dataskydd.net

ORG.NR 802495-4797 – HTTPS://DATASKYDD.NET
– INFO@DATASKYDD.NET

DFRI
Föreningen för digitala fri- och rättigheter

ORG.NR 802461-0852 – HTTPS://WWW.DFRI.SE
– DFRI@DFRI.SE

Dataskydd.net Sverige
Alsnögatan 18
116 41 Stockholm

DFRI
Box 3644
103 59 Stockholm

MOTTAGARE: Enhet L4 Krishantering, osv., Justitiedepartementet, 103 33 Stockholm

# *Remiss på promemorian Tillhandahållande av tekniska sensorsystem – ett sätt att förbättra samhällets informationssäkerhet (Ju2017/02002/L4)*

Föreningen för digitala fri- och rättigheter är en ideell organisation med syfte att att främja digitala fri- och rättigheter och verka mot censur och inskränkning av yttrandefrihet och personlig integritet.[1] Dataskydd.net är en ideell organisation med syfte att verka för informerade beslut om lagstiftning och teknologi i enlighet med de grundläggande rättigheterna till dataskydd och personlig integritet.[2] Detta är ett gemensamt remissyttrande.

Yttrandet börjar med inledande observationer och förslag på åtgärder som Justitiedepartementet och regeringen bör vidta innan de går vidare med förslaget om ett tekniskt sensorsystem. Vi går sedan igenom den bild av effektiviteten, proportionaliteten och ändamålsenligheten av tekniska sensorsystem som framgår av forskning och utifrån andra europeiska länders erfarenheter. Särskild vikt läggs vid promemorians bristfälliga integritetsanalys, men även vid vad som förefaller vara en brist på beredskap hos Myndigheten för samhällsskydd och beredskap att förvalta denna sorts system. Längst ned återfinns en källförteckning, med länkar till webbpublicerat material i de fall detta är aktuellt.

## *Inledning och förslag*

I promemorian föreslås att Myndigheten för samhällsskydd och beredskap (MSB) får rättsligt mandat att tillhandahålla sensorsystem till de organisationer och verksamheter som så begär och efter MSB:s behovsprövning och beslut. Tillhandahållandet innebär att MSB installerar och underhåller utrustningen som behövs, samt bedriver övervakning av ingående och utgående internettrafik hos organisationen ifråga.

Förslaget rymmer inga begränsningar av sådan övervakning, något som är rimligt att förvänta sig för ett sådant system som MSB föreslår. I promemorian upprepas det flera gånger att övervakningen inte kommer att omfatta personuppgifter i någon högre utsträckning, men också att systemet förutsätter att man kan spela in både personuppgifter och kommunikationsinnehåll (så som

[1] https://www.dfri.se/dfri/stadgar/
[2] https://dataskydd.net/om

webbplatser och e-postmeddelanden). Då både metadata och kommunikationsdata kommer att snappas upp, påverkas inte bara de anställda i offentlig sektor utan även medborgare som kontaktar offentlig sektor i det fall att en myndighet väljer att köpa MSB:s lösning. Förslaget rymmer inga krav på insyn eller tillsyn. Förslaget bygger istället på att MSB får full handlingsfrihet.

Föreningen för digitala fri- och rättigheter (DFRI) och dataskydd.net avråder regeringen från att ge MSB föreslagna rättsliga mandat av följande skäl:

1. Inga resultat av nytto- och riskanalyser av sensorsystem presenteras.
2. Säkerhetsvärdet med sensorsystem är inte givet. Effekterna är förenade med osäkerhet och kan till och med vara kontraproduktiva.
3. Hantering av ospecificerade personuppgifter motiveras med att sensorssystem handlar om samhällets säkerhet trots att säkerhetsvärdet är oklart.
4. Säkerhets- och integritetsrisker med lagring av person- organisations- och kommunikationsuppgifter ignoreras, trots att sensorsystem medför risk för misstag, missbruk och dataintrång.
5. Alternativa säkerhetsåtgärder beaktas inte, till exempel offentlig rapportering av incidenter som incitament för ett större egenansvar i säkerhetsarbetet.
6. Insyn och tillsyn är viktig komponent i styrning och ledning av säkerhetsarbetet. Inget nämns om det i promemorian, vilket är särskilt allvarligt då MSB saknar ledningssystem för sitt nationella cybersäkerhetsarbete.

Mot den här bakgrunden rekommenderar DFRI och dataskydd.net en utvärdering av befintliga nationella system för avvikelse- och incidenthantering, samt en utredning av samhällets behov på området. Motiveringarna utvecklas i svaret som följer.

## *Bristande plan för styrning och uppföljning*

Promemorian har sin upprinnelse i betänkandet Informations- och cybersäkerhet i Sverige (SOU 2015:23) där en strategi förslås med följande mål:

*att* stärka styrning och tillsyn inom området,

*att* staten ska ställa tydliga krav vid upphandling på it-området,

*att* statliga myndigheter ska kommunicera säkert,

*att* samtliga statliga myndigheter rapporterar it-incidenter,

*att* arbetet med att förebygga och bekämpa it-relaterad brottslighet stärks och

*att* Sverige ska vara en stark internationell partner.

