FOI MEMO

Projekt/Project | Sidnr/Page no

NRFB – Scenarioutveckling cyber | 1 (27)

Projektnummer/Project no | Kund/Customer

E13369 | MSB

FoT-område

Handläggare/Our reference | Datum/Date | Memo nummer/number

Ester Veibäck, Fredrik Malmberg Andersson, Lars Westerdahl | 2014-06-18 | FOI Memo 4936

Ett första steg mot informations- och cybersäkerhetsrelaterade analyser i nationell risk- och förmågebedömning

Sändlista/Distribution:

Kerstin Borg, MSB

Magnus Winehav, MSB

Christina Goede, MSB

Eva Mittermaier, FOI

Erik Carlsson, FOI

Innehållsförteckning

1 Introduktion

Informationshantering är en viktig del av samhället, och den blir allt mer omfattande och komplex. Händelser som påverkar informations- och cybersäkerheten kan få mycket stor betydelse i våra liv. En stor del av den funktionalitet vi använder oss av i vardagen automatiseras och digitaliseras i IT-system. Detta gör vår vardag i många fall effektivare, och underlättar för oss att söka information, hantera data, kommunicera och ta beslut. Den snabba teknikutvecklingen gör det möjligt både att förbättra informationshanteringen och att samhället blir mer sårbart för avbrott. Baksidan av den ökade integrationen är att de negativa konsekvenser som kan uppstå av fel kan bli lika magnifika.

Detta uppdrag, som har genomförts av Totalförsvarets forskningsinstitut (FOI) på uppdrag av Myndigheten för samhällsskydd och beredskap (MSB), har haft som mål att utveckla två scenarier inom området informations- och cybersäkerhet, för fortsatt analys inom NRFB. I detta memo ger vi en sammanställning över arbetet som bedrivits för att utveckla dessa scenarier. Memot utgörs av en bakgrund som bland annat belyser komplexiteten i området, och ett förslag till hur vi fortsatt bör arbeta för att analysera det. De två scenarierna som vi har arbetat med presenteras i varsin bilaga till memot.

Syftet med nationell risk-och förmågebedömning (NRFB) är att utveckla samhällets förmåga att förebygga och hantera kriser. Detta görs genom att identifiera och analysera allvarliga risker i Sverige, vilka konsekvenser dessa kan ge upphov till samt vilken förmåga som krävs för att förebygga och hantera dem. Analysen görs normalt genom scenarioanalys där ett stort antal aktörer är delaktiga i att genomföra analysen. Arbetsprocessen bidrar också till att skapa en gemensam förståelse för de olika analyserade riskerna.

1.1 Definition av typhändelsen

Händelser som påverkar informations- och cybersäkerhet kan inte betraktas som enbart en typ av händelser (jämför till exempel med ”naturolyckor” som kan vara storm, skred, regnoväder et cetera). Informations- och cybersäkerhet finns i alla delar av samhället och kan därmed inte utgöra grund för enbart ett scenario. Vår syn på vilka typer av händelser som kan benämnas cyber- eller informationssäkerhetshändelse beskrivs också närmare under avsnitt 3.1.

De typhändelser som i detta projekt valdes för att titta närmare på och utveckla scenario för, är en antagonistisk attack som riktar sig mot industriella informations- och styrsystem (SCADA[1], i detta fall i ett vattenverk) och en icke-antagonistisk händelse som sker inom sjukvården som leder till problem i läkemedelshanteringen.

1.2 Slutsatser av utfört arbete

Under arbetets gång har området informations- och cybersäkerhet analyserats i syfte att få en överblick över vad som karaktäriserar det och för att kunna utveckla scenarier som är representativa för detsamma. Projektet har, precis som MSB[2], identifierat att cyberområdet är så integrerat med samhället och dess funktioner att det angår alla och är en övergripande utmaning för samhället. Detta gör det svårt att analysera konsekvenser genom enskilda scenarier.

De olika karakteristiska dragen för området, se avsnitt 3.1, är allomfattande i sin natur. Speciellt de som handlar om tät integration i hela samhället och oklara orsaks- och konsekvenssamband. Detta innebär en stor utmaning om man vill beskriva ett scenario, som är begränsat till en sektor, som ska representera cyberområdet. Om man gör så missar man viktiga delar av de aspekter som är förknippade med området.

[1] Supervisory Control And Data Acquisition

[2] MSB 2013 *Övergripande utmaningar för samhällsskydd och beredskap- - Analys av fem scenarier om samhället år 2031* Publikation MSB 563

Det intressanta ur ett cyberperspektiv på samhällsnivå landar inte i om IT-system X eller Y fallerar. Det intressanta, och det som tydligast sätter fokus på samhällets förmåga att hantera cyberincidenter är just en beskrivning av bredden i hur störningar i informationsflöden kan uppträda och vilka konsekvenser det kan leda till.

Som nämndes inledningsvis inriktades arbetet med att utveckla scenarier i två spår: ett antagonistiskt scenario som rör industriella informations- och styrsystem, i detta fall i vattenförsörjningen. Det andra scenariot inriktades till att vara ett oavsiktligt fel som uppstår i en programvara, vilket orsakar att läkemedelsdoseringen i så kallade dos-påsar blir fel. Det första scenariot finns med i sin helhet i bilaga 1 till detta memo, men det andra scenariot har vi i ett sent skede beslutat att inte slutföra. En bidragande anledning är att systemet i fråga, och situationen kring det, i dagsläget redan är omdebatterat. Det är en pågående diskussion och ett utvecklingsområde kring hur denna hantering ska se ut. Detta i kombination med resonemanget ovan, att scenariot är begränsat till en sektor och inte ensamt kan ses som representativt för cyberområdet gör att vi inte har färdigutvecklat det. I bilaga 2 finns bakgrundsmaterial och en inledning till scenariot som dokumentation.

1.3 Hur kan vi analysera informations- och cybersäkerhet?

Med ett bredare angreppssätt i analysen kan man fokusera på saker som t.ex. hur samhället drabbas generellt vid olika typer av brister i hanteringen av information, till exempel brister i tillgänglighet, konfidentialitet, riktighet eller spårbarhet. Här kan man med fördel analysera ett antal typfall, utifrån exempelscenarier, som belyser dessa aspekter och även några av de karaktärsdrag som vi lyfter fram i avsnitt 3.1, såsom informationsberoenden, interaktioner över tid och rum osv.

Det är inte fullt tydligt vilken nivå man bäst börjar analysen på men ett alternativ kan vara att analysera exempelscenarierna på ett övergripande plan, diskutera hur samhället påverkas och vilken beredskap som finns eller krävs i samhället. Det kanske inte är nödvändigt (eller ens fruktbart) att gå in för djupt i detaljer avseende dessa. Alltså, man utgår från de karakteristiska dragen inom cyber, och cyberproblematiken, och ser vilka effekter som uppstår var i händelse av incident, och vilka generella förmågor som är specifika för informationssäkerheten. Vad gör man när man inte har tillgång till informationen, eller att riktigheten eller konfidentialiteten i den kan ifrågasättas?

Att anlägga ett fokus på cyber och dess karakteristika gör det även lättare att undvika fällan med att välja en sektor som man vill ska drabbas av specifika konsekvenser, vilket lätt leder vidare till att man inte längre har ett *cyber*scenario framför sig, utan ett scenario som fokuserar mer på vatten, el, logistik eller liknande. På sikt kan det kanske även vara förtjänstfullt att, just med tanke på områdets övergripande karaktär, ha med cyber som en komponent i flera av de scenarier som analyseras inom ramen för NRFB eller liknande aktiviteter.

En bredare översyn av problematiken och hur samhället behöver förhålla sig till området innebär, förutom ovan nämnda fördelar, att MSB:s arbete med att förbättra samhällets beredskap och kunskap inom området stöds. En övergripande analys av samhällets utmaningar inom området kan naturligt följas upp med analyser av konsekvenser för olika typer av cyberincidenter.

2 Metod

Arbetet har bedrivits av en projektgrupp bestående av Ester Veibäck, Fredrik Malmberg Andersson och Lars Westerdahl på FOI samt Kerstin Borg på MSB:s enhet för strategisk analys. Som stöd till arbetet har Christina Goede, Martin Eriksson, Svante Nygren, Katrin Berggren och Ann-Marie Alverås Lovén från MSB:s verksamhet för samhällets informations- och cybersäkerhet (ICS) deltagit.

För att välja scenarier i en helt öppen utfallsrymd konstaterades att vi först behöver förstå och om möjligt beskriva vad som skiljer cyber- och informationssäkerhetsområdet från övriga sektorer och riskområden som behandlas i NRFB. Projektet har därför genomförts i huvudsak i tre delar:

1. Reda ut hur området cyber- och informationssäkerhet kan förstås ur ett NRFB-perspektiv och urval av scenarioidéer att utveckla.
    - Vad är karakteristiskt för cyber- och informationsområdet, och vad skiljer det från andra områden som hanteras inom NRFB?
    - Vilka typer av icke-antagonistiska händelser inom området är intressanta att analysera?
    - Vilka sektorer i samhället är intressanta att ha med i scenario?
2. Bakgrundsbeskrivning i memo
3. Utveckling av scenarier
    - Intervjuer och informationssökning
    - Författande

En mötesserie om tre möten genomfördes tillsammans med ICS, med syfte att utreda punkt 1. Det första mötet (den 21 januari 2014) syftade till att ge förståelse för om och hur cyber- och informationssäkerhets-området skiljer sig från andra områden, samt kartlägga olika typer av icke antagonistiska händelser. Ett något bearbetat resultat av detta finns redovisat i avsnitt 3.1.1 och 3.1.2. Det andra mötet (den 11 februari 2014) ägnades åt att diskutera vilka sektorer i samhället som vore intressanta att lyfta upp, vilka presenterades i avsnitt 3.1.3. Under det tredje mötet (den 18 februari 2014) diskuterades val av scenario och alternativen industriella informations- och styrsystem/vatten och sjukvård/läkemedelsförsörjning föreslogs. Här beslutades att det steg i händelseutvecklingen som är av störst vikt för val av scenario var vilken typ av verksamhet som drabbades. Andra aspekter i detta val hade kunnat vara typ av inledande händelse, karaktärsdrag hos cyber- och informationssäkerhetsområdet, drabbade funktioner eller drabbade skyddsvärden.

Parallellt med att utredningen av området genomfördes påbörjades del 2, bakgrundsbeskrivningarna. Del 3, utveckling av själva scenarierna vidtog först då de två scenarioförslagen hade beslutats.

FOI har under en längre tid studerat hot mot industriella kontrollsystem och då främst industriella informations- och styrsystem, bland annat inom Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3). Inom ramen för dessa studier har studiebesök genomförts på vattenreningsverk i Linköpings omgivningar men även andra närmare Stockholm.

Med stöd av deltagare från NCS3 genomfördes en idékläckningssession i syfte att ta fram ett par möjliga scenarier vilka har som mål att påverka vattenförsörjningen, vilket ligger till grund för föreliggande vatten-scenario.

