CENTER FOR CYBERSIKKERHED

FE

DIGITALISERINGSSTYRELSEN

Cyberforsvar der virker

DECEMBER 2013

Forord

Cybertruslen mod Danmark er reel. Danske offentlige myndigheder og private virksomheder er dagligt udsat for forstyrrende eller skadelige aktiviteter fra forskellige aktører. Center for Cybersikkerhed vurderer, at de alvorligste trusler kommer fra fremmede statslige aktører, der udnytter internettet til at spionere og stjæle dansk intellektuel ejendom.

Når Center for Cybersikkerhed bliver opmærksom på tegn på angreb, tager centret kontakt til den berørte myndighed eller virksomhed. Det er erfaringen, at organisationen typisk ikke er klar over, at den er under angreb. I værste fald er den allerede kompromitteret, og forretningshemmeligheder eller anden følsom information er stjålet.

Center for Cybersikkerhed og Digitaliseringsstyrelsen arbejder målrettet med at sikre en høj grad af cybersikkerhed og sætte emnet på dagsordenen.

Denne vejledning beskriver **en konkret, prioriteret køreplan** for, hvordan myndigheder og virksomheder kan mindske risikoen for cyberangreb og undgå at udsætte sig for markant risiko ved cyberangreb.

Vejledningens fokus er således **begrænset** til den del af det samlede informationssikkerhedsarbejde, der håndterer forebyggelse af angreb fra internettet (hackerangreb). Øvrige aspekter af arbejdet med informationssikkerhed, så som fysisk sikkerhed eller opbygning af robust it-arkitektur, berøres ikke i denne vejledning.

Ændringer i sikkerhedsopsætning og tankegang kan ikke gennemføres uden ledelsesopbakning i myndigheder og virksomheder. Derfor henvender denne vejledning sig primært til **ledelsesniveauet** i organisationerne.

Til manges overraskelse kan en væsentlig del af de målrettede cyberangreb forhindres ved hjælp af fire konkrete sikkerhedstiltag, som enhver topledelse bør kende og prioritere. Tiltagenes anvendelighed og vigtighed understreges af, at Rigsrevisionen for nylig har gennemført it-revision hos bl.a. Statens It på baggrund af netop disse tiltag.

Rigsrevisionen anbefalede i den forbindelse, at Digitaliseringsstyrelsen eller Center for Cybersikkerhed udarbejdede en vejledning om, hvilke sikringstiltag en statslig virksomhed bør overveje til at imødegå aktuelle trusler fra hacking.

Det er disse tiltag, som beskrives i denne vejledning. De fire tiltag, "top fire"-tiltagene, løser ikke problemet alene, men de løfter angrebsbyrden til et niveau, hvor færre modstandere kan være med. Vejledningen beskriver desuden andre tiltag, som kan forbedre cybersikkerheden yderligere.

En robust informations- og kommunikationsteknologisk infrastruktur er en forudsætning for beskyttelse af Danmark og danske data mod cyberangreb. Digitale systemer og data skal beskyttes, så grundlaget for fortsat økonomisk vækst sikres. Det er nødvendigt, at cybersikkerhedsarbejdet tager udgangspunkt i en klar forståelse af, hvordan truslerne kan håndteres. Denne forståelse kan vejledningen forhåbentlig bidrage til.

God læselyst.

Thomas Lund-Sørensen
Chef for Center for Cybersikkerhed

Lars Frelle-Petersen
Direktør for Digitaliseringsstyrelsen

Køreplan for et godt cyberforsvar

Den følgende køreplan, som består af syv skridt, beskriver, hvordan en organisation kan etablere et velfungerende cybersikkerhedsprogram, som sikrer, at organisationen får et cyberforsvar, der virker

Køreplanens første skridt: *Forankring i topledelsen*

God cybersikkerhed starter hos topledelsen. Uden opbakning og prioritet fra topledelsen fejler selv de bedste hensigter om god cybersikkerhed.

Regeringen har besluttet, at statens institutioner skal styre informationssikkerheden efter ISO 27001-standarden. I forlængelse af denne skal der etableres et 'ledelsessystem' for styringen. Dette ledelsessystem er et samlet udtryk for de politikker, procedurer, beslutningsgange og aktiviteter, som udgør komponenterne i organisationens arbejde med informationssikkerhedsstyring. Se litteraturlisten for mere information.

