IN2120 Informasjonssikkerhet
Høst 2023

Del 11a: Sikkerhetskultur

Audun Jøsang
Universitetet i Oslo

Tema sikkerhetskultur

- Generelt om sikkerhetskultur
  - Bevissthet og adferd rundt digital sikkerhet
- Personlig integritet
  - Forhindre at ansatte blir innsideaktører (utro tjenere)
- Forsvar mot sosial manipulering
  - Sørge for at ansatte ikke blir offer for sosial manipulering

Digital sikkerhetskultur
Cybersecurity Culture

- **Definisjon: (ISACA)**

Sikkerhetskultur er kunnskap, tro, oppfatninger, holdninger, antagelser, normer og verdier til mennesker angående sikkerhet og hvordan de manifesterer seg i menneskers atferd/oppførsel i bruk av informasjonsteknologi.

- **Definisjon: (NSM)**

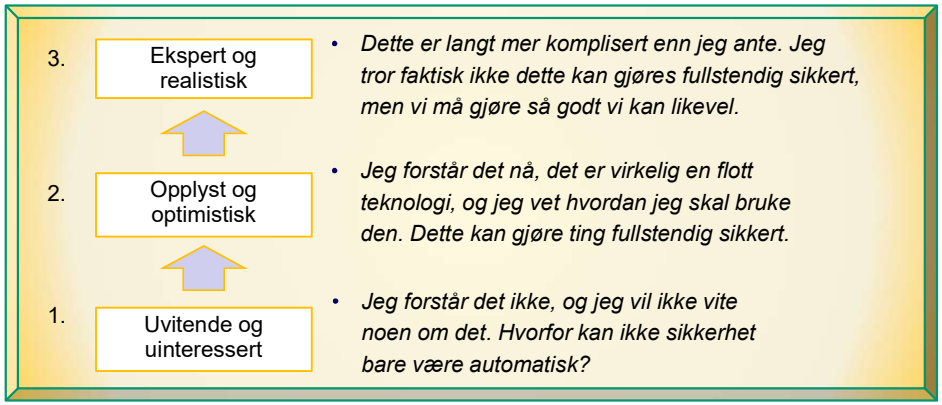
Sikkerhetskultur er summen av de ansattes kunnskap, motivasjon, holdninger og atferd som kommer til uttrykk gjennom virksomhetens totale sikkerhetsatferd.

- Målsettingen med å utvikle en sikkerhetskultur er å stimulere de ansattes atferd for å støtte god sikkerhet i organisasjonen.

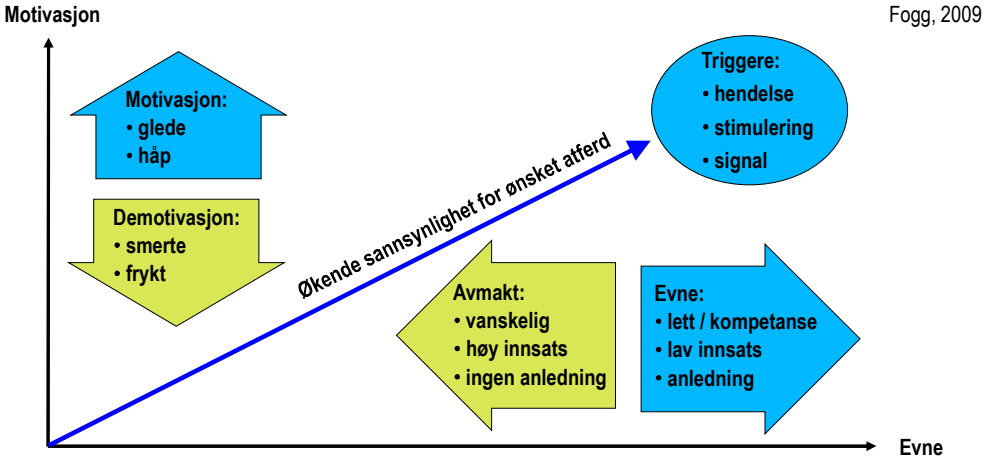
Dimensjoner av sikkerhetskultur (Roer og Petric, 2017)