För scenariot inom sjukvården utfördes ett förarbete genom att först genomföra intervjuer med apotek, personal inom ordinationsverktyget PASCAL, två sjuksköterskor inom kommunal hemtjänst samt sjukhus. Kontakter togs med Region Halland med anledning av att de drabbades av en liknande händelse under 2012-2013. Vid ett möte med MSB den 29 april 2014 framkom dock att detta scenario inte var lämpligt att slutföra (se argumentation i kap 1.2) varpå utvecklingen stoppades.

3 Bakgrund

Säkerhet kan beskrivas på flera sätt och med olika syften. Vissa begrepp är tämligen etablerade såsom informationssäkerhet och IT-säkerhet. Andra begrepp, såsom cybersäkerhet, har inte riktigt mognat ännu. Vare sig begreppen är etablerade eller ej används de bitvis slentrianmässigt vilket gör att skillnaden mellan dem kan vara otydlig.

Informationssäkerhet[3] är en övergripande beskrivning av åtgärder som vidtas för att skydda information. På en övergripande nivå tas ingen hänsyn till vilken form informationen har, det vill säga om den är tryckt på papper eller i digital form på en lagringsenhet. Informationssäkerhet beskrivs som teknisk och administrativ.

IT-säkerhet[4] är en delmängd av informationssäkerhet och utgör den tekniska säkerheten som skyddar datorer och kommunikation.

En cybermiljö och tillhörande cybersäkerhet är ett nytillskott i begreppsfloran. Cybermiljön är den virtuella miljö som skapas mellan IT-system och användare och där information skapas, utbyts och lagras. Internet är en del (en komponent) av cybermiljön, men där internet fokuserar på teknik genom protokoll och standarder fokuserar cybermiljön på att hantera processer, informationsutbyten, sociala kontexter och policyer.[5] Transaktioner eller sociala utbyten som tidigare skedde i den fysiska världen, men som nu kan ske i den virtuella cybermiljön påverkar hur nutida och framtida verksamheter kommer att genomföras. Cybersäkerhet syftar således till att skydda den del av en organisations verksamhet som bedrivs med stöd av IT-system och i en virtuell värld.

Inom informationssäkerhet brukar begreppen *konfidentialitet*, *riktighet* och *tillgänglighet* användas som grundpelare i diskussioner kring informationshantering och vad som är skyddsvärt. Denna samling har sedermera byggts på med fler aspekter, exempelvis *spårbarhet*, men det är de tre förstnämnda som är de grundläggande och beskriver olika aspekter som data bör skyddas[6]. *Konfidentialitet* beskriver att man försöker behålla en informationsmängd hemlig på så sätt att den endast kan tillgodogöras av den som har rätt att tillgodogöra sig den. Detta uppnås vanligen via olika former av kryptering där behöriga personer förses med rätt ”nycklar”. *Riktighet* syftar till att säkerställa att information, som t.ex. skickas mellan personer eller system, inte kan ändras längs resans gång utan att det upptäcks. Meddelandet ska helt enkelt inte kunna förvanskas hur som helst utan att man märker detta. För att uppnå detta används vanligen, även här vissa aspekter av krypteringsalgoritmer. *Tillgänglighet*, handlar om att informationen ska finnas tillgänglig när den behövs. Om vi exempelvis har informationen på våra servrar, men inte kommer åt den för att kunna göra bokslutet i tid, kan man säga att vi inte har fullgod tillgänglighet.

3.1 Typhändelsens karaktär

I nationell risk- och förmågebedömning finns målsättningen att de scenarier som analyseras dels är representativa för den aktuella typhändelsen (t.ex. storm, skred, översvämning), dels är så pass allvarliga att de är av nationell relevans. Urvalskriterier för detta har bland annat varit att händelsen direkt orsakar att 30 eller fler personer omkommer eller blir allvarligt skadade eller sjuka, att händelsen medför direkta kostnader i storleksordningen med kostnaderna efter stormen Per (750 miljoner kronor) eller att politiska eller sociala konsekvenser upplevs som allvarliga.

[3] Swedish Standards Institute (SIS) (2007). Terminologi för informationssäkerhet (SIS Handbok 550). Utgåva 3, Stockholm: SIS Förlag AB. (Samma terminologireferens som används i t.ex. MSB:s rapport “Samhällets informationssäkerhet, Nationell handlingsplan 2012, Publ.nr: MSB423 - augusti 2012)

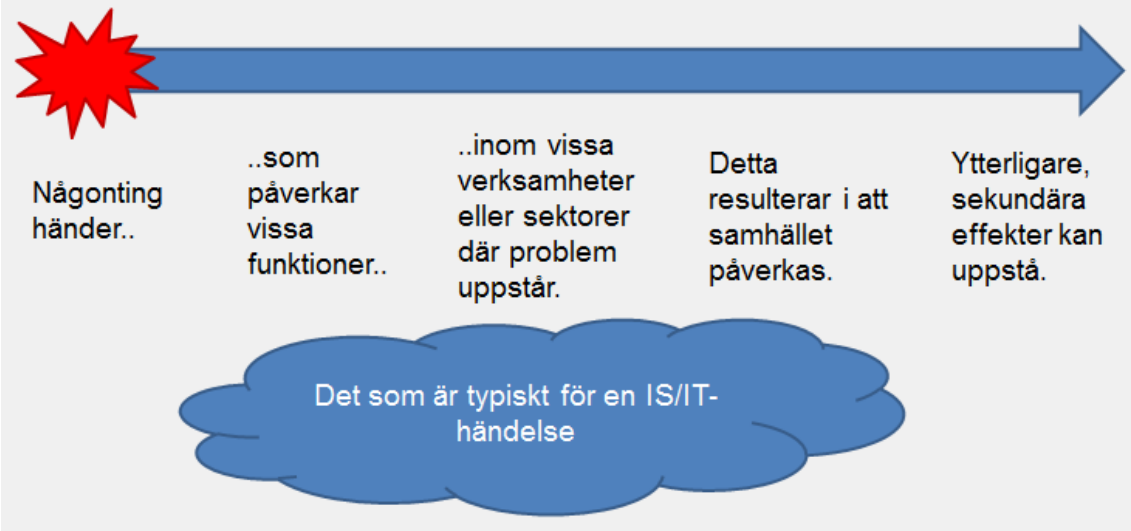
[4] Ibid.

[5] McConnell, M. (2011). The Road to Cyberpower – Seizing Opportunity While Managing Risk in the Digital Age. Booz Allen Hamilton. http://www.boozallen.com/media/file/road-to-cyberpower.pdf [2013-13-10]

[6] Swedish Standards Institute (SIS) (2007). Terminologi för informationssäkerhet (SIS Handbok 550). Utgåva 3, Stockholm: SIS Förlag AB.

För området cyber- och informationssäkerhet går det inte att finna enbart en händelse som kan representera hela riskområdet, eftersom det inte kan beskrivas i så begränsade termer. En haltande jämförelse kan vara att försöka hitta *en* händelse som är representativ för området naturolyckor. Det låter sig inte göras då karaktären av till exempel en storm och ett skred är helt olika. Detta konstaterades redan tidigt i arbetet. Med syfte att välja *två* representativa scenarier som både uppfyller de syften som NRFB ställer och möjligheten för MSB att använda dem även i andra sammanhang genomfördes en mötesserie tillsammans med MSB:s verksamhet för samhällets informations- och cybersäkerhet. Svårigheten ligger bland annat i att själva området är så pass stort och brett, helhetsbilden över hur beroendena egentligen ser ut är bristfällig med mera.

Projektet valde att beskriva scenarierna på ett förenklat linjärt sätt. Någonting sker, en olycka eller en attack, som påverkar funktioner, till exempel tillgängligheten till verksamhetssystem eller riktigheten i data. Detta i sin tur påverkar huvudsakligen en eller flera verksamheter eller sektorer. Följderna i verksamheterna påverkar sedan samhället i flera led. Se skiss i Figur 1, nedan. Arbetet inleddes med att kartlägga vad som karakteriserar området, vilket beskrivs i nästa avsnitt.



Figur 1: Förenklad skiss över en informations- eller cybersäkerhetshändelse, där brister i antingen tillgänglighet, konfidentialitet, riktighet eller spårbarhet ger effekter på samhället.

3.1.1 Vad karakteriserar området informations- och cybersäkerhet?

Med syfte att kunna göra ett intressant val av scenarier som på olika sätt representerar de utmaningar som är kännetecknande för, eller karakteriserar, området informations- och cybersäkerhet har en övergripande kartläggning av vad som kännetecknar detta område genomförts tillsammans med MSB. Aspekterna behöver inte nödvändigtvis vara unika för området, men utgör karaktärsdrag som kan ses som typiska.

Det första karaktärsdraget är den *utbredda användningen* av IT-stöd i de flesta verksamheter idag. *Beroendet* av att dessa stöd fungerar oavbrutet ser olika ut i verksamheterna, men störningar leder i de flesta fall till markant nedsatt effektivitet, om det över huvud taget går att fortsätta verksamheten. I princip alla verksamheter använder IT-stöd i någon form, i vissa fall utan att de själva kanske reflekterar över det (t.ex. i passerkort/dörrar).

Beroendet av IT kan beskrivas som *komplext*, eftersom det är svårt att på förhand beskriva de exakta beroendena. Det kan vara sektorsöverskridande i meningen att konsekvenser snabbt kan sprida sig till andra sektorer än där felet först uppstod. Ett fel i en verksamhet kan sprida sig till en annan verksamhet utan att någon i förväg ens anade att det fanns en koppling dem emellan.

Tidsaspekten är också viktig. En störning kan momentant uppstå på flera ställen samtidigt och spridas mycket snabbt, beroende på vad som har skett. Effekten av en händelse (till exempel skadlig kod eller

virus) kan också vara mycket fördröjd, något som bland annat ökar svårigheten att identifiera vad det var som hade hänt. En händelse kan ha sitt ursprung i ett fel som har funnits under en lång period. Det kan även vara svårt att upptäcka var det egentliga felet befinner sig (man kanske bara ser konsekvenser som byggs upp). Det finns kanske inte en direkt koppling mellan angreppets tidpunkt och effekten av angreppet. Tidsfördröjningen kan därmed göra det svårt att identifiera när, var och hur angreppet har skett. Tiden för händelsen kan också styra hur stora konsekvenserna blir. Vissa tider på dygnet eller året kan känsligheten vara högre eller lägre.

Det finns en logik i hur fel sprids och uppstår, men att förstå denna kräver mycket god kunskap om systemen och hur information lagras. Det uppfattas dock av de flesta som att det *till synes inte finns någon tids- och rumsmässig koppling* mellan de fel som har uppstått och konsekvenserna av dem i samhället. Detta eftersom den geografiska kopplingen mellan IT-systemen och verksamheten som de stödjer suddas ut ju mer tjänster som outsourcas och till exempel lagras i så kallade molntjänster. ”Produktionen” och ”konsumtionen” av IT-tjänster behöver inte vara på samma plats, och kan också vara separerat mellan olika organisationer. Även olika lagrum kan gälla i olika delar av en systemkedja.