NISU-utredningen (SOU 2015:23) lägger fram flera förslag, varav två konkreta säkerhetsåtgärder i MSB:s regi, obligatorisk incidentrapportering respektive sensorsystem. Incidentrapportering infördes 1 april 2016 och i den aktuella promemorian föreslås att MSB nu också ges rättsliga mandat att tillhandahålla sensorsystem, dvs. att bedriva övervakning av internettrafik.

Åtgärderna i MSB:s regi föreslås nu genomföras innan regeringens arbete med en nationell strategi för informations- och cybersäkerhet är avslutat, och innan andra frågor om nationell styrning och uppföljning är besvarade. Att införa större operativa funktioner innan den övergripande styrningen är klargjord är en bakvänd ordning som i promemorian motiveras med att MSB anser att sensorsystem är angeläget och bör prioriteras. Ingen närmare förklaring ges.

Det är just denna brist på styrning och uppföljning som påtalats som en allvarlig brist i samhällets arbete med informationssäkerhet.[3]

När det gäller incidentrapportering går det att luta sig mot ett explicit mål i betänkandet (SOU 2015:23). Men det är oklart vilka behov och prioriteringar som vägleder arbetet i praktiken, vems informationsmål, behov och krav som tillgodoses i och med incidentrapporteringen som redan genomförts, och vilka ytterligare behov och prioriteringar, krav och informationsmål man nu vill uppnå genom sensorsystemet.

Ett återkommande argument i promemorian är att säkerhetsändamålet motiverar ett sensorsystem, men det saknas en genomlysning av konsekvenserna av tillämpning av ett sådant system för myndigheternas styrning och uppföljning i fråga om organisations- och personuppgifter, cybervarningar och larm.

## *Utåt- och inåtblick*

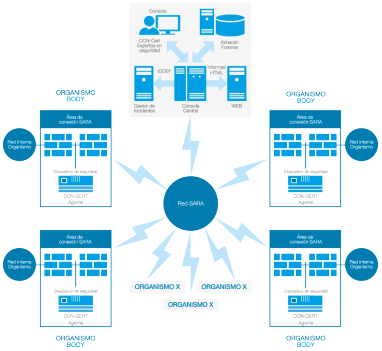
I samband med den första årsrapporten om incidentrapportering framhöll MSB att det förelåg underrapportering, samt att systemet var, för att citera, ”i sin linda”.[4] Det innebär att ett nationellt system har rullats ut trots oklara kriterier för bedömning, rapportering och informationsdelning. Nationella säkerhetsåtgärder forceras utan närmare behovs- och kravanalys, utan att det finns ett tydligt ledningssystem för det nationella informations- och cybersäkerhetsarbetet.

När det gäller promemorian om sensorsystem är nytto- och riskanalyser, mål och effekter än mer oklara. Promemorian lutar sig mot NISU-utredningen (SOU 2015:23) där motiveringarna är av spekulativ karaktär, varav det starkaste argumentet är en internationell reflektion.

> ”*Sverige, till skillnad från sina grannländer Norge, Finland och Danmark saknar i dag nationella sensorsystem kopplade till ansvariga myndigheter. Denna brist på nationella sensorsystem i Sverige innebär med stor sannolikhet att ett stort antal allvarliga it-incidenter aldrig upptäcks, eller upptäcks för sent.*”

Vare sig statistik eller fakta presenteras som underlag. Påståendet att nationella sensorsystem har de effekter som sägs är bara spekulation. Sensorsystems design och funktioner varierar. Gränserna mellan sensorsystem, brandväggar och ”honeypots”, samt mellan system för varningar och incidenthantering mer generellt, är flytande.

I promemorian görs en indelning mellan nationella sensorsystem, till exempel FRA:s TDV, och övriga system (organisationers enskilda system). De nationella sägs vara mer effektiva. Det finns inget som styrker det. Även enskilda organisationer har mer avancerade skydd än traditionella brandväggar. Skillnaden mellan FRA och andra organisationer handlar mer om rättigheter att




*Spanska sensorsystemet SAT-SARA.* I Spanien publicerar CCN-CERT en schematisk bild över vilka sorters interaktioner och kommunikationer som kan fångas upp av CCN-CERT:s varningssystem. Statistiken från SAT-SARA är sekretessklassad, liksom statistiken från den publika motsvarigheten SAT-INET. Även INES-rapporterna, som kontinuerligt utvärderar offentliga ansträngningar på IT-säkerhetsområdet, är otillgängliga för allmänheten. Det gör det svårt att veta om systemen har någon positiv effekt i realiteten.

Bildkälla: https://www.ccn-cert.cni.es/

[3] Riksrevisionen (2016). Informationssäkerhetsarbete på nio myndigheter. RiR 2016:8.

[4] Myndigheten för samhällsskydd och beredskap (pressrelease, 15 mars 2017), Första årsrapporten inlämnad till regeringen om arbetet med allvarliga it-incidenter.

