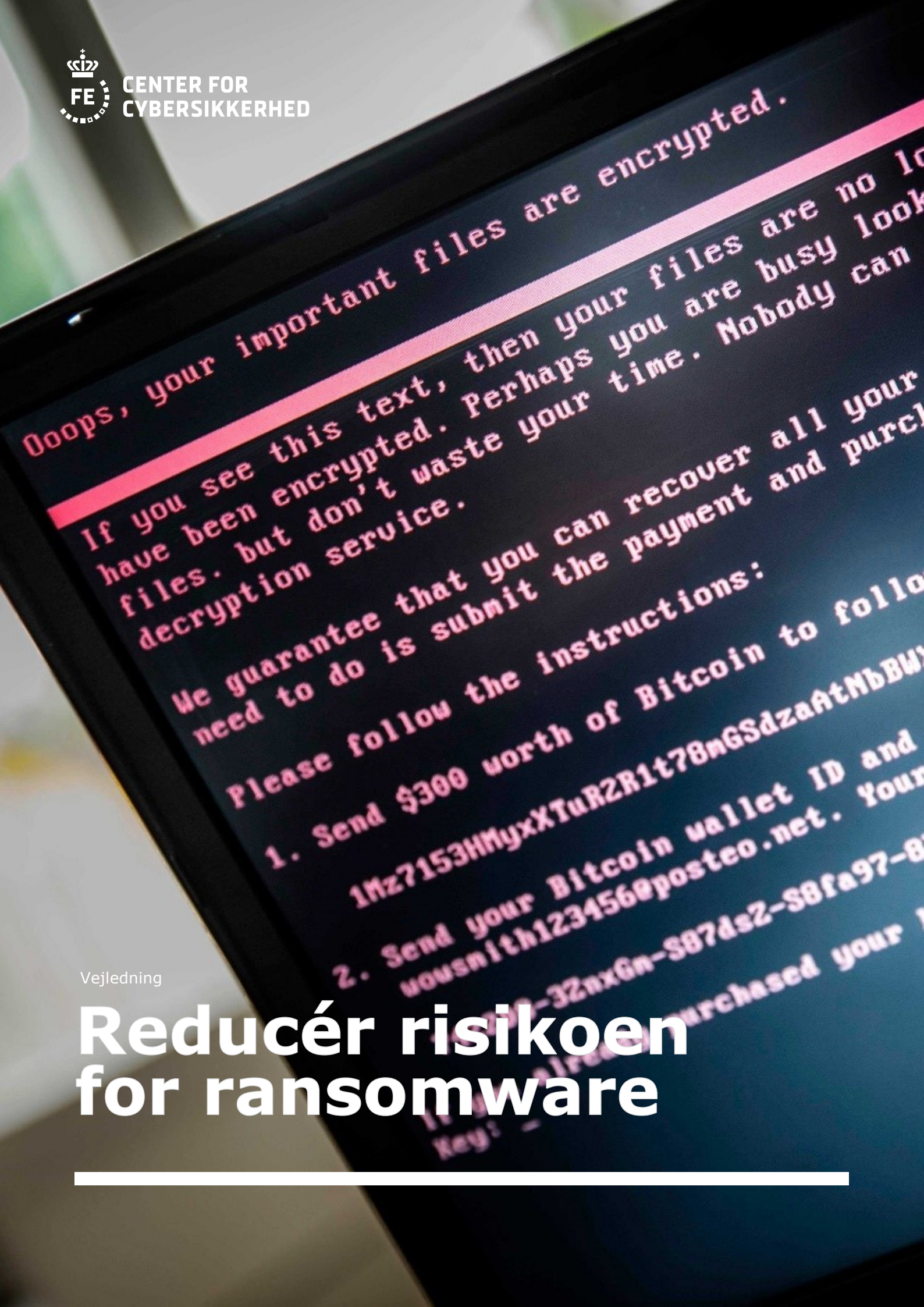
CENTER FOR CYBERSIKKERHED




Vejledning

# Reducér risikoen for ransomware

## Indhold




CENTER FOR CYBERSIKKERHED

Kastellet 30
2100 København Ø
Telefon: + 45 3332 5580
E-mail: cfcs@cfcs.dk



Forsideillustration: Rob Engelaar/EPA/Ritzau Scanpix
2. udgave, april 2023.

