IN1020: Notat sikkerhet uke 5

Om sikre datasystemer

1 Sikkerhet for data som lagres

Digital informasjon oppbevares eller lagres på en fysisk enhet, ofte som filer eller i databaser: Disk i en laptop eller på en lagringsserver, en minnepinne, mobiltelefon, nettbrett, hos en skyleverandør, eller kanskje på en litt gammeldags magnetisk tape. En av sikkerhetsutfordringene ved lagring er at uvedkommende får tilgang til data, f.eks. på grunn av mangelfull tilgangskontroll, mistet eller stjålet enhet (f.eks. en laptop eller mobiltelefon), eller datainnbrudd hos lagringsserver eller en skyleverandør.

Ved manglende tilgangskontroll vil sikkerhetstiltaket være å innføre gode regler for tilgang, samt tilgangskontroll. For mistet/stjålet enhet eller hackerangrep vil vi ha behov for mekanismer som kan hjelpe med å sikre at både konfidensialitet, integritet og tilgjengelighet ivaretas best mulig også om noen får *uautorisert tilgang* til ressursene som inneholder data.

1.1 Kryptering: Beskyttelse mot innsyn og endring

Det vil i mange tilfeller være svært enkelt for en som er litt kyndig å få tak i og lese innholdet på en disk, selv uten riktig autentisering. For å beskytte data mot innsyn (ivareta konfidensialitet) og endring (ivareta integritet) vil *kryptering av data* fungere som et forebyggende sikkerhetstiltak, der kun den med tilgang til en *krypteringsnøkkel* kan dekryptere de krypterte dataene.

Kryptering av data ivaretar konfidensialitet ved at data er uleselig/uforståelig når de er kryptert, og integritet på den måten at endring eller sletting av krypterte data stort sett vil bli oppdaget, bl.a. fordi praktisk implementasjon av krypteringsalgoritmer svært ofte involverer sjekksummer av dataene.

Kryptering kan gjøres på flere nivåer: Kryptering av enkeltfiler, kryptering av et helt filsystem, eller det som kalles fulldiskkryptering, at absolutt alt på en disk krypteres. Kryptering og dekryptering er ressurskrevende for datasystemer, hvilket betyr at tilgang til data kan gå tregere, så dette er en viktig avveining når metode velges. Krypteringsnøkkel må også beskyttes godt og helst sikkerhetskopieres. Hvis forsvinner eller glemmes kan den krypterte informasjonen rett og slett ikke dekrypteres og er tapt.

1.2 Sikkerhetskopiering: Tiltak for gjenoppretting

Å ta backup (sikkerhetskopi) er definert som en planlagt strategi for å ta vare på informasjon over tid. En sikkerhetskopi gir et øyeblikksbilde av en tilstand på et gitt tidspunkt, og gjør det mulig å gå tilbake til nøyaktig den tilstanden. Det er altså et *gjenopprettende* tiltak som kan hjelpe til å gjenopprette systemer eller informasjon der enheter er stjålet/mistet, eller ved uønsket endring eller sletting av informasjon.

Et par viktige huskeregler for god strategi for sikkerhetskopiering:

- Versjonering: Informasjon i datasystemer endres som regel ofte. For å ta vare på informasjon over tid må man naturlig nok også ta vare på flere ulike versjoner bakover av denne informasjonen.

- Sikre sikkerhetskopien: Sikkerhetskopien må lagres separat fra de opprinnelige dataene. Lageres den sammen med eller samme sted som de opprinnelige dataene, kan sikkerhetskopien bli utsatt for nøyaktig det samme angrepet eller uhellet.
- Sikkerhetskopiering er ikke det samme som datasynkronisering. Mens datasynkronisering dreier seg om å synkronisere data på og fra en rekke enheter, er sikkerhetskopiering å lagre et øyeblikksbilde av informasjon som så kan tas vare på så lenge det er nødvendig.

