DeiC
DANISH eINFRASTRUCTURE CONSORTIUM

Galina Ianchina, Chef for DKCERT, DeiC Konference 2025

Forsvar af den akademiske sektors digitale frontlinje - visioner og planer

DeiC
DANISH eINFRASTRUCTURE CONSORTIUM

INTRODUKTION OG FORMÅL

TRUSSELSBILLEDET – HVORFOR UNIVERSITETER ER MÅL

TRUSLER OG PRIORITERING AF DEM

DKCERTS ROLLE OG SERVICES – OVERSIGT OVER YDELSER

VISIONER OG 2026-AKTIVITETER

OPSUMMERING

Q&A

Da virkeligheden ramte – ransomware-angreb på UWS, Juli 2023

Angriber:

- Rhysida ransoware-gruppe (formodet russisk oprindelse)

Metode:

- Systemnedlukning
- Datatyveri og trussel om offentliggørelse
- Krav om løsesum på 20 Bitcoins (ca. 4,5 mio.kr.)

Konsekvenser:

- Over 1 million dokumenter lækket (ID-kort, helbredsdata, økonomiske oplysninger)
- Undervisning og drift forstyrret
- Økonomisk tab på £18,3 mio. og samlet underskud på £14,4 mio

Ingeniøren

Version2 Nyheder Blogs Debat Nyhedsbreve Tip os IT job Events Mere

Cyberangreb koster danske universiteter millioner: Alligevel mangler flere a[illegible]rende våben

It-sikkerhed · 15. april kl. 10:20

Nyheder Om os Kontakt

[illegible]uslen Forebyggelse Opgaver NIS2

[illegible]n mod danske

Play Podcast

FRONTPAGE

EXPLORE

CYBER SECURITY

DTU is expose[illegible] on a daily bas[illegible]

The threat of cyberattacks is gr[illegible] heightened IT security measur[illegible] August 2022, DTU plays it sa[illegible]

Ekstra Bladet

Køb Ekstra Bladet+

Jo mere vi slår op,
jo mere finder vi sammen

Danmarks Nationalleksikon

SAMFUND 31. aug. 2020

Gem artikel

Aalborg Universitet udsat for cyberangreb

Universitetet har udsendt en mail til studerende om cyberangreb[illegible]

DeiC

DANISH eINFRASTRUCTURE CONSORTIUM

At give indblik i trusselsbilledet, DKCERTs rolle og fremtidige visioner for cybersikkerhed i sektoren.

FORMÅL

DeiC
DANISH eINFRASTRUCTURE CONSORTIUM

Hvorfor er universiteter mål for cyberangreb?

1	2	3	4	5
ÅBENHED	VÆRDIFULD OG INNOVATIV FORSKNING	STOR MÆNDER AF DATA	POLITISK AKTIVISME	DECENTRALISERE IT-STRUKTURER

DeiC
DANISH eINFRASTRUCTURE CONSORTIUM

Styrelsen for Samfundssikkerhed

INGEN	Der er ingen tegn på en trussel. Der er ingen aktør, der både har kapacitet til og intention om angreb/skadelig aktivitet.
LAV	En eller flere aktører har kapacitet til og intention om angreb/skadelig aktivitet. Men enten er kapaciteten eller intentionen eller begge dele begrænset.
MIDDEL	En eller flere aktører har kapacitet til og intention om angreb/skadelig aktivitet. Men der er ikke indikationer på specifik planlægning af angreb/skadelig aktivitet.
HØJ	En eller flere aktører har kapacitet til og foretager specifik planlægning af angreb/skadelig aktivitet, eller har allerede gennemført eller forsøgt angreb/skadelig aktivitet.
MEGET HØJ	Der er enten oplysninger om, at en eller flere aktører iværksætter angreb/skadelig aktivitet, herunder oplysninger om tid og mål, eller en eller flere aktører iværksætter kontinuerligt angreb/skadelig aktivitet.