- **Holdninger:** Ansattes følelser og meninger om de ulike aktivitetene som berører informasjonssikkerhet i organisasjonen. Dette inkluderer frykt og forståelse av risiko.
- **Atferd:** Ansattes faktiske eller tiltenkte aktiviteter og risikotaking som kan ha en direkte eller indirekte innvirkning på informasjonssikkerheten. Dette inkluderer personlig integritet.
- **Kognisjon:** Ansattes bevissthet, verifiserbar kunnskap og oppfatning om praksis, aktiviteter og mestringstro, f.eks. forståelse av cybertrusler, sensitivitet, og innholdet i policyer.
- **Kommunikasjon:** Måter ansatte kommuniserer med hverandre på, deres tilhørighetsoppfatning og deres aktive støtte for varsling og rapportering av hendelser.
- **Overholdelse:** Ansattes respekt for organisatoriske sikkerhetspolicyer samt bevissthet om eksistensen av og kunnskap om innholdet i slike policyer.
- **Normer:** Oppfatninger om sikkerhetsrelatert organisatorisk oppførsel og praksis som uformelt anses å være normal eller avvikende av ansatte eller andre som er i kontakt med organisasjonen.
- **Ansvar:** Ansattes forståelse av rollene og ansvaret de har for opprettholdelse av informasjonssikkerhet i organisasjonen, og hvordan de kan sette informasjonssikkerheten i fare dersom de ikke oppfyller det ansvaret.

Kognisjon og modenhet av kunnskap om sikkerhet



Modell for menneskelig atferd



Sikkerhetskultur

Bevissthet og adferd rundt cybersikkerhet

Veileder fra NSM: Grunnprinsipper for personellsikkerhet

https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-personellsikkerhet/introduksjon//

- Forklar og forstå hvorfor IT-sikkerhet er viktig og hva slags sikkerhet virksomheten trenger.
- Ledelse må involveres og gå foran som gode eksempler på god sikkerhetsatferd.
- Forstå og kommuniser nåværende tilstand.
- Finn målbare forbedringspunkter i virksomheten og evaluer om forbedringstiltakene fungerer.
- Bruk ulike virkemidler for å stimulere bevissthet og adferd.
- Ros fungerer bedre enn ris.
- Evaluer og kommuniser endring i sikkerhetskultur.
- Forbedre tiltakene og gjenta.

Personlig integritet

Forhindre at ansatte blir utro tjenere (innsideaktører)

- Fokus:
  - Ansatte
  - Ledelse og toppledere
  - Kunder
  - Besøkende
  - Underleverandører og konsulenter
- Alle disse gruppene har visse tilgangsprivilegier
- Hvordan sørge for at tilgangsprivilegiene bare blir brukt i henhold til policy, dvs. at privilegiene ikke blir misbrukt ?

Statistikk om innsidetrusselen

- En betydelig del av cyberangrep utføres av innsideaktører

- US Statistics (PWC) 2014, 2015, 2016
  - http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf
  - https://insights.sei.cmu.edu/blog/2016-us-state-of-cybercrime-highlights/
  - 28% hadde innsideangrep, 32% mener innsidetrusler er alvorlig
- Australian Statistics (CERT Australia) 2021
  - https://auscert.org.au/wp-content/uploads/2022/04/Cyber-Survey-Report-2021.pdf
  - 14% hadde innsideangrep, 60% svært bekymret over innsidetrusler
- Kriminalitets- og sikkerhetsundersøkelsen i Norge (KRISINO 2021)
  - https://www.nsr-org.no/uploads/documents/Publikasjoner/Krisino-2021.pdf
  - 8% av bedrifter var utsatt for innsideangrep (utro tjener).

Styrking av ansattes integritet

- Vanskelig å bedømme langsiktig integritet ved ansettelse
  - Personlig integritet påvirkes av hendelser i og utenfor jobb
- Alle ansatte bør gjennomgå bevissthetstrenging som også omhandler integritet og holdning til policy
- Påminnelse om sikkerhetspolicy og oppmerksomhet rundt følger ved (bevisst) brudd på policy
  - Vil styrke integritet og dømmekraft
- Ansatte med vide tilgangsprivilegier bør få særlig opplæring og oppfølging (og lønn)
- Gi støtte og monitorer ansatte i spesielle situasjoner
  - Ansatte i særlig ansvarsfulle stillinger
  - Ved konflikt og urettferdig behandling, ved personlige problemer
  - Endret jobbsituasjon
- Viktig å opprettholde positivt forhold til ansatte som slutter

