Rådet for Digital Sikkerhed

Kære læser

Velkommen til marts måneds nyhedsbrev fra Rådet for Digital Sikkerhed. I dagens kronik i Børsen (11. marts 2024) gør Rådet for Digital Sikkerhed status i forhold til de centrale udfordringer på digitaliseringsområdet.

Sprækker i Danmarks digitale maskinrum

Henning Mortensen, Rådets formand og Claus Hjorth, sekretariatschef

I Danmark bryster vi os af at gå hele vejen med digitaliseringen af den offentlige sektor og erhvervslivet. Senest blev Danmarks digitale selvforståelse bekræftet af en flot samlet andenplads i OECD's Digital Government Index, der blev offentliggjort i januar 2024, blandt 33 medvirkende lande.

Rumlende alarmklokker
Imidlertid rumler alarmklokkerne. I 2023 oplevede den danske energisektor sit første store cyberangreb, flere mindre virksomheder mistede deres data via et hackerangreb hos deres eksterne it-leverandør. Alt for mange borgere blev svindlet af dygtigt gennemført digitalt tyveri.

Det digitale Danmark stod året igennem, men der er mindst tre sprækker i det ellers robuste fundament:

Den første sprække så vi, da Rigsrevisionen i december 2023 fremlagde deres beretning om it-sikkerheden på Statens It-servere. Med sit velkendte skarpe ordvalg – "utilfredsstillende" – vurderede Rigsrevisionen, at Statens It hverken har styr på egne servere eller de systemer, som findes rundt i staten.

På et samråd i januar 2024 blev det tydeligt, at problemstillingen navnlig handler om "teknisk gæld" og om det delte sikkerhedsansvar mellem Statens It og statens forskellige myndigheder.

Den tekniske gæld handler om, at fordi netop Danmark gennem mange år har udbygget sin digitale infrastruktur, så står vi i dag med systemer, som er vigtige for den offentlige service, men som ikke lever op til aktuelle sikkerhedskrav.

Teknisk gæld handler ikke kun om penge, men om balancen mellem at opretholde digital service, mens man opdaterer og udskifter systemerne. Den opgave handler om ledelse, kompetente medarbejdere og samarbejde på tværs af myndighederne og mellem det private og det offentlige.

Manglende dataetik
Den anden sprække begyndte at slå rod i starten af 2024 med Datatilsynets længe ventede afgørelse om brugen af Google Workspace i folkeskolen. Afgørelsen siger

kort, at der ikke er hjemmel til videregivelse af personoplysninger til Google til alle de formål, der videregives til i dag.

Datatilsynet anerkender på den ene side, at der i dag sker en væsentlig højere grad af dataindsamling for, at systemerne overhovedet kan fungere. På den anden side har man hverken har haft det fornødne fokus på databeskyttelsesreglerne eller hensynet til borgerne.

Chromebook-afgørelsen er et tydeligt signal om, at dataetikken ikke har været fast følgesvend i udbygningen af det digitale Danmark. Digital fascination, pilotprojekttænkning og disruption har i lidt for stor udstrækning har været kodeordene, mens stikord som sikkerhed, dataansvar, privatlivsbeskyttelse og gennemsigtighed stod for langt nede på listen.

Resultatet står vi med nu: Udover at adressere de helt fundamentale menneskeretlige aspekter, skal vi til at rydde op med jura, leverandørstyring, standarder og informationssikkerhedspolitikker som værktøjer.

Få lovgivning på plads
En tredje brik til det noget vingeskudte digitale foregangsland er den pludselige udskydelse af den danske implementering af EU's NIS2-direktiv om cybersikkerhed, der var planlagt fremsat for Folketinget her i februar, men nu først sker til oktober.

Rådet for Digital Sikkerhed har tidligere givet udtryk for, at hvis lovgivningen kommer meget sent, så har danske virksomheder ringe mulighed for at justere deres sikkerhedsorganisation, systemer og leverandørstyring, som er helt afgørende for NIS2-direktivets målsætning om bedre cyberforsvar.

Vi har også udtrykt bekymring i forhold til, om det spredte ministeransvar vil medføre uigennemsigtighed og overbureaukrati, især for de virksomheder, der skal følge flere regelsæt inden for cybersikkerhed.

