UKE 9

Plan for i dag

- Kursevaluering
- Gjennomgang av pensum
- Oblig-jobbing/ukesoppgaver

Angrepsvektor og skadevare

- **Digital sårbarhet:** svakhet i et datasystem som gjør det mulig å utnytte systemet
  - **Nulldags-sårbarhet:** en digital sårbarhet der produsenten av en tjeneste ikke har tid (null dager) til å rette opp en feil.
  - **To forskjellige typer sårbarheter:**
    - **Kjente og aksepterte**
      - Sårbarheter man er villig til å akseptere basert på risikoen (kostnadene for håndtering av sårbarheten vs. konsekvens av sårbarheten)
    - **Ukjente/feilvurderte (ikke håndterte)**
      - Hverken systemeier eller bruker er klare over at de kan være utsatt for angrep
- **Angrepsvektor:** metoden en angriper benytter for å utføre et angrep på et system
- **Skadevare**: skadelig programvare, som ofte utnytter sårbarheter i datasystem
  - Kan overføres via
    - Lenker (e-post
    - Ondsinnede nettsider
    - Internett
    - Eksterne enheter (USB)

Typer skadevare

 Virus	Kjennetegnes ved at det sprer seg hver gang en fil med virus blir åpnet av bruker eller systemet.
 Dataorm	Skadevare som på egenhånd er i stand til å spre seg og finne nye ofre.
 Trojaner	Skadevare som utgir seg for å være et nyttig program.
Bakdør	En ubeskyttet og ukjent åpning inn i et datasystem, laget av en angriper.
 Spionvare	Programvare for å spionere på en bruker i håp om å få tak i f.eks. informasjon, passord, kontoinformasjon.
 Tastelogger (Keylogger)	En enhet eller programvare som er koblet til tastatur eller maskin og som lagrer eller videresender alle tastetrykk. En variant av spionvare.
Rootkit	Skadevare som endrer eller erstatter funksjoner i OS eller applikasjoner, med mål å ta kontroll over en maskin eller et system.
Exploit	Et program, en sekvens med data, eller en oppskrift på hvordan en sårbarhet kan utnyttes.

Systemsikkerhet og applikasjonssikkerhet

Systemsikkerhet er viktig for å forhindre at systemprogramvaren angripes

- Eksempler på systemprogramvare:
  - Operativsystemet
  - Minnet
  - Bootloaderen

Applikasjonssikkerhet er viktig for å forhindre at applikasjonsprogramvaren angripes

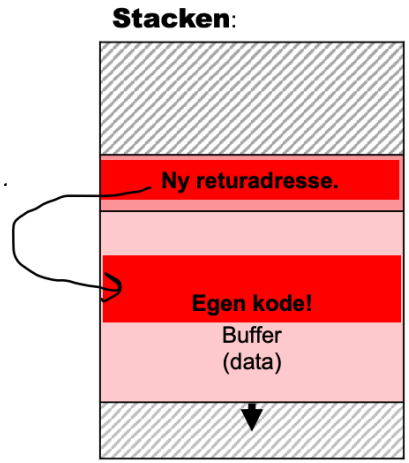
- Applikasjonsprogramvare er programvare som løser brukerorienterte oppgaver (altså applikasjoner):
  - Gjør f.eks. at brukere kan lytte til musikk eller streame film

Husk at god kommunikasjonssikkerhet ikke er like my verdt uten god sikkerhet i endesystemer

- Datasystemer er sårbare

Systemsikkerhet

- **Systemsikkerhet:**
  - **Operativsystemet:**
    - Styrer alle ressurser i en datamaskin
    - Alle brukerprosesser må via kjernen for å ta i bruk perifer-enheter (minne, tastatur, skjerm f.eks.)
      - Derfor er det veldig viktig å ivareta sikkerhet i OS-kjernen (en sårbarhet i kjernen vil kunne gi trusselaktører tilgang til alle ressurser)
  - **Buffer:** sammenhengende seksjon i minnet
    - Bufferoverskridelse (buffer overflow): feil i et program som gjør at minnet kan overskrives
      - Angriper kan kjøre egen kode, gi tilgang til ressurser eller forårsake at et program krasjer
  - **Ved oppstart av en datamaskin:**
    - Før operativsystemet kjører, startes bootloaderen, deretter laster bootloaderen kjernen i operativsystemet.
      - Derfor er det viktig å sørge for at ingen har manipulert bootloaderem
        - Kan løses ved å kjøre en integritetssjekk



