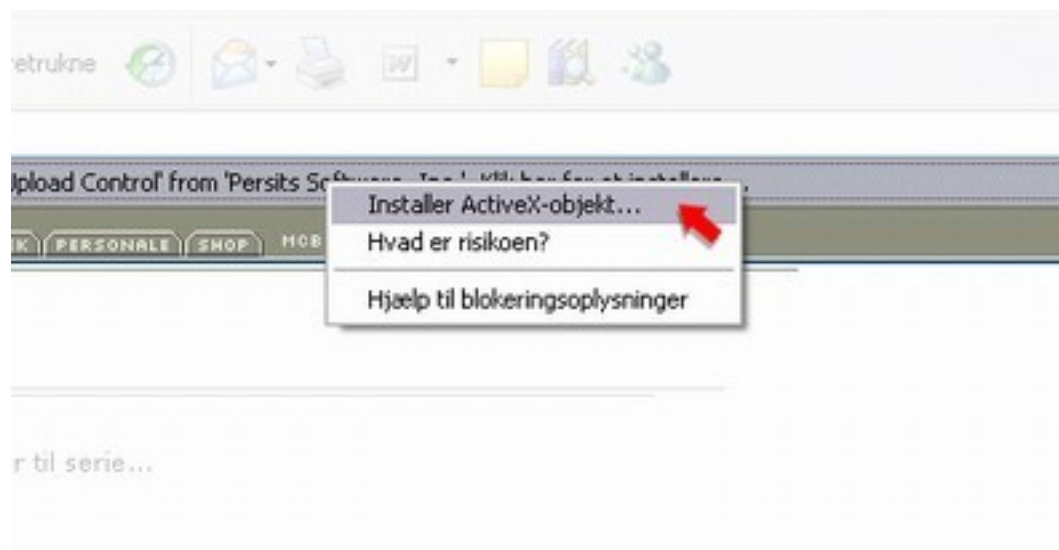
## Installation af active X objekt

### Trin 1



Kommer vinduet ikke frem, vil der efter kort tid dukke en menu bjælke op under adresse linien. Som vist herunder, tryk på den.

## Trin 2



Efter du har trykket kommer der en lille menu frem. Her vælger du knappen ”Installer ActiveX-objekt..”



Vælg installer. Når installationen er afsluttet skulle vinduet blive vist, så du kan komme til at lægge dine billeder op. Kommer vinduet ikke, vil vi anbefale at Marsterpiece lukkes helt ned og åbnes på ny hvorefter vinduet dukker op.

**Men, Men, men men..... tænk meget over det næste.....**

**DirectX: En ny multimedie API til Windows. Det er en samling programmer, der giver spil og andre multimedie-programmer meget større kontrol (low-level-kontrol) over hardwaret. DirectX omfatter: DirectDraw, DirectSound, DirectSound3D, DirectPlay, DirectInput, DirectSetup. Alle disse programmer er beregnet på, at spil og andre multimedie-programmer kan udvikles med effekter indenfor lyd og billede. Fordelen med DirectX er, at programmerne kan skrives direkte til Windows og samtidig opnå maksimal kontrol over hardware.**

Problemet med Active X – og sikkerhed, er at Microsoft har flyttet kontrollen af hvad Active X må og ikke må, - og om brugeren skal spørges, eller ej, **ud til programmøren.**

Den pæne programmør, vil gøre som det herover, men den som har u-ærlige hensigter, vil helt undlade dette.

Selv om man så benytter sig af muligheden til at trimme i browserens sikkerhedsindstillinger, som omtales i det efterfølgende , så browserens kun acceptere sikre og klassificerede Active X, så er det programmøren som fastsætter hvad hans Active X skal klassificeres som, så derved er al kontrol overladt til programmøren.... **Tankevækkende - meget tankevækkende...**

**Det virker som om Microsoft helt har misset et væsentligt sikkerheds problem her, og kun troet på at det vil blive brugt på en pæn og ordentlig måde.**

**Værre bliver det når programmøren – binder alle de sjove faciliteter sammen, Java, Active X, PHP , Perl-script etc... og benytter dem via Dot.NET funktionen, - som er en basis del af styresystemet, for så er der ingen begrænsninger i hvilken browser man anvender, Internet Explore, Firefox, Opera, etc.. – der er frit spil ind på ens computer, især hvis man benytter en bruger med administrative rettigheder, men selv denne funktion kan omgås, dersom man ikke har passwordbeskyttet sin administrator adgang...**

