

Kære læser

Velkommen til maj måneds nyhedsbrev fra Rådet for Digital Sikkerhed.

Haveredskaberne er taget ud til den digitale dagsorden

Henning Mortensen, Rådets formand og Anne Dorte Bach, Rådets næstformand

Forårssolen har langt om længe vist sig fra sin gode side. Vi får luftet ud, der kommer farver på, optimismen rykker et par takker. På it-fronten har vinteren budt på tunge sager om brugen af chromebooks i skolerne, en utilfreds rigsrevision om sikkerheden i statens it-systemer samt en udskydelse af den danske implementering af NIS2-direktivet.

Men nu er det forår, og der er masser at tage fat på!

I april skrev Rådet for Digital Sikkerhed et åbent brev til digitaliseringsministeren, erhvervsministeren og justitsministeren om chromebooksagen. Her pegede vi på, at den offentlige sektor ikke bør operere i grumset farvand når den anvender 3. partstjenester, der indsamler identificerbare persondata. Det bør være fuldstændig klart, at vores data anvendes til formål, der relevant i forhold til den pågældende forvaltningsaktivitet. I modsat fald risikerer vi, at både det generelle tillidsniveau i samfundet og tilliden til offentlige it-systemer svækkes. De dataetiske præmisser, som er lagt til grund for persondataretten, lægger netop vægt på, at nøglen til tillid i samfundet er, at vi værner om og er tydelige omkring anvendelsen af borgernes private data. I brevet pegede Rådet også på mulige tekniske løsninger, som man kan arbejde videre med fremfor at forsøge sig med kvikke fix i den danske sektorlovgivning. Læs Rådets åbne brev til de pågældende ministre på Rådets hjemmeside.

Rigsrevisionen er stadig ikke helt tilfreds med sikkerheden i statens it-løsninger, men der arbejdes på sagen. I april fulgte revisionen op med en tilfredsstillende vurdering af 3 centrale styrelses efterlevelse af minimumskrav til it-sikkerhed, mens 2 styrelser lader vente på sig. Rigsrevisionen kunne også afslutte sagen om behovet for at præcisere minimumskravene for statslige myndigheders it-sikkerhed, idet Digitaliseringsministeriet har opdateret kravene med virkning fra 1. juli 2024. Rådet for Digital Sikkerhed glæder sig over, at statens it-myndigheder har handlet hurtigt, men understreger behovet for, at vi inden for den offentlige sektor løbende får opdateret og udskiftet it-systemer, der ikke lever op til de aktuelle udfordringer på sikkerhedsområdet. Læs Rigsrevisionens opfølgingsnotat [her](#).

Indsatsen i forhold til den danske implementering af NIS2 er lagt i hænderne på forsvarsministeren, der i marts kunne meddele Folketingets Forsvarsudvalg, at den

kommende danske lovgivning vil blive fremsat for Folketinget til oktober med henblik på ikrafttræden 1. januar 2025. Lovforslaget vil blive udsendt i høring til foråret 2024, så det er rigtig snart! Forsvarsministeren betoner da også, at virksomheder og myndigheder "... allerede fra den offentlige høring i foråret (vil) få et overblik over de krav, der forventeligt vil træde i kraft ved årsskiftet." Fra Rådets side ser vi frem til lovforslaget, og den kommende vejledningsindsats. Læs forsvarsministerens svar til Forsvarsudvalget [her](#).

På AI-området har EU-parlamentet nu endelig vedtaget AI Act (13. marts 2024). Forordningen ventes offentliggjort i maj-juni 2024 med ikrafttræden 20 dage efter. AI Act vil dog først være fuldt implementeret om 24-30 måneder afhængigt af hvilke risikokategorier, der er på tale. Efter Rådets opfattelse kan vi i Danmark og Europa kvittere EU-samarbejdet for en fremsynet lovgivning, der med sin risikobetonede tilgang har skabt et godt fundament for udviklingen af AI-løsninger, som fremmer innovation med ansvarlighed og respekt for menneskerettigheder i centrum. Læs mere om AI Act vedtagelsen [her](#).