Systemen är komplexa och skiktade, de kan komma från olika leverantörer och hopkoppling sker av olika system/program. Man kan i många fall till och med prata om system av system där komplexiteten blir ytterst svåröverskådlig. Ett *fåtal aktörer (om ens några) kan ha total överblick* över dessa komplexa system, vilket gör det svårt att bedöma konsekvenserna av incidenter.

Ett annat karaktärsdrag är den grad av komplexitet som finns inom systemen och själva tekniken. Takten i *teknikutvecklingen är snabb*, vilket bland annat innebär att det redan kan finnas verktyg för att utnyttja en sårbarhet innan folk får så kallade ”patchar”[7] på plats. En angripare kan studera en patch och bygga ett verktyg som angriper den sårbarhet som patchen skall fixa, innan den har hunnit införas brett. Detta drabbar system med dåliga eller inga uppdateringsrutiner. Den snabba teknikutvecklingen innebär också att sättet som vi använder oss av tekniken utvecklas snabbt och kan ge upphov till nya sårbarheter eller eliminera gamla.

Kunskapsnivån är generellt relativt låg hos de många användare som använder IT-stöd i sin vardag. Graden av specialisering är hög hos dem som har kunskapen. Ytterligare en aspekt är att de verktyg som finns tillgängliga för användarna är mycket kraftfulla och kan åstadkomma avancerade saker, som kan påverka i flera led och på många platser. Vi kan göra en förenklad jämförelse med en samhällsviktig verksamhet som också de flesta är momentant beroende av, nämligen elektricitet. I det fallet är kravet på kunskapen hos den vanliga användaren låg i jämförelse, och det är också begränsat i vilken grad en användare kan interagera med elsystemet: det sträcker sig i princip till att tända och släcka lampor och stoppa i stickkontakter, möjligen byta proppar och säkringar. Få har tillträde till de mer avancerade anläggningar som ställverk, transformatorer eller produktionsanläggningar. När det gäller IT så har de flesta användarna tillgång till dessa *kraftfulla verktyg*, och om kunskapen finns (eller inte finns) så kan användarens handlingar medföra stora konsekvenser. Detta sammantaget gör att det finns ett relativt stort utrymme för människan att göra fel.

Riskerna inom området kan betraktas om *abstrakta*, i och med att det kan vara svårt att förstå riskerna med det man gör när det är så komplext och kunskapskrävande. Utfallet kanske inte heller kommer direkt eller i tydlig form, vilket spär på den abstrakta egenskapen.

Området informations- och cybersäkerhet kan ses som relativt *omoget* för en stor del av befolkningen och användarna. Exempel på detta är att det saknas standarder, många företag ser inte IT som en ledningsfråga, man är inte helt överens om olika begrepp och hur de används. Inom företag och organisationer där IT-stödfunktionen är perifer i förhållande till kärnverksamheten kan olika mål för verksamheterna utvecklas.

IT-system och informationen däri exponeras idag mot omvärlden i större utsträckning då den finns i digital form istället för i pappersform, eller genom att system (t.ex. styr- och reglersystem) som tidigare har varit helt isolerade ansluts för fjärrstyrning via internet. Tappade så kallade USB-minnen, glömda eller slutna

[7] Patch = Mindre justering/uppdatering som ofta täpper till och lagar upptäckta fel i systemet

datorer m.m. innehåller mycket information. Likaså kan slarvig (möjligen på grund av okunskap) informationshantering i publika servrar ge en ofrivillig exponering.

Redan efter denna översiktliga och svepande beskrivning av karakteristiska drag för området cyber- och informationssäkerhet kan vi inse att det är svårt att finna ett eller två scenarier som är representativa för området. Aspekterna utgör också en utmaning för att analysen.

Figur 2 nedan syftar till att kartlägga de ovan nämnda utmaningarna och vi har också inordnat dem i två ”kluster”. Klustren är ett sätt att sortera karakteristiken i två områden av aspekter som på något sätt hör ihop.

Figur 2: Översikt av karaktärsdrag hos cyber- och informationssäkerhetsområdet.

Dessa beskrivna karaktärsdrag hos området cyber- och informationssäkerhet skulle kunna användas som utgångspunkt för att välja intressanta scenarier.

3.1.2 Vad skulle kunna hända?

För att få upp exempel på inledande händelser som har ett icke-antagonistiskt ursprung genomfördes en brainstorming-övning tillsammans med verksamheten för informations- och cybersäkerhet på MSB. Detta resulterade i en lista med exempel. Listan är sorterad, utan vidare bearbetning, efter olika teman i tabellen nedan.

Skadlig kod	**Trasig hårdvara**	**Identitet**
Spritt utbrett skadlig kod. Skadlig kod inne på Svenska Kraftnät via VPN-tunnel hemifrån. (VPN – Virtual Private Network)	Tunnelbygge under hus ger vibrationer och trasig hårdvara. Trasig router orsakar bortfall av koppling till Länskommunikations-	Grundläggande personuppgifter blandas ihop vid byte av server på Skatteverket. Kryptobankcertifikat information kommer ut vilket leder till att all

	centralen och numret 11414. Kretskort i utrustning i flygledartorn går sönder och flyget står stilla. Trasig styrdator sänker inomhus temperatur på äldreboende. Bugg i populär applattform (eg. webbserver). ”Centraliserade” system med ev. felaktiga program. Stora konsekvenser för till exempel Statens Service Center.	certifiering är värdelös. Certifikat till polisens WAN går ut. Nätet går ner och närpolisen blir utan kontakt till centrala system. (WAN – Wide Area Network)
Förtroenderelaterat Människor tappar förtroende för att lämna [person]-uppgifter på grund av dålig sekretess eller fel utnyttjande av data. Ingen åtkomst till journalsystem.	**Kommunikationsförlust** Grundstruktur störning, t.ex. DNS. (DNS – Domain Name System) Kommunikationsbortfall på kärnkraftverk leder till produktionsstopp. Internetkabeln under östersjön slits av. Övervakningssystem slås ut. Fysiska låssystem slås ut. .se försvinner. Rakelproblem. Fel i larmkanal, till exempel MiniCall eller SOS alarm.	**Misstag** Oavsiktligt raderande av uppgifter. Systadmin glömmer laptop med okrypterade konton på buss. Tappat/glömt dator/minne på offentlig plats. Sammankoppling av system på grund av okunskap, till exempel SCADA. Användare mejlar till en lista istället för en person. Hemliga uppgifter kommer ut. Felkonfigurerad sniffer orsakar överbelastning av internetlina (ofrivillig DOS). (DOS – Denial of Service) Oavsiktlig överbelastning på grund av hysteri. Utslagen dricka i telefonistbord. Företagsväxel slutar fungera. Uppgradering av nätverk hos ISP går fel. Företag står utan nät. (ISP – Internet Service Provider) Uppdatering av mjukvara slår ut administratörssystem. Lång omstart. Centralt uppdateringsfel, t.ex. Microsoft Update.
Server Brand i datahall, saneringsbehov. Översvämning i datahall.	**Kabel/fiber** Spikar på elnätet slår ut lagring i datahall/SAN (Storage Area Network).	**Dataförlust** Grundläggande personuppgifter och bankuppgifter försvinner på grund av serverbyte och dålig

Brandssläckningsutrustning i datahall slår sönder hårddiskar på grund av ljud vid utläsning av gas. Fel i lagringsnät. Ett serverrum i X ”brinner upp” och tillgång till (ekonomiska) system går ner. Polisbeslag av annan hostingkund hos samma leverantör.	Solstorm slår ut elektronik. Avgrävd kabel. Skred i exempelvis Göta Älvdalen leder avslitna kablar	back-up.
Tid Tillgång till riktig tid slås ut. Störsändare slår ut tidssynk på Stockholm vatten.	**Underhåll** Dieselgenerator startar inte på grund av dåliga underhållsruntiner och projektering. Stillastående styrsystem stoppar vattentillgången på Karolinska sjukhuset. Avsaknad av kritisk komponent under pågående naturkatastrof, t.ex. askmoln.	**Nyckelperson/-kompetens** Odokumenterat system blir stillastående. Trafikolycka drabbar systemadministratör som dör.

Dessa exempel har använts som inspiration till scenarierna och visar också på spridningen i vad som kan leda till avbrott eller ställa till problem. De inledande händelserna är i denna tabell både av olika karaktär (interna fel, misstag, yttre omständigheter) och på olika systemnivå (att riktig tid slås ut är på hög systemnivå, medan serverproblem kan vara både hög och låg systemnivå).

3.1.3 Drabbade sektorer

Även om ett av karaktärsdragen hos problem som uppstår inom cyber och informationssäkerhet är att det inte alls behöver stanna inom en enda organisation eller ens samma sektor så behöver vi av praktiska skäl för att underlätta analysen göra vissa avgränsningar. En sådan blir att välja vilken sektor som scenarierna främst ska utspelas inom. Följande sektorer och motiv har under arbetet förts på tal:

Skydd och säkerhet/kriminalvården – eftersom det är ett relativt outforskat område. Vad skulle hända om inte häktessystemet var åtkomligt, skulle man behöva släppa folk? Vad skulle hända om man behöver utrymma exempelvis Hall? Möjliga utmaningar är att det ställer stora säkerhetsmässiga krav, leder till oro hos allmänheten, att integritetsfrågor uppstår, med mera.

Offentlig förvaltning, kommunal IT-drift och molntjänster – ett högintressant område eftersom kunskapsnivån om hur det ser ut generellt är låg både hos aktörer och hos MSB. Kommunerna själva kan ha bra kunskap men begränsade resurser att hantera långvariga incidenter. Det skulle kunna leda till konsekvenser för enskilda individer genom problem med socialbidrag och för omsorgstagare. Användningen av molntjänster är svåröverblickbar.

Kommunalteknisk försörjning, vatten – intressant eftersom vatten är ett grundläggande behov och om detta inte fungerar blir konsekvenserna snabbt besvärliga. Tidigare incidenter (ej cyberhändelser) i Östersund och Skellefteå har visat på sårbarheten. Systemet är tidskritiskt och problem får relativt snabb effekt. Konsekvenser slår främst mot människor, djur och miljö. Det skulle kunna drabba flödet eller handla om kontaminering.

Utslaget GSM-nät – att utreda konsekvenser av att GSM-nätet är totalt utslaget vore intressant med bakgrund av hur utbredd användningen är. Det används i många fall till annat än bara telefonsamtal, till exempel larm. Det är helt beroende av el.

Finanssystemet – vore intressant att analysera på grund av det tydliga momentana kraven på tillgänglighet, riktighet, spårbarhet och konfidentialitet. Problem skulle snabbt leda till förtroendekriser. Dock sker analyser i andra fora och vi konstaterar att området inte är högst prioriterat att analysera inom NRFB.