**Nu er jeg ikke selv ekspert i Dot.Net i de forskellige versioner, eller dens afløser ASP.Net, – men mon ikke der også findes en række kommandoer – som kan bruges til at omgå mange funktioner i XP, så Active X alligevel kan benytte systemkommandoer, uden at være i administrator mode.... – men her er lidt viden velkommen ...**

**Tager man de mange online Virusscannere – så laver de da også mange ting på ens pc, alene styret af Active X.. så derfor spørger jeg, hvad kan man egentlig gøre via denne funktion.???**

**Et eks på at der er udvikling inden for dette, ses i det nyeste tiltag fra Microsoft, -**

**Silverlight, hvor man tilbyder komplet service mod vira, orme og meget andet, alt sammen via ASP.net i en automatiseret online funktion... så nogen form for harddiske access er åbenbart mulig, og når man tænker på hvad andre programmer kan via Active X, så er dette produkt fra Microsoft næppe bagud mht muligheder.**

**Hvad andre så senere kan få ud af ASP.Net – tjaa det må tiden vise, men vi har nok ikke set det værste endnu.**

**Måske var det en slags forsmag på denne fagre nye verden, vi så ”in live” dengang Vista blev hacket i fuld offentlighed, lige efter den første frigivelse.. her mangler jeg en link...**

**Vista har en funktion – hvor man skal bekræfte brugen af system kommandoer – men de fleste brugere føler sig generet af den slags pop-up vinduer, og slår den funktion fra, så mon ikke man kan tolke det således, at brugerne ikke interesserer sig for noget sikkerhed de ikke forstår, og helst ikke vil bruge tid på at sætte sig ind i.**

**Det største problem jeg ser med dette – er at man gladelig har kopieret disse funktioner over i andre styresystemer, så jeg tror kun det er et spørgsmål om tid for problemet findes i såvel Linux, Unix og på Mac.. –**

## men igen – jeg savner lidt viden til en uddybelse af disse punkter.

-----  
Fra [www.cert.dk](http://www.cert.dk)

### SIKKERHED I BRUGEN AF ACTIVEX

Den 22-23 august 2000 var CERT Coordination Center i USA vært for en workshop, hvis formål var at identificere de situationer, hvor ActiveX og lignende teknologier kan bruges sikkert og producere en rapport indeholdende sikkerhedsbetragtninger anvisninger. Denne rapport er offentliggjort på [CERT CCs hjemmeside.](#) □

”ActiveX control” er Microsofts betegnelse for en Component Object Model (COM) baseret teknologi. Teknologien bruges i de fleste programmer på Microsoft Windows platformen, specielt i de web-baserede programmer.

ActiveX er binær kode, der kan udføre de samme funktioner på maskinen som brugeren. ActiveX er ikke et lukket system, og det er derfor meget vigtigt, at man har fuld tillid til den, der har fremstillet ActiveX kontrollen.

Konklusionen på Workshopen er at sikkerhedsspørgsmål relateret til ActiveX ikke kan ignoreres. ActiveX er en integreret og væsentlig del af mange systemer og programmer og det er derfor væsentligt, at man har tilstrækkelig viden omkring funktionaliteten og sikkerhedsrisikoen ved at anvende ActiveX, til at kunne tage velkvalificeret stilling til det ønskede risikoniveau ved at anvende ActiveX.

Rapporten fra CERT CCs workshop indeholder informationer, der kan hjælpe til at tage det rigtige valg for den enkelte.

Rapporten

- Klarlægger visse misforståelser omkring ActiveX
- Diskuterer sikkerhedsanliggender og risici
- Beskriver de fordele, der kan have betydning for beslutningen
- Lister de sikkerhedsforanstaltninger, der kan tages, når man vælger at anvende ActiveX

Rapporten indeholder vejledninger til ledelse, systemadministratorer, sikkerhedspersonale, udviklere og brugere.

<https://www.cert.dk/vejled/activexogjava.shtml>

ActiveX og Java-scripts er teknologier, der ofte ses anvendt i forbindelse med angreb fra Internettet. Det er dog muligt for brugeren selv at gøre noget for at minimere risikoen, for at blive udsat for utilsigtet aktivitet med de nævnte teknologier.