1.3 Trygg avhending av data

Å kvitte seg med data eller informasjon på en slik måte at ingen andre får tak i dem kan være utfordrende. Mens papir kan sendes i makuleringsmaskin eller brennes, vil informasjon på et digitalt lagringsmedium være vanskeligere å bli kvitt. Slettes data fra disk, slettes som regel kun *referansene* til data, og en litt kyndig person vil ganske enkelt kunne gjenskape informasjon fra en slik disk. Skrekkhistorier om sensitive helsedata som er hentet ut fra avdankede datamaskiner er dessverre sanne. Det er viktig å være bevisst på faren dette utgjør og finne egnede verktøy for å sikre at kassert datautstyr ikke inneholder data som ikke skal komme på avveie.

2 Nettverkssikkerhet

Datanettverk brukes til kommunikasjon. Endesystemer som laptoper, mobiltelefoner, printere, og sensorer kommunisere over nettverk ved å sende meldinger i form av datapakker. Når en melding sendes ut på internett, har man ingen kontroll med hvem som leser meldingen underveis i transporten. Nettverket, med alle sine mellomstasjoner, kan være i stand til *å levere, slette, endre eller forfalske meldinger* som sendes. Dette kan sammenlignes med å sende en fysisk pakke med posten uten kontroll over hva som skjer underveis.

Kommunikasjonssikkerhet håndterer behovet for å sikre informasjon i transit over nettverk, altså når data overføres. Dette behovet er til stede både mellom ulike virksomheter (f.eks. UiO og Skatteetaten) og mellom noder innad i egen virksomhet.

Datanettsikkerhet, som består av skallsikring/perimeterforsvar er det å beskytte virksomheters egne dataressurser mot angrep og uautorisert tilgang fra omverdenen (typisk internett), f.eks. datatyveri, spionasje eller sabotasje.

2.1 Sikkerhetstrusler i nettverk

Sikkerhetstruslene som berører nettverk og bruk av nettverk er mange:

Avlytting (eavesdropping): Man kan risikere at trafikken avlyttes og uvedkommende får tak i konfidensiell informasjon, som brukernavn og passord sendt over nettverket. Dette er et passivt angrep.

Man-in-the-middle-angrep: Kjennetegnes ved at uvedkommende griper inn i kommunikasjonen og modifiserer data, for eksempel ved å sende deg til en falsk nettside.

Forfalskning av nettverkstrafikk: Noen utgir seg for å være en annen når en melding sendes, altså brudd på dataautentisitet. Datamodifikasjon og forfalskninger regnes som aktive angrep.

Tjenestenektangrep (Denial of Service - DoS og DDoS): En vanlig teknikk er å bombardere en tjeneste med nettverkstrafikk slik at den til slutt blir overbelastet og utilgjengelig for alle som har et legitimt behov for å bruke den.

Misbruk av nettverk og nettverksressurser: For eksempel til tjenestenektangrep, men også til å sende ut svindel-e-poster.

Sikkerhetstruslene er til en viss grad de samme når man kommuniserer over kablede nettverk som når man bruker trådløs forbindelse (wifi), men det er også noen naturlige ulikheter:

Trådløse nettverk: Kommunikasjon i trådløse nett strømmer fritt i eteren via radiosignaler, noe som skaper utfordringer da hvem som helst faktisk kan lytte til trafikken. Avlyttingsutstyr for trådløse signaler kan kjøpes relativt billig. Signaler følger heller ikke fysiske grenser som vegger og gjerder, noe som åpner for uautorisert nettverkstilgang uten at en potensiell inntrenger må ha fysisk tilgang til en lokasjon. Fysiske sikkerhetstiltak som krav til nøkkelkort for å komme inn i en kontorbygning vil dermed ikke være til hjelp.

Radiosignalene er sårbare for signalforstyrrelser (støy), både tilsiktet og utilsiktet, og kan føre til at signalene ikke kan fanges opp. Tilsiktede radioforstyrrelser kalles gjerne *jamming*, og kan være veldig vanskelig å beskytte seg mot.

Trådløse aksesspunkter kan også utgjøre en sikkerhetsrisiko, både ved at de forfalskes eller de kompromitteres (hackes). Aksesspunkter som styres av uvedkommende kan brukes for både avlytting av datatrafikk, men også for å spre virus eller annen skadevare til datamaskiner som kobler seg opp. Slike falske aksesspunkter utgjør en reell sikkerhetstrussel fordi de er enkle å sette opp og mange ukritisk kobler seg opp til tilsynelatende ekte trådløse nettverk.

