Projektnummer/Project no
E21410
Kund/Customer
MSB
FoT-område
Inget FoT-område

Författare/Author
Sten E Nyholm, Kia Wiklundh, Tomas Hurtig

Datum/Date
2021-03-25
Memo nummer/Number
FOI Memo 7507

Incidenthantering av elektromagnetiska hot mot samhällsviktiga tjänster

Trådlös kommunikation har på många håll blivit en väsentlig del av den infrastruktur som ligger till grund för många samhällsviktiga tjänster, även i anslutningen till industriella informations- och styrsystem. Detta utgör en potentiell sårbarhet, då det ger antagonistiska aktörer en möjlighet att påverka leveransen av de samhällsviktiga tjänsterna genom att störa den trådlösa kommunikationen, alternativt genom att göra utrustningen obrukbar.

Sedan tidigare har det identifierats ett behov av att agera medvetandehöjande inom området elektromagnetiska hot (EM-hot), och MSB har med hjälp av FOI tagit fram material för utbildning inom området och en vägledning i hur man gör en risk och sårbarhetsanalys. FOI har även genomfört en studie om rapporterade incidenter och hot mot trådlösa system, vilken även innefattar några förslag på åtgärder.

Detta FOI Memo är avsett att komplettera tidigare arbeten med en vägledning dels för hur man kan hantera en pågående incident med EM-hot och dels vilka åtgärder som kan vidtas för att förhindra liknande incidenter. Detta i syfte att så gott det går hantera incidenten samt underlätta senare analys av förloppet och eventuell identifiering av förövare. Åtgärdspunkterna som listas i detta memo är generella och bör anpassas till förutsättningarna i den specifika verksamhet som ska skyddas. Memot utgör slutleverans till MSB inom uppdraget *NCS3 Studie: Incidenthantering av Elektromagnetiska hot mot samhällsviktiga tjänster*.

Sändlista/Distribution

Gustav Söderlind, MSB

Inledning

En antagonistisk elektromagnetisk attack kan vara svår att skilja från naturliga störningar, som t.ex. kan orsakas av blixtnedslag eller solstormar, eller från oavsiktligt emitterade elektromagnetiska störningar från elektriska utrustningar, eller störningar som sker på ledningar i form av variationer i nätspänning, glappkontakt eller avbrott i signalkablar, störande utrustning eller maskiner i närheten.

Blixtnedslag och solstormar kan generera kraftiga transienta spänningspulser på det fasta elnätet, vilket kan förstöra ansluten elektronisk utrustning eller störa utrustning som är belägen nära en påverkad kraftledning. Typiskt för dessa typer av störningar är att påverkan drabbar ett större område samtidigt, t.ex. inom några kilometer från ett blixtnedslag eller över en hel landsända eller en kontinent när det gäller solstormar.

Solcellsanläggningar är kända för att kunna emittera störningar som kan koppla in på kommunikationssystem via dess antenn. Störningar yttrar sig ofta som tillfälliga avbrott i signalförbindelser, förvrängda data (t.ex. brusig bild, felaktiga tecken i en text),orimligt långa svarstider vid kommunikation eller svårighet att få utrustningar att kommunicera med varandra. Även reservkraftaggregat av typen UPS har visat sig kunna generera störningar på elektronisk utrustning.

En antagonistisk elektromagnetisk attack mot en anläggning kan genomföras på olika sätt, t.ex. med enkla kommersiella störsändare med kort räckvidd, med avancerade militära störsändare som verkar på längre avstånd, eller med ännu kraftigare mikrovågsvapen med förmåga att störa eller fysiskt förstöra elektronisk utrustning. Enklare hotsystem kan bäras av en person eller liten drönare, större anordningar kan transporteras med bil, båt, större drönare, robotar eller flygplan. Attacken kan utföras av en enskild angripare eller genomföras som en koordinerad attack med flera aktörer som har olika uppgifter. Verkan av en antagonistisk elektromagnetisk attack kan likna de naturliga eller oavsiktliga som beskrivs ovan, vara smalbandig eller bredbandig, kontinuerlig eller pulsad, men förekommer ofta inom ett begränsat geografiskt område, ibland inom några hundra meter.

