DIGITALISERINGSSTYRELSEN

CENTER FOR CYBERSIKKERHED

Cyberforsvar der virker

Januar 2017

Cyberforsvar der virker

Forord

Danske myndigheder og 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.

For at imødegå disse trusler arbejder Center for Cybersikkerhed og Digitaliseringsstyrelsen målrettet med at sikre en høj grad af cybersikkerhed i danske organisationer og samtidig tilskynde til, at organisationerne sætter emnet på dagsordenen.

Denne vejledning beskriver en **konkret, prioriteret plan** for, hvordan myndigheder og virksomheder kan mindske risikoen for cyberangreb samt håndtere de værste konsekvenser, når et angreb rammer.

Vejledningen fokuserer på den del af det samlede informationssikkerhedsarbejde, der direkte kan medvirke til at reducere risikoen ved angreb fra internettet (cyberangreb). Øvrige aspekter af arbejdet med informationssikkerhed, så som fysisk sikkerhed eller opbygning af robust it-arkitektur, berøres ikke i denne vejledning.

Forbedring af sikkerheden gennem ændringer i sikkerhedsstyringen og -kulturen kan ikke gennemføres uden ledelsens opbakning hos de enkelte myndigheder og virksomheder. Derfor henvender denne vejledning sig primært til topledelsen og managementniveauet.

Ledelsen skal sikre sig rådighed over de rigtige faciliteter og tekniske kompetencer og udarbejde en plan for organisationens vej gennem vejledningens syv trin.

Status 2016

Udviklingen af malware og hackerangreb har inden for de seneste år betydet, at myndigheder og virksomheder har fået et væsentligt større fokus på cyber- og informationssikkerhed.

Center for Cybersikkerhed og Digitaliseringsstyrelsen vurderer, at der forsat er behov for et øget ledelsesstyret fokus på, hvorledes organisationerne bliver bedre rustet til at imødegå cybertruslerne. Dette øgede fokus skal blandt andet sikre, at relevante sikkerhedsmæssige initiativer gennemføres med de nødvendige og tilstrækkelige ressourcer.

Planens syv trin, som enhver topledelse med fordel bør kende og prioritere, omfatter blandt andet fire grundliggende sikringstiltag, ”Top 4”, som er tiltrådt af en lang række lande og offentlige cybersikkerhedsorganisationer.

Tiltagene vil kunne imødegå op mod 80 procent af cyberangrebene. Vil man have et cyberforsvar, der er mere optimalt, så anbefaler Center for Cybersikkerhed, at alle syv trin i planen bliver fulgt.

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 denne del af grundlaget for fortsat økonomisk vækst sikres.

Det er nødvendigt, at cybersikkerhedsarbejdet tager udgangspunkt i en klar forståelse af, hvordan truslerne kan håndteres. Det er målet, at vejledningen vil bidrage til en klarere forståelse heraf.

