Universitetet i Oslo
IN2120 Informasjonssikkerhet
Høst 2023
Teoretiske oppgaver med løsningsforslag

Teori 5 (Del 5): 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?

Løsningsforslag

a. Phishing, også kalt nettfisking, er den vanligste cyberangrepsvektoren. Phishing er typisk kombinert med en eller flere andre angrepstyper som skadelige vedlegg eller lenker til skadelige nettsider.

b. Deepfake stemme som del av angrep er for eksempel ved å spoofe en anne persons identitet over telefonsamtaler. Flere hendelser er rapportert, f.eks. https://www.businessinsider.com/couple-canada-reportedly-lost-21000-in-ai-generated-voice-scam-2023-3

   Deepfake bilde og stemme som del av angrep er for eksempel å spoofe en annen persons identitet i zoom/teams-møter, eller å spoofe identitet i videoanrop, f.eks. https://gizmodo.com/deepfake-ai-scammer-money-wiring-china-1850461160

c. En USB-enhet som ligner på en minnepinne kan konfigureres som en HID-enhet (Human Interface Device), som lurer datamaskinen til å tro at den er et tastatur og sender en strøm av tastetrykk som utgjør skadelige kommandoer.

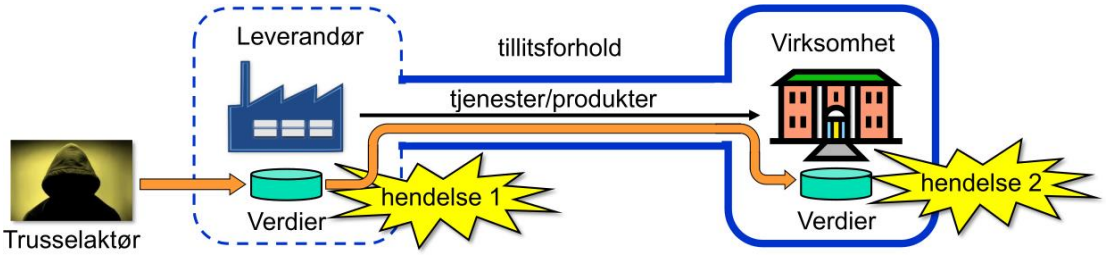
Oppgave 2: Leveransekjedeangrep

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)?

Løsningsforslag

a. Et leveransekjedeangrep består av to trinn, der det første angrepet kompromitterer og skaper en sårbarhet i et produkt eller tjeneste hos en leverandør, som deretter gjøre det mulig å angripe leverandørens kunder. Et angrep som bare utnytter en utilsiktet sårbarhet i en leveransekjede er altså ikke et leveansekjedeangrep. Et angrep på leverandøren kan f.eks. legger inn en

bakdør i programvaren som leverandøren produserer og leverer. Når den kompromitterte programvaren installeres hos virksomheten, har sårbarheten forplanter seg til virksomheten. Figuren nedenfor illustrerer dette prinsippet.



b. Alvorlige leveransekjedeangrep som skjedde i 2021 er:

- *SolarWinds Orion: IT-Styring og fjernmonitorering.*

  SolarWinds er et selskap som leverer programvare for styring og overvåking. Orion er SolarWinds sitt nettverk styringssystem (NMS) produkt. I desember 2020 ble det oppdaget at Orion var blitt kompromittert. Omfattende etterforskning viste at angripere fikk tilgang til SolarWinds-nettverket, muligens ved å utnytte en nulldagssårbarhet i en tredjeparts applikasjon eller enhet, et inntrengningsangrep eller gjennom sosial manipulering. Etter å ha fått tilgang samlet angriperne informasjon over en lengre periode. Skadevaren ble injisert inn i Orion, og den kompromitterte programvaren ble deretter lastet ned direkte av kundene og ble brukt til å samle inn og stjele informasjon. Omrent 18 000 av SolarWinds sine 33 000 Orion-kunder hadde skadevaren i sine nett, men bare en brøkdel ble angrepet. Norges Bank hadde også skadevaren, men ble antagelig ikke angrepet. Angrepet ble attribuert til APT29-gruppen.

- *Kaseya: IT-administrasjonsverktøy som ble kompromittert med løsepengevirus*

  Kaseya er en programvareleverandør som spesialiserer seg på fjernmonitorering og verktøy for IT-administrasjon. Den tilbyr VSA (Virtual System/Server Administrator) programvare som kunder kan laste ned eller benytte som skytjenester. MSPer (Managed Service Providers) kan bruke VSA-programvaren og tilby ulike IT-tjenester til andre kunder. I juli 2021 utnyttet angripere en nulldagssårbarhet i Kaseyas egne systemer som gjorde det mulig for angriperne å eksternt kjøre kommandoer på VSA-programvaren til Kaseyas kunder. Kaseya sendte ut oppdateringer til alle VSA-servere fredag 2. juli 2021 som utførte skadevare fra angriperne. Denne skadevaren distribuerte i sin tur løsepengevirus til kundene med nettverk som ble administrert gjennom VSA.

c. Det er utfordrende å styre risiko forbundet med leveransekjedesårbarheter, fordi virksomheten som regel har begrenset mulighet for å gjøre risikovurdering og revisjon i leverandørens infrastruktur. En generell tilnærming til sikkerhet i leveransekjeder er å sørge for at risikostyring for digitale leveransekjeder er

inkludert i virksomhetens ISMS. Gjennom avtaler kan virksomheter kreve uavhengige rapporter om sikkerhetsrevisjon og risikovurdering av leverandører. Elementer i kontrakter kan f.eks. være:

- Rapportering og varslingsplikt om sikkerhetsrelaterte ting som sikkerhetshendelser sikkerhetspolicyer og endringer av eierstruktur.
- Tilsyn og revisjonsrapporter om sikkerhet.
- Nivå for risikoaksept hos underleverandør.
- Forventet oppetid av tjenester, og underleverandørens risikoaksept for overholdelse av denne.
- Endrings- og exit-klausuler, f.eks. basert på avvik eller endring i eierstruktur

Virksomheter bør i alle fall følge med på rapporterte sårbarheter i tredjepartsprogramvare, og sørge for rask oppdatering for å fjerne sårbarheter. En anerkjent veileder for C-SCRM er NISTs SP 800-161 Rev. 1 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (2022). Dette dekkes også av NSMs grunnprinsipp 2.1: Ivareta sikkerhet i anskaffelses- og utviklingsprosesser.