Livsmedelsförsörjning – eftersom livsmedel också hör till våra grundläggande behov skulle det vara intressant att analysera närmare. Problem här skulle också till viss del drabba sjukvård.

Hälsa och sjukvård – en analys inom denna sektor vore intressant eftersom kunskapsnivån avseende IT generellt är relativt låg. Storskaliga systembyggen pågår för närvarande. Det sker mycket incidenter, hanteringen måste vara snabb och all data måste hanteras varsamt för att skydda den personliga integriteten. Förtroendet från kunderna/patienterna är mycket viktigt.

3.1.4 Antagonistiska händelser

I det ena scenariot som vi har utvecklat är en angripare inblandad. I detta avsnitt beskriver vi kort hur vi ser på olika typer av antagonister utifrån vilken förmåga den har.

Angriparen har tidigare ofta beskrivits efter motiv eller metod. Inte sällan har vi bilden av en ensam men mycket kompetent angripare som agerar för utmaningens skull men som inte har något direkt mål efter det att ett intrång lyckats. En annan vanlig bild är politiskt motiverade angrepp. Angrepp mot företag och andra organisationer är idag en organiserad verksamhet. Drivkraften kan vara politisk, så kallad hacktivism, men lika gärna driven av ekonomisk vinst genom cyberbrottslighet. Till detta kommer även nationer eller nationellt sponsrade hackinggrupper vilka agerar för en nations intressen, så kallade (eng.) Advanced Persistent Threat, APT. Hackinggrupper är cybervärldens legoknektar vilket gör att de även kan arbeta för kriminella grupper.

Vad som motiverar en angripare har betydelse när en riskanalys genomförs men för syftet med den här rapporten är kanske en angripares förmåga mer intressant. Defence Science Board,[8] en del av Amerikanska Department of Defence, kom 2013 ut med en rapport där angripare delades in efter förmågor snarare än efter motivation. Lite förenklad kan förmågorna för en angripare delas in i:

- angripare som kan utnyttja kända svagheter i IT-system,
- angripare som på egen hand kan identifiera svagheter,
- samt angripare som kan skapa svagheter i IT-system under tillverkningen.

I och med att det finns hackinggrupper med hög kompetens som går att hyra och att stora kluster av fjärrstyrda datorer (eng. Bot net) går att hyra för riktade överbelastningsattacker (eng. Distributed Denial-of-Service Attack, DDOS attack) är inte motivet det som kanske främst styr hur ett system skyddas. Det är i den här kontexten mer intressant att identifiera vad som krävs av en angripare för att denne rimligtvis skall lyckas med ett angrepp.

Ett grundläggande skydd med en effektiv uppdateringsrutin skapar goda förutsättningar för skydd mot angrepp som inte är riktade. En dedikerad angripare som riktar in sig mot en specifik organisation eller verksamhet är dock svårare att hindra. En angripare som kan identifiera och utnyttja svagheter i organisationens IT-system som tidigare inte har varit kända (eng. Zero-Days Vulnerabilities) är mycket svår att upptäcka med statiska skyddsfunktioner.

[8] Defense Science Board (2013). Resilient Military Systems and the Advanced Cyber Threat. Department of Defense. Washington: DOD.

3.2 Tidigare inträffade händelser

Avseende incidenter i Sverige där kritisk infrastruktur har angripits finns det inte så många rapporterade incidenter, och än så länge finns det inga rapporter om angripna industriella informations- och styrsystem där systemet missbrukats. Däremot finns rapporter om *intrång* i sådana system, men där angriparen nöjt sig med den bedriften. Det här visar på att industriella informations- och styrsystem innehåller svagheter som en angripare kan utnyttja. Än så länge har det dock inte uppkommit en situation i Sverige där en angripare kan tjäna pengar på ett angrepp eller är motiverad att störa samhällsfunktioner för att få frihet att göra ett annat angrepp på samhället. Ett känt angrepp mot samhällsfunktioner, om än inte mot ett industriellt informations- och styrsystem, är angreppet mot Logicas stordatorer 2012 där 16 GB data stals. Logica (nuvarande CGI) levererar outsourcingtjänster till bland annat Skatteverket och Kronofogden.[9]

Det enda rapporterade cyberangreppet som har inträffat i Sverige är ett angrepp mot en webbapplikation vilken styrde värmeinställningen i 700 hushåll och ett affärscenter i Motala. Under en natt 2010 sänkte en angripare temperaturen i dessa hus men angreppet uppmärksammades på morgonen och ingen kom till skada. Flertalet husägare märkte aldrig av angreppet.[10]

Det kan finnas flera möjliga orsaker till att mängden rapporterade angrepp är så lågt. För det första kan det vara svårt att avgöra vad som är ett angrepp och vad som bara är naturliga fel i systemen. Spionage och stöld av uppgifter behöver inte lämna tydliga spår efter sig. Det blir tydligare om en angripare vill styra eller förstöra de system som angrips men en sådan situation har ännu inte uppstått. En annan möjlighet kan vara att det i Sverige inte finns någon lag som tvingar myndigheter och organisationer att anmäla cyberangrepp mot kritisk infrastruktur, något som exempelvis finns i de flesta stater i USA.

Olika typer av informations- och cybersäkerhetsrelaterade incidenter sker varje år. Följande incidenter är ett historiskt axplock av incidenter relaterat till sjukvårdssektorn, som belyser potentiella konsekvenser av att en incident sker i tillräcklig skala, vid ”fel” tidpunkt och hos ”fel” aktör.

Feldosering av läkemedel

I region Halland upptäcktes april 2013 att patienter fått felaktig medicin förskriven. Denna händelse blev möjlig på grund av ett fel i det datoriserade systemet för läkarnas medicinförskrivning. Felet upptäcktes i ett antal fall av apoteken som uppmärksammade att något inte stämde med föregående förskrivningar. I andra fall har patienterna själva reagerat på felaktiga styrkor av medicinerna (jämfört med vad de brukade få). Det visade sig att felet uppstått redan i december 2012, och alltså var i effekt under tre till fyra månader. Ingen kom till skada, men felet i procedurer och teknik var ändå anmärkningsvärt[11].

Kvinna allvarligt sjuk efter datorfel

Från *It i vården*: ”Kvinnan kom akut till Skånes universitetssjukhus i Lund efter att ha fallit och fått en bäckenfraktur. När hon efter några dagar fick komma hem överfördes hennes medicinlista automatiskt från den läkemedelsmodul som ligger i journalsystemet från Siemens. Men vid överföringen inträffade ett tekniskt fel som innebar att doseringen av den medicin som hon ordinerats för en reumatisk sjukdom och som påverkar cellerna och immunförsvaret föll bort. I stället för att få den en gång i veckan som ordinerat fick hon den därför varje dag. Efter en vecka var hon akut sjuk och det har krävts lång vårdtid innan hon nu uppges vara återställd.”[12]

Denna incident är av principiellt viktig karaktär då den pekar både på möjligheterna till teknikfel och möjligheterna till procedurfel. Båda delarna kan inträffa och då ge allvarliga konsekvenser.

[9] Ryberg, J. (2013). *Så hackades Logica*. Computer Sweden, 29 april: http://computersweden.idg.se/2.2683/1.505012/sa-hackades-logica [2014-06-16]
[10] Baltzer, H. (2010). *Värmesystemet hackades via webben*. Computer Sweden, 15 december 2010: http://www.idg.se/2.1085/1.359447/varmesystemet-hackades-via-webben [2014-06-16]
[11] Sveriges Radio, P4 Halland, ” Patienter har fått fel dos läkemedel”
[12] It i vården, ”Kvinna allvarligt sjuk efter datorfel”, 2013-10-17

Nytt system med kraftigt nedsatt förmåga

Sommaren 2012 ersattes ordinationsverktyget e-Dos med det nya systemet PASCAL i den svenska sjukvården. Systemet hade under den första tiden stora problem med prestanda och användarvänlighet likväl som ändamålsenlighet och beskrevs i negativa ordalag. Läkare och annan personal på vissa håll hade svårigheter att logga in, och de som väl lyckades logga in fann snart att systemet var svårjobbat och krångligt. Upplevelsen av ett system som minst av allt hade den prestanda och funktionalitet som behövdes uppmärksammades bl.a. av Socialstyrelsen som genomförde en tillsyn och manade berörda vårdgivare till skärpt beredskap och observans i övergången till Pascal. I ett meddelandeblad skrev Socialstyrelsen ” Socialstyrelsen vill genom detta meddelande uppmärksamma vårdgivare med flera att vidta åtgärder vid läkemedelshantering med ordinationsverktyget Pascal, så att inte patientsäkerheten hotas. Socialstyrelsen har uppmärksammat riskerna i och med att verktyget Pascal för dos-dispensering av läkemedel, har införts. I takt med införandet har lex Maria-anmälningar och klagomål kommit till Socialstyrelsen.”[13]

Störningar hos leverantör av IT-drift

Från sammanfattningen av MSB:s studie *Reflektioner kring samhällets skydd och beredskap vid allvarliga it-incidenter*[14]: ”Fredagen den 25e november 2011 drabbades it-driftleverantören Tieto av ett tekniskt fel, vilket kom att få direkta konsekvenser för cirka 50 av företagets kunder inom såväl privat som offentlig sektor. Konsekvenserna varierade kraftigt. Vissa kunder kom lindrigt undan, med enstaka funktioner utslagna under några dagar. De värst drabbade saknade i princip möjlighet att använda sina IT-lösningar under flera veckor. Konsekvenserna av driftstörningen hade nationell spridning, var tvärsektoriell och drabbade i flera fall samhällsviktiga verksamheter. Effekterna höll i sig i flera månader.”

På kort tid slutade ett stort antal servrar fungera som de skulle. Driftstörningen drabbade flera olika, varav vissa samhällsviktiga, sektorer och hade spridning över hela landet. Exempel på drabbade aktörer är Apoteket, Bilprovningen och Nacka kommun. Detta scenario belyser i hög grad de aspekter som är kännetecknande för IT- och cyberområdet, exempelvis geografisk obundenhet i sin spridning och effekt, snabb effekt och osäkerhet i om och när man är tillbaks i normal drift efter en incident.

Region Skåne drabbas av virus

I januari 2009 drabbades Region Skånes intranät av ett virusangrepp. Det var ett så pass nytt virus så att det slank igenom befintliga skydd. Viruset infekterade snabbt ca 10 000 datorer och ca 500 servrar. I samband med att nätverket blev obrukbart föll även andra funktioner bort så som centralenheten i intensivvårds-övervakningen, möjligheten att läsa och skicka remisser, diagnostik- och laboratoriedatorer, medicinteknisk utrustning. Sammantaget ledde detta till att undersökningar och behandlingar blev inställda och försenade. Arbetet med att rensa datorutrustning och återställa funktionalitet pågick under flera veckor, fram till den 26 mars[15].

I takt med att all funktion inom sjukvården, precis som överallt annars, blir allt mer ”internetiserad” ökar de potentiella konsekvenserna vid störningar. Detta kräver ordentlig beredskap på både teknisk och administrativ nivå. Som exempel på konsekvenser vid störningar i vården kan nämnas, förutom möjlig risk för skada på person, merarbete för vårdpersonal. Båda dessa effekter kan innebära signifikanta kostnader i flera led.