övervaka, snarare än effektivitet. Det sistnämnda är en öppen fråga eftersom systematiska utvärderingar saknas på området. Trots detta sprider myndigheterna uppgifter om ”effektivitet” som liknar mer marknadsföring än utvärdering.

I FRA:s årsrapport (2016) nämns att FRA:s system flaggar 10 000 nätaktiviteter per månad. FRA gick även ut med uppgiften till SVT och andra nyhetsmedier. Inget nämns om nyttan, dvs. om de organisationer och verksamheter som berörs klarar av att hantera dessa aktiviteter själva. Det är oklart om någon aktivitet har inneburit en reell verksamhetsstörning. Siffran ”10 000” är vidare ointressant i sig. Antivirusprogram i vanliga persondatorer hanterar virusdefinitioner i storleksordningen miljoner.

Mot den här bakgrunden bör frågan ställas vad ett sensorsystem i MSB:s regi skulle tillföra utöver det som redan finns hos myndigheter och andra organisationer. Inget konkret går att utläsa från promemorian.

## *Översikt av effektivitetsstudier på varningssystem*

Det finns inga naturliga indelningar av sensorsystem med avseende på deras effektivitet. Nytta och risker är en öppen fråga. Sensorsystem kan bygga på mer eller mindre komplexa signaturer – statiska signaturer, mönsterigenkänning, eller både och. Design och funktioner är avgörande för effektivitet, nytta, kostnader och risker.[5] I vare sig betänkandet (SOU 2015:23) eller promemorian diskuteras det närmare.

Den grundläggande funktionen i sensorsystem är i likhet med brandväggar och andra typer av filter att identifiera skadliga trafikmönster. I praktiken kan sensorsystem vara så ineffektiva att de är kontraproduktiva, genom att falska varningar och larm leder till att organisationen missar riktiga larm.[6]

En av de allvarligaste it-säkerhetsincidenterna i vår tid är dataintrånget i butikskedjan Target i USA i december 2014. Det resulterade i att över 110 miljoner kunder informerades om att deras kontokortsuppgifter inte var säkra och kunde vara i händerna på kriminella.[a] I efterhand har analyser och fallstudier pekat på en rad säkerhetsbrister, ineffektiva sensorsystem är ett av dem, kvalitetsbrister i system och processer för hantering av varningar.[b]

[a] ZDnet (2 februari 2015). Michael Kassner. Anatomy of the Target data breach: Missed opportunities and lessons learned.

[b] Radichel, Teri (2014). Case Study: Critical Controls that Could Have Prevented Target Breach. SANS. US.

I rapporten *The State of Malware Detection & Prevention*[7] uppger två av tre personer med ansvar för it- och säkerhetsfrågor att de tillbringar en stor andel av sin arbetstid på att jaga falska larm och varningar. C:a en av tre uppger att de spenderar en ansenlig del av arbetstiden åt att prioritera olika varningar och larm. En av tre varningar och larm undersöks, varav två av fem visar sig vara falska varningar och larm.

Med andra ord, ineffektiva varningssystem, vare sig de går under namnet sensorsystem eller brandväggar, är inga triviala säkerhetsproblem. Ett dagligt


*Svårtolkad information.* Trots att det finns olika sorters sensorsystem i Polen, Nederländerna, Sverige, Danmark, Finland, Norge, Spanien och Frankrike, saknas det offentligt publicerad information kring vilken nytta sensorsystemen gör. De tar upp utvecklartid, kostar pengar, och är omtyckta i alla fall i vissa EU-länder, men den information som skulle möjliggöra en utvärdering av effektiviteten och ändamålsenligheten med åtgärderna sekretessbeläggs med hänvisning till nationell säkerhet. Från Försvarets radioanstalt har vi fått reda på att de kan detektera över 10 000 nätaktiviteter per månad – en imponerande stor siffra, men inte i sig informativ. En statlig utredning, även en mindre formell sådan som en promemoria, borde göra större ansträngningar att motverka kunskapshålet.

[5] Anderson, R. (2008). Security engineering. John Wiley & Sons.

[6] CSO Online (2 november 2015) Bob Violino. Security tools' effectiveness hampered by false positives.

[7] Ponemon Institute (2016). The State of Malware Detection & Prevention. Report sponsored by Cyphort, independently conducted by Ponemon Institute LLC, US.

flöde av varningar ställer krav på kvalitetssäkrade processer för intern och extern avvikelsehantering. Ändå lyser frågan med sin frånvaro i NISU-utredningen (SOU 2015:23) och i promemorian. Inga kvalitetskrav, risker eller resursbehov diskuteras. Det gäller allt från signaturer till ansvarsfördelningar och samordning mellan MSB och andra samhällsaktörer, till exempel hur varningar och stora mängder inspelat material hanteras inom och mellan organisationer.