TRUSSELSVURDERING

Cybertruslen mod den danske universitetssektor

April • 2025

DeiC
DANISH eINFRASTRUCTURE CONSORTIUM

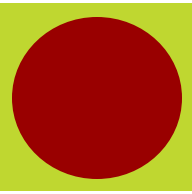
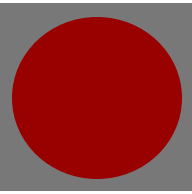
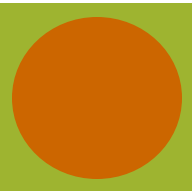
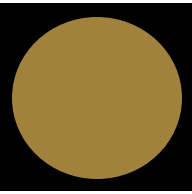
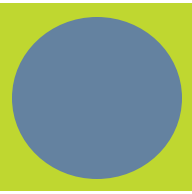
CYBERSPIONAGE

CYBERKRIMINALITET

CYBERAKTIVISME

DESTRUKTIVE CYBERANGREB

CYBERTERROR

Styrelsen for Samfundssikkerhed

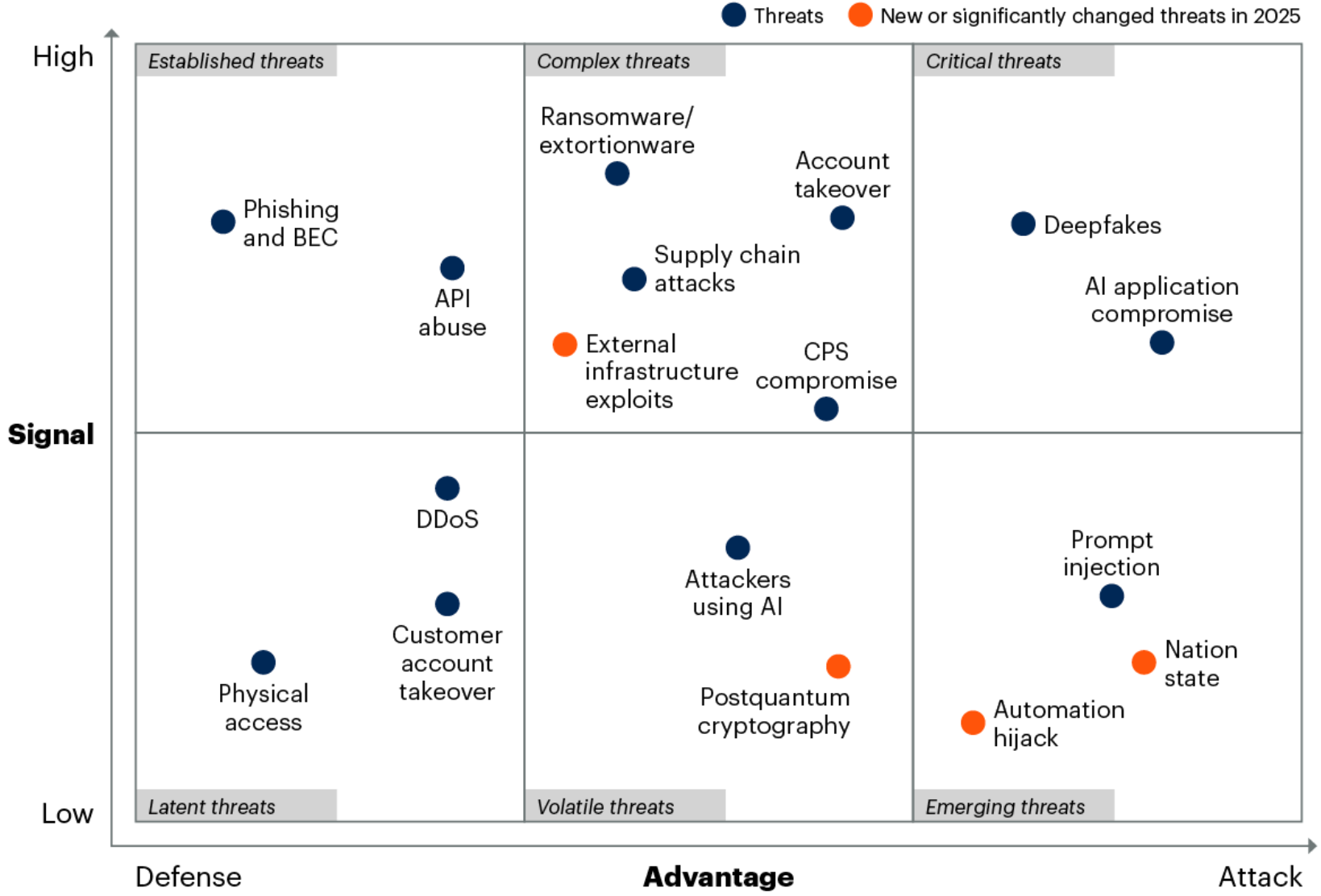
TRUSSELSVURDERING

Cybertruslen mod den danske universitetssektor

April • 2025

DeiC
DANISH eINFRASTRUCTURE CONSORTIUM

Gartner 2025 ThreatScape



Source: Gartner
827923_C

DeiC
DANISH eINFRASTRUCTURE CONSORTIUM

