TK2100 INFORMASJONSSIKKERHET

OPPGAVE 1

Definer «informasjonssikkerhet». Ta utgangspunkt i CIA-modellen.

Sikkerheten i et system er i forhold til et trusselbilde. I forhold til C.I.A. er det Konfidensialitet, Integritet og Tilgjenglihet som gjeller. Konfidensialitet er å ungå at uautoriserte personer skal få tilgang på informasjonen, ved hjelp av forskjelige verjtør som kryptering, adgangskontroll, autentifisering, fysisk tingang, osv. Integritet er at inforamsjonen ikke har blitt endret på av en uautoriset måte, å en måte og sjekke dette er sjekksummer og backups. Tilgjenglihet er den siste ponkte i trekanten, det er at inforamsjonen skal være muig å endre innen rimelig tid av en autorisert person. Å det er disse punktene som er viktig i informasjonsikkerhet.

OPPGAVE 2

Drøft hva som er de største truslene mot din egen informasjonssikkerhet. Beskriv de viktigste tiltakene for å redusere risiko.

Det vanligste truselen for normale folk er repitisjon av et passord flere steder. Dette medfører vist en av de stedene blir komprimert, så blir alle stedene du har brukt det passordet, også mye lettere å komme seg inn på. Derfor er det lurt å bruke forskjelige passord på forskjelige steder, og ikke bare en annen tall i pasordet du hadde fra før av, for det kan man også bruke til å brute force passordet. Så anbefaler å lage nye passord på vært nytt sted. Ett nyttig vertgøy til å gjøre dette for deg er en «password manager», men da er det også ett passord smom besytter alle dine andre passord, så da må du være sikker på at det programet er sikker. Vist vi går et steg opp fra dette så er det 2 factor authentication som er det neste. Dette går ut fra at du har ett passord og en annen enhet som f.eks. en telefon der du får en SMS med en timet 6 sifferet pinkode som du må taste inn innen en periode. Dette er en annen måter å autorisere deg på for nettsiden. Det finnes også produkter som en USB-stick som autorisere deg når du prøver å logge inn. Det er også f.eks. touch id, eller finger avtrykk er det også andre applikasjoner som bruker som 2FA. En annen ting som folk ofte utsetter eller ikke gjør er og opptattere programvaren som de bruker på pc-en. Detter medfører at kjente angrepsmetoder ikke blir fikset fordi man ikke har

oppdatert. Dette har påvirket mange som f.eks. Spekter, meltdown, osv. som påvirket mange gamle og ikke oppdaterte pc-er, f.eks. sykehus sine pc-er, statlige og private bedrifter som kjører på gamle versjoner av programvarer.
Også en ting man må værer oppmerksom på er hvor mye informasjon man deler på nette, dette kan medføre at hackere kan bruke den informasjonen til å sende deg en melding som ser ut som f.eks. Telenor som trenger at du oppdaterer personopplysningene og sender en lenke til deg. Så du tenker ikke noe over det, og gjør akkurat det, og så plutselig har de alt de trenger for å få mer ut av det. Derfor er det viktig og dobbel sjekke hvor du får informasjon om sånt, sjekke at du fikk det fra riktig person/ firma, at man kanskje ikke bruker lenken som ble sendt i meldingen, men heller går inn på telenor.no selv og oppdater det der og ikke via den måten hackere ville at du skulle gjøre det. Dette gjeller også telefon samtaler og e-post.

OPPGAVE 3

3.1 Teoretisk oppgave

Forklar kort hva som skiller asymmetrisk (public key) kryptering fra symmetrisk kryptering. Forklar hva som er den vanligste block cipher krypteringsmetoden, og hva som er den vanligste asymmetriske krypteringsmetoden– og bruk disse i forklaringen.

Asymmetrisk krypterings metode er en måte der du har en nøkkel som krypterer filen og en annen nøkkel som dekrypterer den krypterte filen, sånn at ingen andre enn den som har dekrypteringsnøkkelen kan åpne denne filen. Så det er en nøkkel man har som er offentlig som krypterer filen, men kan ikke de kryptere filen. Så har man også en nøkkel som er privat som kan dekryptere filene fra den offentlige nøkkelen. AES er den vanligste block cipher krypteringsmetoden. AES har vært standeren i USAs statlige stander siden 2002. det bruker block størrelse på 128bits, og kan ta imot 3 mulige nøkkel størrelser (128, 192 og 256 bits) og jo større nøkkelen er jo sterkere er krypteringen.
Den mest brukte public key algoritme er RSA. RSA er basert på multiplikasjon av 2 store primtall, der den offentlige nøkkelen er summen av primtallene, men selve primtallene er hemmelige (privat nøkkelen).

OPPGAVE 4

I utgangspunktet sier man innen informasjonssikkerhet at en angriper som kan få fysisk tilgang til en maskin har full kontroll – og for eksempel bærbare maskiner kan være enkle mål. Forklar hvordan man kan beskytte en datamaskin på best mulig måte, ta utgangspunkt i en bærbar maskin som står på en kontorpult og lag sikkerhetsmodellen din rundt dette. Beskriv en løsning som omfatter både operativsystemsikkerhet, brukerpolicyer, og fysisk sikkerhet.

Vist vi starter med operativsystemsikkerhet så kan man implementere i BIOS passord og kryptering som hindrer deg i å komme inn til OS før man taster dette inn riktig, man kan også bruke BitLocker volume kryptering som krypterer hele harddisken med AES. Sette opp Patch Guard til å flytte på Windows kennelen som at ikke angrep skal kunne bruke den. Det er også viktig å installere et bra antivirus, men dette fjerner fortsatt ikke at brukeren må tenke selv hva han kjører selv. Vist vi ser på brukerpolicyer så er en at brukeren skal ikke ha samme konto som root/administratoren, dette hindrer folk til å kjøre ting i administrator uten at bruker vil dette også å ha et antivirus her og at alle programvarer er patchet er viktig, spesielt Windows. En viktig ting er at bruker skal låse pc-en når han går fra den, selv om det er bare i noen minutter. En annen ting er å stenge IO porter vist de ikke blir brukt som f.eks. ps2, ekstra USB. Og at man må godkjenne ekstra taratur og mus for å hinder at noen skal koble opp en rubber ducky. Den siste er det fysiske, der er mulig å bruke kensington Lock på PC-en til å låse fat i bordet eller vegen. Det finnes også USB keys som du må ha i pc-en får å kunne låse den opp. Viktig også å ikke la kontoret være ulåst og sette opp kamera til å overvåke gangene vist det er noe.

OPPGAVE 5

Forklar hvordan og hvorfor TCP/IP modellen resulterer i så store sikkerhetssvakheter, og hvilke praktiske problemer dette resulterer i. Herunder skal du forklare problemer med protokoller som HTTP og Telnet, du skal forklare om TCP hijacking, og du skal vise hvordan ARP poisioning og MAC flooding fungerer. Hvis du skal jobbe med å sikre nettverket hos et selskap, hva har dette å si for deg og din jobb?

TCP/IP modellen er svak av mange grunne, en er at det er ukryptert overføring. men en av de er fordi man kan lage en falsk avsender-adresse og gjøre et angrep som er kjent som DoS (denial-of-service) angrep. Da sender man mange pakker med Flaske avsender-adresser til en server med SYN flagget i hederen. Da åpner tjenesten en socket og svarer med SYN/ACK, men får ikke noe respons, så blir kapasiteten til

tjenesten brukt opp sånn normale folk som vil bruke denne tjenesten får ikke en socket å må vente veldig lenge for et svar fra serveren. En annen del av dette er at det er ukryptert Problemet med HTTP er at det ikke er sertifisert i forhold til HTTPS, som medfører noen problemer. Første er at nåen kan sette opp et angrep der det ser ut som en helt normal nettside, men er egentlig en annen nettside uten at du vet det. Det er også en annet problem og det er session hijacking. Som vil si at noen stjeler en cookie fra deg, og for serveren så er cookie-en eneste måten for å skille brukere fra hverandre. Så da gjør angriperen ting som ser ut som kommer fra din maskin. TCP hijacking funker som MITM angrep der man sitter mellom severen og klienten. Og man forfalsker at man er klienten for serveren og at man forfalsker at man er serveren for klienten. Dette medfører at du plukker opp alt imellom klienten og serveren. Men må gjøres under Three way handshaken. Og vil plukke opp http-coockies. ARP poisining er nå man sender umotiverte svar til noen for ARP cachen oppdateres ved hvert ARP-svar, selv man ikke jar sent forespørselen. MAC flooding fungerer på den måten at en switch har en MAC-tabell. Angriper sender mange data-link protokoller til switchen med forskjellige MAC-adresser sånn at al minne i tabellen blir brukt opp. Dette medfører at klienten som vil koble seg til får ikke tilgang. Sikre at vi bruker nyeste versjoner av protokoller og at man følger det nye retningslinjer.

OPPGAVE 6

Tenk deg at du skal angripe en stor norsk bank, formålet ditt er å enten stjele penger eller finne bedriftshemmeligheter du kan utnytte senere. Dette er en penetrasjonstest og det er selskapets CIO og CEO som har bedt deg utføre testen, og ingen andre er informert. Beskriv hvordan du ville gått frem for å komme deg inn i banken. Din begrensning er at du ikke har lov til å true ansatte på noen måte, og du har ikke lov til å oppsøke noen ansatte eller deres familier utenfor bankens lokaler – ellers skal du fullt ut bruke en kriminell sine metoder for å utføre angrepet. