Stockholm 2021-01-29

Justitiedepartementet
Enheten för lagstiftning om allmän ordning och
säkerhet och samhällets krisberedskap (L4)

Er referens: Dnr: Ju2020/04335
Vår referens: 21-002

Netnod är ej remissinstans men har valt att komma med synpunkter på *Kommunikationstjänsten SGSI – utvidgad användarkrets och förtydligande av MSB:s uppdrag*.

Slutsats: Netnod anser fokuseringen på överbelastningsattacker i underlaget är felaktig. En sådan fokusering kan leda till en falsk trygghet. En modern risk- och sårbarhetsanalys (där överbelastningsattacker är ett av flera hot) behöver ligga till grund för framtida implementation och användning av SGSI. Vidare anser Netnod att lösningar för elektronisk kommunikation som bygger på etablering av speciell infrastruktur eller speciella lösningar inte kommer leda till att önskade krav gällande kontinuiteten i tjänsterna kommer uppnås.

Att ha en lista med anslutna organisationer kommer alltid kräva kommunikationslösningar mellan en organisation som är ansluten och en som inte är det, speciellt allmänheten. Sådana lösningar blir dessutom extremt känsliga gällande säkerheten inom de olika anslutna organisationerna. Även kommunikation mellan organisationer på listan och de utanför behöver säkras. Därför är det för samhället bättre att bygga en modern lösning med hjälp av internetarkitekturen, där SGSI är en funktion, än att bygga en separat infrastruktur.

Speciellt håller Netnod varken med om beskrivning i avsnitt 3.1 (Den driftsäkra kommunikationstjänsten SGSI) eller förslag i 3.5 (Konkurrensrättsliga överväganden).

Patrik Fältström
Teknik- och Säkerhetsskyddschef

Tel: +46-706059051
Email: paf@netnod.se

Netnod
Greta Garbos Väg 13
169 40 Solna

Synpunkter i detalj:

1. SGSI måste använda en modern kommunikationsarkitektur

Idag består all kommunikation av flera olika delar där de olika delarna kan levereras av flera olika spelare. Detta har bland annat slagits fast av Kungl. Ingenjörsvetenskapsakademien (IVA) som säger att Sverige har övergått *från att bygga stuprör till att bygga en lasagne*[1]. Gällande SGSI saknas tydlighet gällande vilka olika funktioner som vid samverkan ger att SGSI uppnår önskad effekt, dvs kan leverera de funktioner som användarna önskar.

Den modell som SGSI bygger på är enligt denna syn en gammaldags stuprörs-arkitektur.

Att se planering och investering i stuprör anser Netnod vara bekymmersamt.

2. Felaktig syn på överbelastningsattacker

I avsnitt 3.1, i sammanfattningen och på andra ställen, går det att finna argument att lösningen ska skydda mot bland annat överbelastningsattacker.

> *Eftersom nätet är skilt från internet påverkas inte tjänsten av internetbaserade störningar, exempelvis överbelastningsattacker.*

I all modern kommunikation används idag internetarkitektur [2]. I denna kan en överbelastning alltid uppstå i lösningar som dimensionerats för en maximal kapacitet som understiger den som i praktiken uppstår. Detta kan uppstå oavsett om det som blir överbelastat (dvs är underdimensionerat) är nåbart från Internet eller inte. Merparten av dagens kommunikationsinfrastruktur används också för Internet så antagandet att man kan vara opåverkad av störningar i samhällets it-infrastruktur är överdriven. Överbelastning på ett nätelement eller motsvarande (även el- eller radionät) kan ge bieffekter på till synes helt separerad kommunikation. Därför måste man istället bygga så robust och på ett sådant sätt att man är opåverkad givet alla typer av sådana störningar.

Dessutom har PTS har i sitt robusthetsarbete pekat ut ett flertal olika hot mot elektronisk kommunikation [3].

> *Naturkatastrofer, sabotage och terroristhandlingar mot telesystem och samhällets elförsörjning bedöms vara tänkbara hot i fredstid. Andra hot är intrång via telenät i teleoperatörernas styr- och övervakningsnät med stödsystem.*

Detta är hot som visat sig inte bara vara teoretiska utan reella genom till exempel fällningen av Häglaredsmasten [4] och den explosion som drabbade AT&T i Nashville, USA [5]. För att säkerställa kontinuitet kan man inte fokusera på överbelastningsattacker, för dessa är inte det enda hotet mot fungerande kommunikation.

Netnod anser fokuseringen på och beskrivningen av överbelastningsattacker på det sätt som gjorts innebär en felaktig fokusering och prioritering.

3. Konkurrensrättsliga överväganden är för begränsade

I avsnitt 3.5 beskrivs de konkurrensrättsliga överväganden som gjorts. I dessa nämns det att behovet för till exempel Polisen att på ett säkert sätt kunna kommunicera med SOS Alarm Sverige AB vid en olyckssituation *överväger den eventuella negativa inverkan som ett sådant tillhandahållande kan tänkas få för konkurrerande företag*. Detta beskriver enbart en typ av konkurrenssituation och inte den negativa påverkan på marknaden det innebär att Polisen och SOS Alarm AB **inte** köper de tjänster de anser sig behöva på den öppna marknaden. Att på detta sätt ta bort de köpare som kräver säker kommunikation från marknaden för elektronisk kommunikation får för marknaden negativa konsekvenser. De produkter som önskas kommer i förlängningen inte utvecklas eftersom antal kunder är få. De aktörer som inte får använda SGSI kan därmed inte köpa de tjänster som de har behov av.