En anläggning som är lokaliserad på en bestämd plats är lättare att skydda från antagonistiska attacker, t.ex. med avspärrningar eller inpasseringskontroll, än ett infrastrukturobjekt som är utspritt över ett större geografiskt område, t.ex. ett trafiksignalsystem som fjärrstyrs med trådlös kommunikation eller ett nät av basstationer för mobil kommunikation.

Om man inte är medveten om möjligheten att utsättas för en antagonistisk elektromagnetisk attack kan det dröja länge innan man förstår orsaken till problemen som attacken leder till. En antagonistisk elektromagnetisk attack kan lätt förväxlas med andra, hittills vanligare, störande orsaker. Om en kommunikationsradio eller dataförbindelse slutar fungera eller om en datorskärm flimrar och slocknar är det ofta naturligt att tro att det rör sig om ett apparatfel eller en bugg i programvaran, att orsaken är en glappkontakt, att en säkring gått eller att det blivit ett strömavbrott.

Den som verkar inom samhällsviktig verksamhet bör dock vara medveten om att det bland aktivister, kriminella, terrorister och fientligt sinnade nationers aktörer kan finnas incitament att störa ut en verksamhet, tillfälligt eller permanent, som påtryckning i fredstida förhandlingar, för att störa en pågående insats av blåljusmyndigheter, för att försvåra mobilisering i ett gråzonsläge eller utgöra en ytterligare påfrestning under pågående krig.

För att belysa problematiken med EM-hot ges här två exempel på scenarier med störningsincidenter.

Scenarier med störningsincidenter i hamn eller vattenverk

Störningsincident i en containerhamn:

Under pågående lastningsarbete i en containerhamn upphör plötsligt kommunikationen mellan hamnkontoret och kranföraren samt med truckförarna. Efter någon minut rapporteras att VHF-trafiken med fartygen liksom fartygsrapporteringssystemet SafeSeaNet och det automatiska identifieringssystemet AIS alla är utslagna. Detta gör att man inte har full kontroll över fartyg som är på väg in mot hamnen. Endast radarn fungerar, vilket innebär att man kan se var fartygen befinner sig. Ansvarig chefsoperatör försöker ringa säkerhetschefen, men mobiltelefonen saknar kontakt med basstationen som står utanför hamnområdet. Chefsoperatören blir istället tvungen att gå över till en annan byggnad för att muntligen informera säkerhetschefen att all radiotrafik är utslagen.

Säkerhetschefen tar fram sin checklista för åtgärder under pågående misstänkt elektromagnetisk attack och beger sig till hamnkontoret. Chefsoperatören för protokoll och noterar vilka system som är utslagna, när avbrotten skedde och hur störningarna yttrar sig i de olika systemen (brus, tystnad, störd hörbar kommunikation, avsaknad av uppdaterad positionsinformation, etc.) när man byter frekvens och slår av och på störda utrustningar. Vaktbolaget får i uppgift att kontrollera om obehöriga personer eller fordon befinner sig inom hamnområdet eller på angränsande vägar utanför staketet. Elektrikern beger sig till elcentralen för att mäta upp spänningsnivåerna på inkommande och utgående ledningar samt även med oscilloskop registrera spänningskurvor för att se om det finns en överlagrad störning på sinusformen. En annan medarbetare ringer till Elsäkerhetsverket och PTS för att meddela att hamnen är utsatt för störningar.

Efter en stund kan man konstatera att det inte finns någon obehörig person eller misstänkt fordon i närheten och att det inte förekommer överlagrade störningar på spänningsförsörjningen. Eftersom det enbart är trådlöst kommunicerande utrustning som är störd och inte nätanslutna datorer, fast installerad reglerutrustning för portar och lastbryggor eller passagekontrollsystem drar man slutsatsen att det rör sig om en trådlös störning på kommunikationsfrekvenser i VHF- och UHF-banden. När en inspektör från Elsäkerhetsverket anländer med spektrumanalysator och pejlutrustning kan man konstatera att störningarna härrör från ett av fartygen som ligger längs kajen i väntan på att lossas. Efter kontakt med kaptenen finner man att en besättningsman använder en hemmabyggd kortvågsradio som inte är frekvensavstämd utan genererar brus i högre frekvensområden.