Ansatte som slutter

- Forskjellige grunner til å slutte
  - Frivillig egen oppsigelse
  - Oppsigelse ved nedbemanning
  - Avskjed ved misligheter
- Alternative former for terminering av ansettelsesforhold
  - Tidligere ansatte beholder begrensede privilegier
  - Velordnet og avtalt sletting av alle privilegier
  - Umiddelbar sletting av alle privilegier, sikkerhetsvakt følger vedkommende til utgangen ...
- Ved avslutning av ansettelsesforhold kan avtaler gjennomgås med hensyn på hvilken informasjon den tidligere ansatte kan ta med seg, karantenetid, begrensning i å jobbe for konkurrerende selskap osv.

Ledelsens ansvar for ansattes integritet

- Ledelsens rolle er viktig for håndteringen av innsidetrusselen.
- Være oppmerksom på, og ta tak i uønsket atferdsendring.
- Sørge for «rettferdighet» når nedbemanningen er nødvendig
- De oppsagte og de gjenværende ansatte forventer ofte ulik lederadferd under en nedbemanningsprosess.
- Essensielt med god dialog med de ansatte under oppsigelse.
- Retningslinjer, prosedyrer og risikostyring bør inkludere innsidetrusselen under ansettelse og nedbemanning.
- NSM Temarapport 2020: «Innsiderisiko»
- https://nsm.no/regelverk-og-hjelp/rapporter/temarapport-om-innsidere/
- Petroleumstilsynet: 2019: «Håndtering av innsiderisiko».
- https://www.ptil.no/fagstoff/utforsk-fagstoff/prosjektrapporter/prosjektrapporter-2019/hvordan-handtere-innsiderisiko/

Sosial Manipulering

Mennesker som forsvarsmekanisme

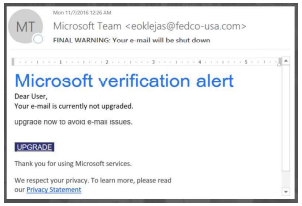
Sosial manipulering
Social Engineering Attacks

- According to Kevin Mitnick:
  - "The biggest threat to the security of a company is not a computer virus, an unpatched hole in a program, or a badly installed firewall. In fact the biggest threat could be you."
  - "What I found personally to be true was that it's easier to manipulate people rather than technology. Most of the time, organisations overlook that human element".

From "How to hack people", BBC NewsOnline, 14 Oct 2002

Typer av sosial manipulering

- Tekno-social manipulering
  - Manipulere gjennom elektronisk kontakt med ofre
  - E-post, telefon, SMS, sosiale nettverk, chat, nettsteder
  - Kombinasjon av ulike kanaler



- Ansikt-til-ansikt sosial manipulering
  - Manipulere mennesker i en fysisk omgivelse
  - Overbevise ofrene til å utføre handlinger som kompromitterer sikkerheten
  - Åpne dører, gi fysisk tilgang, tillat bruk av IT-ressurser

Phishing-angrep

- Et tekno-sosialt angrep der kriminelle bruker falske e-poster for å lure folk til å dele sensitiv informasjon eller installere skadevare på en computer.
- Faser
  1. Angriper sender phishing-e-post, komme gjennom spamfilteret og lande i offerets innboks
     - Stadig vanskeligere å komme gjennom e-postfiltrering (SPF, DKIM, DMARC)
     - Innholdet må være tilstrekkelig troverdig til å lure brukeren
  2. Offeret blir lurt, og utfører den foreslåtte handlingen i meldingen
     - Aksesser til et falskt nettsted
     - Svar med sensitiv informasjon
     - Installere skadevare
  3. Angriperen utnytter handlingen, f.eks. For å stjeler penger

Typer av phishing-angrep

- **Massephishing –** Masseangrep med stort volum ment å nå så mange mennesker som mulig
- **Spyd-phishing –** Målrettet angrep rettet mot bestemte personer eller selskaper. Met etterretning kan angriper tilpasse meldingen og gjøre svindelen vanskeligere å oppdage
- **Direktørsvindel (Hval-phishing) –** En type spyd-phishing som er rettet mot "stor fisk", inkludert høyprofilerte individer eller de som har mye autoritet eller tilgang
- **Klone-phishing –** Kopi av en legitim og tidligere levert e-post, med originale vedlegg eller hyperkoblinger erstattet med skadelige versjoner, som sendes fra en forfalsket e-postadresse, slik at den ser ut til å komme fra den opprinnelige avsenderen eller en annen legitim kilde

