CENTER FOR
CYBERSIKKERHED

5. juli 2016

Vejledning til underretningsunderordning i tilfælde af cyberangreb

Formålet med denne vejledning er at sikre effektiv underretning vedrørende cyberangreb på samfundsvigtige funktioner. Vejledningen er rettet mod statslige myndigheder, kommuner og regioner samt private virksomheder, der varetager opgaver, der er vigtige for samfundets opretholdelse. Statslige myndigheder har de sidste to år været forpligtet til at underrette Center for Cybersikkerhed i tilfælde af større it-sikkerhedsmæssige hændelser i deres digitale infrastruktur, og i den gældende fællesoffentlige digitaliseringsstrategi er det aftalt, at kommuner og regioner også skal underrette Center for Cybersikkerhed, mens det er en frivillig ordning for private virksomheder.

Pr. 1. juli 2016 træder lov om net- og informationssikkerhed i kraft og vil blandt andet indebære at oplysninger fra både offentlige myndigheder og private virksomheder, der modtages som led i underretningsordningen, i deres helhed automatisk er undtaget fra aktindsigt.

I den forbindelse opfordrer Center for Cybersikkerhed særligt private virksomheder til at underrette om større it-sikkerhedsmæssige hændelser i den digitale infrastruktur, som virksomhederne er ansvarlige for, særligt inden for – men ikke udelukkende – hos følgende sektorer:

- It- og Telesektoren*)
- Finanssektoren
- Energi- og Forsyningssektoren
- Leverandører til Forsvaret
- Transportsektoren

Det bemærkes, at denne frivillige underretning ikke erstatter andre former for indberetninger eller orienteringer, som virksomheden er forpligtet til i medfør af andre aftaler eller lovgivning. *) For telesektoren er nærværende underretningsordning et frivilligt supplement til den obligatoriske ordning, der gælder i medfør af lovgivningen på net- og informationssikkerhedsområdet.

Underretninger fra myndigheder og private virksomheder sætter Center for Cybersikkerhed i stand til at varsle hurtigere og bedre om trusler. Endvidere vil underretningerne styrke grundlaget for både centerets trusselsvurderinger og for centerets rådgivning til myndigheder og virksomheder om risici og passende sikkerhedstiltag. I denne vejledning kan virksomheder såvel som offentlige myndigheder læse om, hvilke angreb Center for Cybersikkerhed gerne vil underrettes om, samt hvordan en underretning helt konkret finder sted.

Siden den 1. september 2014 har alle statslige myndigheder været forpligtet til at underrette Center for Cybersikkerhed ved større it-sikkerhedsmæssige hændelser i den digitale infrastruktur. Kommuner og regioner har siden maj 2016 ligeledes været forpligtet til at underrette, som beskrevet i den nye fællesoffentlige digitaliseringsstrategi 2016-2020.

Hvilke cyberangreb bør Center for Cybersikkerhed underrettes om?

Myndigheden eller virksomheden bør underrette Center for Cybersikkerhed, når et af nedenstående kriterier er opfyldt, uanset om hændelsen har haft konsekvens for myndigheden eller virksomhedens forretning:

- Uautoriseret adgang til interne netværk fra internettet.
- Modtagelse af formodede eller erkendte spear-phishing mails såvel som rene phishing mails.
- Infektion med malware[1].
- Alle DDoS-angreb mod samfundsvigtige services.
- At der på internettet er fundet virksomhedsfølsomme data fra interne netværk.
- Angreb mod industrielle kontrolsystemer (SCADA).
- Angreb mod særligt kommunikationsudstyr, for eksempel videokonference og overvågningsudstyr.
- Angreb mod teleinfrastrukturen i mobilnet, fastnet og internettet.

Hvordan underrettes Center for Cybersikkerhed?

Kontakt Center for Cybersikkerheds netsikkerhedstjeneste pr. e-mail til underretning@cfcs.dk. Er der tale om en alvorlig og igangværende hændelse, hvor der ønskes hjælp fra centret, så ring til vagttelefonen på 32 89 89 89. Følsom information kan beskyttes ved at fremsende underretningen med PGP-krypteret e-mail. Nøglen kan findes her:
http://pgp.mit.edu/pks/lookup?op=get&search=0x53130FA6D5578465

Ved kontakt til Center for Cybersikkerhed bedes virksomheden eller myndigheden udfylde vedlagte skema.

Hvad sker der med informationerne i Center for Cybersikkerhed?

Når Center for Cybersikkerhed - via underretning eller på anden vis - erfarer, at en myndighed eller virksomhed er mål for et særlig avanceret cyberangreb, vil centeret kontakte den pågældende myndighed eller virksomhed. I den forbindelse vil Center for Cybersikkerhed eventuelt kunne tilbyde bistand, men formen og omfanget af Center for Cybersikkerheds bistand afhæn-

[1] Rapportering om sager med forsøg på phishing mails og forsøg på infektion med almindelig malware kan være omfangsrigt for virksomheder og myndigheder. Center for Cybersikkerhed søger i disse tilfælde blot underretning om omfang (antal modtaget pr. uge/måned afhængigt af omfang) og tendenser (stigning, uændret, faldende), vedlagt et enkelt eksempel på pågældende phishing mail og/eller malware-kampagne.

ger af den konkrete situation. Gængse angreb forventes håndteret af virksomheden selv. Såfremt Center for Cybersikkerhed bistår en myndighed eller virksomhed, vil det skulle aftales nærmere, hvorledes informationerne fra en cybersikkerhedshændelse kan anvendes. I forhold til underretning fra private virksomheder, vil det ske i form af en skriftlig samtykkeerklæring mellem virksomheden og Center for Cybersikkerhed. Informationer, der modtages som led i underretningsordningen og i forbindelse med Center for Cybersikkerheds bistand til myndigheder og virksomheder, vil alene blive videregivet til tredjemand, hvis myndigheden eller virksomheden konkret har givet samtykke til en sådan videregivelse.

Udover at anvende underretningerne som en del af udgangspunktet for Center for Cybersikkerheds varslinger, kan Center for Cybersikkerhed anvende informationen – i anonymiseret form – i de generelle og sektorspecifikke trusselsvurderinger, som centeret løbende udarbejder, såvel som med henblik på generel rådgivning. Hertil kommer, at informationerne – ligeledes i anonymiseret form – vil kunne anvendes i de strategiske og tekniske samarbejdsfora, som centeret er vært for, og hvor der orienteres om konkrete trusler for virksomheder og myndigheder.

De oplysninger om cyberangreb, som Center for Cybersikkerhed modtager, behandles i henhold til Forsvarets Efterretningstjenestes restriktive sikkerhedsbestemmelser om fysisk sikkerhed, personelsikkerhed og it-sikkerhed. Alle medarbejdere i Center for Cybersikkerhed er sikkerhedsgodkendt til klassifikationsgraden HEMMELIGT eller derover, og alle medarbejdere har tavshedspligt i henhold til straffeloven. Centerets brug af indberettede oplysninger vil således også internt blive håndteret med diskretion og anonymitet.

Tilsynet med Efterretningstjenesterne, der er en uafhængig myndighed, fører tilsyn med Center for Cybersikkerheds behandling af personoplysninger.