## *Uppdrag och tillsyn*

Ett återkommande, generellt argument i promemorian är att MSB:s mandat till övervakning faller inom ramen för MSB:s uppdrag att samordna samhällets informationssäkerhet, att ge lägesbilder, samt behovet av skyddsåtgärder för samhällsviktiga verksamheter. Detta generella argument förutsätter (1) att behov föreligger, (2) att säkerhets- och integritetsrisker är korrekt bedömda, (3) att MSB kan hantera dem, och (4) att det inte finns några bättre lösningar. Behovet är som sagt en öppen fråga. Samtliga punkter behandlas styvmoderligt både i NISU-utredningen (SOU 2015:23) och promemorian.

I promemorian framhålls flera gånger att den internettrafik som ska övervakas och spelas in troligtvis inte är av karaktären känsliga personuppgifter, samtidigt som det framhålls att inget kan uteslutas. Kriterierna för signaturer och trafikövervakning är mycket allmänt och vagt formulerade. Å ena sidan försöker ge sken av att övervakningen av trafikmönster bara handlar om ip-adresser och skadlig kod som signaturer; å andra sidan lämnar det helt öppet vilka signalmönster (signaturer) som i praktiken kan komma att övervakas på olika nivåer av kommunikationsprotokoll, från IP till applikationer. Inte heller har man etablerat någon process för risk- eller konsekvensanalyser, vare sig inför införandet av systemet, under arbetet med systemet eller vid tillämpningen av systemet inne på myndigheten. Mandatet blir i praktiken villkorslöst. Det är anmärkningsvärt. Inte ens FRA är befriade från tillsyn, utan är underställda Datainspektionens och Statens inspektion för försvarsunderrättelseverksamhetens (Siun) tillsynsverksamhet.

**INGEN DATASKYDDSBEDÖMNING**

Inga av de bakomliggande utredningarna kan sägas innefatta en konsekvensbedömning på det sätt som avses i dataskyddsförordningens artikel 35.1.

Förslaget till nationellt sensorsystem innebär att MSB hanterar känsliga uppgifter i form av dels förteckningar över signaturer, dels inspelad trafik till följd av detektion av potentiell eller reell skadlig trafik, ingående eller utgående från samhällsviktiga verksamheter. Promemorian undviker problematisering. Vår bedömning är att risker för misstag, missbruk eller regelrätta attacker på systemet är stora, tillräckligt stora för att inte bortses ifrån.Det innebär enligt vår uppfattning att användandet av sensorsystemet sannolikt kommer att leda till en hög risk för fysiska personers rättigheter och friheter. Det betyder i sin tur att varje ansvarig myndighet enligt dataskyddsförordningens artikel 35.1 innan sensorsystemet börjar användas, måste utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter. Inga av de bakomliggande utredningarna kan sägas innefatta en konsekvensbedömning på det sätt som avses i dataskyddsförordningens artikel 35.1.

I promemorian presenteras ingen intresseavvägning mellan övervakning, säkerhet, integritet och dataskydd. En sådan avvägning bör göras för alla behandlingar där personuppgifter och kommunikation mellan medborgare och myndigheter ingår, både enligt PUL och dataskyddsförordningen.

Ett första steg är att identifiera vilka personuppgifter och vilken kommunikation som ingår. Här nöjer sig förslagsställaren med svepande formuleringar om att personuppgifter bara kommer att hanteras i begränsad utsträckning. Det är emellertid mycket tveksamt om man kan begränsa insamling, behandling och kartläggning av personuppgifter i någon större utsträckning mot bakgrund av att avancerade sensorsystem använder och löpande uppdaterar en stor mängd signaturer och signalmönster i nätverks- och kommunikationsprotokoll på alla nivåer.[8] På grund av osäkerheten kring vad som kan utgöra ett hot och vilken trafik som kan behöva spelas in används normalt statistiska metoder och signaluppgifter i stora mängder och av varierande karaktär.

Signaturer kan vara av många slag, dels IP-adresser eller skadlig kod, dels indikatorer, signaler och signalmönster som i statistisk mening utgör potentiella hot, men som inte nödvändigtvis är reella. Det senare innebär en mer öppen och bred övervakning av internettrafik från och till organisationer, vilket innebär större integritets- och förtroenderisker.[9]

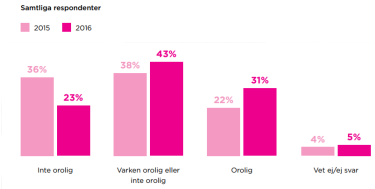
## *Konsekvenser för medborgarna*

Att övervaka innehållet i internettrafiken, till exempel e-post, utgör i princip en dataförlust. En annan aktör än avsändaren och mottagaren tar del av innehållet. Vissa medborgare och konsumenter kan uppfatta sådan övervakning som ett regelrätt dataintrång, något som blir uppenbart när allmänheten får reda på att myndigheter bedriver omfattande övervakning utan deras kännedom, så som blivit känt att till exempel NSA (en av USA:s säkerhetstjänster) gör. Upplevelsen kan påverka medborgarnas öppenhet gentemot myndigheter, det vill säga minskad informationsdelning, så kallade ”chilling effects”.