Å detektere phishing-svindel

- Kjennetegn:
  - Stavefeil (f.eks. "Passward"), manglende tegnsetting eller dårlig grammatikk
  - Mystisk URL, eller URL er forskjellig seg fra den som vises, eller den er skjult
  - Truende språk som krever umiddelbar handling
  - Forespørsler om personlig informasjon
  - Kunngjøring som indikerer at du har vunnet en premie eller lotteri
  - Forespørsler om donasjoner

- Vær skeptisk, bruk sunn fornuft
- Likevel, alle kan bli lurt hvis en phishing e-post er godt nok laget
- Trusselaktører må bruke mye tid og ressurser for spydphishing
  - men ML kan effektivisere generering av spydphishing-tekst.

Å beskytte seg selv – Ikke ta agnet

- **STOPP. TENK. SPØR.**
  - Før du klikker, se etter vanlige phishing-taktikker, spør kollegaer
- Vær ekstremt forsiktig med å klikke på lenker i en e-post
  - Bruk datamusen til å sveve over hver lenke for å bekrefte den faktiske adressen, selv om meldingen ser ut til å være fra en trygg kilde
  - Vær oppmerksom på URL-en og se etter feil stavemåten eller et annet domene (f.eks. ndsu.edu vs. ndsu.com)
  - Vurder å navigere til kjente nettsteder «manuelt» i stedet for å bruke lenker i meldinger
- Undersøk nettsteder nøye
  - Ondsinnede nettsteder kan se like ut som legitime nettsteder.
  - Alle nettsteder har «https», hvis bare «http» er det mistenkelig.
  - Klikk på hengelåsikon for å se hvem som eier domenet.

Tok du agnet?
Beskytt deg selv – du må handle umiddelbart!

Hvis du mistenker at…	Da må du…
du har utført handlinger I en phisning-epost eller en svindel-nettside	Kontakt umiddelbart helpdesk eller en annen relevant enhet.
du kanskjne har oppgitt sensitive, personlig eller økonomisk informasjon	Endre umiddelbart passord for berørte kontoer. Hvis du bruker samme passord for flere kontoer og nettsteder, kan du endre det for hver konto. Ikke bruk samme passord i fremtiden. Se etter tegn på identitetstyveri ved å gå gjennom bank- og kredittkortutskrifter for mulige uautoriserte kostnader og aktiviteter. Hvis du merker noe uvanlig, må du umiddelbart kontakte banken. Vurder å rapportere angrepet til politiet.

Ansikt-til-ansikt sosial manipulering

- Nevro-Lingvistisk Programmering (NLP)
- Bygge tillit
- Indusere emosjoner
- Informasjonsoverlast
- Gjenytelse
- Fordreining av plikt og ansvar
- Forpliktelseskryp
- Autoritet

Taktikk: Nevro-Lingvistisk Programmering (NLP)

- NLP er en pseudovitenskapelig tilnærming til menneskelig kommunikasjon som går ut på at språk og nevrologiske prosesser kan påvirke atferdsmønstre (programmering).
- Gjøre det mulig for en angriper å påvirke offeret gjennom å speile
  - kroppsspråk,
  - stemmebruk,
  - tonefall og ordbruk
- Indusere en emosjonell forbindelse med offeret på et underbevisst nivå, noe som gjør det lettere å påvirke offeret.
- NLP er en teknikk som brukes av selgere for å påvirke kunder.