I de underlag som beskriver SGSI och även i den remitterade rapporten anses kommunikation mellan de deltagande aktörerna vara viktig för samhället. Vi har i Sverige, till skillnad från till exempel Estland, inte bestämt vad som ska prioriteras. Istället är det respektive aktör som själv avgör om de tillhandahåller samhällsviktiga tjänster, vilka i så fall ska skyddas. Vad Netnod ser är att det finns viktig kommunikation mellan inte bara de i rapporten nämnda inblandade aktörerna, utan mellan dessa och andra inte nämnda aktörer och inte minst allmänheten. I förlängningen kan med denna syn all kommunikation med extraordinära krav flyttas från den av marknadsekonomiska krafter etablerade infrastrukturen till speciella lösningar som kravställs, upphandlas och etableras på annat sätt. Den konkurrensrättsliga övervägandet täcker inte den negativa påverkan gällande tillgång på tjänster som kommer finnas för samhället i stort givet nämnda aktörer tas bort från marknaden.

Netnod anser den konsekvensanalys gjorts som gäller marknadsekonomiska effekter inte är heltäckande.

5. Separation från Internet ger falsk säkerhet

Design av SGSI och rapporten bygger på en tanke att alla till SGSI anslutna aktörer och all den utrustning som används kan vara betrodda. Det vill säga att det finns en säker insida och en osäker utsida. Detta är ett designtänk som användes i Internets barndom men som slogs i spillror slutligen 2008 då en öppen presentation av Federal Bureau of Investigation (FBI) [6] visade hur förfalskad utrustning från Cisco använts för intrång hos diverse aktörer i världen. Senare har liknande incidenter skett bland annat hos Maersk [7] och nyligen SolarWinds [8].

Netnod anser rapporten visar en övertro på implicit säkerhet genom separation från Internet.

6. Tydligare risk- och sårbarhetsanalys krävs

Existensen för SGSI, och i förlängningen detta förslag på utökad användning av SGSI, argumenteras det för i formen av att det är åtgärder som krävs för att minska sannolikhet för, eller konsekvens av, en viss risk. Dock beskrivs inte den risk och åtgärder på ett tydligt sätt. En sådan risk- och sårbarhetsanalys krävs till exempel i 1 kap. 12 § i *Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster*.

Netnod anser inte beslut kan tas om vidare investering i SGSI utan att en adekvat risk- och sårbarhetsanalys görs.

7. Den lösning som väljs måste vara modern

Åtgärder som baserar sig på en korrekt risk- och sårbarhetsanalys ska enligt 15 och 16 §§ i Lag (2018:1174) som nämns ovan sägas vara ändamålsenliga och proportionella, säkerställa en nivå på säkerheten i nätverken och informationssystemen som är lämplig i förhållande till risken och syfta till att säkerställa kontinuiteten i tjänsterna.

Netnod har tillsammans med Svenska Universitetsnätet (SUNET) genom Vetenskapsrådet på uppdrag av Post- och telestyrelsen undersökt lösningar för hög tillgänglighet till webbaserade tjänster genom projektet *Särimner* [9]. I detta arbete ingick därmed en risk- och sårbarhetsanalys tillsammans med en efterföljande stresstest som pekar på andra risker än överbelastningsattacker. De största problemen som identifierades fanns vara förknippade med möjlighet till kommunikation, det vill säga att säkerställa kontinuitet, vilket även stämmer överens med Post- och Telestyrelsens analyser av uppkomna driftavbrott.

Netnod anser lösningen som väljs för SGSI måste ha ett ökat fokus på att säkerställa kontinuiteten i tjänsterna.

8. Säkerställning av kontinuitet erhålls genom diversitet

För att på ett modernt sätt etablera säkerställd kontinuitet med internetarkitekturen måste en lösning väljas där möjlighet till kommunikation maximeras. Detta erhålls genom att för en tjänst vid varje tillfälle och på varje plats kunna använda ett flertal olika sinsemellan oberoende bärare. Om två oberoende bärare var och en har 99% driftsäkerhet ger användning av båda 99,99%, och använder man tre blir resultatet ännu bättre. Driftsäkerheten växer exponentiellt med antal alternativa oberoende spelare.

Netnod anser lösningen måste fokusera på diversifierad framföring av trafik.

Referenser:

1. *Digitalisering för ökad konkurrenskraft*, Kungl. Ingenjörsvetenskapsakademien (IVA), ISSN: 1100-5645, 2019, https://www.iva.se/globalassets/projekt/201902-iva-digitalisering-slutrapport-l.pdf
2. *Svenska delen av Internet*, Statskontoret, Statskontoret (1997:18), https://www.snus.se/internetutredningen/
3. *Hotbilder*, Post- och telestyrelsen, 2020-11-09, Läst 2020-12-28, https://www.pts.se/sv/bransch/internet/robust-kommunikation/hotbilder/
4. *Frågor och svar om masthaveriet i Borås*, Teracom, Läst 2020-12-28, https://www.teracom.se/privat/nyheter/Nyhetslista/q--a-masthaveri-boras/
5. *Nashville recovery efforts*, Jeff McElfresh, 2020-12-27, Läst 2020-12-28, https://about.att.com/pages/disaster_relief/nashville.html
6. *FBI worried as DoD sold counterfeit Cisco gear*, Stephen Lawson, Robert McMillan, IDG News Service, 2008-05-12, https://www.infoworld.com/article/2653167/fbi-worried-as-dod-sold-counterfeit-cisco-gear.html
7. *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, Andy Greenberg, Wire, 2018-08-22, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
8. *Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor*, FireEye, 2020-12-13, https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
9. *Att motverka överbelastning av samhällsviktiga webbplatser - Slutrapport 2018 från projekt Särimner*, Vetenskapsrådet på uppdrag från Post- och telestyrelsen, 2018-12-07, https://www.pts.se/globalassets/startpage/dokument/icke-legala-dokument/rapporter/2018/internet/slutrapport-sarimner-2018.pdf