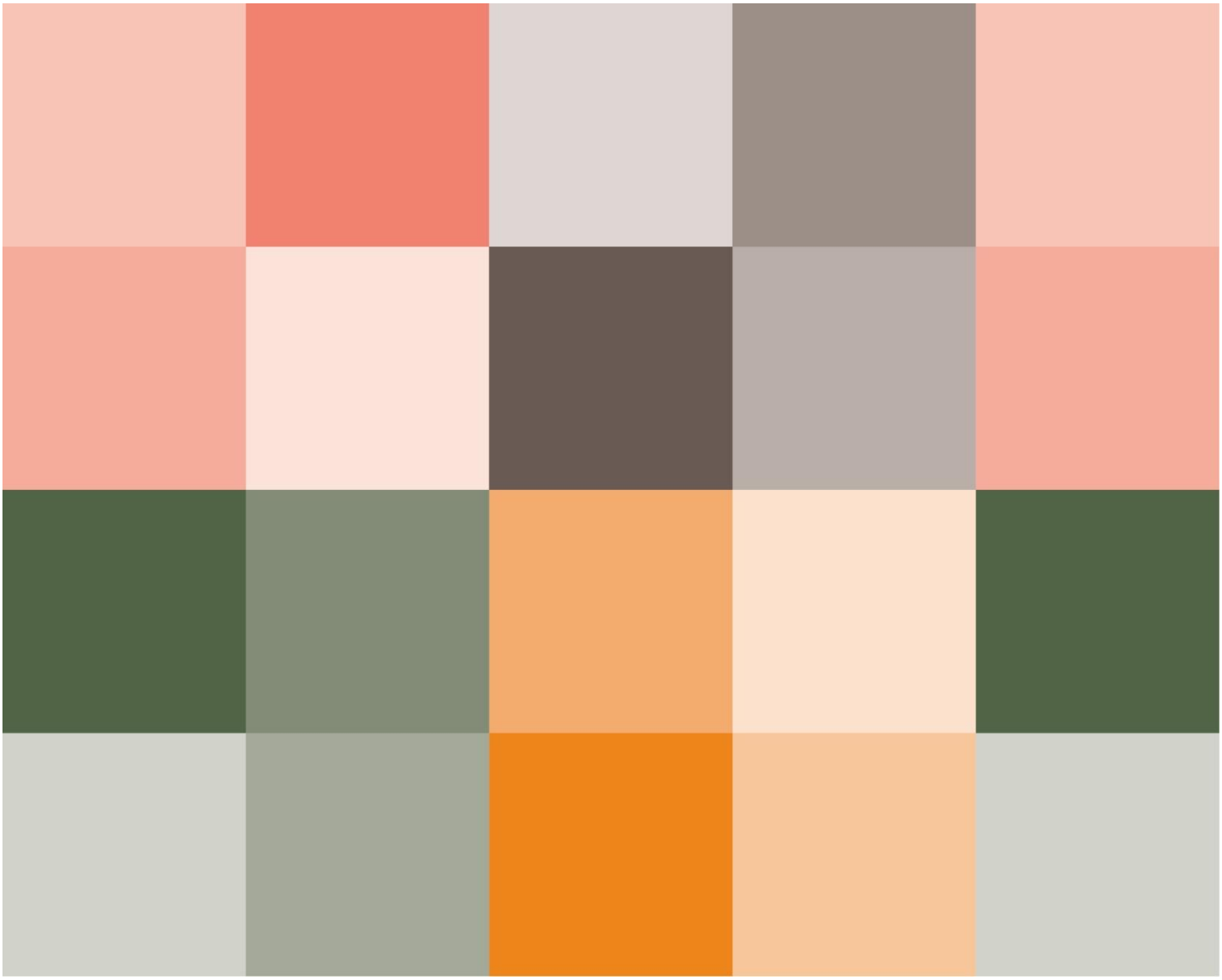

Spårbarhet

Förslag på byggblock

MYNDIGHETEN FÖR
DIGITAL FÖRVALTNING
Agency for Digital Government

Innehållsförteckning

1 Bakgrund och motiv

Syftar till att möjliggöra att i efterhand rekonstruera händelseförlopp.

I princip all verksamhet inom offentlig förvaltning, även utför av privata utförare, ställer höga krav på riktighet och medför krav på spårbarhet, dvs. att i efterhand kunna se vem som gjort vad och när detta gjordes (eller försökte göras). Säkerhetsåtgärder i form av loggning och logguppföljning ger förutsättningar att kunna spåra historiska förändringar hos informationstillgångar. Logguppföljning är en viktig åtgärd för att kunna upptäcka skadlig eller otillåten påverkan, obehörig åtkomst och funktionsstörningar i ett informationssystem. Att kunna jämföra loggar från flera delar i ett system ger möjlighet att efterkonstruera händelser och ge underlag för vilka åtgärder som ska genomföras för att minska risken att de sker igen.

Behovet av spårbarhet kan variera från enstaka atomära händelser (t ex skrivning till en fil) till komplexa händelsekedjor. Spårbarhet är alltid reaktivt. Analys av information för att förutse pågående eller framtida händelser är inte en del av spårbarhet.

