Aktuelt fra sikkerhedsfronten – trends og tendenser i cyber- og informationssikkerhed

DeIC konference

7. oktober 2015

DKCERT
www.cert.dk

Henrik Larsen
Email: henrik.larsen@cert.dk

DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

Agenda

- DKCERT
  - Hvem er vi og hvad gør vi?
- Hvad er status?
  - Tal og statistikker fra DKCERT
  - Aktuelle trends
- Tiltag til at forbedre informationssikkerheden

  - som vi har talt om længe
- Udfordringer for informationssikkerheden

  – hvordan kommer vi videre?

DKCERT:
opgaver og tjenester

DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

Hvem er DKCERT? - Opgaver

- DKCERT **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 over 300 CERT/CSIRT teams, samt i den europæiske organisation **Trusted Introducer**
- DKCERT har et **bredt samarbejde** med danske og nordiske organisationer og myndigheder

DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

Hvem er DKCERT? - Tjenester

- Informationstjenesten.
  - Webnyheder, nyhedsbreve, advarsler, tweets, awareness, trendrapport mv.

- Sagsbehandlingen.
  - Modtager og behandler rapporter om sikkerhedshændelser på eller relateret til Forskningsnettet.
  - Rådgiver og støtter efter behov

- Sårbarhedsscanninger
  - Otte parallelle Nessus Enterprise-scannere
  - Omfattende rapport til institutionen
  - Også on-demand scanning

Status:
Tal og statistikker

DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

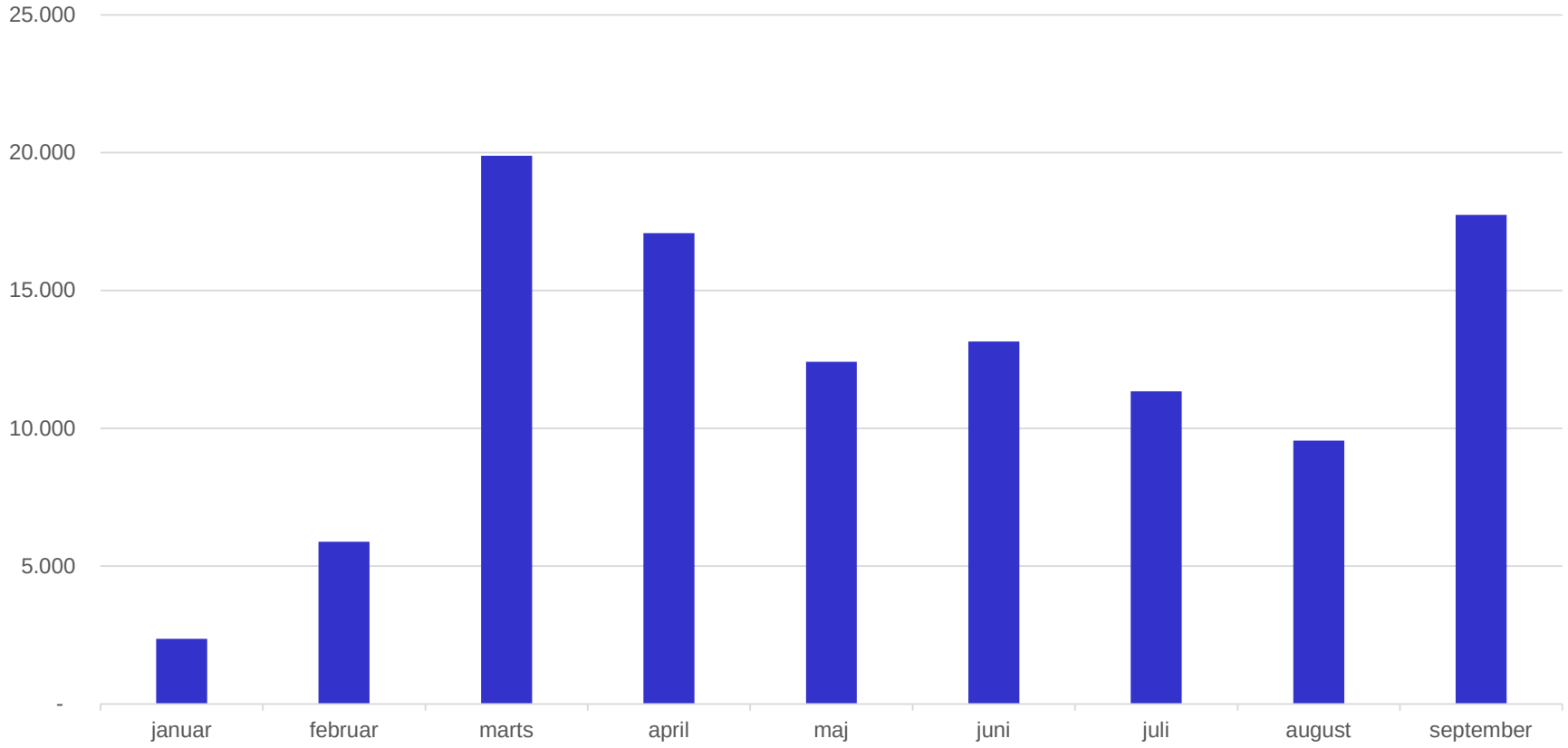
Tendenser fra Trendrapport 2015

https://www.cert.dk/trendrapport2015/DKCERT_Trendrapport_2015.web.pdf

- DKCERT håndterede i 2014 i alt **65.267** sikkerhedshændelser, hvoraf langt de fleste havde tilknytning til Forskningsnettet
- Det er en stigning på 250 procent i forhold til 2013 – det meste af stigningen lå i november/december
- 2015 til og med september: 109.416
- Væksten skyldes flere faktorer:
  - vi har modtaget flere henvendelser,
  - flere af vores samarbejdspartnere indrapporterer nu hændelser automatisk, og
  - vi har effektiviseret og automatiseret vores sagsbehandling yderligere

DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

Sikkerhedshændelser 2015



DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

Tendenser fra Trendrapport 2015

- Halvdelen af hændelserne i 2014 var portscanninger.
  Ny område, steg kraftigt i december: scanning efter åbne NTP-services, der kan bruges til reflection-angreb

- Denne tendens er fortsat i 2015, hvor vi har set flere og flere reflection- (eller amplification-) angreb.

- Mere om det senere!

DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

Tendenser fra Trendrapport 2015

- 12 procent af sikkerhedshændelserne i 2014 var brud på ophavsretten, primært piratkopiering af film

- Andre 12 procent handlede om computere, der uden deres ejers vidende blev fjernstyret og misbrugt af it-kriminelle i botnet – det er en firdobling i forhold til 2013!

- Spam og phishing udgjorde 3,7 %

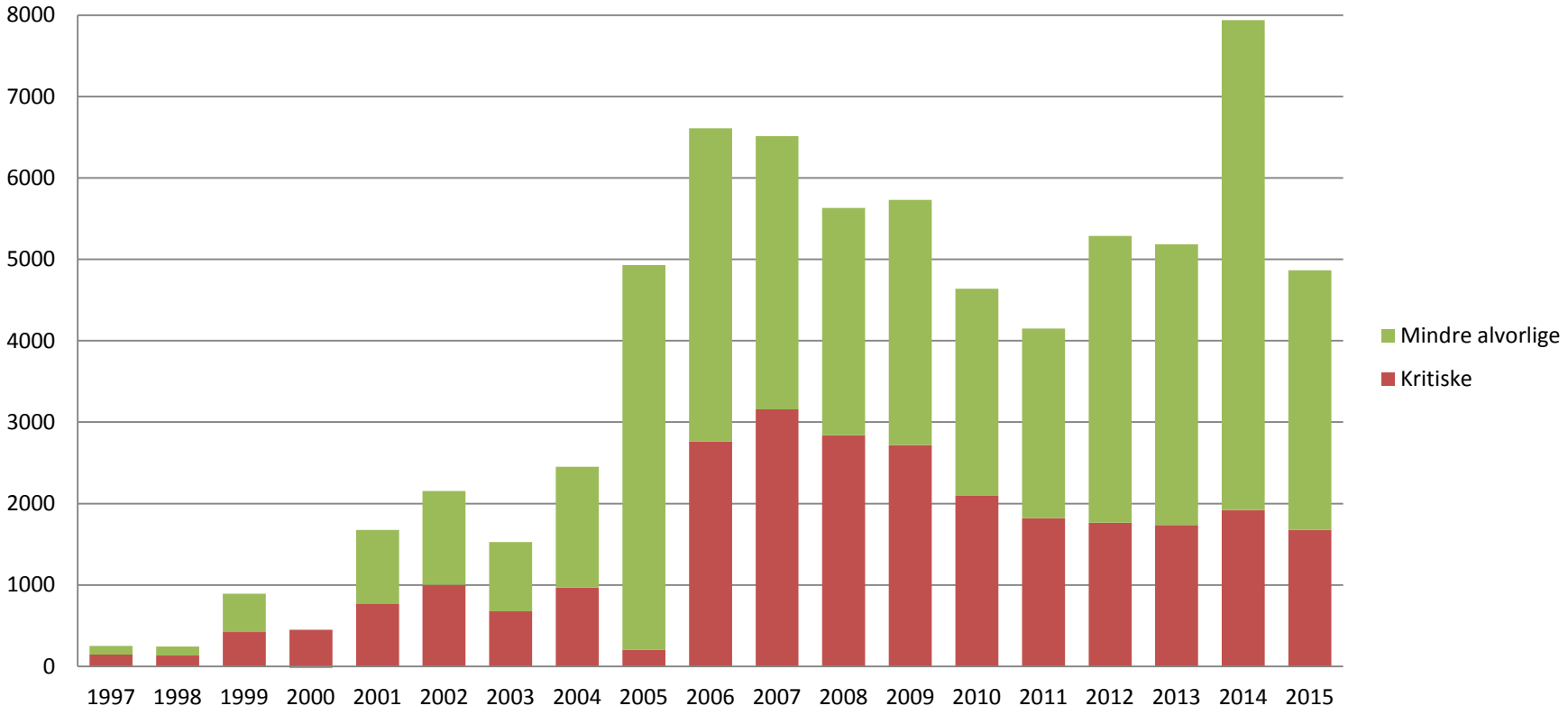
DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

