Til den it-sikkerhedsansvarlige

Varsel: Forebyggelse af ransomware kræver opmærksomhed på brugerkonti

Dato: 18. juni 2021

Forsvarets Efterretningstjeneste
Kastellet 30
2100 København Ø

Tlf.: 33 32 55 80
E-mail: cfcs@cfcs.dk
www.cfcs.dk

Center for Cybersikkerhed har observeret adskillige ransomware-angreb inden for den seneste tid. CFCS' vurderer, at lækkede passwords fra tidligere administratorer og konsulenter m.fl. kan have været en medvirkende årsag til at organisationerne har kunnet kompromitteres.

Anbefaling

Center for Cybersikkerhed anbefaler, at man etablerer og følger en fast procedure for håndtering af bruger- og administratorkonti. Proceduren skal sikre, at alle konti gennemgås periodisk med henblik på at afdække om de stemmer overens med de faktiske behov. Desuden skal eventuelle afvigelser håndteres. Ansvaret for at processen følges bør forankres hos udpegede nøglepersoner i organisationen. Processen bør samtidig sikre, at konti øjeblikkeligt spærres ved afgang af såvel medarbejdere som konsulenter m.fl.

Desuden anbefaler Center for Cybersikkerhed:

- At der anvendes multifaktor autentifikation (MFA) på alle systemer med fjernadgang (herunder webmail, mobilmail, VPN osv.).
- At der anvendes multifaktor autentifikation (MFA) på privilegerede konti herunder administratorer.
- At alle standardpasswords i systemer og software ændres inden disse sættes i produktion.
- At anvendelsen af passwords i organisationen i øvrigt efterlever de retningslinjer, der er givet i CFCS' vejledning "Passwordsikkerhed".
- At passwords til kritiske komponenter ændres, hvis en medarbejder med adgang til disse komponenter forlader organisationen.

Rådgivning

Center for Cybersikkerhed kan i nogle tilfælde bistå med rådgivning om cyber- og informationssikkerhed, herunder styring af informationssikkerhed og risikovurderinger. Center for Cybersikkerheds rådgivning tager som udgangspunkt afsæt i de vejledninger, der kan findes på centerets hjemmeside.

Vejledning

Center for Cybersikkerhed har udarbejdet en række vejledninger om cyber- informationssikkerhed, herunder "Cyberforsvar der virker", som er en konkret og prioriteret plan til at komme i gang med cyber- og

informationssikkerhedsarbejdet. Alle vejledninger kan findes på centerets hjemmeside og kan frit benyttes.

Kontakt
Hvis du har spørgsmål til overstående varsel eller ønsker at høre mere om mulighederne for rådgivning, er du velkommen til at kontakte Center for Cybersikkerhed på enten telefon 33 32 55 80 eller på mail cert@cert.cfcs.dk.

Om Center for Cybersikkerhed
Center for Cybersikkerhed under Forsvarets Efterretningstjeneste har som hovedopgave at understøtte et højt informationssikkerhedsniveau i den informations- og kommunikationsteknologiske infrastruktur, som samfundsvigtige funktioner er afhængige af.

Denne opgave løses blandt andet ved, at Center for Cybersikkerheds Netsikkerhedstjeneste opdager, analyserer og bidrager til at imødegå avancerede cyberangreb mod myndigheder og virksomheder, der er beskæftiget med samfundsvigtige funktioner.

Om TLP-markeringen
Dette dokument er markeret med Traffic Light Protocol (TLP), som er defineret af den internationale it-sikkerhedsorganisation FIRST. Denne markering fortæller dig som modtager, hvordan eller hvorvidt indholdet af dokumentet kan deles ud fra, hvor følsomme informationerne er.

Det er alene Center for Cybersikkerhed som afsender, der kan afgøre dette efter en konkret vurdering af, hvor stor skade en offentliggørelse af informationerne ville medføre. Derfor er det vigtigt, at du som modtager forstår og respekterer den TLP-markering, som vi har angivet.

Definitioner af TLP
TLP-skalaen er opdelt i fire niveauer, som både i navn og farvekode indikerer, hvor følsomme informationerne er, og hvordan de må anvendes af dig som modtager. Det er vigtigt at understrege, at restriktionerne for deling både gælder det markerede dokument samt anden mundtlig og skriftlig omtale af indholdet. Niveauerne er defineret herunder:

TLP:RED = må ikke deles med andre, udelukkende forbeholdt modtager(e).
TLP:RED vælges, når afsender vurderer, at informationen ikke har relevans for andre end de udvalgte modtagere, og at et muligt misbrug af informationerne kan påvirke en parts privatlivspolitik, omdømme eller operationer. Modtagere må ikke dele oplysninger markeret med TLP:RED med andre uden for kredsen af specifikke modtagere eller med andre uden for mødet eller samtalen, hvori oplysningerne oprindeligt blev delt. I forbindelse med eksempelvis afholdte møder må oplysninger markeret med TLP kun deles med mødedeltagerne. I de fleste tilfælde bør TLP:RED deles mundligt eller personligt.

TLP:AMBER = begrænset deling, kan deles internt i egne organisationer.
TLP:AMBER vælges, når afsender vurderer, at modtager er nødt til at involvere andre for at kunne reagere hensigtsmæssigt på indholdet, selv om det muligvis vil kunne påvirke privatlivspolitikker, omdømme og operationer, hvis det deles bredt med andre end de involverede organisationer. Modtagere må kun dele oplysninger markeret med TLP:AMBER med organisationsmedlemmer eller med kunder eller klienter, der er nødt til at kende indholdet for at kunne beskytte sig selv eller forhindre yderligere skade. **Afsender kan frit fastsætte yderligere begrænsninger på de oplysninger, der må deles. Disse begrænsninger skal overholdes.**

TLP:GREEN = begrænset deling, kan deles med andre inden for egen sektor og branche.
TLP-GREEN vælges, når afsender vurderer, at informationen har relevans i forhold til kendskabet om et område, der vedrører egne organisationer såvel som samarbejdspartnere inden for branchen eller sektoren. Modtager må dele oplysninger markeret med TLP:GREEN med egne organisationer og samarbejdspartnere inden for egen sektor eller branche, men ikke gennem offentligt tilgængelige kommunikationskanaler. Information i denne kategori kan deles bredt inden for en

bestemt branche. TLP:GREEN må ikke deles uden for branchen/egen sektor.

TLP:WHITE = ingen begrænsninger på deling.
TLP:WHITE kan vælges, når afsender vurderer, at der er minimal eller ingen risiko for misbrug af informationerne i henhold til gældende regler og procedurer for offentliggørelse. Informationer markeret med TLP:WHITE kan frit distribueres, hvis de er i overensstemmelse med reglerne for ophavsret.

Kilde: https://www.first.org/tlp