När incidenten är över rapporterar säkerhetschefen händelsen till MSB och PTS via respektive hemsida genom att fylla i formulär och bifoga en kort redogörelse för händelseförloppet. Efteranalysen leder till att man installerar en radiospektrumövervakande utrustning med pejlfunktion som både loggar den elektromagnetiska miljön och kan upptäcka störningar samt utbildar personalen i hur man använder utrustningen för att snabbt kunna identifiera störkällor.

Attack mot ett kommunalt vattenverk:

En varm sommardag med en gräsbrand på ett fält strax utanför staden går ett larm vid stadens vattenverk. Det är den trådlösa IP-radiokommunikationen för övervakning och styrning av vattenverkets pumpar, vattennivåer i bassänger och tryck i ledningar som fallerar. I kontrollrummet ger datorskärmarna med instrumentdisplayerna kraftiga svängande utslag och några ger inga utslag alls. Dessutom upptäcker personalen att monitorerna som visar bilder från övervakningskamerorna på området inte visar någon bild utan flimrar. När man ska rapportera detta till huvudkontoret i city finner man att även mobiltelefonin ligger nere. Däremot fungerar en fast telefon.

De två operatörerna sitter i en kontorsbyggnad i ena änden av vattenverkets område och har ingen direkt överblick över renings- och filtreringsbassänger samt cistern. Efter två timmar kommer servicepersonal för att undersöka den störda utrustningen. De berättar att det är ett hål i stängslet vid vägen några hundra meter från porten till området. En av operatörerna beger sig till stängslet och kan konstatera att cisternen som ligger intill det uppklippta hålet är tömd och pumparna som pumpar ut vattnet i ledningsnätet går på högvarv.

Servicepersonalen hittar inget fel på övervakningsutrustningen som nu fungerar normalt igen, men man kan konstatera att dataloggen inte innehåller några läsbara data. På övervakningsfilmerna ser man att strax före incidenten stannar det en bil utanför staketet på den plats där man senare hittade det uppklippta hålet. Det går dock inte att identifiera några personer. Vattenverkets personal tar prover på det vatten som är kvar på botten i cisternen men hittar inga substanser som avviker från vad som är normalt. Ansvarig chef rapporterar incidenten till MSB och PTS eftersom man misstänker att vattenverkets övervaknings- och kontrollutrustning har utsatts för en avsiktlig störning.

Dagen efter insjuknar över hälften av stadens befolkning i svåra magsmärtor och diarré. Sjukvården överbelastas och många kommunala förvaltningar och privata företag drabbas av personalbrist och störningar i verksamheten. Vid provtagning i ledningsnätet finner man rester av ett biologiskt stridsmedel som är känt för att kunna ge kramper, kraftigt illamående och feber. Med den kunskapen kan man ge rätt behandling till de drabbade och skickar ut ett viktigt meddelande till allmänheten med uppmaning att inte använda vattnet från ledningsnätet utan hämta vatten från tankbilar på Stortorget och vid köpcentrumet utanför staden. Efter ett par dagar har man spolat igenom ledningsnätet och vattendistributionen återupptas.

I den efterföljande analysen kommer man fram till att avsikten med störningsincidenten var att förgifta stadens befolkning för att skapa oro och missnöje med den kommunala tekniska förvaltningen. För styrning av pumpstationerna väljer man att gå tillbaka till ledningsbunden kommunikation och övervakningskamerorna kompletteras med rörelsesensorer med fasta ledningar till kontrollrummet för övervakning av området strax innanför stängslet.

Förberedande sårbarhetsanalys och eventuella åtgärder

Ansvarig för en samhällsviktig anläggning, infrastruktur eller verksamhet som använder elektronisk utrustning för styrning eller kommunikation bör regelbundet genomföra risk- och sårbarhetsanalys (RSA) där man tar med antagonistiska elektromagnetiska hot som en möjlig risk för den egna verksamheten. Syftet med en RSA bör vara att identifiera svagheter i skyddet av elektroniska styr- och reglersystem, kommunikationsutrustning, datalagring/bearbetning etc.

