dansk•it

# CIOViewpoint 2011

# Industrivirus og industrispionage

## It-sikkerhed 2011

Formålet med denne undersøgelse er at afdække i hvor stort omfang danske virksomheder oplever industrispionage samt angreb mod basis it-infrastruktur og produktionssystemer, som fx "Stuxnet" angrebet.

Undersøgelsen er gennemført i DANSK IT's it-chefpanel, som består af 456 it-chefer i både offentlige og private virksomheder samt store som små virksomheder. I denne undersøgelse har 119 it-chefer deltaget, hvoraf ca. 1/3 kommer fra den offentlige sektor, mens godt 2/3 kommer fra den private sektor. It-cheferne i undersøgelsen repræsenterer en omsætning på over 40 milliarder kr. og over 185.000 ansatte.

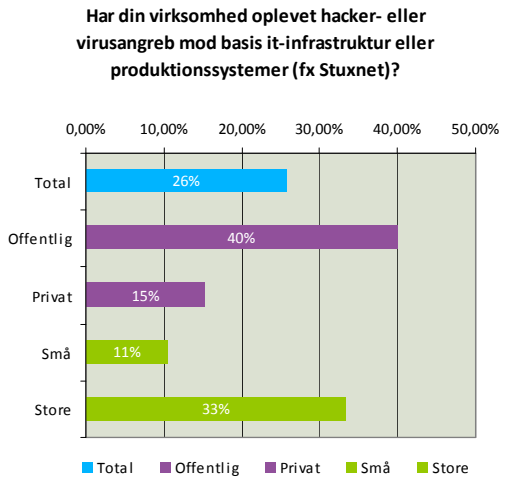
## VIGTIGSTE POINTER

- Hver fjerde danske virksomhed har været udsat for virusangreb á la Stuxnet, der går efter at lamme basis it-infrastruktur eller produktionssystemer. Kun lidt over halvdelen har taget særlige forholdsregler mod disse nye trusler, beretter danske it-chefer i ny panelundersøgelse fra interesseorganisationen DANSK IT (DIT).

- 44 procent af virksomhederne har ikke indført skærpede forholdsregler for at imødegå angreb mod basis it-infrastruktur eller produktionssystemer.

- Fem ud af 100 it-chefer har med sikkerhed oplevet industrispionage. I disse tilfælde kommer den største trussel fra personer med en nuværende eller tidligere tilknytning til virksomheden. Kun i ét tilfælde er der drevet industrispionage via computerbaseret angreb. Knap hver tredje it-chef er ikke klar over om virksomheden har været udsat for industrispionage

**Hver fjerde virksomhed udsat for angreb mod basis it-infrastruktur og produktionssystemer**.
Forskellige typer af computerbaserede angreb på virksomheders it hører hverdagen til for de fleste it-chefer. Typisk giver disse florerende angreb ingen større problemer. Men i foråret 2010 berettede flere virksomheder verden over, at de havde været udfordret af en ny type virus, som gik efter at lamme deres basis it-infrastruktur og produktionssystemer. Et år senere beretter DANSK IT's undersøgelse nu om, at 26 procent af it-cheferne i undersøgelsen har oplevet den type af angreb som Stuxnet er et eksempel på.




**Figur 1:** Andelen af it-chefer som har oplevet computerbaseret angreb mod basis it-infrastruktur eller produktionssystemer.

26 procent af it-cheferne i undersøgelsen angiver, at de har oplevet computerbaseret angreb, som er eller minder om "Stuxnet"-angrebet. Det fremgår endvidere, at 40 procent af offentlige virksomheder har været ramt på netop disse væsentlige dele af it-porteføljen.

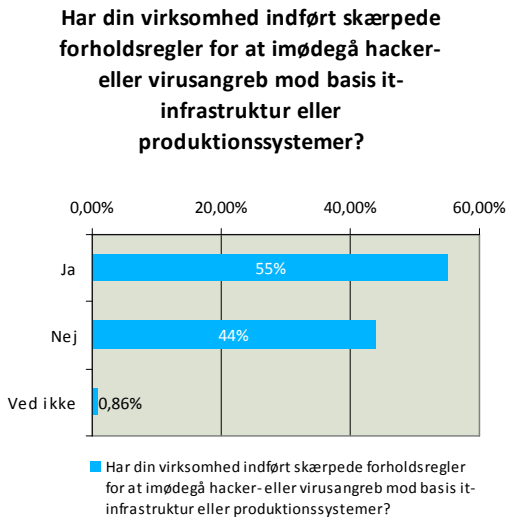
Sondres der mellem små[1] og store virksomheder, tegnes et klart billede af, at det er de store virksomheder, som oplever angreb i denne form. Men det er også værd at bemærke, at 11 procent af de små virksomheder har oplevet det samme.

Den nye trussel har fået lidt over halvdelen (55 procent) af virksomhederne til at indføre skærpede foranstaltninger.

**Om Stuxnet**
*Stuxnet er en Windows-specifik computerorm først opdaget i sommeren 2010 og som var målrettet kontrol-systemer og systemer til dataopsamling (SCADA), der anvendes til at kontrollere og overvåge industrielle processer. Inficerede systemer kan med Stuxnetormen omprogrammeres eller ødelægges.*

*Kilde: Wikipedia.org*

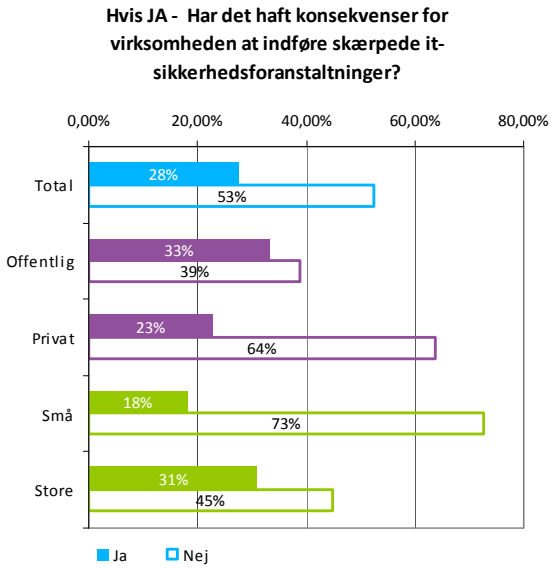
[1] Se definitionen på små og store virksomheder på sidste side i denne publikation.




**Figur 2:** Andelen af it-chefer som angiver at deres organisation har skærpet it-sikkerheden som følge af trusler imod basis it-infrastruktur og produktionssystemer.

En stor gruppe på 44 procent har dog endnu ikke skærpet sikkerheden på området.

**Skærpet it-sikkerhed har konsekvenser**
De virksomheder, der har skærpet sikkerheden mod angreb mod basissystemer, formår også at nedbringe antallet af angreb. Omvendt har den øgede sikkerhed også negative konsekvenser, idet virksomhedernes omkostninger til fx sikkerhedssoftware og hardware øges, ligesom virksomhedens kommunikation gøres mere besværlig. Blandt andet fordi der kommer flere restriktioner for brugernes anvendelse af virksomhedens it. Hertil bliver administrationen af sikkerhedsstrategier og beredskabsplaner mere kompliceret.

