DKCERT

DeiC

DeiC-konferencen 2021:
Trends 2021

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

> Indhold

- > Om DKCERT – lyt med i morgen kl. 13.30
- > Vores trusselsvurdering og metode, baggrund og resultat
- > Eksempler på hændelser fra sektoren og konsekvenser (udenlandske, danske)
- > Fokus på de trends, vi har beskrevet i Trendrapporten og hvad status er på dem her ½ år efter
- > Trends som vi ikke så, men som måske skulle være med
- > Spørgsmål

> DKCERT Trusselsvurdering 2021: Hovedvurderinger

> Truslen fra cyberspionage mod den danske uddannelses- og forskningssektor er **meget høj**. Fremmede stater og kriminelle har stor interesse i at stjæle forskningsdata og intellektuel ejendom fra sektoren.

> Truslen fra cyberkriminalitet er **meget høj**. Det er sandsynligt at cyberkriminelle angreb kan forstyrre den daglige drift eller skade forskningsdata.

> DKCERT Trusselsvurdering 2021: Hovedvurderinger

> Truslen fra cyberaktivisme er **lav**. Truslen er ofte motiveret af enkeltsager og truslen mod sektoren kan derfor stige uden eller med kort varsel.

> Truslen, at fremmede stater vil rette destruktive cyberangreb mod dansk samfundsvigtig infrastruktur, herunder uddannelses-sektoren er **lav**.

> DKCERT Trusselsvurdering 2021: Hovedvurderinger

> Insidertruslen mod uddannelses- og forskningssektoren er **meget høj**. Der er manglede opmærksomhed vedrørende truslen og konsekvenserne heraf, hvilket øger sandsynligheden for menneskelige fejl, uanset om disse er bevidste eller ubevidste.

DKCERT

TECHNISCHE UNIVERSITÄT BERLIN

STUDIEREN LEHREN FORSC

Alle News

Einschränkung IT-Services Studieren Arbeiten Forschen

IT-Services der TU Berlin nach Angriff weiterhin eingeschränkt

03.05.2021

NEW LINUX MALWARE ON THE BLOCK —

High-performance computers are under siege by a newly discovered backdoor

Stealthy Kobalos malware has infected HPC networks belonging to high-profile organizations.

DKCERT

Tjenester Information FAQ Om DKCERT

Ransomware rammer college og universitet i Irland

Af Eskil Sørensen, 07/04/21

It-systemer taget ned og campus lukket.

National College of Ireland (NCI) og Technological University of Dublin har meddelt, at et ransomware-angreb har ramt deres it-systemer. Det skriver Bleeping Computer.

TECHNISCHE UNIVERSITÄT BERLIN

STUDYING

All news

Restricted IT services News

IT Attack: Additional Data Published on the Darknet

06/11/2021

Updated on Friday, 11 January 2021, at 16:23

On 10 June 2021, 5,483 files illegally obtained as part of a criminal cyberattack on TU Berlin were published on the darknet.

Catalin Cimpanu

May 4, 2021

Government Nation-state News

Belgium's government network goes down af massive DDoS attack

Most of the Belgium government's IT network has been down today after a mas distributed denial of service (DDoS) attack knocked offline both internal systems and public-facing websites.

The attack targeted Belnet, a government-funded ISP that provides internet connectivity for Belgian government organizations, such as its Parliament, educational institutes, ministries, and research centers.

