Stockholm 2020-08-17

Post- och Telestyrelsen
Avdelningen för säker kommunikation

Er referens: Dnr: 20-7032
Vår referens: 20-003

Netnod fick den 25 juni 2020 från Post- och Telestyrelsen möjlighet att komma med synpunkter på ett förslag till PTS nya föreskrifter om säkerhetsåtgärder för leverantörer av samhällsviktiga tjänster inom sektorn digital infrastruktur enligt NIS-lagen.

Netnod inkommer härmed med följande synpunkter:

- Termen *resursblockering* är ej definierad.
  Netnod föreslår termen *resursblockering* definieras.
- *Informationssystem* relaterat till tjänster som täcks bör skyddas med tvåfaktorautenticering. Netnod anser de allmänna råden ska göras mycket tydligare.
  Netnod föreslår införande av termen *kritiska informationssystem*.
- Beskrivning av krypteringsnycklar och deras skydd behöver förtydligas, speciellt i fallet att assymetriska kryptosystem med privata och publika hemligheter används.
  Netnod anser beskrivning av krypteringsnycklar förtydligas.
- Beskrivning av relationen mellan rotnamnservrar och rotnamnserveroperatörer är felaktig. Likaså hur delegering till auktoritativa namnservrar går till.
  Netnod anser dessa beskrivningar ska korrigeras.
- PTS gör bedömningen att alternativet att ta fram detaljerade krav på säkerhetsåtgärder oaktat leverantörens riskanalys inte är aktuellt i nuläget.
  Netnod håller med om denna slutsats.
- Trots att PTS drar slutatsen att detaljerade krav inte behövs i nuläget ställs på ett flertal ställen krav som är detaljerade och kostnadsdrivande.
  Netnod anser på de ställen krav är detaljerade istället dessa kan ges som exempel. Istället kan tydligare krav på och relation till aktörens egen riskanalys framgå.
- PTS anser att berörda leverantörers kärnverksamhet består bl.a. av att tillhandahålla den nu utpekade samhällsviktiga tjänsten, men detta utan att ge något underlag.
  Netnod anser PTS ej kan dra den typen av slutsatser.
- PTS beräknar timkostnad i genomsnitt är 500kr/h för tid som behöver läggas ner, samt att antal timmar för respektive insats (engångs eller återkommande) kan räknas i enstaka tiotal.
  Netnod anser timkostnaden för personal som måste göra många av de beskrivna åtgärderna i genomsnitt är mycket högre, både gällande timkostnad och antal timmar som går åt för olika arbetsuppgifter.

Netnod
Greta Garbos Väg 13
169 40 Solna

Slutligen anser Netnod att konsekvensanalysens avsnitt 4 bör göras om, och detta med mer realistiska kostnader och tidsaspekter för att ge en mer sannolik kostnadsanalys. Dessutom bör det undersökas hur den typ av krav som dessa föreslagna föreskrifter ställer kan ställas inte bara av tillsynsmyndighet utan även av kunder, speciellt offentlig sektor i sina upphandlingar för att minimera påverkan gällande konkurrenssituationen på marknaden. Även om denna inte ingår i själva föreskriften vore det olyckligt om förarbeten till densamma beskriver orealistiska förväntningar.

Patrik Fältström
Teknik- och Säkerhetsskyddschef

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

Bilaga 1 - Detaljerade kommentarer

1. Termen Resursblockering - 8 §

I 8 § används termen ***resursblockering***. Denna är ej definierad och vi kan heller inte finna någon vedertagen definition av den. Termen har dock använts tidigare, såväl i Statskontorets rapport *Svenska delen av Internet* (1997:18, allmänt kallad *Internetutredningen)*[1] som i Slutbetänkandet av *e*-komutredningen, *Toppdomän för Sverige (SOU 2003:59)*[2]. Netnod anser termen måste definieras.

2. Access till informationssystem - 11 §

Vid *Åtkomsthantering, 11 §* står det:

> *Flerfaktorsautentisering bör användas vid åtkomst till informationssystem från externa nätverk.*

Netnod anser att *informationssystem* är alldeles för generellt även om det bryggas till 6 § där det hänvisas till organisationens egen riskanalys. T.ex. kan vissa informationssystem exponera information för läsning, som en websida med statistik. Netnod föreslår därför istället att det specificeras att det gäller access till system som vid icke-auktoriserad access kan leda till påverkan på informationssystemet, vilket vi föreslår kan benämnas **kritiska informationssystem**. Naturligtvis måste därmed andra system, inklusive de som enbart används för läsning, säkras så de inte kan användas för påverkan, men detta genom säker design och inte genom flerfaktorautenticering. Dessutom skulle de allmänna råden kunna ändras från bör till ska. Vilka system som är kritiska informationssystem kan tillåtas framgå av riskanalysen. Föreslagen ny text skulle kunna vara:

> *Flerfaktorsautentisering **ska** användas vid åtkomst till **kritiska** informationssystem från externa nätverk.*

3. Krav på funktionalitet som (tyvärr) ej alltid finns - 14 §

Netnod noterar kraven i 14 § och anser generellt dessa vara rimliga. Dessa matchar t.ex. rekommendationer av andra myndigheter gällande s.k. audit-loggar gällande access till system. Dock är detta inget som normalt skapas vid t.ex. användning av standardprogramvara för DNS eller REST-API:er. Det finns dock ofta begränsade loggar i form av loggfiler för HTTP-transaktioner som genom bearbetning kan ge motsvarande information. Att strikt implementera det som är beskrivet kräver separata stödsystem från normal DNS-hantering och detta är ett exempel på en typ av krav som är kostnadsdrivande (se separat avsnitt om kostnadsberäkningar).

[1] Se bilaga 16 i Svenska delen av Internet, Statskontoret 1987, Statskontorets Rapport 1997:18, https://www.snus.se/internetutredningen/bilaga/bil16.html
[2] Sid 132, Slutbetänkande av *e*-komutredningen, SOU 2003:59, Toppdomän för Sverige

4. Uppgifter som är konfidentiella - 14 §

Netnod noterar att som exempel på vad som anses vara konfidentiellt inkluderas ***krypteringsnycklar***. Det behöver specificeras att det t.ex. vid användning av krypteringstekniker som är assymetriska är det den s.k. ***privata*** delen som ska anses vara konfidentiell. Ej den ***publika***.

5. Konsekvensanalys 2.1 - rotnamnservrar

Det står:

> *Idag finns det ca 1100 auktoritativa rotnamnservrar utspridda över världen. Dessa sköts av tolv oberoende rotnamnserveroperatörer. En av dessa rotnamnserveroperatörer finns i Sverige och ansvarar för elva instanser (kopior) av roten.*

Korrekt text skulle vara:

> *Idag finns det ca 1100 auktoritativa rotnamnservrar utspridda över världen. Dessa sköts av tolv oberoende rotnamnserveroperatörer som ansvarar för tretton instanser (kopior) av roten. En av dessa rotnamnserveroperatörer finns i Sverige.*

6. Konsekvensanalys 2.1 - delegering till auktoritativ namnserver

Texten som beskriver auktioritativ namnserver är felaktig. Delegering behöver inte ske i samband med registrering. Dessutom föreslår Netnod ytterligare ett exempel på driftorganisation som hanterar auktoritativa namnservrar läggs till.

Det står:

> *I samband med registrering av ett domännamn måste sedan minst en auktoritativ namnserver pekas ut för domännamnet, annars går det inte att hitta fram till domänen via DNS.*
> *Det kan antingen vara en namnserver som innehavaren av domännamnet själv gör tillgänglig på internet eller också en namnserver som drivs av någon annan, t.ex. en internetleverantör eller ett s.k. Webbhotell.*

Korrekt text skulle vara:

> ***För att det ska gå att hitta fram till domännamnet via DNS måste minst en auktoritativ namnserver pekas ut för detta genom delegering.***
> *Denna kan antingen vara en namnserver som innehavaren av domännamnet själv gör tillgänglig på internet eller också en namnserver som drivs av någon annan, t.ex. en internetleverantör,* ***fristående DNS-leverantör*** *eller ett s.k. Webbhotell.*

7. Konsekvensanalys 2.4.2 - Detaljerade krav

PTS gör bedömningen att alternativet att ta fram detaljerade krav på säkerhetsåtgärder oaktat leverantörens riskanalys inte är aktuellt i nuläget. Netnod håller med om denna

slutsats men noterar att de föreslagna föreskrifterna innehåller mycket detaljerade krav i ett flertal punkter. T.ex. i avsnittet om spårbarhet i 14 §. Detta visar sig även gällande slutsatser i avsnitt 2.4.3.

8. Konsekvensanalys 3.2 - Omsättning hos anmälda aktörer

Det står:

> *Därtill finns också två svenska stiftelser, vilka har cirka 30 respektive 70 anställda, men vars årsomsättning är okänd.*

I den sändlista som bifogades finns de 11 anmälda organisationerna namngivna. Vi kan inte i den se två utan bara en stiftelse, Stiftelsen för internetinfrastruktur, och dess årsredovisningar är tillgängliga, och därmed är dess årsomsättning känd.

9. Konsekvensanalys 4.1.2 - Kärnverksamhet

Det står:

> *Berörda leverantörers kärnverksamhet består bl.a. av att tillhandahålla den nu utpekade samhällsviktiga tjänsten.*

Det framgår inte hur PTS har kommit fram till den slutsatsen. I vissa fall kan den utpekade tjänsten vara något som inte alls kan anses vara kärnverksamhet, och med det menar Netnod att det kan vara vanskligt att dra slutsatser från företagets årsomsättning gällande den utpekade tjänstens omkostnader. Detta gäller speciellt krav som rör funktioner som normalt inte finns i standardprogramvara för de utpekade tjänsterna, utan kräver speciella investeringar.

