Informasjonssikkerhet: Teori og praksis

Audun Jøsang
2. utgave 2023
Universitetsforlaget

Oppgaver

Kapittel 2: Angrepsvektorer og skadevare

Oppgave 1: Angrepsvektorer

a. Hva er den vanligste angrepsvektoren for cyberangrep?
b. Hvordan kan deepfake-stemme og video brukes i cyberangrep?
c. Hvordan kan USB-enheter som f.eks. (ligner på) en minnepinne brukes for å angripe en datamaskin?

Oppgave 2: Leveransekjedeangrep

a. Forklar hva som menes med leveransekjedesårbarheter.
b. Beskriv eksempler på leveransekjedeangrep som har skjedd i de siste årene.
c. Hvilke tiltak kan en virksomhet benytte for å redusere leveransekjederisiko (eng. Cyber Supply Chain Risk Management, C-SCRM)?

Oppgave 3: Bottnett

a. Hva er et bottnett?
b. Hva er et DDoS, og hvordan kan et bottnett brukes til å gjøre et DDoS-angrep?
c. Mirai er en skadevare som ble brukt til å «ta ned» internett i store deler av USA gjennom et angrep på en Dyn DNS en dag i oktober 2016. Beskriv kort Mirai og hvordan dette angrepet ble utført

Oppgave 4: XSS

Du er medlem av en ny sosial plattform kalt FAGSNAKK utviklet av og for studenter ved universitetet hvor dere kan ha faglige diskusjoner, organisert med én side for hvert fag. En dag er FAGSNAKK-siden full av det samme hundebildet som (det ser ut som) har blitt postet av ulike brukere (inkludert deg), uten at noen kan huske at de har gjort. En medelev mener at dette kan skyldes en XSS-sårbarhet i FAGSNAKK og at bildene er et resultat av et XSS-angrep.

a. Hva et XSS-angrep?
b. Hvordan kan XSS-angrepet beskrevet ovenfor vært gjennomført?
c. Hvordan kunne angrepet på FAGSNAKK ha vært forhindret?