# Indledning

Danske virksomheder og myndigheder rammes hyppigt af ransomware-angreb, som gør organisationens data utilgængelige. I værste fald kan sådanne angreb skade driften og påvirke leveringen af samfundsvigtige ydelser.

Ved et ransomware-angreb bliver offerets data og systemer taget som gidsel. De krypteres og bliver dermed utilgængelige for offeret. Ofte kræver angriberen en løsesum, typisk i form af kryptovaluta (eksempelvis Bitcoin), for at give offeret adgang til data igen. Kravet om løsesum følges ofte op med en trussel om, at data vil blive lækket eller videresolgt, hvis løsesummen ikke betales

Det kan være svært at gardere sig imod ransomware. Et effektivt cyberforsvar mindsker dog risikoen for og konsekvenserne af et ransomware-angreb. Vejledningen *Cyberforsvar der virker* (Center for Cybersikkerhed [CFCS] 2021a) er en konkret plan til virksomheder og myndigheder, der vil opbygge et effektivt cyberforsvar.

I denne vejledning gives en række yderligere anbefalinger, som organisationen bør implementere for at reducere risikoen for at blive ramt af ransomware-angreb samt mindske konsekvenserne ved at blive ramt.

Vejledningen henvender sig til organisationens it- og sikkerhedsledelse, it-drifts-afdeling og it-driftsleverandører, som er med til at sikre cyber- og informations-sikkerheden. Anbefalingerne kan indgå i organisationens arbejde med at forbedre eksisterende sikkerhedspraksis.

Hvis en organisation har outsourcet hele eller dele af sin it-drift, kan vejledningen læses som et redskab til den nødvendige dialog med driftsleverandøren. Det er organisationens ansvar at stille krav til leverandører, herunder også til leverandørens imødegåelse og håndtering af ransomware-angreb. Yderligere information kan findes i Center for Cybersikkerheds og Digitaliseringsstyrelsens vejledning om *Cybersikkerhed i leverandørforhold* (2022).

Denne vejledning er opdelt i to afsnit. Første afsnit har fokus på at beskytte organisationen mod ransomware-angreb, mens det andet afsnit handler om, hvordan man håndterer ransomware-angreb.

Ingen af afsnittene eller de enkelte anbefalinger bør stå alene. For at imødegå ransomware-angreb hensigtsmæssigt bør man tage alle anbefalinger i betragtning og beskytte sig med flere forskellige lag af sikkerhed.

**Ransomware-angreb**

Ved ransomware-angreb bliver data og systemer gjort utilgængelige for offeret, ofte ved kryptering, og derved holdt som gidsel. Angriber kræver en løsesum, typisk i form af kryptovaluta, for at give offeret adgang til sine data igen.

Der findes overordnet tre typer af ransomware-angreb:

- Målrettede angreb, som manuelt igangsættes af hackerne, når de har opnået tilstrækkelige rettigheder og indsigt til at forrette stor skade
- Simple angreb, som eksekverer straks ved levering på en maskine
- Angreb, som eksekverer straks ved levering på en maskine og automatisk spreder sig (kryptoorme, som eksempelvis Wannacry)

# Overordnede anbefalinger

På de følgende sider opstiller og uddyber Center for Cybersikkerhed en række anbefalinger, som kan hjælpe organisationen med at reducere risikoen for og ved ransomware-angreb. Anbefalingerne er udtryk for best practice, men kan ikke læses som en udtømmende liste.

