FORSVARSMINISTERIET

Et styrket dansk cyberforsvar

Nye værktøjer skal beskytte Danmark i cyberspace

Juni 2021

Indhold

Forsidefoto: Mads Jensen/ Ritzau Scanpix.

Forord

Danmark er dagligt mål for angreb eller forsøg på angreb i cyberspace. Angrebene kan ramme alle. Fra offentlige myndigheder og private virksomheder. Til kritisk infrastruktur eller borgere.

Bagmændene er alt fra småkriminelle til fremmede stater. De udnytter sårbarhederne i vores digitaliserede samfund til at angribe vores virksomheder, forsvar og myndigheder. Vores hverdag og vores værdier. Men vi må aldrig lade ansigtsløse spioner og hackere slå skår i vores samfunds stabilitet og levevis.

Derfor skal vi hele tiden være på vagt over for nye trusler. Mod vores myndigheder, kritiske infrastruktur og virksomheder og arbejdspladser. Mod os selv og vores nærmeste.

Det kræver, at vi er et skridt foran. Investerer og opbygger – både i systemer og kompetencer. Også selvom angrebene ikke er synlige for øjet eller i bedste fald afværges. Konsekvenserne hvis vi ikke handler rettidigt kan være endog meget store. Derfor er det afgørende, at vi står vagt om vores tryghed og sikkerhed – også i cyberspace.

Dette udspil, der er baseret på myndighedernes anbefalinger, afspejler en stribe forslag til investeringer i værktøjer, der skal styrke vores værn mod cybertruslen. Det er værktøjer, der opsnapper og forebygger angreb, der er på vej. Værktøjer der sikrer, at et cyberindsatshold med specialister kan rykke ud, når der er angreb. Og værktøjer der gør os i stand til at identificere og forfølge bagmændene. Samtidig er det afgørende, at vi får udbredt forståelsen af cybertruslen bredere i vores samfund – og at vi får endnu flere kompetencer og kræfter bragt i spil i kampen mod cyberangreb.

Udspillet ”Et styrket dansk cyberforsvar” skal styrke Danmarks evne til at modstå cybertrusler. Det har betydning for borgere og virksomheder. Det er afgørende for vores tryghed og sikkerhed.

Trine Bramsen
Forsvarsminister

Et styrket dansk cyberforsvar

Regeringen vil over de kommende år iværksætte nye tiltag, der styrker Danmarks cyberforsvar. Det sker på baggrund af myndighedernes anbefalinger.

Tiltagene skal samlet løfte Danmarks evne til at opfange og varsle danskerne om angreb, øge hjælpen når angrebene rammer og sætte øget fokus på uddannelse af fremtidens talentmasse.

Datamonitorering skal opfange og varsle om cyberangreb

Nyt digitalt bolværk skal bremse og beskytte mod angreb

Rådgivning skal nå virtuelt og fysisk ud til brændpunkter

Uddannelse og forskning skal opdyrke talenter

Offensive værktøjer skal udpege og sanktionere bagmændene

Videndeling skal sikre fælles front mod sårbarheder

Styrket dansk cyberforsvar til gavn for hele samfundet

Danskernes hverdag er digital

Vores hverdag i Danmark er på få årtier gået fra at være analog til at være digital. Det er en udvikling, vi nyder godt af hver eneste dag. Som giver os masser af fordele. Under coronakrisen har vores digitale hverdag været med til, at vi som samfund har klaret os bedre igennem krisen end mange andre lande, fordi mange har kunnet arbejde hjemmefra. Til gavn for vores demokrati, økonomi og samfundets sammenhængskraft.

Men med muligheder følger også udfordringer. Den digitale udvikling efterlader sprækker af sårbarheder. Sprækker, som for de forkerte mennesker er en åben dør ind til unik viden og personlige oplysninger.

Cybertruslen rammer ind i kernen af vores samfund. Vores måde at leve på. Det er kort sagt en trussel mod vores velfærd, værdier og sammenhængskraft.

