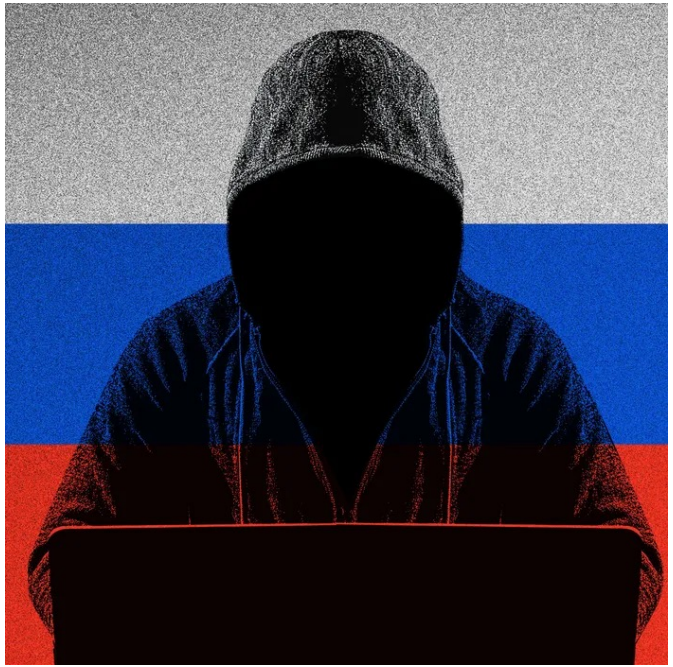
Forebyggende IT-sikkerhed

MAC-PC
V/J. ANDERSEN

TEKNISK HJÆLP TIL SMÅ & STORE VIRKSOMHEDER

Forebyggende IT-sikkerhed

”Russiske hackerangreb er et fact of life.”



Kilder:
tv2.dk
Nymag

MAC-PC V/J. ANDERSEN
TEKNISK HJÆLP TIL SMÅ & STORE VIRKSOMHEDER

Anmeldelse af hackerangreb

Kilder:
Version 2
SVM DK

MAC-PC V/J. ANDERSEN
TEKNISK HJÆLP TIL SMÅ & STORE VIRKSOMHEDER

Anmeldelse af hackerangreb

I 2022 anmeldte danske virksomheder 2075 hackerangreb til politiet, hvilket er en stigning på 64 procent i forhold til år 2021.

Kilder:
Version 2
SVM DK

Anmeldelse af hackerangreb

I 2022 anmeldte danske virksomheder 2075 hackerangreb til politiet, hvilket er en stigning på 64 procent i forhold til år 2021.

”Det er helt essentielt, at virksomhederne anmelder hackerangreb til politiet”

Kilder:
Version 2
SVM DK

Anmeldelse af hackerangreb

Følgende typer af kriminalitet, skal ikke anmeldes som hacking, men i stedet som økonomisk kriminalitet:

Kilde: https://politi.dk/hacking/anmeld-hacking

Anmeldelse af hackerangreb

Følgende typer af kriminalitet, skal ikke anmeldes som hacking, men i stedet som økonomisk kriminalitet:

- Der er forsvundet penge fra din bankkonti uden din viden, eller nogen har haft uberettiget adgang til din netbank.

Kilde: https://politi.dk/hacking/anmeld-hacking

MAC-PC V/J. ANDERSEN
TEKNISK HJÆLP TIL SMÅ & STORE VIRKSOMHEDER

Anmeldelse af hackerangreb

Følgende typer af kriminalitet, skal ikke anmeldes som hacking, men i stedet som økonomisk kriminalitet:

- Der er forsvundet penge fra din bankkonti uden din viden, eller nogen har haft uberettiget adgang til din netbank.
- Afpresning via e-mail, herunder trusler om eks. offentliggørelse af data, hvis ikke der betales et beløb i kryptovaluta.

Kilde: https://politi.dk/hacking/anmeld-hacking

MAC-PC V/J. ANDERSEN
TEKNISK HJÆLP TIL SMÅ & STORE VIRKSOMHEDER

Anmeldelse af hackerangreb

Følgende typer af kriminalitet, skal ikke anmeldes som hacking, men i stedet som økonomisk kriminalitet:

- CEO/BEC fraud.

Kilde: https://politi.dk/hacking/anmeld-hacking

Anmeldelse af hackerangreb

Følgende typer af kriminalitet, skal ikke anmeldes som hacking, men i stedet som økonomisk kriminalitet:

- CEO/BEC fraud.
- Ransomware.

