SIKKERHET

BEGREPER/FORKLARINGER

Sikkerhet: Tilstand: fravær av uønskede hendelser eller frihet fra fare og frykt

Verdi: alt som er verdifullt

Entitet: noe som har fysisk, juridisk eller prosessuell eksistens. Entiteter kan gis en identitet, noe som gjør det mulig å referere til entiteten

Identitet: et sett med attributter som er tilordnet entiteten, eks. fødselsnummer, passnummer etc.

Digital identitet: Den digitale representasjonen av de attributtene som er identiteten

Identitetshåndtering: prosessen med å registrere og autentisere identiteter

Skadelige hendelser (tilsiktet eller utilsiktet): naturkatastrofer, krig, ulykker, skade, påført med hensikt osv.

Informasjonssikkerhet: sikre informasjon, beskytte informasjonsressurser (IT-utstyr, infrastruktur, datafiler, programvare etc.). En kontinuerlig prosess for å oppdage og hindre trusler og å fjerne sårbarheter

Cybersikkerhet: sikre ting som er sårbare via IKT (f.eks. informasjon, selvkjørende biler, pacemaker osv.)

Personvern: handler om retten til et privatliv og retten til å bestemme over egne personopplysninger

Innebygget personvern: å ta hensyn til personvern i alle utviklingsfaser av et system eller en løsning, setter en standard for hva som skal ligge til grunn for et system eller et program

Sikkerhetsmål: uavhengig av spesifikk implementering og kan ivaretas med ulike sikkerhetstiltak

Sikkerhetstiltak: tiltak for å oppdage, forebygge eller gjenopprette, basert på spesifikk implementering, ofte bundet til produkter

DoS-angrep (Denial of Service): hindrer tilgangen til noe som skal has tilgang til

Sikkerhetsstyring: systematiske aktiviteter for å oppnå og opprettholde et sikkerhetsnivå i overensstemmelse med de mål og krav en organisasjon har satt seg

Risiko: risiko = sannsynlighet for angrep * kostnad eller tap i kroner

Trussel: uønsket hendelse som kan inntreffe

Angrep: noen forårsaker med hensikt en uønsket hendelse

Man in the Middle-angrep: ondsinnet aktør avlytter, endrer eller avbryter kommunikasjonen mellom to parter uten at disse er klar over det. Angriperen «sitter» mellom senderen og

mottakeren og kan avlytte, stjele informasjon eller manipulere data som overføres. Eks. aktiv avlytting

Navnetjener: en tjenermaskin på internett som oversetter lesbare internettadresser til numeriske IP-adresser

Autentisering: mekanismen for å bekrefte en hevdet identitet

Brukerautentisering: «bevismateriale» for at du faktisk er deg. Tre hovedkategorier av bevismateriale: noe du VET, noe du HAR, noe du ER (eksempler under autentisering)

Beskytte verdier: HVA som utgjør en trussel vil variere – det er situasjonsbetinget. HVILKE trusler det er nødvendig å forholde seg til er også situasjonsbetinget

Kryptografi: å gjøre ting uleselig

Plaintext/klartekst: den åpne beskjeden

Ciphertext/kryptert tekst: den krypterte teksten

Sikkerhetskopiering: sikkerhetstiltak hvor man kan gjenopprette data ved uønsket hendelse som sletter/endrer data. Husk: også sikkerhetskopien må sikres

Digital sårbarhet: en feil i et IKT-system som kan utnyttes

Skadevare: samlebetegnelse på programvare som har som mål å gjøre skade

Angrepsvektor: metoden en angriper bruker for å utføre et angrep på en datamaskin, et nettverk eller et datasystem

Cross Site Scripting (XSS): en type sikkerhetssårbarhet som finnes i webapplikasjoner. Når en angriper klarer å injisere ondsinnet skript i innholdet som sendes til en annen bruker via en webapplikasjon: fører til f.eks. tyveri av sensitive data, kapring av brukeraktører, distribusjon av malware

Brute-force-angrep: metode for å finne passord, kryptografiske nøkler eller andre hemmeligheter gjennom systematisk prøving og feiling. Angriper prøver alle mulige kombinasjoner av bokstaver, tall og spesialtegn inntil riktig kombinasjon er funnet

Sensitive data: helsedata, data om etnisitet og rase, politiske meninger, religiøse eller filosofiske standpunkt, fagforeningsmedlemskap etc.