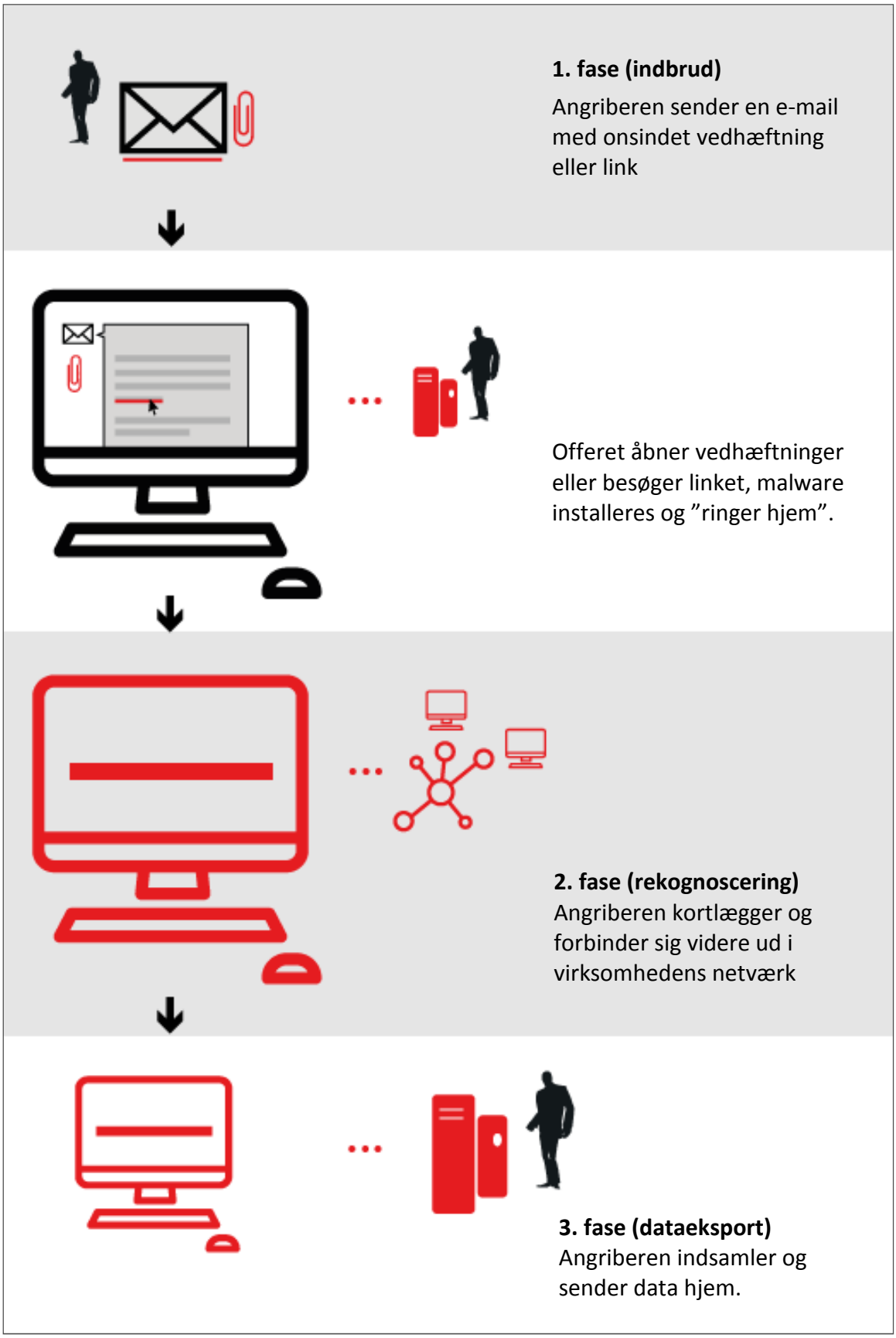
God læselyst.

Thomas Lund-Sørensen
Chef for Center for Cybersikkerhed

Lars Frelle-Petersen
Direktør for Digitaliseringsstyrelsen

Det typiske cyberangreb – et eksempel

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:



Plan for et godt cyberforsvar

Vejledningens består af syv trin, der beskriver, hvordan organisationen kan få et cyberforsvar, der virker.

Trin 1 Forankring i topledelsen

- Forstå cybertruslen, støt cyberforsvaret og uddelegér det daglige ansvar.
- Gennemfør en overordnet it-risikovurdering.

Trin 2 De rette tekniske kompetencer

- Sørg for, at organisationen råder over de rette tekniske kompetencer eller har adgang til dem.

Trin 3 De grundlæggende sikringstiltag

- Implementer tiltagene til sikring af højrisikomål.
- Udbred derefter til øvrige risikomål.

Trin 4 Awareness, awareness, awareness

- Introducer sikkerhedspolitikken for nyansatte.
- Udsend løbende information om cybertruslen.

Trin 5 En reaktiv kapacitet

- Start i det små og prioriter højrisikomål.
- Opbyg relevante reaktive kompetencer.

Trin 6 Løbende sikkerhedstekniske undersøgelser

- Test det reelle sikkerhedsniveau løbende.
- Afhold kriseøvelser og simuler angreb.

Trin 7 Flere tekniske og organisatoriske tiltag

- Styring af mobile enheder, to-faktor-autentifikation, segmentering af netværk.