Tendenser fra Trendrapport 2015

- På verdensplan voksede mængden af registrerede sikkerhedshuller i 2014 med 53 procent til 7.937 sårbarheder
- Kritiske sårbarheder udgjorde en fjerdedel
- I 2015 er der til og med september registreret 4.864 sårbarheder – heraf en tredjedel kritiske

DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

Sårbarheder i National Vulnerability Database



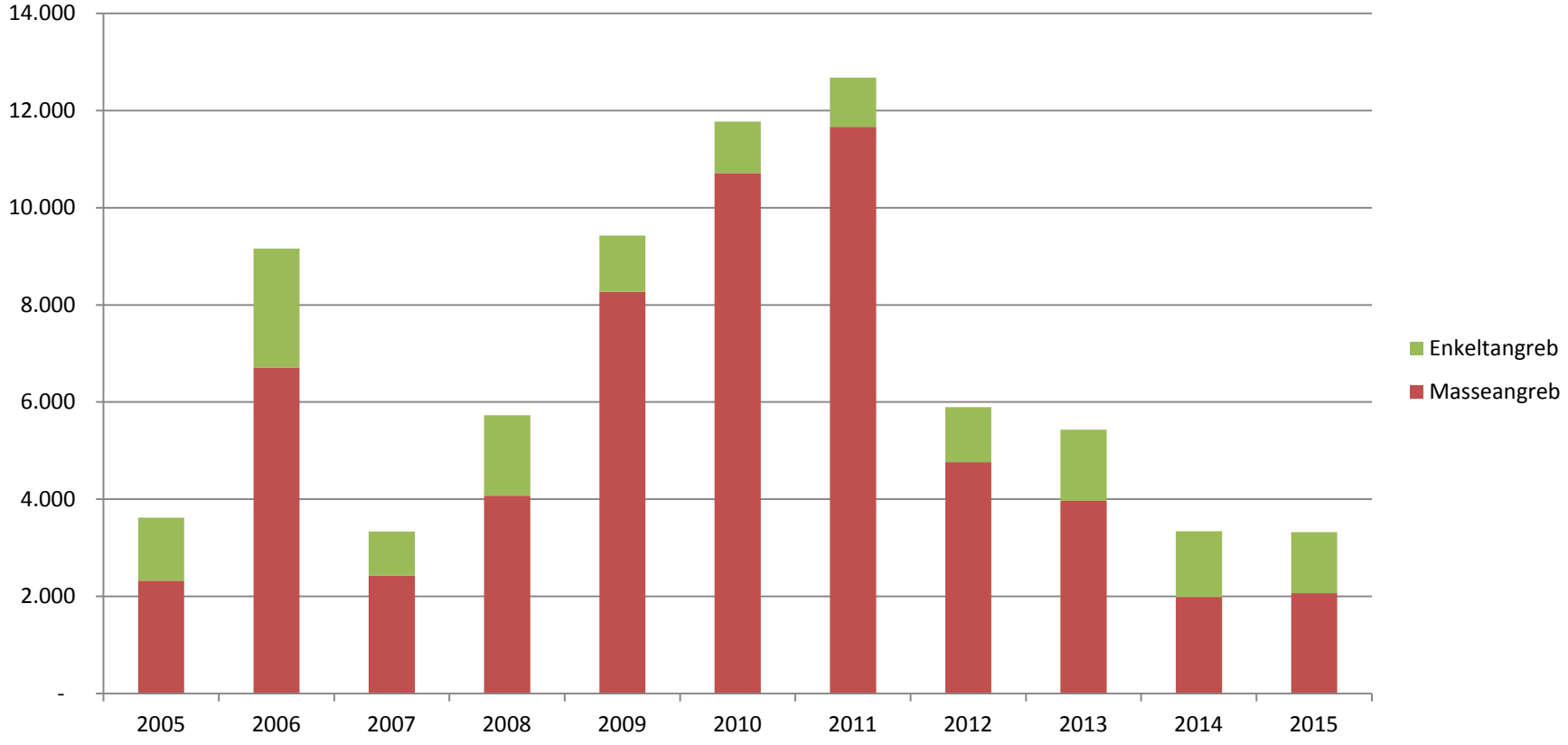
Status:
Aktuelle trends

Defacements

- Efter en faldende tendens i nogle år ser vi nu igen flere defacement-angreb
- Allerede efter ni måneder har vi nu set ligeså mange angreb som i hele 2014
- Bølge i foråret – værst så det ud i april