Virtuelle maskiner: programvarebaserte emuleringer av fysiske datamaskiner. En fysisk virtuell maskin kan kjøre sitt eget operativsystem og applikasjoner akkurat som en fysisk datamaskin. Muliggjør å kjøre flere uavhengige databehandlingsmiljøer samtidig på én fysisk maskinvare

Redundante systemer: man har skyggesystemer, reservesystemer, som gjør akkurat det samme som hovedsystemet, som kan settes inn om hovedsystemet av en eller annen grunn er nede

Skallforsvar: samlebetegnelse for alle typer beskyttelse av datamateriale

Phishing: angrep der det blir gjort forsøk på å stjele penger fra deg eller identiteten din ved å få deg til å avsløre personlige opplysninger

Buffer Overflow: en sammenhengende seksjon i minnet i datamaskinen, allokert til å inneholde alt fra en streng til en array med heltall, kalles en buffer. En sårbarhet i et program som gjør at programmet overskrider bufferets grenser i minnet kalles buffer overflow

SQL-injection: spørrespråk mot relasjonsdatabaser: brukes ofte i vak-kant av web-applikasjoner for lagring av data. SQL-injection: når det lures inn spørresetninger sammen med informasjon som input i et grensesnitt. Input fra bruker valideres ikke før den sendes videre som spørresetning til databasen

KIT (CIA – confidentiality, integrity, availability)

Konfidensialitet: sikre at kun de med rettmessige behov har tilgang på en ressurs. **Tiltak**: kryptering, tilgangskontroll, perimetersikring, gode policy for hvordan data skal håndteres og hvordan kommunikasjon skal foregå. **Trussel**: tyveri, lekkasje

Integritet: sikre at en ressurs ikke endres eller slettes utilsiktet, ingen har tuklet med dataene. **Tiltak**: tilgangskontroll, endringskontroll, kryptografisk sjekksumalgoritme, perimetersikring (f.eks. brannmur) og digital signering også av programvare (code signing). **Trussel**: korrupsjon av data og systemer

Tilgjengelighet: dataressurser skal være tilgjengelige når den som skal ha tilgang trenger de. **Tiltak**: sikkerhetskopier, redundante tjenester, gode rutinger for hendelseshåndtering og gjenoppretting. **Trussel**: (D)DoS-angrep, systemfeil (også en trussel, forekommer nok oftere enn (D)DoS-angrep)

Autentisering: skape tillit til ektheten av en oppgitt identitet, hvordan muliggjøre tillit til at identiteter (entiteter) er autentiske, **identifikasjon** – hvem du er, **autentifikasjon** – legitimere at du er den du sier du er

- Kan skje gjennom noe du **HAR** (eks. kodebrikke, bank-id), noe du **VET** (eks. passord, pin-kode), eller noe du **ER** (eks. biometri – fingeravtrykk, ansiktsgjenkjenning)
- Kryptografiske autentiseringsprotokoller (eks. systemsertifikater som verifiseres av en tredjepart) som TLS, VPN og IPSec (BankID)
- Kryptografiske mekanismer: PKI, digital signatur, elektronisk signatur

Uavviselighet: sikre at mottaker eller avsender ikke kan bestride å ha sendt eller mottatt en melding, bevis for at melding er mottatt. **Tiltak**: digitale signaturer

Sporbarhet: sikre at en gitt hendelse kan spores til en gitt identitet. **Tiltak**: logging av alle hendelser, identifisere alle identiteter, perimeterforsvar (ikke gi uvedkommende tilgang)

Sikkerhetstiltak

Man må veie sikkerhetstiltak opp mot brukervennligheten og finne en balanse.