Trussel = Hensigt + Kapacitet + Mulighed

CVSS = *Kapacitet (hvad der kan ske, hvis den udnyttes)*

fortæller dig:

Hvor slemt kan det være?

+

EPSS = *Mulighed (hvor sandsynligt er udnyttelse)*

fortæller dig:

Hvor sandsynligt er det, at det bliver udnyttet?

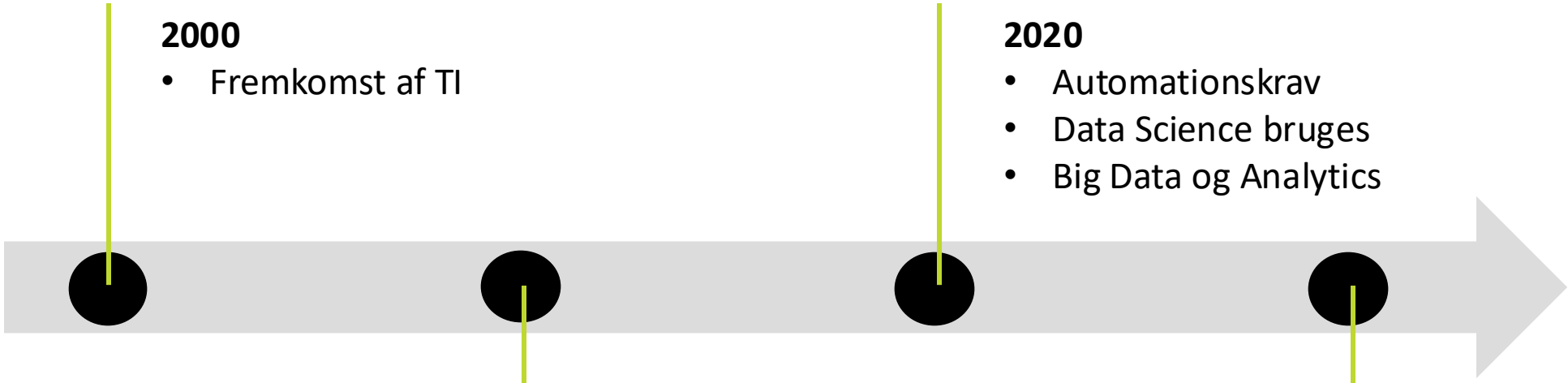
=

Ved at kombinere begge prioriterer du de sårbarheder, der repræsenterer **de mest realistiske og virkningsfulde trusler** mod din organisation.

VIGTIGE DEFINITIONER

CVE/EUVD:	• *Hvad er det? Entydigt id for en sårbarhed (f.eks. CVE-2024-12345).*
CVSS:	• *Hvad er det? Score for teknisk sværhedsgrad (0-10).*
EPSS:	• *Hvad er det? Score for sandsynlighed for udnyttelse (0-1).*

