

Din forretning er bygget på it
inu:it holder den på sporet



Anders Hoffgaard
Adm. Direktør
IT sikkerhed



Morten K. L. Olsen
Landechef Grønland
Hosting & Service



Casper Danielsen
Senior Netværkskonsulent
Netværk & telefoni

nu:it

nu:it Kattuffiat

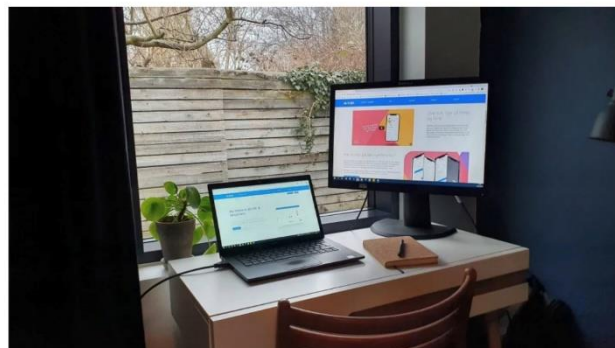
From "Domi

16.15 ↗



It-ekspert: Hjemme- arbejdspladser er en gave til hackerne

Mange danske virksomheder er ikke rustet til at håndtere cybertruslen fra Rusland, mener it-ekspert.



Center for Cybersikkerhed (CFCS) har onsdag hævet trusselsniveauet fra lav til middel. Det kunne være gjort en måned tidligere, mener it-ekspert. | Foto: Visma Enterprise/PR

AF RITZAU

Offentliggjort: 18.05.22 kl. 18:04

Da danske virksomheder under coronakrisen sendte deres ansatte hjem til hjemmearbejdspladsen i hobetale, fik hackerne pludselig nye muligheder for at gå til angreb.

Det siger Peter Kruse, der er it-sikkerhedsekspert. Han er også medstifter af sikkerhedsfirmaet CSIS.

"Og det er min vurdering, at mange virksomheder ikke er rustet til at håndtere den trussel, som hjemmearbejdspladserne er med til at skabe," siger han.

Udmeldingen kommer, efter at Center for Cybersikkerhed (CFCS) onsdag hævede

rganizations



14-10-2022

inu:it

2022



While we “wait” for the Russian cyber revenge wave

*“Russia is currently waging a conventional war against Ukraine, but both companies and public organizations may just as well begin to prepare for a looming **Russian cyber-revenge wave**.”*

The Russians (will) throw themselves on revenge operations against both the governments and private companies that have imposed sanctions and boycott on Russia, as well as they have closed production and offices in the country.”

Christian Wernberg-Tougaard, Head of Cyber, KPMG

The three Russian cyber-attacks the West most fears (BBC News March 2022)



Russia is a cyber-superpower with a serious arsenal of cyber-tools, and hackers capable of disruptive and potentially destructive cyberattacks.

BlackEnergy - targeted critical infrastructure attack

In 2015 Ukraine's electricity grid was disrupted by [a cyber-attack called BlackEnergy](#), which caused a blackout for 80,000 customers of a utility company in western Ukraine.

NotPetya - uncontrollable destruction

The destructive software was hidden in an update of popular accounting software used in Ukraine but spread worldwide destroying the computer systems of thousands of companies and causing approximately \$10bn of damage.

Colonial Pipeline - cyber-criminal attacks intensify

In May 2021, a state of emergency was declared in a number of US states after hackers caused a vital oil pipeline to shut down.



May 2021

Hacker attacks create long queues for gas stations in the United States

This is due to a major hacker attack on the Colonial Pipeline Company, the company behind an 8,850-kilometer pipeline that supplies large parts of the United States with fuel.

Over the past 5 years, CPC had invested \$ 200 million in IT and IT security.

Ransom: 90 m \$





Sermersooq: Sociale ydelser forsinkes på grund af sikkerhedsbrud

De omfattende it-problemer i Selvstyret har lammet flere økonomisystemer, oplyser Kommuneqarfik Sermersooq.

Cyberangreb giver store problemer i sundhedsvæsenet

Naalakkersuisut melder nu ud, at sundhedsvæsenets it-problemer skyldes et cyberangreb.