Topledelsen bør søge svar på en række centrale spørgsmål:

- Ved vi, hvad der er vores vigtigste informationer, hvor de er, og hvordan informationsteknologien understøtter vores forretning?
- Ved vi, hvad det betyder for vores forretning, hvis vores vigtigste informationer stjæles eller lækkes, eller hvis vores online-services er utilgængelige i kortere eller længere tid?
- Er vi overbevist om, at vores informationer er tilstrækkeligt beskyttet?
- Har vi en nedskrevet informationssikkerhedspolitik, som vi aktivt støtter, og som vores medarbejdere forstår og følger?
- Opfordrer vi vores tekniske specialister til at videndele om cybersikkerhed med lignende organisationer samt deltage i erfaringsudvekslingsfora?
- Har vi en sikkerhedsorganisation (bør indgå i et ledelsessystem), der er forankret på chefniveau?
- Bliver vi løbende opdateret om, hvilke cybertrusler og -aktører der truer os, deres metoder og motivation?
- Har vi gjort os klart, at topledelsen selv er et oplagt mål for cyberangreb?

Der er mange fordele ved at kende svaret på disse spørgsmål, herunder:

- Strategiske fordele ved bedre at kunne indtænke præcis viden om cybertruslen i organisationens beslutningsprocesser.
- Økonomiske fordele ved at reducere antallet af succesfulde angreb gennem bedre cybersikkerhed.
- Operationelle fordele ved at være bedre forberedt på angreb, reagere effektivt og have cybersikkerhedspolitikken på plads.

Køreplanens andet skridt: *Den rette tekniske kompetence*

Den daglige opgave med at imødegå cyberrisici skal uddelegeres af topledelsen. Det er vigtigt, at de, der får opgaven, forstår teknikken, formår at kommunikere med topledere og kan lede medarbejdere med de rette tekniske kompetencer.

Der er behov for både gode systemadministratorer og medarbejdere med analytiske kompetencer.

Medarbejderne med de rette kompetencer kan være placeret andre steder i en koncern eller hos en leverandør. Det er dog vigtigt, at den enkelte organisation selv tager ansvaret for sikkerheden, også selvom opgaven er uddelegeret til andre.

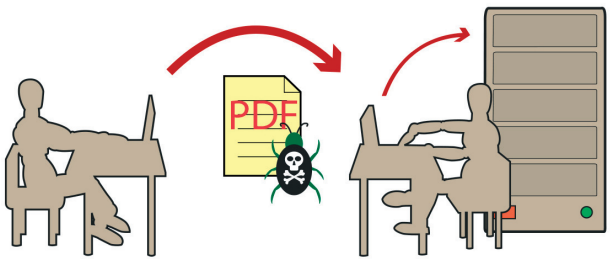
Cyberforsvar, der virker

Godt forsvar kræver en forståelse af angrebet. Ved målrettede cyberangreb bruger angriberne ofte en metode, der går ud på at lokke modtagere af e-mails til at åbne en ondsindet vedhæftning eller klikke på et link til en ondsindet hjemmeside.

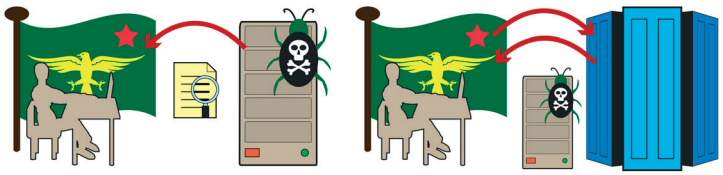
God cybersikkerhed sigter på at *forhindre* så mange angreb som muligt ved laveste omkostninger. Total beskyttelse er desværre en umulighed. Tiltagene skal derfor også medvirke til at *mindske* og ikke mindst *detektere og reagere på angreb.*

Endelig bør myndigheden eller virksomheden komme angriberen i forkøbet med *proaktive tests*, så svagheder kan findes og forbedres, før de bliver udnyttet.

1. fase (indbrud):
Angriberen sender en e-mail med ondsindet vedhæftning eller link. Offeret åbner vedhæftningen eller besøger linket, malware installeres og "ringer hjem".



