Kristina Westerdahl

2020-01-30 2020/287

Öppen hotbild för elsektorn (januari 2020)

BOX 1200
172 24 SUNDBYBERG

STUREGATAN 1,
SUNDBYBERG

TEL: 010-475 80 00

REGISTRATOR@SVK.SE
WWW.SVK.SE

Innehåll

1 Syfte, underlag och avgränsningar

Syftet med följande hotbild är att uppdatera den antagonistiska hotbilden som ingår i den nationella risk- och förmågebedömningen för elsektorn som Svenska kraftnät tar fram. Hotbilden ska ses som ett komplement till Säkerhetspolisens ”Hotbild mot säkerhetskänslig verksamhet” som är mer generellt formulerad. Följande hotbild omfattar kända hot och den ska inte uppfattas som heltäckande för alla hot mot elförsörjningen som kan förekomma.

Målgruppen för hotbilden är aktörerna i elsektorn. För att hotbilden ska vara tillgänglig för elsektorn är den öppen och den baseras på öppna källor. Den här hotbilden kan bidra till att aktörerna själva skapar en egen hotbild anpassad till sin organisation och verksamhet, vilket i förlängningen kan underlätta för dimensionering av skydd.

2 Sammanfattning

Främmande makts informationsinsamling och kartläggning är fortsatt det största hotet mot Sveriges elförsörjning. Säkerhetspolisens första hotbild specifikt för säkerhetskänslig verksamhet publicerades i juni 2019 och nämner Ryssland och Kina som stater med intresse för sådan verksamhet. Hotet från terrorism och organiserad kriminalitet är lågt men kan inte uteslutas. Bedömningarna i Svenska kraftnäts nationella risk- och sårbarhetsanalys 2018 består alltså. Angreppssätten är också i stort sätt de samma, bland annat phishing-mejl, kontaktförsök via sociala medier och rekrytering av anställda eller entreprenörer inom elsektorn. Säkerhetspolisen lyfter också fram att leverantörskedjor och upphandlingar kan nyttjas av antagonister för att nå sina mål.

3 Hot

3.1 Fysisk skadegörelse

Under 2019 har sprängdåd i Sverige ökat till det dubbla jämfört med 2018. Sprängningarna utförs huvudsakligen av och mot kriminella nätverk. Nationella bombskyddet ser en trend med kraftigare sprängladdningar och att sprängningar sker även i mindre städer. Explosivämnen har blivit åtråvärda för kriminella och stölder sker bland annat på byggarbetsplatser där sådana ämnen förvaras. Explosivämnen har även upphittats utomhus i naturen i ett bebyggt område.

Andra former av fysisk skadegörelse kan också förekomma.

Hot mot elförsörjningen:

Fysisk infrastruktur inom elförsörjningen kan drabbas indirekt av en sprängning i närheten av anläggningen. Inbrott kan ske för att komma över explosivämnen, tändhattar och annan utrustning för bombtillverkning.

3.2 Phishing-mejl och andra cyberhot

Mejl i syfte att lura mottagagaren, s.k. phishing, att gynna angriparen på något sätt (ofta ekonomiskt) är vanligt förekommande idag. Angriparen kan även ha som syfte att få åtkomst till inloggningsuppgifter och it-system, De falska mejlen blir alltmer sofistikerade. Avsändaren kan se ut att vara en välkänd person, t.ex. en högt uppsatt chef eller en leverantör som man normalt har kontakter med. Innehållet utformas så att det är svårare att upptäcka att det inte är från den påstådda avsändaren, t.ex. genom att vara språkligt korrekt.

Det finns en rad andra cyberhot (dvs. hot via internet) som är vanligt förekommande. Informationsinhämtning kan ske genom inspelning (avlyssning) eller avbildning genom fjärrstyrning av elektronisk utrustning som mobiltelefoner och datorer men även smartklockor och liknande. Kapning av konton, lösenord och identiteter ger antagonister möjligheter att sprida vilseledande information under en trovärdig täckmantel. Under november 2019-januari 2020 har ett energibolag i Europa utsatts för it-angrepp, troligen i syfte att samla in användarnamn, lösenord och annan känslig information.

