Anvisningspromemoria 2021 för periodiska bedömningar

1 Allmänt

När periodiska bedömningar beställs/utförs år 2021 använder Transport- och kommunikationsverket denna promemoria för att ta fram olika teman. Temana gäller brister som upprepats i de tidigare periodiska bedömningarna eller förbättringsförslag till bedömningsprocessen. Syftet med rådgivningen är att minska behovet av preciserande kompletteringsbegäranden och att snabba upp behandlingen av bedömningen både hos leverantörer av identifieringstjänster och hos Traficom.

Anvisningspromemorian kan indelas i två delar

- Helheter som kräver speciell uppmärksamhet och som rapporterats bristfälligt vid de tidigare periodiska bedömningarna

Frivillig Excel-tabell i standardformat vars syfte å ena sidan är att säkerställa bedömningens och själva rapportens omfattning och å andra sidan att snabba upp behandlingen

2 Författningar

I 29 § i lagen om stark autentisering och betrodda elektroniska tjänster (617/2009, autentiseringslagen) finns bestämmelser om skyldighet för en leverantör av identifieringstjänster att regelbundet låta ett sådant bedömningsorgan som nämns i 28 § bedöma om identifieringstjänsten uppfyller kraven på interoperabilitet, informationssäkerhet, dataskydd och annan tillförlitlighet som föreskrivs i lagen om stark autentisering och betrodda elektroniska tjänster. Syftet med en kvalitetsrevision är att bedöma i vilken utsträckning en identifieringstjänst och företagets verksamhet uppfyller de uppställda kraven.

Enligt 31 § i autentiseringslagen är inspektionsberättelsen i kraft den tid som anges i den standard som användes vid bedömningen, dock högst 2 år.

Bestämmelser om Transport- och kommunikationsverkets rätt att meddela närmare föreskrifter om bedömningsgrunderna vid bedömningen av identifieringstjänster överensstämmelse finns i 42 §.

Bestämmelser om förutsättningarna för identifieringstjänster ingår i lagen om stark autentisering och betrodda elektroniska tjänsten samt delvis i Europeiska unionens kommissions genomförandeförordning (EU) 2015/1502 (förordning om tillitsnivåer) och i bilagan till den.

I 15 § i Kommunikationsverkets föreskrift 72A/2018 M preciseras de kravområden som ska ingå i en oberoende bedömning. I 16 § i föreskriften preciseras de kravområden som en leverantör av identifieringstjänster kan visa en egen utredning om.

Transport- och kommunikationsverkets anvisning 211/2019 O om bedömning av elektroniska identifieringstjänster, som utfärdats som stöd för kvalitetsrevision av identifieringstjänster, innehåller de allmänna kriterierna för kvalitetsrevision av identifieringstjänster samt särskilda kriterier gällande lösningar för mobilidentifiering. Leverantörerna av identifieringstjänster kan använda de nämnda

kriterierna eller andra kriterier eller kombinationer av andra kriterier som uppfyller kraven i 15 § i föreskrift 72.

3 Tidsplan

Inspektionsberättelserna jämte bilagor ska skickas till Transport- och kommunikationsverket senast 31.12.2021. Alla aktörer som inlett sin identifieringstjänst före år 2021 har samma tidsfrist år 2021.

Aktörerna kan lämna in den periodiska bedömningen även tidigare utan att det påverkar tidtabellen för följande bedömningsomgång.

Traficom bedömer och informerar vid behov separat om tidsfristerna för den periodiska bedömningen till eventuella nya identifieringstjänster som registreras.

4 Traficoms tillsynsriktlinjer för krypteringslösningen ChaCha20+Poly1305

Traficom bereder en ändring i föreskrift 72A/2018 M som avses träda i kraft vid början av 2022. Enligt 7 § i gällande föreskrift ska krypteringsalgoritmen som används i symmetrisk kryptering vara AES eller Serpent. Hashfunktionen ska vara SHA-2, SHA-3 eller Whirlpool.

I samband med periodiska bedömningar av identifieringstjänsternas överensstämmelse med krav och i samband med beredningen av föreskriften har det framkommit att det utöver de algoritmer och hashfunktioner som uppräknas i föreskriften även finns nyare tillräckligt säkra alternativ. Det bereds en ändring i föreskriften som kommer att även tillåta krypteringsalgoritmen ChaCha20 samt autentiserings-koden Poly1305.

Transport- och kommunikationsverket kommer inte att ingripa i användningen av ChaCha20-algoritmen och Poly1305-autentiseringskoden eller kräva att användningen ska upphöra vid sin tillsyn av överensstämmelse med krav för kryptering av identifieringstjänster.

5 Objekt som kräver speciell uppmärksamhet vid den periodiska bedömningen

5.1 Beskrivning av identifieringsmetoden

En beskrivning och/eller dokumentation om identifieringsmetoden och autentiseringsmekanismen ska bifogas inspektionsberättelsen. Beskrivningen ska vara tekniskt så noggrann att det är möjligt att fastslå att alla faktorer som är relevanta med tanke på kraven har beaktats i bedömningen. Beskrivningarna ska omfatta underleverantörerna.

- Vilka är de autentiseringsfaktorer som har använts för metoden (minst två faktorer från olika kategorier)?

- På vilket sätt har oberoendet mellan faktorerna säkerställts?

- På vilket sätt är autentiseringsfaktorerna bundna till innehavaren av identifieringsverktyget?