Kilde: https://politi.dk/hacking/anmeld-hacking

MAC-PC V/J. ANDERSEN

TEKNISK HJÆLP TIL SMÅ & STORE VIRKSOMHEDER

Anmeldelse af hackerangreb

- Anmeldelse bør ske inden for 72 timer.

Kilde: Datatilsynet.dk

Anmeldelse af hackerangreb

- Anmeldelse bør ske inden for 72 timer.
- Blanket til anmeldelse af ”sikkerhedsbrud”.

Kilde: Datatilsynet.dk

MAC-PC V/J. ANDERSEN
TEKNISK HJÆLP TIL SMÅ & STORE VIRKSOMHEDER

Anmeldelse af hackerangreb

- Anmeldelse bør ske inden for 72 timer
- Blanket til anmeldelse af ”sikkerhedsbrud”
- Ingen differencering af begrebet hacking:
  - Malware
  - DoS
  - Ransomware
  - IT-udstyr – eks. server, e-mail mfl.

Kilde: Datatilsynet.dk

At sikre sin mail

- Anvend MFA.

At sikre sin mail

- Anvend MFA.
- DMARC (hvis du har e-mails på eget domæne).

Kilde: Hostmaster

At sikre sin mail

- Anvend MFA.
- DMARC (hvis du har e-mails på eget domæne).
- Klik *aldrig* på link fra ukendte afsendere.

At sikre sin mail

- Anvend MFA.
- DMARC (hvis du har e-mails på eget domæne).
- Klik *aldrig* på link fra ukendte afsendere.
- Anvend ”Sikker mail” integration til eks. Outlook.

MAC-PC V/J. ANDERSEN

TEKNISK HJÆLP TIL SMÅ & STORE VIRKSOMHEDER

At sikre sin mail

- Anvend MFA.
- DMARC (hvis du har e-mails på eget domæne).
- Klik *aldrig* på link fra ukendte afsendere.
- Anvend ”Sikker mail” integration til eks. Outlook.
- Digital post.

Ransomware

Kilde: [Wikipedia]

MAC-PC V/J. ANDERSEN
TEKNISK HJÆLP TIL SMÅ & STORE VIRKSOMHEDER

Ransomware – forebyggelse

- Hold OS og andet software opdateret.

Ransomware – forebyggelse

- Hold OS og andet software opdateret.
- Backup.

Ransomware – forebyggelse

- Hold OS og andet software opdateret.
- Backup.
- Restore test 2 gange årligt.

MAC-PC
V/J. ANDERSEN
TEKNISK HJÆLP TIL SMÅ & STORE VIRKSOMHEDER

Ransomware – forebyggelse

- Hold OS og andet software opdateret.
- Backup.
- Restore test 2 gange årligt.
- Antivirus.