SECURITY CAPABILITIES

SECURITY MANAGEMENT

- Security program
- Management & org.
- Risk management
- Supplier management
- Policies & doc.
- SaaS requirements
- Audit
- Evaluation & improvement
- Culture & competencies
- Compliance & privacy
- Incident response

PROTECTION

- Application security
- Endpoint / mobile device
- Network security
- Physical security
- Production systems
- Data protection
- Host / server security
- Social media & e-mail

OPERATIONAL SECURITY

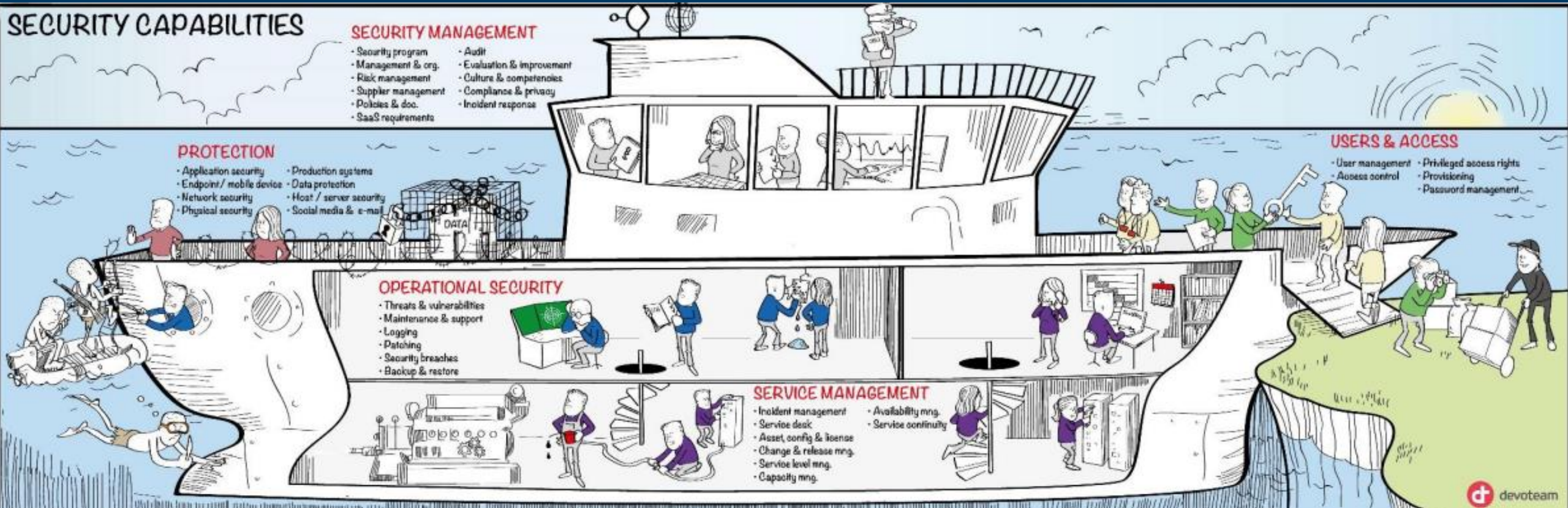
- Threats & vulnerabilities
- Maintenance & support
- Logging
- Patching
- Security breaches
- Backup & restore

SERVICE MANAGEMENT

- Incident management
- Service desk
- Asset, config & license
- Change & release mng.
- Service level mng.
- Capacity mng.
- Availability mng.
- Service continuity

USERS & ACCESS

- User management
- Access control
- Privileged access rights
- Provisioning
- Password management



inu:it and i-trust






enablør



I-Trust | enabler

AktivitetcenterTilsynStamdataRapporter

Gå til...



KlausI-Trust

Du svarer for Kunde 4

1%

1 Cybersikkerhed CIS18

CIS Kontroller

1: Registrering og kontrol af virksomhedens aktiver

2: Registrering og kontrol af softwareaktiver

3: Databeskyttelse

4: Sikker konfiguration af aktiver og software

5: Brugeradministration

6: Adgangskontroladministration

7: Kontinuerlig sårbarhedsstyring

8: Administration af revisionslogfiler

9: E-mail- og webbrowserbeskyttelse

10: Malwarebeskyttelse

11: Datagendannelse

1: Registrering og kontrol af virksomhedens aktiver

Aktivt administrere (opgøre, spore og korrigere) alle virksomhedens aktiver (slutbrugerenheder, herunder bærbare og mobile enheder, netværksenheder, ikke-computere/Internet of Things (IoT)-enheder og servere), der er forbundet til infrastrukturen fysisk, virtuelt, eksternt og i cloud-miljøer, for at få et præcist kendskab til alle de aktiver, der skal overvåges og beskyttes i virksomheden. Dette vil også støtte identifikation af uautoriserede og uadministrerede aktiver, der skal fjernes eller afhjælpes.