Netnod saknar också en koppling mellan kostnader för införande av de av PTS föreslagna detaljerade kraven på produktionskostnader för tjänsterna och i slutänden slutkundspriser. Det intressanta måste ändå vara att se vilken skillnad i slutkundspris det blir att köpa dessa tjänster från tillhandahållare som faller under NIS jämfört med att köpa tjänster av andra.

10. Konsekvensanalys 4.1.2 m.fl. - Beräknade kostnader

PTS har beräknat kostnaden för internt arbete på uppgifter från 2018 och då genomsnittslön för driftingenjör inom telekommunikation och kommer fram till en genomsnittskostnad på 500kr/timme. Netnod vill påpeka att detta gäller driftpersonal och ej sådan personal som krävs för att t.ex. utvärdera, utveckla och implementera de krav som ställs. Likaså inte heller de som krävs för att leda t.ex. det kontinuerliga säkerhetsarbetet. Att räkna med samma timkostnad för utveckling och drift ser därför Netnod som alltför optimistiskt.

Netnod anser även tidsåtgång underskattas. Låt oss ge några exempel.

Normalt hanteras resultat av risk- och sårbarhetsanalys (inklusive resultat av analyser av incidenter) som ändringsbegäran i produktutvecklingen. Detta vid sidan av andra önskemål (interna såväl som externa). Det tillkommande kravet att *leverantörens riskanalys och*

dokumentation ska bevaras i fem år från det att den upprättats eller uppdateras kräver en separat hantering av just dessa, vilket framgår av PTS analys. Att separera den dokumentation som ska sparas i 5 år från det normala flödet kräver dels en engångsutveckling av såväl processer som verktyg, dels speciell hantering av detta. Detta även fast det finns väl fungerande system för ändringshantering (change management) som är koordinerad med det kontinuerliga säkerhetsarbetet.

Ett annat exempel är kostnader för speciella arbetsuppgifter och moment som omvärldsbevakning. Netnod anser inte personal kan ha speciella arbetsuppgifter som kräver dokumentation och aktivt arbete under 10% av en heltid som minimum. Naturligtvis kan samma roll utföra andra liknande arbetsuppgifter inom dessa 10% om inte arbetsuppgiften i praktiken kräver 10% arbetstid, men mindre än 10% går inte att hantera. Motsvarande underskattning av tidsåtgång återfinns på ställen där PTS föreskrifter kräver tillägg till MSB informationssäkerhetsföreskrifter.

Normal omvärldsbevakning sker genom prenumeration på notifieringar från de leverantörer och CERT som täcker aktörens produkter och tjänster. Aktören bedriver sådan normal omvärldsbevakning baserat på sin egen risk- och sårbarhetsanalys samt analys av de rapporter och den information som andra parter analyserat fram, och slutligen uppdaterar och uppgraderar programvara och operativsystem på ingående komponenter efter respektive tillverkares rekommendationer.

Om detta ska lyftas till ett *aktivt* deltagande, vilket Netnod tolkar PTS föreslår, krävs att aktören själv samlar in information till den grad att egna slutsatser kan dras. Detta i sin tur kräver deltagande på mailinglistor, konferenser och motsvarande. Netnod uppskattar att detta innebär ett pålägg i form av c:a 10% av en tjänst för att följa de pågående diskussionerna, analys av t.ex. månadsbrev från CERT (inklusive CERT-SE) och leverantörer samt deltagande på möten och konferenser.

Om det är sådant aktivt deltagande där egna bedömningar ska kunna göras ska PTS inkludera tid för detta i sina beräkningar.

Även kostnad för utbildning underskattas. Administration av utbildning på företaget kräver en speciell kompetens i sig, även om utbildningsinsatsen köps in av extern tillhandahållare. Kostnaden för en kurs i DNS håller Netnod med om kan vara 26kSEK för tre dagar, men kostnad för förlorad arbetstid tillkommer för kursdeltagarna. I praktiken måste man räkna med att en person som är på tre dagars kurs effektivt blir frånvarande från arbetsplatsen i en hel vecka om man räknar in förberedande arbete och summering efter kursen, dvs 40h arbetstid ytterligare kostnader.

Likaså kostnader för hantering av en incident underskattas. Möjligtvis kan ett post-mortem-möte ta 1,5h vilket stämmer med PTS uppskattning, men arbetet med att göra en rotsaksanalys, översätta till föreslagna förändringar, analys av dessa, dokumentera (enligt krav på andra ställen i den föreslagna författningen) och slutligen beslut om implementation och förbättringar är en större process.

