

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

## **Pas på E-boks - det kan være farligt.**

Når man læser den artikel ; Danske e-Boks er på vej ud i Europa , så kan jeg bekymres.

Hvorfor ???

Se siden de begyndte - har Danske e-Boks baseret sig på brug af pop-op vinduer, når man skal læse sine beskeder.

skal man endda printe eller hente info, så yderligere pop-op vinduer.

Det man så skal gøre for ikke dette blokkes i ens pop-op vindue blokkering, er at lade E-boks være en sikker side,

så man ikke får den blokkering når man er på denne side.

Denne metode svarer til hvad vi gør når vi anvender vores Netbank, hvor vi også markerer den som en sikker side.

**Det at man markerer en side som sikker - betyder at man slår webbrowsers indre forsvars metoder fra, når man besøger de sider man har markeret som sikker.**

Nu er det blevet mange ting man kan via modtage E-boks, og for at lette det for brugeren, så kan man i E-boks vælge mellem de service som E-boks yder, og de åbner så i et nyt pop-op vindue.

Lad os nu antage vi er igang med Netbank, - og ens bank er begyndt at sende alle ens konto udskrifter mv via E-boks, så betyder det at vi via Netbank benytter browseren på netbank siden, - men for at læse vores udskrifter så skal vi tillade

E-boks pop-op vinduet inde i den sikre netbank..

Det der her sker er at vi tillader "Cross site scripting" - vi tillader data ind i vores maskine fra en anden site end netbanks.

[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting) for dem som vil vide mere om "Cross site scripting"

Tænk også på, er der fejl i den link som sender dig til det næste vindue - så kan du havne på en site som er helt uden for kontrol.

Fænomenet kaldes typo-squatting. <http://en.wikipedia.org/wiki/Typosquatting> for dem som vil vide mere.

Så længe der ikke er noget galt med de 2 site Netbank og E-boks, så betyder det ikke noget, men E-boks sælger jo netop deres service til mange andre - og så kommer problemet for alvor til at være en trussel.

Se når vi bruger vores browser i almindelig - så checker den om der sker cross site scripting - og advare os om evt problemer.

Men når vi markerer Netbank som en sikker side, så slår vi en masse af disse advarsler fra, og derved er der fri adgang ind i vores maskine.

Se i de moderne Internet security pakker, der er man netop endnu mere fokuseret på den slags problemer mht "Cross site scripting" og den nye Internet Explore 8 har direkte mange filtre for at for hindre dette, netop fordi det er et utrolig farligt problem.

Hvorfor??? - jo for de sidste knapt 2 år - er det blevet den måde man har smittet flest maskiner på med diverse malware.

<http://da.wikipedia.org/wiki/Malware> for dem som ikke lige ved hvad Malware er.

Alene i efteråret blev en række store dagblade offer for den slags - så de smittede brugerne der kigge på deres websider, og det endda uden brugerne skulle gøre noget. Her var de endda i stand til at gøre det uden man havde markeret de berørte dagblades sites som værende sikre sider.

Forestil jer så - at en af de leverandøre som anvender E-boks benytter sig af et ældre og demed meget sandsynligt, usikker kode på en del af deres site, feks Skat eller en kommune .. og vær sikker på det sker ( se bare længere nede ),

så kan man komme ind via den site - og forurene E-boks systemet .

Med de krav der stilles til brugerne - tillade pop-op og E-boks skal være en sikker side, så er der garanteret fri adgang til brugernes pc'er..

Desværre er det ikke alle internet security programmerne som er istand til at holde sig selv rene - så brugerene vil næppe opdage de er inficeret - før lang tid efter.

Så hvad det eventuelt kan betyde for den enkelte er det derfor svært at svare på.

**Men jeg føler det problematisk - at man dels kræver brugerne slækker på sikkerheden mht sikrede sites, og så kræver man tillader "Cross site scripting" - for hvem har ansvaret - og hvem sikre der ikke sker noget..**

Min konklution:

Jeg er ikke længere bruger af E-boks, min tillid er væk, eftermange indgåede spørg/svar - til/fra E-boks supportten.

--

Allan I Jensen  
Vinterbuen 5  
DK-2750 Ballerup  
Telf 44654488  
Mob 40684488  
Ham Callsign: OZ1DIS

**Her i det efterfølgende - vil du finde eksempler på de problemer jeg forsøger at belyse i min tekst om E-boks problemerne. Mere så i kan forstå - det er ikke bare en hypotese - men et faktisk problem**

<http://www.computerworld.dk/art/47002?cid=10&a=cid&i=10&o=15&pos=16>

## Danske e-Boks er på vej ud i Europa

Danske e-Boks gør klar til at tilbyde elektroniske dokumenter til europæerne. Med giganterne KMD, PBS og PostDanmark i ryggen kan det blive en succes, vurderer ekspert.

Af [□ Kristian Hansen](#)

---

□ Publiceret d. 16. juli 2008 kl. 10.03 | [□ \(3\)](#)

Danske e-Boks vil til udlandet.

"Vi er blevet så modne, at det er tid til at se ud over landets grænser," siger Flemming L. Jensen, administrerende direktør i PBS, der sammen med KMD og PostDanmark står bag e-Boks.

Direktøren, der er tidligere bestyrelsesformand for e-Boks, forklarer, at PostDanmark, KMD og PBS alle har kontakter i udlandet, hvor efterspørgslen efter et lignende system er stort.

"Der har været stor interesse, selv om andre er mislykket. Men e-Boks er en unik løsning og et dansk fyrtårn i EU. Nu skal fyrtårnet eksporteres", siger Flemming L. Jensen.

### Naturligt at kigge ud over grænserne

I e-Boks' direktørkontor er udmeldingen mere forsigtig.

"Det er endnu for tidligt at sige, hvordan, hvornår og hvor vi begynder, men der arbejdes på modeller," siger direktør Henrik Andersen fra e-Boks.

Han forklarer, at e-Boks i Danmark har vist sin modenhed. Blandt andet giver selskabet nu [omsider overskud](#).

"Vi har den tilgang, at vi vil have skruen godt i vandet i Danmark, inden vi overvejer udlandet. Det har vi nu," siger han.

Derfor er det naturligt at kigge ud over grænserne.

Henrik Andersen forklarer, at det bliver en stor udfordring, fordi andre lande ikke har den samme tradition for eksempelvis at bruge netbank.

"Så det er ikke bare lige sådan at gå til," siger han.

Sidste år havnede mellem 50 millioner og 60 millioner elektroniske dokumenter i danske borgeres e-bokse.

I Danmark bruger 1,7 millioner danskere e-Boks, heraf er de 70.000 virksomheder.

Derudover leverer staten og samtlige kommuner samt en række private virksomheder lønsedler til deres medarbejdere via e-Boks - i alt godt 900.000 lønsedler hver måned.

## Giganter i ryggen

Selvom kun syv medarbejdere formelt er tilknyttet e-boks i dag, vil de store selskaber bag e-Boks hjælpe til med det udenlandske eventyr.

I første omgang er Norden interessant, men også resten af EU er spændende, lyder det fra direktøren.

## Ekspert: Succes venter

Professor Kim Viborg Andersen fra CBS vurderer, at selskabet kan få succes i udlandet. Allerede i foråret 2007 var [han i Computerworld](#) inde på de samme ideer om, at udlandet var den rigtige vej frem for e-Boks.

"Selskabet har jo skabt en unik position i Danmark og ligger lunt i svinget til at kunne blive endnu mere markedsdækkende i Danmark," siger han.

Udfordringen for den slags services som e-boks tilbyder er at fortsætte de gode takter og have et skarpt øje på tilsvarende tjenester i udlandet, forklarer han.

"E-Boks er jo forholdsvis sårbar for globale tjenester af samme kaliber. Det er en mulighed for e-boks at ekspandere til andre lande, men altså også en trussel mod dem," siger professoren.

[http://www.comon.dk/news/webtrafik.er.farligere.end.e-mails\\_36829.html](http://www.comon.dk/news/webtrafik.er.farligere.end.e-mails_36829.html)

## Webtrafik er farligere end e-mails

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.

<http://www.version2.dk/artikel/7912?nyhedsbrev>

## Upatchedede systemer autohackes på minutter

Det kan være svært at nå at patche sit it-system, før hackerne slår kløerne i det. Og paradoksalt nok forudsætter patch-processen ofte, at der er adgang til det internet, som hackerne netop angriber fra. Brug firewall, lyder eksperternes råd.

Af Jakob Møllerhøj, torsdag 17. jul 2008 kl. 11:08

Upatchedede maskiner med især ældre operativsystemer lever livet farligt på nettet. De fleste er godt klar over, at det der med opdateringer fra eksempelvis Windows Update er vigtigt, men i praksis kan det dog være svært at nå til Windows Update-sitet og installere opdateringerne, før det går galt.

Problemet kan for eksempel opstå, når en maskine bliver udstyret med en frisk, ikke-servicepakket udgave af Windows XP. Der er nemlig stadig så mange orme i omløb, der er på evig jagt efter sårbare systemer, at maskinen risikerer at blive inficeret helt automatisk, minutter efter den har fået netforbindelse.