Kablede nettverk: Det er naturlig nok nødvendig med fysisk tilgang til en nettverkskabel for å lytte til eller modifisere trafikk i et kablet nettverk. Har man først fysisk tilgang, er det fullt mulig å modifisere eller koble seg til en nettverkskabel på en slik måte at man får tilgang til alle data som transporteres via denne. Utstyr for dette kan enkelt kjøpes eller lages.

En fysisk kabel kan også ødelegges, rett og slett kuttes over, tilsiktet eller utilsiktet, noe som fører til brudd på tilgjengelighet. For kritisk infrastruktur som nettverkskabler, er det svært viktig å ha et redundant system slik at man raskt kan få en alternativ forbindelse på plass hvis et uhell er ute. Nettverksutstyr som routere og switcher kan selvfølgelig hackes og kompromitteres akkurat som trådløse aksesspunkter. I tillegg kan kompromitterte enheter, for eksempel en datamaskin som er infisert av virus eller er i hendene til en hacker, utgjøre en direkte risiko for andre datamaskiner på samme fysiske nettverk.

2.2 Sikkerhetstiltak for nettverk

Fordi avlytting av nettverkstrafikk er enkelt, og kommunikasjon over spesielt trådløse nettverk kan sammenlignes med å rope til hverandre, må man gjøre datatrafikken uleselig for andre enn dem meldingene er tiltenkt. En løsning er altså bruk av kryptografi – meldinger som sendes må krypteres. Ulike nettverksprotokoller tilbyr kryptert og sikker kommunikasjon, selv om sårbarheter i protokoller og krypteringsalgoritmer dessverre også finnes.

Gjennom skallforsvar er man interessert i å styre og kontrollere hva slags datatrafikk som slipper inn til og ut fra et lokalt nettverk. For tilgangskontroll til et nettverk benyttes gjerne det som kalles *brannmur*. Hva slags trafikk som slippes igjennom sjekkes mot et regelsett, og hvorvidt en brannmur fungerer etter hensikten avhenger derfor av at regelsettet er godt og dekkende. En brannmur kan være en egen datamaskin eller programvare.

Skallforsvaret gjerne også av inntrengningsdeteksjon (eller innbruddsdeteksjon), som er overvåkning av nettverkstrafikk for å oppdage eller detektere mistenkelig aktivitet. Dette er en viktigere og viktigere del av informasjonssikkerhet, og teknologiene er i stadig utvikling. Overvåkning bør for eksempel kunne avdekke om hackere utfører såkalt *scanning* av nettverk og datamaskiner etter sårbarheter, og overvåkningen vil kunne avdekke mistenkelig aktivitet i nettverkstrafikken brannmuren tillater. Denne type overvåkning er ressurskrevende, og det er behov for svært effektive teknologier og algoritmer.

3 Sikre Datasystemer

Et typisk datasystem består av en datamaskin med sin interne systemarkitektur og med en rekke tilknyttede perifere enheter som skjerm, tastatur og mus. Maskinen er også tilknyttet et nettverk, og en sluttbruker bruker datamaskinen enten via en nettapplikasjon eller kjører programvare lokalt. Systemene inneholder operativsystem og applikasjoner, mens nettverket binder dem sammen. Både operativsystem, drivere og nettverksprotokoller er programvare som noen har utviklet, og kalles gjerne systemprogramvare. Felles for all programvare – både systemprogramvare og applikasjoner – er at de er sårbare for programvareangrep.

Så hvordan kan vi kan oppnå sikre datasystemer, både gjennom trygg systemprogramvare og sikre applikasjoner?

3.1 Nødvendige definisjoner:

3.1.1 Sårbarheter

En *sårbarhet* er en feil eller en svakhet i et datasystem som åpner for mulighet til å utnytte systemet. Datasystemer er svært komplekse, så det finnes til enhver tid svært mange feil og svakheter i de aller fleste systemene.

En sårbarhet som oppdages og offentliggjøres av angripere før den oppdages av produsenten av tjenesten kalles **nulldagssårbarhet (Zero-day vulnerability)**. Navnet refererer til at produsenten har hatt nøyaktig null dager til å rette den oppdagede feilen, noe som betyr at det finnes ingen fiks eller patch, og sårbarheten ligger åpen for utnyttelse i alle eksemplarer av produktet.

