FORSVARSMINISTERIET
DANISH MINISTRY OF DEFENCE

30. maj 2014

NOTAT

om

definitionen af "sikkerhedshændelse" i lovforslaget om Center for Cybersikkerhed (L 192)

1. Begrebet "sikkerhedshændelse" er et centralt element i forslaget til lov om Center for Cybersikkerhed. Det følger således af lovforslaget, at Center for Cybersikkerhed kun må foretage analyse af data, der stammer fra de tilsluttede civile myndigheder og virksomheder, hvis der er tale om en sikkerhedshændelse. Endvidere må alene data, der er knyttet til en sikkerhedshændelse, videregives efter lovens særlige videregivelsesbestemmelse, ligesom der gælder særlige regler for sletning af data, der er knyttet til en sikkerhedshændelse.

Når ordet "cyberangreb" anvendes i bemærkningerne til lovforslaget, sker dette i samme betydning som det mere tekniske begreb "sikkerhedshændelse", der anvendes i lovteksten. Sagt med andre ord er en sikkerhedshændelse et cyberangreb eller en trussel herom.

Center for Cybersikkerhed indsamler i dag primært data ved hjælp af elektroniske alarmenheder, som er opsat hos de frivilligt tilsluttede myndigheder og virksomheder, hvor de monitorerer ind- og udgående internetkommunikation.

Monitoreringen giver et normalbillede af internetkommunikationen og dermed også det overblik, der er nødvendigt for at opdage afvigelser. Cyberangreb (sikkerhedshændelser) vil typisk optræde som afvigelser fra normalbilledet og udløse en alarm hos centerets netsikkerhedstjeneste.

Netsikkerhedstjenesten foretager således allerede i dag en automatiseret (altså maskinel) løbende monitorering af internettrafikken for at se, om den indeholder trusler mod it-sikkerheden. Det sker faktisk mange, mange tusinde gange om dagen, at der udløses en alarm. Det er imidlertid i gennemsnit ganske få gange i døgnet, at en alarm har en så alvorlig karakter, at den fører til, at en analytiker i centeret foretager en nærmere analyse, fordi der er en begrundet mistanke om en sikkerhedshændelse, og fordi analysen er nødvendig

HOLMENS KANAL 42
1060 KØBENHAVN K
TELEFON: 33 92 33 20
TELEFAX: 33 32 06 55
MAIL: FMN@FMN.DK
WEB: www.FMN.DK
CVR: 25-77-56-35
EAN: 5798000201200

for afklaring af forhold vedrørende hændelsen. Der skal således foreligge konkrete indikationer på et cyberangreb eller en trussel herom, før der kan foretages en analyse af data.

Analysen har alene til formål at klarlægge konkrete sikkerhedshændelsers karakter, og netsikkerhedstjenestens interesse er derfor kun rettet mod tekniske oplysninger om sikkerhedshændelserne, f.eks. analyse af en virus i en fil, der er vedhæftet en e-mail, og ikke mod selve indholdet af kommunikationen, herunder personoplysninger.

Når en analyse er gennemført, logges den, og Tilsynet med Efterretningstjenesterne vil kunne kontrollere, at betingelserne for analysen i det enkelte tilfælde har været opfyldt. Derudover fører centerets ledelse og centerets jurister løbende kontrol med, at analyserne foretages i overensstemmelse med reglerne.

Tilsynets årlige redegørelse skal indeholde oplysninger om antallet af sager med relation til sikkerhedshændelser, der er behandlet i centeret. Den årlige redegørelse skal herudover indeholde en anonymiseret beskrivelse af et eller flere konkrete cyberangreb, og der skal være en statistik over, hvor mange gange analytikere fra centeret har foretaget analyse af data.

Hvad der skal forstås ved en sikkerhedshændelse, er nærmere uddybet og illustreret nedenfor i pkt. 2-5.

2. I lovforslaget er en sikkerhedshændelse defineret således:

> **§ 2.** I denne lov forstås ved:
> 1) Sikkerhedshændelse: En hændelse, der negativt påvirker eller vurderes at ville kunne påvirke tilgængelighed, integritet eller fortrolighed af data, informationssystemer, digitale netværk eller digitale tjenester.