2. fase (rekognosering):
Angriberen forbinder videre ind og kortlægger virksomhedens netværk



3. fase (dataeksport):
Angriberen indsamler data og sender det hjem.

Køreplanens tredje skridt: *Implementér "top fire"*

Ethvert cybersikkerhedsprogram bør fokusere på fire sikringstiltag – "top fire" – før noget andet. Samlet reducerer de risikoen for cyberangreb i alle angrebets faser, de er yderst effektive, og de kan indføres gradvist.

Sikringstiltag skal indføres med udgangspunkt i en risikobaseret tilgang ud fra vigtigheden af informationerne, systemerne og den enkelte medarbejderfunktion, der skal beskyttes.

Fokuser indsatsen på topledelsen og andre højrisikomål. Udbred senere til hele organisationen. Gør det samme for forretningskritiske data.

Tabellen på næste side giver et overblik over de fire tiltag.

At implementere "top fire" kan være teknisk komplekst, indebære omkostninger og kan møde medarbejdermodstand. God planlægning kan reducere forhindringerne og mindske modstanden. Konkret teknisk vejledning til gennemførelse af "top fire" kan findes i litteraturlisten.

Hvis enkelte programmer ikke længere kan *opdateres*, bør organisationen lave en plan for udfasning eller isolering af disse programmer. Det er en stor risiko at lade enkelte programmer, der ikke længere kan opdateres, påvirke organisationens generelle sikkerhedsniveau.

Få brugere har behov for lokale *administratorrettigheder*, så de skal så vidt muligt fjernes overalt. Domænerettigheder for systemadministratorer bør ligeledes begrænses mest muligt. Hvis det er nemt for en systemadministrator at bevæge sig rundt i et system, er det også nemt for en angriber.

Det er it-afdelingen, som kan være placeret internt et andet sted i en koncern eller hos en leverandør, der efter konkret behovs- og risikovurdering bør beslutte, *hvilke programmer der må køre på et system*. Det gør et angreb vanskeligt.

Sikringstiltag	Medarbejdermodstand	Etableringsomkostninger	Driftsomkostninger	Designet til at forhindre eller detektere	Designet til at hjælpe med at modvirke angrebsfase 1	Hjælper med at modvirke angrebsfase 2	Hjælper med at modvirke angrebsfase 3
Udarbejd positivliste over applikationer af godkendte programmer, for at forhindre kørsel af ondsindet eller uønsket software	Medium	Høj	Medium	Begge	Ja	Ja	Ja
Opdatér programmer, fx. Adobe Reader, Microsoft Office, Flash Player og Java, med seneste sikkerhedsopdateringer, højrisiko inden for to dage	Lav	Høj	Høj	Forhindre	Ja	Muligt	Nej
Opdatér operativ-systemet med seneste sikkerhedsopdateringer, højrisiko inden for to dage. Undgå Windows XP eller tidligere	Lav	Medium	Medium	Forhindre	Ja	Muligt	Muligt
Begræns antallet af brugerkonti med domæne- eller lokaladministratorprivilegier. Disse brugere bør anvende separate uprivilegerede konti til email og websurfing	Medium	Medium	Lav	Forhindre	Muligt	Ja	Muligt

Med "top fire" gennemført og vel vedligeholdt er cybersikkerheden væsentligt forbedret i organisationen. Herefter kan man – baseret på en risikoanalyse med udgangspunkt i truslerne mod organisationen – gå videre i retning af et mere avanceret cyberforsvar, som beskrives i de næste skridt af køreplanen.

Køreplanens fjerde skridt: *Gennemfør løbende awareness*

Sørg for, at de tekniske foranstaltninger bliver bakket op af velinformerede medarbejdere, som er bekendt med de angrebsmetodikker, der ofte benyttes parallelt med et teknisk angreb.

"Social engineering" udføres både via fysisk kontakt, telefonsamtaler og mail - og har alene til formål at franarre medarbejdere information eller andre elementer, der kan give adgang til organisationens aktiver. Et efterfølgende angreb vil blive udført under dække af, at angriberen har legitime brugerrettigheder og er dermed nærmest umuligt at dæmme op for - eller for den sags skyld at opdage. Derfor skal organisationens medarbejdere allerede ved ansættelsen gøres opmærksom på disse risici og løbende holdes opdateret på området.

