IN2120 – Informasjonssikkerhet

Del 5: Angrepsvektorer og skadevare

Nils Petter Wien

Høst 2023

Universitetet i Oslo

1

Endring i obliger

- En oblig fjernet
- To slått sammen (skadevare og pentesting)
- Det er nå krav om 350 poeng
  - Fortsatt krav om minst 20 poeng per oblig
- Uendret frist: 5.november

2

Eksamen

- Skriftlig (digital) eksamen i Silurveien 2 (27.11 kl. 09:00-13:00)
- Teller 100%
- Ingen hjelpemidler
- Minimalt med matte
- Gamle eksamensoppgaver finnes tilgjengelig på kursets nettsider:
  - https://www.uio.no/studier/emner/matnat/ifi/IN2120/h23/tidligere-eksamener.html

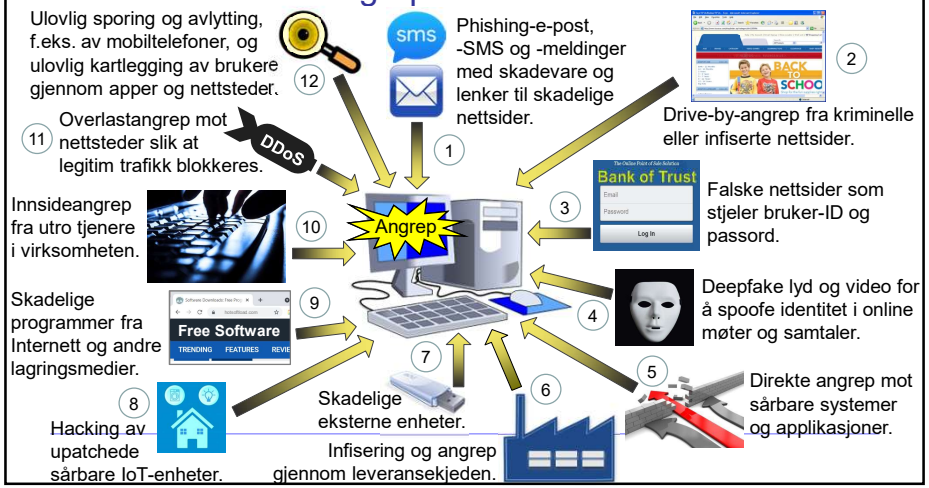
3

Oversikt

- Skadevare
  - *"Skadevare innen IT er en samlebetegnelse på programkode som uten brukerens tillatelse utfører handlinger med brukerens systemer eller informasjon.» (Store norske leksikon)*
- Angrepsvektor
  - En måte å overføre skadevare, eller annen form for hacking

4

Angrepsvektorer



5

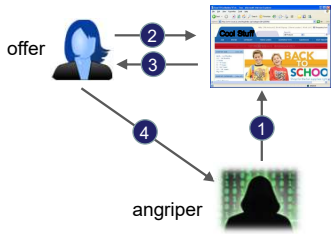
Drive-by-angrep

- Mange ulike scenarioer for drive-by-angrep.
- Generelt skjer drive-by-angrep uten at brukeren trenger å klikke på noe, eksplisitt laste ned noe eller åpne noe vedlegg for at klienten skal bli infisert. Brukeren trenger bare å besøke nettsiden for å bli angrepet.
- Kan være en vanlig nettside infisert av trusselaktør, eller en falsk nettside kontrollert av trusselaktør.
- Mulige scenarioer er:
  - Direkte nedlasting av skadelige JavaScript
  - Videresending til falsk nettside

6

Drive-by-angrep - eksempelscenario

XSS (Cross Site Scripting) er et angrep hvor et ondsinnet skript er injisert i en nettside (som ellers er godartet).



Scenario med direkte nedlasting av skadelig JavaScript, f.eks. som følge av en XSS-sårbarhet på en nettside.