Denne definition svarer til definitionen i den gældende GovCERT-lov (lov nr. 596 af 14. juni 2011), der blev enstemmigt vedtaget af Folketinget, og denne afgrænsning af begrebet sikkerhedshændelse har dermed dannet grundlag for netsikkerhedstjenestens arbejde i knap 3 år.

Det fremgår således af bemærkningerne til lovforslagets § 2, stk. nr. 1, at definitionen af sikkerhedshændelse er en videreførsel af definitionen fra GovCERT-lovens § 3, nr. 3, med en sproglig præcisering af, at sikkerhedshændelser er hændelser med en negativ påvirkning af tilgængelighed, integritet eller fortrolighed af data, informationssystemer, digitale net-

værk eller digitale tjenester. Det præciseres endvidere, at begrebet sikkerhedshændelse omfatter hændelser, der vurderes at ville kunne have den beskrevne påvirkning.

Definitionen indebærer, at enhver unormal situation, der potentielt kan kompromittere informationssystemer, digitale netværk, digitale tjenester eller andre elektroniske systemer eller data, der lagres, processeres eller transmitteres af disse systemer, vil være at betragte som en sikkerhedshændelse.

Desuden præciseres det, at begrebet omfatter data, informationssystemer, digitale netværk og digitale tjenester, således at det udtrykkeligt fremgår, at også hændelser, som rammer lukkede netværk (netværk, der ikke er forbundet til internettet), kan have karakter af sikkerhedshændelser.

Et eksempel på en sikkerhedshændelse, der negativt påvirker tilgængeligheden af en digital tjeneste, er et overbelastningsangreb (denial-of-service angreb), hvor f.eks. en hjemmeside rammes af et stort antal forespørgsler, så brugere ikke kan få adgang til hjemmesiden. En sikkerhedshændelse, der negativt påvirker integriteten af såvel data som et informationssystem, kan eksempelvis være indtrængen i en database, hvor oplysninger ændres uden databaseejerens vidende. En sikkerhedshændelse, der negativt påvirker fortroligheden af et informationssystem, kan være en såkaldt »trojansk hest«, hvor der installeres et program på en myndigheds informationssystem, som muliggør uautoriseret kopiering af data fra myndigheden.

3. I et spørgsmål fra Forsvarsudvalget blev forsvarsministeren anmodet om at yde teknisk bistand til et ændringsforslag, således at definitionen af sikkerhedshændelser svarer til Beredskabsstyrelsens definition.

Besvarelsen af spørgsmålet lyder således:

"Et forslag til ændring af definitionen af sikkerhedshændelse som anført i spørgsmålet vil f.eks. kunne affattes således:

"Sikkerhedshændelse: Elektroniske angreb rettet mod informations- og kommunikationsteknologi, herunder computere, servere, netværk og tjenester, som er forbundet direkte eller indirekte til internettet, med det formål at skade eller ødelægge informations- og kommunikationsteknologi, tilegne sig kontrol over styringen af informations- og kommunikationsteknologi eller uretmæssigt at få adgang til data lagret på informations- og kommunikationsteknologi."

Indledningsvist bemærkes det, at Beredskabsstyrelsen ikke opererer med en egentlig definition af begrebet sikkerhedshændelse. Beredskabsstyrelsen har imidlertid i Nationalt Risikobillede af 9. april 2013 beskrevet en række karakteristika ved cyberangreb, og disse er anvendt ved affattelsen af ændringsforslaget.

Ændringsforslaget indebærer, at begrebet sikkerhedshændelser defineres mere snævert, således at begrebet alene omfatter angreb på informations- og kommunikationssystemer, men ikke trusler om sådanne angreb. Dette vil have som konsekvens, at Center for Cybersikkerhed i medfør af lovforslagets § 3, stk. 1, alene vil have til opgave at opdage, analysere og bidrage til at imødegå deciderede angreb. Centeret vil dermed i mindre grad få mulighed for at foretage forebyggende arbejde ved at opdage, analysere og bidrage til at imødegå trusler med henblik på at hindre angreb. Det kan endvidere være vanskeligt at fastslå, hvornår en hændelse kan karakteriseres som et angreb.