Hot mot elförsörjningen:

Som alla andra sektorer i samhället kan även elsektorn drabbas av phishing-mejl och andra cyberhot. Informationsinsamling, spridning av falsk information och åtkomst till inloggningsuppgifter för it-system kan ha allt från försumbar påverkan till förödande effekter för elförsörjningen, beroende på hur höga kunskaper och andra skydd mot cyberhot som finns i den drabbade organisationen.

3.3 Informationsinsamling genom affärskontakter och sociala medier

Genom kontakter med anställda kan information samlas in om en verksamhet och de anställda själva. Informationsinsamling kan ske på en rad olika sätt, t.ex. vid affärsmöten, konferenser, genom LinkedIn och andra sociala medier. Säkerhetspolisen pekar på att Kina men även Ryssland och andra stater har en aktiv informationsinsamling om säkerhetskänslig verksamhet i Sverige.

Hot mot elförsörjningen:

Genom kontakter med personal inom elförsörjningen kan en antagonist få tillgång till information (uppgifter) av betydelse för elförsörjningen, inklusive om annan personal med nyckelfunktioner, tillgång till it-system (t.ex. genom

inloggningsuppgifter) och möjlighet att påverka hur personal agerar (t.ex. under kriser).

3.4 Uppköp av fastigheter och mark

Uppköp av mark- och sjöområden eller fastigheter i närheten av objekt som är strategiska för Sveriges säkerhet, kan genomföras i syfte att komma åt säkerhetskänslig verksamhet. Säkerhetspolisen nämner två stater som intresserar sig för säkerhetskänslig verksamhet i Sverige: Ryssland och Kina (se avsnitt 4.2). Strategiska köp av fastigheter och mark, genomförda av dessa aktörer, eller med kopplingar till dessa aktörer, är därför av intresse i sammanhanget. Uppköp av fastigheter, mark- och sjöområden kan också användas som ett strategiskt instrument i hybridkrigföring, där verksamhet under det förberedande skedet har en stor betydelse.[1] I Finland finns det exempel på utländska köp av mark och fastigheter nära anläggningar som kan ha strategisk betydelse för samhället och totalförsvaret. Finland har också en ny lag om tillstånd för fastighetsköp för köpare utanför EU- och EES-området som trätt i kraft 2020.[2]

Hot mot elförsörjningen:

För elförsörjningens del kan detta handla om att en främmande makt, eller personer med kopplingar till en främmande makt, köper mark- eller sjöområden eller fastigheter nära till viktiga elanläggningar, broar eller vägar (som krävs för att transportera både personal och materiel till anläggningar). Syftet kan vara att kunna blockera vägar till anläggningar, avlyssna eller sabotera dessa. Det kan även röra sig om sådana områden som ligger nära viktiga kommunikationsnoder för elförsörjningen. Här handlar de främsta hoten om avlyssning och möjligheten att störa viktig kommunikationstrafik för elsystemet.

3.5 Leverantörskedjor och underentreprenörer

Det privata näringslivet ansvarar alltmer för säkerhetskänsliga verksamheters viktiga leveranser och globaliseringen innebär att verksamheternas leverantörer kan finnas i flera länder. Därför är det viktigt att verksamhetsutövare inom säkerhetskänslig verksamhet är medvetna om potentiella risker som utkontraktering av verksamhetskritiska delar till en tredje part kan medföra.

Ett hot är att spionutrustning planteras i kritiska komponenter som används inom elförsörjningen. Det går inte att utesluta att en kvalificerad angripare planterar avancerad skadlig kod i hårdvara hos leverantörer som sedan köps in och används i samhällskritiska IT-system, exempelvis i SCADA-system.

Leverantörskedjor möjliggör flera angreppssätt för en angripare. Ju längre leverantörskedja, dvs. ju fler bolag som finns i kedjan, desto fler potentiella

[1] Se finska Säkerhetskommitténs bedömning: https://svenska.yle.fi/artikel/2016/02/15/ryska-markaffarer-ett-hot-sakerhetskommitten-listade-hybridkrigsfenomen

[2] < https://www.defmin.fi/sv/aktuellt/tillstand_for_fastighetskop_for_kopare_utanfor_eu-_och_ees-omradet>

angreppspunkter finns för angriparen. En antagonist kan också, i syfte att komma åt den säkerhetskänsliga verksamheten, bli en leverantör av kritisk utrustning.

Även utländskt delägande i företag eller strategiska investeringar (av utländska aktörer) i företag som driver säkerhetskänslig verksamhet kan utgöra ett hot, om syftet är att angripa eller utöva påtryckningar mot den säkerhetskänsliga verksamheten. Genom delägandeskap/strategiska investeringar kan man få tillgång till känsliga uppgifter om den säkerhetskänsliga verksamheten och därigenom en möjlighet att påverka hur verksamheten styrs. Även här hänvisas till den bedömning som Säkerhetspolisen gör angående Ryssland och Kina som intresserar sig för säkerhetskänslig verksamhet i Sverige (och andra europeiska länder).Globaliseringen har medfört att det inte är ovanligt att företag i olika länder är sammankopplade genom ägarskap. Ett exempel från elsektorn är det statliga kinesiska företaget State Grid Corporation of China som äger den grekiska nationella systemoperatören (TSO) till hälften och är delägare i minst en portugisisk TSO. Samma företag har 2018 försökt köpa in sig i tyska TSO:n 50Hertz.[3] I Sverige visade företaget intresse för att köpa ABB Power Grid (som har verksamhet Ludvika) när den var till salu.[4]

Hot mot elförsörjningen:

Inom elförsörjningen finns ett stort beroende av entreprenörer och leverantörer för både byggnation, underhåll, reparationer och kritiska komponenter, även från utlandet. Det finns vissa leverantörer som tillhandahåller verksamhetskritiska tjänster/komponenter åt flera nordiska och europeiska systemoperatörer för el. Vid ett eventuellt angrepp mot dessa leverantörer, eller mot tjänster som dessa leverantörer tillhandahåller, finns en risk för en kaskadeffekt i de verksamheter som anlitar samma leverantör. Antagonisters insteg i leverantörskedjor och delägarskap i företag som är leverantörer och entreprenörer till elsektorn kan inte uteslutas.

3.6 Gråzon och hot mot Sveriges totalförsvar

Med gråzon menas ett tillstånd av osäkerhet som varken kan beskrivas som fred eller regelrätt krig men där antagonistiska handlingar riktas mot Sverige från en annan stat, mer eller mindre öppet. Under gråzon kan ryktesspridning, motsägelsefull information, kriminell verksamhet, sabotage samt nätverks- och påverkansoperationer förekomma.

Hot mot elförsörjningen:

Attacker kan riktas mot elnätet i syfte att destabilisera samhällets funktionalitet och försämra totalförsvarsförmågan. I förlängningen kan en antagonist vilja utöva

[3] Reuters, ”China's State Grid seals purchase of stake in Greek power grid”, 2016. The Asset, ”State Grid renews attempt to buy into German electricity transmission grid”, 2018. Second Opinion, ”Laddat när Kina vill köpa energiföretag”, 2018.

[4] Dalabygden, ”Ludvika förbereder sig få kinesiska herrar”, 2018.

inflytande på Sveriges utrikes- och säkerhetspolitiska agerande. I händelse av att Sverige blir utsatt för väpnad konflikt bedöms sabotage mot elförsörjningen utgöra ett led i hybridkrigsföring. Sabotage kan ske både genom cyberangrepp och genom fysiskt sabotage. Sabotage i mindre omfattning kan genomföras i fredstid i syfte att testa elförsörjningens förmåga att förebygga och hantera angrepp.

4 Antagonistiska aktörer

4.1 Allmänt

Antagonister som orsakar eller utför angrepp mot elförsörjningen kan, då de är kända, delas in i olika typer av antagonister. Några typer beskrivs nedan. Det är inte heller ovanligt att antagonister förblir helt okända och inte kan hänföras till någon typ.

4.2 Främmande stat

Säkerhetspolisen nämner två stater som intresserar sig för säkerhetskänslig verksamhet i Sverige: Ryssland och Kina. Det utesluter inte att fler stater också är intresserade. Ryssland samlar in information och kartlägger säkerhetskänslig verksamhet, vilket kan ingå i att hålla Sverige i en gråzon och vara förberedelser för att kunna angripa Sverige.

