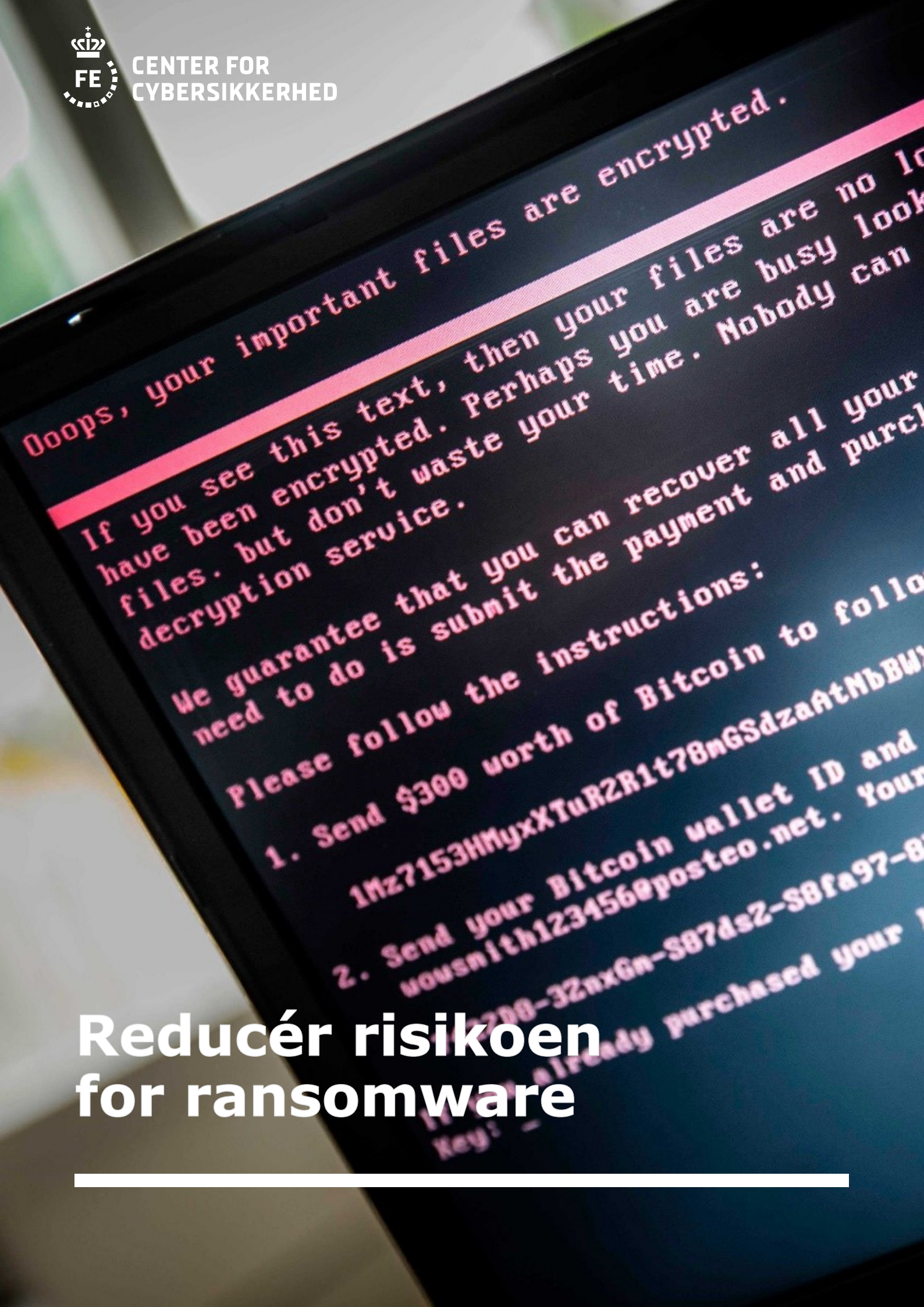
CENTER FOR CYBERSIKKERHED



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
1. udgave oktober 2020.

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 holdt som gidsel, da de krypteres og derved bliver utilgængelige for offeret. Angriberen kræver en løsesum, typisk i form af kryptovaluta (fx Bitcoin), for at give offeret adgang til sine data igen.

Det kan være svært at gardere sig 100 % imod ransomware. Et effektivt cyberforsvar mindsker dog sandsynligheden for og konsekvenserne af et ransomware-angreb.

Vejledningen *Cyberforsvar der virker* er en konkret plan til virksomheder og myndigheder, der vil opbygge et effektivt cyberforsvar.