AI Act indikerer en udviklingsbane, som først lige er begyndt. Fra Rådets side har vi taget initiativ til en medlemsundersøgelse om forventningerne på området med fokus på udviklingen i den private og offentlige sektor samt ikke mindst potentielle udfordringer i forhold til det generelle trusselsbillede, cybersikkerheden og databeskyttelsen. Svarfristen er 13. maj med henblik på drøftelse af resultaterne på Rådets generalforsamling til juni.

Så tak skæbne! Haveredskaberne er i den grad kommet ud til en digital dagsorden, der kalder på innovation og dialog om teknologiudvikling, der sikkert og menneskeretligt bidrager til at styrke dansk erhvervsliv og den offentlige sektor.

Medlemsmøde og generalforsamling i Rådet for Digital Sikkerhed torsdag den 20. juni 2024

Generalforsamlingen finder i år sted hos Alexandra Instituttet på IT Universitet i København. Sekretariatet har udsendt indkaldelse og kalenderinvitation til medlemmerne for tidsrummet 14-17. Medlemmerne opfordres til at tilmelde sig.

Forslag til generalforsamlingen skal fremsendes til formanden senest den 9. maj.

I tilknytning til generalforsamlingen holder vi medlemsmøde med fokus på kunstig intelligens. Her vil Thomas Foege fra Boston Consulting Group præsentere BCG's store undersøgelse om AI i Danmark fra marts 2024. Resultaterne fra Rådets igangværende AI-medlemsundersøgelse vil også blive præsenteret.

Læs mere om BCG's AI undersøgelse [her](#).

Rådets medlemsundersøgelse om udbredelse og anvendelse af AI i Danmark

Som nævnt har Rådets AI-faggruppe og bestyrelse forberedt en medlemsundersøgelse om forventningerne til AI-udviklingen i dansk kontekst med særligt blik på det generelle trusselsbillede, cybersikkerhed og databeskyttelse.

Undersøgelsen skal bidrage til at tegne perspektiver for de kommende 5-10 år, herunder Rådets fremtidige fokus og indsats på området.

Medlemmerne opfordres til at besvare spørgerammen. Sekretariatet har angivet en svartid på 20-25 minutter, men erfaringerne viser allerede nu, at de, som allerede har svaret, har brugt 8-9 minutter i gennemsnit.

Undersøgelsen er fuldstændig anonym. Modsat sekretariats angivelse i introduktionen får sekretariatet ingen data om, hvem der har svaret – så vi er nødsaget til at udsende de nødvendige påmindelser til hele medlemskredsen.

Svarfristen er fastsat til mandag den 13. maj - lige efter Kristi Himmelfartsferien.

Rådets gode råd om at spotte digital svindel

En TV2-artikel om at spotte digital svindel fra den 11. april 2024 præsenterer Rådets 5 gode råd om emnet. Artiklen tog afsæt i nye tal fra Finans Danmark, der viser at den digitale svindel er fordoblet fra 2022 til 2023. Rådene, som Rådets formand Henning Mortensen fik formidlet til TV2, gengives her:

5 gode råd til at spotte svindel

1. **Vær skeptisk:** Du skal altid være skeptisk, når nogen vil have dig til at klikke på et link, en vedhæftet fil eller vil have dig til at indtaste oplysninger. Det kan enten være på skrift eller ske telefonisk. Hvis noget er for godt til at være sandt, er det formodentlig svindel.
2. **Tjek kilde uden at klikke:** Er der tale om en mail, kan du holde musen hen over linket uden at klikke eller trykke 'besvar' og se, om mailadressen er den samme, som den udgiver sig for at være.
3. **Tjek sproget:** Med online oversættelser og kunstig intelligens er der i dag mange svindelhenvendelser, der er sprogligt fejlfrie. Sproget er derfor ikke så god en indikator, som det har været. Alligevel kan det være en god idé at holde øje med engelske ord, stavfejl eller atypiske formuleringer.
4. **Tjek site i stedet for at klikke:** Hvis du er i tvivl, kan du se, hvilket domæne linket henviser til, og taste det manuelt i browseren i stedet for at klikke. På den måde undgår du at blive ledt ind på et skadeligt site.
5. **Skift kommunikationskanal:** En af de bedste måder at verificere, om en henvendelse er korrekt, er ved at verificere henvendelsen via en alternativ kommunikationskanal. Modtager du en mail og er i tvivl, så slå den påståede afsender op på internettet og ring. Kan du ikke finde vedkommende, er afsenderen nok falsk.