Sikkerhedsjusteringen sker i Internetindstillinger, som man får adgang til via Start -> Indstillinger -> Kontrolpanel -> Internetindstillinger. Vælg fanebladet 'Sikkerhed'.

Det er op til den enkelte, hvor højt sikkerhedsniveauet skal være, hvis man sætter indstillingerne til det højeste sikkerhedsniveau mister man samtidig store del af den funktionalitet de to teknologier yder.

Indstillingerne gælder for både Internet Explorer og Outlook/Outlook Express. Vejledningen er skrevet ud fra en Internet Explorer version x.x og Outlook version x.x, men der er ikke den store forskel i indstillingsmulighederne for andre versioner.

Under Internetindstillinger findes forskellige zoner; Internet, Lokal Intranet, Websteder, du har tillid til og Klassificerede Websteder. Den mest interessante er Internet, men de andre kan indstilles efter samme retningslinier, hvis det ønskes.

Marker "Internet" og klik på "Brugerdefineret niveau". Et vindue med et væld af valgmuligheder åbner.

### **ActiveX-objekter og plug-ins**

1. "Aktiver scripting af ActiveX-objekter, der er markeret som sikre". Den er som udgangspunkt aktiveret. Det sikreste er at deaktivere denne funktion, men dermed vil en del sider og e-mail blive vist ukorrekt. Et alternativ er at vælge 'Spørg', dermed vil man have et valg, og samtidig blive i stand til at danne sig et overblik over i hvilket omfang, det bliver brugt.
2. "Hent ActiveX-objekter uden signatur". Den er som udgangspunkt deaktiveret, og bør være det.
3. "Hent signerede ActiveX-objekter". Den er som udgangspunkt sat til 'Spørg' og det er det bedste valg.
4. "Initialiser og aktiver scripting af ActiveX-objekter, der ikke er markeret som sikre". Den er som udgangspunkt deaktiveret, og bør være det.
5. "Kør ActiveX-objekter og plug-ins". Den er som udgangspunkt aktiveret. Det sikreste er at deaktivere denne funktion, men dermed vil en del sider og e-mail blive vist ukorrekt. Et alternativ er at vælge 'Spørg', dermed vil man have et valg, og samtidig blive i stand til at danne sig et overblik over i hvilket omfang, det bliver brugt.

### **Brugergodkendelse**

1. Brugen heraf afhænger af forholdene i forbindelse med computerens anvendelse og opkobling.

### **Cookies**

1. Cookies indebærer ingen særlig risiko

### **Diverse**

1. Disse funktioner har størst interesse for systemadministratorer og brugere i et netværk og opsættes derfor individuelt afhængigt af dette.

## Microsoft VM (Virtual Machine)

1. "Java-tilladelser". Den er som udgangspunkt markeret til "Høj sikkerhed" men kan som en yderligere stramning af sikkerheden deaktiveres, dog med tab af funktionalitet.

## Overførsler

1. "Filoverførsel". Funktionen er som udgangspunkt slået til, hvilket ud fra et sikkerhedsmæssigt synspunkt ikke er heldigt. Da det eneste alternativ er at slå det helt fra, hvilket ikke er særligt funktionelt, anbefales det at lade det være slået til, men at vise omtanke, når man henter filer fra Internettet.
2. "Overførsel af skrifttyper". Udgør ingen fare.

## Script

1. "Active-scripting". Den er som udgangspunkt aktiveret. Det sikreste er at deaktivere denne funktion, men dermed vil en del sider og e-mail blive vist ukorrekt. Et alternativ er at vælge 'Spørg', dermed vil man have et valg, og samtidig blive i stand til at danne sig et overblik over i hvilket omfang, det bliver brugt.
2. "Scripting af Java-applets". Den er som udgangspunkt aktiveret. Det sikreste er at deaktivere denne funktion, men dermed vil en del sider og e-mail blive vist ukorrekt. Et alternativ er at vælge "Spørg", dermed vil man have et valg, og samtidig blive i stand til at danne sig et overblik over i hvilket omfang, det bliver brugt.
3. "Tillad indsættelser via script". Den er som udgangspunkt aktiveret. Det sikreste er at deaktivere denne funktion, men dermed vil en del sider og e-mail blive vist ukorrekt. Et alternativ er at vælge "Spørg", dermed vil man have et valg, og samtidig blive i stand til at danne sig et overblik over i hvilket omfang, det bliver brugt.