Taktikk: Bygge tillit

- Folk stort sett naturlig hjelpsomme og tillitsfulle.
- Grunntillit kan forsterkes og utnyttes for sosial manipulering.
- En angriper kan starte med å bygge tillit ved å stille tilsynelatende uskyldige spørsmål under normale samtaler, og deretter sakte og umerkelig utnytte tilliten ved å be om stadig viktigere informasjon.
- Angriperen lærer seg bedriftssjargong, navn på nøkkelpersoner, navn på prosjekter og avdelinger, navn/lokasjon på servere og applikasjoner.
- Snakk negativt om fiender/konkurrenter, og positivt om venner/partnere

Taktikk: Indusere emosjoner

- Emosjoner er nært knyttet til atferdsmønster
- Kan avbryte nåværende atferd og frembringe en annen type atferd.
- Hvis en person vanligvis forsøker å vurdere argumenter rasjonelt, kan plutselige sterke emosjoner gjøre personen mindre årvåken og mindre i stand til å identifisere villedende argumenter.
- Angriperen kan f.eks.
  - indusere spenning/glede («du har vunnet en pris»),
  - frykt («du kommer til å miste jobben din»)
  - forvirring («prosjektleder sier X, men avdelingsleder sier det motsatte»).

Taktikk: Informasjonsoverlast

- Evne til å tolke informasjon og vurdere argumenter kan reduseres ved at angriperen gir for mye informasjon.
- Angriperens mål er å skape en kognitiv og mental blindhet, f.eks. ved å beskrive mange relevante og irrelevante aspekter samt å gi argumenter fra uventede vinkler, noe som skaper en høy mental belastning.
- Når belastningen går over en viss grense, kan offeret til en viss grad slutte å tolke informasjonen og slutte å vurdere argumentene

Taktikk: Gjenytelse

- Vi har et iboende instinkt om å gjenytelse av tjenester og favører.
  - Instinktet slår inn selv om den første favøren ikke ble forespurt
  - Gjenytelsen kan være mer verdifull enn den første ytelsen.
- Hvis offeret har mottatt en favør av angriperen, vil offeret lettere la seg manipulere av angriperen.
- Dobbel uenighet er en angrepsteknikk der angriperen først ber om to favører som offeret i utgangspunktet ikke er villig til å gi.
  - Hvis angriperen deretter trekker tilbake forespørselen om den ene favøren, vil offeret ubevisst føle en slags forpliktelse til å ettergi den andre favøren.
- Forventning er en teknikk som går ut på at forespørselen om en favør forbindes med (løfte om) at angriperen blir en fremtidig alliert og vil gjengjelde favøren i fremtiden.

Taktikk: Fordreining av plikt og ansvar

- Få offeret til å tro at ingen trenger å stå til regnskap for den type handlinger angriperen ber om
- Få offeret til å føle at det er en moralsk plikt å tilfredsstille angriperens forespørsel.
- Si at sikkerhetspolicyen ikke bør følges f.eks. med argumentere som:
  - sikkerhetspolicyen er ulogisk og har uheldige sider
  - sikkerhetspolicyen er utdatert,
  - eksempler på at kolleger og ledere ikke følger sikkerhetspolicyen

Taktikk: Forpliktelseskryp

- Vi har en tendens til å følge opp forpliktelser vi har tatt på oss,
  - Selv når de erkjenner at oppfølgingen kan være uklokt.
  - Å trekke tilbake inngåtte forpliktelser tolkes som å ha en svak karakter.

- Angriper skaper en situasjon der angriperen først gjør en relativt ufarlig forespørsel som offeret utfører, deretter en alvorlig forespørsel som logisk ligner på den første.
- Offeret føler seg forpliktet til å utføre den andre og alvorlige forespørselen.

- Eksempel:
  - Først spørre om å bruke offerets arbeidsstasjon til en enkel oppgave.
  - Dagen etter spør angriperen om å få bruke offerets passord til å logge på en annen arbeidsstasjon.
  - Hvis offeret kvier seg for å gi fra seg passordet, kan angriperen f.eks. si at det i praksis er det samme som det de gjorde dagen før, og at det derfor ikke fins noen grunn til å nekte.

Taktikk: Autoritet

- Vi har en tendens til å adlyde autoriteter
- Det er generelt ansett som frekt å utfordre ektheten av autoriteter.
- Mange måter å ikle seg en falsk autoritet på, f.eks.
  - falsk legitimasjon
  - falsk påstand om å være direktør, overordnet eller ha en rolle i en ekstern organisasjon.

- Det kreves skuespillertalent for å kunne gjøre dette på en overbevisende måte, og noen mennesker har et slikt talent (con artist).

Forsvar mot fysisk sosial manipulering

Source: David Gragg: https://www.sans.org/white-papers/920/

Slutt på presentasjonen om sikkerhetskultur