Ransomware-angreb bør indgå i organisationens risikovurdering, således at risici er kendt, passende mitigerende tiltag er implementeret, og ansvarsområder er fastlagt, inden angrebet rammer.

**Center for Cybersikkerhed anbefaler, at man:**

- Har styr på den basale it-sikkerhed, herunder opdatering af systemer og applikationer, segmentering af det interne netværk, antivirus, brugerkonti- og adgang samt logning.
- Sikrer fjernadgang med flerfaktor-autentifikation og kryptering.
- Uddanner medarbejderne, så de kan identificere og håndtere mistænkelige mails.
- Beskytter særligt privilegerede konti med ekstra sikkerhed.
- Mindsker brugen af unødig software og begrænser skriverettigheder for brugere og programmer.
- Etablerer aktiv monitorering af netværkstrafik.
- Etablerer logning på alle systemer og services.
- Tager backup af data og konfigurationer, som opbevares separat fra produktionsmiljøet og med en kopi offline, samt tester, at backup kan bruges til reetablering.
- Forbereder organisationen ved at implementere procedurer om ransomware-angreb i beredskabsplaner.

# Hackere bruger forskellige typer ransomware-angreb

Der er en vedvarende trussel fra ransomware-angreb mod danske myndigheder og virksomheder. Måden, hackerne angriber på, har dog ændret sig væsentligt i de seneste år.

Oprindeligt var ransomware-angreb designet til at angribe så mange individuelle computere som muligt, typisk via brede phishing-angreb, som krypterede de enkelte maskiner direkte ved levering. Her bad hackerne om en relativt lille løsesum for en dekrypteringsnøgle.

I de seneste år har hackerne imidlertid i stigende grad vægtet et større udbytte ved det enkelte angreb. Frem for at kryptere så mange som muligt har flere hacker-grupper nu målrettet deres indsats mod virksomheder og myndigheder, som de forventer både kan og vil betale en stor løsesum, hvis deres vitale it-systemer bliver krypterede.

Derudover har konceptet Ransomware-as-a-Service (RaaS) bredt sig. Reelt er der tale om en form for platformsøkonomi til cyberkriminalitet, hvor kriminelle mod betaling kan skaffe sig adgange, værktøjer og infrastruktur, som de bruger i cyberangreb, frem for at udvikle det selv. De cyberkriminelle, der køber og gennemfører ransomware-angreb på denne måde, tjener både penge til sig selv og til de bagmænd, der ejer platformen. Rekruttering til platformene og samarbejdet mellem hackerne sker bl.a. gennem hackerfora på det mørke net (dark web).

Udover at kryptere data og kræve løsepenge truer hackerne ofte med at lække følsomme data, indsamlet fra ofrenes netværk i forbindelse med ransomware-angreb. Det kan dreje sig om kildekode, produktbeskrivelser, finansielle oplysninger, kontrakt-forhold, person- eller kundeoplysninger. Det vil sige oplysninger, der kan skade organisationens funktionsdygtighed, konkurrenceevne, omdømme eller medføre bødestraf, hvis lækket medfører brud på reglerne for håndtering af persondata.

**Ransomware-angreb mod danske virksomheder**

En dansk producent af bl.a. medicoteknisk udstyr blev i september 2019 udsat for et ransomware-angreb, der medførte, at de måtte lukke ned for it-systemer på tværs af virksomheden. Det blev vurderet, at angrebet medførte et tab på op mod 650 mio. kr.

I 2021 blev et dansk selskab i energibranchen ramt af et ransomware-angreb, hvor de, ud over at blive lukket ude af deres systemer, også blev afpresset til at betale for undgå at få deres data lækket. Virksomheden valgte ikke at betale, så den fjendtlige aktør lækkede virksomhedens data. Heriblandt var der blandt andet tekniske produktionstegninger, medarbejderes pas, fakturaer og data om samarbejdspartnere.

