Rådet for Digital Sikkerhed

Kære læser

Velkommen til oktober måneds nyhedsbrev fra Rådet for Digital Sikkerhed. Vi har indsamlet en masse nyttig information til dig nedenfor. God læselyst.

Månedens leder – kom med i Rådets arbejdsgrupper

fra Rådets formand, Henning Mortensen

Cyberforsvar har været et nøgleord for oktober - og det fortsætter nok i en rum tid. Cybersikkerhedsmånedens mange velbesøgte aktiviteter vidner om, at der i danske offentlige og private virksomheder er stor opmærksomhed på at beskytte virksomheden, brugernes data og leverandørkæderne, men selvfølgelig også for at leve op til kommende lovkrav. Fra myndighedernes side arbejdes der på højtryk på implementeringen af NIS2-direktivet, hvor de danske lovgivningsrammer skal være klar i 2024. Endelig har hele feltet af sikkerhedsbureauer og standardiseringsmodeller fra for eksempel Dansk Standard og D-mærket skærpet deres fokus på cybersikkerheden. Alligevel fandt Rådet for Digital Sikkerhed det relevant at ringe med alarmklokken, hvor Rådets bestyrelse gav udtryk for sin bekymring, om vi når godt i mål med NIS2-implementeringen. Det kan du kan læse mere om i dette nyhedsbrev.

Oktober måned gav også mulighed for hæder og blomster. Årets CISO blev kåret i et stærkt kandidatfelt, der alle har arbejdet ihærdigt på at udbrede forståelsen for, at cybersikkerhed ikke kan parkeres i it-afdelingen, men kræver deltagelse af alle medarbejdere og ledelsens aktive involvering. Så stort tillykke til Jannie Noer Mortensen fra BEC, der blev årets CISO 2023.

Endelig er Rådet godt i gang med arbejdet i Rådets arbejdsgrupper. I den kommende tid har vi selvsagt fokus på NIS2-implementeringen, men også kunstig intelligens og borgernes digitale sikkerhed er blandt de fokusområder, vi har taget fat på. Alle medlemmer opfordres til at deltage i arbejdsgrupperne både for at udbygge netværket, men også for at styrke Rådets indsats i forhold til samfundets digitale dagsorden.

Venligst
Henning Mortensen
Formand, Rådet for Digital Sikkerhed

Rådets NIS2-bekymring

De mange danske ministerier, der er beskæftiget med det danske cyberforsvar, har en stor koordinationsopgave i forhold til det nye EU-direktiv om net- og informationssikkerhed – NIS2-direktivet, som bliver til dansk lov med virkning fra efteråret 2024. I forhold til implementeringen er Rådet for Digital Sikkerhed

bekymret på mindst tre fronter:

For det første savnes der klarhed over, hvordan direktivets bestemmelser omsættes til dansk lovgivning, og hvilke danske - private såvel som offentlige - virksomheder, som bliver omfattet.

For det andet er vi bekymret i forhold til, om det spredte ministeransvar giver tilstrækkelige muligheder for harmonisering af sikkerhedskravene på tværs af sektorer.

For det tredje rejser Rådet for Digital Sikkerhed flaget i forhold til koordination af NIS2-kravene på tværs af EU-landene.

Deadline for afklaring af problemstillingerne nærmer sig, hvis vi skal nå i mål til 2024. I Rådet for Digital Sikkerhed følger vi lovgivningsprocessen på dansk og europæisk plan. Vi har fokus på best practice, og på hvordan danske virksomheder kan omsætte allerede etablerede sikkerhedsforanstaltninger og -procedurer til de kommende NIS2-krav. Endelig er det helt afgørende, at vi på tværs af virksomheder og sektorer får udvekslet erfaringer og synspunkter.

Læs mere om Rådets NIS2-bekymring her...

Åbent brev til justitsministeren om EU-Kommissionens forslag til CSA-forordning

Regeringen har med justitsminister Peter Hummelgaard som ansvarlig minister besluttet at støtte et kontroversielt forslag til EU-forordning om forebyggelse og bekæmpelse af seksuelt misbrug mod børn, den såkaldte CSA-forordning.