Trin 1: Forankring i topledelsen
God cybersikkerhed begynder hos topledelsen. Uden forankring i topledelsen fejler selv de bedste hensigter om god cybersikkerhed.

De statslige institutioner styrer informationssikkerheden efter ISO/IEC 27001-standarden. I overensstemmelse med standarden skal der etableres et 'ledelsessystem' til styring af informationssikkerheden. Ledelsessystemet er et samlet udtryk for de politikker, procedurer, beslutningsgange og aktiviteter, som udgør organisationens arbejde med informationssikkerhedsstyring (se litteraturlisten for mere information).

Topledelsen bør i relation til ledelsessystemet søge svar på en række centrale spørgsmål:

- Ved vi, hvad der er vores vigtigste informationer, hvor de er, hvor de anvendes, og hvordan informationsteknologien understøtter vores forretning?
- Ved vi, hvad det betyder for vores forretning, hvis vores vigtigste informationer ændres, stjæles eller lækkes, eller hvis vores it-service er utilgængelig 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 udveksle viden og erfaringer med medarbejdere fra lignende organisationer samt indberette cyberhændelser til Center for Cybersikkerheds underretningsordning?
- Har vi en sikkerhedsorganisation, der er forankret på chefniveau?
- Holder vi os løbende orienteret om de 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 bl.a. disse fordele ved at kende svaret på ovenstående spørgsmål:

- Strategiske fordele ved bedre at kunne indarbejde præcis viden om cybertruslen i organisationens beslutningsprocesser.
- Sikre at investeringer og anvendte ressourcer medfører en forretningsmæssig gevinst.
- Operationelle fordele ved at være forberedt på angreb, reagere effektivt og have cybersikkerhedspolitikken på plads.

Trin 2: De rette tekniske kompetencer
Den daglige opgave med at imødegå cyberrisici uddelegeres af topledelsen, som skal sikre sig, at de rette kompetencer er til stede i organisationen eller tilknyttet denne. Det er vigtigt, at de, der

får opgaven, både forstår organisationens tekniske opsætning og formår at kommunikere med topledelsen. De ansvarlige skal sikre, at opgaverne bliver gennemført af teknisk kompetente medarbejdere.

Der er behov for flere forskellige medarbejderprofiler, herunder f.eks. gode systemadministratorer og medarbejdere med analytiske kompetencer.

Medarbejderne med de rette kompetencer kan være placeret andre steder i organisationen end i it-afdelingen eller hos en leverandør. Det er dog vigtigt, at den enkelte organisation selv tager ansvaret for egen sikkerhed. Der skal være overblik over ressourcer – særligt i forbindelse med en eventuel beredskabssituation.

Trin 3: De grundliggende sikringstiltag

Ethvert cybersikkerhedsprogram bør fokusere på de grundlæggende sikringstiltag før implementering af andre **tekniske** tiltag. Det skyldes, at netop disse fire tiltag reducerer risikoen for cyberangreb væsentligt.

Tiltagene skal implementeres med udgangspunkt i en vurdering af risikoen for tab af fortrolighed, integritet og/eller tilgængelighed for de informationer og systemer, der skal beskyttes. Tabellen på næste side giver et overblik over de grundliggende sikringstiltag. Det er vigtigt at være opmærksom på følgende:

- At implementere de grundlæggende sikringstiltag kan være teknisk komplekst, indebære omkostninger og møde medarbejdermodstand. God planlægning, herunder information til medarbejderne, kan reducere forhindringerne og mindske modstanden. Center for Cybersikkerhed udgiver løbende nye og opdaterede vejledninger, herunder vejledninger om de grundliggende tekniske sikringstiltag.
- Det er it-afdelingen, placeret internt i organisationen eller hos en leverandør, der på grundlag af organisationens risikovurdering bør anbefale, hvilke programmer der må køre på organisationens netværk.
- Hvis programmer eller operativsystemer ikke længere kan opdateres, bør organisationen udarbejde en plan for udfasning eller isolering af disse. Det er forbundet med stor risiko at lade sådanne legacy-løsninger forblive i produktion og dermed påvirke organisationens generelle sikkerhedsniveau.
- Få brugere har behov for lokale administratorrettigheder, og derfor skal disse rettigheder 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. Når der er behov for at anvende lokale administratorrettigheder, bør disse tildeles i en tidsbegrænset periode.
- Med de grundlæggende sikringstiltag implementeret og vel vedligeholdt vil cybersikkerheden være væsentligt forbedret i organisationen. Herefter bør man – baseret på en risikovurdering med udgangspunkt i truslerne mod organisationen – gå videre i retning af et mere avanceret cyberforsvar, herunder de næste skridt i planen.

