

Forebyggende IT-sikkerhed

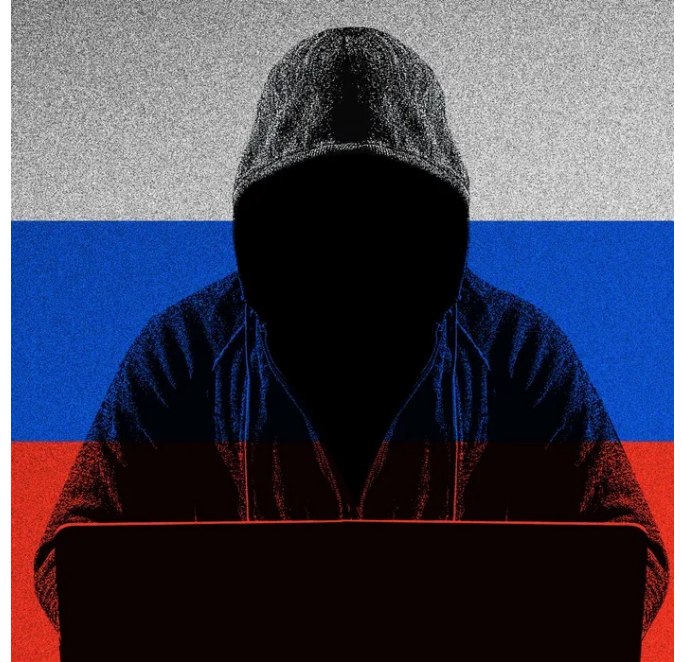


MAC-PC
V/J. ANDERSEN

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.

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”

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>



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 bankkonto 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 bankkonto 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>



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.
- 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](https://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”.

Kilde: [Datatilsynet.dk](https://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.

At sikre sin mail

- Anvend MFA.

At sikre sin mail

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

Kilde: [Hostmaster](#)

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.

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.

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

Wana Decrypt0r 2.0

Ooops, your files have been encrypted! English

What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Payment will be raised on 5/16/2017 00:47:55
Time Left 02:23:57:37

Your files will be lost on 5/20/2017 00:47:55
Time Left 06:23:57:37

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

Send \$300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw Copy

Check Payment Decrypt

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.



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.



Ransomware – forebyggelse

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



MAC-PC
V/J. ANDERSEN

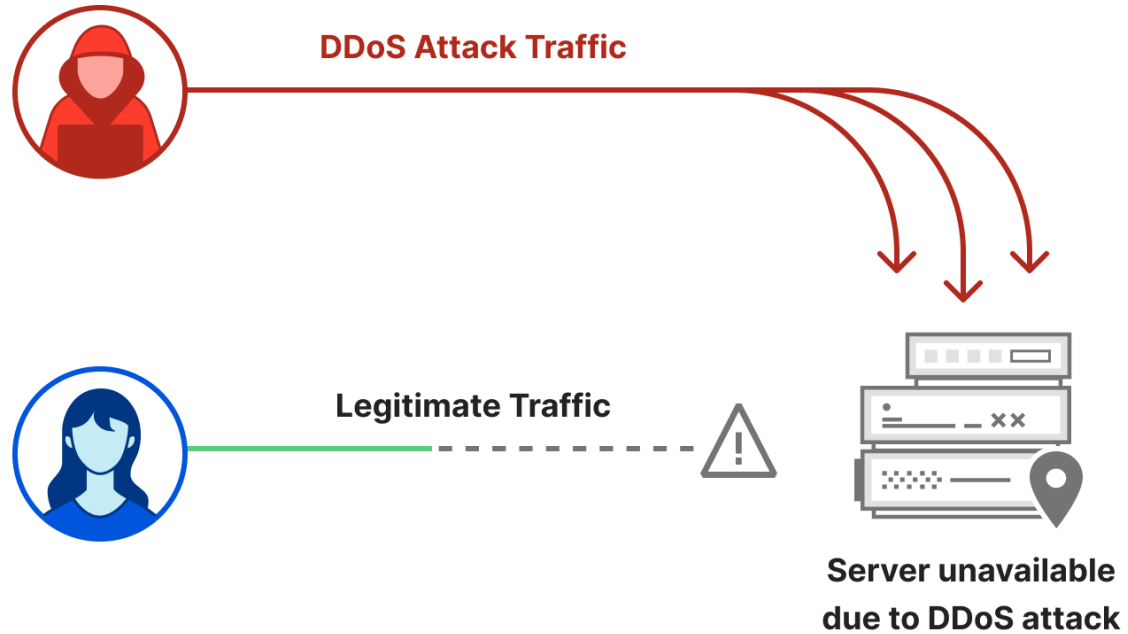
TEKNISK HJÆLP TIL SMÅ & STORE VIRKSOMHEDER