Vores hverdag er truet

Truslen i cyberspace er alvorlig. Forsvarets Efterretningstjeneste vurderer den som ”meget høj” – det højest mulige niveau.

Fremmede magter kan bruge internettets anonymitet til at spionere. Til at stjæle viden fra myndigheder og virksomheder. Og til at påvirke vores holdninger med falske nyheder og desinformation og endda gennemføre destruktive angreb.

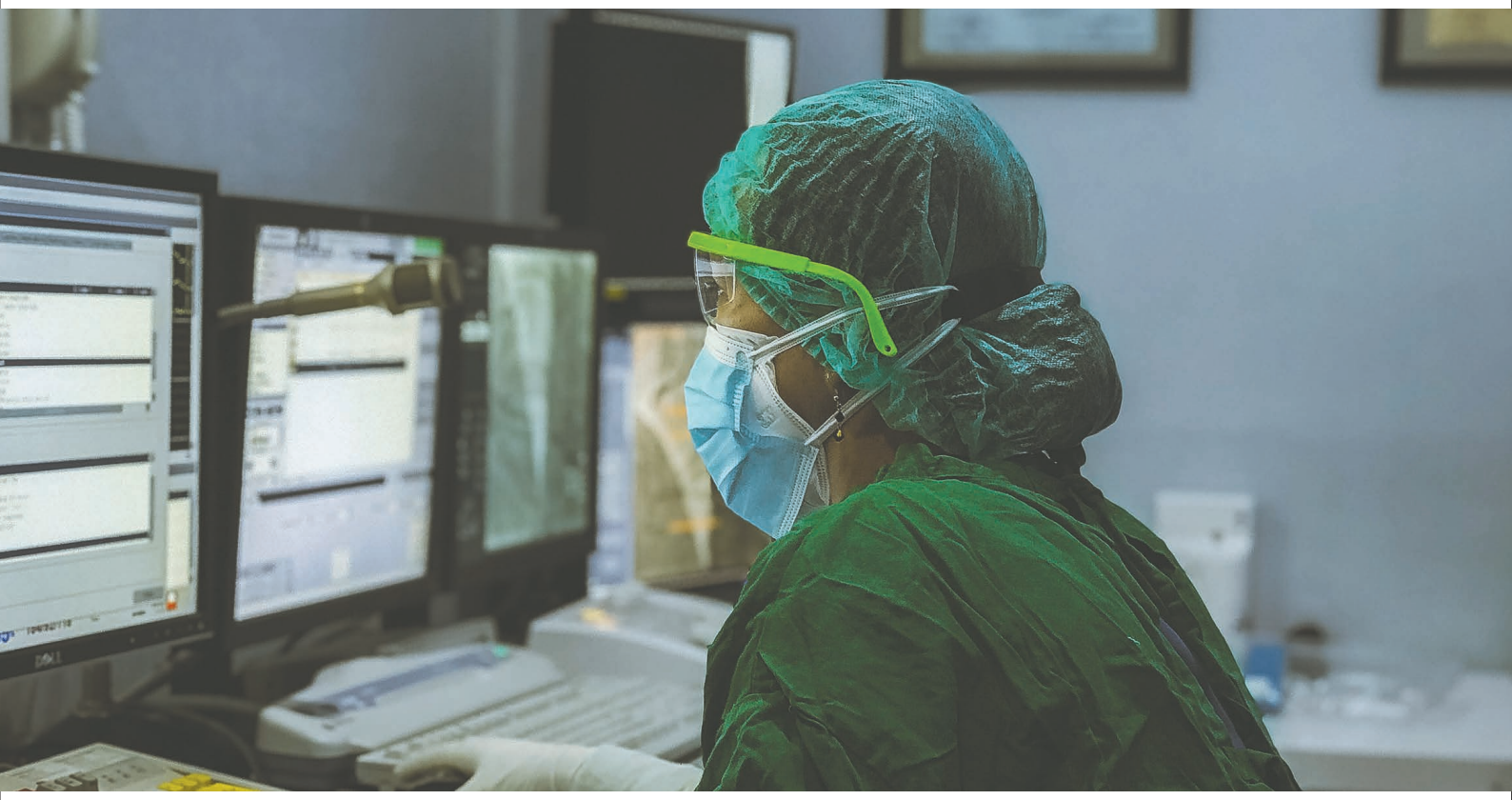

Foto: Irwan. Unsplash.