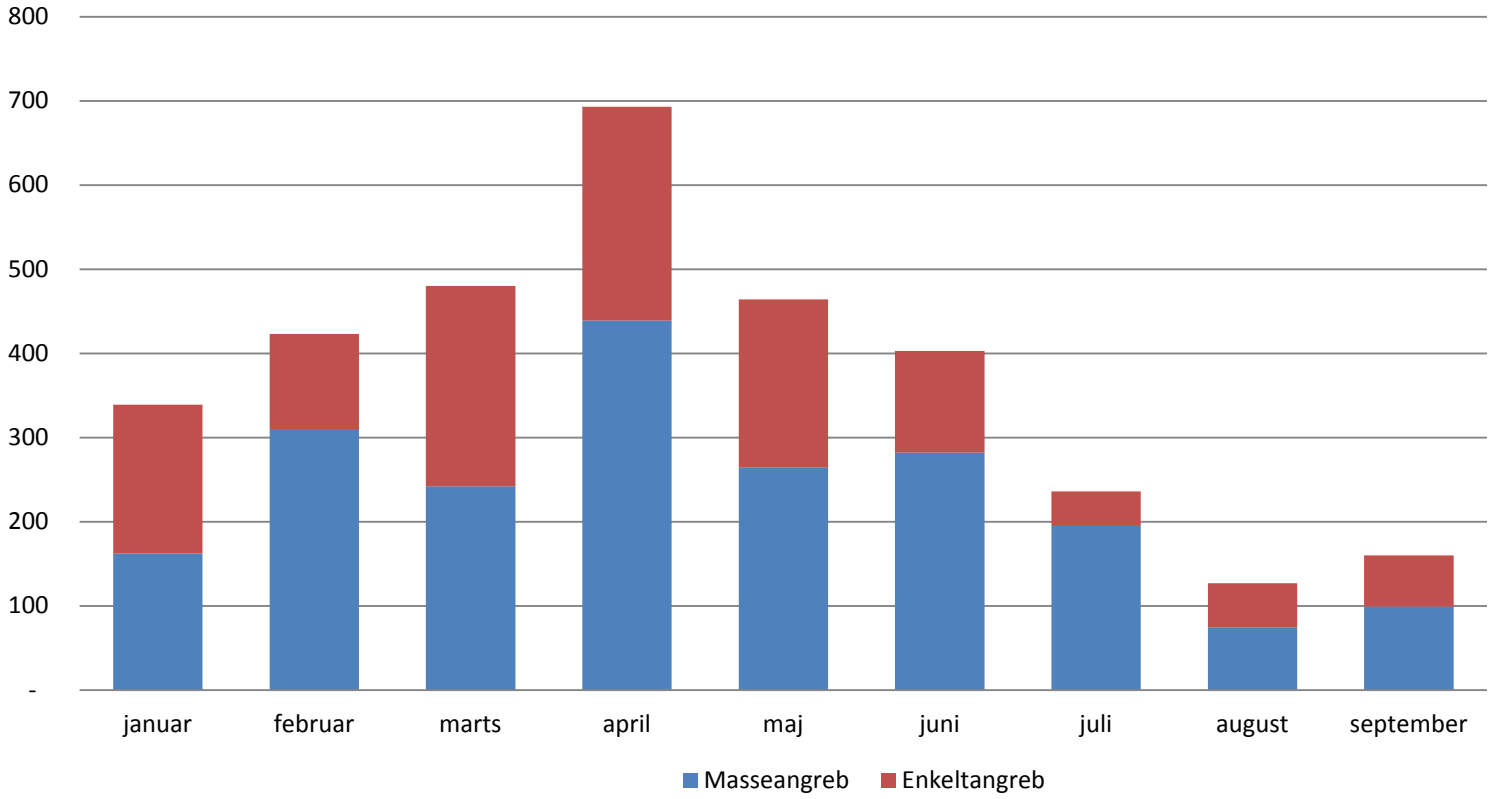
DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

Defacements dk-domæner 2005-15



DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

Defacements på dk-domæner 2015



DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

DDoS – Distributed Denial of Service

- DDoS er nemt, billigt og let tilgængeligt, hvis man vil genere virksomheder eller enkeltpersoner
- Kan bestilles på nettet for få dollars
- Kan være svært at beskytte sig imod – især for enkeltpersoner og mindre virksomheder

DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

Reflection- eller amplification-angreb

- Åbne UDP-services (NTP, DNS …) udnyttes til at forstærke angreb
- Pakkestrømmen reflekteres fra en intetanende parts åbne NTP eller tilsvarende (”reflection”) ved, at angriberen sender en forespørgsel med offerets IP-adresse angivet som afsender
- Herved forstærkes pakkestrømmen med en høj faktor (”amplification”)
- DNS-amplification 1:70
- NTP-amplification 1:20 – 1:200 eller mere ..!

Reflection- eller amplification-angreb

- Nemt at finde lister med tilgængelige NTP-services via Metasploit eller The Open NTP Project
- Stadig mange åbne NTP-services på universiteterne og andre steder på Forskningsnettet

DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

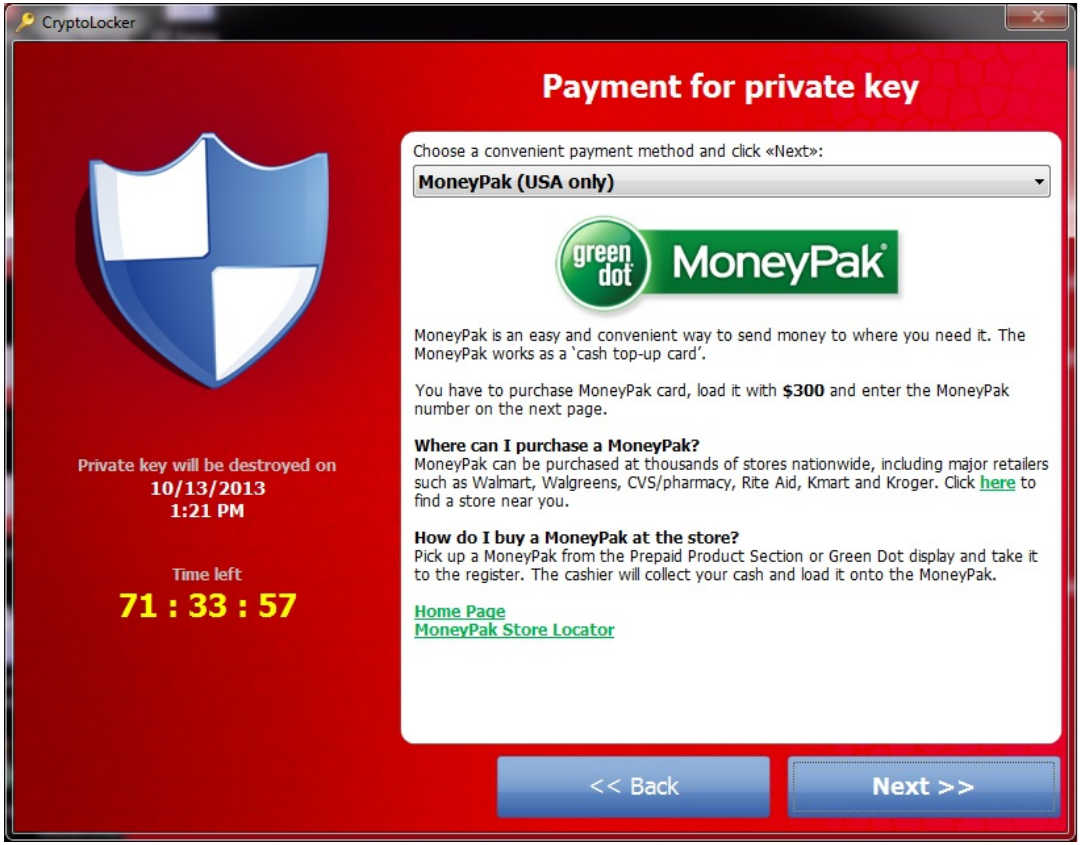
Danske forskningsnetinstitutioner angriber den indiske finanssektor!

- Denne overskrift kunne have været bragt i aviserne i forrige uge
- Henvendelse fra indiske CERT om omfattende DDoS-angreb mod indiske banker og andre finansvirksomheder i juni og juli
- Mange forkert konfigurerede NTP, DNS og SSDP-instanser i en lang række lande anvendt til reflection/amplification
- **73 IP-adresser på Forskningsnettet deltog i angrebene!**
- Der er pr. 3. oktober 186 åbne NTP-servere og 9 SSDP på Forskningsnettet

DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

Afpresning

- Ransomware tager til – flere eksempler fra universiteterne
- Hidtil pc'er, nu også disksystemer (Synolocker)
- DDoS-angreb som afpresning – betal, eller vi lukker dit websted!



DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

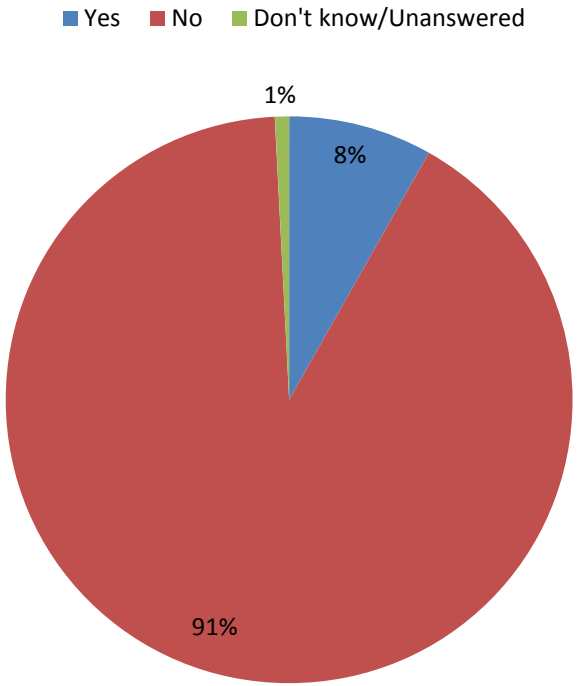
Afpresning

DKCERT anbefaler:

- *Hav backup af alt*
- *Brugeren skal ikke have administratorrettigheder (begræns skaden)*
- *Awareness om phishing*