Applikasjonssikkerhet

For å sørge for å ha sikre applikasjoner, er det viktig å tenke på sikkerhet under alle faser av systemutvikling



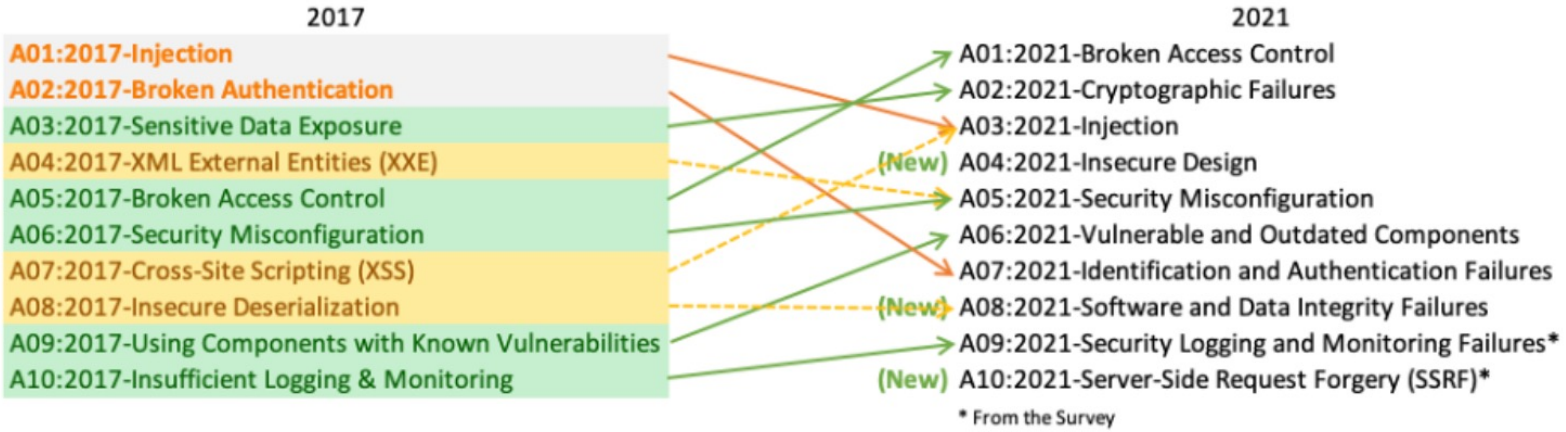
OWASP – organisasjon som har som mål å forbedre sikkerhet til tjenester på nettet

- OWASP Top 10 rangerer de 10 mest kritiske sikkerhetsrisikoene for tjenester på nett
- Gir råd om hvordan sårbarhet og risiko kan reduseres

Applikasjonssikkerhet

OWASP – organisasjon som har som mål å forbedre sikkerhet til tjenester på nettet

- OWASP Top 10 rangerer de 10 mest kritiske sikkerhetsrisikoene for tjenester på nett
- Gir råd om hvordan sårbarhet og risiko kan reduseres



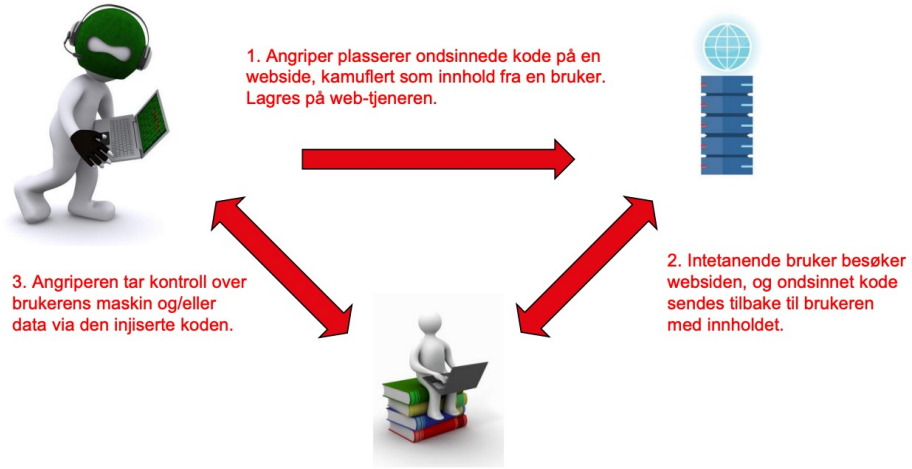
SQL-injisering og Cross Site Scripting (XSS)