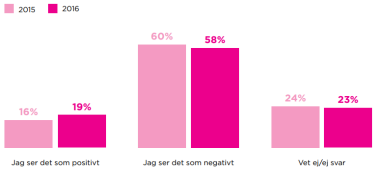
I USA har flera studier inom hälsovårdsområdet styrkt effekter av dataintrång på patienternas öppenhet och informationsdelning gentemot vården.[10] En svensk studie visar även på effekter på medborgarnas förtroende i ett bredare konsumentperspektiv.[11] Sådana förtroendeeffekter kan mycket väl komma att uppstå med sensorsystem i MSB:s regi, till exempel övervakning av internettrafik till och från sjukhus, skolor och andra verksamheter. FRA och svenska staten har hittills klarat sig från allvarliga förtroendekriser, men det är ingen garanti för framtiden.[12] Den årliga enkätundersökningen *Delade meningar*, som senast publicerades i mitten av april 2017, visar till exempel att ”*andelen [svenskar] som svarar att de är oroliga för att ens information används i syften man inte är*

*Attityder till övervakning*. Nedan återges två frågeställningar ur studien *Delade meningar* som ger en fingervisning om hur attityder till övervakning förändras över tid.

1. I VILKEN utsträckning är du orolig för att information som du delar med dig av digitalt används i syften som du inte är bekväm med?




2. SER DU den ökade insamlingen och användandet av personlig digital information i samhället generellt som positivt eller negativt för dig som privatperson?




Källa: *Delade meningar*, 2017.

[8] Johnson, C. W. (september 2015). Barriers to the use of intrusion detection systems in safety-critical applications. In International Conference on Computer Safety, Reliability, and Security (pp. 375-384). Springer International Publishing.

[9] Richards, N. M. (2013). The dangers of surveillance. Harvard Law Review, 126(7), 1934-1965.

[10] *Se* Agaku, I. T., Adisa, A. O., Ayo-Yusuf, O. A., & Connolly, G. N. (2014). Concern about security and privacy, and perceived control over collection and use of health information are related to withholding of health information from healthcare providers. Journal of the American Medical Informatics Association, 21(2), 374-378. *och* Kwon, J., & Johnson, M. E. (2015). The Market Effect of Healthcare Security: Do Patients Care about Data Breaches? Paper presented at the 14th annual Workshop on the Economics of Information Security (WEIS), 22-23 June, 2015.

[11] Wahlund R, Dellham R, Åberg D och Lakomaa E (2016). Anseenderisker och dataskydd. Kapitel 5, utdrag ur Risker och riskhantering i näringsliv och samhälle. Wahlund R (red.) Stockholm School of Economics Institute for Research.

[12] Hugh Eakin (19 januari 2017). The Swedish Kings of Cyberwar. The New York Review of Books.

*bekväm med ökat med nio procentenheter [sedan förra årets undersökning].*"[13] Ökningen av oron inför storskalig informationsdelning är större än ökningen av optimism inför att informationsdelning kan medföra positiva saker.

MSB:s påtänkta sensorsystem innebär potentiellt en kraftig insamling och lagring av känsliga uppgifter om personer och organisationer. Så fort systemet varnar för någon "signatur" kommer trafiken av potentiell relevans att spelas in. I promemorian ges ingen bedömning av omfattningen, men med tanke på den osäkerhet som är förenade med dessa system lär resultatet vara mycket stora informationsmängder. Det ökar riskerna för misstag, missbruk och attacker.

Låt oss illustrera med ett scenario:

> En angripare kan medvetet använda sig av skadliga signaturer för att skapa och sprida falska varningar, kanske med ett botnet, samtidigt som den reella attacken har en ännu ej fastställd signatur och därmed faller utanför sensorsystemets detektionsmöjligheter.

I promemorian nämns att hanteringen av personuppgifter lär bli begränsad. Det är dock bara en bedömning som avser grundläggande signaturer för internettrafik. Den sortens bevakning MSB vill genomföra kan inte vara effektiv om den bara omfattar vilka webbplatser anställda inom en viss samhällsviktig verksamhet besöker, varför övervakningen inte kommer att begränsas till dessa fall. MSB förstår troligen detta, eller ännu värre – förstår inte detta. Det finns alla skäl att tro att inspelat material med mer känsliga organisations- och personuppgifter kommer att användas för att utveckla mer avancerade signaturer.

## *Stora datamängder medför stora säkerhetsrisker*

> "*Neither size nor frequency of data breaches has increased over the past decade.*"
> – Edwards m.fl., 2015.[14]

Den här något överraskande slutsatsen kommer från en forskningsartikel som presenterades på 2015 års konferens *Workshop on the Economics of Information Security*. Slutsatsen bygger på rapportering och offentlig redovisning av dataintrång i USA, där flertalet stater har lagkrav på att organisationer ska rapportera dataintrång och meddela berörda konsumenter. I genomsnitt växer inte redovisade dataintrång i antal eller storlek, trots att den digitala kommunikationen och informationshanteringen växer närmast exponentiellt.