Krav på spårbarhet är ofta domänspecifik på grund av legala krav.

1.1 Förmågor

I regeringsuppdraget Säkert och effektivt informationsutbyte, genomfördes en analys av förmågor kopplade till området Tillit och säkerhet. Byggblocket Spårbarhet kopplades till 2 förmågor.

1.1.1 Förmåga att följa ett händelseförlopp

Det är viktigt att kunna återskapa (eller i alla fall utreda) ett händelseförlopp vid ett informationsutbyte i systemet. För att detta ska vara görbart behöver de som kommunicerar ha samma identitet i samtliga ingående system. För den centrala infrastrukturen kan det behövs en central funktion för att lagra händelser medan informationsägare och datavärdar kan skapa lokal spårbarhetsinformation. Det kan även uppstå komplexa kommunikationsmönster där hela kommunikationsflöden behöver kunna följas.

1.1.2 Förhindra otillbörlig förändring

För att kunna tillse att information är riktigt (bibehållen integritet, ej datakvalité) behövs förmågan att förhindra otillåten förändring, oaktat om denna är medveten eller ej. Vid informationsutbyte är det framför allt i transporten av information som mekanismer behöver finnas för att förhindra eller upptäcka sådana förändringar.

2 Befintliga lösningar

Det saknas i dag en nationell gemensam lösning för hantering av spårbarhet. Dock hanteras detta som särskilda lösningar för varje unikt informationsutbyte.

2.1 Omvärld

Omvärldsanalysen som genomfördes i regeringsuppdraget Säkert och effektivt informationsutbyte beskriver hur andra nationer hantera frågan om spårbarhet. Nedan återfinns en liten del av hela analysen.

I princip samtliga lösningar i de analyserade länderna har funktionalitet för spårbarhet i form av loggning av meddelanden och signering av meddelanden. Omfattningen av loggningen varierar beroende på olika förutsättningar i de olika länderna. Vissa lösningar loggar hela meddelandet (inklusive payloaden) medan andra bara loggar metadata över transaktionen. Ofta beror detta på lokala rättsliga förutsättningar och krav snarare än tekniska begränsningar.

3 Förslaget belyst ur olika perspektiv

3.1 Politiskt

Fr4ån tidigare regeringsuppdrag finns förslag på byggblocket spårbarhet som en del av området Tillit och säkerhet. Generellt ses området avseende både IT- och informationssäkerhet som högt prioriterat område i det politiska landskapet idag. Flera olika incidenter har visat på den politiska vikten av att ha främja en agenda som starkt inriktar sig på säkerhet.

3.2 Juridiskt

Kraven i dataskyddsförordningen är sammankopplad med myndighets säkerhetsansvar på flera plan. Det är viktigt att information klassas för att klargöra vilket skyddsvärde den har oavsett om den påverkas av dataskyddsförordningen eller inte. Som en helhet måste inbyggd säkerhet (eller integritet) omhändertas vilket påverkar ett systems hela livscykel, från förstudie och kravställning via design (formgivning) och utveckling till användning samt avveckling. Det påverkar beställare och kravställare som är ansvariga för personuppgiftsbehandlingen likväl som leverantören av de produkter och tjänster som används. Begrepp som personuppgiftsansvar, ändamålsbegränsning, informationsägarskap, rättslig grund, de registrerades rättigheter, uppgiftsminimering, behörighetsadministration, arkivering och spårbarhet måste omhändertas inom ramen för dataskyddsförordningens regelverk.

3.3 Organisatorisk/verksamhetsmässigt

Den digitala infrastrukturen som utvecklas syftar till att öka och effektivisera informationsutbytet inom och med offentlig sektor. Infrastrukturen bidra till att det digitala ekosystemet utvecklas. Ur detta perspektiv framgår att spårbarhet avses att kunna visa hur information har flödat mellan många olika aktörer mellan olika sektorer och organisationer.

3.4 Semantiskt

Ett troligt scenario för det föreslagna byggblocket är att det resulterar i någon typ av ramverk för spårbarhet. Kanske finns detta ramverk i ett större och bredare säkerhetssammanhang tillsammans med andra byggblock inom tillit och säkerhet. Oavsett den frågan är det troligt att ett ramverk kommer styra semantiken i loggning. Att rätt information lagras i loggar och i rätt struktur.

3.5 Tekniskt

Det är oklart om byggblocket avser definiera, utveckla eller någon utveckla en teknisk lösning, system eller tjänst. Behoven av det föreslagna byggblocket visar att varje aktör i en informationsutbytes kedja behöver kunna hantera kraven på spårbarhet så att en eventuell spårning är möjlig. Ett troligt scenario är att ett ramverk tas fram och där ställs tekniska krav på varje aktör som använder infrastrukturen ska uppnå kraven på spårbarhet.

4 Intressenter

4.1 Berörda aktörer

Flera olika aspekter inom området tillit och säkerhet kommer påverka samtliga aktörer som avser använda den digitala infrastrukturen.