Kina visar framförallt intresse för forskning, teknologi och innovationer som landet vill tillägna sig för att främja sin egen industri. Under 2019 har relationerna mellan Sverige och Kina försämrats. I december 2019 har Kinas ambassadör i Sverige uttalat att landet avser att begränsa utbytet och samarbetet inom handel och ekonomi med Sverige. Det betyder inte att risken för industriellt spionage i Sverige minskar.

Statliga aktörer har stora resurser, bred kompetens och arbetar långsiktigt för att nå sina mål avseende information om Sverige, inklusive säkerhetskänslig verksamhet.

4.3 Övriga antagonister

Terrorister i Europa har sporadiskt visat intresse för kärnkraftverk men i Sverige finns inga tecken på att elförsörjningen skulle vara ett mål (enligt öppna källor). På samma sätt förefaller inte heller kriminella antagonister intressera sig för elförsörjningen. Förmågan hos båda typerna av antagonister kan variera mellan olika grupper och över tid.

Det troligaste hotet från terrorister eller kriminella är skador på elförsörjningen som en konsekvens av angrepp riktade mot ett annat närstående mål, antingen fysiskt/geografiskt eller i cyberrymden.

Ensamagerande antagonister kan förekomma. Motiven för deras agerande varierar. Det kan bland annat vara missnöje med att mark används för elförsörjningens infrastruktur (t.ex. ledningar och ledningsstolpar) vilket kan yttra sig som fysisk skadegörelse.

5 Mål inom elförsörjningen

Mål inom elförsörjningen för ett antagonistiskt angrepp kan vara infrastruktur, it-system, information (uppgifter) och personal.

Infrastruktur kan angripas fysiskt eller via it-system, t.ex. med en cyberattack. It-system är kritiska för elförsörjningen samtidigt som de kan vara svåra att skydda eftersom det ligger i deras funktionalitet att de ska vara tillgängliga dygnet runt, för flera aktörer och från flera geografiska platser. Attackerna 2015 och 2016 mot elförsörjningen i Ukraina visar att cyberangrepp är möjligt och att konsekvenserna då kan bli omfattande.

Information i form av data i elförsörjningens it-system kan vara det egentliga målet för en antagonist men även information om anläggningar, it-system, sårbarheter i elförsörjningen och personer i kritiska funktioner kan vara mål för informationsinhämtning och kartläggning.

6 Mer information

Följande är en del av underlaget till hotbilden och utgör aktuella publikationer på området. De ger bredare beskrivningar av hoten mot Sverige och samhällsviktig verksamhet som är väl värda att sätta sig in i.

Svenska kraftnät, "Nationell risk- och sårbarhetsanalys 2018" (2018)https://www.svk.se/siteassets/om-oss/rapporter/2018/risk-och-sarbarhetsanalys-2018.pdf

Säkerhetspolisen, "Hotbild mot säkerhetskänslig verksamhet" (2019)

https://www.sakerhetspolisen.se/download/18.7acd465e16b4e0e54c64a/1560776860929/Hotbild-mot-sakerhetskanslig-verksamhet-juni-2019.pdf

Säkerhetspolisens årsbok 2018 (2019)

https://www.sakerhetspolisen.se/download/18.6af3d1c916687131f1fae5/1552543607309/Arsbok-2018.pdf

Militära underrättelse- och säkerhetstjänsten (MUST), "Årsöversikt 2018" (2019)

https://www.forsvarsmakten.se/siteassets/4-om-myndigheten/dokumentfiler/rapporter/must-arsoversikt-2018f.pdf

Försvarets radioanstalt (FRA), "Årsrapport 2018" (2019)

https://www.fra.se/download/18.69cf97cd167832fc038250/1548773731405/FRA-arsrapport-2018.pdf

Nationellt centrum för terrorbedömning, "Helårsbedömning 2019" (2019)

https://www.sakerhetspolisen.se/download/18.6af3d1c916687131f1fba2/1553223698807/NCT-Helarsbedomning-2019.pdf#search='nct'

Myndigheten för samhällsskydd och beredskap (MSB), "Nationell risk- och förmågebedömning 2019" (2019)

https://rib.msb.se/Filer/pdf/28836.pdf

ENISA, "ENISA Threat Landscape Report 2018" (2019)

https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018/at_download/fullReport

FOI, “Typfall 5: Utdragen och eskalerande gråzonsproblematik” (2018)

https://www.foi.se/rest-api/report/FOI%20MEMO%206338