3.3 Varför är det relevant att analysera informations- och cybersäkerhet inom NRFB?

Stora mängder av information hanteras i många delar av samhället och det sker i allt större utsträckning integrerat i IT-system. Tillgång till funktioner som stödjer sig på IT-system genomsyrar allt mer av vårt

[13] Socialstyrelsen, Meddelandeblad Nr 7/2012, Juni 2012.
[14] MSB, Reflektioner kring samhällets skydd och beredskap vid allvarliga it-incidenter,
[15] Socialstyrelsen, Kamedo-rapport 96, IT-Haverier i vården

dagliga liv, från det att vi drar vårt busskort i spärren, till att vi mailar kollegorna på arbetet, till att vi får snabb korrekt vård på sjukhuset. Inom organisationer sker många processer med stöd av verksamhets-system som sköter exempelvis mail, löner och åtkomst till olika typer av information på intranät. Dessutom har många verksamheter specifika system som monitorerar och styr fysiska processer så som exempelvis i kärnkraftverk, blandning av djurfoder, koordinering av flygtrafik och hantering av dricksvatten. Till detta kommer många system som används direkt för att kunna leverera den produkt som verksamheten producerar (produkt i detta sammanhang kan vara allt från myndighetsspecifik service till medborgarna via webben och digitalt ID till bankomater).

Utvecklingen på senare tid handlar mycket om uppkoppling av systemen mot internet. Tillgång till att kunna hantera system via internet erbjuder ofta förenklingar och kostnadsbesparingar i verksamheter. Man kan helt enkelt göra samma jobb billigare och bättre i och med utvecklingen. Samtidigt sker en parallell utveckling där fler aktörer väljer att fokusera på sin kärnverksamhet och överlämna stödverksamheten att drivas av andra. Ett typiskt exempel på detta är när organisationer outsourcar sin IT-drift till en utomstående aktör. Dessa driftsaktörer får ofta bättre skalfördelar ju mer drift de kan koncentrera till samma plats.

Egenskaperna ”mer uppkopplad informationsinfrastruktur” och ”koncentrering av driften” erbjuder var för sig, och i ännu större grad i kombination, större och fler möjliga sårbarheter och konsekvenser vid eventuellt inträffat fel jämfört med tidigare. Än mer än tidigare av den samhällsservice som vi erbjuds är beroende av fungerande IT-system i botten. Med ökande grad av centralisering, ökande grad av beroende av att systemen fungerar och ökande komplexitet i de beroenden som återfinns systemen emellan är det relevant att analysera vad för händelser och konsekvenser vi kan ställas inför.

När något i systemen går fel, vare sig det handlar om avbrott (tillgänglighet) eller felaktig data (riktighet alternativt integritet), blir det av vikt att ha fungerande rutiner både för den manuella hanteringen av verksamheten och för hur man går över till manuell hantering. Med ett IT-stöd som hjälper organisationer att få mer gjort med färre anställda kan konsekvenserna snabbt bli tunga när stödet försvinner.

Utöver tanken på hur de IT-system som vi i vardagen förlitar oss på handlar cyber- och informations-säkerhet om informationshanteringen generellt i samhället. Det är lätt att vid en analys rikta fokus mot de system som hanterar informationen, men det kan vara mer intressant att snarare ställa frågan hur *bristen på*, eller *felaktigheten i informationen* kan påverka oss i vardagen. Detta oavsett vilket IT-system som havererar, eller om problemet grundas i någon annan form av bristande informationshantering.

I analysen kommer vi att utgå från de nämnda principerna tillgänglighet, riktighet, konfidentialitet och spårbarhet för att exemplifiera vad som kan hända och vilken typ av problem det kan leda till. Detta beskrevs kort i avsnitt 1.3.

4 Förslag till sannolikhetsbedömning

Inom NRFB har beslut fattats att inte göra sannolikhetsbedömningar på antagonistiska händelser. När det gäller icke-antagonistiska hot kan man ibland studera tidigare händelser för att hitta data att bygga en sannolikhetsbedömning på. Beroende på vilken typ av scenario som väljs i slutändan kommer mer eller mindre data att finnas tillgänglig för en sådan bedömning. Om tillgänglig data inte erbjuder tillräckligt med information för att göra en tillräckligt säker bedömning så får andra metoder undersökas (till exempel expertbedömningar.).

Avseende sjukvårdsscenariot finns det ett antal påverkande faktorer som gör en sannolikhetsbedömning utmanande. För det första är scenariot inte färdigställt. Men det är inte den mest problematiska aspekten. Scenariot har en ”mänsklig” komponent, att folk agerar på vissa sätt (missar att upptäcka det fel som uppstår, samt missar att kontrollera läkemedel enligt rutin med mera). Detta är svårt att sätta en sannolikhet på. Det man erfarenhetsmässigt kan säga med god säkerhet är att inom alla områden där människor är med och påverkar (både konstruerar och hanterar systemen) kommer man att uppleva att saker går snett. Tittar man på hela cyberdomänen kan man tänka sig att det alltid kan gå snett någonstans, men exakt vad som går snett, och var, vet man inte. (Denna aspekt framkom tydligt under scenarioutvecklingen.)

Båda scenarierna är teknikbaserade (bygger på fel, eller intrång, i IT-baserade system). Givet att teknikutvecklingen skulle stå helt still skulle man kunna lägga fram en hypotes att ett liknande scenario inträffar åtminstone en gång per hundra år, och troligen en gång per tio år. Teknikutvecklingen står dock inte still, och om tio år kanske tekniken används på ett idag totalt oförutsett sätt, med nya problem och lösningar.

Slutligen kommer analysen inte att fokusera enbart på något av dessa scenarier, varför det blir ointressant att i detta läge göra en bedömning av sannolikheten för scenariot.

4.1 Beredskapsläge

Sannolikheten för att något ska inträffa och också ge konsekvenser i samhället påverkas på något sätt av hur medvetna människor är om risken och huruvida förberedande eller förebyggande åtgärder genomförs. Detta avsnitt syftar till att ge en bild av om det finns en ”allmän medvetenhet” för riskområdet generellt.

Avseende hela informations- och cybersäkerhetsområdet kan vi inte svara fullödigt på detta. Det kan vara på sin plats att påpeka att informationssäkerhet är ett relativt oreglerat område, alla organisationer har egna behov och intressen som styr nivån på säkerheten.

MSB ska enligt sin instruktion stödja och samordna arbetet med samhällets informationssäkerhet. I det ingår att lämna råd och stöd till andra statliga myndigheter, kommuner och landsting samt företag och organisationer, avseende förebyggande arbete. MSB ska också analysera och bedöma omvärldsutveck-lingen inom området, rapportera till regeringen om förhållanden på informationssäkerhetsområdet som kan leda till behov av åtgärder inom olika nivåer och områden i samhället.[16] MSB har en Nationell operativ samverkansfunktion för informationssäkerhet (NOS) som aktiveras vid allvarliga informations-säkerhetshändelser.

Såsom nämns i inledningen till vatten-scenariot nedan är vanan att skydda sig mot olyckor betydligt större än att skydda sig mot riktade attacker, vilket gör att det kan finnas industriella informations- och styrsystem som har brister i säkerheten samtidigt som de är dåligt övervakade.

[16] Förordning (2010:1901) med instruktion för Myndigheten för samhällsskydd och beredskap 11 a §

4.2 Förmåga att förebygga och förbereda

Avsnittet är tänkt att beskriva specifika aktiviteter som görs för att stärka förmågan att förebygga och förbereda. Denna sammanställning är inte på något sätt täckande med avseende på detta. MSB:s verksamhet för samhällets informations- och cybersäkerhet ansvarar för en nationell funktion för stöd till samhället i arbetet med att hantera och förebygga it-incidenter. Detta sker bland annat genom att sprida information, samordna åtgärder och medverka i det arbete som krävs för att avhjälpa eller lindra effekter av en händelse. Samverkan sker med andra myndigheter med särskilt ansvar inom informationssäkerhetsområdet.[17]

Vid MSB finns Sveriges nationella CSIRT (Computer Security Incident Response Team), CERT-SE. CERT-SE har till uppgift att stödja samhället i arbetet med att hantera och förebygga IT-incidenter. CERT-SE ska bland annat agera skyndsamt vid inträffade IT-incidenter genom att sprida information samt vid behov arbeta med samordning av åtgärder och medverka i arbete som krävs för att avhjälpa eller lindra effekter av det inträffade. Man ska samverka med myndigheter med särskilda uppgifter inom informationssäkerhetsområdet och vara Sveriges kontaktpunkt gentemot motsvarande funktioner i andra länder samt utveckla samarbetet och informationsutbytet med dessa.[18]

Grunden för att behålla en hög säkerhet i informationssystem är att fortlöpande driva detta arbete. MSB ger stöd till organisationer och företag, bland annat genom broschyren *Vägledning till ökad säkerhet i industriella kontrollsystem*.[19]

För att öka förmågan att förebygga och hantera allvarliga it-incidenter krävs det att alla aktörer i samhället, på alla ansvarsnivåer, ökar sin förmåga.[20]

[17] Förordning (2010:1901) med instruktion för Myndigheten för samhällsskydd och beredskap 11 a §
[18] www.cert.se/om-cert-ce
[19] MSB Vägledning till ökad säkerhet i industriella kontrollsystem
[20] MSB (2013) *Risk och sårbarhetsanalys samt förmågebedömning 2013 – Redovisning enligt förordningen (2006:942) om krisberedskap och höjd beredskap* Diarienummer: 2013-2891 (2013-11-05)

5 Inledande konsekvenskartläggning

5.1 Samhällssektorer/skyddsvärden som kan tänkas påverkas

Avseende det antagonistiska ingreppet mot reningsverk handlar de huvudsakliga konsekvenserna om en nedsatt funktionalitet i samhället på grund av att många människor kommer att drabbas av magbesvär. Om trycket i friskvattenledningarna sjunker så lågt att föroreningar dyker upp i ledningarna tar det lång tid till det att ett fullgott vatten kan garanteras. Fram till dess kommer invånarna, när väl trycket är återställt, att få koka sitt dricksvatten. Denna hantering är både kostsam och sänker effektiviteten i processer som är beroende av friskt vatten. Att händelsen är antagonistisk medför också en ökad oro bland kommun-invånarna.

Scenariot som drabbar sjukvården medför inledningsvis stora osäkerheter innan det står klart vari problem-et ligger. Även då de första misstankarna fattas är det svårt att överblicka vidden av problemet. Här förvänt-as konsekvenserna drabba människors liv och hälsa. Både direkt genom den felmedicinering som sker, och förmodligen under den tid som sker när felet identifieras och arbetsbördan växer på grund av tidsfördröj-ningar och att man måste använda manuella rutiner. Rädslan för felmedicinering när problemet blir känt kan leda till att människor undviker att ta sina mediciner, vilket kan ge ännu värre medicinska följder.