Sikkerhetstiltak i ulike faser:

- **Preventive (forebyggende) tiltak**: eks. kryptering

- **Detekterende tiltak**: varsle angrep som kan forsøkes eller har skjedd. Eks. inntregningsdeteksjon (IDS)
- **Korrigerende tiltak**: gjenopprette skade på dataressurser etter angrep. Eks. hente sikkerhetskopi av programmer og data

Ulike typer:

- Opplæring
- Kryptering (asymmetrisk, symmetrisk, sjekksum, kryptering av trafikk) – sikre trygg lagring av data i utrygge lagringsenheter, sikre trygg overføring av data i f.eks. åpne nett
- Perimeterforsvar
- Tilgangskontroll
- Sikkerhetsoppdatering
- Sikkerhetskopiering
- Gjenoppretting
- Redundans av tjenester

Sikkerhetstiltak i ulike datatilstander: Lagring, overføring, bruk

Skadevare (ulike typer)

- **Virus**: spres gjennom åpning av fil av bruker eller systemet
- **Ormer**: sprer seg og finner nye ofre på egenhånd
- **Trojaner**: skadevare som utgir seg for å være et nyttig program
- **Bakdør**: en ubeskyttet og ukjent åpning inn i et system
- **Spionvare**: programvare for å spionere på en bruker for å få tak i nyttig info
- **Logisk bombe**: skadevare som kjøres ved et gitt tidspunkt eller ved en gitt handling eller hendelse
- **Tastelogger / keylogger**: (en variant av spionvare) enhet/programvare som er koblet til tastaturer eller maskin som lagrer alle tastetrykk
- **Rootkit**: skadevare som endrer funksjoner i OS eller applikasjoner, kan ta kontroll over maskin/system

Hackere: er stort sett ute etter tilgang til informasjon, endre/forfalske informasjon eller å tilgjengeliggjøre informasjon. **Ønsker**: å utnytte sårbarheter i programvare, få noen til å gi de det de vil ha eller ID-tyveri

Trussel-aktører: er de som truer noens systemer/data. Det er viktig å vite HVEM trussel-aktørene er i forhold til hvilke verdier som skal beskyttes. En trussel-aktør kan være en nasjonalstat, kriminelle, aktivister eller virksomheter/selskaper.

Kryptering / kryptografi

Kryptering/kryptografi sikrer konfidensialitet. Det handler om å gjøre ting uleselig. **Strategier**: filkryptering, kryptering av filsystem, fulldiskkryptering

Hvorfor? For å beskytte fortrolige data -> lagring på skytjenester, maskinen etc. For å gi autentisitet til systemer -> hvordan vet vi at noe er autentisk?

Kryptering i forskjellige lag:

- **Applikasjon**: Secure Sockets Layer (https): kryptering fra ende-til-ende (nettbank, nettbutikker etc.)
- **IP/Internett**: kryptering i nettverkslaget, VPN
- **Linklag**: WPA – WiFi Protected Access

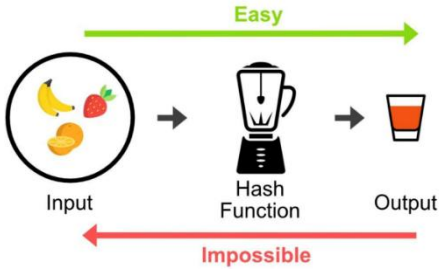
Kryptering på flere lag gjør det vanskeligere for uvedkomne å lytte til kommunikasjonen

Hemmelige koder:

- **Cæsarschiffer**: skifte bokstaver 3 ganger fremover (DOZEN -> GRCHQ)
- **Dekoderringer**: substituerer bokstaven n bokstaver videre (hvis n er 1 blir HAL -> IBM)
- **Monoalfabetisk chiffer**: tilfeldig mapping

Sjekksumalgoritmer (hash-funksjoner) – kryptografiske enveisfunksjoner

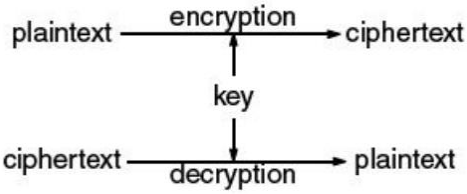
- Enveis identifikasjon, trenger ingen nøkkel
- Brukes for å sjekke dataintegritet, og er ikke-reverserbar
- Den skal gjøre det enkelt å regne ut og enkelt å finne ut om en beskjed er ekte eller ikke, men det skal være umulig å gå motsatt vei
- Man bruker tilfeldige tall for å generere deler av hash-funksjoner
- Sjekksum: at man kjører en data gjennom en algoritme hvor man får en tekststreng som svar



Kriterier for en god sjekksumalgoritme: Enkelt å regne ut sjekksum for en gitt beskjed. Ikke mulig å - finne en beskjed for en gitt sjekksum, endre en beskjed uten at sjekksummen blir endret eller finne to forskjellige beskjeder med samme sjekksum. **Anvendelse**: sammenligning av filer (sjekk av integritet), beskyttelse av passord

Symmetrisk kryptering

Består av en nøkkel som både avsender og mottaker må kjenne til. Plaintexten blir kryptert med nøkkelen og blir til ciphertext. Brukes for kryptering av data, kryptering av meldinger.