Udvikling af Threat Intelligence



2000
- Fremkomst af TI

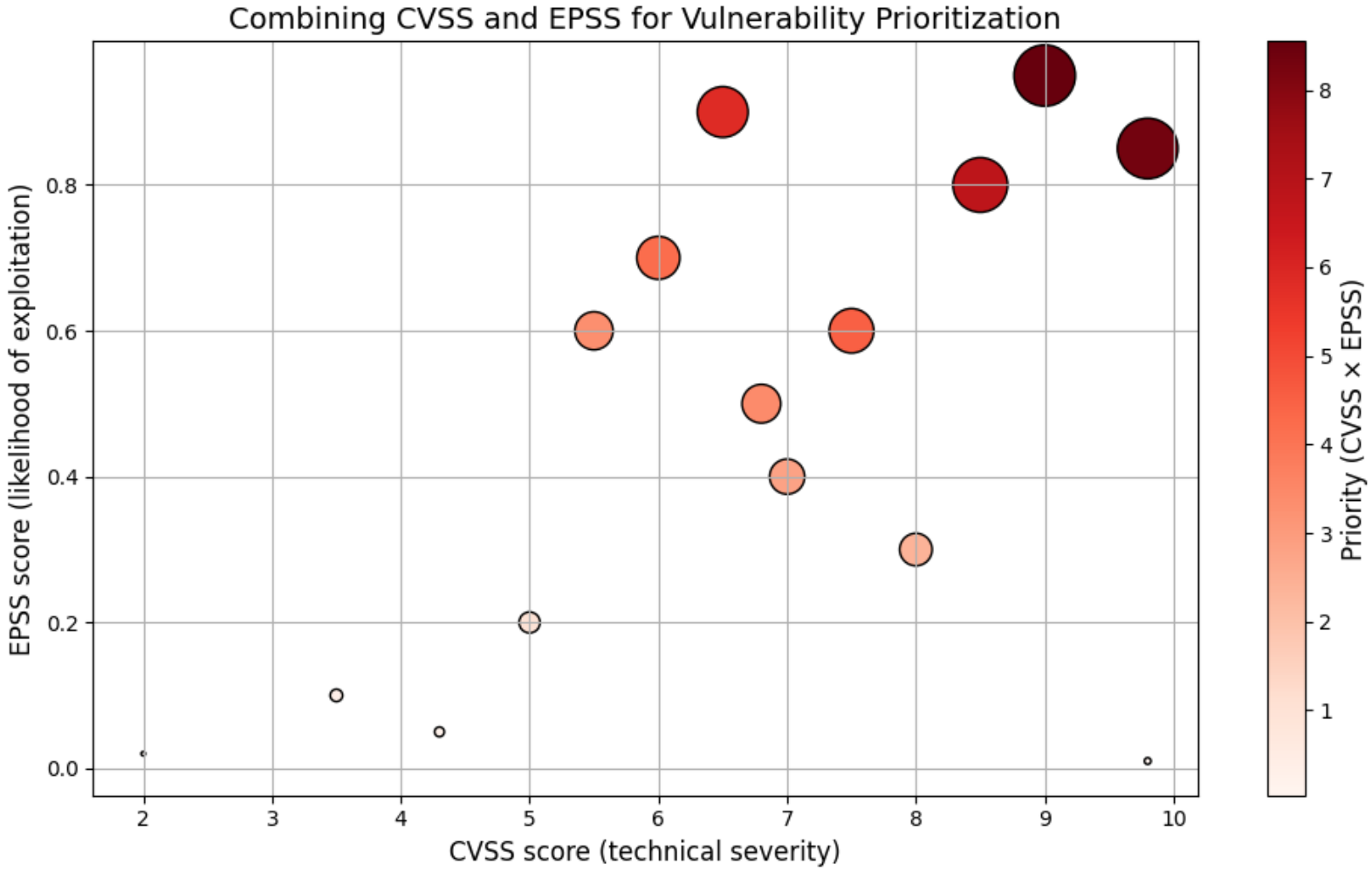
2010
- Udbredelsen af TI
- Justering af sikkerhedsbudgetter
- Dedikerede TI teams etableres

2020
- Automationskrav
- Data Science bruges
- Big Data og Analytics

Fremtid
- Multisignalindsamling og analyse
- Ibrugtagning hos flere virksomheder
- Flere AI-teknikker i brug
- Vægt på vejledning og håndteringsevner

DeiC
DANISH eINFRASTRUCTURE CONSORTIUM

Hvordan prioriterer I trusler i jeres organisation?



