Myndigheten för samhällsskydd och beredskap

FAKTA

Publ.nr: MSB1342 – januari 2019

AVDELNINGEN FÖR CYBERSÄKERHET OCH SKYDD AV SAMHÄLLSVIKTIG VERKSAMHET

Introduktion till avsiktliga elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur

Detta faktablad syftar till att ge en kort introduktion till vad avsiktliga elektromagnetiska hot (EM-hot) är och hur de av antagonistiska grupper skulle kunna användas vid attacker mot offentliga aktörers anläggningar och system. Faktabladet är baserat på en längre rapport, ”Introduktion till avsiktliga elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur”.

Introduktion

I det moderna samhället används elektroniska apparater och system för att lagra och distribuera information, kommunicera via telefoni och internet, styra industriprocesser och serviceanläggningar som TV- och radioutsändningar, kraftverk, vattenverk, kommunikationscentraler, vägbelysning, trafiksignaler, trafikledning, inpasserings- och övervakningssystem, sjukvårdsutrustning, etc. Mindre radarsystem används för övervakning, för fartreglering i moderna bilar och inom en snar framtid i självkörande bilar. Utvecklingen av automatiserade elektronikberoende system har accelererat kraftigt de senaste decennierna. Parallellt med expansionen av elektroniskt kontrollerade system i samhället har det uppkommit möjligheter att avsiktligt störa dessa med elektromagnetiska fält. Militärt har telekrigområdet blivit ett av de centrala verktygen i konflikter runt om i världen. Detta inkluderar avlyssning av fiendens elektroniska kommunikation, generering av störande eller vilseledande signaler, samt olika skyddsåtgärder för att skydda egen utrustning. Störsändare har även kommit att användas civilt, t.ex. av polis för att ta ner drönare, men tyvärr också för kriminella syften, som att blockera villalarm vid inbrott.

Enkelt exempel på en risk- och sårbarhetsanalys (RSA)

Första steget mot att kunna skydda samhällsviktig verksamhet och kritisk infrastruktur mot denna typ av nya avsiktliga hot är att bli medveten om deras existens och hur de skulle kunna användas av antagonister för att störa ut eller inkapacitera viktiga samhällssystem. Sedan behöver man genomföra en risk- och sårbarhetsanalys för egna kritiska system och åtgärda de risker som bedöms allvarliga. Det är dock viktigt att komma ihåg att risk- och sårbarhetsanalyser bör genomföras med viss regelbundenhet eftersom hoten och deras användning utvecklas. En RSA avseende EM-hot kan ha följande huvudpunkter:

1. Presentation av hotscenario
2. Riskidentifiering – Tekniska konsekvenser
3. Riskanalys – Verksamhetskonsekvenser
4. Riskutvärdering
5. Sårbarhetsreducerande åtgärder

EM-hot
Elektromagnetiska hot (EM-hot) utgörs av elektriska och/eller magnetiska fält som är tillräckligt starka för att kunna påverka elektriska/elektroniska apparater och system. EM-hot kan härröra från naturligt förekommande fenomen eller vara genererade av människor, antingen oavsiktligt eller med avsikt att åstadkomma störningar i verksamheten. De senaste decennierna har sett en utveckling och test av utrustning som på några hundra meters avstånd fysiskt kan förstöra fiendens elektronik. Idag säljs kommersiella störsändare via internet medan glada amatörer på samma informationskanal diskuterar och lägger ut information om hur man själv kan bygga utrustning som stör eller förstör elektronik på några tiotals meters avstånd. Kunskapen om dessa möjligheter sprids samtidigt som man kan konstatera att det inte krävs några exotiska, svårhanterliga material eller industriell kapacitet för att konstruera utrustning som kan åsamka system som innehåller och styrs av elektronik stora störningar.

Att skydda samhällsviktig verksamhet och kritisk infrastruktur
Det bästa och billigaste sättet att skydda kritisk utrustning är att kravställa den med avseende på EM-hot under anskaffningsförfarandet. Det är oftast mycket svårare och mer kostsamt att skydda redan befintliga system.