Man kan undvika många onödiga risker att bli utsatt för en antagonistisk elektromagnetisk attack genom att i förväg analysera sin situation, vilka elektroniska system som verksamheten är kritiskt beroende av och vilka som man klarar sig utan i en krissituation. När man identifierat svagheter kan man åtgärda dem under ordnade former med minimal påverkan på kärnverksamheten. Det kan röra sig om att flytta känslig utrustning till en bättre skyddad plats, att begränsa åtkomsten till vissa lokaler, att förse viss utrustning med olika typer av skydd, överväga att använda trådbundna system eller förbättra robustheten för de trådlösa systemen, eller att se till att det finns lätt tillgänglig reservutrustning om den ordinarie blir utslagen. Vilka åtgärder som kan behöva vidtas beror på verksamhetens natur, dess betydelse för totalförsvaret i en krissituation, beroendet av vissa typer av utrustning, samt ett antal områdesspecifika faktorer.

För exempel på hur avsiktliga elektromagnetiska hot kan vara utformade och hur en elektromagnetisk attack kan se ut hänvisas till följande publikation på MSB:s hemsida:

”Introduktion till avsiktliga elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur”, Tomas Hurtig, Sara Linder, Kia Wiklundh, Karina Fors, Sten E Nyholm, MSB1180, 2018. (https://www.msb.se/sv/publikationer/introduktion-till-avsiktliga-elektromagnetiska-hot-mot-samhallsviktig-verksamhet-och-kritisk-infrastruktur/)

Hur man steg för steg kan ta med antagonistiska elektromagnetiska hot i en risk- och sårbarhetsanalys för sin verksamhet beskrivs i följande publikation på MSB:s hemsida:

”Vägledning för risk- och sårbarhetsanalys avseende antagonistiska elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur”, Kia Wiklundh, Sara Linder, Karina Fors, Tomas Hurtig, Sten E Nyholm, MSB1178, 2018. (https://www.msb.se/sv/publikationer/vagledning-for-risk--och-sarbarhetsanalys-avseende-antagonistiska-elektromagnetiska-hot-mot-samhallsviktig-verksamhet-och-kritisk-infrastruktur/)

Åtgärder under pågående misstänkt incident (i syfte att hantera denna och samla bevis)

En incident med misstänkt elektromagnetisk störning bör behandlas som en säkerhetsincident enligt etablerade rutiner. Säkerhetsansvarig kan besluta om vilka åtgärder som ska vidtas, t.ex. enligt en verksamhetsanpassad checklista. Här följer en punktlista med åtgärder som kan vidtas vid en misstänkt elektromagnetisk störning. Eftersom elektromagnetiska vågor inte lämnar direkta spår som kan användas i en forensisk undersökning är det betydelsefullt om man kan samla in data under en pågående incident.

- Rapportera genast till säkerhetsansvarig, systemansvarig eller motsvarande som kan besluta om åtgärder och ha större möjligheter att undersöka en misstänkt incident. Exempelvis kan man behöva engagera personal med tillgång till lämplig mätutrustning eller annan kapacitet att hantera incidenter. Efter inrapportering ska fortsatt informationsinsamling ske.
- Undersök om det finns annan utrustning i närheten som också är störd. Om man kan kartlägga ett större eller mindre geografiskt område som är påverkat av en elektromagnetisk incident blir det lättare att hitta källan till störningen.
- Försök att ta reda på om det bara är trådlös utrustning som är påverkad, eller om även utrustning som är ansluten till det fasta elnätet eller till signalkablar också är påverkad.
- Beskriv vilken utrustning som är störd och vilken utrustning som inte är störd. Markera på en karta eller skiss var alla påverkade system och deras antenner befann sig vid tidpunkten för störningen eller, om störningen uppträdde i olika system vid olika tidpunkter, vilka system som störddes vid vilka tidpunkter. Detta är viktigt för att kunna fastställa påverkansområdet och lokalisera störkällan.
- Det är viktigt att notera hur störningar yttrar sig:
    - Upprätta en skriftlig beskrivning av upplevda effekter så snart som möjligt.
    - Ta en bild av en skärm eller filma en apparatdisplay.
    - Undersök i vilka frekvensområden som en radioutrustning eller liknande trådlös förbindelse störs. Dvs. prova att byta frekvens ett flertal gånger om det är möjligt.
    - Notera vid vilka tider på dagen eller under veckan, året, etc. som återkommande störningar eller avbrott uppträder. Periodicitet kan vara viktig för att identifiera en störkälla.
- Om det gäller störning mot trådlösa system som exempelvis radiomottagare, mobiltelefonisystem eller GNSS-mottagare:
    - Kontrollera mottagningsförhållanden genom att säkerställa att radiomottagarens antenn inte är skymd.
    - Kontrollera att kablage som förbinder antennen med radiomottagaren är oskadade och ihopkopplade.
    - Om det är möjligt prova att flytta antennen eller använda en annan antenn.
    - Kontrollera att radiosystemet inte störs av oavsiktliga störningskällor genom att säkerställa att radiomottagarens antenn inte står i närheten av elektriska utrustningar med spännings- eller frekvensomvandlare, klockor/oscillatorer, LED-lampor, eller andra utrustningar som kan störa.

