Stockholm 2025-01-15

Justitiedepartementet

Er referens: Ju2024/02286
Vår referens: 24-009

Netnod har den 22:a november från Justitiedepartementet beretts möjlighet att lämna synpunkter på ett förslag på *Utkast till lagrådsremiss för Datalagring och tillgång till elektronisk information.*

Netnod vidhåller sina tidigare åsikter och synpunkter i tidigare remissrunda[1]. Netnod inkommer härmed med en reviderad formulering av sina synpunkter:

- Lagrådsremissen argumenterar att (cyber)säkerheten inte sänks av det lagda förslaget som kommentar på Netnods kommentarer på remissen av SOU 2023:22. **Netnod anser att utredningen har felaktiga uppgifter och det inte finns några lösningar som uppfyller sagda krav utan att väsentligt sänka (cyber)säkerheten, exempelvis genom att bakdörrar byggs in.**
- Lagrådsremissen argumenterar för att regelverk för nummerbaserade och nummeroberoende tjänster skall harmoniseras.
  Netnod anser att nummerbaserade och nummeroberoende tjänster har olika arkitekturprinciper och användningsområden, och att det därmed inte finns någon anledning eller motivation för att harmonisera dessa regelverk.

Se bilaga för en fördjupad analys.

Patrik Fältström
CSO

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

[1] Se https://www.netnod.se/netnod-response-to-the-swedish-data-storage-act

Netnod AB
Greta Garbos väg 13
169 40 Solna

Bilaga 1 - Detaljerade kommentarer

1. Sårbarheter får aldrig byggas in i tjänster

Lagrådsremissen föreslår att samma / liknande regelverk ska gälla för tillhandahållare av nummeroberoende kommunikationstjänster som för nummerbaserade dito. Netnod är av åsikten att både den tidigare utredningen och den nu lagda lagrådsremissen bortser från de fundamentalt olika arkitekturer som ligger till grund för hur nummerbaserade tjänster (ex telefoni och sms) byggs i jämförelse med nummeroberoende tjänster (allt annat än telefoni och sms).

Både den tidigare utredningen (som producerade SOU 2023:22) och lagrådsremissen sägs vara skrivna efter följande princip:

> *En grundläggande princip bör vara att det är tekniken som ska följa lagstiftningen och inte lagstiftningen som ska följa tekniken.*
>
> (SOU 2023:22, s. 415)

Netnod vill åter påpeka att grundtesen är god, det vill säga att land skall med lag byggas, men lag måste vara skriven på ett sådant sätt att den (tekniskt) går att följa. Bland annat skrivs det i remissen:

> *Även tillhandahållare av Noik ska alltså vara skyldiga att bedriva sin verksamhet så att beslut om hemliga tvångsmedel kan verkställas och så att verkställandet inte röjs. Det omfattar även de fall en tillhandahållare för sina kunder möjliggör totalsträckskryptering, dvs. när bara sändare och mottagare har tillgång till meddelandena i läsbar form. I dessa fall innebär anpassningsskyldigheten att tillhandahållaren ska kunna göra uppgifterna tillgängliga för brottsbekämpande myndigheter i läsbar form.*
>
> (lagrådsremissen, s. 137)

Detta är tekniskt omöjligt att uppfylla för en totalsträckskrypterad[2] tjänst utan att kompromettera totalsträckskrypteringen. Och om informationen är krypterad med nyckelmaterial i säkert element kan denna nyckel inte delas med en tredje part (dvs tjänstetillhandahållaren) på ett sådant sätt som lagrådsremissen och utredningen föreslår, dvs det går inte att kompromettera konfidentialitetsaspekten av totalsträckskrypteringen[3].

Detta innebär därmed att bakdörrar måste byggas in i kommunikationstjänster. Bakdörrar är att likställa med sårbarheter ur ett riskhanteringsperspektiv, och sårbarheter får aldrig byggas in i tjänster enligt Netnod. Dessutom går det lagda förslaget stick i stäv med NIS2, speciellt skäl 98, enligt nedan:

---

[2] Både begreppen *helsträckskrypterad* och *totalsträckskrypterad* förekommer i nu pågående remissrundor och där kopplat på såväl EU som svensk nivå. Detta remissvar använder begreppet *totalsträckskryptering* med böjningar då detta är det primära begreppet som används i lagrådsremissen.

[3] Däremot kan tillgängligheten påverkas.