De grundlæggende sikringstiltag	Med-arbejder-modstand	Etablerings-omkostninger	Drifts-omkostninger	Designet til at forhindre eller detektere et angreb	Designet til at hjælpe med at modvirke angreb i specifik fase.		
					angrebs-fase 1 - indbrud	angrebs-fase 2 – rekognoscering	angrebs-fase 3 – data-eksport
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, f.eks. Adobe Reader, Microsoft Office, Flash Player og Java, med seneste sikkerheds-opdateringer, højrisikoopdateringer inden for to dage.	Lav	Høj	Høj	Forhindre	Ja	Muligt	Nej
Opdatér operativsystem med seneste sikkerhedsopdateringer inden for to dage efter opdateringerne er kommet.	Lav	Medium	Medium	Forhindre	Ja	Muligt	Muligt
Begræns antallet af brugerkonti med domæne- eller lokaladministrator-privilegier. Husk at disse brugere bør anvende separate ikke-privilegerede konti til e-mail og websurfing	Medium	Medium	Lav	Forhindre	Muligt	Ja	Muligt

Der kan være konkrete tilfælde, hvor forretningshensyn sættes over styr ved implementering af de grundliggende sikringstiltag. I sådanne tilfælde, hvor fordelene opvejes af ulemper, bør tiltagene selvsagt ikke implementeres. I stedet bør midlertidige alternative sikringstiltag overvejes, indtil de grundlæggende tiltag kan gennemføres.

Trin 4: Awareness, awareness, awareness

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

F.eks. udføres "social engineering" både via fysisk kontakt, telefonsamtaler og mails 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 det 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.

Trin 5: En reaktiv kapacitet

Intet forsvar er 100 procent sikkert. Succesfulde angreb vil forekomme, men de skal forudses, opdages og håndteres korrekt som del af et forsvar, når den proaktive indsats ikke er tilstrækkelig.

En vigtig forudsætning for dette er **logning** med tilknyttede alarmer. God logning øger chancen for at kunne undersøge et angreb til bunds, men det er de opsatte alarmer, der kan gøre opmærksom på, at noget uønsket er under opsejling. Alternativt kan man gennemføre regelmæssige gennemgange af kritiske logs med henblik på at afdække mistænkelige hændelser i infrastrukturen.

I mange organisationer sker logningen ikke på en fornuftig og optimal måde. Erfaringer viser, at man ofte ikke gemmer de rigtige logs, eller man undlader at gemme de vigtigste detaljer. For nogle organisationer virker opgaven uoverskuelig, og derfor indsamles der ingen logdata. Andre organisationer forsøger at gemme det hele, og de drukner derved i data. Selv med gode logs prioriterer organisationerne ofte ikke at undersøge dem for cyberangreb. Det er vigtigt at være opmærksom på tidsperspektivet i forbindelse med opsætning af logningsværktøjer. Mange angreb opdages først længe efter, at de er gennemført, og derfor kan situationen være, at loggen for længst er slettet. Det gør oprydningsarbejdet svært, fordi der er meget få data at analysere og arbejde med.

Start i det små med få logs af højrisikomål og fokuser på enkelte værktøjer i analyse-platformen. Centralisér logs og få værktøjet til at virke. Udbyg så med flere logs og flere værktøjer. Indfør med andre ord logning ud fra en risikobaseret tilgang. Center for Cybersikkerhed har udgivet vejledningen Logning - en del af et godt cyberforsvar der kan bidrage med yderligere viden på dette område.