- Prova att stänga av och starta om störd utrustning. Notera om detta hjälper och hur snabbt efter omstart som störningar återkommer.
- Prova att stänga av och starta om annan utrustning i närheten. Särskilt viktigt om störningar först uppkom när den andra utrustningen installerades eller startades. Notera hur snabbt efter omstart som störningar återkommer.
- Prova, om möjligt, att koppla bort delar av utrustningen eller ansluta enheter för att se om man kan identifiera en specifik del som är störd eller orsakar störningar.
- Om möjligt, försök att mäta upp störningarnas styrka, frekvensinnehåll, pulsform, etc. med mätprob och oscilloskop, spektrumanalysator eller annan mätutrustning.
- Notera om det förekommer möjlig misstänkt aktivitet i omgivningen. Exempelvis fordon som står parkerade utanför ett stängsel eller kör oförklarligt långsamt längs en närbelägen väg. Andra suspekta situationer kan innefatta okända personer, fartyg eller drönare som uppehåller sig i närheten.
- Notera om det förekommer åska eller atmosfärisk elektricitet. Det senare kan yttra sig som att det sprakar (ljud och ljus) kring kraftledningar, från masttoppar eller andra spetsiga objekt.
- Om man har upptäckt en misstänkt störande utrustning kan man försöka att stänga av den. Om utrustningen är ansluten till en yttre spänningskälla, t.ex. ett vägguttag i en entréhall, kan man försöka att koppla bort kabeln till spänningskällan utan att röra det misstänkta objektet.
  Observera dock att en utrustning som används av en antagonist för att avsiktligt störa en verksamhet kan vara apterad med en sprängladdning eller liknande, som kan utlösas vid beröring eller annan yttre påverkan alternativt om elförsörjningen bryts. I de flesta fall är det bäst att tillkalla polis som får ta hand om det misstänkta föremålet.

Åtgärder när incidenten är över (i syfte att samla bevis som kan underlätta analys)

- Notera om den störda utrustningen fungerar normalt efter att störningen upphört. Om inte kan komponenter eller kretsar vara skadade. Man kan prova att stänga av utrustningen och starta om den för att se om detta avhjälper eventuella kvarstående fel.
- Om utrustningen inte fungerar eller är helt död bör den undersökas av en kompetent tekniker/ingenjör för att konstatera var felet finns. Är det en nätdel, förstärkare, ledning, kontakt, mikroprocessor eller annan komponent/del som är trasig?
- Notera om det nyligen har gjorts installationer av ny utrustning i närheten. Det kan vara nya kraftledningar eller transformatorstationer, solcellsanläggningar, kommunikationsantenner, utrustning för avbrottsfri kraftförsörjning (UPS:er), spännings- eller frekvensomvandlare, LED-belysning eller annan fast ansluten eller trådlös utrustning i närheten eller i den egna byggnaden.
- Tag kontakt med kollegor som arbetar i andra delar av en anläggning eller med annan typ av apparatur för att höra om de också upplevt störningar vid samma eller andra tidpunkter.
- Kontakta aktörer i intilliggande anläggningar, byggnader, etc. för att höra om de också upplevt störningar vid samma eller andra tidpunkter.
- Kontrollera data (tid och datum) som samlades in under incidenten och jämför mot annan information om besök, övervakningskameror och andra system som övervakar händelser på platsen. Både i tid och geografiskt med hänsyn till var störst påverkan upplevdes.
- Spara om möjligt loggfiler från datorsystem som upplevt störningar.
- Är det bara system som använder radiokommunikation som störts eller är det även andra, icke radiokommunicerande system som störts? Detta kan vara svårt att avgöra i vissa situationer t.ex. kan alla datorer vara anslutna via Ethernetkablar men dessa är i sin tur kopplade till internet via mikrovågslänk på taket. Om störningen skett på mikrovågslänken eller direkt in på kablar och datorer kan vara svårt att avgöra. Om störningen skett direkt på mikrovågslänken blir naturligtvis hela internettillgången för alla användare påverkad medan en störning som kopplar in på det trådbundna nätet kan vara avgränsad.
- Kontrollera om det förekommer/förekommit kända störningar över den aktuella regionen, t.ex. åskväder (kontakta SMHI), kraftig solaktivitet (kontakta SMHI eller IRF) eller om det finns kända störande anläggningar i närheten (kontakta Elsäkerhetsverket).
- Sammanställ en dokumentation av ovanstående, med händelseförlopp och observationer. Tag kontakt med berörd myndighet (se MSB:s checklista för incidentrapportering) och skicka in sammanställningen.
- Man kan även anlita en erfaren expert eller specialiserad konsultfirma för att analysera dokumenterade störningar av elektronisk utrustning med syftet att identifiera ursprung och orsak till uppkomna elektromagnetiska störningar.