I båda fallen drabbas man av att effektiviteten i de normala processerna minskar då man inte kan förlita sig på IT-systemen som vanligt. Hanteringen av detta kan bli kostsam. Det är svårt att uppskatta kostnader för nedsatt effektivitet, men även denna torde vara betydande. Scenarierna kan också leda till att förtroendet för systemet och/eller aktören påverkas, vilket kan få långtgående effekter.

5.2 Vad är mest relevant för analysen att utreda vidare?

Som nämndes i avsnitt 1.2 förespråkar vi ett bredare angreppssätt än att fokusera på ett enskilt scenario vad gäller analys av cyber inom NRFB. Analysen skulle kunna ge ett antal korta exempelscenarier för att visa på bredden i hur cyber- och informationssäkerhetsrelaterade händelser kan drabba samhället. För att undvika fällan att fokusera analysen i allt för hög utsträckning på de befintliga IT-stöden och istället rikta ljuset på informationen och informationshanteringen i sig bör analysen kan utgå från de centrala principerna tillgänglighet, riktighet, konfidentialitet och spårbarhet. Riskidentifieringen i avsnitt 3.1.2 bör fördjupas och kopplas till vilken typ av problem med informationshanteringen som det kan leda till.

Sjukvårdsscenariot belyser ett antal faktorer som kan anses vara generella för IT-stödd verksamhet. Oavsett vilken specifik bransch man befinner sig i blir följande faktorer relevanta att beakta vid scenario som utgår från fel i systemstöden. Förmågor kopplat till hantering av ett problem i informationshanteringen skulle kunna diskuteras med utgångspunkt i de frågeställningar som ges i tabellen nedan.

Upptäckt	**Övergång till manuella rutiner**	**Uthållighet i manuella rutinerna**
Hur sker upptäckt?	Hur sker detta?	Hur länge kan man hålla ut?
När?	Har det övats?	Hur tungt blir det?
Varför?	Vet folk hur detta ska göras?	Effekter på övriga samhället?
Var?	Hur lång tid tar övergång till manuella rutiner?	Tillförs förstärkningsresurser?
Hur rapporteras/eskaleras detta vidare i organisationen, och ut från organisationen?	Hur lång tid tar eskaleringen?	
	Vad hinner hända under eskaleringsfasen?	

6 Referenser

6.1 Tryckt material

Defense Science Board (2013). *Resilient Military Systems and the Advanced Cyber Threat*. Department of Defense. Washington: DOD

Förordning (2010:1901) med instruktion för Myndigheten för samhällsskydd och beredskap

MSB (2009) *Vägledning till ökad säkerhet i industriella kontrollsystem* MSB 0049-09

MSB (2012a) *Reflektioner kring samhällets skydd och beredskap vid allvarliga it-incidenter – En studie av konsekvenserna i samhället efter driftstörningen hos Tieto i november 2011* MSB 367-12

MSB (2012b) *Samhällets informationssäkerhet, Nationell handlingsplan 2012*, Publ.nr: MSB423 - augusti 2012

MSB (2013a) *Övergripande utmaningar för samhällsskydd och beredskap – Analys av fem scenarier om samhället år 2031* Publikation MSB 563

MSB (2013b) *Risk och sårbarhetsanalys samt förmågebedömning 2013 – Redovisning enligt förordningen (2006:942) om krisberedskap och höjd beredskap* Diarienummer: 2013-2891 (2013-11-05)

Socialstyrelsen, Kamedo-rapport 96, *IT-Haverier i vården*

Swedish Standards Institute (SIS) (2007). *Terminologi för informationssäkerhet* (SIS Handbok 550). Utgåva 3, Stockholm: SIS Förlag AB.

6.2 Internet, dagspress och radio

Socialstyrelsen, Meddelandeblad Nr 7/2012, Juni 2012. http://www.socialstyrelsen.se/Lists/Artikelkatalog/Attachments/18788/2012-6-61.pdf [2014-04-15]

Sveriges radio Halland, Patienter har fått fel dos läkemedel, 19 april 2013: http://sverigesradio.se/sida/artikel.aspx?programid=128&artikel=5509856&playaudio=4526656 [2014-04-15]

Lindström, K *Kvinna allvarligt sjuk efter datorfel.* It i vården, 17 oktober 2013: http://itivarden.idg.se/2.2898/1.528494/kvinna-allvarligt-sjuk-efter-datorfel [2014-04-15]

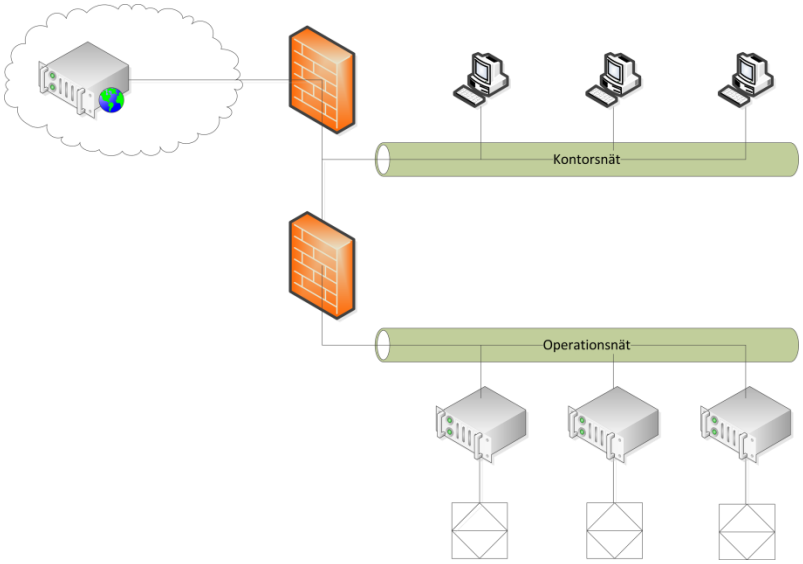
McConnell, M. (2011). *The Road to Cyberpower – Seizing Opportunity While Managing Risk in the Digital Age*. Booz Allen Hamilton. http://www.boozallen.com/media/file/road-to-cyberpower.pdf [2013-12-10]

Baltzer, H. (2010). *Värmesystemet hackades via webben*. Computer Sweden, 15 december 2010: http://www.idg.se/2.1085/1.359447/varmesystemet-hackades-via-webben [2014-06-16]

Bilaga 1: Scenario industriella informations- och styrsystem för vattenrening

SCADA-system (Supervisory Control And Data Acquisition) är en form av industriella kontrollsystem (eng. Industrial Control System, ICS). SCADA-system används för att fjärrstyra automatiserade system, exempelvis vattenreningsverk och elproduktion. Tidiga system var isolerade, även om de var fjärrstyrda, från omvärlden i den betydelsen att de kommunicerade över telefonledningar och med unika övervaknings-system.

Genom moderniseringar samt ett ökat intresse att kunna få statusrapporter från kontrollsystemen till datorer i kontorsmiljö har kontrollsystem kopplats ihop med vanliga datorsystem, exempelvis internetanslutna kontorssystem. Den här sammankopplingen har öppnat upp för möjligheter att angripa styrsystem ifrån vanliga datorsystem. Figur 3 visar en generisk bild av ett sammankopplat system.

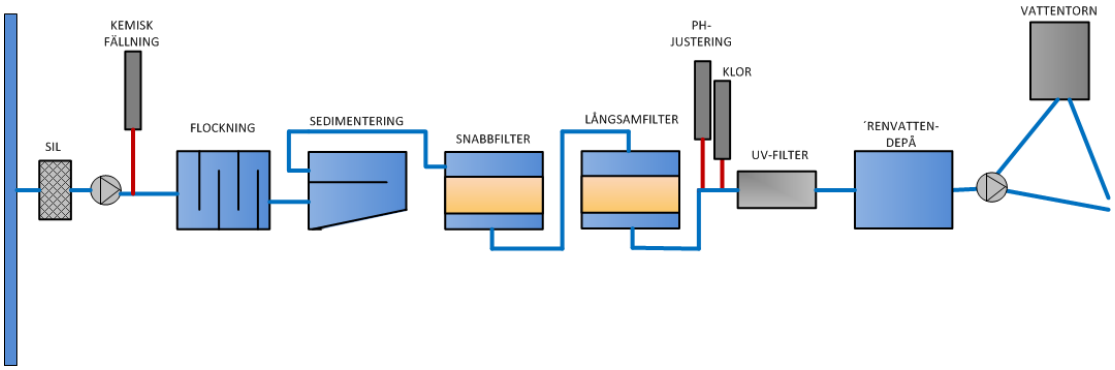


Figur 3: Exempelbild vattenverk med ett sammankopplat kontors och operationsnät.

Flertalet anläggningar som kontrolleras av industriella kontrollsystem utgör kritisk infrastruktur. Det gör anläggningarna till mer intressanta mål för de som vill påverka samhällets möjlighet att fungera.

Säkerhetsfunktioner kan beskrivas med syfte att skydda användarna från olycksrelaterade skador (eng. safety) alternativt med syftet att skydda systemen eller det systemen innehåller från en medveten angripare (eng. security). Industriella kontrollsystem har flera säkerhetsfunktioner inbyggda i sig men de flesta av dessa funktioner är till för att förhindra olyckor. Skydd mot en medveten angripare är något som är eftersatt då det tidigare inte har varit en sannolik hotbild. Typiska skydd utgörs av varningsmeddelanden i form av varningstexter eller varningssignaler. Dessa är bra för att uppmärksamma en användare att något är på väg att gå fel, men har ingen hindrande förmåga mot en medveten angripare.

Det är vanligt att en kommun endast har en vattenreningsanläggning för att täcka kommunens behov. I större städer kan det finnas fler anläggningar men dessa täcker behoven för avgränsade delar av staden. Detta innebär att det sällan finns total redundans om anläggningen skulle råka ut för problem vilket gör vattenreningsförmågan till en sårbar resurs.



Figur 4: Generisk vy av ett vattenreningsverk.

6.3 Geografi

Ett modernt vattenreningsverk är en anläggning som ofta är automatiserad och fjärrstyrd (Figur 4). Automationen gör att det inte behöver finnas fast personal på plats då övervakningen kan ske från en annan plats. Om ett larm kommer från vattenverket kan en beredskaps- eller en jourstyrka skickas till anläggningen. En sådan styrka är sannolikt inte tränad på att hantera ett medvetet cyberangrepp.

Scenariot har inte specificerat kommun, utan beskriver ett generellt förlopp, som avslutas med hotet om att flera kommuner kan komma att drabbas av en liknande attack. En förutsättning är att det är en kommun som inte har så bra redundans, exempelvis genom att den har flera vattenreningsverk.

6.4 Tidpunkt

Vattenreningsverket angrips under högsommaren, efter en period som har varit varm och torr. Effekten av angreppet kan komma att bli större på grund av en högre vattenkonsumtion till följd av det varma vädret.