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

Vejledningen henvender sig til organisationers IT- og sikkerhedsledelse, IT-driftsafdeling og IT-driftsleverandører, som er med til at sikre cyber- og informationssikkerheden. Anbefalingerne kan indgå i organisationers arbejde med at forbedre eksisterende sikkerhedspraksis.

Hvis en organisation har outsourcet hele eller dele af sin IT-drift, kan vejledningen også bruges i dialogen med leverandører for at sikre sig, at leverandøren har implementeret de rette sikkerhedstiltag for at imødegå ransomware.

Ransomware-angreb
Der findes overordnet tre typer af ransomware-angreb:

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

Læsevejledning
Denne vejledning er opdelt i to afsnit. Første afsnit har fokus på at beskytte organisationen mod ransomware-angreb, mens andet afsnit omhandler håndtering af ransomware-angreb.

Det er vigtigt at bemærke, at hverken hovedafsnittene 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 sikkerhed.

God læselyst.

Sammenfatning

På de følgende sider opstiller og uddyber Center for Cybersikkerhed en række anbefalinger, som kan hjælpe organisationer med at reducere risikoen for og ved ransomware-angreb. Anbefalingerne kan anses for best practice, men er ikke en udtømmende liste over alle relevante tiltag for den enkelte organisation.

Ransomware-angreb bør indgå i organisationens risikovurdering, så risiko er kendt, passende mitigerende tiltag er implementeret og ansvarsområder er fastlagt, inden angrebet rammer. Hvis en organisation har vurderet, at risikoen for og ved ransomware skal håndteres, anbefaler Center for Cybersikkerhed, at man som minimum:

- Har styr på den basale IT-sikkerhed, herunder opdatering af systemer og applikationer, segmentering af det interne netværk, antivirus, brugerkonti- og adgang og logning
- Sikrer fjernadgang med fler-faktor autentifikation og kryptering
- Uddanner medarbejderne, så de kan identificere og håndtere mistænkelige mails mv.
- Beskytter særligt privilegerede konti med ekstra sikkerhed
- Mindsker brugen af unødig software og begrænser skriverettigheder for brugere og programmer
- Etablerer aktiv overvågning af netværkstrafik
- Tager backup af data og konfigurationer, som opbevares separat fra produktionsmiljøet og med en kopi offline. Test også, 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 ville kryptere de enkelte maskiner direkte ved levering. Her bad hackerne om en relativt lille løsesum for en dekrypteringsnøgle.

Den første ændring skete i 2017, hvor WannaCry krypterede tusindvis af computere verden over i løbet af få dage. Som noget nyt var WannaCry en såkaldt kryptoorm, der var designet til at sprede sig automatisk ved at udnytte en sårbarhed, når først den var blevet leveret til én computer. Pludselig kunne organisationer se hele netværk blive krypteret på én gang, hvis blot én enkelt computer blev inficeret med ransomware.

I de seneste par 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 hackergrupper 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.

Senest er hackerne begyndt også at true med at lække følsomme data indsamlet fra ofrenes netværk i forbindelse med ransomware-angrebene, hvis offeret ikke betaler løsesummen. Dermed risikerer offeret ikke kun at miste tilgængeligheden af sine systemer, men også at følsomme oplysninger offentliggøres.

Konsekvenserne ved et målrettet ransomware-angreb kan være meget alvorlige for den ramte virksomhed eller myndighed. Ransomware-angreb kan også få alvorlige konsekvenser for samfundsvigtige funktioner, hvis de bliver ramt.

Ransomware-angreb mod danske virksomheder

Den danske producent af bl.a. høreapparater, Demant, blev i september 2019 udsat for et ransomware-angreb, der medførte, at virksomheden lukkede ned for it-systemer på tværs af virksomheden. Demant vurderer, at angrebet medførte et tab på op mod 650 mio. kr.

Distributionsselskabet NRGi blev i 2015 udsat for et målrettet ransomware-angreb, der påvirkede virksomhedens forretningssystemer i væsentlig grad. Cyberkriminelle havde ikke adgang til kritiske netværk, men angrebet påvirkede administrative netværk.

GlobalConnect, ISS, Danish Agro og Desmi er også eksempler på danske virksomheder, der er blevet ramt af målrettede ransomware-angreb i de seneste år.

Læs eventuelt mere om truslen fra målrettede ransomware-angreb på CFCS' hjemmeside. Her findes også en dybdegående rapport, som beskriver de ti faser, som hackerne gennemgår undervejs i et målrettet 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 beskrives 10 tekniske tiltag, 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.

10 tekniske tiltag

- Opdater operativsystemer og applikationer
- Segmenter netværk og begræns trafik mellem segmenter
- Beskyt klienter med antivirus og firewall
- Styr brugerkonti og rettigheder
- Anvend sikre passwords og flerfaktorautentifikation
- Tag back-up af data og konfigurationer og test reetablering
- Etabler logning af ændringer og sikkerhedshændelser
- Beskyt fjernadgang til systemer
- Krypter 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 sikringstiltag 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

Hackerne kan opnå adgang til virksomheden eller myndigheden på flere måder. Den indledende kompromittering foregår typisk med phishing-mails[1], udnyttelse af sårbare internetvendte servere eller adgang via usikre Remote Desktop Services opsætninger eller andre fjernadgangssystemer. For at mindske angrebsfladen, bør følgende tiltag overvejes.

- Opdater løbende antivirus og anvend korrekte regler i firewalls. Det bør overvejes, om indgående e-mails skal filtreres og sættes i karantæne, hvis de indeholder links eller filer med potentielt skadeligt indhold såsom eksekverbare filer

- Opdater altid software, hardware og firmware, når nye versioner eller sikkerhedsopdateringer frigives. Hackerne glemmer ikke, og bruger ofte gamle sårbarheder til at kompromittere offeret. Lav derfor hurtigst muligt en plan for opdatering af usikre enheder og programmer. Overvej også at gennemføre sårbarhedsscanninger med fast frekvens. For mindre virksomheder, som bruger standardudstyr og software, kan automatiske opdateringer overvejes

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

- Fjernadgang til organisationens systemer bør altid foregå ved brug af to-faktor autentifikation

- Anvendelse af fjernadgangsløsninger som fx Remote Desktop Services[2] bør altid foregå ved brug af VPN eller RDP Gateway. Brugere bør altid bruge stærke passwords og autentificere sig ved brug af flerfaktor autentifikation, ligesom gentagne forsøg på adgang med forkerte passwords bør låse brugeren ude.

Medarbejderne kan fungere som et første bolværk mod angreb, hvis de ved, hvad de skal gøre, når de fx modtager en mistænkelig mail eller tilgår inficerede hjemmesider. Uddannelse af medarbejdere bør prioriteres højt.

[1] DMARC kan sikre, at en organisations eget domæne ikke kan misbruges til at sende phishing-mails, jf. vejledningen Reducer risikoen for falske mails
[2] Yderligere information om sikkerhed i RDP: Securing Remote Desktop (RDP) for System Administrators.

Alle medarbejdere bør vide:

- Hvad phishing-mails er, og hvordan det 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-sticks, download af software og lignende
- Hvor de skal henvende sig ved mistanke om hackerangreb (fx efter at have klikket på et link eller vedhæftning eller efter besøg på mistænkelig hjemmeside)

Hackerne er blevet meget dygtige og sætter den årvågne medarbejder på prøve, fx ved at bryde ind i igangværende mailkorrespondance efter at have kompromitteret leverandører eller samarbejdsparter. 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, fx administratorer, ledelse og sekretariater.

Beskyt de indre linjer

En god sikkerhed inden for organisationens mure, gør livet surt for hackerne, som vil bevæge sig rundt i netværket for at finde de mest kritiske data og it-systemer at kryptere. Med den nye tendens, hvor data lækkes i forbindelse med ransomware-angreb er særlig beskyttelse af organisationens følsomme data om muligt blevet endnu mere vigtig end tidligere.

- Placer kritiske forretningssystemer- og data i sikrede segmenter uden direkte adgang fra internettet. Placer backup systemer separat.

- 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, fx ved at kræve yderligere autentifikation inden adgang og begræns antallet af konti med skrive-rettigheder.

- Brugerkonti, som ikke længere benyttes, nedlægges straks (fx afgående medarbejdere, eksterne konsulenter mv.)

- Privilegerede konti beskyttes med ekstra sikkerhed, fx i form af skærpede krav til passwords og to-faktor autentifikation. Brug kun privilegerede konti, når der skal udføres privilegerede aktiviteter og aldrig til dagligdags kontoropgaver

- Lokaladministratorkonti begrænses og anvender altid individuelle passwords

- Skriveadgang til fællesdrev mv. reduceres til det funktionelt nødvendige
- Hav opdateret antivirus på klienter og relevante servere

- Fjern eller blokér adgangen til unødvendig software, fx Powershell[3] eller andre administrationsværktøjer[4], hvis der ikke er et konkret behov

- Begræns eller blokér anvendelsen af indlejret kode, fx makro'er og JS-scripts

- Husk, at også ikke ondsindede programmer kan gøre brug af disse funktionaliteter

- Begræns malwarens mulighed for at kommunikere med angriberne ved at implementere sikker DNS eller proxy løsninger

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.

