CENTER FOR CYBERSIKKERHED

Reducér risikoen for ransomware

Center for Cybersikkerhed

Maj 2016

CENTER FOR CYBERSIKKERHED

Indledning

Center for Cybersikkerhed bliver løbende opmærksom på stadigt flere danske virksomheder, myndigheder og privatpersoner, der bliver ramt af cyberangreb i form af den særlige type malware, kaldet ransomware, som gør ofrets data utilgængelige.

Et ransomware-angreb foregår typisk ved, at målets it-system inficeres med malware som følge af, at ofret i god tro har åbnet vedhæftede filer eller links sendt med ond hensigt i en mail. Malwaren krypterer herefter alt indholdet på ofrets harddisk og de drev, der er skriveadgang til. Når krypteringen er fuldført, vil ofret typisk blive mødt med en besked fra angriberne, som lover at dekryptere ofrets data mod en løsesum – deraf navnet ransomware.

En ny og meget bekymrende udvikling er fremkomsten af nye typer af ransomware, der retter sig mod sårbarheder på servere, som er tilgængelige fra internettet. Denne form for ransomware kræver ikke en aktiv handling fra en brugers side. Det er især virksomheder, der rammes, og konsekvenserne for dem kan potentielt være meget alvorlige.

Det kan være svært at gardere sig 100 % imod infektioner med ransomware. Men efterlevelse af Top 4-sikringstiltagene fra vejledningen "Cyberforsvar der virker" vil reducere risikoen betragtelig for, at organisationen bliver ramt.

Top 4-sikringstiltagene fra publikationen "Cyberforsvar der virker":

- Opdatér programmer, fx. Adobe Reader, Microsoft Office, Flash Player og Java med seneste sikkerhedsopdateringer, højrisiko inden for to dage.
- Opdatér operativsystemet med seneste sikkerhedsopdateringer, højrisiko inden for to dage. Undgå Windows XP eller tidligere versioner.
- Begræns antallet af brugerkonti med domæne- eller lokaladministratorprivilegier. Disse brugere bør anvende separate uprivilegerede konti til e-mail og websurfing.
- Udarbejd positivliste over applikationer af godkendte programmer for at forhindre kørsel af ondsindet eller uønsket software.

Anbefalinger til øvrige forebyggende tiltag

I betragtning af den store potentielle skadevirkning ved ransomware anbefaler Center for Cybersikkerhed, at følgende initiativer også overvejes grundigt og afvejes i forhold til risiko, konsekvens og funktionelle behov. Det skal fremgå, hvem der har ansvaret for udførelsen af de nedenstående initiativer, der iværksættes, herunder hvem der har bemyndigelse til at lukke et netværk:

- Systematisk sikkerhedskopiering af alle kritiske informationer, centrale konfigurationsfiler og andre opsætningsdata er absolut påkrævet. Udvælgelsen af informationer skal ske på baggrund af en forretnings- og ledelsesgodkendt plan.
- Backup-rutinen gennemføres med høj frekvens.
- Systematisk og løbende kontrol af at sikkerhedskopieringen fungerer efter hensigten.
- Alle medarbejdere holdes løbende orienteret/undervises om sikkerhedsmæssige forhold og risici, herunder om risikoen ved at åbne mails indeholdende vedhæftede filer.
- Løbende og hurtig opdatering af programmer og biblioteker på serverinfrastrukturen med henblik på at minimere risikoen for, at malware udnytter kendte sårbarheder.
- Anvendelse af en bred og ofte opdateret virus-beskyttelse på alle systemer. Ransomware videreudvikles ofte indenfor få timer for at omgå virusbeskyttelse.
- Anvend application-whitelisting på servere som supplement til virusbeskyttelsen.
- Filtrér indgående e-mails, som bliver sat i karantæne, hvis de indeholder links eller filer med potentielt skadeligt indhold, for eksempel eksekverbare filer såsom .exe og komprimerede filer såsom .zip.
- Behovet for medarbejderes skriveadgang til fællesdrev reduceres til det funktionelt nødvendige.
- Segmentér om muligt placeringen af kritiske forretningsdata, så disse ikke er placeret på samme drev/server som organisationens e-mail miljø.
- Iværksæt tiltag, der sikrer en betryggende anvendelse af Microsoft Office-filer med indlejrede macro'er, evt. at blokere for anvendelsen af macro'er.
- Overvej at deaktivere mulighederne for afvikling af JScript-filer på Microsoft Windows systemer. Overvejelserne skal tage højde for, at Ikke-ondsindede programmer kan anvende denne type filer.