Angreppet genomförs under kvälls- och nattetid. Även om vattenreningsverket normalt är obemannat är beredskapen lägst utanför kontorstid och det tar längre tid att reagera på eventuella larm. Ett angrepp under semestertider kan även medföra att kritisk personal kan vara ledig och svår att nå.

Angreppet mot filterbassängerna tar tid och ger synliga bevis på att något är fel. På bemannade anläggningar kan detta upptäckas genom att personalen observerar bassängerna. Om ett sådant angrepp sker i början av helgen kan ändå bassängerna få tid på sig att fyllas utan att någon upptäcker detta.

6.5 Händelseförlopp

X är en kriminell organisation vilken är under hård press från samhället. Under det senaste året har polisen genomfört en riktad aktion mot X i syfte att förstöra organisationen. Efter ett antal större tillslag har flera av X:s ledare gripits och inväntar nu rättegång. De kvarvarande inom X beslutar sig för att hämnas mot samhället som helhet, vilka de anser vara skyldiga till polisens agerande.

Det finns viss vana inom X att genomföra angrepp mot IT-system, till exempel att angripa webbservrar i syfte att publicera politiska meddelanden på företags eller myndigheters webbsidor. Ambitionen med X:s hämndaktion är dock högre den här gången, varvid de kontaktar en fristående hackinggrupp för att kunna genomföra ett mer tekniskt avancerat angrepp. Målet för X är att få alla att lida ”på samma sätt som de har lidit”. Tillsammans med hackinggruppen utarbetar de en plan där stadens vattenverk ska angripas med målsättningen att skapa kaos genom allmän spridning av magsjuka, för att sedan med en kampanj på nätsidor utöva påtryckning mot samhället.

Hackinggruppen påbörjar genast den underrättelsefas som föregår ett angrepp. Genom att studera öppna källor, såsom offentliga handlingar, tidningar, fora och specifikationer från tillverkare av IT- och kontrollsystem, skapar de sig en god uppfattning över hur vattenverket är uppbyggt. Hackinggruppen har viss förmåga att analysera de system som de skall angripa och identifiera svagheter men vänder sig ändå till egna kontakter och anonyma fora för att söka efter kunskap om hittills okända sårbarheter. De är framgångsrika och kommer över en opublicerad sårbarhet vilken kan möjliggöra kontroll över enskilda vattenpumpar av den sort som används inom vattenverket.

Hackinggruppen har identifierat ett antal anställda på vattenverket och lyckats få dem att svara på designade mejl med länkar till preparerade webbsidor. När den anställde besöker dessa webbsidor laddas programvara ner till den anställdes dator. Med denna programvara kan sedan hackinggruppen etablera en kanal in på vattenverkets kontorsnät.

Vid det här laget är hackinggruppen och X redo att inleda sitt angrepp mot vattenverket. Själva vattenverket är i stort automatiserat vilket gör att det endast är bemannat under vissa tider och då främst normal arbetstid under veckodagarna. För att få så mycket tid på sig som möjligt innan en upptäckt kan ske av en förbipasserande beslutar sig hackinggruppen för att inleda sitt angrepp sent en fredagskväll. De har då minst två och ett halvt dygn på sig innan någon förväntas komma tillbaka. Vid det här laget har hackinggruppen redan tagit sig in i de system som kommunicerar med pumpsystemen i vattenverket. Det första hackinggruppen gör är att angripa den larmserver som tar emot felmeddelanden från anläggningens kontrollsystem och förmedlar dessa vidare till en larmcentral. Genom att angripa larmservern isoleras anläggningen från omgivningen och angriparna kan arbeta ostört en längre tid. Angreppet fortsätter därefter med att hackinggruppen slår ut de pumpar som trycksätter det utgående vattenledningssystemet. Vattenpumparna kontrolleras av ett styrsystem (eng. Programmable Logic Controller, PLC) vilka i sin tur kontrolleras av ett industriellt kontrollsystem. Hackinggruppen skriver över den befintliga konfigurationen över hur vattenpumparna skall fungera och använder därefter det verktyg som de har tillverkat och som utnyttjar den okända svagheten i pumpsystemet. Verktyget möjliggör för vattenpumparna att gå på maximalt varvtal, för att därefter snabbt stanna och sedan gå upp på max igen. Förhoppningen från angriparnas sida är att snabba tryckförändringar skall skada distributionsnätet och därmed förorena vattnet däri. Målet med denna del av angreppet är att få trycket i vattenledningsnätet som går ut till allmänheten att sjunka. I normalfallet hålls detta nät med ett övertryck i syfte att hindra smuts och annat att komma in i vattnet genom sprickor. Genom att sänka trycket kommer föroreningar att spridas i hela nätet och det tar lång tid att återställa nätet så att man med säkerhet kan säga att vattnet är rent igen.

Nästa steg i anfallsplanen är att angripa det kontrollsystem som styr pumparna. Detta angrepp är ett komplement till det första angreppet. Angriparna raderar de konfigurationsfiler som styr hur pumparna skall arbeta från SCADA-servern och försätter sedan servern ur funktion genom att förstöra systemfiler. Avstängda pumpar och raderad styrprogramvara går att återställa men det tar tid och måste göras manuellt.

Avslutningsvis utförs ett angrepp mot vattenflödet i början av reningsprocessen. Genom att stänga av vattenflödet från den långsamma reningsbassängen kommer denna att fyllas på och svämmas över. Det är inte ovanligt att styr- och filtersystem för denna del av processen är placerade under bassängen då anläggningen försöker behålla så mycket självfall som möjligt i vattenflödet. För den här anläggningen är dessutom långsamfiltret placerat inomhus vilket gör att den höjda vattennivån inte kan uppmärksammas av en tillfälligt förbipasserande. När bassängen har fyllts kommer vattnet att svämma över och söka sig till den lägsta punkten. Då blir filterrummet och vägarna dit den lägsta punkten, med följden att dessa utrymmen vattenfylls. Sannolikt kommer då även kortslutningar att uppstå i de elektroniska systemen. Detta angrepp har en lägre sannolikhet att lyckas då det tar längre tid och har därmed en högre sannolikhet för upptäckt. Om angreppet är framgångsrikt kommer det dock att ta längre tid att dränera kontrollrummet samt ersätta utrustningen.

Angreppets olika faser tar sannolikt inte särskilt lång tid att genomföra, förutsatt att hackinggruppens förarbete har varit bra. Förhoppningen från angriparnas sida är att angreppet inte skall upptäckas förrän effekten i form av förorenat vatten upptäcks av vanliga användare.

Kommunen har i samband med automatiseringen av flera anläggningar outsourcat övervakningsfunktionen till ett vaktbolag. Vaktbolagets uppgift är att ta emot larm och skicka en väktare som undersöker den lokala larmcentralen. Under själva angreppet märker de inte av något i och med att rapporteringen inte skiljer sig från vad de väntar sig. Framåt lördagsmorgonen börjar det dock komma in samtal från kunder om att vattnet är brunt och att det smakar konstigt. Vaktbolaget kan inte se någon anledning till detta på sina larmsystem men skickar ut en väktare för att undersöka saken på plats.

En timme senare är väktaren på plats på vattenreningsverket. Väktaren kan dock inte se några fel då den lokala larmcentralen inte visar på några fel. Angreppet mot larmservern har fungerat som angriparna avsåg. Vid det här laget har fler anmälningar om dåligt vatten inkommit till larmcentralen så man beslutar att ringa upp en tekniker på kommunen enligt en förutbestämd larmlista. Teknikern undersöker statusen på vattenreningsverket via sin dator hemma men ser inget annorlunda än vad larmcentralent och väktaren tidigare har sett. Teknikern beslutar sig för att ge sig av till vattenreningsverket för att undersöka problemet på plats.

Väl på plats kontrollerar teknikern larmcentralen men finner inget konstigt där. Istället beslutar sig teknikern för att gå igenom alla kontrollplatser och ger sig av på en patrullrunda. Först beger sig teknikern till de pumpar som ser till att trycket i friskvattennätet hålls uppe. Teknikern upptäcker snabbt att pumparna inte är igång men lyckas inte återstarta dem heller. Efter ytterligare undersökning konstaterar teknikern att styrsystemet är ”tomt”; hårdvaran verkar okej och det finns ström, men det finns ingen mjukvara som reagerar vid uppstart eller på reglage och knapptryckningar. Den här typen av fel ligger utanför den normala kompetensbilden för tekniker så kommunen får beställa en driftsingenjör från leverantören av kontrollsystemet.

I väntan på att en driftsingenjör skall komma patrullerar teknikern av resten av anläggningen. När teknikern kommer in i byggnaden med snabbfilter upptäcker teknikern att vattennivån har stigit så mycket att bassängen har börjat svämma över. Teknikern beger sig genast ner i kontrollrummet under bassängen och finner även dessa pumpar avstängda. För att få stopp på tillflödet stänger teknikern av tillförseln av nytt vatten och provar sedan att öppna flödet från bassängen in i reningsverket. Styrsystemet för denna del av reningsverket verkar fungera utan problem men då vattnet inte har någonstans att ta vägen stänger teknikern av flödet igen. I och med att tillflödet är spärrat kan vattennivån inte stiga mer och överskottet kan hanteras, men det är inte lika akut.

Strax efter att lokalradion har gått ut med vattenverkets begäran om att koka dricksvattnet börjar organisation X proklamera över egna webbsidor, Twitter och nyheternas kommentatorfält att de har stängt av reningsverket och att detta är en inledande hämndaktion mot samhället. Om inte X:s medlemmar friges kommer fler liknande angrepp mot samhället att ske, inte bara inom en stad utan i flera där X har förgreningar.

Fram till nu har ingen orsak till felen varit uppenbart. Flödet från bassängen var ”bara” avstängt, liksom pumparna i slutänden av reningsverket. Även om detta inte är normalt så verkar de dock fungera som de ska. Mer svårförklarligt är mjukvarufelet i kontrollsystemet för pumparna.

Tillverkarens driftingenjör anländer till reningsverket några timmar senare och bekräftar att pumparna verkar okej men att styrsystemet för dem inte fungerar. Efter en undersökning konstateras att programvaran verkar vara där men att konfigurationen, det vill säga hur programmet skall arbeta, verkar saknas. Det går dock inte ännu med säkerhet att säga om pumparna är opåverkade eftersom styrprogrammet måste fungera för att en fullständig teknisk diagnos skall gå att genomföra. Grundinstallation av mjukvara är ingenting som brukar ske som normal serviceåtgärd vilket gör att ingångsättandet ytterligare fördröjs. Driftingenjören blir tvungen att hämta programvara för att kunna installera om styrsystemet. Även andra komponenter behöver ersättas eller installeras om innan systemen kan fungera normalt igen. Detta kommer dock att ta tid då det inte går att genomföra via en fjärranslutning utan måste ske lokalt.