Oppgi brukernavn: anneh Oppgi passord: xyxyxy OR 1=1

Dette kan resultere i følgende gyldige SQL-setning:

```
SELECT * FROM Bruker
WHERE Brukernavn = anneh and Passord = xyxyxy  OR 1=1;
```

- Løsning på SQL-injisering og Cross Site Scripting?
  - Filtrer alt av input!
    - Ikke tillat SQL-kode i brukernavn og passord
    - Ikke tillat å legge igjen kode



Sikkerhetskultur og sosial manipulasjon

Menneskelige sårbarheter:

- Grunnet manglende forståelse, sikkerhetsbevissthet og dårlig sikkerhetskultur, kan mennesker utgjøre en stor sårbarhet.
- Vi kan utsettes for sosial manipulasjon (at man er et offer for utpressing/svindelangrep):
  1. Phishing-epost: epost som er designet for å lure en til å oppgi sensitiv info f.eks.
     - Masse-phishing
     - Spyd-phishing
     - Direktørsvindel
  2. Tilbud om penger for å få tak i konfidensiell informasjon eller for å få tilgang til ressurser
  3. Spoofing: Forfalske avsender i e-post eller SMS

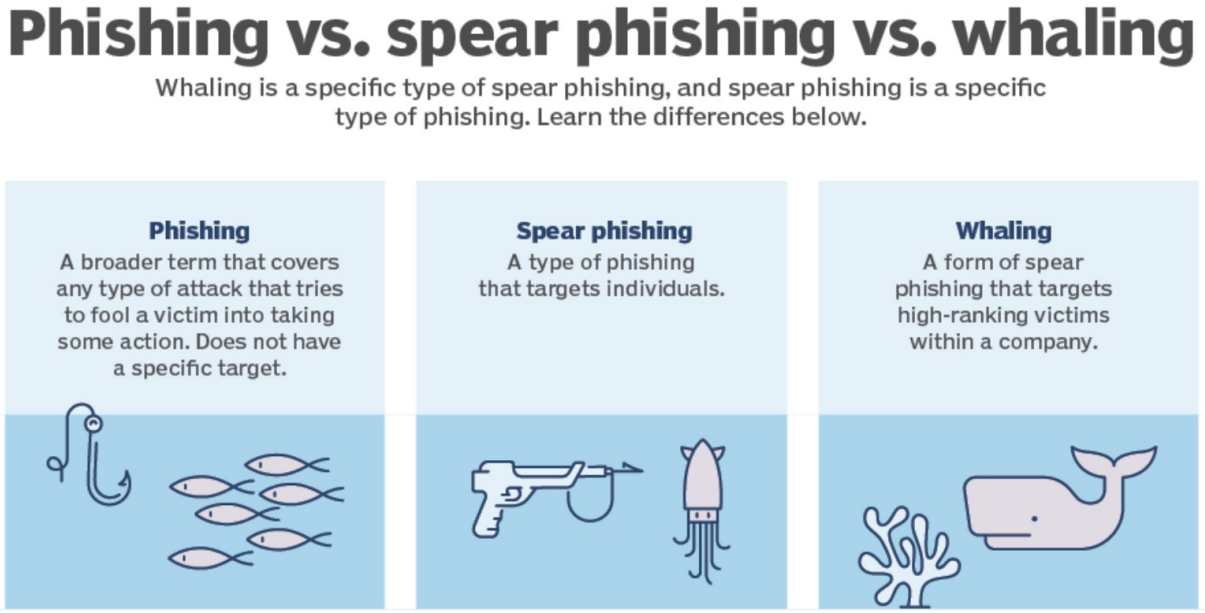
«Sikkerhetskultur er summen av de ansattes kunnskap, motivasjon, holdninger og adferd som kommer til uttrykk gjennom virksomhetens totale sikkerhetsadferd»