Lidt info fra ordbogen om IT... : <http://www.multimediatek.dk/supl/pomaFiles/ordbog.html>

**Applet:** Afledt af applikation - en lille applikation, oftest et program der automatisk hentes og udføres i en browser, men hvis programkode er adskilt fra websidens øvrige indhold (i modsætning til et script der udgør en del af teksten i websiden).

**ASP:** Active Server Pages. ASP er en dokumenttype, som Microsoft lancerede i forbindelse med udgivelsen af Internet Information Server 3.0 i foråret 1997. ASP er et hybrid-format, hvor HTML-kode og programmeringskode (script-kode) forenes i samme dokument - et dokument.asp - med henblik på at frembringe dynamisk web-indhold. Det primære grundlag for Active Server pages er programmeringssprog (script-sprog), som understøtter ActiveX Scripting, som fx. VBScript, JavaScript og PerlScript og muligheden for at afvikle disse scripts på serveren i stedet for på klienten. Dermed bliver det eksempelvis muligt at opstille betingelser for, hvilke oplysninger, og således også hvilken HTML-kode, brugeren skal modtage.

**ASP.NET:** Den nye version af ASP, der følger med .NET-plattformen. Er radikalt anderledes end ASP, men en integral del af .NET, hvilket betyder, at mange af programmeringsteknikkerne fra almindelig Windows-udvikling kan genbruges. se [www.asp.net](http://www.asp.net).

**DHTML:** Dynamic Hyper Text Markup Language. En udvidelse af HTML, som giver mulighed for mere "liv" på hjemmesiderne. Microsoft og Netscape er ikke enige om standarden.

**DirectX:** En ny multimedie API til Windows. Det er en samling programmer, der giver spil og andre multimedie-programmer meget større kontrol (low-level-kontrol) over hardwaren. DirectX omfatter: DirectDraw, DirectSound, DirectSound3D, DirectPlay, DirectInput, DirectSetup. Alle disse programmer er beregnet på, at spil og andre multimedie-programmer kan udvikles med effekter indenfor lyd og billede. Fordelen med DirectX er, at programmerne kan skrives direkte til Windows og samtidig opnå maksimal kontrol over hardware.

**Hardware:** Er betegnelsen for computerens kabinet med indhold, elektronik, ledninger o.s.v.

**Hjemmeside:** Hjemmeside eller Homepage. Et HTML-dokument, som offentligt tilgængeligt via en web-server. Den første webside man møder, når man kalder op til en website. Hjemmesiden er en velkomst til brugeren, og indeholder typisk navnet på firmaet eller forfatteren, som har lavet den pågældende website, og en menu over, hvad der tilbydes. En homepage kan sammenlignes med forsiden på en trykt brochure..Hjemmesiden benævnes oftest som INDEX.HTML eller DEFAULT.HTML.

**HTML:** Hyper Text Markup Language. Det "tekstbehandlings-sprog" (og filformat) som benyttes til at skrive hjemmesider i, og som forstås af alle browsere, uanset computer-type (Windows, Macintosh eller Unix).

**HTTP:** Hyper Text Transport Protocol. En underprotokol til TCP/IP, som benyttes til hjemmesider, men som også tillader overførsel af andre filtyper. Hypertekst. Et skærm-baseret tekstformat som gør det muligt at springe fra ét sted i teksten til et andet ved at klikke på links.

**Java:** Java er et netværksorienteret programmeringssprog udviklet af Sun Microsystems. Java er specifikt udviklet til at skrive programmer, som via Internettet sikkert kan downloades til din computer og straks afvikles uden risiko for vira eller anden skade til din computer eller dine filer. Ved at anvende små Java programmer ("Applets") kan websides indeholde funktioner som animationer, beregninger og andre fancy tricks.

**JavaScript:** JavaScript er et programmerings-sprog, som bruges til at lave lidt mere avancerede ting på hjemmesiderne, som f.eks. scrolltekster, indkøbskurve osv.. Ældre browsere kan have problemer med at forstå JavaScript.

