IN1020: Notat sikkerhet uke 1

Om digital sikkerhet, sikkerhetsmål og sikkerhetstiltak

1 Introduksjon til digital sikkerhet

Begrepet sikkerhet omfatter mye forskjellig i det norske språket. Vi snakker gjerne om fysisk sikkerhet, samfunnssikkerhet, personsikkerhet, miljøsikkerhet eller kanskje datasikkerhet. Sikkerhet kan være å sikre verdigjenstander i en safe, å overvåke områder, å verne naturen, eller å ikke dele sin BankID med andre.

På engelsk uttrykkes sikkerhet hovedsakelig gjennom tre begreper (safety, security og certainty), som alle oversettes til det litt upresise *sikkerhet* på norsk. Mer presise oversettelser vil være:

- Safety (Trygghet): Handler om å beskytte mot utilsiktede hendelser eller ulykker. Et eksempel er å holde fast i et trapperekkverk for å unngå å falle. Et annet er å ta sikkerhetskopi av data fordi du er redd for at mobilen skal falle i vannet og alt innhold skal gå tapt.
- Security (Sikkerhet): Handler om å beskytte mot tilsiktede, ondsinnede handlinger. Et eksempel er å holde fast i et trapperekkverk for å hindre at det blir stjålet, eller å ta sikkerhetskopi av data fordi du er redd for hacking og ødeleggelse av innholdet. Merk deg at tiltak for å bedre sikkerheten eller tryggheten vil ofte avhjelpe begge deler.
- Certainty (Visshet): Handler om overbevisning – å være vis på noe, det vil si å med sikkerhet kunne si at noe er slik eller slik.

1.1 Sikkerhet som dynamisk tilstand

Mer generelt kan sikkerhet defineres som beskyttelse av verdier mot skade, og en vanlig definisjon er sikkerhet som en tilstand av *fravær av uønskede hendelser, eller frihet fra fare og frykt.*

En slik tilstand vil ikke være statisk, den påvirkes kontinuerlig av endringer i faktorer som trussel og farer, sårbarhet og verdi. Dette understreker at arbeidet med god sikring og sikkerhet er en pågående prosess som krever kontinuerlig vurdering av nye eller endrede trusler, sårbarheter og verdier. Fokuset kan altså aldri legges helt til side.

1.2 Å beskytte verdier

Å identifisere verdiene som skal eller må beskyttes er grunnlaget for å vurdere sårbarheter, trusler og risiko. Hva som er en verdi, er fullstendig avhengig av hva som er viktig for noen eller noe i et gitt tilfelle. Nøyaktig den samme informasjonen kan for eksempel ha ulik verdi for en privatperson og en kommersiell virksomhet. Det som er viktig for deg som privatperson er ikke nødvendigvis sammenfallende med det som er viktig for samfunnet eller en virksomhet.

1.3 Sikkerhet i en digital kontekst

Mange er flinke til å tenke på og ivareta sikkerhet og trygghet i ikke-digitale omgivelser, for eksempel ved å låse dører, installere alarm i hjemmet for å hindre innbrudd, samt ha røykvarslere for å oppdage brann. Dette kan skyldes både medfødte egenskaper, erfaringer og kulturelle

betingelser. I en digital kontekst mangler imidlertid mange den grunnleggende forståelsen for digital sikkerhet; De stoler blindt på IT-systemene, eller stoler kanskje ikke på dem i det hele tatt. I IN1020 er fokuset naturlig nok sikkerhet i en digital hverdag.

1.4 Ulike begreper, samme betydning?

I omtale av digital sikkerhet møter man ofte flere ulike begreper som har nesten samme betydning, og som det er greit å ha kjennskap til. De vanligste begrepene er informasjonssikkerhet, datasikkerhet og cybersikkerhet, og de er delvis overlappende:

Informasjonssikkerhet: Dette er det mest generelle begrepet, og handler om å beskytte informasjon eller data, enten den er analog (på papir) eller digital (som filer i et datasystem). Informasjon kan være personopplysninger, programvarekode, konfigurasjonsdata for et IT-system eller bedriftsdata. I takt med digitaliseringstrenden minker mengden analoge data, mens mengden digitale data er sterkt økende, og begge trenger sikring. I dette kurset vil begrepet informasjonssikkerhet hovedsakelig bli brukt.

Datasikkerhet (computer security): Har fokus på sikringen av IKT-tjenester og datamaskiner, altså det teknologiske. Dette overlapper delvis med informasjonssikkerhet, da beskyttelse av digital informasjon nødvendigvis krever beskyttelse av IKT-systemer og datamaskiner som inneholder eller behandler data. IKT-systemer og datamaskiner som inneholder eller behandler data kalles informasjonsressurser.