Læs artiklen fra TV2 [her](#).

Rådets bemærkninger om misbrug af kendte personer i falske annoncer

Henning Mortensen er i en artikel om misbrug af kendte personer i falske annoncer citeret for, at det er svært at gå efter bagmændene, og at kunstig intelligens formentlig vil kunne øge svindelannoncernes effektivitet.

Artiklen blev bragt hos TV2 19. marts 2024 under overskriften 'TV 2-vært misbruges i falske annoncer, men de bliver ikke fjernet'. Læs mere [her](#).

20 Talks - I anledning af EDPS 20-års jubilæum

EDPS – European Data Protection Supervisor – har 20 års jubilæum i år. EDPS, som er etableret i henhold til EU-lovgivning, “... is the European Union’s independent data protection authority, tasked with ensuring that the institutions and bodies of the EU respect data protection law.” Læs mere om EDPS [her](#).

I anledning af jubilæet udgiver EDPS 20 interviews med toneangivende it- og privacy-specialister.

“20 Talks” is a series of insightful discussions with 20 experts and influential personalities across diverse domains, looking into the profound implications of privacy and data protection within their specific spheres. In these talks, we will delve into the privacy domain, seeking to foster a deeper understanding of interplays between technology, policy, and other areas. By discussing the challenges and opportunities that lie ahead, we want to highlight the pivotal role that data protection plays in our society. The series of talks is scheduled for release throughout 2024.

Læs EDPS 20 Talks [her](#)

EU’s Digital Service Act’s første sag

EU’s Digital Service Act – Forordning om digitale tjenester – trådte i kraft i august 2023. Visse dele er implementeret i dansk lovgivning fra december 2023. I henhold til den danske lovgivning har Konkurrence- og Forbrugerstyrelsen fået opgaven som DSA-tilsyn.

I henhold til Digital Service Act er tilsynet med digitale tjenester delt mellem EU-kommissionen og medlemslandene. EU-kommissionen har tilsynskompetencen i forhold til meget store onlineplatforme og søgemaskiner (med mindst 45 millioner brugere), mens de nationale myndigheder har koordinerende funktioner og fører tilsyn med de mindre tjenester (der har brugere i medlemslandene – tilsynet er ikke baseret på jurisdiktion).

I februar 2024 rejste EU kommissionen den første formelle sag af sin art med henvisning til bestemmelser i DSA. Der er således indledt formelle procedurer i forhold til TikTok om følgende mulige brud på EU-bestemmelserne:

- The compliance with the DSA obligations related to the assessment and mitigation of systemic risks, in terms of actual or foreseeable **negative effects** stemming from the design of TikTok's system, including algorithmic systems, **that may stimulate behavioural addictions and/ or create so-called ‘rabbit hole effects’**. Such assessment is required to counter potential risks for the exercise of the fundamental right to the **person's physical and mental well-being, the respect of the rights of the child as well as its impact on radicalisation processes**. Furthermore, the mitigation measures in place in this respect, notably **age verification tools** used by TikTok to prevent access by minors to inappropriate content, may not be reasonable, proportionate and effective;
- The compliance with DSA obligations to put in place appropriate and proportionate measures to **ensure a high level of privacy, safety and**

- security for minors**, particularly with regard to default privacy settings for minors as part of the design and functioning of their recommender systems;
- The compliance with DSA obligations to **provide a searchable and reliable repository for advertisements** presented on TikTok;
 - The measures taken by TikTok to increase the transparency of its platform. The investigation concerns suspected **shortcomings in giving researchers access to TikTok's publicly accessible data** as mandated by Article 40 of the DSA.

Læs mere om Digital Service Act hos Konkurrence- og Forbrugerstyrelsen [her](#).

Læs mere om EU kommissionens rejste sag i forhold til TikTok [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**