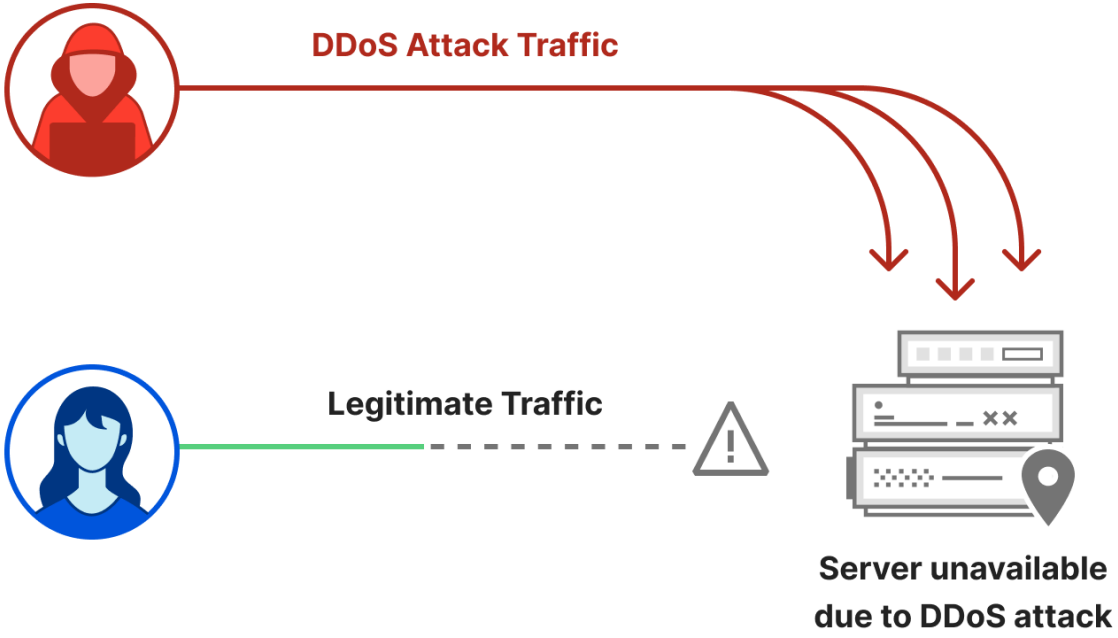
Ransomware – forebyggelse

- Hold OS og andet software opdateret.
- Backup.
- Restore test 2 gange årligt.
- Antivirus.
- Restriktive PC rettigheder.
  - ingen admin rettigheder.
  - download af software i begrænset omfang.

MAC-PC V/J. ANDERSEN

TEKNISK HJÆLP TIL SMÅ & STORE VIRKSOMHEDER

Ddos - hjemmesider



MAC-PC
V/J. ANDERSEN
TEKNISK HJÆLP TIL SMÅ & STORE VIRKSOMHEDER

Ddos - Forebyggelse

- ”Antivirus” installering via udbyder.

Ddos - Forebyggelse

- ”Antivirus” installering via udbyder.
- Opdatering af hjemmeside.

Ddos - Forebyggelse

- ”Antivirus” installering via udbyder.
- Opdatering af hjemmeside.
- Undgå klik på spam mails / links.

Ddos - Forebyggelse

- ”Antivirus” installering via udbyder.
- Opdatering af hjemmeside.
- Undgå klik på spam mails / links.
- Geo blokering.

Ddos - Forebyggelse

- ”Antivirus” installering via udbyder.
- Opdatering af hjemmeside.
- Undgå klik på spam mails / links.
- Geo blokering.
- Backup af hjemmeside.

MAC-PC V/J. ANDERSEN

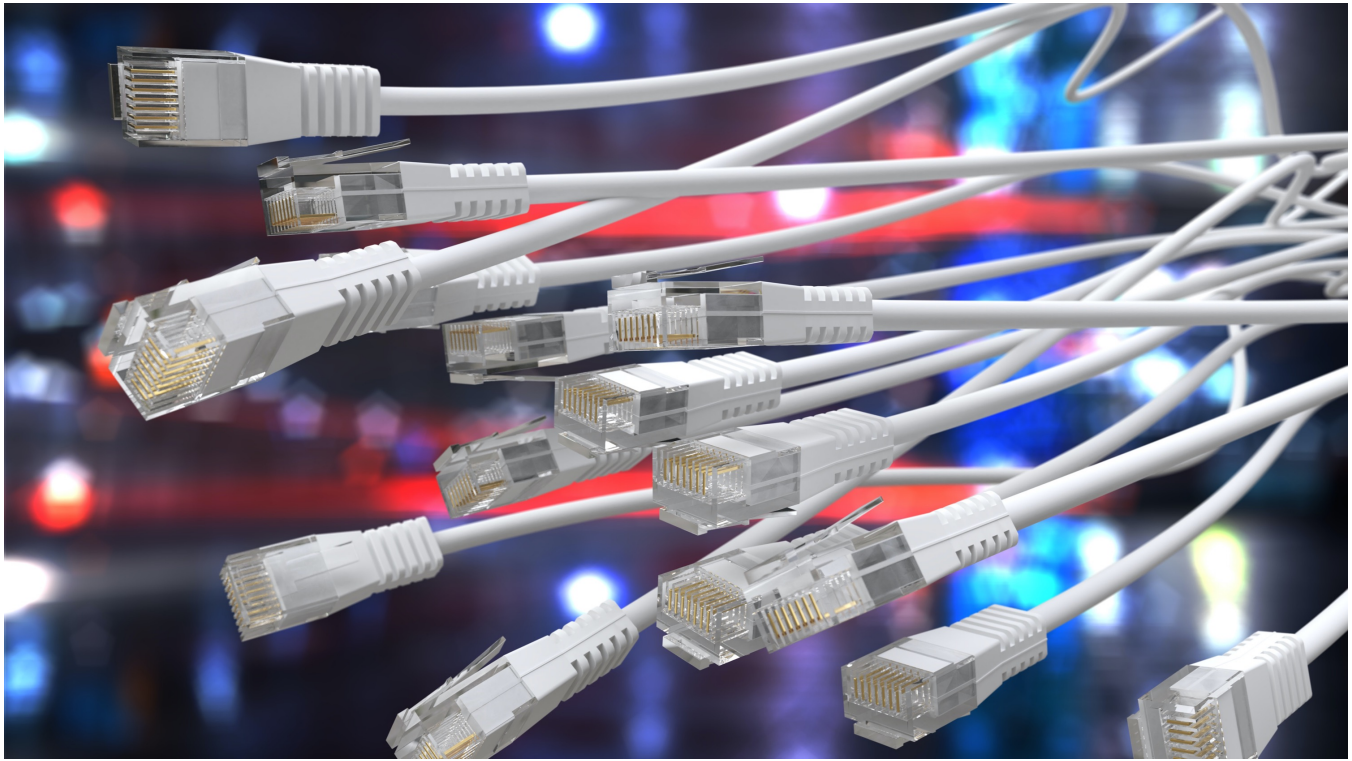
TEKNISK HJÆLP TIL SMÅ & STORE VIRKSOMHEDER