Cybersikkerhet: Brukes gjerne om sikkerhet i "cyberspaceeller rett og slett for alle systemer og all infrastruktur som er koblet sammen via internett. Eksempler inkluderer industriroboter, selvkjørende tog, fly og internettkabler. Hva som faller inn under cybersikkerhet er delvis overlappende med datasikkerhet og informasjonssikkerhet.

1.5 Trusselaktører

En trusselaktør er den som utfører dataangrep Dette kan være hvem som helst, fra hvor som helst i verden, så lenge de har internettforbindelse. Eksempler på trusselaktører inkluderer:

- Sporadiske hackere: De som hacker for moro skyld, for anerkjennelse eller fordi de ser det som en utfordring. Selv om de har begrensede ressurser, kan angrepene deres ha alvorlige konsekvenser for den som rammes.
- Aktivister: Saboterer eller markerer seg for å understreke og nå frem med et budskap.
- Kriminelle: Har flyttet sin virksomhet over i den digitale verden, for eksempel ved å loppe banker eller kunder online i stedet for fysiske innbrudd. Kriminelle nettverk kan ha enorme ressurser og profesjonelt satse på dataangrep, noe som gjør dem svært vanskelig å beskytte seg mot.
- Virksomheter/organisasjoner: Kan være ute etter å få tak i forretningshemmeligheter eller annen informasjon fra andre virksomheter, eller til og med direkte skade konkurrenter for egen vinnings skyld.
- Nasjonalstater: Har også flyttet mye av sin virksomhet over i cyberspace, blant annet etterretningsvirksomhet og spionasje. Nasjoner kan ha enorme ressurser og profesjonell tilnærming til dataangrep.

Fellesnevner for mange angrep er økonomisk vinning (å tjene penger), men også det å oppnå makt eller å påvirke politiske prosesser er aktuelle drivkrefter. Man kan merke seg at motivene for angrep i bunn og grunn er de samme som i en ikke-digital verden.

1.6 Økende trussel

Statistikker viser at datakriminaliteten stadier er økende. Flere og flere tjenester digitaliseres, noe som igjen øker den generelle sårbarheten og insentivene for angrep blant kriminelle. Digitale angrep kan føre til reelle farer som direkte påvirker oss fysisk i det virkelige liv, som utfall av strøm eller vann. Dette understreker at digital sikkerhet er særdeles viktig, og samfunnet er heldigvis i økende grad bevisst dette.

Hendelser som datainnbrudd og datalekkasjer er fremdeles underrapportert, da enkelte virksomheter dysser ned og dekker over fremfor å være åpne om hendelser som rammer dem. Mange opplever det som mer tabubelagt å bli utsatt for datainnbrudd enn ordinært innbrudd. Heldigvis er denne trenden i ferd med å snu, og stadig flere er åpne om datainnbrudd. Denne åpenheten er verdifull da den bidrar til deling av erfaringer, og andre virksomheter kan være oppmerksomme på de samme feilene og fellene, og man kan stå sammen mot kriminalitet.

1.7 Tilfeldige eller målrettede angrep?

Dataangrep kan være både tilfeldige og målrettede:

Tilfeldige angrep. Svindel for småpengerer ofte tilfeldig. Det sies gjerne at den som er sårbar blir et offer. Mange privatpersoner tror de er uinteressante for hackere og er derfor ikke nøye nok med sikring av sine verdier. Eksempelvis kan en datamaskin med en spesiell sårbarhet bli funnet og skannet av en tilfeldig kriminell via internett, og plutselig kan du være rammet av et løsepengevirus hvor filer tas som gissel og det kreves betaling av løsepenger for å få dem lesbare igjen.

Målrettede angrep. Kriminelle velger mål som gir størst mulig avkastning, enten økonomisk eller i form av interessant informasjon. Eksempler inkluderer direktørsvindel, sabotasje eller spionasje som er målrettet mot virksomheter, personer eller andre stater.