Åtgärder efter incidenten (i syfte att förhindra framtida incidenter)

- Om man har noterat att störningarna varit trådbundna eller kommer via utrustningens antenn kan man installera skyddskomponenter på ledningar eller antennkablar som ansluter till den störda utrustningen. Det kan röra sig om olika typer av transientskydd, lågpass- eller bandpassfilter, drosslar, gnistgap, m.m. Möjligen kan ledningar behöva ersättas av skärmade eller dubbelskärmade kablar. Detta bör göras av erfaren servicepersonal. För att installera skyddskomponenter är det viktigt att känna till störningarnas frekvensinnehåll och styrka.

- Om det rör sig om trådlösa störningar som inte kommer via en ansluten antenn kan man installera ett skalskydd runt den utrustning som är störd. Ledningar som behöver passera igenom skalet ska vara försedda med lämplig typ av transientskydd och jordning. Detta bör göras av erfaren servicepersonal eller konsultfirma med kunskaper om hur detta ska göras på rätt sätt.

- Störningar på t.ex. SCADA-system som använder sig av telekommunikation mellan reglage, givare och styrdatorer kan göras väsentligt robustare om telekommunikationen byts mot trådbunden- eller fiberkommunikation.

- Se över placeringen av antennen för det trådlösa systemet, den kan kanske flyttas till en plats där det är mindre risk för störningar. I vissa fall kan kanske två antenner användas för att minska risken att båda störs samtidigt eller så kan en antenn med riktverkan användas för att minska känsligheten i vissa riktningar.

- Om man konstaterat uppträdande av suspekta individer eller fordon i närheten kan man, om det är möjligt, utöka perimeterskyddet och tillträdesskyddet. Detta kan göras genom att flytta staket längre bort från byggnaden med den påverkade utrustningen, spärra av eller begränsa tillgång till vägavsnitt i närheten, installera övervakningskameror, införa kontroller av vilka personer som kan komma i närheten av viktig utrustning eller känsliga installationer, t.ex. kopplingsskåp eller antenner, på en anläggning, eller på annat sätt begränsa tillgång till närområdet för obehöriga.

- Om störningar uppträder med en viss periodicitet kan man försöka korrelera dessa med trafik eller andra aktiviteter. Exempelvis kan störningar som uppträder tillfälligtvis vardagar morgon och kväll förmodas bero på arbetsresor med passerande fordon som genererar störningen, t.ex. via icke avstörda tändspolar eller installerade GPS-störare.

- Vid upprepade störningar eller vid störning av kritiska samhällsviktiga funktioner kan man anskaffa en utrustning som kontinuerligt monitorerar den elektromagnetiska miljön. I många fall kan det räcka att monitorera det frekvensband som används; i andra fall kan man behöva analysera ett mycket brett frekvensspektrum. Detta kan hjälpa till att såväl karakterisera naturliga ostörda förhållanden som identifiera när det uppträder störningar, även sådana som inte manifesterar sig i felfunktion hos elektronisk utrustning.

- Rapportera misstänkt eller bekräftad elektromagnetisk störning till relevant myndighet enligt den information som ges på MSB:s hemsida: https://www.msb.se/sv/publikationer/elektromagnetiska-hot--information-om-kontaktytor-for-incidentrapportering/