Tal på truslen

- **En tredjedel af store danske virksomheder** har oplevet brud på it-sikkerheden (fx mistet adgang til it-services, sletning af data eller læk af fortrolige data)
- **Halvdelen af alle danskere** har oplevet brud på it-sikkerheden (fx phishing-mails, falske hjemmesider eller misbrug af kortoplysninger)

Tal fra Danmarks Statistik, 2020.

Foto: Bermix Studio. Unsplash.

Konsekvenserne er enorme

Cyberangreb har allerede kostet danske virksomheder dyrt. I enkelte tilfælde i milliardstørrelsen. Statslige aktører og cyberkriminelle tager hele tiden nye metoder i brug, som øger omkostningerne for borgere, virksomheder og myndigheder. Og som risikerer at lamme centrale og kritiske dele af samfundet.

Eksperter anslår, at cyberangreb og cyberkriminalitet sidste år kostede verdenssamfundet næsten 1.000 milliarder dollars. Det er mere end det dobbelte af hele Danmarks BNP.

Derfor er det afgørende, at Danmark er rustet til fremtidens cybertrusler. For cyberangreb er en trussel, vi ikke bare skal leve med, men også må bekæmpe.

Første skridt

Regeringen vil efter myndighedernes anbefalinger tage første skridt mod et styrket dansk cyberforsvar, der med nye værktøjer kan tage kampen op i cyberspace.

Værktøjer, der kan bygges videre på i fremtiden. Det gælder også i kommende forsvarsforlig.

Nye tiltag

På baggrund af myndighedernes anbefalinger foreslår regeringen, at der over de kommende år bygges videre på de indsatser og resultater, som er opnået siden Center for Cybersikkerhed blev oprettet i 2012.

For selv om vi er kommet langt, er trusselsbilledet blevet mere alvorligt. Mere aktuelt. Og mere komplekst. Derfor vil vi iværksætte nye tiltag – rettet mod myndigheder, virksomheder og borgere i hele landet.

Cyberforsvar er et kapløb, hvor vi ikke har råd til at ligge midt i feltet, men konstant må arbejde på at være foran.

Der lægges op til at investere ca. 210 mio. kr. i:

- Avanceret datahåndtering
- Styrket cyberanalyse
- Bedre detektion af avancerede cyberangreb
- Understøtte nordatlantisk cybersikkerhed
- Bedre analyse af phishingmails

Foto: Adi Goldstein. Unsplash.

Datamonitorering og varsling

Vi skal opfange og afdække cyberangreb, der kan sætte vores hverdag i stå. Derfor anbefaler myndighederne, at vi monitorerer data med ny teknologi, der kan varsle offentlige myndigheder og de samfundskritiske virksomheder om angreb.

Dataanalyse

Avanceret dataanalyse skal opfange de cyberangreb, der er på vej. Vi skal kort sagt kunne kigge med og varsle danskerne, når hackerne kigger os over skulderen. Så vi er klar til at stå imod. Men også bedre i stand til at styrke vores viden om bagmændenes værktøjer. For ser vi de spor, som hackerne efterlader, kan vi nå at stoppe dem, før de tager næste skridt. Derfor skal der investeres i ny computerkraft og software, som hurtigt kan analysere enorme datamængder og varsle, når nogen forsøger at trænge ind i vores systemer.

Til øget gavn for samfundet

Vi er bedst i stand til at varsle, når vores systemer taler sammen og opdager sårbarheder på tværs af samfundet og vores hverdag. Derfor er den kritiske infrastruktur i Danmark tæt knyttet til de opgraderede analyseværktøjer (fx energisektoren og sundhedsområdet). Efter gensidig aftale konsolideres understøttelsen af Nordatlanten i forhold til at varsle om angreb.

Der lægges op til at investere ca. 105 mio. kr. i:

- Filter mod malware og phishing samt logning af trusler
- Sikret cloudløsning i Forsvaret
- Systemoverblik mhp. automatisering, sikkerhedstjek mv.
- Teknisk løsning til overførsel af klassificeret data
- Mere robuste systemer med færre sårbarheder
- Fælder og snubletråde (honeypots og sinkholes)
- Sikkerhedsgodkendelse af Forsvarets it-systemer og kritisk infrastruktur
- Styrket registrering af klassificerede dokumenter

Foto: Forsvaret.

Digitalt bolværk

Vi skal stoppe de fremmede magter, som sniger sig ind på vores samfund og Forsvar. Derfor lyder anbefalingen fra myndighederne, at vi opsætter et teknisk bolværk, der beskytter kritisk data, alt imens det vildleder spioner og hackere. Samtidig ruster vi os til kamp med et styrket skjold mod hackerangreb og sikkerhedsgodkendelse af private it-systemer.

Falske netværk

Når cyberspioner trænger ind i vores it-systemer, skal de ikke have frit spil. Der skal opsættes digitale snubletråde og falske netværk. Så vi afleder cyber-angreb, aflurer spionernes metoder og er parate, hvis spionerne senere finder vej til de rigtige netværk. Samtidig skal hackerangreb kunne bremses ved at omdirigere angreb fra inficerede computere til et digitalt sort hul.

Værn mod angreb

Vi skal varsle, og vi skal være klar til at begrænse angreb. Men vi skal også være bedre til at beskytte os selv. Vi skal sikre, at de som spionerer mod myndigheder og ikke mindst Forsvaret bliver mødt af nye værn og forhindringer; bl.a. sofistikeret sporing og logning af trusler, mere robuste enheder, styrkede dataplatforme og medarbejdere, som er trænet i cyberparathed.

Cyberskjold

Det er vigtigt, at vi lærer af tidligere cyberangreb. Et styrket cyberskjold skal sikre, at vi kan begrænse datatrafik til danske myndigheder, hvis erfaringer fortæller os, at der er tegn på cybertrusler. Der skal kort sagt opbygges et skjold, der gør os bedre til at forhindre malware og andre trusler, hver gang vi angribes i cyberspace.

Sikkerhedsgodkendelser

Det skal gøres lettere og hurtigere for danske virksomheder at få sikkerhedsgodkendt it-løsninger, som kan konkurrere på det internationale marked. Flere tekniske eftersyn hos myndigheder og samfundskritiske virksomheder skal også bidrage til, at vi løfter samfundets cyberberedskab i fælles flok.

Der lægges op til at investere ca. 105 mio. kr. i:

- Nyt cyberindsatshold (genopretning)
- Bedre rådgivning til statslige myndigheder
- Udbygning af samarbejde med de samfundskritiske sektorer
- Udvidet kapacitet til at følge udvikling i tele/5G
- Nordatlantisk rådgivningsteam
- Digital rådgivning af myndigheder og virksomheder
- Analytisk kapacitet ift. cyberkriminalitet og spionage
- Styrket cybersikkerhed på ambassader
- Øget kapacitet til sårbarhedsanalyser

Observation fra Fennec-helikopter over Esbjerg. Foto: Rune Dyrholm.

Rådgivning og decentral understøttelse

Vi skal kunne træde til og rådgive, når vores samfund er under angreb. Derfor skal der bl.a. oprettes cyberindsatshold, så specialister med kort varsel kan rykke ud til samfundets kritiske digitale brændpunkter. Større tilstedeværelse på tværs af Danmark og ny digital rådgivning skal også sikre, at vi i endnu højere grad kan støtte myndigheder og danske virksomheder i den kritiske infrastruktur.