Hvilke sikkerhetsmål kan ivaretas med symmetrisk kryptering?

Konfidensialitet, integritet (i praksis), autentisitet til dataopprinnelse og mottagers autentisitet (men ikke autentisitet som en helhet).

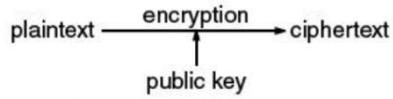
Farer med symmetrisk kryptering

Hvordan kan man dele den hemmelige nøkkelen trygt? Hva skjer om nøkkelen blir tapt? Hva skjer om nøkkelen havner på avveie?

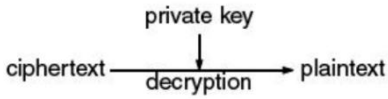
DES (Data Encryption Standard): er en symmetrisk krypteringsalgoritme. Viktig tidlig krypteringsstandard: er nå betraktet som usikker pga. korte nøkkellengder og effektiviteten av moderne angrepsteknikker som brute-force

AES (Advanced Encryption Standard): er en symmetrisk krypteringsalgoritme som ble utviklet som et svar på svakhetene i DES. Krypterer og dekrypterer data i blokker på 128 biter, tar hensyn til både sikkerhet og effektivitet. Mest brukte krypteringsstandarden i dag

Asymmetrisk kryptering

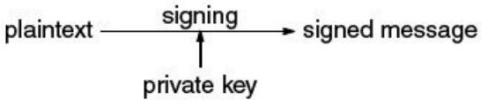


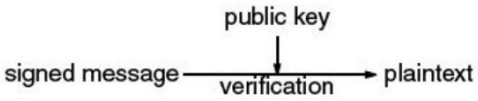
En offentlig og en privat nøkkel, hvor meldingen krypteres med den offentlige nøkkelen, men kun den private nøkkelen kan dekryptere dataen.



Digital signatur

Signatur kan KUN bli generert av eier eller noen som kjenner den private nøkkelen. Signatur kan bli VERIFISERT av alle som har tilgang til den offentlige nøkkelen. En korrekt verifisert signatur bekrefter avsenders identitet, og at meldingen ikke ble endret fra sending til mottak.





Asymetrisk kryptering for digital signering

Fremgangsmåte: sender krypterer (og dermed signerer) en melding med sin private nøkkel. Mottaker dekrypterer (og dermed validerer og verifiserer) meldingen med senders offentlige nøkkel. **Andvendelse**: ivareta tillit til at meldinger kommer fra en hevdet avsender, autentisering

Hvilke sikkerhetsmål kan ivaretas? Integritet (i praksis), autentisering av dataopprinnelse og uavviselighet

Farer: nøkler kan komme på avveie, falske nøkler

Hybrid modell (både asymmetrisk og symmetrisk kryptering): Asymmetrisk kryptering brukes KUN for å bli enige om en midlertidig nøkkel. Symmetrisk kryptering brukes under resten av kommunikasjonen

Offentlig-nøkkel sertifikat

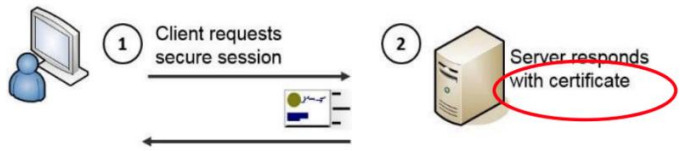
- Hvordan stole på at en offentlig nøkkel er ekte?: en identitet og tilhørende nøkkel knyttes sammen i et offentlig nøkkelsertifikat
- Hvordan stole på at sertifikatet er ekte?: sertifikatet utstedes av en betrodd virksomhet (sertifikatmyndighet – CA), som går god for at nøklene er autentiske, altså tilhører identiteten den utgir seg for å tilhøre
- Består av den offentlige nøkkelen, samt en rekke attributter knyttet til nøkkelen: eier, gyldighetsperiode, utsteder, hvilken kryptoalgoritme som er brukt, nøkkelstørrelse etc.
- Attributtene pakkes sammen og signeres av sertifikatutstederen -> vi får et offentlig-nøkkel sertifikat
- Det finnes standarder for hva et sertifikat skal inneholde