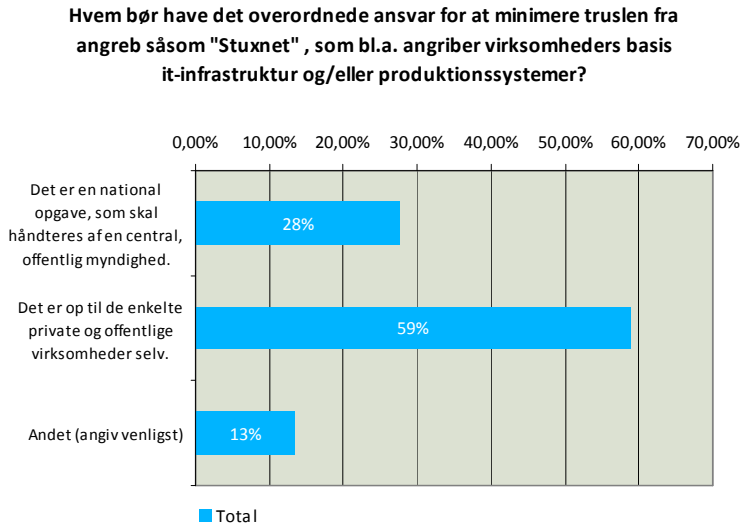



**Figur 3:** Andelen af it-chefer som peger på at det har haft konsekvenser at indføre skærpede it-sikkerhedsforanstaltninger (se figur "2" herover).

Af undersøgelsen fremgår det, at de skærpede it-sikkerhedsforanstaltninger først og fremmest har konsekvenser for de store virksomheder, men også at flere offentlige it-chefer end it-chefer fra det private har mærket konsekvenser af øgede it-sikkerhedstiltag.

**Hvem har ansvaret for it-sikkerheden?**

Computer-baserede vira såsom Stuxnet kan være yderst vanskelige at dæmme op for hos den enkelte virksomhed. Særligt mindre virksomheder - der har færre ressourcer til it-sikkerhed - kan få vanskeligere og vanskeligere ved at håndtere de stadigt mere og mere komplicerede it-angreb. DANSK IT har derfor spurgt sit it-chef-panel, hvem der skal have det overordnende ansvar for at dæmme op for it-sikkerhedstrusler, der er målrettede virksomhedernes it-infrastruktur eller produktionssystemer.




**Om "GovCert"**
*GovCERT står for "Governmental Computer Emergency Response Team" og er en statslig varslings-tjeneste for internettrusler. GovCert overvåger ikke al internettrafik til Danmark, men overvåger al internet-trafik til og fra stat, region og kommune samt centrale dele af energisektoren og den finansielle sektor.*

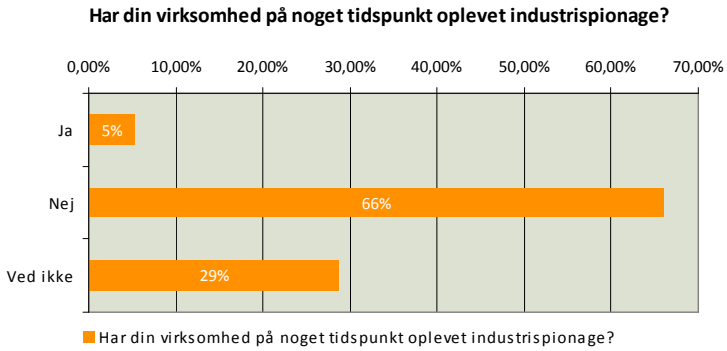
*Kilde: IT- og Telestyrelsen & retsinformation (Beredskabsloven, kap. 5)*

**Figur 4:** Andelen af it-chefer som angiver, hvem de mener skal have det overordnede ansvar for at dæmme op for trusler såsom "Stuxnet" eller lignende angreb, som er målrettet basis it-infrastruktur eller produktionssystemer.

Lidt under en tredjedel peger på, at det offentlige skal spille en mere markant rolle i forhold til at dæmme op for it-angreb som Stuxnet. 59 procent mener til gengæld, at det er virksomhederne selv, der bør have det overordnede ansvar.

Af de 13 procent, som angiver noget andet end de to svarmuligheder, peger it-cheferne på, at det bør være et fælles ansvar for de to parter, eller at en offentlig myndighed skal hjælpe og støtte virksomhederne på forskellige måder fx ved at alarmere og advisere virksomhederne. Et andet synspunkt er, at internetleverandørerne også må på banen og tage en del af ansvaret.