Således viser honeypotmålinger fra SANS (SysAdmin, Audit, Networking, and Security) Institute Internet Storm Center alene for i år, at overlevelsestiden for upatchedede Windows-maskiner er helt nede omkring 30 minutter, UNIX-baserede systemer klarer sig umiddelbart noget bedre.

Også Thorsten Holz på [honeyblog.org](http://honeyblog.org) har lavet målinger med honeypots, der viser, at det er et spørgsmål om minutter, før en upatched maskine bliver kompromitteret - enten gennem huller i sårbare tredjepartsprodukter, åbne og usikrede services eller via sårbarheder i selve operativsystemet.

Akkumulerer man sårbarhederne, viser SANS' honeypots, at infektionstiden er nede under fem minutter.

»Det illustrerer jo meget godt, hvor vigtigt det er, at man patcher. Og at man ikke hopper på nettet uden at have patchet sit system inden,« siger teknisk direktør i den danske virksomhed Secunia til [Version2.dk](http://Version2.dk)

Han erkender dog, at det kan være vanskeligt både at undgå internettet og samtidig patche sit system.

»Man bliver nok nødt til at tage det på en måde, hvor man kan komme på uden at have en offentlig ip-adresse. Altså bag en nat/firewall. Så hvis man hopper på en nat/firewall på et netværk, som man

har en rimelig grad af tillid til ... det skal nok ikke lige være kollegienetværket eller nede på computercaféen,« siger Thomas Kristensen.

Også sikkerhedseksperter fra Symantec Peter Schjøtt ser det problematiske i, at upatched maskiner når at blive hacket, før de bliver patched. Han vurderer dog, at der formentlig er forskel på forskellige systemers sårbarhed alt afhængig af, hvor længe de har eksisteret.

»Man skal gå ud fra worst case. Der er selvfølgelig færre kendte angreb på Vista, end der er på andre kendte styresystemer, der har været der længere. Det er jo selvklart,« siger han og tilføjer:

»Der kører massevis af software derude, der laver automatisk detektering.«

Både Peter Schjøtt og Thomas Kristensen fraråder desuden på det kraftigste brugere at besøge ret meget andet på internettet udover Windows Update for Windows-maskiners vedkommende, indtil computeren er opdateret. Men selvom brugeren er nok så forsigtig og ikke besøger andet end eksempelvis Windows Update, så risikerer Fanden alligevel at være løs i Laksegade. Thi en del af hackerangrebene jo er fuldstændigt automatiserede.

»Selvfølgelig er der en lang række orme, der kører rundt. Der er en lang række downloaders. Og en ting, man skal lade være med, det er at surfe rundt ret mange steder, inden man har patched maskinen op,« siger Peter Schjøtt.

Det vil sige, at orme konstant er på jagt efter blandt andet åbne porte med sårbare services. Og derfor mener Thomas Kristensen også, at det under alle omstændigheder kan være vanskeligt at nå at opdatere visse Windows-maskiner, før ormene når den.

»Det kan man nok ikke, nej. Man kan ikke nå at gøre det, hvis man ikke sidder bag en firewall. Sådant bliver man simpelthen nødt til få fingre i. Og jeg vil nok sige, bare at prøve at få downloadet en eller anden gratis personlig firewall og få smidt på en XP uden servicepack 2, vil være rimelig risky business. Jeg vil ikke have voldsomt meget tillid til min maskine, hvis jeg ikke har en firewall aktiveret fra starten af,« siger han.

Den værste situation Thomas Kristensen kan komme i tanker om, er når den sårbare klient er koblet på nettet med en offentlig ip-adresse:

»Lige så snart du har en offentlig IP-adresse, så kommer du ned med nakken på et eller andet tidspunkt. Så finder de dig helt af sig selv.«

### **Ikke kun Windows**

Selvom Windows er et yndet hacker-offer for blandt andet de automatiserede orme på grund af styresystemets udbredelse, så fortæller Thomas Kristensen, at også Linux-maskiner er udsatte for de automatiserede angreb.

»Hvis du bare åbner en SSH eller en Telnet på en Linux-maskine, så går der vitterlig ikke mange minutter, før de første bruteforce-angreb begynder at komme. Der er simpelthen nogen, der scanner på de porte med jævne mellemrum,« siger han og tilføjer, at det ofte er via svage logins på eksempelvis SSH, at hackerne kommer ind.

Og endeligt er der upatched peer-to-peer klienter og hullede tredjepartsapplikationer generelt, som kan være indgangshuller for ormeangreb. Anbefalingen fra Thomas Kristensen er at sørge for at have holde sit software up-to-date.