En detailkæde blev i 2022 ramt af et ransomware-angreb, som førte til, at alle dets over hundred butikker i Danmark blev midlertidigt lukket, da angrebet låste deres betalingssystemer.

Derudover er danske virksomheder inden for en bred række af forskellige brancher som eksempelvis digital infrastruktur, fødevareforsyning og serviceydelser også blevet ramt af målrettede ransomware-angreb

# Før skaden er sket – beskyt organisationen mod ransomware-angreb

**Hav styr på den basale hygiejne**
Det første skridt for at sikre sig mod at blive ramt af ransomware-angreb er, at få styr på den basale sikkerhedsmæssige hygiejne. Nedenfor foreslås 11 tekniske anbefalinger, som er et godt udgangspunkt, hvis organisationen vil reducere risikoen for ransomware-angreb. Ved at implementere disse mindskes angribernes muligheder for at få adgang til organisationens it-systemer og bevæge sig uset rundt i netværket.

**11 tekniske anbefalinger**

- Opdater operativsystemer og applikationer
- Segmentér netværk, og begræns trafik mellem segmenter
- Beskyt klienter med antivirus og firewall
- Hav styr brugerkonti og rettigheder
- Anvend stærke passwords og flerfaktor-autentifikation
- Tag backup af data og konfigurationer, opbevar en kopi offline og test reetablering
- Etabler logning af ændringer og sikkerhedshændelser
- Beskyt fjernadgang til systemer
- Begræns eller bloker brugen af makroer
- Kryptér data på klienter og mobile enheder samt kommunikationen over andre netværk
- Udarbejd en positivliste over applikationer

Et cyberforsvar i dybden med en række overlappende lag af sikkerhed kan sikre, at organisationen står stærkere i forsvaret mod ransomware-angreb. Et forsvar i dybden betyder, at når et sikringstiltag fejler, står det næste klar til at tage over.
Man skal som organisation altså ikke være nervøs for at dobbeltsikre sig, men derimod se overlappende sikringstiltag som en metode til at holde angriberne ude.
En organisation, som er besværlig at kompromittere og bevæge sig rundt i, bliver et mindre interessant mål for angriberne, som går efter størst mulig gevinst for mindst mulig indsats.

**Hold ransomware uden for døren**
Den indledende kompromittering kan blandt andet foregå ved phishing-mails, udnyttelse af sårbare internetvendte servere, misbrug af stjålne loginoplysninger eller adgang via usikre opsætninger af eksempelvis fjernadgangssystemer.

For at mindske angrebsfladen anbefaler Center for Cybersikkerhed, at organisationen overvejer følgende:

- Opdater løbende software, hardware og firmware samt regler i firewalls. Derved mindskes sandsynligheden for eksempelvis zero-day exploits.

- Indgående e-mails filtreres og sættes i karantæne, hvis de indeholder links eller filer med potentielt skadeligt indhold såsom eksekverbare filer.

- Begræns adgang til kendte malware-sider ved at implementere "sikker DNS" eller proxy-løsninger.

- Fjernadgangsløsninger bør kun tilgå systemer og infrastruktur, som organisationen gennem en risikovurdering ser som acceptable.

- Fjernadgang til organisationens systemer skal altid foregå ved brug af flerfaktor-autentifikation.

- Anvendelse af fjernadgangsløsninger som eksempelvis Remote Desktop Services bør altid foregå igennem VPN eller RDP Gateway.

- Brugerkonti skal låses ud ved gentagne forkerte forsøg på login.

Siden det kun er muligt at mindske angrebsfladen og ikke helt lukke den, bør det også prioriteres højt at uddanne medarbejdere.

Hackerne er blevet meget dygtige og sætter den årvågne medarbejder på prøve, eksempelvis ved at bryde ind i igangværende mailkorrespondance efter at have kompromitteret leverandører eller samarbejdspartnere. Ved brug af social engineering kan hackerne med psykologiske greb opnå offerets tillid og manipulere offeret til at udføre bestemte handlinger. Selv små mistænkelige tegn skal derfor tages alvorligt.