Ransomware gangs have found another set of new targets: Schools and universities

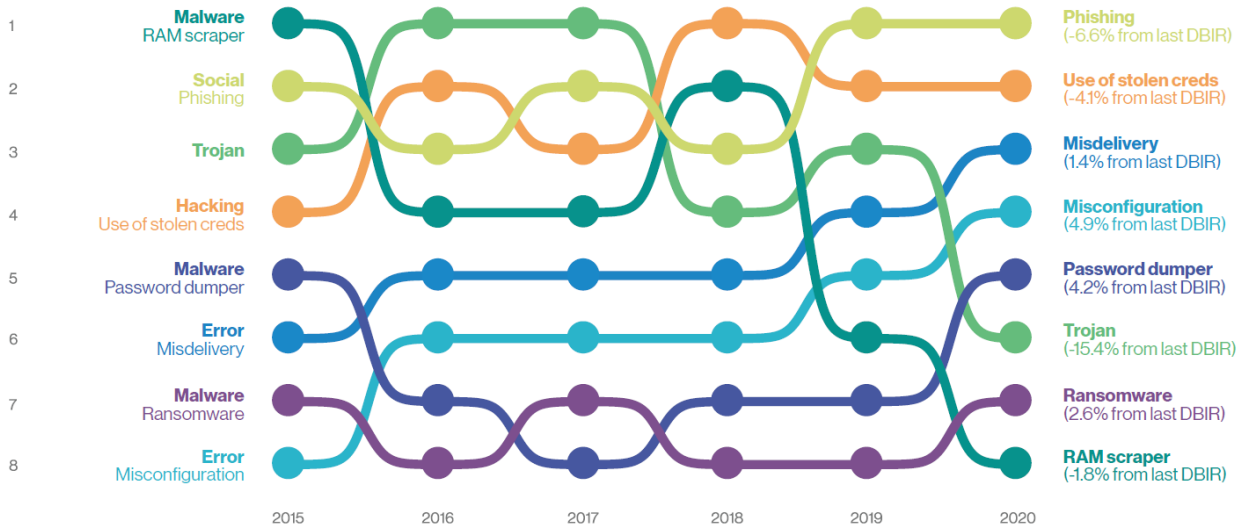
National Cyber Security Centre issues advice on how to protect networks from cyber criminals after a spike in ransomware attacks causing disruption across the education sector over the past month

Check Point

PRODUCTS SOLUTIONS SUPPORT & SERVICES PARTNERS RESOURCES

Check Point Research: Education sector sees 29% increase in attacks against organizations globally

- Check Point Research (CPR) observes a steady increase in the average number of cyberattacks per organization weekly, with the education/research sector showing a higher number of attacks than other sectors
- In July 2021, there was a 29% increase in attacks against organizations in the education sector compared to H121
- By region, organizations in education/research sector in South Asia most targeted, followed by East Asia and ANZ
- By country, Indian education organizations are the most targeted, followed by those in Italy and Israel



Ændringer i hyppighed af sikkerhedsbrud

Kilde: Verizon Data Breach Investigations Report 2020

> Tendenser

> Trusselsvurderingen fremhæver to tendenser af væsentlig betydning

- > Social Engineering
- > Supply Chain Attacks

Hackeren	It-sikkerhedsafdelingen
Masser af tid	Begrænset tid, ofte prioriteret drift
Mange personer	Få personer – ofte prioriteret drift
Specialiserede kompetencer	Mangel på kompetencer
Gratis værktøjer og exploits	Cyberforsvar er dyrt
En sårbarhed er nok	Svært at holde alle systemer opdateret
En succes er nok	En fejl/opmærksomhed kan være fatal
Udbredt vidensdeling	Begrænset videndeling

> Anbefalinger

> På baggrund af trusselsvurderingen og tendenserne, har DKCERT følgende anbefalinger:

- > Øg awareness blandt medarbejdere
- > Baseline sikkerhed for tilkoblet udstyr
- > Etabler og følge op på Patch Management
- > Begræns administratoradgange
- > Integrer god hygiejne i sikkerhedskulturen

> Skærpede anbefalinger

- > Afsæt ressourcer til uddannelse og kompetenceudvikling af alle medarbejdere i informationssikkerhed
- > Adressér løbende behovet for at efterleve retningslinjerne.
- > Overvej evt. disciplinære forholdsregler ved overtrædelse af politik og retningslinjer
- > Foretag løbende risikovurderinger også ved hændelser der rammer lignende institutioner
- > Understøt en kultur, hvor dialog om informationssikkerhed er en del af sikkerhedsarbejdet(SIC!) -> del af det daglige arbejde

> Status på trends 2021

- > Cybertruslen bliver mainstream
- > Intensiteten i hjemmearbejde udfordrer sikkerheden
- > Phishingplagen fortsætter
- > Specialisering af cyberdisciplinerne fortsætter
- > Konkurrencen blandt cyberkriminelle intensiveres
- > Store cyberangreb bliver større og længerevarende
- > Videnssektoren bliver i højere grad mål for cyberkriminelle
- > Ransomware

> Hvad mangler af trends?

- AI
- IOT
- OT
- Flere (forkortelser)?

> Vigtigste take-aways

- > Truslen mod sektoren fra kriminalitet og spionage er **meget høj**
- > Vi ser og har set konkrete eksempler i sektoren
- > Det fremstår tydeligere nu end før, at cyberkriminalitet er en stor forbundet markedsmekanisme, hvor kendte greb i den analoge verden bruges i den digitale
- > Ransomwaregrupper er (ligesom) kommercielle virksomheder
- > Spionagegrupperinger er sandsynligvis mere professionelle end de cyberkriminelle

DKCERT

DeiC

> Spørgsmål?

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