1. Angriper injiserer skadelig skript
2. Offer besøker nettsiden
3. Skadeskript sendes til nettleser
4. Nettleser stjeler og sender sensitive data til angriper

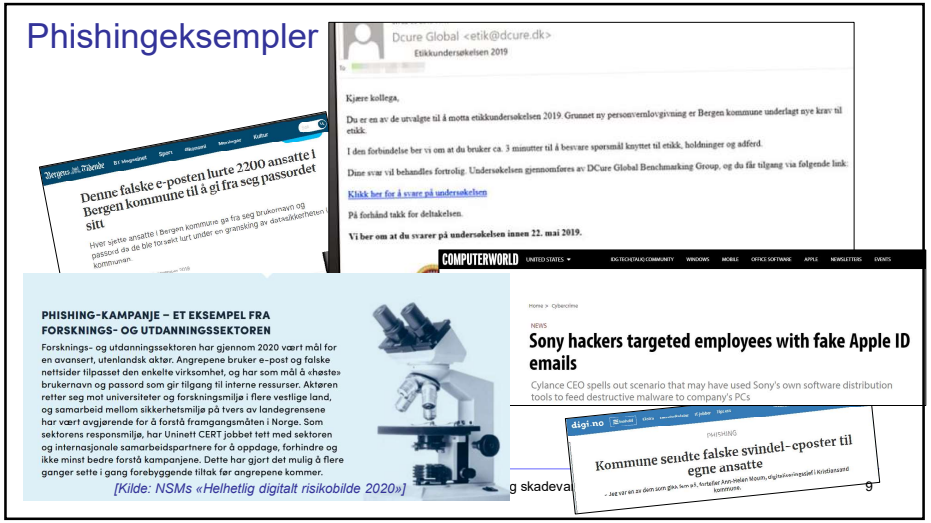
7

Phishing-angrep

- *Phishing* er en type sosial manipulering.
- Kan sendes som e-post, SMS eller andre meldinger.
- En phishing-e-post er f.eks. designet for å lure mottageren til å oppgi sensitiv informasjon, til å besøke en falsk nettside eller til å installere skadevare.
- Fra omtrent år 2020 er phishing den desidert vanligste angrepsvektoren for cyberangrep og datakriminalitet på Internett.
- Sikkerhetskultur, kunnskap og bevissthet rundt phishing er viktig for å forhindre disse typene angrep.

8

Phishingeksempler



9

Kategorier av phishing-angrep

- *Masse-phishing*
  - Stort volum som er ment å nå flest mulig
- *Spyd-phishing (Sphere-phishing)*
  - Målrettet mot bestemte personer eller virksomheter
- *Direktørsvindel (hval-phishing / whale-phishing)*
  - Spyd-phishing rettet mot «store fisker» (f.eks. rike, høyprofilerte, tilgang til mye penger, eller ressurser…)
- *Klone-phishing*
  - Kopi av legitim melding/epost hvor lenker/vedlegg er erstattet av skadelige versjoner

10

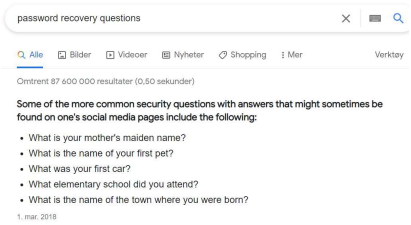
Deepfake

- Verktøy basert på maskinlæring gjør det mulig for en angriper å snakke på en måte som høres ut som deg, eller opptre i et videomøte med ansikt og stemme som deg.
- Deepfake refererer til at falsk lyd og bilde genereres av teknologi basert på dype nevralnettverk (DNN).
- En angriper kan f.eks. spoofe identiteten til virksomhetens direktør under et online-møte, og gi en ansatt med høye autorisasjoner instruks om å overføre en stor pengesum til en konto kontrollert av angriperen.
- Alternativt kan angriperen spoofe identiteten til en ansatt i en bedrift under et videomøte, og sende en chattemelding med en link til en skadelig nettside. Fordi kollegaer kjenner og stoler på den ansatte, vil de typisk klikke på lenken.
- Deepfake kan også brukes til å forfalske biometri.