Hackerne vil ofte gå efter personer med særlig indsigt eller privilegerede rettigheder. Der kan derfor med fordel udvikles et udvidet uddannelsesforløb for udvalgte medarbejdere, eksempelvis administratorer, ledelse og sekretariater.

Her anbefaler Center for Cybersikkerhed, at man uddanner medarbejdere i:

- Hvad phishing-mails er, og hvordan de kan skade virksomheden eller myndigheden.
- Hvordan en mistænkelig mail kan identificeres.
- Hvad de skal gøre, hvis de modtager en mistænkelig mail.
- Hvordan de håndterer modtagelse af USB-nøgle, download af software og lignende.
- Hvor de skal henvende sig ved mistanke om hackerangreb.

**Beskyt de indre linjer**
En god sikkerhed inden for organisationens mure mindsker hackernes mulighed for at bevæge sig rundt i netværket og finde de mest kritiske data og it-systemer at kryptere. Med den nuværende tendens, hvor data ofte lækkes i forbindelse med ransomware-angreb, er særlig beskyttelse af organisationens følsomme data blevet endnu mere vigtig end tidligere.

Derfor anbefaler Center for Cybersikkerhed, at følgende bliver overvejet:

- Segmentér netværket, så man eksempelvis ikke kan tilgå kritiske forretningssystemer eller backupmiljøet fra ens gæstenetværk.

- Ved outsourcing af it-drift til en leverandør skal organisationens data og systemer adskilles fra andre kunders.

- Beskyt kritiske data og systemer med flere sikringstiltag, eksempelvis ved at kræve yderligere autentifikation inden adgang og begrænse antallet af konti med skrive-rettigheder.

- Brugerkonti, som ikke længere benyttes, nedlægges straks. Eksempelvis afgående medarbejdere eller eksterne konsulenter.

- Revision af brugeradgange årligt.

- Administrative konti beskyttes med ekstra sikkerhed, fx i form af skærpede krav til passwords og flerfaktor-autentifikation. Brug kun administrative konti, når der skal udføres administrative aktiviteter og aldrig til dagligdags kontoropgaver. Disse konti skal være medarbejder specifikke.

- Lokaladministratorkonti begrænses og skal altid anvende individuelle passwords.

- Skriveadgange reduceres til det behovsbestemte.

- Der benyttes opdateret antivirus på klienter og servere.

- Adgangen til unødvendig software som eksempelvis Powershell eller andre administrationsværktøjer for ikke-administrative brugere fjernes eller blokeres.

- Anvendelsen af indlejret kode som eksempelvis makroer og JS-scripts begrænses eller blokeres.

- Sikker DNS eller proxy løsninger implementeres for at begrænse malwarens mulighed for at kommunikere med angriberne.

- Der fortages hardening af Active Directory (AD).

**Opdag angrebet i tide**
Der kan gå et stykke tid fra angribernes første kompromittering, til det målrettede ransomware-angreb udrulles. Ofte sker den indledende kompromittering med andre typer malware end ransomware, så tegn på malware kan være en del af et ransomware-angreb under opbygning. Derfor er det vigtigt at have redskaberne på plads til at opdage ubudne gæster i dit netværk, inden det er for sent.

Derfor bør følgende anbefalinger overvejes:
- Etabler detaljeret monitorering; særligt med henblik på at opdage og reagere hurtigt på malware. Så kan opdagelsen og reaktionen ske i de indledende skridt inden krypteringen.
- Benyt analyseværktøjer, som hurtigt kan opdage ændringer i trafikmønstre.