> *(98) För att trygga säkerheten för allmänna elektroniska kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster bör användningen av krypteringsteknik främjas, särskilt **totalsträckskryptering** samt datacentrerade säkerhetskoncept, såsom kartografi, segmentering, taggning, åtkomstpolicy och åtkomsthantering samt automatiserade beslut om åtkomst. Vid behov bör användningen av kryptering, särskilt **totalsträckskryptering**, vara obligatorisk för tillhandahållare av allmänna elektroniska kommunikationsnät eller av allmänt tillgängliga elektroniska kommunikationstjänster i enlighet med principerna om automatisk och inbyggd säkerhet och automatiskt och inbyggt integritetsskydd vid tillämpningen av detta direktiv. Användningen av **totalsträckskryptering** bör förenas med medlemsstaternas befogenheter att säkerställa skyddet av sina väsentliga säkerhetsintressen och sin allmänna säkerhet och att möjliggöra förebyggande, utredning, upptäckt och lagföring av brott i enlighet med unionsrätten. Detta bör dock inte **försvaga totalsträckskrypteringen**, som är en kritisk teknik för ett effektivt dataskydd, integritet och kommunikationssäkerhet.*
>
> (Direktiv (EU) 2022/2555 [SV], s. 99, fetstil tillagt)

I sammanhanget så har även ansvariga myndigheter i USA gått ut och sagt att slutanvändare, både personer och organisationer, i större utsträckning ska använda sig av totalsträckskrypterade tjänster för kommunikation för att minimera påverkan på amerikanska säkerhetsintressen om tjänstetillhandahållare blir kompromettерade[4].

Netnod vill även poängtera att det inte, i Netnods kännedom, finns några *allmänt tillgängliga* totalsträckskrypterade **nummerbaserade** tjänster[5]. Samtliga *allmänt tillgängliga* totalsträckskrypterade tjänster är **nummeroberoende**.

Nummerbaserade tjänster (som telekom-tjänster) byggs enligt andra principer och arkitekturer än nummeroberoende tjänster (i princip allt annat, men gemensamt är att de ofta använder Internet)[6]. Därmed är det inte rimligt att, som remissen föreslår, harmonisera regelverken för nummerbaserade tjänster med dem för nummeroberoende tjänster.

Förslaget gör fortfarande en skillnad på maskin-till-maskin-kommunikationstjänster och interpersonella diton. Detta är en distinktion som enbart är meningsfull när en leverantör tillhandahåller en hel vertikal i en tjänsteleverans, som är fallet för de nummerbaserade tjänsterna sms och telefoni, men som inte är meningsfull för samtliga nummeroberoende tjänster då kommunikationslagret kan vara helt separerat från enheten som använder tjänster.

Det kan därmed vara omöjligt för en tjänst att veta om det är en sensor (som exempel på maskin-till-maskin-kommunikation) eller en människa som är ursprung eller avsedd mottagare till viss kommunikation.

---

[4] Se bland annat rapportering i https://www.nbcnews.com/tech/security/us-officials-urge-americans-use-encrypted-apps-cyberattack-rcna182694

[5] Däremot finns icke-allmänt tillgängliga sådana.

[6] Se bland annat Lindeberg (2021) för en genomgång av de tekniska, företagsekonomiska, och byråkratiska motsättningar och likheter som finns mellan klassisk telekom-modell och Internetbaserade lösningar för kommunikation.

- Lindeberg, Fredrik. “Coordinating the Internet: Thought Styles, Technology and Coordination.” PhD of Technology, Linköping University, 2021. http://urn.kb.se/resolve?urn=urn:nbn:se:liu:diva-173713.

Notera att en kommunikationslösning kan användas till både maskin-till-maskin-kommunikation och interpersonell, det går därmed inte att göra en distinktion på tjänstelösningsnivå, utan distinktionen kan enbart meningsfullt göras på meddelandenivå. Och meddelanden är, som känt, ej läsbara i klartext för tjänstetillhandahållare som använder en totalsträckskrypteringslösning.

Vi vill åter poängtera att bakdörrar inte medvetet får byggas in i tjänster, för de kommer förr eller senare utnyttjas, antingen av de som är tänkta att kunna utnyttja den (ex polisen) eller någon annan (ex främmande makt).

> *Netnod anser att leverantörer av kommunikationstjänster under inga omständigheter får bygga in medvetna sårbarheter och bakdörrar i sina tjänster.*
>
> (Netnods svar på Ju2023/01326, s. 1)