Køreplanens femte skridt: *Opbyg en reaktiv kapacitet*

Intet forsvar er 100 % sikkert. Succesfulde angreb vil forekomme, men de skal forudses og opdages.

God logning øger chancen for at opdage cyberangreb og undersøge dem til bunds. Samtidig hjælper logning til at forstå angrebenes omfang og konsekvenser - og ikke mindst undgå dem i fremtiden. Men mange organisationer gemmer ikke de rigtige logs eller undlader de vigtigste detaljer. Ofte indsamles der ingen logdata, fordi opgaven synes uoverskuelig. Modsat forsøger nogle at gemme det hele og drukner i data. Selv med gode logs prioriterer organisationerne ofte ikke at undersøge dem for cyberangreb.

Start i det små med få logs om højrisikomål og fokuser på enkelte værkstøjer i analyse-platformen. Centralisér loggene og få det til at virke. Udbyg så med flere logs og flere værktøjer. Indfør med andre ord logning ud fra en risikobaseret tilgang, ligesom med sikringstiltagene. Når en organisation erkender et cyberangreb, er det afgørende at være godt forberedt, holde hovedet koldt og undgå overreaktioner. Det er også vigtigt at erkende sine egne begrænsninger og søge bistand fra professionelle it-sikkerhedseksperter.

Køreplanens sjette skridt: *Løbende sikkerhedstekniske undersøgelser*

"Top fire"-tiltagenes dækningsområde, vedligeholdelse og effektivitet bør løbende afprøves gennem proaktive sikkerhedstekniske undersøgelser og øvelser, ligesom eventuelle øvrige eller nye svagheder i it-miljøet løbende bør afdækkes.

Sjette skridt i køreplanen går billedligt talt ud på hele tiden at gå rundt og banke på rørene og udbedre svagheder og fejl, før de udvikler sig. Det har direkte, åbenlyse fordele, men det er også godt til at skabe en sikkerhedsorienteret virksomhedskultur. Man kan for eksempel simulere angreb, måle hvor hurtigt de bliver opdaget og overveje, om udfaldet nødvendiggør yderligere reaktive tiltag.

Det er her, ligesom for de øvrige tiltag, en forudsætning, at myndigheden eller virksomheden har opbygget eller har adgang til tilstrækkelig teknisk kompetence.

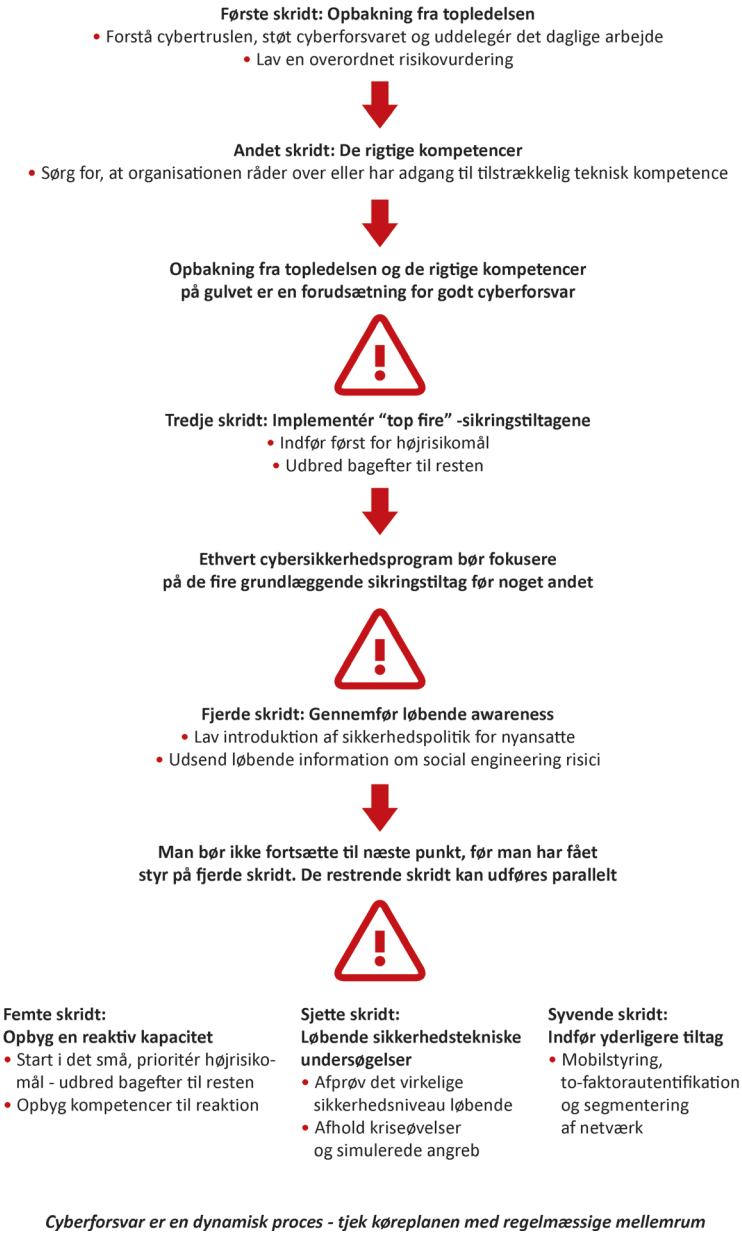
Køreplanens syvende skridt: *Indfør yderligere sikringstiltag*