## **Ikke så slemt i Danmark**

Thomas Kristensen og Peter Schjøtt vurderer, at situationen med de automatiserede ormeangreb er knap så alvorlig i Danmark, blandt andet fordi systemerne generelt er vel-opdaterede. Peter Schjøtt gætter desuden på, at flere danske ISP'ere automatisk blokerer på visse orme-porte, men understreger, at han ikke ved det med sikkerhed.

## **Din erfaring**

Men hvad er din erfaring med upatched systemer? Er det ikke så slemt i Danmark, eller har du også oplevet kapløbet, hvor det kan være vanskeligt at nå eksempelvis Windows Update, før ormene når din computer? Fortæl om dine oplevelser i debatten herunder.

[http://www.comon.dk/news/skats.toldberegning.virker.ikke.med.firefox\\_36923.html](http://www.comon.dk/news/skats.toldberegning.virker.ikke.med.firefox_36923.html)

## **Skats toldberegning virker ikke med Firefox**

Skats hjemmeside til beregning af toldsats er lukket land for alle brugere med andre browsere end Internet Explorer.

Af [Karim Pedersen](#)

onsdag 16. juli 2008, 09:39

Når man besøger Skats hjemmeside til beregning af toldsats [tarif.skat.dk](http://tarif.skat.dk) med Firefox eller en anden alternativ browser mødes man af en helt tom side. Det skyldes at Den elektroniske Toldtarif benytter et JavaScript, der indeholder forældet kode, som kun virker i Internet Explorer.

Skat er netop blevet optaget i Hall of Shame hos [lki.dk](http://lki.dk) (Luk Kunderne Ind), der kæmper for, at internettet skal kunne bruges af alle, uanset hvilken type af computer og programmer der benyttes.

Lki.dk fortæller at man har forsøgt at råbe Skat op, så alle kan få lov at udregne told, men det har hidtil været forgæves.

Problemet kan løses ved at kode, der har været standard siden 2000, og som selv Microsoft anbefaler, så vil beregningssiden også virke i alternative programmer.

Men selv hvis JavaScriptet rettes, kan mange skatteplagede borgere stadig slippe for at beregne told. Hjemmesiden benytter nemlig et pop-up-vindue, der åbnes automatisk uden brugerens medvirken. Den slags vinduer blokeres i mange programmer, og så er resultatet stadig et helt tomt vindue.

---

[http://www.comon.dk/news/offentlige.hjemmesider.er.ikke.gode.nok\\_36733.html](http://www.comon.dk/news/offentlige.hjemmesider.er.ikke.gode.nok_36733.html)

## **Offentlige hjemmesider er ikke gode nok**

Tilgængeligheden på fleste offentlige hjemmesider ikke er god nok. Se Telestyrelsens vurdering af 250 offentlige hjemmesider her.

Af Kasper Villum Jensen

fredag 27. juni 2008, 11:31

Det står rigtigt skidt til med tilgængeligheden på de offentlige danske hjemmesider.

I en gennemgang af næsten 250 af slagsen kommer IT- og Telestyrelsen frem til, at ikke en eneste kan beteges "perfekt". Hovedparten havner i kategorien "Jævn Tilgængelighed".

Styrelsens har bedømt efter dette skema:

1 Perfekt - ingen fejl 2 God tilgængelighed - eventuelle fejl af lille betydning 3 Jævn Tilgængelighed - væsentligt indhold tilgængeligt, men mindre fejl og behov for forbedringer 4 Dårlig tilgængelighed - mange fejl og problemer som gør, at en eller flere typer brugere ikke vil være i stand til at anvende hjemmesiden eller væsentlige dele af den

De forskellige kommuner, ministerier og styrelser fordeler sig således:

Perfekt - 0 procent God tilgængelighed - 6 procent Jævn tilgængelighed - 70 procent Dårlig tilgængelighed - 24 procent

Velfærdministeriet er for eksempel det eneste ministerium, der kan blære sig med at være havnet i grupperingen: "God Tilgængelighed". Resten af ministerierne falder i de mindre attraktive opdelinger.

Den overordnede konklusion er derfor, at der pænt sagt er plads til forbedringer.

»Resultaterne er ikke opmuntrende, men det er vigtigt at understrege, at dette er den første af tre kortlægninger. Dette er første år efter indførelsen af en obligatorisk standard – en slags år 0. Nu skal den til at virke,« siger vicedirektør i IT- og Telestyrelsen Marie Munk.

De to øvrige kortlægninger vil finde sted i 2010 og 2012.