I avsnittet om kontinuitetsplanering uppskattar PTS kostnaderna någorlunda korrekt. De administrativa kostnaderna finns med men inte tekniska i form av t.ex. hård- och mjukvara för duplicerade system, utökad colocation för dubblering av inplacering i datacenter etc. Netnod anser att en konsekvensanalys inte kan ignorera sådana kostnader även om i detta fallet de föreslagna föreskrifterna inte är så detaljerade som övriga. Därmed faller de enligt Netnod under den grundläggande regeln i avsnitt 2.4.2 att åtgärder ska basera sig på aktörens egen risk- och sårbarhetsanalys vilket Netnod anser vara korrekt.

Flera av dessa saker som Netnod lyfter är, som PTS påpekar, sådant som redan MSB kräver så dessa blir inte extra i just dessa föreslagna föreskrifter, men eftersom konsekvensanalysen inkluderar total resursåtgång för de olika förslagen vill Netnod påpeka de generellt är för låga.

Generellt anser Netnod istället att det ska finnas en större frihet att bedöma vilka åtgärder som ska införas ska kunna vara mindre specifik och basera sig på aktörens egen risk- och sårbarhetsanalys, vilket PTS föreslår redan i avsnitt 2.4.2. Därmed skulle också skillnaden mellan att falla under föreskrifternas krav och inte vara mindre. Men, i de fall extra krav ställs måste konsekvensen av dessa vara betydligt mer med sanningen överensstämmande.

11. Konsekvensanalys 4.5.2 - Säker programvaruhantering

Mening "*Säkerheten i nätverk och informationssystem blir inte starkare än den svagaste länken*" är till stor del ett uttryck i talspråk och bör utgå eller ersättas. Den inställning som uttrycket vill förmedla får anses vara väl känt hos de leverantörer dessa föreskrifter vänder sig till och meningen i sig tillför ingen ny kunskap eller förtydliganden.

12. Konsekvensanalys 4.5.2 - Kostnad för öppen källkod

I avsnittet ***4.5.2 Säker programvaruhantering*** dras slutsatsen:

> *System för centraliserad och automatiserad sårbarhetsbedömning och distribution av uppdateringar som kan behöva införskaffas för att komplettera leverantörens säkerhetsnivå finnas på marknaden som opensource-programvara och är därmed gratis.*

Netnod håller inte med om denna slutsats då opensource-programvara dels kräver intern kompetens (se punkt 10 ovan om beräknade kostnader), dels finns kostnader i form av antingen arbetstid nedlagd på donation av förändringar eller avgift i form av supportavtal precis som för kommersiell programvara eller båda. Att dra slutsats att kostnad är noll bara för att källkod är tillgänglig anser Netnod vara fel.

13. Konsekvensanalys 4.5.3 m.fl. - åtkomsthantering

På flera ställen blandas begreppen "tvåfaktorsautentisering", "flerfaktorsautentisering" och "multifaktorsautentisering". Ett mer enhetligt val av begrepp minimerar risker för feltolkningar och andra missförstånd.

14. Konsekvensanalys 4.5.6 - Kostnad för hantering av loggar

Att införa speciella audit-loggar anser Netnod kan vara den delen som är mest kostnadsdrivande. För att dessa ska vara värdefulla måste dels alla åtgärder loggas, dels måste själva loggningen vara motståndskraftig mot påverkan -- *även, eller snarare speciellt, vid intrång*. Detta innebär att speciell hantering av loggar, förutom att naturligtvis vara bland de viktigaste källorna till kunskap vid en undersökning efter en händelse, är bland det mest kostsamma att implementera. Bl.a. för att säker loggning och då inte bara vilka kommandon som utförs utan även vilka förändringar som görs inte finns som standard i de normala programvaror som används utan detta måste implementeras speciellt.

NIS-direktivet i sig ställer krav motsvarande mycket av detta så PTS föreslagna föreskrifter tillför i detta fallet inte mycket extra kostnader, men det också för att beskrivning **hur** detta ska gå till inte är specificerat utan leverantören kan implementera det på det sätt som det passar leverantören, och framför allt baserat på den risk- och sårbarhetsanalys av loggsystemet i sig resulterar i.

Som PTS påpekar finns flera externa leverantörer för loggning som man kan använda och därmed får man automatisk separation av loggar från sin verksamhet, men priserna varierar extremt mycket. Arbete att föra över loggar till sådana aktörer består även det av engångs- respektive återkommande kostnader.

15. Konsekvensanalys 4.6.1 - Övervakning

Texten använder framför allt begreppet “beredskap” men även “jourtjänstgöring” förekommer. Då begreppen har olika innebörd när det gäller bland annat vad som räknas som arbetstid samt hur veckovila och annan ledighet hanteras bör texten se över så att rätt begrepp och därmed innebörd förmedlas.