- X-akse: CVSS-score (teknisk sværhedsgrad)
- Y-akse: EPSS-score (sandsynlighed for udnyttelse)
- Farve og størrelse: Prioritet (CVSS × EPSS) - jo større og mørkere boblen er, jo højere prioritet.
- Øverste højre hjørne: Disse sårbarheder er både alvorlige og vil sandsynligvis blive udnyttet - ret disse først!
- Nederste venstre hjørne: Lavere alvorsgrad og mindre sandsynlighed for at blive udnyttet – lavere prioritet.
- Denne visualisering hjælper dig med hurtigt at identificere, hvilke sårbarheder der repræsenterer de mest realistiske og virkningsfulde trusler, så du kan fokusere din afhjælpningsindsats der, hvor de betyder mest.

Udfordringen ved at bruge TI effektivt

Problem 1: Ufuldstændige data

Mange organisationer træffer stadig kritiske beslutninger baseret på begrænsede eller enkeltkilde-trusselsdata, som mangler den dybde, der er nødvendig for komplekse risikovurderinger.

Problem 2: For meget støj

Sikkerhedsteams oversvømmes med:
Falske positiver
Redundante beskeder
Irrelevante signaler
Denne **overbelastning kan medføre, at reelle trusler overses**.

Problem 3: Svært at operationalisere TI

Det er svært at Identificere **virkelige trusler og mobilisere ressourcer i tide**

Problem 4: Mangel på kvalificeret arbejdskraft

Effektiv trusselsefterretning kræver:
Dygtige analytikere
Kontekstuel forståelse
Hurtig og præcis respons
Men mange teams mangler ekspertisen til at omsætte data til handling.

DeiC
DANISH eINFRASTRUCTURE CONSORTIUM

DKCERT

Danmarks nationale CERT (Computer Emergency Response Team) for forsknings- og uddannelsessektoren.

Vision

- **at skabe værdi** for uddannelses- og forskningssektoren i form af **øget informationssikkerhed**. Det sker gennem **offentliggørelse af viden** om informationssikkerhed skabt **gennem bredt samarbejde.**

Mission

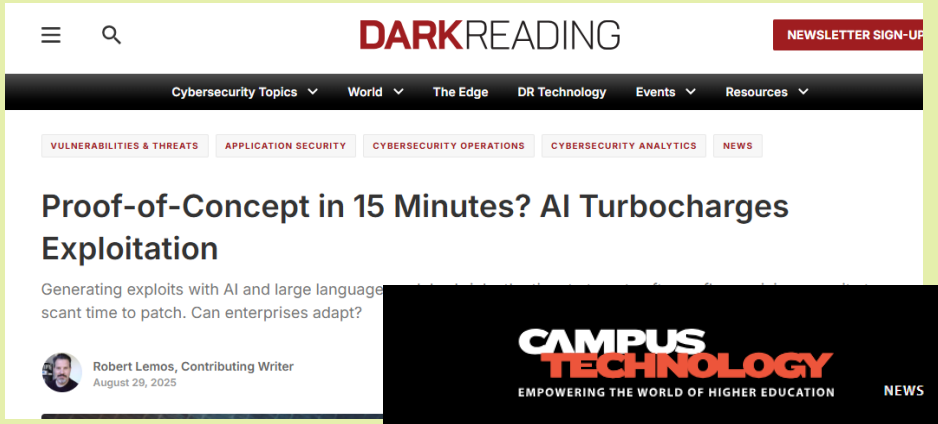
- at skabe **øget fokus** på informationssikkerhed i sektoren ved **at opbygge og skabe aktuel, relevant og brugbar viden.** Denne viden gør os i stand til at offentliggøre og udsende advarsler og anden information om potentielle risici og begyndende sikkerhedsproblemer.

