EKSAMEN TK2100

Oppgave 1

Vi kan definere informasjonssikkerhet ved hjelp av CIA-modellen.

Confidentiality (konfidensialitet), handler om å sikre informasjon, slik at informasjonen bare er tilgjengelige til godkjente personer.

Integrity (integritet), vil si at informasjonen skal være riktig og til å stole på. Dette sikrer at informasjonen ikke blir endret på.

Availability (Tilgjengelighet), det vil si at informasjonen bør være brukervennlig og tilgjengelig for bruk. Hensikten er å sikre at informasjonssystemer er tilgjengelige til enhver tid.

CIA-modellen er laget for å identifisere trusler og svakheter til informasjonssikkerhet.

Oppgave 2

Sosiale medier som Facebook, Twitter, Tiktok og Youtube samler enormt mye data og informasjon om deg. De samler inn personlig informasjon som navn, kjønn og bosted. De samler også inn data om hvor gammel du er, hva du er interessert i, hvilke type mobil du bruker og hva slags operativsystem du har. For å beskytte personvernet ditt og unngå at all denne informasjonen deles, kan det være lurt å gå gjennom personverninnstillingene i appene du bruker.

All denne informasjon blir analysert og solgt videre og delt med ulike selskaper, og brukes deretter til målrettet reklame. Dette kan negativt påvirker personvernet ditt, ettersom flere brukere ikke er så komfortable med at dataen blir brukt til å reklame som er målrettet.

I Europa har vi forskjellige reguleringer og lover som ivaretar personvernet til enkeltpersoner. Dette er for å sikre at personlig informasjon blir behandlet på en ansvarlig måte. I følge regjeringen.no fikk vi 2018 Den generelle databeskyttelsesforordningen (GDPR), den gjelder i hele EU og EØS-området. GDPR er etablert for å beskytte personvernet til enkeltpersoner, her er noen eksempler:

- **Samtykke**, brukere skal være tydelig informert om hva slags informasjon som blir samlet inn, hvem som har tilgang til den og hvordan informasjonen brukes

- **Rettigheter**, enkeltpersoner har ved forespørsel rett til å få all informasjonen slettet.

- **Sanksjoner**, myndighetene har mulighet til å pålegge bøter ved brudd på personvernreglene. Hvor stor boten blir avhenger av flere faktorer.

Oppgave 3

Rootkit er en form for skadelig programvare som har som mål å infiltrere datamaskinen uten at brukeren er klar over det. Rootkits utnytter sårbarhet i systemet og deretter manipulere systemet til å gi inntrengeren privileger, slik at de kan utføre skadelige handlinger uten at sikkerhetssystemene oppdager det. Det tas i bruk flere metoder for å distribuere rootkits, phishing er en av de mest populære metodene.

For å sikre at skadelig programvare ikke skal bli oppdaget, deaktiverer rootkits antivirus og anti-malware. Rootkits tar i bruk teknikker som f.eks. Manipulering av systemskall. Dette gjør det mulig for rootkits å skjule filer og endre brukerrettigheter. Et annet eksempel er hooking-teknikker, dette brukes til å erstatte eller endre funksjoner i operativsystemet.

Oppgave 4

Symmetrisk kryptering tar kun i bruk en nøkkel. Det vil si at man bruker den samme nøkkelen til å kryptere og dekryptere, noe som gjør symmetrisk kryptering veldig effektiv. Et eksempel på symmetrisk kryptering er AES (Advanced Encryption Standard). Dette er den desidert mest brukte krypteringsalgoritmen. AES fungerer ved å bruke en blokkchiffer-algoritme til å lagre informasjon. Dataen blir delt inn i blokker. Noe som er grunnen til at AES blir kalt for blokk-kryptering. Det er tre forskjellige nøkkellengder for AES: 128, 192 og 256 bits, 256 bits er den mest sikre, men tar også lengst tid å regne.