- Etabler detaljeret overvågning; særligt med henblik på at opdage og reagere hurtigt på malware, fx Trickbot, Emotet og Dridex, som ofte anvendes ved den indledende kompromittering

- Reager straks på alarmer, der kan være tegn på inficering med malware

- Overvej brugen af analyseværktøjer, som kan opdage ændringer i trafikmønstre hurtigt. De kan fx være baseret på AI/ML algoritmer (Artificial intelligence og Machine Learning)

[3] Yderligere information om sikkerhed i Powershell:
https://www.cyber.gov.au/publications/securing-powershell-in-the-enterprise
[4] Læs mere om misbrug af legitime programmer i trusselsvurderingen Hackere misbruger legitime programmer

Tag backup
Et ransomware-angreb krypterer data, konfigurationsfiler mv. Angrebet kan have været undervejs længe, hvor hackerne har placeret bagdøre i organisationens netværk. Derfor er det vigtigt at forberede sig ved at have en brugbar backup af alle nødvendige informationer, som kan sikre minimal nedetid og datatab ved tilbagevenden til normaldrift.

- Opbevar backup separat fra produktionsmiljøet og hav en kopi af backup offline
- Beskyt backup med kryptering, password og to-faktor autentifikation
- Overvej en backup løsning, som tilbyder uforanderlig lagring, fx WORM (write once – read many) lagring, hvor den enkelte kopi ikke kan ændres eller slettes og dermed heller ikke krypteres. Der vil oftest være tale om cloud-baserede løsninger, der kan tilbyde denne type uforanderlig lagring separeret fra organisationens produktionsmiljø
- Pas på med at bruge cloud services med automatisk synkronisering (fx Dropbox og Google drev) som eneste backup løsning, da synkronisering samtidig med eller lige efter ransomware-angrebet vil gøre organisationens backups ubrugelige
- Test regelmæssigt, at backup kan bruges ved reetablering
- Kontrollér løbende, at backup ikke er inficeret med malware.

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 forbindelse med organisationens beredskabsplanlægning kan følgende spørgsmål med fordel overvejes:

- 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 internt og eksternt?
- Hvilke essentielle dokumenter bør printes og opbevares fysisk?
- Hvordan håndterer organisationens leverandører hændelser og angreb?

Er organisationen blevet ramt?

Er organisationen blevet ramt af ransomware-angreb, så er det vigtigt ikke at gå i panik, men at 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. 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. Sluk eventuelt enheder og netværksforbindelser

- Søg hjælp hos sikkerhedseksperter

- 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

- Anmeld angrebet til relevante myndigheder og evt. forsikringsselskab. Vær i den forbindelse opmærksom på eventuelle juridiske forpligtelser. Overvej at informere kunder og samarbejdspartner, der kan blive påvirket af angrebet

- Skift passwords for alle brugere, herunder administratorer, men vær inden udskiftningen sikker på, at det ikke lukker jer ude af systemer og netværk

- Identificer årsagen til angrebet, så de udnyttede sårbarheder kan fjernes. Der kan fx være behov for at gennemføre sikkerhedsopdateringer, 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 backupen ikke er fri for malware eller ransomware, 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
    - Kontroller 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.

På virk.dk[5] 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[6]. Viden fra indberetninger om sikkerhedshændelser understøtter Center for Cybersikkerheds opgave med at bidrage til et mere sikkert digitalt Danmark.

[5] https://virk.dk/myndigheder/stat/ERST/selvbetjening/Indberetning_af_brud_paa_sikkerhed/
[6] Læs mere om forskellige underretningsordninger på cfcs.dk (https://cfcs.dk/da/om-os/indberetning/). Vær yderligere opmærksom på Datatilsynets regler for anmeldelse i tilfælde af brud på persondatasikkerheden.

Referencer

Vejledningen er blandt andet udarbejdet med inspiration fra:

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

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

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

Center for Cybersikkerhed (2017): *Reducér risikoen for falske mails*
https://cfcs.dk/da/forebyggelse/vejledninger/reducer-risikoen-for-falske-mails/

The United States Department of Justice: *How to protect your networks from ransomware*
https://www.justice.gov/criminal-ccips/file/872771/download

Europol m.fl.: *No More Ransom*
https://www.nomoreransom.org/da/index.html

National Cyber Security Centre (2020): *Mitigating malware and ransomware attacks*
https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

Cybersecurity & Infrastructure Security Agency: *Ransomware*
https://www.us-cert.gov/security-publications/Ransomware

Cybersecurity & Infrastructure Security Agency: *Security Tip (ST19-001) – Protecting against ransomware*
https://www.us-cert.gov/ncas/tips/ST19-001

UC Berkeley: *Securing remote desktop (RDP) for system administrators*
Securing Remote Desktop (RDP) for System Administrators

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