UiO : Institutt for informatikk

Datateknologi og sikkerhet

IN1020 – Introduksjon til datateknologi

Datasikkerhet temavideo 10: Sikkerhetskultur og sosial manipulasjon

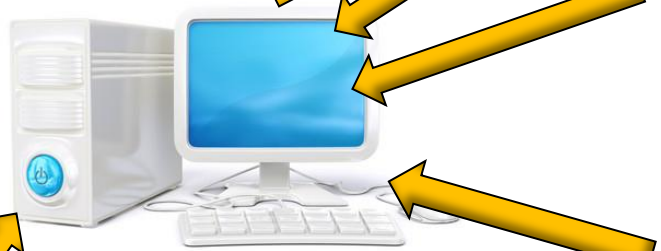
Kristin Skar
kritisk@ifi.uio.no

Angrepsvektorer: Hvordan kompromitteres datasystemer?

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

Plugge inn eksterne enheter som er infisert med skadevare.

Infisering via *leveransekjeden*.



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

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

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

NSM

Mennesket som sårbarhet ;

UiO : Institutt for informatikk

Menneskelige sårbarheter

- Manglende forståelse eller sikkerhetsbevissthet hos brukeren
- Utsatt for sosial manipulasjon:
  - Offer for svindelangrep
  - Offer for utpressing/overtalelser

Sosial manipulasjon: Kjennetegn

- Utnytter menneskelig svakhet og tillitt.
- Er det mest brukte, enkleste, og kanskje det eldste trikset i boka.
- Berører alt fra privatpersoner til store virksomheter.
- Vanlige innfallsvinkler:
  - E-post som inneholder falske lenker eller skadevare
  - Du kontaktes av noen som ber om informasjon (passord, kontoinformasjon) eller å gi dem tilgang til en ressurs (fysisk, et system eller datamaskinen din).
- Målrettet eller tilfeldig?

Sosial manipulasjon: Begreper

- Spoofing: Forfalske avsender i e-post eller SMS.
- Phishing (nettfisking): Lure offeret med falske nettsider eller e-post i håp om å tilegne seg informasjon. Ulike former for *phishing*:
  - Masse-phishing: Bredt utsendt e-post eller sms – ofte mindre troverdig.
  - Spyd-phishing (spear phishing) – målrettet angrep, samler opplysninger i forkant for å gjøre henvendelsen mer troverdig.
  - Direktørsvindel (whaling, eller CEO-phishing) – går etter «de store fiskene», målrettet angrep mot de med makt og myndighet.

Mottiltak: Bevissthet og opplæring

- Opplæring er et svært viktig sikkerhetstiltak
- Huskeliste for brukere:
  - ✓Stopp. Tenk. Klikk. Angripere vil at du skal handle først, tenke etterpå.
  - ✓Virker noe for godt til å være sant så er det mest sannsynlig det…
  - ✓Sjekk avsender på all e-post
  - ✓Vær svært varsom med å følge lenker i e-post
  - ✓Hold alltid operativsystem, drivere, programvare oppdatert med siste versjon.
  - ✓Tillitt: Ikke stol på noen/noe før du vet du kan stole på dem/det

UiO : Institutt for informatikk

Takk!

mn.uio.no/ifi