Ddos - Forebyggelse

- ”Antivirus” installering via udbyder.
- Opdatering af hjemmeside.
- Undgå klik på spam mails / links.
- Geo blokering.
- Backup af hjemmeside.
- Certifikat HTTPS.

MAC-PC
V/J. ANDERSEN
TEKNISK HJÆLP TIL SMÅ & STORE VIRKSOMHEDER

Netværk



Netværk

- UPS.

Netværk

- UPS.
- Redundansløsning via udbyder.

Netværk

- UPS.
- Redundansløsning via udbyder.
- Ingen wifi i praksis til borgerne.

MAC-PC V/J. ANDERSEN

TEKNISK HJÆLP TIL SMÅ & STORE VIRKSOMHEDER

Netværk

- UPS.
- Redundansløsning via udbyder.
- Ingen wifi i praksis til borgerne.
- Begrænse adgang til netværksstik.

Netværk

- UPS.
- Redundansløsning via udbyder.
- Ingen wifi i praksis til borgerne.
- Begrænse adgang til netværksstik.
- VPN.

Hardware

Hardware

- USB port lås(e).

Hardware

- USB port lås(e).
- Server og PC´er aflåses.

Hardware

- USB port lås(e).
- Server og PC'er aflåses.
- Tyverisikring generelt.

MAC-PC
V/J. ANDERSEN
TEKNISK HJÆLP TIL SMÅ & STORE VIRKSOMHEDER

Hardware

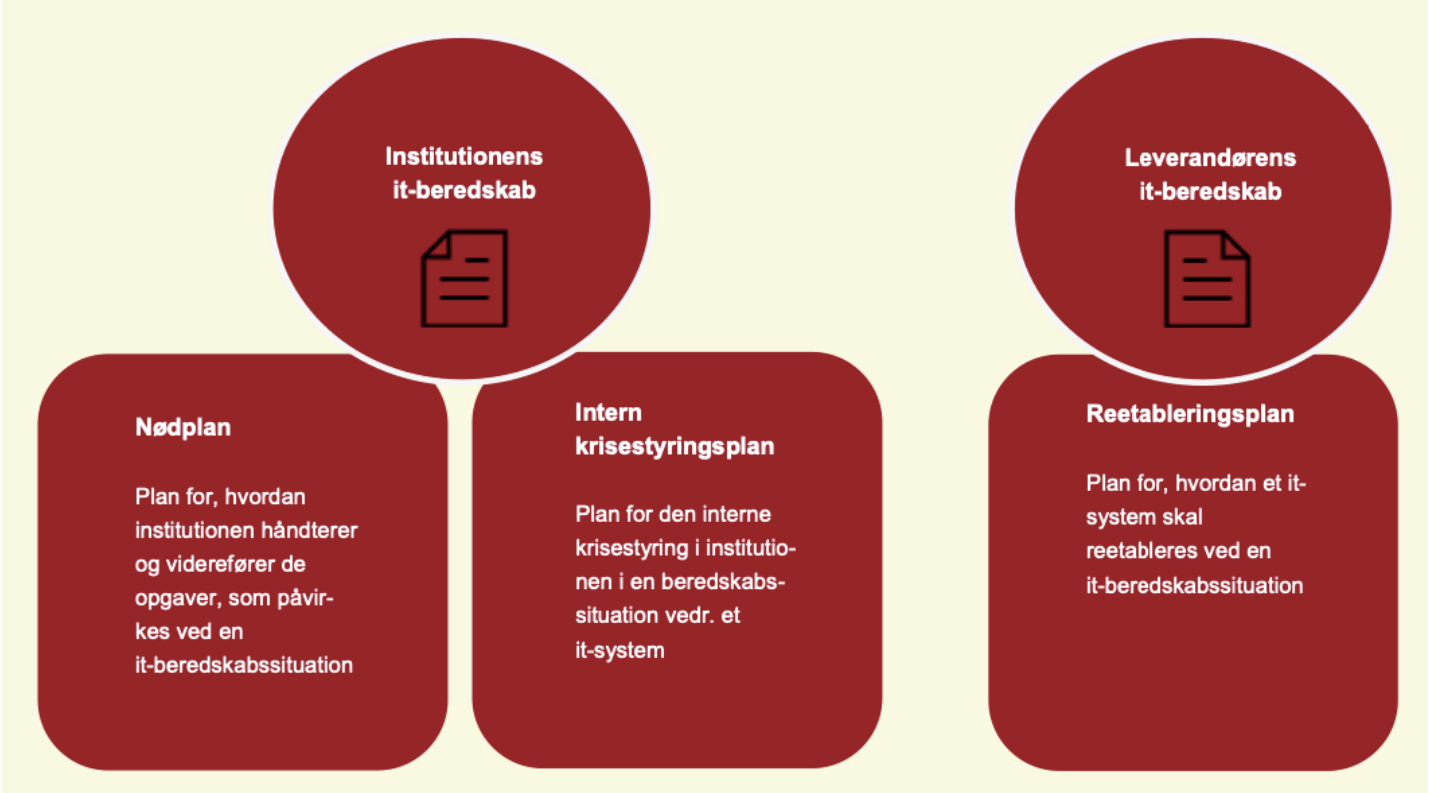
- USB port lås(e).
- Server og PC´er aflåses.
- Tyverisikring generelt.
- Afskaf PC´er på forsvarlig vis ved udskiftning til nyt.