Kommunikation
Det bör eftersträvas att system som är vitala för verksamheten har en inneboende resiliens och robusthet mot EM-hot. Detta kan realiseras genom redundans i systemet och att systemet är anpassat mot tillämpningen. Det gäller då speciellt störtålighet och funktionssäkerhet.
Att kunna byta frekvens vid störning eller att frekvenshoppa är ett skydd mot störningar på vissa frekvenser men kräver tillgång till ett större frekvensområde. För att minimera inverkan från andra oavsiktliga störningar bör man ha ett eget frekvensband.
En grundregel som minskar risken för störningar väsentligt är att inte använda sig av så kallade ISM-band för styrning och reglering av kritiska system.
Om det är möjligt att använda trådbunden kommunikation istället för t.ex. WiFi för kommunikation, styrning och reglering bör man göra det. Ytterligare ett steg mot att skydda kommunikation mellan enheter är att använda optofiber som är helt immun mot EM-hot. Behöver man ändå använda radiokommunikation mellan kritiska system kan man redan vid upphandling kravställa dessa med avseende på robusthet, störtålighet och redundans.
Riktantenner på kommunikationssystemen gör att dessa behöver riktas in mot varandra och minskar störningskänsligheten då antennen inte i samma grad tar emot signaler som kommer från fel håll. Om det är möjligt med hänsyn till användningen bör man skydda information om vilka frekvenser ett visst system är beroende av. En relativt enkel och genomförbar åtgärd är att kartlägga eller övervaka störningsmiljön för att upptäcka förekomsten av oavsiktlig eller avsiktlig störning.

Elektroniska system
Elektroniska system kan kravställas för att tåla en viss elektromagnetisk miljö och förses då med metalliska skal som skyddar elektroniken inuti genom att stoppa elektromagnetisk strålning från att nå innanför metallskalet.
Även vanliga väggar i byggnader ger en viss dämpning av elektromagnetisk strålning utifrån. Därför kan ett första steg vara att flytta känslig utrustning längre in i en byggnad så att den skyddas av flera väggar. Det är givetvis viktigt att även begränsa tillgängligheten.

Nästa steg är att låta bygga ett skärmat rum dedicerat för kritisk elektronisk utrustning. Det är inte alltid enkelt att sätta upp staket eller andra perimeteravgränsningar runt anläggningar för att förhindra tillträde men i de fall detta går är det ofta mycket effektivt.

Olika typer av EM-hot

Naturliga EM-hot
Det är inte ovanligt att kraftiga åskväder leder till störningar på elektronisk utrustning, kommunikationer och elförsörjning. Detta kan orsaka tillfälliga störningar eller permanent skada i utrustningen.
Solstormar, även kallat ”rymdväder”, genereras av utbrott i solens korona och består av elektriskt laddade partiklar som efter några dygn träffar jordens atmosfär och ger upphov till geomagnetiska störningar i jordens magnetosfär. Sådana geomagnetiskt inducerade strömmar genererar ofta synnerligen lågfrekvent störning som kan slå ut elektriska komponenter, t.ex. i transformatorstationer, öka korrosionen i pipelines m.m.

Oavsiktliga EM-hot
Vi omges idag av allt fler apparater som innehåller elektronik som arbetar med svaga spänningar och strömstyrkor, vilket gör dem känsliga för externa elektromagnetiska fält. Detta leder till att apparater allt oftare riskerar att störa varandra. All elektrisk utrustning genererar EM-fält i sin omgivning. Dessa är ibland så kraftiga att de stör annan elektrisk utrustning i närheten. Det händer att utrustning strålar ut mer elektromagnetisk energi än vad som är tillåtet, t.ex. när någon komponent i utrustningen gått sönder. Det finns en rad incidenter där trådlösa system har störts ut av oavsiktliga störningar.

Avsiktliga EM-hot
Det finns många potentiella antagonister som kan tänkas använda sig av elektromagnetiska hot för olika syften, alltifrån teknikintresserade studenter som själva konstruerar och testar enkla störkällor, via kriminella som vill slå ut larm eller andra säkerhetssystem vid inbrott, till terroristorganisationer och främmande makt som vill förlama det civila samhället vid en internationell konfrontation.

Kontakta Myndigheten för samhällsskydd och beredskap

651 81 Karlstad

Tfn: 0771-240 240
Fax: 010-240 56 00
registrator@msb.se
www.msb.se

Kontaktpersoner:
Gustav Söderlind
ics@msb.se

Sabrine Wennberg
ics@msb.se