Det står nu klart för kommunen att reningsverket inte kommer att komma igång förrän om tidigast ett par dygn. Via radion har kommunen åter uppmanat befolkningen att koka sitt dricksvatten men även att vara sparsam med vatten i övrigt då de inte vet när produktionen kommer igång igen. Den tidigare uppmaningen via lokalradion fick tillsammans med X:s informationskampanj motsatt effekt då en stor del av

befolkningen genast började lagra vatten i de kärl som de hade tillgängliga. Detta har medfört att trycket sjunkit betydligt mer och snabbare än initialt beräknat.

Det tog ytterligare ett dygn innan reningsverket var igång igen. Vid det här laget hade det låga vattentrycket gjort att otjänligt vatten hade samlats i lokala reservoarer. För att skölja ut dricksvattennätet inklusive lokala reservoarer samt att ersätta dessa med rent vatten uppmanade myndigheterna att invånarna skulle koka sitt vatten i ytterligare en vecka.

6.6 Känslighetsstudie – relevanta variationer på scenariot

Variationer på scenariot kan exempelvis vara vilken tid på året som angreppet genomförs. Vi bedömer att konsekvenserna blir som störst då vattenproblemen uppstår på sommaren under en period då det är torrt och varmt och efterfrågan på vatten är hög.

Scenariot kan varieras till exempel med hur många kommuner som aktionen genomförs i.

Scenariot påverkas i hög grad av hur tekniker och allmänhet reagerar på händelserna, och därmed kan det varieras i oändlighet.

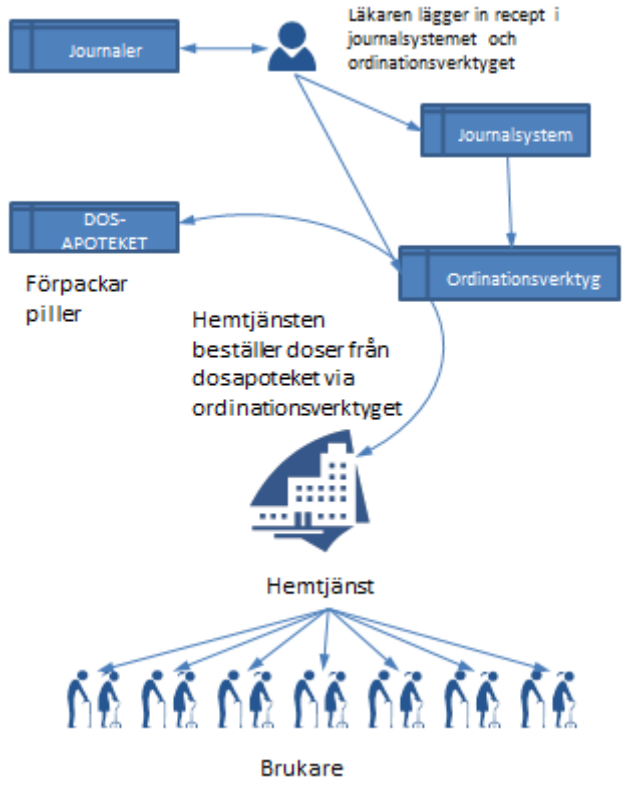
Scenariot kan fortsätta genom att angriparna har förberett för liknande angrepp i ytterligare kommuner, eller ytterligare en gång i samma kommun. Den rigorösa kontroll som måste ske för att ”bli av med” problemet är svår att göra utan att stoppa produktionen under en relativt lång tid, om man inte har redundanta produktionsmiljöer (vilket är ovanligt).

Bilaga 2: Scenario ordinationsverktyg för läkemedel inom sjukvård

Nedan följer ett första utkast till ett scenario som skulle ha kunnat utvecklas inom NRFB. I ett sent skede i arbetet beslutades att inte färdigställa scenariot, följande beskrivning har vi behållit i memot som dokumentation om tråden lyfts igen vid senare tillfälle. Detta är alltså inte att betrakta som en färdig produkt.

Ordinering av doserad medicin till patienter som får sin medicin fördelad i dos-påsar (istället för dosett) sker via ett ordinationsverktyg som används av alla vårdgivare och berör ca tvåhundratusen patienter. Användarna utgörs av sjuksköterskor, läkare och barnmorskor samt andra som ordinerar dospatienter, över femtio tusen användare. Figur 5, nedan, illustrerar hur delarna i kedjan interagerar, från läkare till patient via verktyget och hemtjänst/sjukvård. Läkaren som skriver ut recept interagerar med patienternas journaler samt systemen för att ordinera mediciner. I ett senare skede beställer hemtjänsten mediciner till patienter via ordinationsverktyget. Sjuksköterskan beställer från dosapoteket via verktyget och blir över tid mer och mer beroende av att systemet fungerar som det ska.

Ordinationsverktyget används till vardags av sjuksköterskor i hemtjänsten för att kontrollera brukares läkemedelslistor, för att skriva ut vid-behovsmediciner samt få tillgång till information om olika läkemedel.



Figur 5: Enkel skiss över informationsflödet avseende beställning av dos-förpackade läkemedel. Källa: egen.

6.7 Geografi

De flesta scenarios inom ramen för NRFB är platsbundna på så vis att de är fysiska till sin natur, och även får fysiska effekter där de sker. I detta scenario, som har en cyberkomponent, är konsekvensernas geografiska utbredning beroende på vilka organisationer som i sina verksamhetsprocesser på något sätt är

kopplade till den tjänst som felar. Om felet uppstår hos någon av de tre ”dosfabrikörerna” som servar större städer, med fler patienter, kan konsekvenserna förstås bli större.

6.8 Tidpunkt

Händelsen inträffar under sommaren, då det normalt är större andel vikarier i verksamheten.

6.9 Händelseförlopp

I kommun X njuter människorna av de sista semesterveckorna innan sommaren går mot sitt slut. Inom kommunens olika hemtjänster börjar sommarvikarierna känna sig varma i kläderna efter en turbulent början med många ovana i personalen. De äldre ser fram emot lugnet som kommer att infalla då den ordinarie personalen är tillbaka på plats.

I början av augusti inträffar ett flertal oväntade dödsfall bland kommunens vårdtagare. Detta uppfattas som anmärkningsvärt, men inte konstigt eftersom värmen är påtaglig och dödsfall under sommarmånaderna inget ovanligt. Några av de ordinarie undersköterskorna har dock under den senaste veckan noterat att flera brukare fått försämrat allmäntillstånd och vissa uppvisar anmärkningsvärda beteenden. Inom kommunen börjar den medicinskt ansvariga sjuksköterskan (MAS) att titta närmare på dessa fall för att få en ledtråd till om någonting i vården brister.

Det man inte vet om är att i grannkommunen har flera brukare och undersköterskor lagt märke till att doseringen av läkemedel xxx varit felaktig. Upptäckten har lett till att man gjort en Lex Maria-anmälan och att man börjar dubbelkolla alla mediciner mot medicinlistorna.

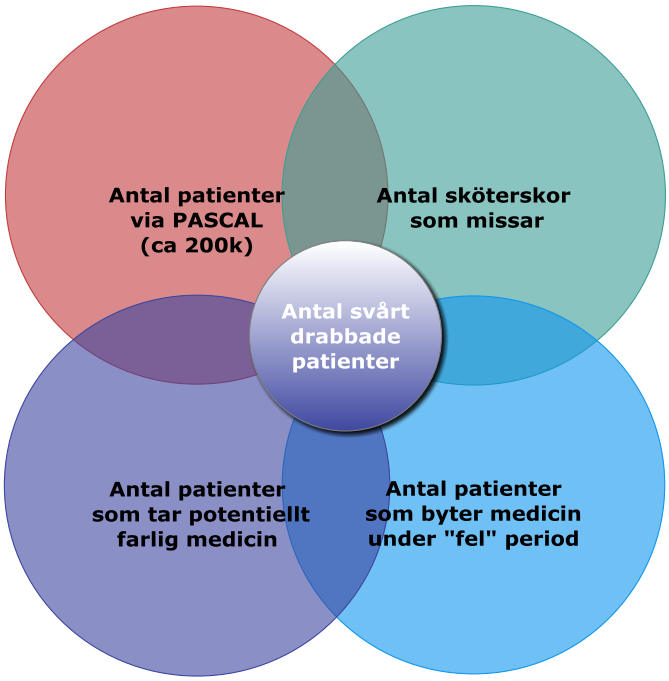
Vid genomgången av ett flertal brukares journaler och medicinlistor ser MAS att något verkar vara fel med antingen journalerna eller doseringarna, eller båda. Antal och typ av piller stämmer med det som står på påsarna men dessa stämmer i sin tur inte med vad som bör vara[21]. Vårdpersonalen får i uppdrag att åka ut till alla brukare och dubbelkolla i deras pärmar, som står hemma hos respektive patient, och ringa in och jämföra historik och doser. Nu uppdagas det att något har gått fel i systemen, och att det inte går att lita på informationen däri överhuvudtaget. Hemtjänstsjukvården larmar de ansvariga för det dosapotek som de tillhör[22] och övergår till manuella rutiner, något man är van vid efter någorlunda återkommande IT-störningar under de senaste åren.

En initial undersökning visar att det troligtvis varit fel i systemen i flera veckor/månader. Den uppdatering av systemet som genomfördes i god tid före semestern medförde inga direkta problem och de initiala testerna visade på att allt var okej, trots vissa komplikationer under uppdateringen. Dock verkar det som ett litet fel har smugit sig in som medfört att korrupta databasposter har orsakat ändringar i ordineringar.

Vad som kan anses vara tur i oturen i detta fall är att andelen svårt drabbade patienter blir förhållandevis liten. De svårt drabbade patienterna i det initiala skedet är de som: 1- får sina läkemedel i dos-påsar, 2- får potentiellt farlig medicin, 3- får ny laddning med medicin under den aktuella perioden, och 4- har en sköterska som missar att kontrollera och/eller kontrollerar men brister i att upptäcka de felaktiga doserna/pillrena. Se figur 6, nedan.

[21] Som ett stöd i tanken kan här alltså anses att parametern ”riktighet”, som tidigare beskrivits, är påverkad.

[22] Varje läns landsting väljer en ”pillerstopparfabrik”. Tre stycken: Apoteket AB, Apotekstjänst, respektive Svensk Dos AB. (Information fån Niklas Franzel, Inerva)



Figur 6: Skiss över förutsättningar för patienter att drabbas svårt av det beskrivna scenariot. Skissen visar att antalet patienter där dessa förutsättningar stämmer bör vara relativt liten. Källa: egen.

Under en lång period blir denna del av sjukvården tvungen att sköta sitt dagliga jobb med manuella rutiner till hjälp. Sjuksköterskor måste konsultera de ordinerande läkarna och kontrollera patienters pärmar ute i fält. Den ökade administrativa bördan innebär i slutändan en risk i sig. Även när verktyget väl är igång igen tar det en lång tid innan de verksamma helt vågar lita på systemet och helt överge sina manuella rutiner. Ingen vågar ge ut medicin om det finns risk att den är potentiellt dödlig. Därför jobbar personal frenetiskt med att säkerställa att allt blir rätt.