Ransomware – forebyggelse

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



Ddos - hjemmesider



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

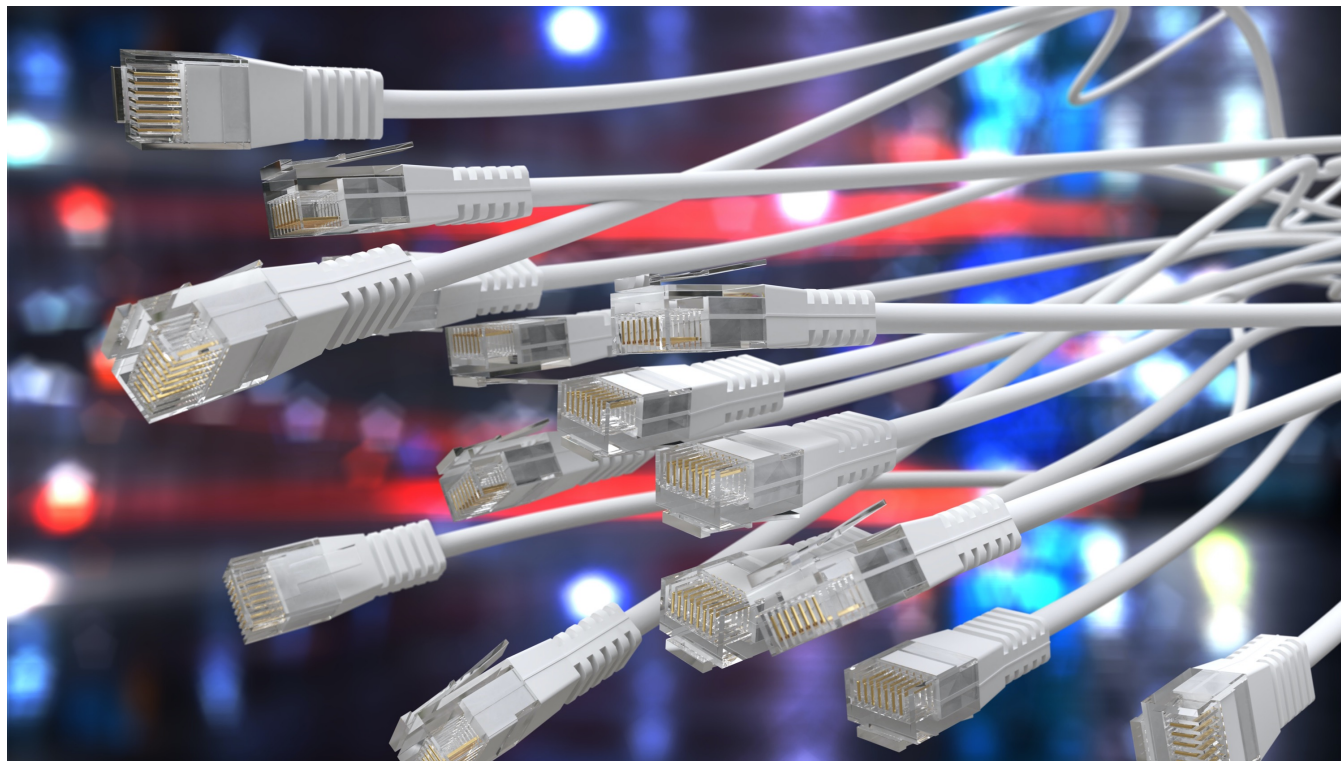
- "Antivirus" installering via udbyder.
- Opdatering af hjemmeside.
- Undgå klik på spam mails / links.
- Geo blokering.
- Backup af hjemmeside.