Selvom en forstærket indsats på området har Rådets fulde tilslutning, har vi i samarbejde med en række andre organisationer og eksperter vurderet, at elementer i forslaget er særdeles foruroligende. I sin nuværende form vil forslaget således give samtlige digitale tjenester adgang til at overvåge enhver form for kommunikation på deres platforme, herunder e-mails, telefonopkald, billeder etc., og det vil i sidste ende risikere at skade almindelige borgeres retssikkerhed og deres ret til at kommunikere privat.

På den baggrund udtrykte en kreds af organisationer, herunder RfDS sine bekymringer til justitsministeren i et brev af 4. oktober.

Justitsministeren takkede for henvendelsen den 6. november og giver blandt andet udtryk for, at han vil tage bekymringerne med i det videre arbejde med CSA-forordningen, og at det spanske formandskab i øjeblikket arbejder på at imødekomme de rejste bekymringer.

Læs ministerbrevet om EU-Kommissionens forslag til CSA-forordning her...

Åbent brev til justitsministeren om AI-forordningen og den danske implementering

Rådets bestyrelse har den 29. oktober sendt et brev til justitsministeren

vedrørende AI-forordningen og den danske implementering med forslag om, at Datatilsynet udpeges som national myndighed på området:

"AI-forordningen får stor betydning i forhold til regulering af brugen af kunstig intelligens hos danske aktører. AI er et vigtigt værktøj til at løse en række samfundsmæssige udfordringer, og det er derfor vigtigt, at udviklingen og anvendelsen fremmes bedst muligt indenfor de rammer, der i AI-forordningen og indenfor rammerne af persondataretten.

Rådet for Digital Sikkerhed, RfDS, anbefaler i forbindelse med den danske implementering, at Datatilsynet udpeges som national myndighed for at sikre et solidt samspil mellem de i forvejen på en række punkter sammenlignelige regler i AI-forordningen og Databeskyttelsesforordningen."

Rådet har uddybet ovenstående synspunkter i ministerbrevet.

Læs ministerbrevet om AI-forordningen og den danske implementering her...

Digitaliseringsstyrelsens analyse om digital sikkerhed og SMV'er

En ny analyse fra Digitaliseringsstyrelsen (oktober 2023) om digital sikkerhed og SMV'er afslører en tydelig tendens: Jo mindre virksomheden er, jo lavere er den digitale sikkerhed.

Blandt mindre virksomheder med 5-9 ansatte er det knap hver tredje, som ikke anvender de to basale IT-sikkerhedsforanstaltninger: Softwareopdatering og backup af data. 35% af alle SMV'er har generelt et for lavt sikkerhedsniveau i forhold til deres risikoprofil.

Analysen afslører samtidig en række positive tendenser. SMV'erne udviser en forbedret digital sikkerhed sammenlignet med sidste år. Hele 84 procent af de danske SMV'er har implementeret de to mest essentielle sikkerhedsforanstaltninger: backup af data og systematiske softwareopdateringer. Til sammenligning var tallet kun 75 procent sidste år.

Læs Digitaliseringsstyrelsens analyse her...

TjekpåNettet analyse om online svindel

PunktumDK har sammen med Global Anti Scam Alliance udgivet en rapport vedrørende status på online svindel i Danmark (oktober 2023). Rapporten er udarbejdet som en del af en global undersøgelse. Den danske undersøgelse er baseret på besvarelser foretaget af 2.000 respondenter, og den globale undersøgelse er baseret på mere end 40.000.

Hovedparten af dem, der udsættes for onlinesvindel, oplever det i forbindelse med shopping. Det kan være gennem sociale medieplatforme, e-mails, hjemmesider etc. Svindlere i dag er meget avancerede, hvilket gør dem svære at gennemskue. Blandt de adspurgte i undersøgelsen har mere 400 personer mistet penge ved onlinesvindel.

Læs mere om den danske og den globale undersøgelse her...

Lancering af IoT-pakke (CFCS, DE og RFDS) 30. november kl. 10-11

Udviklingen inden for digital teknologi har i de senere år resulteret i en markant vækst i antallet af nye typer internetforbundne enheder (IoT-enheder). Både på arbejdspladsen og i samfundet er efterhånden alt fra en højtaler til overvågningskameraer tilkoblet internettet, hvilket giver os mulighed for at foretage ændringer til det tilkoblede apparat fra f.eks. telefonen. De mange IoT-enheder byder på en række fordele, men samtidig opstår der også en væsentlig sikkerhedsmæssig risiko, der skal håndteres af virksomheder og myndigheder.

Rådet for Digital Sikkerhed og Dansk Erhverv har bidraget til Center for Cybersikkerheds nye vejledninger mv. om sikker brug af IoT-enheder.

Læs mere om de nye udgivelser her.

CFCS, Dansk Erhverv og Rådet for Digital sikkerhed præsenterer udgivelserne på et fælles webinar om sikkerhed i IoT-enheder torsdag den 30. november kl. 10-11.

Tilmeld dig webinaret her.

Tilmeld dig webinaret her...

NIS2 for topledere og bestyrelser

NIS2-cybersikkerheds øvelse for topledelse og bestyrelser Den 19. januar 2024 samles topledere fra de 18 samfundskritiske sektorer, der omfattes af de nye EU-regler om cyber- og informationssikkerhed (NIS2). Det sker i Rigsfællesskabets første fælles cybersikkerhedsøvelse om NIS2-direktivet, der bliver til dansk lov i efteråret 2024.

På dagen sættes der fokus på, hvor tæt vi er i mål, ledelses- og organisationsværktøjer samt udveksling af best practice. Eventet finder sted hos Dansk Industri på Rådhuspladsen.

Tilmeldingsfristen er den 30. november 2023. Tilmelding og yderligere information her.

Dagen tilrettelægges i et samarbejde mellem Industriens Fond, IDA, DI - Digital, Dansk Erhverv og Rådet for Digital Sikkerhed.

Tilmelding og yderligere information her...

Et godt nummer at have ved hånden – Cyberhotline for digital sikkerhed

De digitale trusler er mange og vedvarende, og derfor sætter Digitaliseringsstyrelsen og Center for Cybersikkerhed fokus på at udbrede kendskabet til Cyberhotline for digital sikkerhed, så flere borgere og virksomheder kan benytte sig af tilbuddet om telefonisk vejledning.

Du kan som borger og virksomhed få hjælp hos Cyberhotlinen, hvis du har brug for vejledning til at forebygge eller håndtere digitale trusler. Cyberhotlinen kan f.eks. hjælpe ved mistanke om misbrug af borgeres personlige oplysninger og i tilfælde af cyberangreb hos virksomheder.

- Borgere og virksomheder kan kontakte Cyberhotline for digital sikkerhed på 33 37 00 37 kl. 8-20 i hverdagene og kl. 10-16 i weekender. Ved akutte henvendelser, som f.eks. identitetstyveri eller igangværende angreb på virksomheder, kan der ringes døgnet rundt.
- Borgere og virksomheder kan blandt andet få hjælp til, hvordan de spotter falske webshops og laver stærke passwords samt hvordan de ruster sig mod digitale trusler som f.eks. phishing, CEO-fraud og faktura-bedrageri.
- Borgere og virksomheder kan få hjælp til, hvad de skal gøre, hvis de er udsat for et angreb fra it-kriminelle, og hvem det er relevant at kontakte for videre vejledning.

Se mere på Cyberhotline her.

Cyberhotline for digital sikkerhed...

Rådets fokusområder og arbejdsgrupper

Rådets medlemmer opfordres til at melde sig til Rådets arbejdsgrupper:

- NIS2
- Persondatabeskyttelse
- Kunstig Intelligens
- Digital overvågning
- Borgernes digitale sikkerhed
- Sikkerhed og demokrati

Kontakt venligst sekretariatschef Claus Hjorth, hvis du ønsker yderligere oplysninger om planlagte møder. claus.hjorth@digitalsikkerhed.dk - mobil 2490 2522

Kontakt venligst sekretariatsmedarbejder Namwan Gram, hvis du ønsker at deltage i arbejdet. namwan.gram@digitalsikkerhed.dk.

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

Rådet for Digital Sikkerhed - Vester Farimagsgade 37B, 1. Th - 1606 København V
- digitalsikkerhed.dk
Du modtager denne mail, da du har tilmeldt dig vores nyhedsbrev. Afmeld.