Asymmetrisk kryptering eller public key kryptering som det også kalles tar i bruk to nøkler, en public og en private. Public key blir brukt til kryptering av data, mens private key brukes til å dekyptere data. Grunnen til at vi har asymmetrisk kryptering er at vi slipper å dele samme nøkkel. Et eksempel på algoritmer på asymmetrisk kryptering er RSA (Rivest-Shamir-Adleman). Dette er den mest brukte asymmetriske krypteringsalgoritmen og baserer seg på matematikk, faktorisering av primtall.

Hvordan beskytte et dokument ved å kombinere asymmetrisk og symmetrisk kryptering:

- Bob lager en asymmetrisknøkkel, en public og en private key. Bob holder private key hemmelig, mens public key er tilgjengelig for Alice.
- Alice bruker public key til å til å kryptere en symmetrisk nøkkel og sender den til Bob.
- Bob dekryptere den krypterte symmetriske nøkkelen fra Alice og krypterer dokumentet, så sender Bob dokumentet til Alice.
- Deretter bruker Alice den symmetriske nøkkelen til å dekryptere dokumentet

Oppgave 5

XSS og CRSF er to forskjellige former for angrep og fungere på ulike måter:

Cross-site scipting (XSS):

- Brukerens nettleser stoler på en dårlig implementert nettside.
- Da er angriperen i stand til å injisere et skript på nettsiden, og som et resultat av dette kjører brukerens nettleser angriperens skript.

Cross-site request forgery (CRSF):

- Et dårlig implementert nettsted har tillit til brukeren
- Angriperen manipulerer brukerens nettleser for å sende uønskede forespørsler uten brukerens samtykke.
- Som et resultat utfører nettstedet uautoriserte og ondsinnede handlinger initiert av angriperen.

XSS og CRSF er begge et resultat av sikkerhetssvakheter på nettsider, spesielt dette med mangel på autentisering og validering av brukerdata er en betydelig sårbarhet.

Oppgave 6

På nettverkslaget TCP/IP modellen har vi flere utfordringer som kan påvirke funksjonen.Her er noen av dem:

DoS-angrep: Denial of service går ut på at man hindrer andre brukere fra å få tilgang til en tjeneste. Dette gjøres som oftest ved at man sender ekstremt store mengder trafikk (pakker), slik at tjenesten krasjer.

Spoofing: Dette er en metode hvor en person eller maskin sender TCP/IP data pakker med en falsk IP-adresse. Dette fører til at mottakeren feilaktig tror at den mottar data fra en troverdig kilde, men dette er ikke tilfelle. Spoofing blir ofte brukt til Man-in-the-Middle (MitM), angriperen bruker en flask IP-adresse til å plassere seg mellom to enheter/personer som kommunisere sammen. Dette fører til at angriperen kan hente ut sensitiv data som brukernavn og passord.

Oppgave 7

Et eierskap av et dataprogram i Norge kan beskyttes gjennom ulike tiltak. Her har du noen måter man kan beskytte seg på:

En mulig tilnærming for å sikre eksklusive rettigheter til et dataprogram er å søke om patentbeskyttelse. Når det gjelder dataprogrammer, er det visse krav som må oppfylles for å få patentbeskyttelse. Først og fremst må dataprogrammet være noe helt nytt og ha en tydelig teknisk karakter og effekt. I tillegg til å ha en teknisk karakter og effekt, må dataprogrammet også ha oppfinnelseshøyde, det vil si at det må skille seg vesentlig fra tidligere kjent teknologi.

Opphavsrett, er en annen måte å beskytte seg på. Siden dataprogrammer blir sett på som åndsverk, og opphavsretten gir skaperen automatisk beskyttelse av programmet. Her og er det visse krav om må oppfylles. Et av kravene er verkshøyde, dette innebærer at dataprogrammet er et originalt verk. Det må være skapt av et menneske og en konkret utforming kreves f.eks. kildekode.