DeiC
DANISH eINFRASTRUCTURE CONSORTIUM

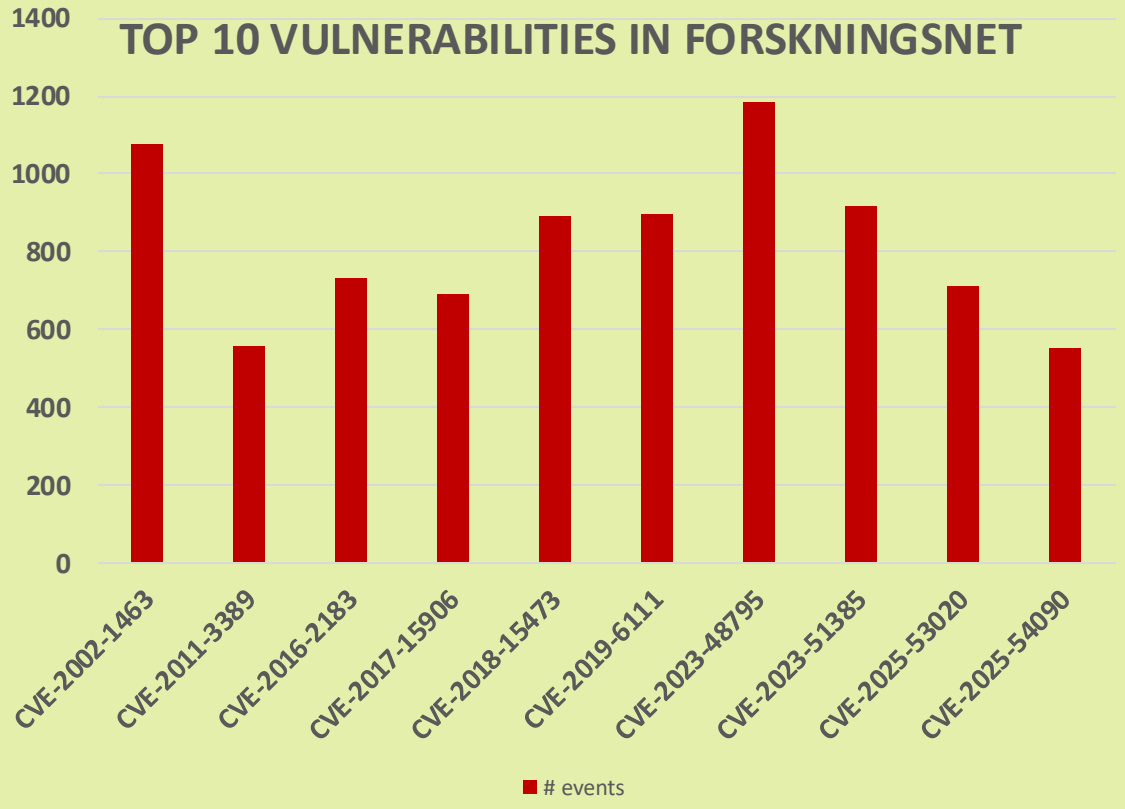
BASIS	TILKØB
Trusselsvurderinger	DPO
Sårbarhedsscanninger	Beredskabsøvelser
Varslinger og andre informationer	Phishingtræning
Incidenthåndtering	ISO / NIS2
International samarbejde	

DeiC
DANISH eINFRASTRUCTURE CONSORTIUM

Trusselsvurderinger



Sårbarhedsscanninger



DeiC
DANISH eINFRASTRUCTURE CONSORTIUM

Varslinger og andre informationer

DeiC
DANISH eINFRASTRUCTURE CONSORTIUM

Modtager og håndterer angreb rettet mod forskningsnettet.

Koordinerer respons ved uønsket trafik fra forskningsnettet.

Formidler information mellem berørte parter – også anonymt og fortroligt.

Rådgiver og analyserer trusler og angreb (fx via logfiler).