**Tag backup**
Et ransomware-angreb krypterer data, konfigurationsfiler med videre. Angrebet kan have været undervejs længe, hvor hackerne har placeret bagdøre i organisationens netværk. Derfor er det vigtigt at forberede sig ved at have flere iterationer af sine backups, der går langt tilbage – op til flere år, alt efter systemet. Så kan man gå tilbage til et punkt, inden bagdøren blev placeret i netværket. Derefter vil man være i stand til at reetablere alle nødvendige informationer samt sikre minimal nedetid og datatab ved tilbagevenden til normaldrift. Her kan organisationens risikovurdering være med til at understøtte ledelsen i valget af prioritering af mitigerende tiltag. Herunder også hvad ekstra tiltag der kan tages til backup af organisationens mest kritiske systemer.

Til backup bør man overveje at:
- Backup opbevares separat fra produktionsmiljøet, og at man har en kopi af backup offline.
- Backup beskyttes med kryptering, password og flerfaktor-autentifikation.
- Der tages regelmæssigt backup, som kan bruges ved reetablering.
- Reetablering af systemer via backups testes regelmæssigt.

For mere sikkerhed kan organisationen overveje uforanderlig lagringsmetoder, såsom 'write once, read many' (WORM). Ydermere bør organisationen opbevare dekrypteringsnøglen til backup separat fra AD og/eller fysisk i en beskyttet lokation.

**Identificer hackerens vej ind**
En del af cyberforsvar i dybden er at være i stand til at identificere, hvad det skete under og inden en given hændelse. Logning er det der gør organisationen i stand til at forbedre sit forsvar efter en hændelse og dermed ikke blive udsat for det samme flere gange. Dette gøres ved, at man logger aktiviteten på ens systemer og servere. Logs kan benyttes til at analysere, hvor og hvordan hackeren har bevæget sig rundt i systemet. Denne information kan så bruges til at identificere, hvilke tiltag der bedst skaber værdi.

Derfor anbefaler Center for Cybersikker, at man:
- Etablerer logning på alle systemer og services

For mere information samt detaljeret vejledning i, hvor man bør logge, kan man se Center for Cybersikkerheds vejledning: *Logning – en del af et godt cyberforsvar* (2023).

# Når skaden er sket – Håndter ransomware-angreb

**Tænk ransomware ind i dit beredskab, inden det går galt**
Uanset hvor godt en organisation beskytter sig mod at blive ramt af ransomware, så er der en risiko for, at et angreb alligevel rammer. At forberede sig på det værst tænkelige kan medvirke til en mere koordineret og effektiv håndtering af ransomware-angrebet og dermed hurtigere tilbagevenden til normaldrift.

I den forbindelse anbefaler Center for Cybersikkerhed, at man overvejer følgende:

- Hvornår kan mistanke om ransomware-angreb aktivere og eskalere beredskabet?
- Er der særlige tiltag og kritiske opgaver, som skal gennemføres straks? Er der systemer, enheder eller lokationer, som skal slukkes eller afkobles fra netværket?
- Er nogle funktioner eller personer, herunder fx eksterne specialister, særligt relevante og nødvendige? Hav afklaret roller på forhånd.
- I hvilken rækkefølge prioriteres reetablering?
- Hvordan håndteres et ransomware-angreb i forskellige faser af beredskabet?
- Hvordan kommunikeres der internt og eksternt?
- Hvilke essentielle dokumenter bør printes og opbevares fysisk?
- Hvordan håndterer organisationens leverandører hændelser og angreb?

**Når organisationen er blevet ramt**
Er organisationen blevet ramt af ransomware-angreb, er det vigtigt ikke at gå i panik, men holde hovedet koldt, så der ikke tages drastiske beslutninger uden overvejelse. Hvis der er udarbejdet en beredskabsplan eller en drejebog for håndtering af ransomware, så følg den.