11

Andre former for sosial manipulering

- Spør pent
  - Folk er generelt hjelpsomme og gir fra seg mye informasjon
- Lur folk til å gi deg tilgang
  - «Hi, I`m calling from Microsoft»
  - Få tak i «hemmeligheter» til å resette glemte passord
- Falske adgangskort
  - Gir en følelse av fellesskap – «du og jeg har noe felles, og derfor stoler jeg på deg»



12

Andre former for sosial manipulering

- Bruk av stjålne/falske kontoer på sosiale nettverk
  - Du tror du får melding fra en venn, men egentlig er det en angriper som har stjålet din venns identitet
  - Hvis det skjer, kontakt din venn gjennom annen «sikker» kanal, f.eks. vanlig telefon

13

Andre former for sosial manipulering

- Bruk av linker i sms, epost eller annet

14

Innsideangrep fra utro tjener

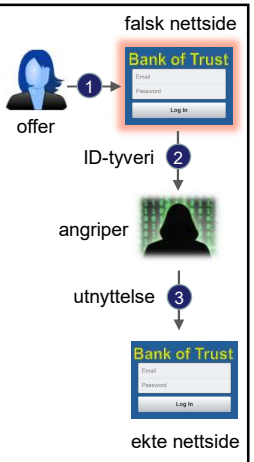
- Innsideangrep er angrep som begås av en ansatt eller annen person som er autorisert for tilgang til virksomhetens systemer og data.

- Begrepet *utro tjener* benyttes typisk om slike personer.
- Innsideangrep kan være svært skadelige fordi angriperen har kjennskap og tilgangsrettigheter til systemer og verdier slik at typiske sikkerhetstiltak har begrenset nytte.
- I tillegg kan innsideangrep være svært vanskelig å oppdage fordi angriperen ofte vet hvordan spor kan skjules.

15

Falske nettsider

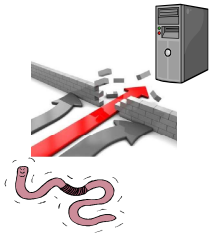
- *Falske nettsider* kan være nesten umulig å skille fra ekte nettsider.
- Brukere kan bli villedet til å besøke en falsk nettside f.eks. gjennom phishing-e-post, gjennom andre falske eller infiserte nettsider eller gjennom skadereklame.
- En bruker som har havnet på en falsk nettside kan bli lurt til å oppgi bruker-ID og passord eller annen sensitiv informasjon.
- Angriperen kan så bruke stjålet bruker-ID til å besøke den ekte nettsiden og logge seg inn som brukeren.
- Måter å unngå falske nettsider er å ikke klikke på lenker i meldinger, eller å sjekke nøye nettsidens URL og sertifikat.



16

Direkte nettverksangrep

- *Automatisk spredning av skadevare* kan skje f.eks. gjennom en dataorm som automatisk sprer seg til andre computere gjennom datanett og internett.
- En dataorm utnytter ukjente eller upatchede sårbarheter for å infisere en computer, og bruker denne som vert for å skanne og infisere andre computere.
- Dette utløser en kjedereaksjon som kan gi eksponentiell spredning på kort tid.
- Foruten å beslaglegge betydelig båndbredde gjennom spredningen, kan dataormer ha alvorlige tilsiktede skadevirkninger.
- Direkte angrep gjøres også med angrepsverktøy som utnytter sårbarheter.



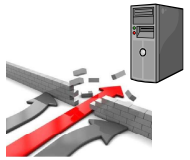
dataorm

SQL-injection

- Eksempel: Applikasjon krever pålogging med brukernavn og passord

SQL-injection

- Misbruker SQL til å få uautorisert utvide-spørring til å få uautorisert tilgang til underliggende databaseløsning typisk gjennom en webside.



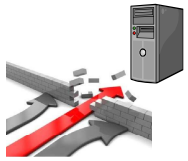
- SQL er et spørrespråk for å hente ut databaser
  - Eksempelvis: «Select * from tabellNavn» henter ut alle data fra tabellen ved navn «tabellNavn»

SQL-injection

- Har ikke passord, men taster inn en logisk korrekt spørring
  - «A' or 1==1»
  - Dette tolker systemet som:
    - «Passordet er A, ELLER 1 er matematisk lik 1»
  - Resultat: ok, fordi:
    - «Passordet er feil, MEN ja, 1 er matematisk likt 1»

- Skyldes manglende validering av brukerinput

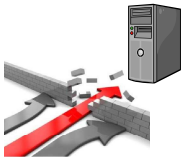
Command injection



- Kombinere/nøste kommandoer for å kjøre uautoriserte kommandoer i tillegg til de tiltenkte, autoriserte kommandoene
- Skyldes manglende validering av brukerinput