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

Løsningsforslag

a. Begrepet "bottnett" refererer vanligvis til en samling av kompromitterte computere (kalt bots eller zombie-maskiner) som kjører bott-skadevare, vanligvis installert via drive-by nedlastinger som utnytter sårbarheter i nettlesere, ormer, trojanere, eller bakdører, under en felles kommando- og styringsinfrastruktur.
b. Et DoS-angrep (tjenestenekt-angrep) er et forsøk på å hindre at legitime brukere av en tjeneste får tilgang til tjenesten. Når dette angrepet kommer fra en enkel node eller nettverk, så er det bare referert til som et DoS-angrep. En mer alvorlig trussel utgjøres av et DDoS-angrep (Distribuert DoS). I et DDoS-angrep, er en angriper i stand til å rekruttere en rekke noder over Internett til samtidig eller på en koordinert måte lansere et angrep på målet. Et bottnett er nettopp et sett av noder som kan koordineres for DDoS-angrep.
c. Mirai utnyttet sårbarheter i IoT (Internet of things) enheter og brukte dem til å danne et bottnett. Mirai er en dataorm som spredde seg og i dette tilfellet er det estimert at botnettet bestod av ca 100 000 enheter. Dette ble så brukt i et DDoS angrep til å ta ned Dyn DNS som blant annet betydde at f.eks. Twitter og Netflix ikke kunne nås i USA og deler av Europa, med en trafikk på 1,2 Tbps mot Dyn DNS.

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?

Løsningsforslag

a. XSS (Skripting på tvers av noder) er en angrepsteknikk som lurer en webside til å reflektere mottatte data tilbake til netlesere der dataene blir tolket og eksekvert som skript. Når en nettleser mottar og kjører et XSS-skript, vil angriperen ha tilgang til nettleserens innhold (informasjonskapsler, logg, programversjon osv.). XSS-angrep utnytter Web-servere som et springbrett for å angripe nettlesere/klienter.
b. I dette tilfellet kunne en bruker ha inkludert i en kommentar på siden et Javascript som legger til en kommentar på veggen som inneholder hundebildet. Når en bruker åpner siden vil kommentaren lastes som medfører at scriptet kjøres. Dette vil da kjøres som den aktuelle brukeren og det vil derfor se ut som brukeren lastet det opp.
c. XSS kan forebygges ved at webservere alltid filtrerer bort skadelig kode de mottar, og forhindrer at det legges ut på en webside. I dette tilfellet må FAGSNAKK sjekke at kommentarer ikke inneholder (skadelig) Javascript-kode.

Oppgave 5 Tilgang for skadevare (eksamensoppgave 2023):

3.1 Tilgang for skadevare

Du kjører uheldigvis skadevare på maskinen din med din administratorbruker. Du har slått av UAC (User Account Control) på maskinen din – Hvilke rettigheter får skadevaren da?

Poeng: 1 for riktig, 0 for feil eller ubesvart.

Velg ett alternativ:

- Bruker
- Gjest
- Administrator
- Power user

Maks poeng: 1

Løsningsforslag

Alternativ tre: Administrator – skadevare kjører med den tilgangen du gir den (altså din bruker). Det at du har slått av UAC gjør at skadevaren da har administratortilgang (tilsvarer å kjøre skadevaren med sudo i linux).

Oppgave 6 Skadevare (eksamensoppgave høsten 2023)

3.4 Skadevare

Velg den kolonnen som passer best med hver rad. Det gis ett poeng for hvert svar, 0 for blanke og minus ett for hvert gale.
Poeng: 1 for hver riktig, -1 for hver feil, 0 for ubesvart, 4 for alle riktig, minimum 0.

Finn de som passer sammen:

	Bakdør	Dataorm	Virus	Løsepengevirus	Trojaner
En skjult metode for å omgå normal autentisering og tilgangskontroll	○	○	○	○	○
Maskerer seg som legitime programmer som faktisk (eller tilsynelatende) har nyttige funksjoner.	○	○	○	○	○
Infiserer andre programmer ved at skadelig kode legges til og flettes inn i andre programmer.	○	○	○	○	○
SQL-slammer er en	○	○	○	○	○

Maks poeng: 4

Løsningsforslag

1: Bakdør
2: Trojaner
3: Virus
4: Dataorm

Oppgave 7 Løsepengevirus (eksamen høsten 2022)

(true/false – 0,5 poeng for riktig svar, -0,5 for galt – minimum 0 poeng)

a) Mange løsepengevirus krypterer offerets systemer ved hjelp av av SHA-256

b) Et viktig sikkerhetstiltak mot løsepengevirus i virksomheter er å ikke gi brukerne administratorrettigheter

Løsningsforslag

a) Nei. SHA-256 er en hash- ikke en krypteringsalgoritme. Det er, som kjent(?), ikke teknisk mulig å gå fra en hash og tilbake til klartekstmeldingen.

b) Ja, ref oppgave 5 (skadevaren kjører med dine rettigheter – som admin kan du kryptere hele systemet)