En sårbarhet kan ha følgende tilstand:

- **Kjent og akseptert:** Stort sett som følge av økonomisk spørsmål, som handler om kostnadene ved å håndtere sårbarheten sett opp mot konsekvensen hvis den blir utnyttet på verst tenkelig måte.
- **Kjent og uakseptert:** Må håndteres umiddelbart, selv om det kan innebære å skru av et datasystem eller fjerne det fra internett frem til feilen er rettet, da konsekvensen ved et eventuelt angrep er noe man ikke kan akseptere.
- **De ukjente eller feilvurderte:** Disse er de desidert farligste, da systemeier eller brukere rett og slett ikke er klar over at de kan bli eller er utsatt for angrep.

3.1.2 Angrepsvektor

Angrepsvektor er benevnelsen for metoden en angriper velger bruke for å sette inn et angrep. Det er en kombinasjon av *kanalen* og det skadelige innholdet som benyttes i et angrep.

3.2 Systemsikkerhet: Trygg systemprogramvare

Operativsystemet er styringsprogrammet som er nødvendig i de aller fleste datamaskiner. Kjernen er i operativsystemet og styrer så å si alle ressurser i en maskin, inkludert kommunikasjon med perifere enheter. Dette betyr at alle brukerprosesser må gå via kjernen for å kunne ta i bruk f.eks. tastatur og skjerm. Kjernen er et dataprogram og kan dermed inneholde sårbarheter. De fleste operativsystemer har ulike tilgangsnivåer, der kjernen er privilegert mens brukerprosessor har få privilegier. En sårbarhet i kjernen er derfor potensielt svært kritisk og kan gi inntrengere vesentlige tilganger til mye programvare og maskinvare, og det ivareta sikkerhet i operativsystem og drivere er svært viktig. Programvaren må i utgangspunktet være laget slik at den ikke inneholder sårbarheter, men den må også videre i sitt livsløp holdes oppdatert når ny funksjonalitet legges til eller ukjente sikkerhetshull oppdages.

3.2.1 Bufferoverskridelse

Et buffer er et midlertidig lagringsområde i en datamaskins minne som brukes til å holde data mens de overføres eller behandles. *Bufferoverskridelse* er en type programvarefeil i hvor et dataprogram skriver mer data til en minnebuffer enn bufferet er avsatt til å holde, noe som får data til å overskrive naboområder i minnet. F.eks. plassere en tekststreng med 50 tegn i en variabel som i programkoden er definert til å kun ha plass til 20 tegn.

Overskrivelse av buffer kan føre til at programmet krasjer, oppfører seg uforutsigbart, men den farligste konsekvensen er nok at hackere kan utnytte bufferoverskridelsen til å *injisere og kjøre* sin egen kode på en annens datamaskin. Dette kan i verste fall gi dem full kontroll over det angrepede IT-systemet.

Mottiltak mot bufferoverskridelse er kompetanse på hvordan kode trygge programmer. All input til et dataprogram bør filtreres, det vil si at uventet eller skadelig input fjernes av programmet. Produsentene av prosessorer og operativsystemer forsøker også å vanskeliggjøre denne typen utnyttelser. Programmeringsspråk uten innebygget sjekk av buffergrenser er spesielt utsatt, men er samtidig svært effektive og mye brukt i operativsystemer på grunn av effektiviteten.

3.2.2 Oppstarten av en datamaskin

Det som skjer før operativsystemet er lastet og kjører, er også et kritisk punkt. Ved oppstart startes *bootloaderen* fra BIOS, og deretter laster bootloaderen kjernen i operativsystemet. Det er viktig å sikre at BIOS eller bootloaderen ikke er manipulert, noe som kan løses blant annet gjennom *integritetssjekk* av systemprogramvare ved oppstart. Leverandører av datamaskiner og operativsystemer har flere ulike tilnærminger til løsning på denne utfordringen.

3.3 Applikasjonssikkerhet

Applikasjoner (som også er dataprogrammer) kjennetegnes ved at de gjerne har et grensesnitt mot brukere, ofte over internett (for eksempel webapplikasjoner eller mobilapper). Dette betyr at de i stor grad er eksponert for angrep og skadevare utenfra.