NSM

Sosial manipulasjon spiller ofte på menneskers følelser

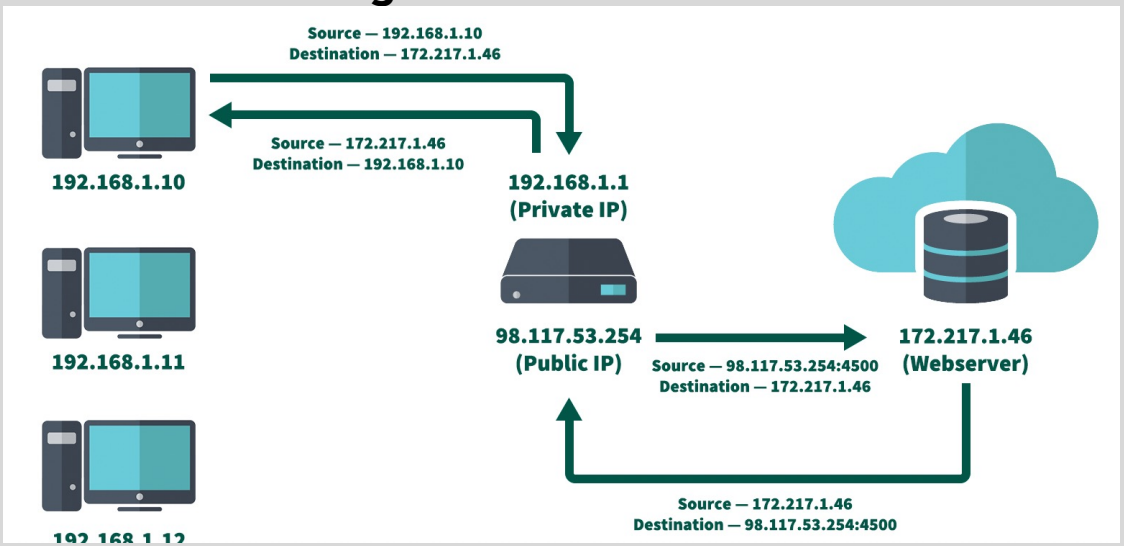
- Glede: «Du har vunnet et gavekort!»
- Frykt: «Jeg lekker informasjon om deg om du ikke oppgir informasjon»

Sikkerhetskultur og sosial manipulasjon



NAT – Network Address Translation

- Gjør det mulig for flere enheter på et lokalt nettverk dele på en offentlig IP-adresse
  - Vi kan altså gjenbruke IP-adresser
- Brukes for å sørge for at vi ikke går tom for IP-adresser
- Alle enheter som er koblet til et subnett har forskjellige **private** IP-adresser. Subnettet har en **offentlig** IP-adresse



Overføringshastighet

4.3 Overføringshastighet

Du ønsker å laste ned en fil på 150 megabyte, og hastigheten på din Internettlinje er 50 megabit per sekund ned og 20 megabit per sekund opp. Hva er den teoretisk korteste overføringstiden?

Velg ett alternativ:

- 7,5 sekunder
- 60 sekunder
- 24 sekunder
- 150 sekunder
- 3 sekunder

IP-adresser (IPv4)

- IP-adresser er adressen til en datamaskin i et nettverk
  - Unik: to maskiner i samme nettverk kan ikke ha samme IP-adresse
- I IPv4 har vi **IP-adresser** på 32 bit
  - Deles inn i 4 oktetter på 8 bits, skilt med punktum
    - Eks: 172.16.254.1 (base 10)
      - 10101100.00010000.11111110.00000001
- **Nettverksmaske**
  - Forteller om dataen skal sendes ut av det lokale nettet (LAN), eller ikke.
  - Bits som er satt til 0 i nettverksmasken kan varieres for å angi IP-adresser i subnettet
  - Bits som er satt til 1 angir delen som identifiserer selve nettverket

CIDR og punktnotasjon

- To måter å oppgi en IP-adresse på:
  - **Punktnotasjon**
    - F.eks. 192.168.1.0
      - Må da oppgi nettverksmasken
        - 255.255.255.0
  - **CIDR-notasjon**
    - Punktnotasjon + antall bits nettverksmasken består av
      - 192.168.1.0/24
    - Hvordan ser man antall bits nettverksmasken består av?
      - 255.255.255.0 = 11111111.11111111.11111111.00000000
        - Antall enere er 24

Antall IP-adresser

Et subnett har nettverksmasken 11111111.11111111.11111111.11111000
Hvor mange gyldige IP-adresser kan tildeles verter i subnettet?
Velg ett alternativ:

- 256
- 8
- 30
- 32
- 6