Den detaljerede oversigt kan se hos [It- og Telestyrelsen](#). Det er firmaet Sensus, der har lavet undersøgelsen for styrelsen. Efterfølgende har de vurderede hjemmesider haft mulighed for at kommentere på vurderingen. Kommentarene kan også ses hos styrelsen.

<http://www.computerworld.dk/art/47028?cid=10&a=cid&i=10&o=10&pos=11>

## **Danske it-chefer neddrogler fokus på sikkerhed**

It-sikkerhed er i højere grad blevet en integreret del af forretningsudviklingen. Derfor har de danske it-chefer nedprioriteret fokus på investeringer i sikkerhed en anelse, siger brancheformand.

Af [Rune Pedersen](#)

□ Publiceret d. 16. juli 2008 kl. 14.45

Tre fjerdedele af de danske it-chefer har en forventning om at deres virksomhed vil øge investeringerne i it i 2008.

Det viser en ny undersøgelse, som brancheorganisationen Dansk IT har foretaget blandt medlemmerne af sit panel af it-chefer.

Undersøgelsen viser, at de deltagende it-chefer i modsætning til tidligere ikke prioriterer sikkerhed

så højt på listen over planlagte investeringer.

### **Tidligere topscorer**

Investeringerne i it-sikkerhed har tidligere været topscorer på it-chefernes prioriteringsliste over, hvad budgettet skal bruges til. Men i den nye undersøgelse er sikkerhedsinvesteringerne rykket ned af listen.

Det fortæller næstformand i Dansk IT, Klaus Kvorning Hansen.

"Det er jo bemærkelsesværdigt," siger Klaus Kvorning Hansen.

### **Sikkerhed mere integreret**

Ifølge næstformanden skyldes dette dog ikke, at virksomhederne nedprioriteter it-sikkerheden.

I stedet handler det om, at sikkerhed er blevet en mere integreret del af planlægningen.

"It-sikkerhed har ikke længere behov for et særligt fokus i samme udstrækning som tidligere," siger Klaus Kvorning Hansen.

I stedet for sikkerhed er det nu forretningsudvikling, der har den højeste prioritet hos it-cheferne.

Og når man laver forretningsudvikling er sikkerhed et aspekt som medtænkes, mener Klaus Kvorning Hansen.

Derfor kan dette være en naturlig forklaring på nedprioriteringen af sikkerhed på listen over de vigtigste investeringsområder hos it-cheferne, forklarer Klaus Kvorning Hansen.

"Vi er heldigvis på vej ind i en situation, hvor det medtænkes. Og derfor har det ikke brug for helt så stærkt et selvstændigt fokus længere, siger næstformanden.

Undersøgelsen er baseret på svar fra 74 ud af de 175 danske it-chefer, som er med i Dansk IT's panel for it-chefer.

42 procent af de deltagende it-chefer er offentligt ansat, mens resten er ansat hos private virksomheder.

<http://www.computerworld.dk/art/46963?cid=10&a=cid&i=10&o=44&pos=19>

## **Computerworld ramt af netsvindlere - hvad med dig?**

Glemmer du d'et i Computerworld.dk ryger du ind på en side, der tilhører amerikanske svindlere. Fænomenet kaldes typo-squatting. Se listen over danske typo-squattede domæner her.

Af [□ Jacob Ø. Wittorff](#)

Glemmer du nogensinde d'et i Computerworld?

En banal forglemmelse, men hvis du ikke har sikkerhedsopdateret din computer, kan forglemmelsen betyde, at din computer bliver inficeret med skadelig software.

Der er nemlig en verden til forskel på [computerworld.dk](http://computerworld.dk) og [computerworl.dk](http://computerworl.dk).

Den første adresse leder dig ind på nærværende hjemmeside. Den sidste adresse leder dig ind på en hjemmeside kontrolleret af svindlere med adresse i Palm Beach i USA, der gladelig fortæller dig, hvor du kan købe en ny computer.

### **Kan være farlige**

I visse tilfælde indeholder sider som [computerworl.dk](http://computerworl.dk) en kode, som kan inficere din computer med skadelige programmer, hvis ikke computeren har de seneste sikkerhedsopdateringer.

Fænomenet hedder typosquatting og er ekstremt udbredt. Det anvendes af svindlere, der forsøger at vride internettrafik uden af internetbrugernes tastefejl. Ofte er der blot en enkelt tastefejl til forskel mellem et velbesøgt domæne som computerworld og et domæne, der er ejet af svindlere.

Det danske sikkerhedsfirma CSIS har gennem de seneste dage samlet en liste over typosquattede danske domæner.

Ifølge CSIS er listen blot toppen af isbjerget. Herunder kan du se om dit domænenavn, også er på liste