3.3.1 SQL-injeksjon

SQL er er spørrespråk som brukes til å hente ut eller manipulere data i relasjonsdatabaser. SQL-injeksjon er et angrep der en angriper manipulerer slike spørringen ved å injisere skadelig SQL-kode, f.eks. i et felt for brukerinput på en nettside. Hvis applikasjonen ikke håndterer brukerinput korrekt, blir den skadelige koden en del av den opprinnelige SQL-spørringen til databasen, og kan gi hackeren uauorisert tilgang til data i databasen. Et opplagt mottiltak er også her å filtrere all brukerinput for å fjerne uventet eller skadelig input, men også gjennomtenkte formateringer av SQL-spørringene er viktig.

3.3.2 Cross site scripting.

Cross-site scripting (XSS) er en type angrep der det injiserer skadelig kode (ofte JavaScript) på et nettsted, kanskje som innhold i en *brukeranmeldelse* i en nettbutikk el. Når et offer besøker den infiserte nettsiden er risikoen at offerets nettleser kjører den skadelige koden. Dette kalles et såkalt *drive-by-angrep*. Den skadelige koden kan uten at brukeren er klar over det overføre vedkommende til en falsk nettside med mål å stjele innloggingsdetaljer, eller den benyttes til å stjeler sensitiv informasjon som informasjonskapsler (cookies). For å hindre denne typen angrep er det også her viktig å filtrere all brukerinput for å fjerne uventet eller skadelig input, både i webapplikasjonen men også hos klienten.

3.3.3 Trygg applikasjonsutvikling

Med andre ord er det viktig å sørge for applikasjoner som er trygge i bruk, og sikkerhet må involveres i alle faser av applikasjonsutviklingen:

- I designfasen må potensielle trusler kartlegges og tiltak som kan motvirke truslene identifiseres. Dette krever nødvendigvis kunnskap om sikkerhet og sikkerhetstrusler allerede hos de som designer nye tjenester.
- I programmeringsfasen må det legges vekt på å kode programmer uten sårbarheter, noe som krever kompetanse også hos utviklerne.
- Til slutt må tjenestene forvaltes med tanke på god sikkerhet, hvilket krever kompetanse også hos de som står for den daglige driften av en IT-tjenesten.

3.4 Prinsippet om svakeste punkt

Sikkerhet er aldri sikrere enn det svakeste punktet i kjeden. Du kan designe og programmere så sikkert du bare klarer, men hvis operativsystemet er fullt av sårbarheter har hackere like fullt en mulighet til å gjennomføre vellykkede angrep. Dette kan sammenlignes med sikring av et hus: Det hjelper ikke å låse døra for å stoppe inntrengere hvis alle vinduer står på vidt gap. Moralen er derfor at for å oppnå tilstrekkelig sikkerhet i et datasystem, må sikkerhet ivaretas på absolutt alle nivåer i systemet. Det krever en **helhetlig tilnærming**. Jo mer kritisk et system er, jo viktigere er selvfølgelig denne ivaretakelsen.

4 Skadelig programvare

Skadevare (engelsk *malware*) er en samlebetegnelse på programvare som er skapt med den hensikt å gjøre en eller annen form for skade på eller i et datasystem, altså ondsinnet programvare. Skadevaren er hackerens "verktøykasse"og benyttes av angripere med flere formål, som å tilegne seg tilgang til dataressurser, for å få tilgang til informasjon som kan utnyttes videre til utpressing, eller for sabotasje. For å oppnå dette utnytter skadevaren de sårbarhetene som finnes i et datasystem.

Skadevaren kan være avhengig av å være en del av et vertsprogram, eller den kan være et enkeltstående program som kan kjøres som en egen prosess av operativsystemet. Noe skadevare formerer seg og infiserer andre systemer den kan nå, som regel avhengig av en eller annen trigger som en bestemt hendelse eller et bestemt tidspunkt. Vanlige spredningsmetoder er via nettverkskoblinger i datasystemet eller som vedlegg i e-post.

