Karaktergivende opgave i it-sikkerhed

Carsten Jørgensen og Troels Larsen

DIKU, blok 4, 10. juni 2013

Generelt

Opgaven stilles 10. juni 2013 og skal afleveres via Absalon senest 17. juni kl. 23:55.

Opgavebesvarelsen er individuel, i den forstand, at hver enkelt skal skrive og aflevere sin egen rapport, som dokumenterer eget arbejde. Det er tilladt at diskutere opgaven med andre kursusdeltagere, men den skriftlige rapport skal afspejle egne tanker om (og eget arbejde med) det valgte emne.

Dette vil også sige, at alt materiale, som er hentet udefra (citater mv.) skal markeres tydeligt og med kildeangivelse.

Opgaver

Der skal løses én af de tre nedenstående opgaver; der kan vælges frit mellem dem.

OPGAVE A: Sikkerhedsanalyse af BYOD

Den moderne medarbejder vil gerne bruge sine private mobile enheder på arbejdet, fx sin egen mobiltelefon og tablet. Det er del af den voksende trend "bring-your-own-device" (BOYD). I denne opgave skal der foretages en sikkerhedsanalyse af BYOD.

Der tages i denne opgave udgangspunkt i den fiktive virksomhed BIOmedix, som har optrådt i kursets øvelser. Konkret ønsker BIOmedix, at medarbejdernes mobile enheder skal forbinde til virksomhedens brugernetværk ("workstation net", jf. øvelse fem) med brug af WiFi for at synkronisere med mailserveren og desuden have samme rettigheder som de øvrige maskiner på brugernetværket (jf. firewall politikken fra øvelse fem).

Du bør i din sikkerhedsanalyse af BYOD bl.a. komme ind på, hvordan autentificeringen af de mobile enheder bør foregå (passwords, certifikater, tokens, biometri, protokoller, m.m.), før de får adgang til brugernetværket, samt overvejelserne omkring samblanding af private data og virksomhedsdata på de mobile enheder. Din analyse må ikke henvise til arbejde udført i øvelserne.

OPGAVE B: Sikkerhedsanalyse af sociale medier

Moderne virksomheder har en aktiv tilstedeværelse på sociale medier. I denne opgave skal der foretages en sikkerhedsanalyse af sådanne brug af sociale medier.

Der tages i denne opgave også udgangspunkt i BIOmedix. Hos BIOmedix er det kommunikationsafdelingen, som står for at opdatere BIOmedix' profiler på Facebook, Twitter og LinkedIn. De har én konto på hvert medie, hvis brugernavn og password deles blandt kommunikationsmedarbejderne. Derudover har BIOmedix et ikke-offentligt socialt netværk på tjenesten Yammer, som bruges som en slags intern Facebook og samarbejdsplatform, hvor medarbejderne opdaterer deres arbejdsstatus, danner projektgrupper og udveksler forretningsidéer og filer. Enkelte samarbejdspartnere har også adgang til nogle af projektgrupperne på BIOmedix' Yammer netværk.

Du bør i din sikkerhedsanalyse bl.a. komme ind på, hvad, om noget, angrebet på AP's Twitter-konto og password-lækagen fra LinkedIn har af relevans for BIOmedix, samt overvejelser omkring ejerskab og placering af data på de sociale medier. Din analyse må ikke henvise til arbejde udført i øvelserne.

OPGAVE C: Sikkerhedsanalyse af NemID-løsningen

NemID-løsningen har været i drift siden sommer 2010. I denne opgave skal det analyseres om NemID er en sikkerhedsmæssig tilfredsstillende løsning.

Såvel nøgleudstedelse og -opbevaring som brug til autentifikation (fx login til netbank), signering og i e-mail samt valg af implementeringssprog, tilgængelighedsproblematikker og kendte angreb bør dækkes. Du bør også komme ind på, hvordan du ville designe løsningen i dag.

Der kan tages udgangspunkt i Peter Lind Damkjærs præsentation (tilgængelig på Absalon under "Undervisningsmateriale"), men analysen bør også inddrage andre kilder, fx om 2-faktor autentifikation og de teoretiske og praktiske problemer, offentligheden peger på.

Krav til løsning

Rapporten skal dokumentere opfyldelsen af kursets læringsmål: ”En studerende, der fuldt ud har opfyldt kursets mål, vil kunne:

1. Opremse alle de vigtigste problemstillinger der skal adresseres i en sikkerhedsanalyse af et givent system
2. Definere operationelle sikkerhedsmål for et givent system
3. Analysere en systemanvendelse og identificere normale trusler, sårbarheder og risici
4. Opremse mulige foranstaltninger mod de normale trusler, sårbarheder og risici i et givent sikkerhedssystem
5. Forklare og sammenligne væsentlige teknologier inden for it-sikkerhed, og herunder kryptografiske teknikker og protokoller
6. Analysere og diskutere de nødvendige sikkerhedsmekanismer i et givent sikkerhedssystem
7. Implementere (dele af) et sikkerhedssystem[1]
8. Foretage en (ikke formel) evaluering af en samling af sikkerhedspolitikker og -mekanismer med henblik på at afgøre om de tilfredsstiller en given liste af sikkerhedsmål
9. Dokumentere deres arbejde med sikkerhedsprocessen i en velskrevet og koncis rapport”

Sidste punkt opfyldes ved, at rapporten er kort (ti sider eller derunder, idet forside, indholdsfortegnelse, litteraturliste eller illustrationer ikke medregnes) og veldisponeret, fx med afsnit der inkluderer indledning (formål og afgrænsning), tekniske afsnit, konklusion med en opsummering af vigtigste ideer og resultater, og en referenceliste med al den anvendte litteratur.

Der lægges vægt på at rapporten afspejler en klart og systematisk tilgang til sikkerhedsanalyse, inklusive hvor relevant:

- Resumé af systemet under analyse, med fremhævelse af aspekter af særlig interesse
- Identifikation af aktiver og sikkerhedsmål, samt deres vigtighed
- Identifikation af trusselsaktører og trusler
- Identifikation af sårbarheder
- Identifikation af eksisterende modforanstaltninger
- Evaluering af risici (overvej tabelopsætning)
- Diskussion af mulige yderligere modforanstaltninger og andre "større" sammenhænge såsom etik, sandsynlighed systemet vil udvikle sig, lovgivning, etc.
- Konklusion

Opgaveteksten er ikke særlig detaljeret. Det er en del af opgaven at afgrænse emnet/opgaven og at søge yderligere viden om emnet. Disse afgrænsninger, fortolkninger, antagelser, m.m. skal beskrives klart i rapporten. Rapporten må afleveres på dansk eller engelsk.

[1] Bemærk: Punktet om implementering ikke er aktuelt i denne opgave.