I lyset af forsvarsministerens melding om en hovedlov, der vil læne sig tæt op ad NIS2-direktivet, kan vi kun gentage opfordringen til, at de berørte ministerier rækker ud til de virksomheder, der har den egentlige opgave med at sikre Danmark, for at skabe det bedst tænkelige afsæt for den kommende række af NIS2-bekendtgørelser.

Vi skal ikke tabe pusten på digitaliseringen af Danmark, men trække vejret dybt. På sin vis er det heldigt, at vi har været ramt af cyberangreb, at vi vedkender os den tekniske gæld, og at Datatilsynet har råbt vagt i gevær i forhold til dataetikken.

Vi har et rigtig godt udgangspunkt for at få ryddet op og tage nye digitale teknologier i brug. Belært af fortiden skal vi blot huske, at sikkerhed, databeskyttelse og dataetik skal gå hånd i hånd med innovationen i langt højere grad end hidtil.

Rådets vejledning om informationssikkerhed i danske virksomheder

Danske virksomheder har en vigtig opgave med at sikre deres digitale systemer. Ikke kun for at sikre virksomheden, men også for at gøre det danske samfund mere

robust mod digitale angreb som følge af de ændringer der sker i trusselsbilledet.

Derfor har Rådets faggruppe om NIS2 og cybersikkerhed i en ny vejledning samlet gode råd og relevante links om informationssikkerhed. Vejledningen henvender sig særligt til SMV'erne og giver et hurtigt og kvalitetstjekket overblik over de mange specialiserede vejledninger, der kan understøtte arbejdet med at højne den digitale sikkerhed.

Frem mod den kommende danske lovgivning om cybersikkerhed (implementeringen af EU's NIS2-direktiv, der ventes fremsat for Folketinget til efteråret), vil vejledningen forhåbentlig tjene til øge opmærksomheden og identificere sikkerhedskritiske digitale løsninger blandt danske virksomheder.

Link til Rådets vejledning om informationssikkerhed fra februar 2024

Chromebook-sagen

Som omtalt i lederen er Datatilsynet i januar 2024 fremkommet med sin afgørelse om brugen af Google Workspace i folkeskolen (Datatilsynet 2024 01). Med afgørelsen giver Datatilsynet kommunerne et påbud om at bringe behandlingen i overensstemmelse med reglerne ved at sikre, at der er hjemmel til alle de behandlinger, der sker. Det kan eksempelvis ske ved:

- At kommunerne ikke længere videregiver personoplysninger til Google til disse formål. Det vil sandsynligvis kræve, at Google udvikler en teknisk mulighed for, at de pågældende datastrømme afskæres.
- At Google selv afstår fra at behandle oplysningerne til disse formål.
- At Folketinget tilvejebringer et tilstrækkeligt klart retsgrundlag for videregivelse til disse formål.

Kommunerne skal efterleve påbuddet fra 1. august 2024, men skal senest 1. marts tilkendegive, hvordan de har til hensigt at efterleve det.

KL har den 1. marts 2024 besvaret Datatilsynet på vegne af 52 berørte kommuner.

I forhold til de første to forslag, der begge adresserer ændringer i praksis inden for gældende ret, bemærker KL: ”KL er i dialog med Google om begge mulige veje og har bedt Google oplyse, om det er muligt at løse sagen ad disse to veje. Google har i den forbindelse meddelt KL, at den behandling og til de formål, som Datatilsynet mener er ulovligt, mener Google, de kan levere på. Google mener at kunne leve op til påbuddene ved en kombination af ovenstående to veje.”

I forhold til den tredje mulighed – etablering af nyt og præciseret retsgrundlag – bemærker KL: ”KL finder, at denne vej også er et nødvendigt element i at løse sagen. Ift. denne vej konstaterer KL samtidig, at Datatilsynet finder, at udfordringerne med hjemmel ikke synes at være en isoleret udfordring ift. Folkeskoleloven. KL har derfor i forlængelse af afgørelsen anmodet regeringen ved tre ministre om at sikre, at der er tilstrækkeligt retsgrundlag til anvendelse af digitale og teknologiske værktøjer, så lovgivningen følger med og tager højde for den teknologiske udvikling.”

Læs Datatilsynets afgørelse af 30. januar 2024 her
Læs KL’s svarskrivelse af 1. marts 2024 til Datatilsynet her

Den danske lovgivning om NIS2-direktivet er udskudt til efteråret

Forsvarsministerens forslag til 'Lov om implementering af NIS2-direktivet' var oprindelig planlagt til februar 2024, men er som omtalt i lederen nu udskudt.