1.8 Er digital sikkerhet nødvendig?

Det er et sterkt behov for økt kunnskap om og fokus på digital sikkerhet. Dessverre setter vi som forbrukere ofte pris på ny og fancy teknologi fremfor sikkerhet, noe som betyr at aktørene som konkurrerer om forbrukermarkedet gjør den samme prioriteringen. Dette fører igjen til at sikkerhet fort nedprioriteres når utviklere av tjenester har tidspress; Raskest mulig lansering i et konkurranseutsatt marked betyr ofte at sikkerhet overses. Samtidig ser man en rask utvikling av nye og effektive *angrepsverktøy* i den kriminelle verden. Det finnes et stort marked for gode angrepsverktøy som er enkle å bruke, noe som gjør datakriminalitet enkelt tilgjengelig for hvem som helst – man trenger altså ikke være hacker med spesialkompetanse for å lykkes med dataangrep. Til sammen bidrar dette til en sterk økning i antall trusler.

2 Sikkerhetsmål

Et sikkerhetsmål (sikkerhetsmålsetning) defineres som en egenskap man ønsker å tilby eller oppnå, for eksempel i et IT-system. Det er et overordnet begrep, og sier rett og slett noe om hvordan man ønsker at en tilstand skal være – altså målet. Det sier derimot ingenting om hvordan man

oppnår denne tilstanden; For å oppnå en ønsket tilstand vil man måtte iverksette *sikkerhetstiltak*. Sikkerhetsmål omtales ofte også som en *sikkerhetstjeneste* (Security service).

2.1 Etablerte standarder for informasjonssikkerhet

Gjennom tidene er det utviklet ulike standarder for informasjonssikkerhet, blant annet ISO 27000-serien fra International Organization for Standardization. Denne standarden definerer en rekke begreper for å sikre en felles grunnleggende forståelse. De opprinnelige og grunnleggende målene som er definert i standarden er:

- Konfidensialitet (Confidentiality)
- Integritet (Integrity)
- Tilgjengelighet (Availability)

Disse tre omtales ofte med fellesbetegnelsen KIT (eller CIA på engelsk). I nyere revisjoner av standardene er flere egenskaper omtalt, inkludert **autentisitet**, **uavviselighet** og **sporbarhet**. Et annet viktig tema som er aktualisert, spesielt etter at EU i 2018 innførte et felles lovverk for beskyttelse av personopplysninger (GDPR) som også gjelder i Norge, er **personopplysningsvern**.

2.2 Grunnleggende sikkerhetsmål (KIT/CIA)

Konfidensialitet: Handler om å begrense tilgang til informasjon til kun de som skal ha tilgang. Målet er å hindre at uvedkommende får informasjon i hende, enten det dreier seg om å beskytte hemmelige bedriftsdata, personlige data eller å sørge for anonymitet.

Integritet: Handler om å sikre at informasjon bevares i sin helhet, alltid er korrekt og ikke endres eller slettes uten at det er tiltenkt. Dette betyr at data ikke kan manipuleres uoppdaget.

Tilgjengelighet: Handler om å sikre at informasjon er tilgjengelig når den skal være tilgjengelig. Dette innebærer at hvis en person skal ha tilgang til en viss type informasjon i eller fra et IT-system, må også IT-systemet være tilgjengelig for personen akkurat når vedkommende har behov for den aktuelle informasjonen.

For alle disse tre målene kan det defineres ulike nivåer av viktighet, og det er svært ofte nødvendig å gjøre prioriteringer dem i mellom.

2.3 Andre sikkerhetsmål

Autentisitet: Handler om ekteheten til identiteter – hvorvidt noe eller noen er det eller den de utgir seg for å være. Dette er en generell utfordring, men kan være spesielt utfordrende i en digital omgivelse hvor man ikke ser hverandre fysisk eller har håndfaste dokumenter å forholde seg til. Man ønsker gjerne å vite om en bruker er autentisk, om et system eller en organisasjon er autentisk, eller at opprinnelsen til en melding er autentisk (altså at den har autentisk opphav). Evnen til å vite noe sikkert om autentisitet i og for datasystemer er helt essensielt i digital samhandling.

Uavviselighet (Non-repudiation): Sikkerhetsmålet innebærer at det ikke skal være mulig å benekte eller avvise en handling som er utført, eller å påstå at man har utført en handling som ikke er utført. I en digital setting dreier dette seg om sending eller mottak av data/meldinger, og kravet gjelder ikke bare mellom sendere og mottakere, men også overfor en tredjepart. Et eksempel kan være en digital kontrakt for et byggeoppdrag, hvor det er viktig at oppdragsgiveren ikke kan nekte for å ha signert kontrakten, og at det ikke er mulig å forfalske den – slik at alle parter, også en tredjepart, vet at beløpet ikke kan være endret etter signering. *Digitale signaturer* gir en slik løsning.