21

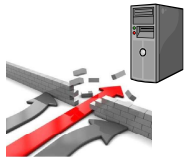
Command injection



- Eksempel: En tjeneste som sjekker om en maskin eller tjeneste er tilgjengelig (ping) ut fra brukers kommando
- Input: «uio.no» blir altså tolket som: «ping uio.no»
- Angrepet: «uio.no && whoami»
  - Dette pinger uio.no OG kjører kommandoen «whoami»

22

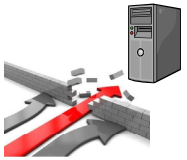
Brukervalidering



- Aldri stol på brukere
- Filtrer bort spesialtegn
  - Første filter kan gjøres hos bruker
    - Mest ressurseffektivt
    - Kan unngås av bruker
      - dvs er bare brukbart til å fjerne utilsiktede feil
  - Ha alltid filter på server (hos deg)
    - Her gjør du ny runde med filtrering
    - Faktisk sikkerhet siden brukere ikke kan stoles på

23

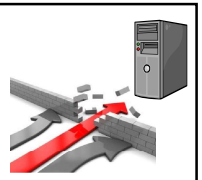
"Man in the middle" (MiTM)



- Angriper setter seg mellom maskiner som snakker sammen
  - Ofte mellom klient og server
  - Eller mellom servere
- Brukes til å avlytte trafikk som går mellom disse
  - Ukryptert trafikk kan leses rett ut
    - Passord
    - Sensitive data

24

"Downgradeangrep"



- MiTM-angrep hvor angriper prøver å tvinge igjennom ukryptert, eller svak kryptering mellom målene for angrep
- Gjør krypterte data enkelt å dekryptere (eller kan leses direkte)
- Brukes ofte i sammenheng med fjernpålogging eller i mobiltelefoni (5g -> 2g)

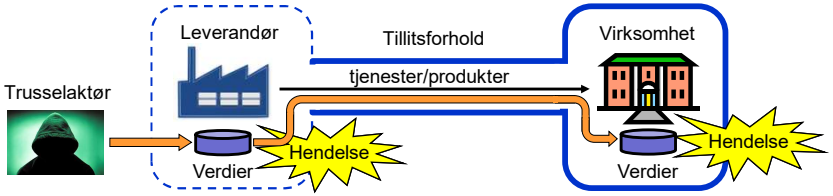
25

Leveransekjedeangrep

- *Leveransekjedeangrep* betyr at angripere kan infiltrere systemer og nettverk gjennom en ekstern partner eller leverandør som har tilgang eller leverer komponenter med tilgang til systemer og data.
- Fra et sikkerhetsperspektiv representerer leveransekjedene en del av angrepsflaten.
- Avhengigheten av lange og komplekse leveransekjeder har ført til en dramatisk forstørrelse av angrepsflaten til virksomheter i de senere år.
- Enhver entitet som bidrar i en leveransekjede, har mulighet til å påvirke sikkerheten lenger opp i leveransekjeden.
- Jo lenger og mer kompleks leveransekjeden er, desto vanskeligere er det å få oversikt over trusler og sårbarheter, og desto vanskeligere er det å håndtere sikkerhetshendelser.

26

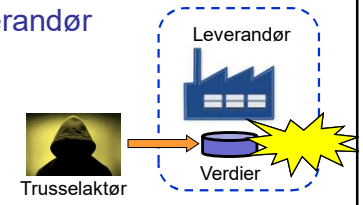
Illustrasjon av leveransekjedeangrep



- Angrep skjer flere trinn
  1. Leverandør blir angrepet for å kompromittere produkter eller tjenester
  2. Virksomheter som bruker kompromittert produkt/tjeneste fra leverandør blir sårbare
  3. Sårbare virksomheter blir angrepet

27

Trusselaktørens angrepsmål hos leverandør



Trusselaktører vil typisk angripe:

- Programvare utviklet av leverandøren
- Konfigurasjoner
  - f.eks. passord, API-nøkler, brannmurregler, URL-er
- Data
  - f.eks. konfidensiell informasjon, kryptografiske nøkler, sertifikater, CRM-data, personopplysninger om leverandørpersonale eller kundeansatte
- Prosesser
  - f.eks. oppdateringsprosesser, backup-prosesser, digitale signaturprosesser
- Maskinvare produsert av leverandøren
- Personer med privilegert tilgang til data og infrastruktur

28

Leveransekjedeangrep – Solarwinds (2020/21)