En anden væsentlig forudsætning for, at organisationen kan håndtere et cyberangreb, er, at organisationen har velfungerende og velafprøvede handlings- eller beredskabsplaner, der kan iværksættes i situationen. Handlingsplanerne skal tydeligt redegøre for ansvar og opgaver i den konkrete situation og indeholde eventuelle referencer og kontaktinformationer på ressourcer, man om nødvendig kan trække på.

Med andre ord - 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 egne begrænsninger og søge bistand fra professionelle it-sikkerhedseksperter, når det er relevant.

Trin 6: Løbende sikkerhedstekniske undersøgelser

De grundlæggende sikringstiltags dækningsområde, vedligeholdelse og effektivitet bør løbende afprøves gennem proaktive sikkerhedstekniske undersøgelser og øvelser, ligesom øvrige dele i og omkring it-miljøet løbende bør kontrolleres og afprøves.

Sjette trin i planen går billedligt talt ud på hele tiden at "banke på" i it-miljøet 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 bør for eksempel sikre, at organisationens ændringsstyring fungerer korrekt, da netop en mangelfuld proces på dette område ofte er en kilde til problemer og sårbarheder i infrastrukturen. Øvrige centrale it-processer, herunder beredskab, bør ligeledes afprøves regelmæssigt, så det kan verificeres, at disse processer afspejler it-miljøet og aktuelle behov i organisationen. Beredskabet kan eksempelvis afprøves med simulerede angreb, hvor man observerer, hvor hurtigt de bliver opdaget, og hvordan de bliver håndteret. Lever resultatet ikke op til de forretningsmæssige krav, bør der iværksættes udbedrende tiltag.

Ligesom for de øvrige tiltag er det her en forudsætning, at myndigheden eller virksomheden har opbygget eller har adgang til tilstrækkelige tekniske kompetencer.

Trin 7: Flere tekniske og organisatoriske tiltag
Selv om planens første tre trin, inklusiv implementering af de grundlæggende sikringstiltag, er basale, og enhver lokal cybersikkerhedsplan med fordel kan fokusere på dem før implementering af andre tekniske kontroller, så er de ikke tilstrækkelige til at kunne imødegå alle angreb.

Når de grundlæggende tiltag er på plads, bør myndigheder og virksomheder indføre yderligere sikringstiltag fordelt over hele it-miljøet, f.eks. vedrørende anvendelse og styring af mobile enheder.

Referenceliste

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

SANS Institute. Critical Security Controls for Effective Cyber Defense, Oktober 2015

UK NCSC: 10 Steps to Cyber Security, 2015.

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

På Center for Cybersikkerheds hjemmeside, cfcs.dk, er der yderligere information om cybertrusler og cybersikkerhed, herunder en række vejledninger, f.eks:

- Logning - en del af et godt cyberforsvar
- Spearphishing - et voksende problem

På Digitaliseringsstyrelsens hjemmeside, digst.dk, kan du finde vejledningen om styring af informationssikkerhed i staten med udgangspunkt i ISO/IEC 27001-2013. Videnscenter for implementering af ISO27001 | Digitaliseringsstyrelsen

Center for Cybersikkerhed

Postadresse: Kastellet 30

Besøgsadresse: Holsteinsgade 63

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.

Cyberforsvar der virker

'Cyberforsvar der virker' blev første gang udgivet 2013. Denne opdaterede version introducerer syv trin, der beskriver vejen til et godt cyberforsvar :

1. **Forankring i topledelsen**
2. **De rette tekniske kompetencer**
3. **De grundlæggende sikringstiltag**
   - Udarbejd positivliste over applikationer
   - Opdatér programmer
   - Opdatér operativsystem
   - Begræns antallet af brugerkonti med domæne- eller lokaladministrator-privilegier
4. **Awareness, awareness, awareness**
5. **En reaktiv kapacitet**
6. **Løbende sikkerhedstekniske undersøgelser**
7. **Flere tekniske og organisatoriske tiltag**

DIGITALISERINGSSTYRELSEN

CENTER FOR CYBERSIKKERHED FE