### *Betaling af løsesum*

Den første indskydelse er måske at give efter for angriberne for hurtigt at komme tilbage til normalsituationen. CFCS anbefaler, at der ikke betales løsesum. Ved at betale løsesum bekræfter man, at ransomware-angreb virker, og at det kan svare sig at udøve kriminalitet. Desuden er der ingen garanti for, at organisationen får de rigtige dekrypteringsnøgler til at låse data op, eller at angriberen reelt forlader it-systemerne, hvilket kan øge risikoen for gentagelse. Hertil kommer, at der kan være juridiske eller omdømmemæssige konsekvenser ved at betale løsesummen.

### *Førstehjælp*

Når angrebet har ramt, skal der handles hurtigt og fornuftigt. Følgende trin er værd at overveje for en organisation under og efter angrebet:

- Isoler alle inficerede enheder ved at afkoble dem fra alle netværk. Det gælder også enheder, der har været forbundet med de inficerede.
- Søg hjælp hos it-sikkerhedseksperter.
- Anmeld angrebet til relevante myndigheder og evt. forsikringsselskab. Vær i den forbindelse opmærksom på eventuelle juridiske forpligtelser. Overvej at informere kunder og samarbejdspartnere, der kan blive påvirket af angrebet. Vær opmærksom på, at CFCS kan ligge inde med konkret teknisk viden, der kan støtte jeres genopbygningsproces.
- Europol har sammen med en række partnere og bidragsydere, heriblandt Rigspolitiet, lavet en hjemmeside om ransomware, hvor organisationer kan finde hjælp til eventuel dekryptering: https://www.nomoreransom.org/da/index.html.
- Skift passwords for alle brugere, herunder administratorer, men vær inden udskiftningen sikker på, at det ikke lukker jer ude af systemer og netværk.
- Identificer hvordan og hvornår angriberen fik adgang til netværket, så angribernes adgang kan fjernes. Der kan eksempelvis være behov for at gennemføre sikkerhedsopdateringer, analysere malware, rette fejlkonfigurationer eller korrigere adgangsstyring. Denne oprydning sikrer, at angriberne ikke umiddelbart kan gentage angrebet.
- Gennemfør kontrolleret reetablering på baggrund af ikke-inficerede backup. Hvis backuppen ikke er fri for malware, kan organisationen under reetableringen blive slået tilbage til start.
    - Foretag komplet geninstallation eller genopbygning af infrastruktur, operativsystemer og applikationer.
    - Start berørte systemer op enkeltvis på et isoleret netværk.
    - Indlæs konfigurationer og data fra backup.
    - Kontrollér de reetablerede data og systemer, kør antivirus, og tag en ny backup inden overførsel til produktionsnetværket.
    - Overvåg netværket for tegn på fortsat inficering af malware.

Det kan være risikabelt at forsøge at rense systemer, da det ikke giver garanti for, at systemet er fri for andre former for malware.

- Del viden og erfaringer fra angrebet med andre organisationer og myndigheder.
- Brug viden fra angrebet til at forbedre organisationens beskyttelse samt processer for backup, overvågning, beredskab mv.

Derudover er der en række relevante sider, som ens organisation kan benytte til eksempelvis at indberette sikkerhedshændelser.

| Relevante ressourcer | Beskrivelse | Adresse |
|---|---|---|
| **Virk.dk** | Her kan organisationer indberette sikkerhedshændelser vedrørende persondata eller væsentlige dele af Danmarks infrastruktur til relevante myndigheder. I nogle tilfælde er organisationen forpligtet til at indberette, mens der i andre tilfælde vil være tale om en frivillig indberetning. | https://virk.dk/myndigheder/stat/ERST/selvbetjening/Indberetning_af_brud_paa_sikkerhed/ |
| **CFCS Situationscenter** | Har din organisation været ramt af en sikkerhedshændelse, kan der være krav om, at du underretter CFCS.<br><br>Du kan også underrette om en sikkerhedshændelse frivilligt. CFCS kan ligge inde med konkret teknisk viden, der kan støtte din organisations genopretning. Ved at orientere CFCS bidrager du også til CFCS' overblik over, hvilke hændelser der rammer Danmark. | https://www.cfcs.dk/da/om-os/indberetning/<br><br>Telefon: +45 3332 5580<br>(spørg efter situationscenteret).<br><br>E-mail: cert@cert.cfcs.dk |
| **Datatilsynet** | Hvis der i forbindelsen med hændelsen har været brud på persondatasikkerheden skal det anmeldes til datatilsynet.<br><br>Anmeldelser foregår via virk.dk | https://www.datatilsynet.dk/sikkerhedsbrud/anmeld-sikkerhedsbrud |
| **No more ransomware** | Er et samarbejde mellem en lang række retshåndhævende myndigheder og it-sikkerheds-firmaer. Her offentliggøres også dekrypteringsnøgle til en lang række forskellige ransomware. | https://www.nomoreransom.org/da/index.html |