Hensikten med skadevaren, altså "jobben" skadevaren er satt til å gjøre kalles **nyttelast** (payload). Nyttelasten kan være f.eks. et dataprogram som spionerer på alle tastetrykk eller signaler til skjermen, eller det kan være et program som krypterer alle filer i datasystemet (løsepengevirus).

4.1 Ulike typer skadevare

Det er først og fremst spredningsmetoden som skiller de ulike typene skadevare, men man kategoriserer og navngir dem også etter hensikten (nyttelasten). Kategoriene er til dels overlappende:

- **Virus (datavirus):** Brukes ofte som en samlebetegnelse på all skadevare, noe som kan være forvirrende. Rene virus har den egenskapen at de sprer seg hver gang de aksesseres, men denne typen skadevare er ikke like vanlig som tidligere.
- **Orm:** Sprer seg uten menneskelig innblanding.

- **Trojaner:** Som navnet sier, utgir den seg for å være noe man har nytte av, f.eks. et program som en bruker derfor laster ned fra internett.
- **Bakdør:** Også nærmest selvforklarende; nyttelasten er å skape en skjult inngang inn til et datasystem, og angriperen omgår på den måten både autentisering og tilgangskontroll.
- **Spionvare (spyware) og tastelogger (keylogger):** Begge er skadevare laget for å spionere på en bruker for å tilegne seg informasjon. En tastelogger, som både kan være et fysisk program eller en liten enhet, har som eneste mål å fange opp og videreformidle tastetrykk til angriperen, og dermed få tak i for eksempel passord eller annen sensitiv informasjon.
- **Rootkit:** Programvare som gir en angriper uautorisert administrator- eller rotrettigheter, altså full tilgang til et datasystem.
- **Exploit:** Er på sett og vis en oppskrift på eller implementasjon av et angrep, og kan bestå av for eksempel et program, en sekvens av kommandoer eller en samling data som kan brukes for å utnytte et datasystem. Slike *utnyttelser* er salgsvare, som det dessverre finnes et stort marked for.

4.2 Spredningsmetoder:

- E-post og e-postvedlegg med skadevare eller lenker til skadevare.
- Spre skadevare til besøkende på infiserte eller ondsinnede nettsider.
- Via tilkobling og bruk av ondsinnede eller infiserte eksterne enheter, som for eksempel en USB-disk.
- Direkte via internett, der sårbarheter i eksponerte applikasjoner eller operativsystem utnyttes.
- Infisering via det vi kaller leveransekjeden: Hackere kan utnytte svakheter og infiltrere teknologi fra leverandører som ditt datasystem igjen bruker og er avhengig av.

Moralen er at man skal tenke seg om minst to ganger før man låner en USB-pinne fra en venn eller ukritisk åpner et vedlegg i e-post, selv om man stoler på vennen sin og er 100 prosent sikker på at vedlegget kommer fra noen man kjenner. Angrep via leveransekjeden viser seg dessverre vanskeligere å beskytte seg mot.

4.3 Mottiltak

Det er slik at svært mange dataangrep involverer skadevare i en eller annen form, og skadevaren er en del av en angrepsvektor. Dette skal man være klar over både som bruker av datasystemene og som den som er ansvarlig for dem. Mottiltak kan settes inn på mange ulike nivåer og involverer alt fra:

- Antivirusprogramvare.
- Å følge alle sikkerhetsoppdateringer av all programvare.
- Å skape god og solid sikkerhetskultur innad i virksomheten.
- Å ha gode rutiner for sikkerhetskopier av data.
- Gode og gjennomprøvde rutiner for gjenoppretting av systemer.

5 Den menneskelige faktoren

En angrepsvektor involverer ofte menneskelige beslutninger, menneskelige valg som påvirkes av det vi kaller sikkerhetskultur. De valgene vi tar kan faktisk være avgjørende for om et angrep er vellykket eller ikke. Vi som mennesker, eller altså brukere, kan rett og slett utgjøre en sårbarhet gjennom å ta feil valg (f.eks. ukritisk åpne vedlegg, klikke på lenker i e-post, lade mobil overalt i ukontrollerte USB-innganger, koble ukjente minnepinner til laptopen).