Cyberindsatshold

Vi skal fysisk rykke ud og yde afgørende rådgivning, når der sker angreb mod det offentlige og de virksomheder, som får hverdagen til at fungere. Flere indsatshold bringer os tættere på – så vi begrænser angrebene, før de breder sig yderligere – og samler erfaringer, så vi er bedre rustet, når bagmændene slår til igen.

Cybersikkerhed for hele Danmark

Center for Cybersikkerhed er Danmarks cyberhjerne. Den anbefaler myndighederne, at vi giver mere kraft, hvor truslen er høj, og efterspørgslen er størst: I de kritiske sektorer, blandt virksomheder og på tværs af øverste ledelsesniveau hos statslige myndigheder. Det gælder i hele landet. Derfor er ambitionen også at styrke cybertilstedeværelsen i Vestdanmark gennem myndigheder, uddannelse mv. Det er initiativer, som der kan bygges ovenpå fremover – også i kommende forsvarsforlig. Derudover styrkes muligheden for vejledning og teknisk bistand til nordatlantiske myndigheder.

Digital krisehjælp

Alle kan blive udsat for cyberangreb – derfor skal vi undersøge muligheden for bedre hjælp i det daglige. Der lægges finansiering til side med henblik på at understøtte en eventuel ny digital krisehjælp, så virksomheder og borgere kan få rådgivning på telefon og mail, hvis de fx udsættes for cyberangreb eller systematiske phishing-forsøg.

Der lægges op til at investere ca. 10 mio. kr. i:

- Permanent cyberværnepligt
- Styrket uddannelse ved Forsvarsakademiet
- Udbygning af forskning og uddannelse

Cyberværnepligtige under uddannelse. Foto: Forsvaret.

Uddannelse og forskning

Skal vi stå stærkt i cyberspace, kræver det ikke bare avanceret teknik, men også skarpe hoveder. Derfor lægges der op til at understøtte talentudviklingen ved at gøre cyberværnepligten permanent, skabe nye uddannelsesmuligheder og generelt målrette forskning og uddannelse.

Permanent cyberværnepligt

Cyberværnepligten i Fredericia har vist sig at være en stor succes, og de gode erfaringer skal bidrage endnu mere til it-sikkerheden hos Forsvaret, virksomheder og i det offentlige. Derfor lægges der op til at gøre cyberværnepligten permanent, så vi også fremover kan inspirere unge talenter til at være med på cyberfronten.

Nye uddannelsesmuligheder

Cybertruslen forandrer sig hele tiden. Derfor skal vi sikre uddannelsesmuligheder, som gør os i stand til at følge med. Forsvarsakademiet vil løfte uddannelse på området ved at tilbyde en ny master i efterretnings- og cyberstudier i samarbejde med Syddansk Universitet, der ligesom nye kurser og efteruddannelse skal bidrage til, at vi er på forkant med udviklingen.

Cyberforskning

Efterspørgslen på forskning inden for cybersikkerhed er enorm – vi skal sikre, at udbuddet er fokuseret og følger med. Derfor lægges der op til at udvide eksisterende forskningsinitiativer, så cyber bringes i spil på nye måder og over for en bredere målgruppe. Nye aktiviteter skal også skabe synergier inden for et smalt vidensfelt, så vi udnytter vores viden om cybersikkerhed så effektivt som muligt.

Der lægges op til at investere ca. 40 mio. kr. i:

- Styrket cyberkapacitet til operative indsættelser
- Planlægning, drift og udvikling af offensive cyberoperationer
- Styrket kapacitet til opsporing og sanktioner
- Detektion af påvirkningstrusler på sociale medier
- Pulje til internationale cybersikkerhedsrelaterede stillinger

Illustration: Forsvarets Efterretningstjeneste.

Offensive værktøjer

Et effektivt cyberforsvar kræver, at vi kan tage kampen op i cyberspace. Derfor skal vores offensive værktøjer forbedres, så vi med eksempelvis større computerkraft og teknisk ekspertise kan standse bagmændene og på sigt svare igen på deres angreb.