Herudover indebærer ændringsforslaget, at en sikkerhedshændelse defineres som angreb på informations- og kommunikationsteknologi, som er forbundet direkte eller indirekte til internettet. Dette vil f.eks. have som konsekvens, at en hændelse, hvor et netværk, der ikke er forbundet til internettet, ødelægges af en virus introduceret via en USB-nøgle, ikke kan karakteriseres som en sikkerhedshændelse. Som eksempel på netværk, der ikke er forbundet til internettet, kan nævnes netværk, der anvendes til klassificeret kommunikation.

Den foreslåede definition vurderes endvidere at være vanskelig at benytte i praksis. Det vil således som udgangspunkt være vanskeligt at påvise det subjektive element, som følger af den foreslåede bestemmelse. En typisk sag i det nuværende GovCERT starter i dag ved, at der opstår en computergenereret alarm i sensornetværket. Det kan eksempelvis ske, hvis der i en tilsluttet myndigheds internetkommunikation ses indikatorer på kommunikation fra en ip-adresse, som er kendt for at sende malware. Grundlaget for at analysere data er således, at der er en formodning for, at der i den pågældende internetkommunikation findes malware, og at det udgør en trussel. Det kan dog ikke uden en nærmere analyse af internetkommunikationen konstateres, om der rent faktisk er tale om malware og endnu mindre, om en eventuel malware har til formål at skade eller ødelægge informations- og kommunikationsteknologi, tilegne sig kontrol over styringen af informations- og kommunikationsteknologi eller uretmæssigt at få adgang til data lagret på informations- og kommunikationsteknologi.

På denne baggrund kan jeg ikke støtte et sådant ændringsforslag."

4. På retsudvalgets høring den 8. maj 2014 om lovforslaget foreslog DANSK IT følgende definition af en sikkerhedshændelse:

"Cyberangreb (sikkerhedshændelsen) er elektroniske angreb rettet mod informations- og kommunikationsteknologi (IKT) herunder computere, servere, netværk, tjenester, som er forbundet direkte eller indirekte til Internettet, med den hensigt at skade eller ødelægge IKT, tilegne sig kontrol over styringen af IKT eller uretmæssigt at få adgang til data lagret på IKT, med det formål at underminere tilgængeligheden, integriteten og tilliden til det ramte eller tilsigtet IKT og/eller at tilegne/forvanske/ødelægge sensitive data."

Som det fremgår, svarer første del af DANSK IT's forslag, dvs. indtil ordene "… *med det formål at underminere* …", til ovennævnte ændringsforslag, og denne del af definitionen er dermed kommenteret ovenfor under pkt. 3.

Med hensyn til anden del af Dansk-It's definition, dvs. "… *med det formål at underminere tilgængeligheden, integriteten og tilliden til det ramte eller tilsigtet IKT og/eller at tilegne/forvanske/ødelægge sensitive data*", svarer denne del af definitionen reelt (med elementer fra lovforslaget) til første del af definitionen, og dermed er første og anden del sammenfaldende. Sagt med andre ord, så siges det samme to gange.

5. Om antallet af sikkerhedshændelser kan oplyses, at netsikkerhedstjenesten (GovCERT) siden 2010 har registreret godt 1.100 sikkerhedshændelser. Heraf vurderes en fjerdedel at være alvorlige. Det er således – som nævnt ovenfor i pkt. 1 – i gennemsnit kun ganske få gange om dagen, at en alarm fører til en nærmere analyse af data.

De registrerede hændelser omfatter overbelastningsangreb og spor efter APT-angreb, fund af sårbarheder, tegn på infektion med vira og fund af forskellige typer malware (crimeware, botnet-malware mv.).

I perioden september 2011 til udgangen af marts 2014 har netsikkerhedstjenesten (GovCERT) udsendt godt 100 varslinger til GovCERT's kundekreds. Tallet omfatter generelle varslinger til en bredere kreds og specifikke varslinger til enkeltkunder på baggrund af en alarm.