4.2 Berörda roller

Arkitekter, IT- och informationssäkerhetsansvariga/-experter, informationsansvariga.

5 Förslag på leverabler

Ingen analys av frågan har genomförts men ett troligt scenario är att byggblocket levererar ett ramverk för spårbarhet. Eventuell ingår ett sådant ramverk samordnat med flera säkerhetsrelaterade ramverk.

6 Potentiell nytta

Vi uppskattar att byggblocket Spårbarhet har potential att skapa samhällsekonomiska nyttor genom att i efterhand återskapa och spåra händelser. Detta förväntas framförallt användas för att spåra oönskade händelser, där en oönskad händelse kan vara någon form av intrång inom den förvaltningsgemensamma digitala infrastrukturen. Genom att återskapa händelser skapas underlag för vilka åtgärder som krävs för att minska risken för att det sker igen. Detta skapar både effektivitetsvinster och ökad kvalitet. Dessa nyttor förväntas framförallt tillfalla offentlig sektor. Byggblocket kommer även bidra med en ökad säkerhet för andra digitala tjänster inom den förvaltningsgemensamma digitala infrastrukturen. Det skapar nyttor även för företag och medborgare.

Byggblocket Spårbarhet är i ett mycket tidigt utvecklingsskede och det är därför ännu inte möjligt att med säkerhet säga vilka nyttor byggblocket kommer realisera. Det är inte heller möjligt att kvantitativt beräkna hur stora nyttorna kommer att bli eller att uppskatta vilka aktörer i samhället som nyttorna kommer tillfalla.

Baserat på den information som finns om byggblocket Spårbarhet och dess roll inom den förvaltningsgemensamma digitala infrastrukturen är det möjligt att

identifiera områden där Spårbarhet skulle kunna skapa nyttor. Vi menar att nyttorna skulle kunna innefatta:

- Tids- och kostnadsbesparingar genom en effektiviserad och förenklad implementering av Spårbarhet när ett nationellt system för detta finns.
- Tids- och kostnadsbesparingar genom att felsökning och incidenthantering blir mer effektiv när logginformation från ingående system blir jämförbara.
- Ökad informationssäkerhet eftersom larm vid överträdelser av givna tröskelvärden möjliggör snabbt agerande, vilket skapar nyttor genom ökad kvalitet
- Ökad informationssäkerhet när konfidentialitet och riktighet av loggar säkerställs genom strikta behörighetskrav till loggarna, vilket skapar nyttor genom ökad kvalitet
- Ökad övergripande säkerhet för den förvaltningsgemensamma digitala infrastrukturen genom en standardisering av loggning och logguppföljning. Även detta förväntas skapa nyttor genom ökad kvalitet.

Vi föreslår att nyttoanalysen för Spårbarhet färdigställs med hjälp av samma metod[1] som använts för övriga byggblock när syftet med byggblocket tydliggjorts och mer information om byggblocket finns tillgängligt.

7 Risk- och konsekvensanalys

En övergripande risk- och konsekvensanalys har genomförts för förslaget på byggblocket. De identifierade riskerna och förslag på åtgärder finns dokumenterat på en skyddad lagringsyta hos DIGG.

Byggblocket påverkar av den förvaltningsgemensamma digitala infrastrukturen vilket visas i den dokumenterade riskanalysen. Dokumenterade risker, sårbarheter och hot bedöms i beskrivna scenarion kunna ge konsekvenser för hela den digitala infrastrukturen och behöver analyseras vidare. Förslag till åtgärder och hantering av risker, hot och sårbarheter i riskarbete har visat sig kunna minska

[1] För en beskrivning av denna metod, se Nyttoanalysens metodbilaga, Slutrapportens bilagor, https://www.digg.se/informationsutbyte-och-grunddata

sannolikheten och sänka konsekvenser om risken ändå inträffar på både kort och lång sikt.

8 Förslag på genomförande

En lösning för att möta behoven av spårbarhet ingår som en del av området tillit och säkerhet. En hittills obesvarad fråga är om det är lämpligt, effektivt eller rimligt att fristående utveckla ett byggblock för spårbarhet. Det kan därför finnas ett syfte i att genomföra en analys om flera säkerhetsrelaterade byggblock bör utvecklas tillsammans, parallellt eller på annat sätt samordnas i sin utveckling.

I ett fördjupat arbete kan t.ex. nyttoanalysen för Spårbarhet färdigställs med hjälp av samma metod som använts för övriga byggblock när riktningen för byggblocket tydliggjorts och mer information om byggblocket finns tillgängligt.

I ett fortsatt arbetet kärvs att ett fortsatt systematiskt informationssäkerhetsarbete sker genom att löpande och kontinuerliga värderingar av sårbarheter, risker och hot inom byggblocket utifrån vilken etapp/fas byggblocket befinner sig i. Det behövs ett riskarbete av beroenden mellan byggblock inom den digitala infrastrukturen och mot grunddatadomänerna, för att riskanalysera och fastställa robusthet och säkerhetsskydd för helheten i den digitala infrastrukturen.