I et svar til Folketingets digitaliseringsudvalg skriver ministeren, at det er forventningen, at hovedloven sendes i høring til foråret med forventet fremsættelse i begyndelsen af oktober 2024.

Det fremgår af forsvarsministerens svar, at lovforslaget "… udarbejdes efter regeringens principper om minimumsimplementering. Dermed vil erhvervslivet i forhold til direktivet ikke blive pålagt mere byrdefulde krav end den forventede implementering i sammenlignelige EU-lande. Udkastet til lovforslag vil således lægge sig tæt op ad direktivets ordlyd."

Læs forsvarsministerens svar af 5. februar 2024 til Folketingets digitaliseringsudvalg her

---

Overbelastningsangreb mod danske hjemmesider

I slutningen af februar blev flere hjemmesider hos navnlig den danske transportsektor angrebet af et såkaldt DDoS-angreb. Ifølge DR Nyheder (25.2) blev brugernes adgang til hjemmesider hos lufthavne, Movia og DOT (Din Offentlige Transport) samt Thisted kommune forhindret, og det er sandsynligt, at den pro-russiske hackergruppe NoName057(16), stod bag angrebene.

Center for Cybersikkerhed udsendte 26. februar 2024 en status om angrebene, der hverken be- eller afkræftede ovennævnte oplysninger, men manede til besindighed:

"Man skal huske på, at overbelastningsangreb rammer hjemmesider, der oftest i sig selv ikke bærer kritisk information. Desuden rykker aktivisterne hurtigt videre, når de ramte organisationer får modforanstaltninger op at stå. For aktivisterne handler det om at få opmærksomhed, og når angrebet bliver fanget af tekniske modforanstaltninger, har angrebet ikke længere en synlig effekt. Så selvom aktivisters overbelastningsangreb kan have en meget synlig effekt, så er de langt fra lige så bekymrende som for eksempel kriminelles og staters løbende forsøg på at ramme danske myndigheder og virksomheder," siger vicedirektør Mark Fiedel fra Center for Cybersikkerhed.

Læs mere om DDoS-angrebene hos DR (25. februar 2024) her

Læs mere om CFCS status af 26. februar 2024 her

Læk af kildekode fra Netcompany

Ifølge TV2-nyhederne (28.2) er en 34-årig mand blevet sigtet for, at han "… under særligt skærpende omstændigheder via et brugernavn og adgangskode til Udviklings- og Forenklingsstyrelsen har skaffet sig adgang til en server i styrelsen, hvorfra der blev downloadet kildekode fra styrelsens datasystem.

Herefter skal han have delt kildekode og password på to forskellige hjemmesider, som pressen ikke må gengive. Det er sket i januar og februar 2024.

Desuden er han sigtet for … at have fremsat trusler om betydelig skade på gods, idet han skrev til en række ansatte i Skattestyrelsen."

Presseomtalen har foranlediget Datatilsynet til at rette henvendelse til Netcompany (28.2) om der i forbindelse med sagen er sket brud på databeskyttelsesreglerne. Datatilsynet angiver, at de ikke har modtaget underretninger herom og ønsker blandt andet svar på, om "… Netcompany har kendskab til personoplysninger i det kompromitterede materiale, hvilke systemer der er omfattet, om Netcompany som databehandler har underrettet de berørte dataansvarlige om eventuelle risici for de registrerede (eksempelvis borgere), og om de lækkede oplysninger kan bruges til at få adgang til personoplysninger."

Læs mere om TV2's pressedækning (28.2) her
Læs mere om Datatilsynets henvendelse af 28. februar 2024 til Netcompany her

Det Nationale Koordinationscenter for Cybersikkerhed

Den 31. januar 2024 lancerede Digitaliseringsstyrelsen og Erhvervsstyrelsen et nyt EU forankret center for cybersikkerhed i Danmark (NCC-DK).

Formålet med NCC-DK er at styrke den danske cybersikkerhedssektor, forøge det danske hjemtag af cybersikkerhedsmidler fra EU samt støtte udvikling og anvendelse af innovative cybersikkerhedsløsninger.