Hardware

- USB port lås(e).
- Server og PC´er aflåses.
- Tyverisikring generelt.
- Afskaf PC´er på forsvarlig vis ved udskiftning til nyt.
- Lad ikke adgangskoder ligge fremme

MAC-PC V/J. ANDERSEN

TEKNISK HJÆLP TIL SMÅ & STORE VIRKSOMHEDER



MAC-PC V/J. ANDERSEN
TEKNISK HJÆLP TIL SMÅ & STORE VIRKSOMHEDER

Guidelines

Informationssikkerhedspolitikker: • Sikkerhedspolitikker skal være tilgængelige for alle medarbejderne • Politikker/retningslinjer skal vedligeholdes	**Operative foranstaltninger:** • Backup foretages, herunder test • Logning, monitorering og softwarekontroller
Organisering af informationssikkerhed: • Roller og ansvar skal være fordelt • Interesseorganisationer skal etableres	**Netværkssikkerhed/håndtering:** • Segmentering af netværk • Anvendelse af sikkerhedsmekanismer på netværket
HR-sikkerhed: • Baggrundstjek ved ansættelse af nye medarbejdere • Korrekt undervisning af medarbejderne i organisationens procedurer (IT-sikkerhed), processer m.fl.	**Systemanskaffelse, udvikling og vedligeholdelse:** • Ændringsprocedurer ved eks. softwareudvikling • Komplet test af softwareopdateringer *inden* udrulning, patching mm.
Håndtering af aktiver: • Overblik over organisationens aktiver • Ejerskab af aktiver defineres	**Leverandørforhold:** • Kontinuerlig revidering af services • Sikkerhedskrav/systemkrav opsættes til den enkelte ønskede service/leverandør
Adgangskontroller: • Adgangskrav/politik skal foreligge • Adgangsstyring/restriktioner/RBAC	**Hændelses håndtering:** • Krav om at alle hændelser indberettes • Læring/udvikling af tidligere hændelser
Kryptering: • Beskyttelse af data via kryptering • Politik for brug af kryptografiske nøgler	**Forretnings kontinuitet:** • Procedurer, poltikker og processer dokumenteres vedvarende • Implementering af test scenarier/øvelser
Fysiske adgange og miljø optimering: • Opsætning af sikkerhedsperimetre ved eks. serverrum • Vedligeholdelse af hardware	**Efterlevelse:** • Dokumentering af efterlevelse af ISO 27001 kravene • Auditere jævnligt

MAC-PC
V/J. ANDERSEN
TEKNISK HJÆLP TIL SMÅ & STORE VIRKSOMHEDER

Evaluering

MAC-PC V/J. ANDERSEN

TEKNISK HJÆLP TIL SMÅ & STORE VIRKSOMHEDER