# Referencer

Vejledningen er blandt andet udarbejdet med inspiration fra:


Australian Cyber Security Centre. (2021). Securing powershell in the enterprise
https://www.cyber.gov.au/publications/securing-powershell-in-the-enterprise

Canadian Centre for Cyber Security. (2021). Ransomware playbook (ITSM.00.099).
https://www.cyber.gc.ca/en/guidance/ransomware-playbook-itsm00099

Center for Cybersikkerhed. (2019). Trusselsvurdering: Digitale gidseltagere på storvildtjagt.
https://cfcs.dk/da/cybertruslen/trusselsvurderinger/malrettet-ransomware/

Center for Cybersikkerhed. (2020a). Undersøgelsesrapport: Anatomien i målrettede ransomware-angreb.
https://cfcs.dk/da/cybertruslen/rapporter/anatomien-i-ransomware-angreb/

Center for Cybersikkerhed. (2020b). Trusselsvurdering: Hackere misbruger legitime programmer i cyberangreb.
https://cfcs.dk/da/cybertruslen/trusselsvurderinger/legitime-programmer/

Center for Cybersikkerhed. (2020c). Trusselsvurdering: Kriminelle spænder den digitale tommelskrue.
https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/dobbelt-afpresning/

Center for Cybersikkerhed. (2021a). Cyberforsvar der virker.
https://www.cfcs.dk/da/forebyggelse/vejledninger/cyberforsvar-der-virker/

Center for Cybersikkerhed. (2021b). Trusselsvurdering: Fjern adgangen.
https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/fjern-adgangen/

Center for Cybersikkerhed. (2022a). DMARC - Reducér risikoen for falske mails.
https://cfcs.dk/da/forebyggelse/vejledninger/reducer-risikoen-for-falske-mails/

Center for Cybersikkerhed. (2022b). Phishing – Beskyt organisationen mod phishing-mails.
https://www.cfcs.dk/da/forebyggelse/vejledninger/phishing/

Center for Cybersikkerhed og Digitaliseringsstyrelsen. (2022). Cybersikkerhed i leverandørforhold.
https://www.cfcs.dk/da/forebyggelse/vejledninger/informationssikkerhed-i-leverandorforhold/

Center for Cybersikkerhed. (2023). Logning – en del af et godt cyberforsvar.
https://www.cfcs.dk/da/forebyggelse/vejledninger/logning/

Cybersecurity & Infrastructure Security Agency. (2021). Security Tip (ST19-001) – Protecting against ransomware.
https://www.cisa.gov/uscert/ncas/tips/ST19-001

Cybersecurity & Infrastructure Security Agency. (u.å.). Stop *Ransomware*
https://www.cisa.gov/stopransomware

Europol. (2021). No More Ransom.
https://www.nomoreransom.org/da/index.html

National Cyber Security Centre. (2021). Mitigating malware and ransomware attacks.
https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

UC Berkeley. (u.å.). Securing remote desktop (RDP) for system administrators.
Securing Remote Desktop (RDP) for System Administrators