DKCERTs opgaver, mål og vision

DeiC-konferencen

4. november 2021

DKCERT
www.cert.dk
Henrik Larsen
Email: henrik.larsen@cert.dk

> Hvem er DKCERT?

- > DKCERT er en tjeneste fra DeiC (Danish e-Infrastructure Cooperation), der følger sikkerheden på internettet og advarer om potentielle it-sikkerhedsproblemer
- > DKCERT tager imod henvendelser om sikkerhedshændelser på internettet fra Forskningsnettet og andre danske og udenlandske kilder
- > DKCERT indgår i FIRST, et verdensomspændende netværk bestående af p.t. 602 CERT/CSIRT teams i 99 lande, samt i den europæiske organisation Trusted Introducer med mere end 440 teams
- > DKCERT har et bredt samarbejde med danske og nordiske organisationer og myndigheder

> Historie

- > Grundlagt 1991 efter en af de første store hackersager i Danmark
- > Dengang en del af UNI·C
- > Inspirationen kom fra det amerikanske CERT Coordination Center (CERT/CC)
- > Siden 2012 en del af Danish e-Infrastructure Cooperation (DeiC)

> Mission og vision

> Mission:

At ***opbygge og skabe aktuel, relevant og brugbar viden*** – og derigennem skabe øget fokus på informationssikkerhed i uddannelses- og forskningssektoren.

> Vision:

At skabe værdi for uddannelses- og forskningssektoren i form af ***øget informationssikkerhed*** gennem offentliggørelse af viden om informationssikkerhed.

> Hvad er en CERT/CSIRT? - I

Authorized to Use CERT™
CERT is a mark owned by
Carnegie Mellon University

- CERT: Computer Emergency Response Team
  - Carnegie Mellon University grundlagde CERT/CC i 1988 efter episoden med “The Internet Worm”.
    Det er et registreret varemærke
  - DKCERT, grundlagt 1. juli 1991, er det ældste af de nu ni danske teams, der er autoriserede til at bruge CERT™

> Hvad er en CERT/CSIRT? - II

- CSIRT: Computer Security Incident Response Team
  - Den generiske og bredt anvendte forkortelse

- Internet Governance Forums definition:
  - A CSIRT is a “team of experts that
    - **responds** to computer incidents,
    - **coordinates** their resolution,
    - **notifies** its constituents,
    - **exchanges** information with others and
    - **assists** constituents with the mitigation of the incident”

> CERT/CSIRTs startede i forskningsnettene

- De ældste og mest erfarne CSIRTs i Europa er grundlagt indenfor de europæiske NRENs (National Research and Education Networks)
- I dag hører knap en femtedel af alle europæiske teams til forskningsområdet – antallet er stabilt, men andelen er faldende
- De har hjulpet nye teams med at få national og international anerkendelse og at blive medlemmer af internationale fora som FIRST, TF-CSIRT og Trusted Introducer

> Internationale organisationer

> DK·CERT blev 1993 som et af de første teams udenfor USA fuldt medlem af FIRST – Forum of Incident Responce and Security Teams – grundlagt i 1990 efter den såkaldte ”Wank Worm”.
I dag er fem danske teams medlem af FIRST, der nu har 602 medlemmer i 99 lande

> DK·CERT var blandt grundlæggerne af det europæiske samarbejde, Trusted Introducer i 2000 og blev akkrediteret medlem 5. februar 2002.
Der er p.t. to certificerede, fire akkrediterede og et listet medlem blandt danske teams – det seneste er kommet til for bare lidt over to måneder siden

> DKCERTs tjenester

- Genemgået af CIO Gruppen og CISO-forum
  - Justeret tjenestekatalog godkendt

- Nordisk samarbejdsprojekt i regi af NORDUnet
  - Tre spor i første fase:
    - Deling af trusselsinformation
    - Samarbejde om sårbarhedsscanninger og sårbarhedsviden
    - Beskyttelse mod overbelastningsangreb (DDoS)

> DKCERTs tjenester I

- Sårbarhedsscanninger og -analyse
  - On-demand eksterne scanning og interne scanninger
  - Rapport til institutionen med vurdering af kritikalitet
  - Løbende rapportering af sårbarheder, fundet af tredjeparter

- Dataanalyse
  - Netflowdata fra forskningsnettet, analyse af trafikdata ifm. forensics
  - (Passiv DNS, SIE Europe)

> DKCERTs tjenester II

- Sikkerhedshændelser
  - Modtager og behandler rapporter om sikkerhedshændelser på eller relateret til Forskningsnettet (abuse-kontakt)
  - Deling af IOC'er og threat intelligence (MISP)

- Videndeling og varsling
  - Lukkede mail-lister, sikker chatserver
  - MISP – for universiteterne og mellem de nordiske forskningsnet-CERT'er
  - SikRef – netværk for sikkerhedsteknikere

> DKCERTs tjenester III

- Informationstjenesten
  - Webnyheder, nyhedsbreve, advarsler, tweets
  - Trendrapport mv.
  - Trusselvurdering for uddannelses- og forskningssektorern

  https://cert.dk, *https://www.cert.dk/da/information/trendrapporter*

- Træning og bevidsthed (on demand-tjenester)
  - Phishing-tjeneste
  - Krisestyringsøvelser

> DKCERTs tjenester IV

- Databeskyttelsesrådgivertjeneste
  - Rådgivning til universiteter og andre forsknings- og uddannelses-institutioner om databeskyttelse
    - Hjælp til overholdelse af EUs persondataforordning (GDPR)
  - Databeskyttelsesrådgiver (DPO) as-a-service til en række institutioner
  - Netværk for DPO'er ved universiteter, kunstneriske uddannnelser og professionshøjskoler

> DKCERTs tjenester fremadrettet

- > Opbygning af kapacitet til koordinering af kriseberedskab
- > Udvidet nordisk videndeling om trusler, sårbarheder og DDoS-beskyttelse
- > Fælles uddannelsesinitiativer
- > ISO 27001 implementering og audit
- > Rammeaftale for penetrationstest mv.

DKCERT

DeiC

> Spørgsmål?

henrik.larsen@cert.dk
www.cert.dk – cert@cert.dk