Men vi kan faktisk også være et forsvarsverk ved å ta gode valg, vi kan bevisst eller ubevisst avverge angrep. Som brukere er vi en del av et *menneskelig innbruddsdeteksjonssystem*, og hvor godt dette systemet fungerer avhenger i stor grad av hvor god jobb den enkelte av oss gjør. Typiske hendelser er at vi kan mangle forståelse for digital sikkerhet, hva som utgjør trusler og hva som kan være eller bli sårbarheter, og dermed ta feil avgjørelser på bakgrunn av den manglende kompetansen. Vi kan også risikere å bli utsatt for såkalt *sosial manipulasjon*.

5.1 Sikkerhetskultur

Nasjonal Sikkerhetsmyndighet (NSM) definerer sikkerhetskultur som summen av de ansattes kunnskap, motivasjon, holdninger og adferd som kommer til uttrykk gjennom virksomhetens totale sikkerhetsadferd. Den kulturen vi er en del av til enhver tid, enten det er som nasjon eller organisasjon, gir oss et sett av verdier som hjelper oss å forstå omgivelsene. Disse verdiene utstyrer oss med et kompass som sier hvordan vi gjør ting "her hos oss".

5.2 Sosial Manipulasjon

Sosial manipulasjon er et svindelangrep hvor angriperen utnytter sider av deg som menneske, de spiller ofte på tillit eller svakheter. Sosial manipulasjon rettes mot og berører alt fra enkeltpersoner til store virksomheter. En *innsidebruker* (f.eks. en ansatt i en virksomhet) vil typisk være et godt mål for både utpressing og overtalelser.

Angrep med sosial manipulasjon benytter ofte e-post med falske lenker eller skadevare i en eller annen form. Innholdet må være tilstrekkelig troverdig, så for å lure deg kan en falsk avsender være noen du kjenner (kanskje en kollega eller en myndighetsperson hos arbeidsgiveren din) eller en kjent virksomhet. Angrep kan også spille på følelser som glede (typisk pengepremier, gaver eller lignende) eller frykt (typisk utpressing). En annen vanlig fremgangsmåte er at offeret blir kontaktet av noen som ber om informasjon de trenger til et eller annet formål, kanskje fra . De færreste agrep er veldig målrettet, men man ser også flere og flere avanserte angrep som retter seg direkte inn mot for eksempel ansatte med myndighet i en virksomhet.

Spoofing er benevnelsen for forfalskning av avsender i f.eks. e-post eller SMS.

Phishing: Betyr rett og slett å "fiske" etter opplysninger, og fremgangsmåten er å lure mottakeren/offeret til å oppgi informasjon angriperen er ute etter. Avhengig av hvem mottaker er, har man ulik benevnelse på phishing-angrep.

Masse-phishing: Som navnet antyder, en bredt utsendt e-post som ikke inneholder korrekte detaljer om mottaker.

Spear-phishing: Et mer målrettet angrep der avsender har samlet informasjon om mottaker. Dette gjør i mange tilfeller henvendelsen mer troverdig og er vanskeligere å avsløre.

Whaling (Direktørsvindel): Svært målrettet phishing mot personer med makt og myndighet, gjerne økonomisk sådan.

5.3 Mottiltak og viktigheten av sikkerhetskultur

Det finnes en rekke teknologiske tiltak for å begrense angrepsflaten, også for de angrep som benytter sosial manipulasjon. De aller fleste e-posttjenere vil for eksempel ha funksjonalitet for skanning og filtrering av e-post (et såkalt *spamfilter*) med mål å fjerne ondsinnede e-post. Bortfiltrering av ondsinnede e-post er en vanskelig øvelse, da man for eksempel ikke ønsker falske positiver (viktig e-post som ikke blir levert fordi man tror det er spam). Dette betyr også at noe ondsinnede e-post alltid vil slippe gjennom og nå sluttbrukeren. Derfor er en sterk og god sikkerhetskultur helt essensielt, både i samfunnet generelt og i alle virksomheter som benytter datasystemer. Som en del av dette er grundig opplæring av sluttbrukere avgjørende. Dette minimerer sjansen for å bli offer for svindelangrep og forhåpentligvis også utpressing eller overtalelsesangrep. **For hva er enklest å manipulere, mennesker eller teknologi?**