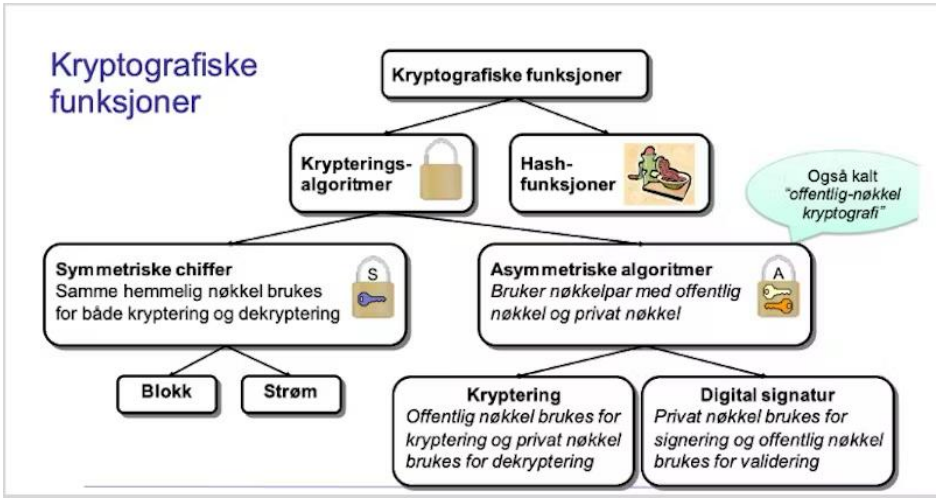
Hvordan distribuere offentlige nøkler?

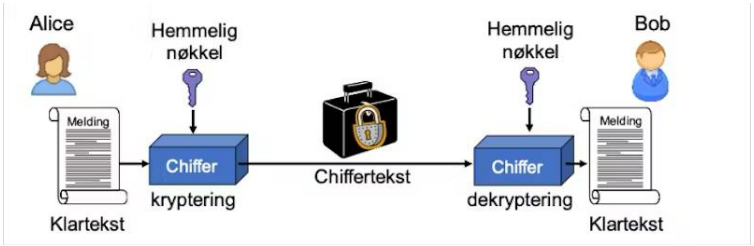
- Utarbeide en «offentlig-nøkkel infrastruktur» (PKI)
- Rammeverk for hvordan man skal utstede, administrere og bruke digitale sertifikater med offentlige nøkler hovedformål: sikre ektheten av offentlige nøkler, samt trygg og forsvarlig distribusjon

PKI (Public Key Infrastructure)

- Sikrer autentiske offentlige nøkler: binder en offentlig nøkkel til en navngitt enhet, og bindingen kan bekreftes av en betrodd «myndighet» som utsteder et sertifikat: et sertifikat forteller følgende: «offentlig nøkkel K eier av X»
- Rammeverk for kryptering/autentisering og signering av dokumenter og programvare
- Hensikt: knytte sammen en offentlig nøkkel og et individ
- Må bestå av: en policy for sertifikat-håndtering, teknologi for å implementere policyen, prosedyrer for hvordan håndtere og forvalte nøklene, tillitsmodell for sertifikatene med offentlige nøkler
- Grunnlag for forskjellige tjenester for elektronisk ID: MnID, BankID, Buypass, Commfide
- Sikrer sikker kommunikasjon i helsevesenet: eResept, elektronisk sykemelding etc.
- Internett-PKI







Nettverkssikkerhet

Tradisjonell sikkerhetsmodell: stoler på endesystemet, nettverket er det som er upålitelig om noe skjer

Tradisjonelle trusler: avlytting (passivt), forfalskning (aktivt), modifisering av data (aktivt)

To hovedområder: kommunikasjonssikkerhet og perimeterforsvar

Kommunikasjonssikkerhet: skal beskytte data i transportlaget og er basert på PKI. IP-security står for sikkerhet i nettverkslaget som baserer seg på kryptering, autentisering og nøkkelhåndtering

Perimeterforsvar: sikkerhet ved hjelp av brannmur og innbruddsdeteksjon.

