

UiO : Institutt for informatikk

Datateknologi og sikkerhet

IN1020 – Introduksjon til datateknologi

Temavideo 1 uke 11: Angrepsvektor og skadevare

Kristin Skar
kritisk@ifi.uio.no

Begreper:

- Digital sårbarhet:
  - En feil i et IKT-system grunnet svakhet, feildesign eller feilimplementering
- Nulldags-sårbarhet:
  - En sårbarhet som er ukjent for eller uadressert av leverandør
- Angrepsvektor:
  - Den konkrete metoden en angriper velger for å utføre et angrep på en datamaskin, et nettverk eller et system.
- Exploit
  - En konkret *utnyttelse* av en sårbarhet

Digital sårbarhet

To kategorier sårbarheter:

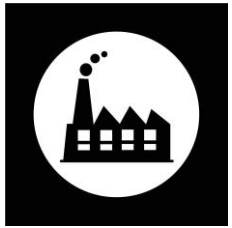
1. Kjente og aksepterte
2. Ukjente eller feilvurderte, og dermed heller ikke håndterte



Angrepsvektorer: Hvordan kompromitteres datasystemer?

Aksessere ondsinnede eller infiserte nettsteder som inneholder ondsinnede script, eller laste ned og installere skadevare fra nettsteder.





Infisering via *leveransekjeden*.



Kjøre vedlegg som kommer med e-post, som inneholder utnyttelser og skadevare.







Plugge inn eksterne enheter som er infisert med skadevare.



Direkte angrep fra internet, som f.eks. utnytter sårbarheter i operativsystem eller applikasjoner som web-tjenere eller SQL-databaser.

Skadelig programvare, *skadevare*

Skadevare:

- er en samlebetegnelse på ulik programvare som har som oppgave å gjøre skade.
- utnytter sårbarheter i et datasystem.
- kan være et enkeltstående program, eller en del av et *vertsprogram*.
- kan ha den egenskapen at den formere seg og infiserer andre systemer.

Skadevares oppbygning

1. Stridshode – hvordan skadevaren skal infisere et datasystem
2. Spredning – hvordan skadevaren skal spre seg videre
3. Nyttelast – oppgaven skadevaren er satt til å gjøre

Et utvalg av typer skadevare:

Gruppene er til dels overlappende, og ikke alltid presist definert.

 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.



UiO : Institutt for informatikk

Takk!

mn.uio.no/ifi