Ddos - Forebyggelse

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



Netværk



MAC-PC
V/J. ANDERSEN

TEKNISK HJÆLP TIL SMÅ & STORE VIRKSOMHEDER

Netværk

- UPS.



MAC-PC
V/J. ANDERSEN

TEKNISK HJÆLP TIL SMÅ & STORE VIRKSOMHEDER

Netværk

- UPS.
- Redundansløsning via udbyder.



MAC-PC
V/J. ANDERSEN

TEKNISK HJÆLP TIL SMÅ & STORE VIRKSOMHEDER

Netværk

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

Netværk

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



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.
- **VPN.**

Hardware



MAC-PC
V/J. ANDERSEN

TEKNISK HJÆLP TIL SMÅ & STORE VIRKSOMHEDER



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.



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.
- Lad ikke adgangskoder ligge fremme



MAC-PC
V/J. ANDERSEN

TEKNISK HJÆLP TIL SMÅ & STORE VIRKSOMHEDER

Institutionens it-beredskab



Nødplan

Plan for, hvordan institutionen håndterer og viderefører de opgaver, som påvirkes ved en it-beredskabssituation

Intern krisestyringsplan

Plan for den interne krisestyring i institutionen i en beredskabssituation vedr. et it-system

Leverandørens it-beredskab



Reetableringsplan

Plan for, hvordan et it-system skal reetableres ved en it-beredskabssituation

Guidelines

<u>Informationssikkerhedspolitikker:</u> <ul style="list-style-type: none">• Sikkerhedspolitikker skal være tilgængelige for alle medarbejderne• Politikker/retningslinjer skal vedligeholdes	<u>Operative foranstaltninger:</u> <ul style="list-style-type: none">• Backup foretages, herunder test• Logning, monitorering og softwarekontroller
<u>Organisering af informationssikkerhed:</u> <ul style="list-style-type: none">• Roller og ansvar skal være fordelt• Interesseorganisationer skal etableres	<u>Netværkssikkerhed/håndtering:</u> <ul style="list-style-type: none">• Segmentering af netværk• Anvendelse af sikkerhedsmekanismer på netværket
<u>HR-sikkerhed:</u> <ul style="list-style-type: none">• Baggrundstjek ved ansættelse af nye medarbejdere• Korrekt undervisning af medarbejderne i organisationens procedurer (IT-sikkerhed), processer m.fl.	<u>Systemanskaffelse, udvikling og vedligeholdelse:</u> <ul style="list-style-type: none">• Ændringsprocedurer ved eks. softwareudvikling• Komplet test af softwareopdateringer inden udrulning, patching mm.
<u>Håndtering af aktiver:</u> <ul style="list-style-type: none">• Overblik over organisationens aktiver• Ejerskab af aktiver defineres	<u>Leverandørforhold:</u> <ul style="list-style-type: none">• Kontinuerlig revidering af services• Sikkerhedskrav/systemkrav opsættes til den enkelte ønskede service/leverandør
<u>Adgangskontroller:</u> <ul style="list-style-type: none">• Adgangskrav/politik skal foreligge• Adgangsstyring/restriktioner/RBAC	<u>Hændelses håndtering:</u> <ul style="list-style-type: none">• Krav om at alle hændelser indberettes• Læring/udvikling af tidligere hændelser
<u>Kryptering:</u> <ul style="list-style-type: none">• Beskyttelse af data via kryptering• Politik for brug af kryptografiske nøgler	<u>Forretnings kontinuitet:</u> <ul style="list-style-type: none">• Procedurer, politikker og processer dokumenteres vedvarende• Implementering af test scenarier/øvelser
<u>Fysiske adgange og miljø optimering:</u> <ul style="list-style-type: none">• Opsætning af sikkerhedsperimetre ved eks. serverrum• Vedligeholdelse af hardware	<u>Efterlevelse:</u> <ul style="list-style-type: none">• 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