- *Orion* er et produkt utviklet av *Solarwinds* for nettverksstyring
  - Mange rettigheter
  - Et av de mest brukte produkter for dette formålet, både i offentlig og privat sektor
- Angrepet var først rettet mot Orion og ikke virksomhetene som bruker det
- Når Orion-produktet var kompromittert var alle som brukte det sårbare
- Med andre ord så skjedde angrepet gjennom tredjepartsleverandør av programvare, og er derfor et angrep på leveransekjeden
- Angrepet deployert i en oppdatering til Orion
- Opp mot 18 000 virksomheter berørt

29

Skadelige eksterne enheter

- *Skadelige eksterne enheter* kan f.eks. kobles til USB-kontakten og brukes i angrep.
  - Enheten kan f.eks. inneholde skadevare som brukeren kanskje installerer av nysgjerrighet.
  - En USB-minnepinne konfigureres som en HID-enhet (Human Interface Device), som lurer computeren til å tro at den er et tastatur og sender en strøm av tastetrykk som utgjør skadelige kommandoer.
  - Et *drop-angrep* er når angriperen legger igjen skadelige USB-minnepinner f.eks. på kafeer, og venter på at noen finner dem og plugger dem inn i en computer.

Stuxnet
- Dataorm/rootkit
  Flere nulldagssårbarheter
- Angrep en av Irans atom-reaktorer i 2010
- Krysset «air-gap» gjennom overføring over USB
- USA og Israel (trolig) bak

30

Uvitende innstallering av skadevare

- Å lure brukere til å installere skadelige programmer gjennom nettsteder eller andre lagringsmedier kan brukes som del av angrep.
- Brukeren kan bli lurt til å installere skadevare i den tro at programvaren er legitim.
- Det fins en rekke ulike typer skadevare
- Trojaner (trojansk hest) er en type skadevare som faktisk har en nyttig funksjon, men som samtidig har skjulte skadelige funksjoner.
- Unngå skadevare ved å kun laste ned fra anerkjente nettsteder, og sjekke digital signatur.

31

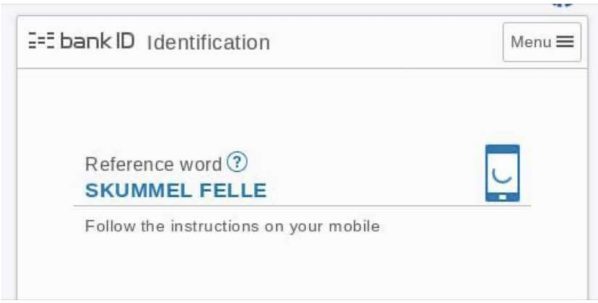
Skadevare

- Datavirus
- Løsepengevirus
- Spionvare
- Bott-program
- Exploit
- Makro-virus
- Trojaner
- Dataorm
- Rootkit
- Bakdør
- Skadelig JavaScript
- Logisk bombe

32

Skadevare

For å beskytte mot nettsvindel ber vi deg bekrefte denne og gå videre. Da kan du føle deg helt trygg.



33

Datavirus

- En datavirus infiserer andre programmer ved at skadelig kode legges til og flettes inn i et annet program.
- Viruset utføres bare når det infiserte programmet kjøres.
- At et virus er flettet inn i et annet program gjør det spesielt vanskelig å fjerne, og selv de beste antivirusprogrammene sliter med å gjøre dette riktig.
- Rene datavirus er uvanlige i dag, og utgjør mindre enn 10 % av all skadevare.
- Vær oppmerksom på at begrepet «virus» ofte brukes som et generelt navn på alle typer skadevare, noe som kan være forvirrende.

34

Trojaner

- Trojanere maskerer seg som legitime programmer som faktisk (eller tilsynelatende) har nyttige funksjoner, men som samtidig har skjulte skadelige funksjoner.
- Trojanere er populære blant hackere og har stort sett tatt over etter datavirus.
- Trojanere blir typisk lastet ned fra kriminelle eller infiserte nettsteder, eller kommer som et vedlegg til phishing-e-post.
- Brukeren blir lurt til å tro at programmet er nyttig, og velger eksplisitt å installere det.
- Det er ironisk at falske antivirusprogrammer er en utbredt type trojaner.