Sporbarhet: Er muligheten til å knytte en gitt identitet til en gitt hendelse, rett og slett "hvem gjorde hva når". Dette er interessant for å etterforske hendelser, for eksempel hvis en eksamenskarakter for en student i et studentsystem plutselig er endret fra ståkarakter til strykkarakter. For å ivareta sporbarhet må man kjenne alle identiteter som kan utføre handlinger i datasystemet, loggføre alle hendelsene (med hva, hvem og tidspunkt), og ha mulighet til å analysere disse loggene (drive etterforskning). I store systemer kan slike logger bli enorme, og det kan være nødvendig med egne IT-verktøy for å spore hendelser. Imidlertid vil de som utfører datainnbrudd ofte forsøke å fjerne alle spor etter seg, noe som vil gjøre etterforskning vanskelig.

2.4 Personopplysningsvern

Vern av personopplysninger er regulert i norsk lov (personvernforordningen/GDPR), som stiller krav til hvordan det vi kaller behandling av personopplysninger utøves. Dette omfatter all håndtering av personopplysninger og gjelder alle som kan tenkes å håndtere slike opplysninger, både privatpersoner, organisasjoner og selskaper. Lovverket stiller blant annet krav til:

- Lovlig registrering, lagring og varighet på lagring.
- Den registrertes mulighet til innsyn i opplysninger om seg selv, og mulighet til å få slettet opplysninger om seg selv.
- At behandlingen foregår på en slik måte at personopplysninger for eksempel ikke kommer på avveie.
- Forebygging av uautorisert innsamling og at innsamlede data om den registrerte ikke benyttes til andre formål enn det man har hjemmel til eller den registrerte har samtykket til.

Personvern er avhengig av informasjonssikkerhet, fordi det må sørges for beskyttelse av lagring og behandling av personopplysninger mot hendelser som fører til brudd på lovverk. Nødvendige sikkerhetstiltak må for eksempel være på plass for å sikre konfidensialitet. Brudd på personvernforordningen fører til utstedelse av *gebyrer* til virksomheter som bryter lovverket.

En personopplysning er en opplysning som kan knyttes til deg som enkeltindivid og som gir mulighet til å identifisere deg. Loven skiller mellom:

Alminnelige personopplysninger: Typisk navn, brukernavn, telefonnummer. En IP-adresse kan også bli en personopplysning når datamaskinen den identifiserer entydig kan knyttes til en bruker på et gitt tidspunkt, og denne brukeren igjen kan knyttes til en fysisk person.

Særlige kategorier personopplysninger (sensitive personopplysninger): Opplysninger loven sier det er ekstra viktig å beskytte, og som man dermed stiller enda større krav til lovlighet for behandling av. Eksempler er helseopplysninger, politisk overbevisning og religiøs overbevisning.

Fødselsnummer er ikke definert som en sensitiv personopplysaning, men lovverket stiller ekstra krav til behandling av fødselsnummer: Fødseslnummer kan kun behandles når det er et saklig behov for sikker identifisering av en person, der fødselsnummeret er nødvendig for å oppnå slik identifisering. Det skal altså tungtveiende grunner til å bruke fødselsnummer i en behandling.

3 Sikkerhetstiltak

Et sikkerhetstiltak er et tiltak som iverksettes/gjøres for å oppnå ett eller flere sikkerhetsmål. Det forteller altså hvordan vi skal oppnå sikkerhet, og er basert på en helt spesifikk, konkret implementering. Sikkerhetstiltak omtales også som sikkerhetsmekanismer. Sikkerhetstiltak kan brukes for å::

- Forebygge hendelser (f.eks. ved å låse en dør for å hindre tyveri).
- Oppdage hendelser når de skjer (f.eks. en alarm).
- Gjenopprette status quoetter at en hendelse har skjedd (f.eks. ved å rydde opp etter et innbrudd).

For å hindre uvedkommende i å lese filer og innhold på din personlige datamaskin, er det å kreve et brukernavn og passord for å logge inn på maskinen et vanlig forebyggende tiltak for å hindre andre i å bruke maskinen – man må *autentisere* seg for å få tilgang. Det er verdt å merke seg at å iverksette ett enkelt tiltak alene sjelden vil gi god (nok) sikkerhet.

3.1 Kategorier av sikkerhetstiltak

Sikkerhetstiltak kan deles inn i kategorier basert på type tiltak og hvor ansvaret bør plasseres i en virksomhet.