Oppgave 8

Som en følge av at det kom hjemmekontor under pandemien, medførte dette en rekke utfordringer innenfor informasjonssikkerhet.

En av de mest betydelige utfordringene for bedrifter er håndteringen av hjemmenettverk. Sammenlignet med bedriftsnettverk er hjemmenettverket ekstremt sårbart. I et hjemmenettverk er det ofte slik at flere deler samme nettverk. Dersom en av enhetene til noen i familien blir infiltrert, kan føre til at andre enheter på det samme nettverket blir påvirket. Hjemmenettverk er vanligvis betydelig svakere enn bedriftsnettverk, da de ofte har veldig svake passord og manglende brannmur eller kryptering.

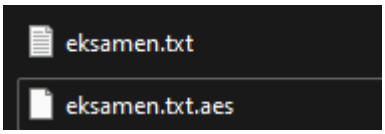
En annen utfordring knyttet til hjemmekontor er at ansatte låner bort datamaskiner til andre familiemedlemmer. Dette kan medføre en økt risiko for virus og malware. Den fysiske sikkerheten er betydelig svakere ved hjemmekontor. Enheter kan enkelt bli mistet eller stjålet, noe som utgjør en reell trussel mot konfidensialiteten og integriteten til bedriftens data. For å forbedre sikkerheten ved hjemmekontor, er det flere tiltak som kan iverksettes:

Regelmessig opplæring, det bør tilbys regelmessig opplæring til de ansatte om informasjonssikkerhet. Dette inkluderer opplæring om hvordan man identifiserer phishing-Eposter og bruk av passord.

Bruk av VPN, dette gir en sikker og kryptert forbindelse mellom den ansattes enhet og bedriftsnettverket. Dette beskytter dataoverføringen mot uautorisert tilgang og avlytting.

Oppgave 9

```
PS C:\Users\chris\desktop> openssl enc -aes-256-cbc -v -e -salt -in eksamen.txt -out eksamen.txt.aes
bufsize=8192
enter AES-256-CBC encryption password:
Verifying - enter AES-256-CBC encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
bytes read   :        6
bytes written:       32
```



Oppgave 10

```
PS C:\Users\chris> nmap -p- 172.20.51.85
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-08 14:15 Vest-Europa (sommertid)
Nmap scan report for 172.20.51.85
Host is up (0.00061s latency).
Not shown: 65519 closed tcp ports (reset)
PORT      STATE    SERVICE
135/tcp   open     msrpc
137/tcp   filtered netbios-ns
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
2869/tcp  open     icslap
3306/tcp  open     mysql
5040/tcp  open     unknown
7680/tcp  open     pando-pub
10801/tcp open     unknown
33060/tcp open     mysqlx
49664/tcp open     unknown
49665/tcp open     unknown
49666/tcp open     unknown
49667/tcp open     unknown
49699/tcp open     unknown
49720/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 7.03 seconds
PS C:\Users\chris>
```

Fremgangsmåte:

- Først skrev jeg inn ipconfig inn i cmd for å få IP-adressen
- Deretter skrev jeg inn nmap -p- «IP-adresse»

Dersom porten er åpen betyr det at det kjører en nettverkstjeneste på porten.

Kilder:

Kaspersky.no. "What is Rootkit?"Tilgjengelig på: https://www.kaspersky.no/resource-center/definitions/what-is-rootkit

GeeksforGeeks.org (2021). "Difference between XSS and CSRF." Tilgjengelig på: https://www.geeksforgeeks.org/difference-between-xss-and-csrf/

Regjeringen.no. (2018). Ny personopplysningslov. Tilgjengelig på: https://www.regjeringen.no/no/tema/statlig-forvaltning/personvern/ny-personopplysningslov/id2340094/

Østby, B. 2023, 'Oppsummering', forelesning holdt ved Høyskolen Kristiania, Oslo.