Universitetet i Oslo
IN2120 Informasjonssikkerhet
Høst 2018
Workshop-spørsmål

Forelesning 5: Ledelse/styring av informasjonssikkerhet, Menneskelige faktorer for info-sikkerhet

Spørsmål 1

- Se på listen over standarder i ISO27000 serien, for eksempel på Wikipedia, http://en.wikipedia.org/wiki/ISO/IEC_27000-series
- Se på NIST SP800 (Special Publications) serien på: http://csrc.nist.gov/publications/PubsSPs.html

a. Prøv å identifisere lignende standarder i ISO 27000-serien og i NIST SP800 serien.
b. Hvilke faktorer driver utviklingen av sikkerhetsstandarder generelt, og hva kan grunne være for at ulike organisasjoner utvikler separate sett med lignende standarder?

Spørsmål 2

a. Hvordan er standardene ISO/IEC 27001 og ISO/IEC 27002-relatert?
b. Hva betyr "system" i forkortelsen ISMS (Information Security Management System)?
c. Hvilken av ovennevnte standarder danner grunnlag for sertifisering, og hvorfor?
d. Hvordan bør en organisasjon avgjøre hvilke sikkerhetstiltak som skal implementeres?

Spørsmål 3

a. ISO27002 og 20CSC har samme fokus. Forsøk å sette opp en korrespondans mellom de 14 kategoriene av sikkerhetstiltak i ISO27002 og de 20 kategoriene av sikkerhetstiltak i 20CSC. Presentasjonen fra forelesningen (s.16 og s.18) gir en oversikt over kategoriene. Legg f.eks. s.16 og s.18 ved siden av hverandre og trekk/tenk streker mellom dem.
b. Gjør en vurdering av hvor godt sammenfallende kategoriene fra ISO27002 og 20CSC er.

Spørsmål 4

Standardene *ISO/IEC 27002* og *CIS-20CSC-V7* beskriver en rekke sikkerhetstiltak. Info om standardene fins på wikien for IN2120.

a. Hvordan kan effektiviteten til et bestemt sikkerhetstiltak måles? Nedenfor finner du eksempler på sikkerhetstiltak fra *CIS-20CSC-V7*.
b. Hvordan kan effektiviteten til disse tiltakene måles? Du kan foreslå en målemetode, eller du kan ta en titt på tilhørende dokument *CIS-Controls-Measures-and-Metrics-V7*.
   i) CIS Control 2.2. Ensure that Software is Supported by the Vendor
   ii) CIS Control 16.9. Disable Dormant Accounts

Spørsmål 5

Anta at selskap A og selskap B av samme størrelse blir ofre for cyber-angrep, og at begge selskapene får betydelige tap som negativt påvirker kunder og aksjonærer. Under etterforskning av hendelsene ble det funnet at selskap A hadde implementert et ISMS og hadde god modenhet for ledelse/styring av informasjonssikkerhet, mens selskap B manglet ISMS og bare ad-hoc ledelse/styring av informasjonssikkerhet. Hvis man antar at tap for begge selskapene var i samme størrelsesorden, forklare mulige forskjeller for konsekvenser og sanksjoner mot ledelsen av selskapene.

Spørsmål 6

a. Beskriv måter å bruke Social Engineering for;
   1. få uautorisert tilgang til et selskap bygning,
   2. installere skadevare på PCen til administrerende direktør i et selskap.

   Du kan få inspirasjon fra SANS InfoSec Reading Room on Social Engineering (`http://www.sans.org/rr/whitepapers/engineering/`) eller andre relevante kilder.
b. Forestill deg at selskapets ansatte utgjør funksjonen for «intrusion detection» mot sosial manipulerings-angrep. Hva ville være en «falsk positiv» og en «falsk negativ» deteksjon i dette scenariet?
c. La oss se på menneskelig forsvar mot sosial manipuleringsangrep som en analogi til brannmurer i nettverk. For å gi tilstrekkelig beskyttelse, må brannmurer være riktig programmert og konfigurert. Hva ville være en analog prosess for å sørge for at ansatte gir tilstrekkelig beskyttelse mot sosial manipuleringsangrep?