DeiC
DANISH eINFRASTRUCTURE CONSORTIUM

Samarbejde

Internationale samarbejdspartnere

- FIRST (Forum of Incident Response and Security Teams) - forening af organisationer, der håndterer sikkerhedshændelser. DeiC Sikkerhed / DKCERT er fuldt medlem af FIRST.
- TF-CSIRT (Task Force on Computer Security Incident Response Teams) - organisation under de europæiske forskningsnets fælles organisation, GÉANT
- Trusted Introducer - aktivitet under TF-CSIRT, der registrerer og certificerer Computer Security Incident Response Teams (CSIRT'er). DeiC Sikkerhed / DKCERT er certificeret medlem af TF-CSIRT Trusted Introducer.
- CERT Division - et center ved Software Engineering Institute under Carnegie Mellon University.
- DeiC Sikkerhed / DKCERT yderligere er autoriseret til at anvende betegnelsen CERT, som er er et varemærke for CERT'er ejet af Carnegie Mellon University.

Samarbejde

Nordiske forskningsnet-CERT'er

- Funet CERT (Finland)
- NORDUnet CERT (Norden)
- RHNet CERT (Island)
- SUNet CERT (Sverige)
- Sikt (Norge)

Danske samarbejdspartnere

- Center for Cybersikkerhed under Forsvarets Efterretningstjeneste - varetager sikkerheden for den statslige sektor, samt for virksomheder, der leverer kritisk infrastruktur
- Ministeriet for samfundssikkerhed og beredskab (tidligere Digitaliseringsstyrelsen) - beskæftiger sig blandt andet med myndighederne, virksomhederne og borgernes informationssikkerhed.
- ISP-sikkerhedsforum - forum for sikkerhed for internetudbydere
- Rådet for Digital Sikkerhed - en uafhængig medlemsorganisation med højt specialiseret viden og erfaring om informationssikkerhed og privatlivsbeskyttelse.
- Cybersikkerhedsrådet - DeiC Sikkerhed / DKCERT er medlem af regeringens cybersikkerhedsråd, der bl.a. rådgiver regeringen om digital sikkerhed, understøtter videndeling på tværs af myndigheder, erhvervsliv og forskningsverden og bidrager strategisk til arbejdet med den nationale cyber- og informationssikkerhedsstrategi.
- CISO-forum - forum for sikkerhedsansvarlige ved de danske universiteter

DPO

DeiC Sikkerhed / DKCERT tilbyder DPO-tjeneste til universiteter og uddannelsesinstitutioner, der ikke ønsker at ansætte en egen DPO, eller som ønsker rådgivning i forbindelse med GDPR-spørgsmål.

Brugen af DPO-tjenesten kan medvirke til at give institutioner

- viden om nyeste praksisser og fortolkning for uddannelses- og forskningsinstitutioner i EU. DeiC Sikkerhed / DKCERT deltager i et fælleseuropæisk netværk om forordningen i GÉANT-regi og er derfor fuldt opdateret om det nyeste indsigter på området.
- en ressourceeffektiv DPO-tjeneste, der er tilpasset den enkelte institutions behov, herunder omfang og karakteren af persondatabehandling.

Beredskabsøvelser

Vores specialister er højt kvalificerede og arbejder ud fra et gennemprøvet metodeapparat udviklet i samarbejde med internationale partnere, hvilket sikrer en professionel og struktureret gennemførsel af beredskabsøvelser.

Phishing træning

DKCERT tilbyder målrettet phishing-træning, der styrker organisationers modstandsdygtighed mod sociale angreb. Træningen omfatter realistiske simulerede phishing-kampagner, opfølgende analyser og rapportering, samt rådgivning om best practices for at reducere risikoen for kompromittering. Formålet er at øge medarbejdernes bevidsthed og forbedre den samlede sikkerhedskultur.

ISO / NIS2

DeiC Sikkerhed / DKCERT har etableret en tjeneste, som skal hjælpe institutionerne på forskningsnettet med at håndtere de stigende krav til Informationssikkerhed og databeskyttelse.

For mange forsknings- og uddannelsesinstitutioner er det i sig selv en stor udfordring at holde sig løbende orienteret om nye tiltag.
Derudover er der en risiko for, at den enkelte institution opbygger separate og måske endda konfliktende regelsæt til de mange hensyn, som reguleres separat. Det gælder f.eks. beskyttelse af virksomhedsdata aht. virksomheden selv (ISO27001), beskyttelse af persondata aht. de registrerede (GDPR) og beskyttelse af samfundsvigtige data aht. hele samfundet (NIS2).