NCC-DK er ansvarlig for at styrke samarbejdet inden for Danmarks cybersikkerhedssektor, herunder at danne professionelle faglige netværk. NCC skal også administrere en række tilskudspuljer finansieret af EU, Digitaliseringsstyrelsen og Erhvervsstyrelsen, som fokuserer på at støtte brancherettede cybersikkerhedsløsninger og fremme viden- og datadeling. Fra 2024 til 2025 er der i alt afsat 17,3 millioner kroner til disse tilskud.

NCC-DK indgår i et netværk af koordinationscentre i hele EU, og er etableret og delvist finansieret som led i EU's cybersikkerhedsstrategi.

Læs mere om NCC-DK her

EU's ministerråd har enstemmigt godkendt EU forslag til AI-Act

I Rådets nyhedsbrev fra december 2023 skrev vi, at medlemslandene og EU-parlamentet var nået til enighed om væsentlige elementer i den kommende AI-forordning (Artificial Intelligence Act) i de såkaldte trialog-forhandlinger. Den 2. februar 2024 blev medlemslandenes tilslutning til den kommende AI Act genbekræftet i enighed.

Ifølge Thierry Bretton, EU-kommissær for det indre marked, har EU sammen med (gen)bekræftelsen nået to milepæle:

“We reached two important milestones in our endeavour to turn Europe into the global hub for trustworthy AI:

- **Today**, EU Member States unanimously endorsed the political agreement that we reached in December on the AI Act. The agreement resulted in a balanced and futureproof text, promoting trust and innovation in trustworthy AI.
- **Last week**, we adopted a wide range of measures to support Europe’s AI start-ups, complementing the regulatory framework. Both milestones are equally important for European innovators in AI. They reflect our comprehensive approach to AI: promoting both trust and excellence in AI.”

Læs Thierry Brettons linkedin-opslag fra 2. februar 2024 her

Regeringens ekspertgruppe om tech-giganter offentliggør anbefalinger om kunstig intelligens

Sidst i februar offentliggjorde regeringens ekspertgruppe 13 anbefalinger om tech-giganters udvikling og anvendelse af kunstig intelligens.

Anbefalingerne har til formål at give kunstig intelligens den plads i vores samfund, som gør det muligt at udnytte de mange potentialer og samtidig imødegå skadevirkningerne i forhold til bl.a. børn og unge.

Anbefalingerne er bygget op omkring fire temaer:

- Tech-giganternes medansvar for informationstroværdighed på deres platforme
- Beskyttelse af børn og unge mod skadelig anvendelse og udvikling af kunstig intelligens på tech-giganternes tjenester
- Regulering af tech-giganters uautoriserede brug af ophavsretligt beskyttet materiale
- Tech-giganternes markedsdominans inden for udviklingen af kunstig intelligens

Læs mere om ekspertgruppens anbefalinger her

Nyt undervisningsmateriale om kunstig intelligens fra TjekDet

Det danske faktatjekmedie TjekDet efterkommer nu den store efterspørgsel på undervisningsmateriale om kunstig intelligens. Materialet er gratis og er udviklet sammen med TjekDets norske søsterorganisation, ´Faktisk’. Det er målrettet 8-10 klasse og ungdomsuddannelserne.

Rådets sekretariatschef Claus Hjorth, der også er medlem af TjekDets bestyrelse, finder initiativet kærkommen og helt nødvendigt: "Hvis vi skal høste frugterne af kunstig intelligens er det helt afgørende, at vi lærer hinanden at forholde os kritisk til teknologien. Det handler både om at kunne spotte de stadig mere avancerede former for desinformation og om at forstå maskineriet bag eksempelvis chatbots".

Læs mere om materialet her

Rådets fokusområder og arbejdsgrupper

Rådets medlemmer opfordres til at melde sig til Rådets arbejdsgrupper:

- NIS2/cybersikkerhed
- Persondatabeskyttelse
- Kunstig intelligens
- Digital overvågning
- Borgernes digitale sikkerhed
- Sikkerhed og demokrati

Kontakt venligst sekretariatschef Claus Hjorth, hvis du ønsker yderligere oplysninger eller at tilmelde dig en eller flere af grupperne. Claus.hjorth@digitalsikkerhed.dk – mobil 53342522

Vil du være med til at fremme et trygt og frit digitalt samfund?

Bliv medlem af Rådet for Digital Sikkerhed. Se her hvordan og følg Rådet på LinkedIn, hvor vi jævnligt opdaterer nyheder, informerer om Rådets arbejde og kommende projekter!

Venlig hilsen
Bestyrelsen

Rådet for Digital Sikkerhed