- Autentiseringsmekanism, dvs. en teknisk beskrivning av hur identifieringstransaktionerna genomförs

Inspektionsberättelsen ska också innehålla uppgifter om produkt- eller tjänstenamn så att användare och tjänster för ärendehantering kan identifiera tjänsten. Dessutom är det bra att uppge de benämningar som identifieringstjänsten använder internt, om benämningarna förekommer i inspektionsberättelsen eller dokumentationen om identifieringstjänsten.

5.2 Underleverans

I 15 § i Traficoms föreskrift M72 ingår bestämmelser om kriterier för kvalitetsrevision av en identifieringstjänst. Kvalitetsrevisionen ska omfatta identifieringstjänsten i sin helhet.

Leverantören av identifieringstjänster ska alltså även bedöma hela underleveranskedjan och dess överensstämmelse med krav. Alla underleverantörer ska identifieras och underleverantörens roll ska bedömas vid genomförandet av identifieringssystemet.

Underleveransorganisationens egen certifiering, t.ex. ISO 27001, kan beaktas men i bedömningen ska man fästa avseende vid certifieringarnas omfattning och lämplighet för de funktioner som deltar i genomförandet av identifieringssystemet. Att enbart tillgodoräkna certifieringarna täcker i allmänhet inte alla avsnitt och därför är leverantören av identifieringstjänster skyldig att se till att underleveransnätverkets överensstämmelse med krav bedöms som en del av de periodiska bedömningarna.

Vid relevanta ändringar i verksamheten ska en bedömning göras och en anmälan om ändringar och en inspektionsberättelse ska lämnas in innan ändringarna införs i produktionen. Relevanta ändringar inkluderar också byte eller ändringar i underleverantörernas underhåll, utrustning, system eller program.

5.3 Arkitekturbeskrivningar

Man har i regel skickat heltäckande beskrivningar av arkitekturen i samband med periodiska bedömningar 2019.

En bild, ett schema eller någon annan tydlig presentation av identifieringssystemets helhetsarkitektur ska bifogas inspektionsberättelsen. Utifrån arkitekturutredningen och inspektionsberättelsen ska det vara möjligt att säkerställa att alla relevanta faktorer som påverkar säkerheten i systemet har beaktats och att systemets arkitektur är säker. Beskrivningarna ska omfatta underleverantörerna.

- Systemkomponenterna för identifiering ska framgå av beskrivningen av systemets arkitektur.
- Utifrån utredningen ska det vara möjligt att uppfatta delarna av identifieringssystemet och leverantörerna av delarna, förbindelserna/bryggorna mellan olika delar, praxisen för skydd av förbindelser, gränssnitten mellan olika delar av systemet och andra faktorer.
- Alla funktionella relationer mellan de olika komponenterna i hela identifieringssystemet ska framgå av beskrivningen, bland annat åtskillnad av datalager, åtskillnad av presentationsskiktet och affärslogiken, kopplingar mellan bryggor/miljöer och skydd av kopplingarna samt säkerhetskontroller mellan externa aktörer.

- Beskrivningen bör innehålla information om nättopologi, komponenter på L3-nivå, till exempel brandväggar, servrar och kopplingar till övriga miljöer samt administrationsförbindelser om de har skilts åt.
- Dataflöden i identifieringsprocessen ska också beskrivas.
- Om systemet utnyttjar kommersiella komponenter eller produkter från molntjänster (Amazon Web Services, Google, Microsoft Azure osv.), ska produktkomponenterna uppges vid namn och inkludera dessa externa komponenter i bedömningen gällande underleverantörer.

5.4 Tekniska observationer

I punkt 2.5.2 i bedömningsanvisningen behandlas bedömningsmetoder som man kan använda vid bedömningen. Förutom rapporterna om inspektion, intervjuer och observationer som gjorts på plats ska man också lämna in rapporterna om tekniska observationer som bilaga.

5.5 SDK för mobilapp för identifiering

Flera mobilappar för identifiering har utförts så att man på marknaden har köpt en SDK som genomför identifieringen och som har kombinerats ihop med en större helhet (t.ex. bankapplikation) eller integrerats i en identifieringsapp som hör till leverantören av identifieringsverktyget. SDK är en väsentlig del av identifieringsmetoden, och själva SDK ska bedömas. Bedömningen kan utföras med hjälp av Traficoms kriterier för bedömning av mobilappar, men även tillverkarens egen bedömningsrapport som en tredje part har utfört kan visa att man iakttar kraven på överensstämmelse. Då ska man dock bifoga information om den bedömningsmetod som använts, den organisation som gjort bedömningen och den version som bedömts (och är den version som bedömts samma som används i mobilappen).

6 Rapportering till Traficom och Excel-fil

Traficom har gjort en valbar modell av rapporteringstabellen för bedömningen. Med tanke på att de periodiska bedömningarna sker smidigt är det önskvärt att denna tabell används i samband med periodiska bedömningar år 2021. Genom att använda den valbara tabellen kan leverantören av identifieringstjänster också enklare konkurrensutsätta bedömningar och försäkra sig om att alla nödvändiga delar blir bedömda. Tabellen baserar sig på Traficoms bedömningskriterier i anvisningen 211/2019 O.

Traficom påminner er också om att ju heltäckande bedömningsrapporterna och bilagorna till Traficom är, desto bättre går det att granska den periodiska bedömningen. Om det konstateras brister i bedömningsrapporten bör leverantören av identifieringstjänster lämna en heltäckande utredning av de planerade korrigeringsåtgärderna jämte tidtabell.