Et vigtigt fundament for DeiC Sikkerhed / DKCERTs tjenester er at følge med i og påvirke de reguleringstiltag, som forsknings- og uddannelsesinstitutioner er underlagt på dette område.

Møder med universiteterne: Tekniske behov og samarbejdsmuligheder

01

Nessus-scanninger: Universiteterne arbejder aktivt med scanninger, men oplever udfordringer med falske positiver. Der er interesse for sparring og bedre filtrering.

02

Netflow-analyse: Flere ønsker at styrke deres indsigt i netværkstrafik og efterspørger værktøjer og metoder til analyse.

03

MISP-platformen: Der er bred interesse for et tættere samarbejde og behov for en fælles governance-model, der sikrer effektiv og koordineret brug af platformen.

04

Ønske om bedre forståelse af DKCERTs rapporter og hvordan de adskiller sig fra CFCS og DCIS. Behov for vejledning i anvendelse af rapporterne (hvornår er det alvor) og afklaring af modtagere og distributionslister.

Møder med universiteterne: Strategiske og operationelle perspektiver

01

Der er interesse for pilotprojekter og adgang til egne data, fx via ArcticHub.

02

Ønske om at DKCERT deler viden fra konferencer og workshops, og at universiteterne selv deltager aktivt.

03

Ønske om klarere rollefordeling og governance i samarbejdsfora som SIKREF og MISP. Der er behov for transparens og undgåelse af overlap i ressourcer og beslutningsprocesser.

04

Universiteterne har forskellige behov og modenhedsniveauer, hvilket kræver differentierede ydelser fra DKCERT.

05

Ønske om at bruge SIKREF som platform for projektvidendeling og teknisk sparring.

DeiC
DANISH eINFRASTRUCTURE CONSORTIUM

2026 AKTIVITETER

Pejlemærke 3: Etablere et bredere perspektiv på sikkerheden i den digitale infrastruktur

DeiC
DANISH eINFRASTRUCTURE CONSORTIUM

1

Modernisering af DKCERT's digitale tilstedeværelse gennem en ny webplatform, der effektivt formidler tilgængelige tjenester og styrker kundernes værdioplevelse. ArcticHub videreudvikles som en integreret platform for trusselsinformation.

2

Styrket koordinering med DCIS, universiteterne og CFCS.

3

Bidrag til en koordineret indsats på tværs af DeiC's forretningsområder med henblik på harmonisering af sikkerhedsstandarder og fremme af en højere grad af cybermodenhed.

4

Etablering af en proaktiv kundedialog, der sikrer forståelse for interessenters teknologiske landskab og behov, som grundlag for skræddersyede tjenester og effektmåling – herunder rådgivning og risikovurdering i relation til nye teknologier som AI.

TO DO

- Afklaring af distributionslister og kontaktpersoner.
- Oplæring af nye medarbejdere i rapportbrug.
- Re-vitalisering af SIKREF-møder.
- Evaluering af pilotprojekter og tekniske samarbejder.
- Udvikling af governance-model for MISP.
- Arctic Hub
- Vulnerability Look Up

DeiC

DANISH eINFRASTRUCTURE CONSORTIUM

FREMTIDEN FOR THREAT INTELLIGENCE ER UNIFIED CYBER RISK INTELLIGENCE

DKCERT's mål:
At gøre det muligt for universiteter at træffe informerede, rettidige og strategiske beslutninger baseret på samlet Threat Intellegence – ikke kun trusselsdata.

Udvid datakilder

Brug flere interne og eksterne datakilder til at forbedre beslutningsgrundlaget.

Automatiser og orkestrer

Forbind værktøjer til automatisering af indsamling og analyse af trusselsdata på tværs af virksomheden.

Opkvalificering og styrkelse af teams

Træn teams i at bruge avancerede teknologier som AI og forudsigende modeller effektivt.


DeiC
DANISH eINFRASTRUCTURE CONSORTIUM