**JScript:** Microsofts pendant til JavaScript. De to er ens et langt stykke af vejen, men forskelle eksisterer dog. Se [msdn.microsoft.com/scripting](http://msdn.microsoft.com/scripting)

**.Net:** Ny platform fra Microsoft, der bl.a. er beregnet på at give programmører en fælles platform, hvorfra de kan udvikle både almindelige Windows-programmer og internet-programmer uden at skulle lære nye programmeringssprog og metoder  
Se evt. [www.gotdotnet.com](http://www.gotdotnet.com)

**PHP:** PHP er et scripting sprog som afvikles på serveren. Dvs. at det er uafhængig af hvilken browser brugeren har. Med PHP åbnes der mulighed for at gøre HTML-sider 'intelligente': Grænsen mellem cgi-scripts og statiske HTML-sider udviskes, og man kan med PHP, på forbløffende kort tid, udvikle og vedligeholde avancerede, interaktive web-sites.

**Script:** Et script er et program. Et script der udføres på en server, benyttes fx til at producere websider dynamisk i stedet for blot at kopiere dem fra filer på en disk. Et script der udføres i en browser, benyttes fx til at tjekke indholdet af felter i en HTML-formular.  
Eksempel på brug: Som hovedregel består et script af to dele: selve scriptet og en udløser, der sætter det i gang. Da scriptet er usynligt for læseren, er det god skik at anbringe det i starten af siden - i dens header - som er hjemsted for tekniske oplysninger. Udløseren anbringes derimod typisk i den synlige del af siden - i den

så kaldte body. Det kan f.eks. være i en genvej, i et billede eller i en knap.

**VBScript:** Visual Basic Script. Scriptprog udviklet af Microsoft. kan bruges i web-sider men virker kun i Internet Explorer. Bruges også som sprog i bl.a. ASP.

**VRML:** Virtual Reality Modeling Language. Et nyt format for websider, som muligvis på længere sigt vil afløse den nuværende standard HTML, og kan kort beskrives som HTML i tre dimensioner. Et VRML-dokument kan f.eks. forestille en gade med butikker, som man kan bevæge sig ned ad. I butikkerne kan man måske se på varer, bestille og betale, hvorefter man får varen tilsendt med posten i virkeligheden.

**XML:** Extensible Markup Language. XML er så småt på vej til at blive godkendt som en standard. Som navnet antyder, er XML en udvidelse af det eksisterende HTML-sprog og således ikke tænkt som en erstatning herfor. XML har til hensigt at give web-udviklere mulighed for selv at definere nye tags, så eksempelvis et opslag i en database simplificeres.

Det er særdeles interessant at læse at de store sikkerhedsfirmaer advarer brugerne omkring Aktive X i deres browser, og skriver at brugerne skal slå dem fra.

<http://www.version2.dk/artikel/6154?nyhedsbrev>

Tja - det var ca 1 år siden jeg redegjorde lidt om de problemer den slags kunne medføre,

og jeg rådede til begrænset brug af disse farlige omgørelser af sikkerheden i jeres pc'er.

Men er det gået tilbage med brugen af den slags ting??? - nej det tror jeg ikke.

Mest tror jeg at folk ikke forstår hvad det er, og ligefrem søge informationer om emnet, det kan man nok ikke forvente.

Jeg har derfor lavet en mail, som specielt går lidt i dybden omkring disse problemer, og som i modtager seperat.

Det bliver nok heller ikke nemmere af at mange af disse hjælpe ting til brugerne - faktisk omtales med flere navne, javascripter, aktive X objekter, perl-scripter, php og lignede navne.

Fælles faktor,

de er beregnet til at udføre ting på ens pc uden at spørge om lov, - ok der findes nogen hvor programmørerne har indsat et spørg brugerens, og derefter - forsæt og gør det du skal gøre... men det er op til den som laver scriptet/aktive X - at være så flink...

Værst : de er beregnet til at udføre ting på ens pc uden brugerens indgriben, og mange uden at brugere ved de virker.

En af de mest anvente aktive X- objekter, som omgår alle antivirus systemer, er feks de forskellige toolbar som er så populære.

Et eks: Google toolbar, kommer med når man installerer eller opdatere Java, eller Adobe reader.

Så hvis man ikke aktivt gør noget, så omgår vedligeholdelsen af disse programmer resten af sikkerheden.

Der findes idag ikke et populært program - uden at der følger en eller anden slags Javascripts / aktive X med... enten i programmet eller som tilgift.

Et andet eks: Netbank - dem som anvender en eller anden form for Netbank, har også et javascript/aktive X kørende, og der er jo ingen som går ind i IE7's konfiguration før/efter brug af netbank, og tilpasser den mht opstart af den slags. De fleste koncentrerer sig om deres password, og nøglefil, men de er jo mindfre brikker i det forhold.