En förklaring är att it-säkerheten generellt blir bättre, men att risken för extrema dataförluster ökar på grund av en kraftig tillväxt och aggregering av datamängder, vars komplexitet och värdeökning innebär nya sårbarheter och risker. Det senare är av relevans för det påtänkta sensorsystemet. Systemet ställs inför allt mer komplexa risker och storskaliga hot, varför även underlaget av signaturer till systemet måste bli allt större.

Risken för dataläckor och förluster, oavsett orsak, växer alltså med datamängd, komplexitet och värdet på informationsmängden ifråga. MSB är inte på något sätt befriade från dessa risker. Samtidigt är det oklart vilken kompetens som MSB har att hantera riskerna med lagring av stora mängder känsliga person-

**TVEKSAM EFFEKTIVITET**

"*Effektiviteten [för ett sensorsystem] är högst tveksam. Idag är internettrafiken till 50% krypterad. För den tänkta målgruppen är den siffran antagligen högre. Enligt förslaget ska sensorer sättas upp på utsidan av brandväggar, men då kommer krypteringen i sig vara effektivitetshämmande. Det finns givetvis tekniska möjligheter att komma runt krypteringen, t.ex. SSL interception. Det används redan idag av ett antal organisationer. Då kan man spela in den dekrypterade trafiken i alla fall.*

– Anonym.

[13] Delade meningar (2017). Insight Intelligence i samarbete med i samarbete med Advokatfirman Lindahl, Svensk Handel, Samsung och Stockholms Läns Landsting, samt SICS Swedish ICT.

[14] Edwards B, Hofmeyr S och Forrest S (2015). Hype and Heavy Tails: A Closer Look at Data Breaches. Forskningspresentation på WEIS 2015.

och organisationsuppgifter, eller stora mängder kommunikationsinnehåll. Det är inget som normalt ligger inom myndighetens ansvarsområde, än mindre inom cybersäkerhetsområdet (CERT-SE). Trots att dessa frågor har en direkt inverkan på samhällets informationssäkerhet beaktas inte behovet av riskhantering i promemorian, till exempel behovet av tillsyn. Positiva effekter av sensorsystem antas på ett närmast naivt sätt uppväga alla tänkbara risker.

Förslagsställare och MSB kan till svars säga att de av sekretesskäl inte kan redogöra för eller diskutera enskilda säkerhetsåtgärder, däribland sensorsystemet och dess effektivitet. Det är ett standardsvar som flera europeiska säkerhetsmyndigheter ger om och när utomstående, medborgare och konsumenter, önskar förklaringar eller motiveringar till övervakning, system, rutiner och resultat. Det är bekvämt att hänvisa till sekretess, men argumentet övertygar inte. Andra länder har visat att det går att vara transparent i frågor om säkerhetsstyrning och brister, att det i viktiga avseenden tjänar säkerheten, snarare än att det skulle vara en risk.

> ”*The point of security breach notification is to avoid all the complexity of setting out in detail how data should be protected; instead it provides incentives for that protection.* [...] *As well as informing the data subjects of a data breach, a central clearing house should be informed as well. This ensures that even the smallest of breaches can be located by the press, by investors, by researchers, and by sector-specific regulators.*”
>
> – Anderson m.fl., 2008.[15]

NISU-utredningen (SOU 2015:23) och promemorian om sensorsystem förbiser inte bara säkerhets- och integritetsrisker med sensorsystem. De förbiser också alternativa lösningar. Istället för ännu ett nationellt system för hemlig övervakning av internettrafik, utöver FRA:s TDV, skulle MSB eller annan myndighet kunna ansvara för insamling och redovisning av offentliga uppgifter om organisationers säkerhetsarbete och incidenter. Offentlig rapportering och redovisning av säkerhetsarbete och incidenter är ett potentiellt styrmedel för säkerhetsarbetet som inte alls utnyttjas i Sverige, men väl i andra länder, inte minst USA.

> ”*There is no evidence that when the California Legislature considered the first Security Breach Notification law, that it envisioned an ”encrypt everything” directive as the result. Yet that appears to have become the industry standard, at least for the foreseeable future.*”
>
> – Thaw, 2014.[16]

Införandet av offentlig rapportering och redovisning av dataintrång har fått flera effekter. En av dem är att det interna operativa säkerhetsarbetet har förbättrats. Ett tydligare ansvarsutkrävande har gett incitament till effektivare säkerhetsåtgärder, till exempel kryptering som närmast har blivit standard, något som inte alls är självklart i Sverige och andra medlemsstater i EU. Det är hög tid att Sverige omprövar sitt närmast reflexmässiga motstånd mot offentlig insyn till tillsyn av it-säkerhetsfrågor. Det förutsätter dock en reell kulturförändring, varför regeringen bör föregå med gott exempel. Istället för att ge MSB mandat

[15] European Network and Information Security Agency (2008). Security Economics and the Internal Market. Författare: Ross Anderson, Rainer Boehme, Richard Clayton, Tyler Moore.

[16] Thaw, David (2014). The Efficacy of Cybersecurity Regulation (October 4, 2013). Georgia State University Law Review, Vol. 30.

till hemlig övervakning bör instruktionen förändras till förmån för krav på offentlig redovisning av säkerhetsarbete och incidenter.