Fysiske tiltak: Handler om å sørge for at uvedkommende ikke slipper inn i en bygning, ha låste dører, eller at alle må vise legitimasjon for å slippe inn. Dette er også viktig for IT-systemer, for eksempel å sikre at ingen fysisk tar seg inn til en lokasjon der viktige datamaskiner står for enten å ødelegge, skru av eller stjele dem.

Teknologiske/Tekniske tiltak: Tiltak som gjøres i eller for IT-systemer og med datateknologi. Eksempler på slike sikkerhetstiltak er backup (sikkerhetskopiering), og å sørge for sikkerhetsoppdateringer av programmer eller operativsystem. Dette er typisk et ansvarsområde for ansatte med dypere IT-kompetanse.

Administrative tiltak: Et ansvarsområde som involverer både ledelsen i en virksomhet og IT-kompetanse. Eksempler er opplæring av ansatte i informasjonssikkerhet, ha gode prosedyrer og retningslinjer for hvordan man jobber, og ikke minst rutiner for gjenoppretting etter potensielle hendelser.

3.2 Sikring av data i ulike tilstander

Data som behandles i IT-systemer vil som regel kunne beinne seg i ulike *tilstander*, som hver krever ulike sikkerhetstiltak:

- Lagret på disk: Data må lagres trygt slik at ingen uvedkommende får tilgang.
- Overført i nettverk: Det må gjøres tiltak for å hindre avlytting eller manipulering av data når de overføres.

- I bruk i et system: Datamaskinen og nettleseren må sikres på en slik måte at uvedkommende heller ikke her kan avlytte eller manipulere informasjon.

Dette må man ta alltid høyde for når man jobber med informasjonssikring.

3.3 Planlegg for sikkerhetshendelser

Man er nødt til å jobbe bredt med informasjonssikring og ta høyde for at angrep både kan skje og være vellykket, sett fra en angripers synsvinkel. Man er selvfølgelig nødt til å legge innsats i *forebyggende* tiltak for å jobbe forebyggende for å i størst mulig grad hindre angrep. Siden det uheldigvis viser seg vanskelig å forebygge absolutt alle angrep (det vil alltid finnes en *sårbarhet* man ikke er klar over), er det også nødvendig med *detekterende* tiltak. Slike vil bidra med å kunne varsle angrep som er i gang eller som allerede har skjedd. Et uoppdaget angrep er en IT-systemeiers verste mareritt.

Enkelte ganger kan man rammes av hendelser/dataangrep som påvirker et IT-system negativt slik at det blir ikke-fungerende. I slike tilfeller er det helt essensielt at man har gjort tiltak for å kunne gjenopprette raskt, slik at systemene raskt tilgjengeliggjøres og tap minimeres. Man sier gjerne at det alltid bør *planlegges for katastrofe*.

3.4 Lag på lag med sikkerhet

For å oppnå best mulig beskyttelse mot angrep er det viktig å planlegge for flest mulig ulike scenarier. Sikkerhet må implementeres i mange lag eller nivåer. Hvis inntrengere klarer å lure seg forbi ett nivå, vil man foretrekke at angrepet stoppes eller håndteres i det neste. Sikkerhet er aldri sikrere enn det svakeste punktet i kjeden. For å oppnå tilstrekkelig sikkerhet i et datasystem, må sikkerhet ivaretas på absolutt alle nivåer i systemet. Dette krever en helhetlig tilnærming. Jo mer kritisk et system er, jo viktigere er selvfølgelig denne ivaretakelsen.

Eksempler på lagvise tiltak inkluderer:

- Fysisk sikring: Hindre uvedkommende fysisk tilgang, ta høyde for oversvømmelse, flom, strømbrudd og så videre.
- Sikker lagring: Passe på at informasjon oppbevares på en trygg måte, hindre uvedkommende tilgang.
- Sikre datamaskiner og systemer mot inntrengere: Sørge for at de til enhver tid har de siste sikkerhetsoppdateringene, slik at de ikke er et enkelt bytte for potensielle trusselaktører.
- Sikre nettverk internt (mot avlytting og manipulering) og sikker datakommunikasjon mot omverdenen.
- God opplæring av brukere slik at disse ikke gjør feil.
- Gode arbeidsrutiner slik at for eksempel sikkerhetsarbeid har godt nok fokus.
- En tydelig plan for hvordan gjenopprette systemene hvis eller når en hendelse inntreffer.

Denne listen er på ingen måte uttømmende, men gir en god pekepinn. Sammenhengen mellom sikkerhetsmål og sikkerhetstiltak er selve kjernen i informasjonssikkerhet, hvor nesten all innsats utføres med den hensikt å ivareta ett eller flere sikkerhetsmål