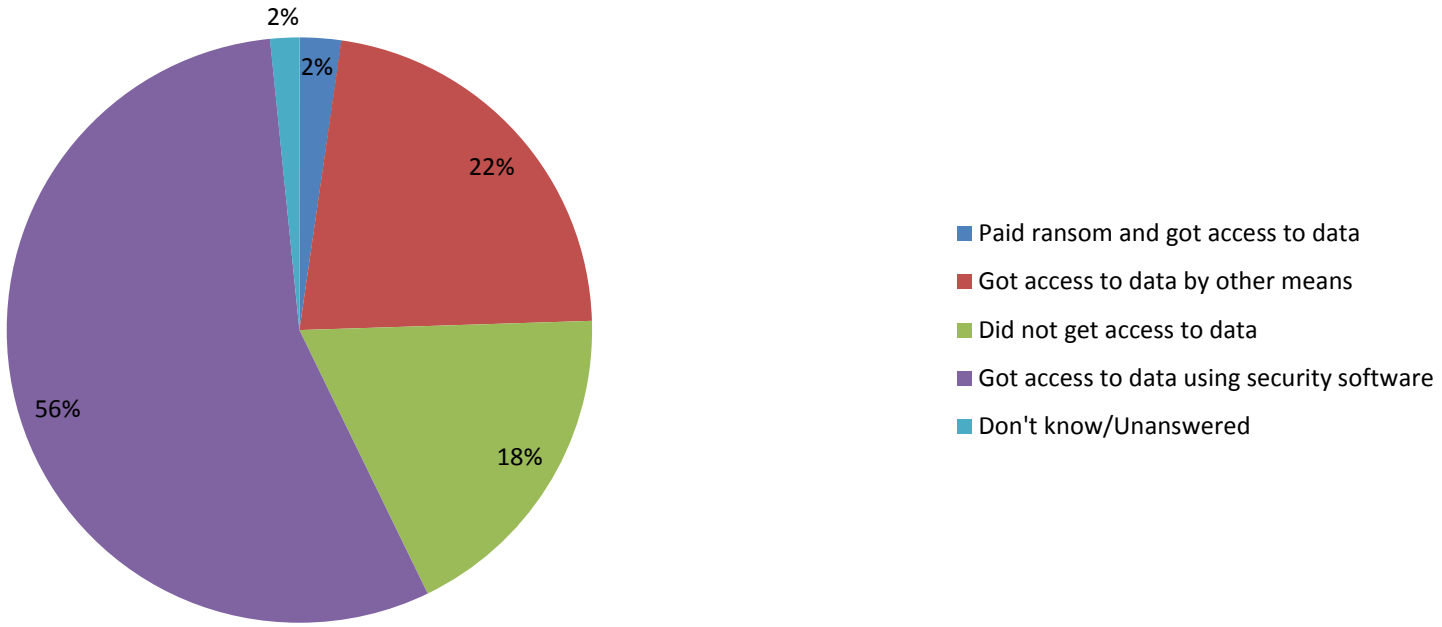
DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

Fra Borgernes informationssikkerhed 2014: Har du været ramt af ransomware?



DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

Fra Borgernes informationssikkerhed 2014: Ramt af ransomware – hvordan reagerede du?



Adobe Flash

- Sårbarheder i Flash udnyttes igen i stigende grad

- Mange upatchede Flash-installationer

(kilde: Cisco Midyear Security Report)

DKCERT anbefaler:

- *Afinstaller Flash, hvor den ikke er nødvendig*
- *Hold installationer opdateret med nyeste patch*

DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

Den endnu ukendte trussel

Fire eksempler fra det seneste halvandet år:

- **HeartBleed** – hidtil ukendt hul i **OpenSSL** giver adgang til potentielt fortrolige data

- **Shellshock** eller **Bashdoor** – hidtil ukendt hul i **Unix Bash Shell** lader udefrakommende køre kommandoer på servere

Den endnu ukendte trussel

Fire eksempler fra det seneste halvandet år:

- **POODLE** (Padding Oracle On Downgraded Legacy Encryption) – man-in-the-middle-angreb mod den forældede SSL v. 3

- **FREAK** (Factoring RSA Export Keys) – ny sårbarhed i OpenSSL (genbrug af svage nøgler) giver risiko for man-in-the-middle-angreb i Safari og Android

DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

POODLE og FREAK på Forskningsnettet

- **Universiteter har styr på FREAK, men er bagud på POODLE**

- DKCERTs internationale kilder følger med i, hvor mange servere der har sårbarheder som fx FREAK (Factoring attack on RSA-EXPORT Keys) eller POODLE (Padding Oracle On Downgraded Legacy Encryption)

- På en tilfældig dag i juni var 17.700 danske servere sårbare med FREAK. 150 af dem var servere på Forskningsnettet

- Med andre ord udgjorde sårbare servere på Forskningsnettet kun 0,8 procent af de danske sårbarheder

DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

POODLE og FREAK på Forskningsnettet

- 3. oktober var 406 danske servere sårbare med FREAK – heraf kun 1 på Forskningsnettet

- Det viser, at universiteterne og andre institutioner på Forskningsnettet har været effektive, når det gælder om at eliminere FREAK, som nu praktisk talt er udryddet

DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

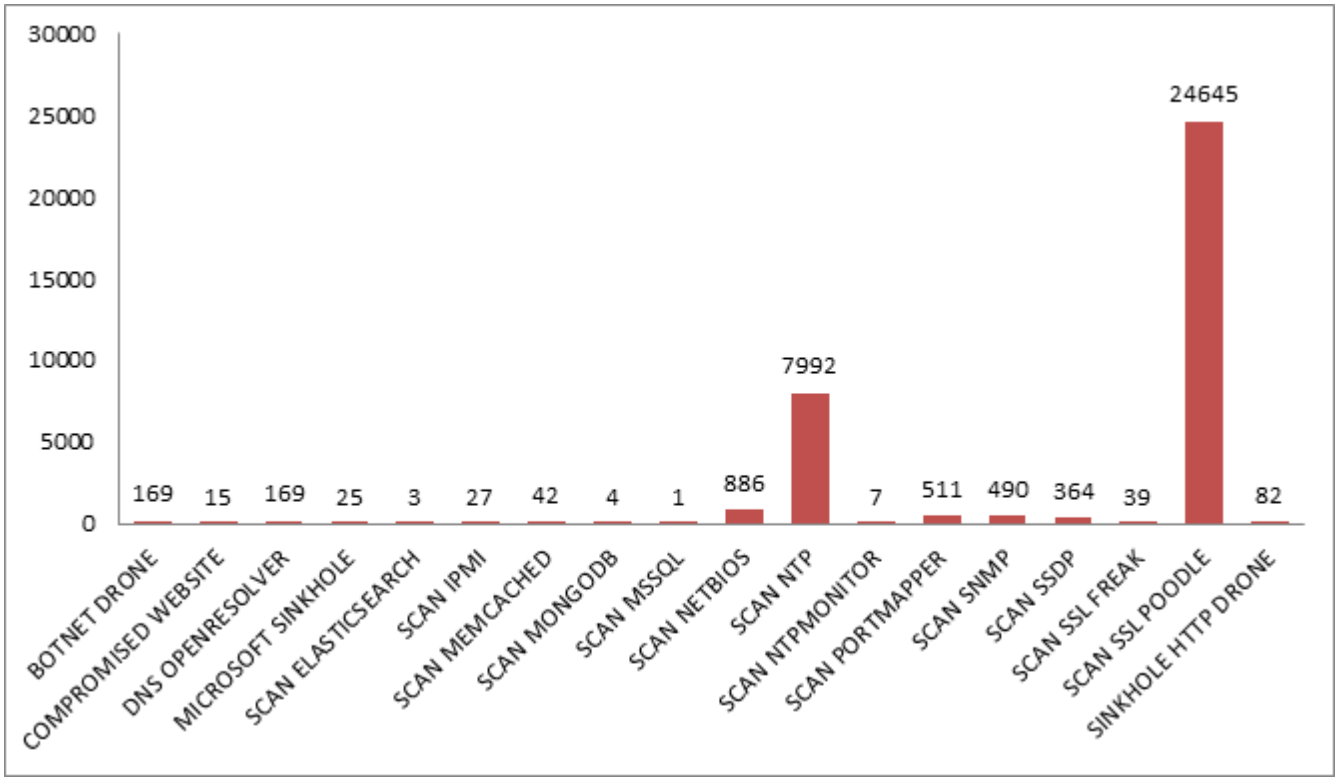
POODLE og FREAK på Forskningsnettet

- Når det gælder POODLE, var der på en given dag i juni 650 sårbare IP-adresser på Forskningsnettet
- 3. september var tallet faldet til 622, 3. oktober til 536
- POODLE udgør således mere end 65% af de sårbarheder, DKCERT kunne rapportere den 3. oktober.
  POODLE og Open NTP udgør nu tilsammen næsten 90% af alle sager. De sidste 10% er fordelt på 16 kategorier
- *DKCERT anbefaler derfor, at institutionerne gør en aktiv indsats for at fjerne systemer med POODLE-sårbarheden fra Forskningsnettet*

DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

Sårbarheder på Forskningsnettet

- Siden medio juli 2015, har DKCERT informeret om 35.471 sager totalt i følgende kategorier for FSKNET – POODLE og NTP udgør 92%:



Den endnu ukendte trussel

Fra den mobile verden – Android:

- **Stagefright bug** – en angriber kan afvikle arbitrær kode og give sig selv udvidede privilegier på en Android-enhed

- **Certifi-Gate** – Skadelige apps kan udnytte sikkerhedshuller i systemer til fjernstyring af Android-enheder til at få øgede privilegier

DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

Den endnu ukendte trussel

Et friskt eksempel – Apple går ikke fri:

- **XcodeGhost** - kopier af udviklerværktøjet Xcode med objektfiler inficeret med malware medfører inficerede apps til iOS – bl.a. Angry Birds 2 og WeChat

Den endnu ukendte trussel




DKCERT anbefaler:

- *Hav en beredskabsplan, der siger, hvem der gør hvad, hvor og hvornår, når den ukendte trussel viser sig*

DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

Malware på mobile enheder

- 0,6 % af systemer koblet op mod mobile netværk er inficeret med malware
- 80 % er Windows (pc'er, Windows Phone, tablets)
- Android er faldet fra 50 % til 20 % - takket være indsats for oprydning i Google Playstore

(Kilde: Alcatel Lucent Report on Infected Systems Connected to Mobile Networks)

DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

Generel stigende trussel mod universiteter

- Harvard University har offentliggjort, at de i juni var udsat for et omfattende hackerangreb: *http://blog.lifars.com/2015/07/07/8-colleges-impacted-in-harvard-data-breach/*

- Det fremhæves i artiklen, at universiteter i stigende grad er udsat for cyberangreb. Stigningen i sektoren menes at være større end den samlede tendens på verdensplan

- *DKCERT anbefaler, at universiteterne overvejer den øgede generelle trussel i deres risikovurderinger*

Tiltag til at forbedre informationssikkerheden

Passwordsikkerhed

Nu, som for 10 år siden:

- Brug forskellige passwords til forskellige tjenester
  - Borgernes informationssikkerhed 2014: 41% af deltagerne svarede, at de bruger samme password til flere onlinetjenester
- Brug komplekse passwords
  - Kravene til komplekse passwords har udviklet sig
- Del aldrig dine passwords med andre
  - heller ikke med phishere ..

DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

To-faktor-autentifikation

Brugeren skal indtaste en engangskode sammen med sit brugernavn/password. Gør det sværere at misbruge et stjålet password

- Eksempler: Kodekortet til NemID, sms-koder til netbanker, autentifikations-app på Android til Google-tjenester

- Apple udvidede brugen af to-faktor-autentifikation til iCloud efter offentliggørelsen af berømtheders private nøgenfotos

Biometri

- To-faktor-autentifikation kan også være biometrisk:
  - Fingeraftryk
  - Irisscanning
  - Stemmeprøve
  - Ansigtsgenkendelse
- Der har været arbejdet meget med området i gennem årene – kun få systemer har fået videre udbredelse

Adgangskontrollister

- Processer, regler, politikker er vigtige og nødvendige
- De kan ikke stå alene:
  - Tekniske kontroller
- Adgangskontrol på filniveau

DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

Begræns administratorrettigheder

- Hvis brugerkontoen har rettigheder som lokaladministrator, kan man alt på computeren: Installere programmer, installere drivere, ændre firewall-opsætning og hvad man ellers har lyst til

- KPMG-undersøgelse

DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

Logning

- Log, hvem der tilgår hvad
- Log, hvem der ændrer hvad
- Gennemgå og kontroller loggerne
- Reager på afvigelser

DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

Krypter e-mails

- En e-mail er som et åbent postkort – andre kan læse med
- Send aldrig følsomme eller fortrolige oplysninger i ukrypterede mails

Kryptering

- Snowden-afsløringerne viser: Hvis du ikke krypterer dine data, deler du dem med NSA/PET/GCHQ… - eller andre…
- Men kryptering kan også have huller (Heartbleed i OpenSSL, POODLE i SSL v.3)
- NSA er aktiv i udviklingen af kryptering – mistanke om bagdøre
- **Behov for uafhængige audits af udbredte krypteringssystemer**

DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

Hvad skal vi kryptere?

- Mailserver
- Filserver
- Hele disken på pc'en
- Smartphone – bliver standard i iOS, Android

- Det virker – en af de dømte i hackersagen om angrebet på CSC havde brugt kryptering på sin bærbare. Politiet har ikke kunnet knække den

- Politisk tendens til at forbyde kryptering for private?

Udfordringer for informationssikkerheden

DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

Ledelsen skal på banen

- Forudsætning i ISO27001
- ”Vandskel” mellem teknikere og forretning
  - Kun ledelsen kan bygge bro
- Faste, dokumenterede processer – der kontrolleres!
- Lyt til rådgivere og revision
- Lav risikovurderinger – og invester i den nødvendige sikkerhed

DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

Processer

- Ændringsstyring
- Test
- Backup
- Logning
- Sikker softwareudvikling

DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

Nyhed fra DKCERT: Virksomhedskultur bestemmer sikker udvikling

- 27-08-2015: Hvis kulturen i en virksomhed siger, at softwareudvikling skal tage aktiv stilling til sikkerheden, bruger udviklerne sikkerhedsværktøjer. De er mere tilbøjelige, hvis de ser deres kolleger gøre det.

  Det fremgår af en undersøgelse, som forskere inden for datalogi og psykologi har foretaget blandt over 250 softwareudviklere. Forskerne fra North Carolina State University og Microsoft Research undersøgte, hvad der får udviklere til at bruge sikkerhedsorienterede værktøjer i deres daglige arbejde.

DKCERT
COMPUTER SECURITY INCIDENT RESPONSE TEAM

Nyhed fra DKCERT: Virksomhedskultur bestemmer sikker udvikling

- De udviklere, der arbejdede på produkter, hvor sikkerhed er et vigtigt element, var ikke mere tilbøjelige til at bruge sikkerhedsværktøjer end andre udviklere.

  Derimod viser undersøgelsen, at udviklere påvirkes af deres omgivelser: Hvis de ser deres kolleger bruge sikkerhedsværktøjer, er de mere tilbøjelige til også selv at gøre det.

  Det næstvigtigste element hos dem, der bruger sikkerhedsværktøjer, er virksomhedskulturen: **Deres chefer forventer, at de bruger dem.**

[Tak for opmærksomheden !]

[Spørgsmål?]

Henrik Larsen

Email: henrik.larsen@cert.dk

DKCERT