**Industrispionage – en trussel?**
Hvorvidt industrispionage er et problem for it-cheferne i DANSK IT's it-chefpanel har DANSK IT med denne undersøgelse søgt at sætte tal på.




**Figur 5:** Andelen af it-chefer som har oplevet industrispionage.

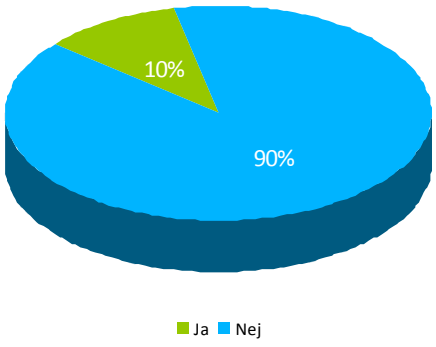
5 procent af it-chefer har med sikkerhed oplevet industrispionage. Det bør dog bemærkes, at næsten hver tredje it-chef ikke kan afvise, at virksomheden har været udsat for industrispionage

Når det gælder industrispionage viser undersøgelsen, at den største trussel kommer fra personer med en nuværende eller tidligere tilknytning til virksomheden. Kun i ét tilfælde er der drevet industrispionage via computerbaseret angreb. Det indikerer, at virksomheder og organisationer bedst sikrer sig imod industrispionage ved at vanskeliggøre muligheden for, at medarbejdere kan tage data med sig.

Undersøgelsen viser dog, at blot 10 procent af virksomhederne har særlige it-sikkerhedsforanstaltninger i forbindelse med nøglemedarbejderes rejser. Særligt i forbindelse med rejser uden for EU tages der særlige it-sikkerhedsforanstaltninger.

De fleste sikrer sig ved, at følsomme data ikke opbevares på it-udstyr som medbringes til udlandet. I stedet hentes følsomme data via en sikker forbindelse til virksomhedens it-systemer. Dette kombineres i mange tilfælde med at følsomme data inden rejsen slettes fra it-udstyret.

**Er der i din virksomhed særlige it-sikkerhedsforanstaltninger for nøglemedarbejdere i forbindelse med deres arbejdsrejser til udlandet?**




**Figur 6:** Andelen af it-chefer som peger på, at der i deres virksomhed tages særlige it-sikkerhedsforanstaltninger i forbindelse med nøglemedarbejders.

**Om CIO Viewpoint 2011 (special edition)**
CIO Viewpoint er baseret på en undersøgelse i DANSK IT's it-chefpanel. Denne udgave af undersøgelsen er gennemført i december måned 2010.

It-chefpanelet består af 456 it-chefer i både offentlige og private virksomheder samt store som små virksomheder. I denne undersøgelse har 119 it-chefer deltaget, hvoraf ca. $^{1}/_{3}$ kommer fra den offentlige sektor, mens godt $^{2}/_{3}$ kommer fra den private sektor. It-cheferne i undersøgelsen repræsenterer en omsætning på over 40 milliarder kr. og over 185.000 ansatte.

**Andre bemærkninger**

*Virksomhedsstørrelse:* I undersøgelsen her er *"små virksomheder"* defineret som virksomheder med under 251 ansatte, hvor *"store virksomheder"* er defineret som virksomheder med mere end 250 ansatte. Der er således ikke taget højde for virksomhedens omsætning.

*DIT (DANSK IT) er en interesseorganisation stiftet i 1958 med det formål at samle folk, der arbejder professionelt med it, samt udbrede kendskabet til informationsteknologien og dens anvendelse til gavn for samfundet og den enkelte borger*



dansk·it

# CIOViewpoint 2011

For yderligere information kontakt:

**Benjamin Willum Funder**
politisk konsulent

E-mail: bwf@dit.dk
Tlf.: 33 17 97 72