- **Brannmur** – førstelinjeforsvar avgjør hva som slippes inn og ut fra et lokalt nettverk. Fungerer som en slags tilgangskontroll i nettverket og avverger uautorisert tilgang til/fra et privat nettverk. Implementeres i programvare eller maskinvare.
- **Innbruddsdeteksjon (IDS)**: system som detekterer mistenkelig aktivitet gjennom nettverksanalyse. Systemet kan detektere misbruk, skadevare og (D)DoS-angrep.

Sikkerhetstrusler: skadevare. Sårbarheter knyttet til: social manipulering, nettverkssikkerhet, applikasjonsikkerhet, sikkerhet i datamaskinen, lagring og anvending av informasjon, bruk av skytjenester.

Personvernloven: GDPR er en stor innstramming i personvernsregelverket i hele EU/EØS og andre land som opererer innenfor EU/EØS

DNS-sikkerhet:

- DNS-forfalskning: uvedkommende introduserer uriktige opplysninger i navnetjener
- DNS-modifisering: Man in the middle-angrep, forfalsker meldinger
- DNS-kapring: endre hvilke navnetjener offerets maskin benytter (hacke maskin)

Tilgangskontroll

- Et subjekt vil utføre handling på et objekt, f.eks. endre et dokument
- Tilgangskontroll = autentisering * autorisasjon
- Autorisasjon = sjekke at subjektet har tilgang til å utføre den ønskede handlingen på objektet etter forhåndsdefinerte regler
- **Tilgangskontroll på flere nivåer**:
    - Brukere og passord kan kontrolleres i applikasjonslaget
    - Tilgang til ulike nettverksporter kan kontrolleres i transportlaget
    - Tilgang basert på IP-adresser kan kontrolleres i nettverkslaget

Referansemonitor: oppgave – kontrollere tilgang fra subjekt til objekt, avviser eller tillater tilgang. Følger en policy som er satt og logger hendelser i en hendelseslogg.

Sikkerhet i operativsystemet: kjerner og drivere er dataprogrammer som kan inneholde sårbarheter. Kjernen har tilgang til alt (supervisor mode) og blir dermed en sårbarhet som er

svært kritisk. Det er viktig å holde operativsystem og drivere oppdatert for å unngå at sårbarheter skal utnyttes.

Lagring av data: data kategoriseres etter hvilket beskyttelsesbehov det har og hvilke tiltak som iverksettes avhenger av beskyttelsesbehovet. Tre ulike behov: åpen informasjon, informasjon med begrenset beskyttelsesbehov og informasjon med sterkt beskyttelsesbehov.

Applikasjonssikkerhet:

- Applikasjoner må designes og utvikles med tanke på å kunne brukes trygt
- I designfasen: trusselmodellering – hvilke trusler ser vi? Hvilke tiltak kan iverksettes for å motvirke truslene?
- I programmeringsfasen: unngå å skape/tilrettelegge for sårbarheter

Innebygget sikkerhet oppnås når informasjonssikkerhet er:

- Innarbeidet i virksomhetsstyringen og understøtter virksomhetens mål
- Innarbeidet i virksomhetens prosesser og prosjekter fra starten av
- Tatt hensyn til i hele livssyklusen til IKT-løsninger
- Et tema alle ansatte i offentlig sektor kjenner til og vet hva innebærer for sine arbeidsoppgaver

Skytjenesten (tjenesteutsetting)

- **Fordeler**: redusert infrastrukturkostnader, besparelser i form av betaling for faktisk bruk og lokasjonsuavhengig tilgang
- **Ulemper**: dersom en virksomhet ønsker å benytte skytjenester til behandling av personopplysninger, er virksomheten juridisk ansvarlig for at personopplysningene prosesseres og lagres i samsvar med personvernregelverket

Trussel modellering

Risiko = sannsynlighet for hendelse * konsekvensen knyttet til hendelsen

Flere innfallsvinkler:

- **Fokus på trusselaktør**: identifisere trusselaktørens mål, hvordan de går fram for å oppnå dem, hva er angrepsvektoren og angrepsflate
- **Fokus på system**: «plukke fra hverandre» systemet, identifisere de ulike delene og avdekke hvor og hvordan de kan angripes
- **Fokus på verdi**: identifisere verdiene i systemet, avdekke hvordan brudd på informasjonssikkerhet kan inntreffe

Risikoanalyse: Hvor skal innsatsen legges? Risikoanalyse er en systematisk prosess for å identifisere, vurdere og priorotere risikoer som kan påvirke mål, prosjekter, prosesser eller beslutninger. Målet med risikoanalyse er å forstå risikoer og deres potensielle konsekvenser, slik at organisasjonen kan implementere passende tiltak for å reduser eller håndtere disse risikoene.

Administrative sikkerhetstiltak:

Hvorfor går det galt?

- Sikkerhet nedprioriteres
- Komplekse systemer
- Evig kappløp om marked
- Fremdeles ikke full åpenhet om feil

Hvilke tiltak kan gjøres?

- Internkontroll
- Styringssystem
- Policyer/standarder
- Prosedyrer og praksis
- Bevissthetstrening/opplæring
- Sikkerhetsøvelser
- Rutiner for hendelseshåndtering

FORKORTELSER

WPA: FiFi Protected Access

TLS: Transport Layer Security

VPN: Virtual Private Network

DoS: Denial of Service

DES: Data Encrypted Standard

AES: Advanced Encryption Standard

DLP: Data Loss Prevention

RSA: «Rivest-Shamir-Adleman» - kryptosystem for offentlig nøkkel-kryptering (navngitt etter sine oppfinnere)

GDPR: General Data Protection Regulation

PKI: Public Key Infrastructure

CA: Certificate Authority

IDS: Instrusion Detection System

DNS: Domain Name System

MITM: Man in the middle

SQL: Structured Query Language (strukturert spørrespråk)

XSS: Cross Site Scripting

TSD: Tjenester for sensitive data (tilbys av UiO for å håndtere og lagre sensitiv og personvernbeskyttet data på en sikker måte)

VMs: Virtuelle maskiner (virtual machines)

PRØVEEKSAMEN

Brudd på sikkerhetsmål

- Forfalskning av nettside – brudd på autentisitet
- Løsepengevirus – brudd på tilgjenglighet
- Spionprogramvare – brudd på konfidensialitet
- DNS-modifisering – brudd på integritet
- DDoS-angrep – brudd på tilgjengelighet
- Identitetstyveri – brudd på autentisitet

Sikkerhetsmål og sikkerhetstiltak

Du er deltager i et IT-prosjekt som utvikler et nytt digitalt pasientsystem for en gruppe privatpraktiserende psykologer. Systemet vil inneholde pasientopplysninger. Oppgaven din er å rådgi prosjektledelsen om nødvendige sikkerhetstiltak for pasientsystemet.

a) Aller først skal du identifisere sikkerhetsmål utover KIT som skal ivaretas i pasientsystemet. Hvilke av følgende er sikkerhetmål som definert i IN1020: personvern og sporbarhet, innbruddsdeteksjon, autorisasjon og brannvern

b) Velg de sikkerhetstiltakene du vil anbefale for å sikre *konfidensialitet* for data som behandles i pasientsystemet:
- Opplæring av alle databehandlere
- Bruke sikre nettverksprotokoller for dataoverføring
- Krav om tofaktorautentisering for innlogging
- Kryptere alle data som lagres i systemet
- Benytte ulike angrepsvektorer
- Sørge for gode rutiner for sikkerhetskopiering av data
- Bruke sjekksumalgoritmer for data som overføres i nettverk
- Loggføre all aktivitet i pasientsystemet

c) Velg de sikkerhetstiltakene du vil anbefale for å sikre best mulig *tilgjengelighet* til data som behandles i pasientsystemet:
- Installere antivirus-programvare
- Sørge for gode rutiner for sikkerhetskopiering av data
- Gjennomføre sikkerhetsøvelser
- Følge opp varslinger om nye sårbarheter
- Benytte ulike angrepsvektorer
- Loggføre all aktivitet i pasientsystemet
- Kryptere alle data som lagres i systemet
- Bruke sikre nettverksprotokoller for dataoverføring