35

Løsepengevirus

- Løsepengevirus er en type skadevare som i første trinn krypterer alle, eller et utvalg, kritiske data på offerets computer, slik at data og applikasjoner blir utilgjengelige.
- Dette er en form for tjenestenektangrep som fører til brudd på *tilgjengelighet*.
- Angriperen følger opp første trinn med å foreta utpressing og kreve løsepenger for å utlevere dekrypteringsnøkkelen.
- Utpressing kan også baseres på en trussel om å offentliggjøre dataene hvis ikke løsepenger blir betalt. Dette kan være en trussel mot personvern.
- En viktig beredskap mot løsepengevirus er å ta regelmessige sikkerhetskopier (backup) av alle viktige data, og ha gode gjenopprettelsesrutiner.
- Løsepengevirus er ikke et datavirus i ordets opprinnelige forstand.

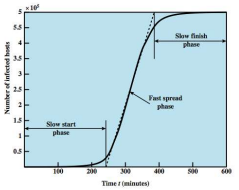
36

Dataorm

- Dataormer sprer seg selv til andre computere innen et datanett eller over hele internett på en automatisk måte, som regel uten brukerinteraksjon.
- Dataormer klarer dette ved at de kobler seg til andre vertsnoder og utnytter sårbarheter i programmer som er eksponert til Internett.
- Kan være svært ødeleggende fordi de sprer seg uten brukerdeltagelse. Virus og trojanere krever i det minste at en bruker starter et program.

Eksempler på dataormer

- Morris-dataormen (1988) laget av en student kalt Robert Morris og er en av de første dataormene på Internett
- Stuxnet
- Wannacry & NotPetya
- SQL Slammer-ormen
  - I januar 2003 infiserte ormen omkring 75 000 Microsoft SQL-tjenere på omtrent 10 minutter
  - viser dens eksponentielle spredningshastighet.



Spionvare

- Spionvare og reklamevare er programmer som spionerer på brukeren eller viser reklame til brukeren.
- En keylogger er en type spionvare som logger tastetrykk, slik at angriperen kan stjele passord og annen sensitiv informasjon.
- Slike programmer blir ofte installert gjennom en form for sosial manipulering kombinert med en av angrepsvektorene, og de starter som regel hver gang systemet starter.

Exploit

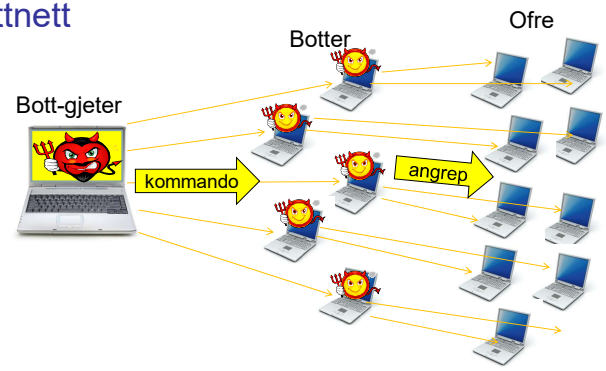
- Exploit er et lite program, en streng med data, en fil eller en sekvens med kommandoer som utnytter en eller flere feil eller sårbarheter i en programvare, maskinvare eller annet datautstyr for å trigge korrupt eller unormal oppførsel.
- En exploit trigger ofte en buffer overflow
- Angriperens hensikt med å trigge slik oppførsel kan for eksempel være å få kontroll over et system, laste ned bakdører, få uautorisert tilgang eller å utføre et tjenestenektangrep.

Bott-programvare

- En computer med bott-programvare kalles en bott (eng.: bot), fra «robot», altså noe som går automatisk.
- Bott-programvare kan brukes til legitime formål
  - f.eks. søkemotorer for å utføre indeksering.
  - Dessverre brukes bott-programvare ofte som skadevare av angripere.
- Bott-skadevare er typisk selvreplikerende, og er i stand til å motta kommandoer fra en sentralisert eller distribuert bott-gjeter. Angripere infiserer computere i stort antall for å lage et bottnett som kan utføre forskjellige typer angrep.
  - F.eks. DDoS-angrep eller utvinning av kryptovaluta med ofrenes elektrisitet og beregningsressurser.

41

Bottnett



Mirai er (en dataorm som) er et eksempel på botnett, med fokus på IoT-enheter og DDoS-angrep.

42

Bakdør

- En bakdør er en skjult metode for å omgå normal autentisering og tilgangskontroll i et system.
- Bakdører har legitime bruksområder, som å gi produsenten av systemer og programvare en måte å foreta vedlikehold og service på.
- En bakdør kan også brukes av angripere for å få uautorisert tilgang til systemer.
- En bakdør kan være en skjult del av et program, et eget program, kode i fastvaren til maskinvaren eller en del av operativsystemet.
- En skadebakdør kan f.eks. bli installert av en trojaner eller av et exploit.

43

Skadelig JavaScript

- De fleste nettsider inneholder JavaScript som automatisk lastes ned og kjører i nettleseren når en bruker besøker nettsiden.
- Vanligvis er JavaScript helt legitimt, og brukes til avanserte funksjoner på en nettside, men det kan også utføre skadelige funksjoner, f.eks. å laste ned et exploit fra et nettsted kontrollert av angriperen.
- JavaScript kan også misbrukes til å få nettleseren til å utvinne kryptovaluta for angriperen eller til å stjele sensitiv informasjon som sendes til angriperen.
- Skadelige JavaScript kan bli injisert i nettsider gjennom XSS-angrep.
- Ettersom JavaScript utføres automatisk og helt uten interaksjon når brukeren besøker en nettside, er JavaScript typisk brukt til drive-by-angrep.

44

Makro-virus

- Makroer brukes for å automatisere funksjoner i Office-dokumenter.
- Imidlertid kan angripere gjemme skadelige Office-makroer i Office-filer som f.eks. sendes som vedlegg til phishing-e-post.
- Disse filene har ofte navn som er ment å lokke eller skremme folk til å åpne dem, og ser typisk ut som fakturaer, kvitteringer, juridiske dokumenter osv.
- Tidligere kjørte Office-makroer automatisk, men ikke nå lenger. Som oftest må nå angriperen lure brukere til å aktivere makroer for at de skal kunne kjøre. Dette gjøres ofte gjennom sosial manipulering.

Logisk bombe

- Logiske bomber er en av de eldste typer skadevare
- Logiske bomber er kode innebygd i et legitimt program, eller et program som går i bakgrunnen.
- Skadelige funksjonalitet aktiveres når bestemte betingelser er oppfylt, f.eks.
  - tilstedeværelse/fravær av en fil
  - bestemt dato/klokkeslett
  - bestemt bruker
- Logiske bomber forårsaker skade når den utløses:
  - endre/slette filer/disker, stoppe maskinen osv.
- Logiske bomber lages typisk av en innsidetrussel

Hvilken tilgang gir skadevaren?

- Exploits og annen skadevare gir tilgangen til vedkommende / tjenesten som kjører
  - Dvs: Kjører man et program som bruker, får skadevaren brukertilgang.
    - Kjører man som administrator – får skadevaren administrator
  - Dette er hvorfor man har sikkerhetsmekanismer som UAC (User Account Control)

Hvilken tilgang gir skadevaren?

- «Privilege escalation»-angrep
  - Dette er angrep som utnytter feil i systemet som gir angriperen høyere rettigheter (typisk root- eller administrator)
  - Eksempelvis buffer overflow

Rootkit

- Rootkit er en type programvare som angriperen installerer for å skjule at vedkommende, eller skadevaren er i systemet
  - Navnet kommer av «root»
- Eksempelvis endrer prosesslisten til å skjule skadevaren
  - Eller skjuler bakdører
  - Eller skjuler brukere opprettet av angriperen

Nulldagssårbarheter (zero-days)

- Sårbarheter det enda ikke finnes oppdateringer til
  - Kan altså ikke patches
  - Navnet stammer fra «Leverandøren får ingen dager til å fikse problemet»
- Avhengig av andre sikkerhetsmekanismer for å beskytte oss
  - Ref «sikkerhetsløken», hvor du kan skrelle av lag på lag med sikkerhet

Skadevare i et KIT-ståsted

- Skadevare kan brukes til:
  - Gi uautorisert tilgang til informasjon
    - Dette er et angrep på KONFIDENSIALITET
  - Manipulere eller endre filer og tjenester
    - Dette er et angrep på INTEGRITET
  - Kryptere eller fjerne filer eller tjenester
    - Dette er et angrep på TILGJENEGLIGHET

Slutt på presentasjonen