Stockholm 2023-11-01

Justitiedepartementet
Enheten för domstols- och åklagarfrågor

Er referens: Ju2023/01326
Vår referens: 23-028

Netnod fick den 7:e juli 2023 från Justitiedepartementet möjlighet att inkomma med remissvar på betänkandet Datalagring och åtkomst till elektronisk information (SOU 2023:22).

Netnod inkommer härmed med följande synpunkter:

- Förslaget anser i praktisk bemärkelse att leverantörer av krypterade kommunikationstjänster enligt end-to-end-modell (s.k. *totalsträckskryptering*) ska bygga in bakdörrar i sina tjänster som kan utnyttjas av tredje part.
  Netnod anser att leverantörer av kommunikationstjänster under inga omständigheter får bygga in medvetna sårbarheter och bakdörrar i sina tjänster.

Se bilaga för utveckling av varför tjänsteleverantörer, eller vem-som-helst, aldrig ska bygga in sårbarheter i sina lösningar.

Patrik Fältström
Säkerhetsskyddschef

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

Netnod AB
Greta Garbos väg 13
169 40 Solna

Bilaga 1 - Detaljerade kommentarer

1. Medvetna sårbarheter kan alltid utnyttjas

Utredningen föreslår att även end-to-end-krypterade (s.k. totalsträckskrypterade) tjänster ska omfattas av förslaget, och omfattas på ett sådant sätt att de medvetet ska bygga in bakdörrar som ska kunna utnyttjas under vissa omständigheter.

> *Sammanfattningsvis föreslår vi att den som i Sverige tillhandahåller allmänt tillgängliga Noik ska omfattas dels av skyldigheten att bedriva sin verksamhet så att beslut om HAK, HÖK och inhämtning enligt inhämtningslagen kan verkställas och så att verkställandet inte röjs*
>
> (SOU 2023:22, s. 418)

> *För en tjänst där totalsträckskryptering erbjuds skulle tillhandahållaren exempelvis kunna välja att utforma tjänsten så att totalsträckskryptering där bara sändare och mottagare kan läsa meddelanden endast används mellan konton som vid tidpunkten för kommunikationen inte omfattas av ett beslut om HAK. Om något av de konton som kommunicerar omfattas av ett beslut om HAK, skulle däremot endast sådan kryptering användas som tillåter att behörig myndighet kan ta del av trafiken i klartext. Med fördel skulle arrangemanget även kunna utformas så att endast myndighet och Noik tillsammans kan aktivera sådan avlyssning.*
>
> (SOU 2023:22, s. 422)

Detta är teknisk omöjligt om klienterna kan använda en hårdvarubaserad krypteringslösning (dvs en nyckel vars privata del finns i en HSM, hardware security module). Detta innebär då att det är olagligt att tillhandahålla krypteringslösningar som används i kommunikation av den typ som är standard i moderna mobiltelefoner och bärbara datorer.

Lagförslaget förbjuder inte totalsträckskryptering i sak, utan gör genom formuleringar i speciellt LEK (2022:482), 9 kap, 19 § gällande att det inte finns något som helst undantag för nummeroberoende interpersonella kommunikationstjänster när det kommer till HAK och HÖK. Netnod kommenterar nedan på utredningens förslag till ändringar i lagen (2022:482) om elektronisk kommunikation.

Utredningens förslag: **9 kap, 19 §**	**Netnods förslag:** **9 kap, 19 §**
Den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § *och den som tillhandahåller en allmänt tillgänglig nummeroberoende interpersonell kommunikationstjänst* ska utan dröjsmål lagra uppgifter enligt vad som anges i 19 a–19 d §§.	Den som bedriver verksamhet som ska anmälas enligt 2 kap. 1 § ska utan dröjsmål lagra uppgifter enligt vad som anges i 19 a–19 d §§.

Motivering: En nummeroberoende interpersonell kommunikationstjänst kan inte tekniskt på ett rimligt sätt jämföras med exempelvis telefoni där operatören av tjänsten har i praktiken fullständig vertikal kontroll av hur tjänsten erbjuds. Speciellt då kommunikationstjänster över Internet inte sällan erbjuds av ett flertal aktörer tillsammans, se exempelvis det idag populära Matrix-protokollet med klienter och federering, eller den äldre XMPP- / Jabber-floran av protokoll och tjänster.

Utredningens förslag: **9 kap, 19 §, andra stycket**	**Netnods förslag:** **9 kap, 19 §, andra stycket**
Första stycket gäller inte vid tillhandahållande av maskin-till-maskin-tjänster.	< *utgår* >

Motivering: Då kommunikationstjänster i regel byggs vertikalt separerade är det tekniskt omöjligt med krypterad trafik att avgöra om kommunikation är maskin till maskin eller något annat. Utredningens förslag ger dessutom möjlighet till ordklyveri då en tjänst avsedd för maskin-till-maskin-kommunikation kan användas även för annan kommunikation. Exempelvis en meddelande-buss tillhandahållen av tredje part ställer här till problem. Det är inte klart för Netnod hur en tillhandahållare av kommunikationstjänster ska kunna avgöra vad som är maskin-till-maskin-kommunikation eller ej utan att bygga in bakdörrar i kommunikationsprotokollen.

Utredningen gör även liknande bedömning för mobila kommunikationer, specifikt avsnitt om 5G SA på s. 410. Om det byggs in bakdörrar i tjänster kommer det få två huvudsakliga vanartiga följder:

- Tjänsternas säkerhet sänks
- Bakdörrar kan utnyttjas av tredje part

Om anpassningsskyldighet ska gälla är det tekniskt rimligare att dessa skyldigheter ligger på tillhandahållare av personliga terminaler, som telefoner, där meddelanden och kommunikation finns i klartext.

Överlag anser Netnod att cybersäkerhetsnivån i samhället i stort är låg, och alla resurser som läggs på att sänka denna (dvs bygga in bakdörrar) är att betrakta som resursslöseri av begränsade resurser.

Dessutom finns det inga garantier att bakdörrar inte utnyttjas av tredje part. Som exempel kan utredningen undersöka “Room 614A”-incidenten, PRISM eller Tempora som har missbrukats av legitima makthavare.

Utredningen gör även följande kommentar på en högre nivå:

> *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 håller med i sak, det vill säga att land skall med lag byggas, men vill påpeka att det gäller då lagstiftningen reglerar de subjekt som lagstiftningen berör och deras ansvarsförhållande gentemot varandra. Detta för att istället för att vara tvingande för interna processer ska lagstiftning ge möjlighet för aktörer att välja lösning som de sedan ställs till svars efter. På ett sådant sätt att det inte blir orimligt.

Exempelvis kan man tänka sig att en aktör som visar sig användas i syfte för grov brottslighet beläggs med striktare krav för identifiering av användare.

Netnod är oroade över att förslaget är ett steg i en riktning som gör krypterade tjänster olagliga.