Fortegnelse over og kontrol med hardwareaktiver

Vedligeholder organisationen en fortegnelse over alt udstyr, der kan lagre eller behandle data?

Nej

Ikke besvaret

Ja

Kommentar

Ved ikke

Ikke relevant

Isolerer, fjernes eller godkendes hardwarekomponenter, der ikke er autoriserede til at indgå i fortegnelsen over udstyr?

Nej

Ikke besvaret

Ja

Ved ikke

Ikke relevant

Bruger organisationen dagligt eller oftere "Discovery tools" til at identificere alle hardwarekomponenter tilknyttet organisationens net?

Nej

Ikke besvaret

Ja

Ved ikke

Ikke relevant

Anvendes DHCP logging ugentligt eller oftere for at opdatere liste af enheder?

Referencer, hjælp og vejledning

Hjælpetekst

Etabler og vedligehold en nøjagtig, detaljeret og opdateret opgørelse over alle virksomhedens aktiver med potentiale til at gemme eller behandle data, herunder: slutbrugerenheder (inklusive bærbare og mobile), netværksenheder, ikke-computing/IoT-enheder og servere. Sørg for, at registrerer netværksadressen (hvis statisk), hardwareadresse, maskinnavn, dataaktivejer, afdeling for hvert aktiv, og om aktivet er blevet godkendt til at oprette forbindelse til netværket. For mobile slutbrugerenheder kan værktøjer af MDM-typen understøtte denne proces, hvor det er relevant. Denne opgørelse inkluderer aktiver, der er forbundet med infrastrukturen fysisk, virtuelt, eksternt og de som er i cloudmiljøer. Derudover omfatter det aktiver, der regelmæssigt er forbundet med virksomhedens netværksinfrastruktur, selvom de ikke er under virksomhedens kontrol. Gennemgå og opdater beholdningen af alle virksomhedens aktiver hvert andet år eller oftere.

Reference

Sans Cis 1.1

Trusler

Taksonomi for Driftsrisiko (Carnegie Mellon University)

Trusselskategori: 1. Menneskelige handlinger

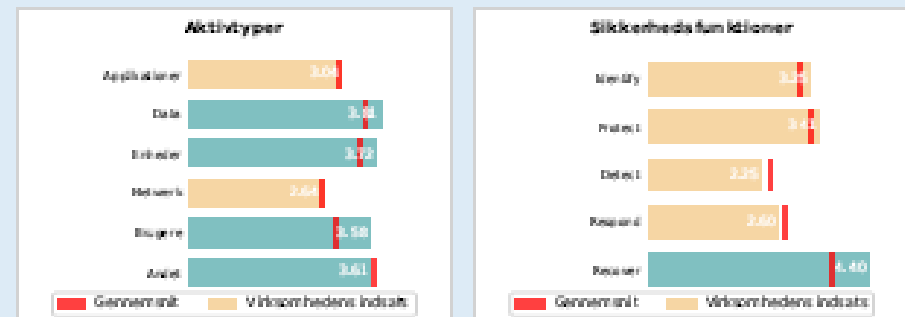
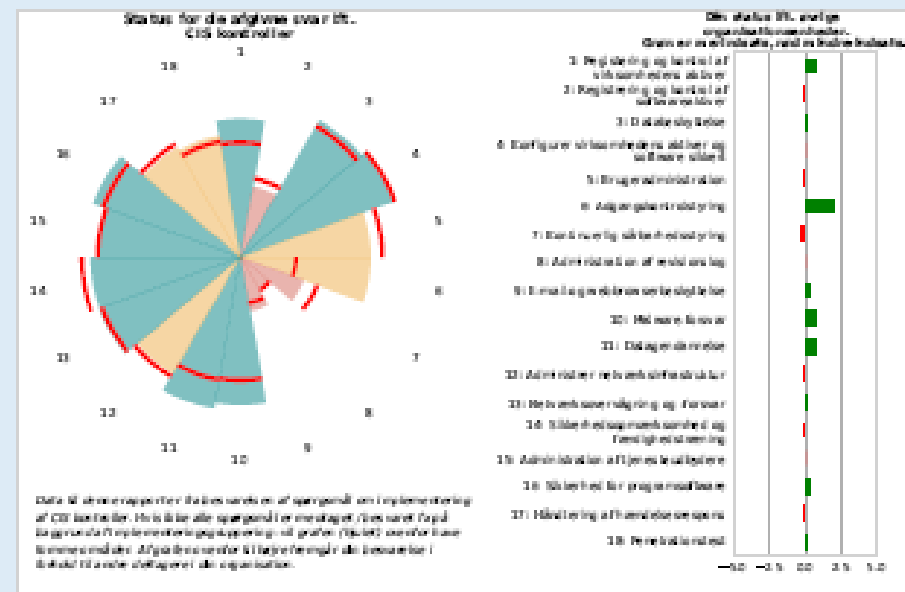
Trusselsgruppe: 1.2 Forsætligt >