## *Har MSB alls rätt (tekniska och organisatoriska) kompetens?*

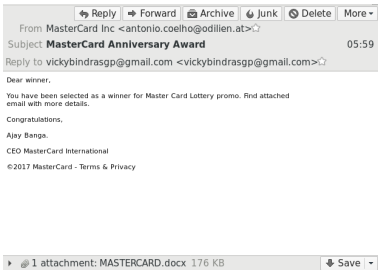
Sist, men inte minst, vill vi sätta ett frågetecken inför MSB hantering av nationella operativa system för rapportering av it-incidenter och övervakning av internettrafik utan att ha ett ledningssystem för det nationella informations- och cybersäkerhetsarbetet. MSB har riktlinjer och rutiner för det interna arbetet, men däremot saknas ledningssystem för det nationella arbetet, till exempel riktlinjer och rutiner för att bedöma och vidareförmedla andra organisationers varningar och larm. Det har också fått något märkliga konsekvenser.

I slutet av sommaren 2015 gick U.S. Food & Drug Administration (FDA) ut och varnade för it- och cybersäkerhetsrisker med en medicinteknisk produkt, Hospira infusionspumpar.[17] Det var första gången i myndighetens historia. FDA rekommenderade att vårdgivarna kopplar bort utrustningen från internet, samtidigt som de varnar för riskerna med manuell hantering. Det resulterade i omfattande diskussioner bland vårdgivare. I Sverige hördes ingenting, trots att Hospira har återförsäljare i Sverige. På MSB tog en medarbetare initiativ till att undersöka om utrustningen fanns i Sverige och informera berörda.[18] Ingen rutin fanns. Ingen information publicerades. Den nationella samordningen i frågan är fortfarande oklar.

Närmare två år senare, april 2017, larmar MSB via SVT och andra nationella nyhetsmedier om ett nytt storskaligt cyberhot APT10/Operation Cloud Hopper.[19] Sverige uppges vara ett av flera länder som har drabbats. Ingen närmare information om de drabbade organisationerna ges. Flertalet större svenska nyhetsmedier rapporterar om larmet. Underlaget för MSB:s larm är en konsultrapport från PwC och BAE Systems som publicerades några dagar tidigare. I praktiken handlar det om klassiska metoder och verktyg för it-angrepp, så som phishing.[20] Konsultrapporten innebar ingen reell nyhet annat än att en ny typ av företag är drabbade, molnleverantörer.

*Ej värt larm.* IT-säkerhetsrisker i insulinpumpar bedömdes inte utgöra ett allvarligt säkerhetshot efter U.S. FDAs varningar.

*




*Värt larm.* Nätfiske (att lura tjänstemän att klicka på bifogade filer eller öppna underliga länkar) bedömdes utgöra ett viktigt hot att kommunicera.

[17] U.S. Food and Drug Administration (pressrelease, 31 juli 2015). Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication.

[18] Medarbetaren är medlem i DFRI och dataskydd.net.

[19] CERT-SE (pressrelease, 7 april 2017). Omfattande cyberangrepp hos driftleverantörer.

[20] Definition av *nätfiske* (phishing) från svenskspråkiga Wikipedia:

> ”Nätfiske eller lösenordsfiske, eller phishing (efter engelskans fishing, ’fiske’, antagligen påverkat av stavningen i phreaking som i sin tur är en kombination av Hacking/Cracking och Phone) är en form av social manipulation och en olaglig metod att lura innehavare av bankkonton och andra elektroniska resurser att delge kreditkortsnummer, lösenord eller annan känslig information.
>
> Nätfiske är oftast utformat som ett e-brev som ser ut att komma från en bank eller ett kreditkortsbolag, innehåller en uppmaning att logga in snarast möjligt, och en länk till en falsk webbsida med inloggningsformulär.
>
> Det förekommer försök, framförallt via e-post att få tag på privat information, till exempel kontokortsnummer, bankinformation och lösenord. Dessa e-postmeddelande kan vara mycket välgjorda och i stort verka autentiska. Oftast uppges de komma från ett företags supportavdelning och man anger ofta att det har uppstått något form av problem med kundens konto eller motsvarande och behöver då lösenord etcetera för att kunna åtgärda felet. Detta är ofta riktat till kunder hos internetbanker.
>
> Nätfiskare kan även använda sig av bilder istället för text för att göra det svårare för anti-phishing filter att upptäcka specifik text som ofta används i nätfisk e-post.”
>
> https://sv.wikipedia.org/wiki/N%C3%A4tfiske

I fallet FDA har vi att göra med en reell varning och rekommendation från en myndighet. I fallet med APT10 är källan två konsult- respektive försvarsföretag med ett affärsintresse av att samhället finansierar cybersäkerhetsåtgärder i så stor utsträckning som möjligt. I det första fallet säger MSB ingenting. I andra fallet larmar myndigheten nyhetsmedierna utan eget underlag. Det speglar en brist på ledningssystem, på riktlinjer och rutiner för det nationella informations- och cybersäkerhetsarbetet. Ett minikrav på att driva sensorsystem för nationella säkerhetssyften bör vara att det finns ett ledningssystem för säkerhetsarbetet.

