KOMBIT

Version 1.2

Instruks til gennemførsel af og rapportering om penetrationstest

Indholdsfortegnelse

1. Formål

Denne instruks er udarbejdet af KOMBIT til brug for KOMBITs kontrakter med leverandører om levering af drift, vedligeholdelse mm. af de enkelte it-systemer (i de enkelte kontrakter benævnt "Systemet").

Instruksen skal følges af leverandørerne ved gennemførsel af og rapportering om penetrationstest under den enkelte kontrakt med KOMBIT.

2. Roller og Ansvar

Det er forudsat, at data, der behandles i Systemet, i mange tilfælde vil være personoplysninger i henhold til persondatalovgivningen, eller på anden måde fortrolige oplysninger. For at sikre, at oplysningerne er tilstrækkeligt sikret mod uvedkommende adgang til data, skal det sikres, at systemet og driftsmiljøet ikke kan penetreres. Alle miljøer, som indeholder produktionsdata, herunder også pseudonymiseret data, skal have foretaget en fuld penetrationstest. Leverandøren er forpligtiget til at bruge et eksternt anerkendt sikkerhedsfirma, godkendt af KOMBIT, til gennemførsel af penetrationstest.

Til brug for KOMBITs og de(n) dataansvarliges tilsyn med leverandøren (underdatabehandler) og dennes underleverandører (under-underdatabehandlere) skal leverandøren i henhold til nedenstående levere en detaljeret rapport samt en selvstændig erklæring, begge udarbejdet af det eksterne sikkerhedsfirma.

De dataansvarlige har en forpligtigelse til at føre tilsyn og har derfor ret til at få den selvstændige erklæring udleveret. I særlige tilfælde vil den detaljerede rapport blive forevist for den dataansvarlige, men ikke udleveret.

3. Omfang

Den detaljerede rapport skal indeholde følgende:

- Detaljeret beskrivelse af de test, som er gennemført, herunder dato for gennemført tests
- Er der afdækket risici og/eller svagheder, herunder i relation til overholdelse af persondatalovgivningen, driftsmiljøet og/eller sikkerhedsprocedurer, skal disse detaljeret fremgå af rapporten
- Beskrivelse af nødvendige tiltag for at fjerne sikkerhedsrisici
- En overordnet risikoanalyse
- Erklæring på, om sikkerhedsfirmaet kan stå inde for sikkerheden for systemet og driftsmiljøet. Erklæringen skal være baseret på de standarder, som betragtes som best practice på området – eksempelvis OWASP og/eller PTES.

Den selvstændige erklæring skal indeholde følgende:

- Beskrivelse af, hvornår der er gennemført penetrationstest
- Erklæring på, om sikkerhedsfirmaet kan stå inde for sikkerheden for systemet og driftsmiljøet. Erklæringen skal være baseret på de standarder, som betragtes som best practice på området – eksempelvis OWASP og/eller PTES.

4. Proces for udarbejdelse af penetrationstest

Leverandører skal forinden påbegyndelse af penetrationstest sammen med KOMBIT og sikkerhedsfirmaet, på 3-partsmøder indkaldt af leverandøren, foretage nedenstående:

- Indledningsvist gennemgå det tekniske setup for systemet og driftsmiljøet med særligt fokus på de forhold, som er relevante i forbindelse med leverandørens leverancer under kontrakten med KOMBIT.

- Identificere og gennemgå det tekniske setup leveret af underleverandører.
- Med udgangspunkt i best practice detaljeret gennemgå og aftale, hvilke typer af penetrationstests som skal gennemføres ud fra sikkerhedsfirmaets anbefalinger.
- Indarbejde KOMBITs skriftlige ønsker til specifikke penetrationstests.
- Tilrettelægge en proces, som sikrer involvering af KOMBIT inden underskrift af erklæring vedr. sikkerheden for systemet og driftsmiljøet med henblik på at afklare eventuelle anmærkninger fra sikkerhedsfirmaet.

Såfremt der i henhold til kontrakten med KOMBIT kan anvendes en generel tværgående rapport, skal leverandøren sikre, at alle relevante penetrationstests er dækket ind for alle systemer og driftsmiljøer, samt at sikkerhedsfirmaet skriftligt redegør for, at systemet og driftsmiljøet indgår i den samlede penetrationsrapport.

Såfremt den detaljerede rapport indeholder bemærkninger, kommentering mv. om forbedringsområder for sikkerheden af systemet og driftsmiljøet, skal leverandøren samtidig med fremsendelsen af rapporten fremsende en fyldestgørende handlingsplan, som beskriver, hvordan og hvornår de omhandlede forhold bringes i orden.

Såfremt der identificeres sikkerhedshændelser (Security Incidents) eller risiko for sikkerhedshændelser i forbindelse med penetrationstest, skal leverandøren håndtere dette som et prioritet A Incident i henhold til driftskontrakten med KOMBIT.

5. Version historik

Dato for revidering:	**Revideret af:**
01/09/2023	Service Management