Browsere som Firefox og Opera - er anderledes, så der kræves andre slags Javascripts / aktive X end til IE7, hvorfor de er mere sikre for en periode, indtil de IT-kriminelle har lært at have flere værktøjer i deres værktøjskasse.

At dem som udnytter den slags til deres egen fordel ved meget af dette, viser sig tydeligt eftersom de overrumplede hele TopDanmarks IT afdeling, så de måtte ominstallere ca 1500 pc i den forløbene uge,

Her burde den almindelige bruger tænke meget over problemet: Hvis den slags kan omgå professionelle itfolk og deres systemer, hvad kan det så gøre ved min pc. På de pc'er som folk anvender i TopDanmark, der har de ikke administrator rettigheder, - så det burde være meget svært at inficere i så stor scala, men et godt script/aktivt x, - så er man uden om det, for Microsoft har jo ladet dørerne stå åben...

<http://www.comon.dk/index.php/news/show/id=34647>

Microsoft har gjort folk en bjørnetjeneste ved at lade alle disse sikkerheds systemer som skulle kunne hjælpe brugerne, være slået fra hvis ikke brugere selv ved hvad der skal stilles på, og hvilke flueben der skal ændres.

Dem som fortæller om alle disse problemer, bliver jo desværre nok beskyldt for at råbe Ulven kommer, - for dem der oplever problemerne, er jo ikke villige til at blive en historie i dagspressen, og efter bare en -2 af slagsen, så er dagspressens behov dækket, hvorfor problemet jo bliver henvist til at være ikke eksisterende.

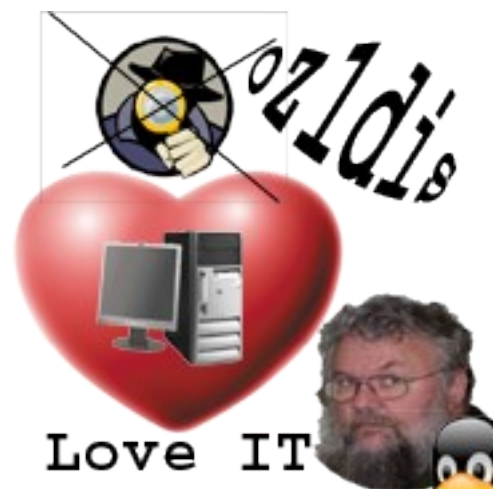
At de IT- kriminelle så har fået adgang til selve sikkerhedskernen i [apache](#) webservere - og inficere ca 10.000 om dagen, så må man sige at de må er flittige.... Deres gevinst må anspore dem til at gøre indsatsen. men for dem er der ikke forskel på om serveren betjener en boligforening, en idrætsforening, eller en avis - de brugere der kommer der og som bliver inficeret, bringer flere maskiner in i de store Botnet, hvor bagmændene så udlejer dem.. altsammen uden pc'ejernes viden og accept. <http://www.version2.dk/artikel/6001>

Ok - der var ca 6 milliarder webservere i 2005, så det varer et par dage ... men det sker, selv et antivira firma fik deres servere inficeret, så de spredte malware istedet for anti-malware tool. <http://www.version2.dk/artikel/6189?nyhedsbrev>

Dem som administrere den slags servere, kan jo være fra skoledrenge til meget IT-proffesionelle - men gør det de skal/bør??? Måske det håb som beskrives her, har lange udsigter... <http://www.comon.dk/index.php/news/show/id=34706>

Nå, men Microsoft fortæller så at man bare skal skifte til Vista - for der er halvt så mange fejl idet system - i forhold til XP. <http://www.comon.dk/index.php/news/show/id=34502> men i praksis - så holder dette ikke vand, for der er andre og mere komplicerede problemer - foreløbig så har jeg opgivet at være positiv over sikkerheden i Vista, når det drejer sig om Microsofts standard indstillinger... Nu er det ikke således at jeg er imod Microsoft, men jeg synes det er mærkeligt at en så stor virksomhed, kan lave så dårlige programmer og styresystemer, og så slippe afsted med at lade brugerne være dem som tester det ... men måske erhvervslivet er ved at se tingene i et andet lys.. <http://www.version2.dk/artikel/6141?nyhedsbrev>

Håber disse linier skaber lidt mere forståelse...



venlig hilsen oz1dis