Anbefalinger, hvis skaden er sket

Hvis din organisation er blevet ramt af et ransomware-angreb, bør denne strukturerede guide følges:

Inddrag de rette personer

- Inddrag straks topledelsen, bemyndigede medarbejdere og de rette tekniske kompetencer, herunder specialister udefra, hvis organisationen ikke selv råder over den fornødne viden.

Stands ulykken

- Etablér et hurtigt overblik over hvilke systemer og data, der er ramt. Især er det vigtigt at fastslå, hvornår det er sket.
- Som følge af de potentielle konsekvenser anbefaler Center for Cybersikkerhed, at man straks slukker eller isolerer alle ramte systemer. Hvis der er tvivl, er det bedre at stoppe et system for meget end et for lidt.

Iværksæt om nødvendigt nøddrift

- Gå ud fra, at nulstilling og reetablering af systemerne er tidskrævende.
- Informér organisationen om situationen og etablér om nødvendigt nøddrift for kritiske systemer.

Reetablering

- De berørte systemer startes op enkeltvis på et isoleret netværk.
- Foretag en komplet reinstallation af det specifikke system (operativsystemer og applikationer).
- Indlæs konfigurationer og data fra sikkerhedskopier, der med sikkerhed er blevet gennemført, før systemet blev inficeret.
- Kontrollér de reetablerede systemer og data og tag en ny sikkerhedskopi.
- Overfør det reetablerede system til produktionsnetværket.

Opfølgning og læring

- Dokumentér alle de data, der måtte være gået tabt.
- Udarbejd en strategi for, hvordan tabet af data håndteres.
- Udarbejd eller opdatér om nødvendigt organisationens politik og retningslinjer for, hvordan medarbejdere skal forholde sig til e-mails med vedhæftede filer og sørg for, at det ofte kommunikeres ud i organisationen.
- Vurdér på baggrund af den aktuelle hændelse, om den etablerede plan for sikkerhedskopiering lever op til forventningerne. Indarbejd og implementér om nødvendigt eventuelle reviderede krav.
- Gennemfør periodiske reetableringsøvelser, hvor et eller flere systemer reetableres på baggrund af gemte sikkerhedskopier.

Tillæg til vejledningen Reducer risikoen for ransomware

December 2019

I forbindelse med stigningen i tilfælde af Ransomware finder Center for Cybersikkerhed det formålstjenligt at tilføje følgende til listen over forbyggende tiltag:

- Der bør altid anvendes to-faktor-autentifikation ved ekstern adgang til organisations it-systemer.
- Fjern eller bloker unødvendig software på bruger pc'er f.eks. powershell, hvis der ikke er et konkret behov.
- Der bør anvendes individueller password til lokal-administratorkonti på organisationens it-systemer. Brugeres lokaladministratorrettigheder bør begrænses.
- Segmenteringen skal tage særlig hensyn til placeringen af backup systemer.
- Der bør altid findes offline kopi af backup.
- Der bør etableres detaljeret overvågning, der sikrer, at organisationen bliver opmærksom på uønsket aktivitet, særlig med henblik på detektering af malware.
- Der bør udarbejdes en forretnings- og ledelsesgodkendt beredskabsplan, for hvordan man vil begrænse konsekvensen af et ransomware-angreb.
- Medarbejdere skal vide, hvad de skal gøre i tilfælde af mistanke om, at de har modtaget en mistænkelig mail eller har klikket på et "uheldigt" link.