Avslutningsvis, MSB är inte en underrättelseorganisation, utan har som huvudsakligt mandat att samordna samhällets säkerhetsarbete. Obligatorisk incidentrapportering kan möjligen ses som ett samordningsprojekt, även om det är tveksamt med tanke på den svepande sekretessen som omgärdar arbetet. Internetövervakning är definitivt inte ett samordningsprojekt. Det liknar underrättelseverksamhet. Ett klargörande av MSB:s roll som underrättelseorganisation bör göras innan myndigheten får ytterligare uppdrag.

*Källförteckning*


1. Agaku, I. T., Adisa, A. O., Ayo-Yusuf, O. A., & Connolly, G. N. (2014). Concern about security and privacy, and perceived control over collection and use of health information are related to withholding of health information from healthcare providers. Journal of the American Medical Informatics Association, 21(2), 374-378.
2. Anderson, R. (2008). Security engineering. John Wiley & Sons. Tillgänglig på webben: http://www.cl.cam.ac.uk/~rja14/book.html
3. CERT-SE (pressrelease, 7 april 2017). Omfattande cyberangrepp hos driftleverantörer. https://www.cert.se/2017/04/omfattande-cyberangrepp-hos-driftleverantorer
4. Delade meningar (2017). Insight Intelligence i samarbete med i samarbete med Advokatfirman Lindahl, Svensk Handel, Samsung och Stockholms Läns Landsting, samt SICS Swedish ICT. https://www.iis.se/docs/Delade-Meningar-2016.pdf
5. Hugh Eakin (19 januari 2017). The Swedish Kings of Cyberwar. The New York Review of Books. http://www.nybooks.com/articles/2017/01/19/the-swedish-kings-of-cyberwar/
6. Edwards B, Hofmeyr S och Forrest S (2015). Hype and Heavy Tails: A Closer Look at Data Breaches. Forskningspresentation på WEIS 2015: http://www.econinfosec.org/archive/weis2015/papers/WEIS_2015_edwards.pdf
7. European Network and Information Security Agency (2008). Security Economics and the Internal Market. Författare: Ross Anderson, Rainer Boehme, Richard Clayton, Tyler Moore. https://www.enisa.europa.eu/publications/archive/economics-sec/
8. Johnson, C. W. (september 2015). Barriers to the use of intrusion detection systems in safety-critical applications. In International Conference on Computer Safety, Reliability, and Security (pp. 375-384). Springer International Publishing.
9. Kwon, J., & Johnson, M. E. (2015). The Market Effect of Healthcare Security: Do Patients Care about Data Breaches? Paper presented at the 14th annual Workshop on the Economics of Information Security (WEIS), 22-23 June, 2015. http://www.econinfosec.org/archive/weis2015/papers/WEIS_2015_kwon.pdf
10. Myndigheten för samhällsskydd och beredskap (pressrelease, 15 mars 2017), Första årsrapporten inlämnad till regeringen om arbetet med allvarliga it-incidenter. https://www.msb.se/sv/Om-MSB/Nyheter-och-press/Nyheter/Nyheter-fran-MSB/Forsta-arsrapporten-inlamnad-till-regeringen-om-arbetet-med-allvarliga-it-incidenter/
11. Ponemon Institute (2016). The State of Malware Detection & Prevention. Report sponsored by Cyphort, independently conducted by Ponemon Institute LLC, US. http://go.cyphort.com/Ponemon-Report-Page.html [OBS: kräver att man uppger e-postadress]
12. Radichel, Teri (2014). Case Study: Critical Controls that Could Have Prevented Target Breach. SANS. US. https://www.sans.org/reading-room/whitepapers/casestudies/case-study-critical-controls-prevented-target-breach-35412
13. Richards, N. M. (2013). The dangers of surveillance. Harvard Law Review, 126(7), 1934-1965.
14. Riksrevisionen (2016). Informationssäkerhetsarbete på nio myndigheter. RiR 2016:8. http://www.riksrevisionen.se/en/rapporter/Rapporter/EFF/2016/Informationssakerhetsarbete-pa-nio-myndigheter/
15. Thaw, David (2014). The Efficacy of Cybersecurity Regulation (October 4, 2013). Georgia State University Law Review, Vol. 30.
16. U.S. Food and Drug Administration (pressrelease, 31 juli 2015). Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication. https://www.fda.gov/medicaldevices/safety/alertsandnotices/ucm456815.htm
17. Wahlund R, Dellham R, Åberg D och Lakomaa E (2016). Anseenderisker och dataskydd. Kapitel 5, utdrag ur Risker och riskhantering i näringsliv och samhälle. Wahlund R (red.) Stockholm School of Economics Institute for Research.

18. ZDnet (2 februari 2015). Michael Kassner. Anatomy of the Target data breach: Missed opportunities and lessons learned. http://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/