Indsats mod påvirkning

Danskere og virksomheder færdes på sociale medier. Et sted hvor ikke alle desværre er, hvem de giver sig ud for at være. Det gælder også fremmede magter, som med koordineret brug af desinformation og falske profiler puster til følsomme emner, der sår splid i befolkningen og kan påvirke vores demokrati. Derfor skal vi blive bedre til at spore, opfange og begrænse udenlandske påvirkningsforsøg.

Ny slagkraft

Der er brug for, at vi styrker vores evne til at slå igen i cyberspace, hvor det er nødvendigt. Derfor skal vi vurdere lovgivningen og sammen med Forsvaret udvikle muligheden for indsættelse af offensive cyberkapaciteter, der kan bruges mod fx terrorgrupper eller pirater, som truer Danmark og danske interesser.

Fokus på bagmændene

Cyberspace er i vidt omfang et lovløst land, hvor anonyme bagmænd har lang snor, og deres angreb sjældent har konsekvenser. Derfor skal vi styrke de værktøjer – tekniske og diplomatiske – som kan udpege, sætte navn på og føre til sanktioner og konsekvens for personer, organisationer og stater, der står bag cyberangreb.

Der lægges op til at investere ca. 30 mio. kr. i:

- Styrkelse af lokal cybersikkerhed
- Styrkelse af samfundets it-beredskab
- Videreførsel af Cybersikkerhedsrådet
- Nyt cyberhjemmeværn

Krisestabsøvelse - Forsvaret og Politiet samarbejder. Foto: Iben Valery.

Videndeling

Danmark har som lille land god mulighed for at dele viden på tværs af myndigheder, virksomheder og uddannelsesinstitutioner – det skal vi blive bedre til at udnytte gennem fx nye beredskabsøvelser. Samtidig videreføres Cybersikkerhedsrådet, og der undersøges fordele og ulemper ved en styrket civil forankring af Center for Cybersikkerhed. Med opbygning af et nyt cyberhjemmeværn vil regeringen også tiltrække talenter og sikre et Hjemmeværn, der følger med tiden.

It-beredskabsplan

Et robust beredskab er helt nødvendigt, hvis vi skal kunne håndtere fremtidens kriser. Derfor skal der udarbejdes en it-beredskabsplan og gennemføres flere øvelser, hvor myndigheder og samfundskritiske virksomheder går sammen om at trykteste vores fælles cyberforsvar.

Cybersikkerhedsrådet består

Cybersikkerhedsrådet er en vigtig rådgiver for vores myndigheder – det skal vi holde fast i. Medlemmer fra både erhvervsliv, myndigheder, forbrugere og forskningsverdenen sikrer en stærk videndeling om cyber- og informationssikkerhed, som vi også skal drage fordel af i fremtiden.

Civil forankring af Center for Cybersikkerhed

Vi skal undersøge Center for Cybersikkerheds organisatoriske placering og ansvar med henblik på at afdække fordele og ulemper ved en styrket civil forankring.

Nyt cyberhjemmeværn

Vi skal organisere borgere med særlig evne eller interesse for IT, så de kan hjælpe med cyber-relaterede opgaver i krisesituationer og udbrede forståelsen af cybersikkerhed. Regeringen vil derfor oprette et cyberhjemmeværn som en del af Hjemmeværnet, så vi på tværs af Danmark bliver bedre til at udnytte civile it-kompetencer og ikke mindst tiltrække dygtige folk. Kort sagt et Hjemmeværn, der følger med tiden, og som der kan bygges ovenpå i fremtiden.

Økonomi

Oplæg til udmøntning af cyberpuljen (mio. kr.)

Område	2021-2023
Datamonitorering og varsling	210
Teknisk bolværk	105
Rådgivning og decentral understøttelse	105
Uddannelse og forskning	10
Offensive værktøjer	40
Videndeling	30
I alt	**500**

FORSVARSMINISTERIET

Holmens Kanal 9
1060 København K
DK - Denmark

Telefon + 45 7281 0000
E-mail: fmn@fmn.dk
www.fmn.dk