Begrepsforståelse

- **Nulldagssårbarhet** er en svakhet som ikke er kjent for leverandør av en tjeneste
- **Hash-algoritme** brukes for å sjekke dataintegritet
- **PKI** brukes for å sikre ektheten av offentlige nøkler, samt trygg nøkkel-distrubsjon
- **Trojaner** har både nyttig og en skadelig funksjon
- **Personopplysninger** har lovpålagte krav om konfidensialitet, integritet og/eller tilgjengelighet
- **Risiko** er en kombinasjon av sannsynlighet for en hendelse og konsekvens av hendelsen

Nettverkssikkerhet

*Under utvikling av et nytt nettsted for en virksomhet blir du rådspurt om det er mest fornuftig å benytte protokollen HTTP eller HTTPS for kommunikasjon over nettverk mellom bruker og virksomhetens nettsted. Hvilke av følgende utsagn er sanne hvis man velger **HTTP** som protokoll:*

- Uvedkommende vil være i stand til å modifisere datatrafikk mellom virksomhetens webtjener og en brukers nettleser
- Uvedkommende vil være i stand til å avlytte og lese datatrafikk mellom virksomhetens webtjener og en brukers nettleser
- Integritet for data sendt mellom virksomhetens webtjener og en brukers nettleser blir ivaretatt.
- Hvis en bruker benytter kryptert forbindelse mellom sin datamaskin og sin trådløse hjemme-ruter, hindres både avlytting og modifikasjon av datatrafikken mellom brukerens nettleser og virksomhetens webtjener.

Egenskaper ved ulik type kryptering *(ikke bekreftet)*

Symmetrisk:

- Sender og mottager deler en felles hemmelig nøkkel
- Raskere og mer effektiv enn den andre
- Kan sikre autentisk dataopprinnelse
- Trygg nøkkelutveksling er utfordrende

Asymmetrisk

- Kan bruke åpne kanaler for nøkkeldistribusjon
- Kan sikre autentisk dataopprinnelse
- Kan sikre uavviseligehet
- Benyttes for digital signering

Ingen av delene:

- Nyttig for å kryptere store mengder data
- Brukes for HTTPS alene
- Nøkkelfri kryptering
- Ødelegger data slik at den ikke kan dekrypteres

Digitale signaturer *(ikke bekreftet)*

Jonas ønsker å inngå en digitalt signert avtale (et dokument) med Trygve på en måte som gjør at det ikke er tvil om at avtalen er signert av ham, heller ikke ovenfor en 3. part som for eksempel pressen eller Stortinget.

Sikkerhetsmålet som ønskes oppnås ved å bruke av digital signatur som gitt over omtales som **uavviselighet**. For å signere avtalen må Jonas bruke **sin egen private nøkkel**. For å validere den digitale signaturen må Trygve bruke **Jonas sin offentlige nøkkel.**

Digital signering av et dokument vil ikke sikre konfidensialitet for innholdet

Digitale sertifikater:

- Knytter sammen en offentlig nøkkel og eiers identitet
- Hindrer falske nøkler og falske tjenester
- Knytter sammen en asymmetrisk og symmetrisk nøkkel
- Hindrer svindlere i å opprette et gyldig domene

Personopplysningsvern *(ikke bekreftet)*

Hvilket utsagn stemmer best med lovkrav til behandling av personopplysninger?

- Behandling av personopplysninger stiller krav om samtykke fra den registrerte for all behandling.
- Personopplysninger skal behandles lovlig, rettferdig og åpent, og med krav om riktighet, dataminimering og formålsbegrensning. Behandlingen skal skje med egnede tekniske og organisatoriske tiltak slik at konfidensialitet, integritet og tilgjengelighet ivaretas.
- Personopplysninger skal behandles lovlig, rettferdig og åpent, og med krav om riktighet, dataminimering og formålsbegrensning.
- Behandling av personopplysninger skal skje med egnede tekniske og organisatoriske tiltak slik at konfidensialitet, integritet og tilgjengelighet ivaretas.

Personopplysningsloven har størst **konsekvens** for **virksomheter**.