Trusselsgruppe: 1.4 Forsætligt/ext >

14-10-2022

inu:it

arbejde med informations-
sikkerhed 2022



Sporøgsmål, der kræver særlig opmærksomhed

Tallitotien kasvutehokas kasvu, kas on määratud suurem osale kasvukohast, mis on juba kasvatatud.

[illegible]

Alle spargen! Der Ausdruck ist ein Beispiel für komplexe Mehrdeutigkeit: Was soll er? Ist es der gelbe Spargel oder der Wein? Der Spargel ist ein *Wort*, das andere *Wörter* spargt. Die Spargel sind die *Wörter*, die andere *Wörter* spargen. Oder es ist ein *Wort*, das andere *Wörter* spargt. Das ist ein Beispiel für eine komplexe Mehrdeutigkeit.

ARBEJDE MED CYBERFORSVAR 2022

Status ift. cyberrobusthed

Inklusiv Center for Cybersikkerheds anbefalede indsatser





14-10-2022

inu:it

KERNEKOMPETENCER

- Network
- IT-security
- Hosting/cloud
- BackUp og Restore
- Database Management
- IMS – Infrastructure Management Services
- AMS – Application Management Services
- Support & Help Desk 24/7/365
- Internet and telefon
- Udvikling

Netværk (MPLS + on prem) – internet - telefoni

- Internet til det meste af Grønland.
- MPLS net som binder din virksomhed sammen på tværs af byer og lokationer
- Flatrate telefoni til hele verden. Ring til hele verden så meget du vil for en fast pris hver måned. Vi leverer det både som Teams telefoni og som 3cx.
- Network as a service
- Rådgivning
- Sikkerheds hardening

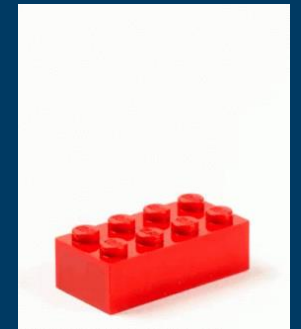
Hosting løsning vi tilbyder:

- I inu:it's datacenter i Nuuk
Adgangskontrol, nødstrøm, køling, redundant setup, osv...
 - Dedikeret hosting*
 - Shared hosting*
- I hosting center i Danmark
- Cloud hosting i Azure
- On-Prem hosting hos dig som kunde



Support / overvågning / rådgivning

- Support på medgået tid
- Flaterate support aftaler
 - Kend din udgift på forhånd – pr bruger / mdr.
 - Tilpasses efter dine behov – LEGO model
- Vagtordning 24 / 7 / 365
- Overvågning af systemer / enheder 24 / 7 / 365
- Rådgivning om IT – timebasis eller projektbasis



Ønsker du at vi hjælper dig med at holde din virksomhed på sporet?

Scan QR-koden og tag kontakt til en af os allerede i dag



Anders Hoffgaard



Morten K. L. Olsen



Casper Danielsen



Allan Sandgreen



Erna Broberg