Selv om "top fire" er grundlæggende - og ethvert cybersikkerhedsprogram bør fokusere på dem før noget andet - er de ikke tilstrækkelige til at kunne imødegå alle angreb.

Myndigheder og virksomheder bør, når de grundlæggende tiltag er på plads, indføre yderligere sikringstiltag på forskellige komponenter fordelt over hele it-miljøet, for eksempel vedrørende anvendelse og styring af mobile enheder.

Derudover kan der i det konkrete tilfælde opstå en situation, hvor forretningshensyn sættes over styr ved implementering af "top fire". I sådanne tilfælde, hvor fordelene opvejes af ulemper, bør "top fire" selvsagt ikke implementeres. I stedet bør midlertidige alternative sikkerhedstiltag overvejes, indtil "top fire" kan gennemføres.

Køreplan for cyberforsvar, der virker



Cyberforsvar er en dynamisk proces - tjek køreplanen med regelmæssige mellemrum

Litteraturliste

Australian Signals Directorate. **Strategies to Mitigate Targeted Cyber Intrusions**, 2012.

Australian Signals Directorate. **"Top 4" Strategies to Mitigate Targeted cyber Intrusions** (teknisk vejledning), 2013

Rigsrevisionen. **Beretning til Statsrevisorerne om forebyggelse af hackerangreb**, oktober, 2013.

UK Department for Business, Innovation & Skills. **Cyber risk management: a board level responsibility**, 2012.

SANS Institute. **The Critical Security Controls**, 2013.

UK Department for Business, Innovation & Skills. **10 Steps to Cyber Security**, 2012.

På Center for Cybersikkerheds hjemmeside, cfcs.dk, er der yderligere information om cybertrusler og cybersikkerhed, herunder løbende opdaterede situationsbilleder og trusselvurderinger samt en årlig risikovurdering.

På Digitaliseringsstyrelsens hjemmeside, digst.dk, kan du finde vejledningen om styring af informationssikkerhed i staten med udgangspunkt i ISO 27001.

Center for Cybersikkerhed
Postadresse: Kastellet 30
Besøgsadresse: Østbanegade 83
2100 København Ø

Email: cfcs@cfcs.dk
Telefon: +45 3332 5580

Center for Cybersikkerhed bidrager til at styrke Danmarks modstandsdygtighed mod trusler rettet mod samfundsvigtig informations- og kommunikationsteknologi og varsler om og imødegår cyberangreb med henblik på at styrke beskyttelsen af danske interesser.

Digitaliseringsstyrelsen
Landgreven 4
Postboks 2193
1017 København K

Email: digst@digst.dk
Telefon: +45 3392 5200

Digitaliseringsstyrelsen står i spidsen for omstillingen til et mere digitalt offentligt Danmark. I forbindelse med informationssikkerhed indtager styrelsen en koordinerende rolle med blandt andet vejledninger til risikovurderinger og awareness. Styrelsen er også ansvarlig for indførelsen af sikkerhedsstandarden ISO 27001 i staten.

CENTER FOR CYBERSIKKERHED

DIGITALISERINGSSTYRELSEN