CENTER FOR CYBERSIKKERHED

Center for Cybersikkerhed: Cybertruslen mod kritisk infrastruktur

November 2013

CENTER FOR CYBERSIKKERHED

5. november 2013

Trusselvurdering: Cybertruslen mod kritisk infrastruktur

Formålet med trusselvurderingen er at orientere om cybertruslen mod kritisk infrastruktur fra statslige og ikke-statslige aktører.

Hovedvurdering

Forsvarets Efterretningstjenestes Center for Cybersikkerhed vurderer, at kritisk infrastruktur i Danmark er et potentielt vigtigt strategisk mål for fremmede stater og ikke-statslige aktører. Dette vil ikke mindst være tilfældet i en konflikt mellem en stat med en udviklet cyberkapacitet og Danmark, eller en koalition af stater, hvor Danmark deltager. Antallet af angrebsmål vil stige i takt med, at flere og flere styrings- og kontrolkomponenter i infrastrukturen opkobles til internettet. Flere stater vil på kort til mellemlangt sigt tage højde for mulighederne for at angribe kritisk infrastruktur i deres planlægning af militære operationer.

Det er sandsynligt, at statslige aktører kortlægger dansk kritisk infrastruktur som led i deres cyberspionage, men det er ikke sandsynligt, at de statslige aktører vil udføre et målrettet angreb på dansk kritisk infrastruktur på kort til mellemlangt sigt. Denne vurdering kan dog ændres i tilfælde af en politisk eller militær krise, hvor Danmark deltager aktivt i en koalition rettet mod disse stater eller mod parter, som disse stater støtter.

Ikke-statslige grupperinger viser interesse for at angribe kritisk infrastruktur, men har ikke de fornødne tekniske kapaciteter til at udføre avancerede angreb. Det er sandsynligt, at kriminelle aktører med mere avancerede kapaciteter på mellemlangt sigt vil udleje deres kapaciteter til aktører, der har til hensigt at udføre angreb mod dansk kritisk infrastruktur.

Detaljeret redegørelse

Kritisk infrastruktur understøtter samfundsvigtige funktioner inden for energi-, transport-, forsynings-, finans- og kommunikationsområdet samt funktioner, som har stor økonomisk betydning for samfundet. Den såkaldte supply chain-trussel, hvor der allerede i produktionen af hard- og software er indbygget malware eller teknisk styrbare komponenter, som en ondsindet aktør kan aktivere ved hjælp af internettet, er behandlet i Center for Cybersikkerheds trusselsvurdering fra januar 2013 og uddybes ikke yderligere i denne trusselsvurdering.

Der er store økonomiske gevinster ved at forbinde kritisk infrastruktur til internettet. Derfor tænkes dette ind i udviklingen af komponenterne til infrastrukturen. Det betyder, at der i de vestlige lande, herunder Danmark, vil ske en stigning i omfanget af kritisk infrastruktur, der bliver forbundet til internettet. Udrulningen af Smart Grid systemer på el-nettet er et eksempel på denne udvikling.

Smart Grid systemer

Smart Grid er betegnelsen for den teknologi, der skal drive næste generation af el-nettet. En hjørnesten i systemet er, at en betydelig del af komponenterne i el-nettet bliver netværksforbundet. Det gælder komponenter i produktionen, transmissionen, distributionen, hos kunden og serviceudbydere samt ved driften og overvågningen af el-nettet.

I takt med at flere kontrol- og styringskomponenter i kritisk infrastruktur bliver forbundet til internettet, stiger risiciene for kompromittering. Sårbarhederne opstår, fordi kontrol- og styringskomponenter ofte ikke har tidssvarende eller tilstrækkelige sikkerhedsmekanismer indbygget.

Dansk kritisk infrastruktur udgør et strategisk mål for fremmede stater og ikke-statslige grupperinger. Det gælder både i forhold til indhentning af intellektuel ejendom, der kan støtte en stats økonomiske målsætning, og som mål, der kan gøres utilgængeligt under en politisk eller militær konflikt.

Hvordan angribes systemerne i kritisk infrastruktur?

Systemer i kritisk infrastruktur adskiller sig i kompleksitet og sårbarhed. Størrelsen og kompleksiteten af infrastrukturen afgør, hvilke kapaciteter der er nødvendige for, at en aktør vil kunne opnå en ønsket effekt ved et angreb. I mange tilfælde vil det være svært at forudsige effekten af et angreb.

Ved større og komplekse systemer skal flere komponenter typisk fejle, før et angreb får en ønsket effekt. Den oftest manglende standardisering af de kontrolsystemer, der eksempelvis styrer elnettet, gør, at eventuelle angreb i høj grad skal være målrettet mod enkeltsystemerne. Det kræver flere stykker højt specialiseret, kompliceret og skadeligt software – såkaldt malware – for at anrette fysisk skade. En fjendtlig aktør skal derfor bruge tid og ressourcer på rekognoscering af målet og udvikling af malware.

Derfor er det primært de særligt teknisk dygtige aktører, herunder stater, der på kort til mellemlangt sigt vil kunne udgøre en trussel mod kritisk infrastruktur i Danmark. Den igangværende standardisering af komponenter i kritisk infrastruktur kan dog ændre denne vurdering.

Den stigende standardisering har medført nye værktøjer til kortlægning af internetforbundne enheder. Et eksempel er søgemaskinen Shodan, der gør det muligt for aktører med begrænsede tekniske kundskaber at finde systemer forbundet til internettet. Et eksempel på sådanne systemer er overvågningskameraer, som er tilknyttet internettet.

Systemerne bliver yderligere sårbare, fordi mange ejere af infrastruktur ikke er opmærksomme på behovet for at opdatere styresystemerne i komponenterne. Kendte sårbarheder bliver derfor meget lette at udnytte. Værktøjer som eksempelvis Shodan gør det muligt for en angriber at søge efter en specifik komponent med en bestemt version af et kendt styresystem. Ligeledes er der eksempler på, at ejere af infrastruktur ikke ændrer standardpasswords eller anvender svage passwords. Dermed opnår en angriber hurtigt adgang.

Statslige aktører

I udlandet findes flere eksempler på, at statslige aktører ofte undersøger og kortlægger industrisystemerne i kritisk infrastruktur. Det sker som led i operationer, hvor det egentlige mål er at stjæle intellektuel ejendom.

Resultatet fra et såkaldt honeypot-forsøg med kritisk infrastruktur bekræfter flere statslige aktørers interesse for industrisystemer.

Det er sandsynligt, at angreb på kritisk infrastruktur vil indgå som en del af en række statslige aktørers militære operationer i tilfælde af en militær konflikt mellem stormagterne.

Ikke-statslige aktører

En række ikke-statslige aktører, herunder al-Qaida, har udtrykt interesse for at gennemføre

Honeypot-forsøg

Et it-sikkerhedsfirma byggede en model af et typisk computersystem, der styrede et større industrianlæg. Modellen blev forbundet til internettet samtidig med, at firmaet monitorerede al trafik til og fra modellen. På den måde kunne firmaet analysere indkommende angreb i et kontrolleret miljø.

angreb mod kritisk infrastruktur. Det er dog ikke sandsynligt, at terrorister på kort til mellemlangt sigt vil være i stand til at udføre skadelige cyberangreb mod kritisk infrastruktur.

Aktører med begrænset teknisk indsigt bruger allerede i dag de tekniske kapaciteter, som kriminelle stiller til rådighed på internettet, til at udføre simple angreb. Angrebene kan dog stadig skabe forstyrrelser i adgangen til offentlige services i Danmark. Et eksempel på dette er overbelastningsangrebet på NemID i april 2013.

En mere alvorlig udviklingstendens er, at kriminelle udnytter forholdsvis simple metoder til at angribe kritiske punkter i kommunikationsinfrastrukturen. Et eksempel er tidligere overbelastningsangreb på telefonlinjer tilhørende alarmcentraler i USA, som blev blokeret for opkald. I udlandet har der også været eksempler, hvor kriminelle kræver løsesum for at stoppe angrebene.

Den generelle udviklingstendens går i retning af, at flere kriminelle og hackergrupperinger vil opnå større tekniske kapaciteter. Det er sandsynligt, at kriminelle grupperinger på kort til mellemlangt sigt vil udleje deres cyberkapaciteter til stater eller ikke-statslige aktører. Herigennem får stater, der ikke har kapacitet til at udvikle malware, en mulighed for at købe et færdigt produkt.

Samlet vurdering og perspektivering

Dansk kritisk infrastruktur udgør et vigtigt strategisk mål for fremmede stater og ikke-statslige aktører. Dette vil ikke mindst være tilfældet i en konflikt mellem en vestlig koalition, hvor Danmark deltager, og et tredjeland med en udviklet cyberkapacitet. Samtidig stiger antallet af angrebsmål i takt med, at flere og flere styrings- og kontrolkomponenter i infrastrukturen opkobles til internettet.

Det er meget sandsynligt, at flere stater på kort til mellemlangt sigt vil tage højde for mulighederne for at angribe kritisk infrastruktur i deres planlægning af militære operationer. Truslen fra ikke-statslige grupperinger består hovedsagligt i, at kriminelle aktører med mere avancerede kapaciteter muligvis vil udleje deres kapaciteter til aktører, der har til hensigt at udføre angreb mod dansk kritisk infrastruktur.

Center for Cybersikkerhed, november 2013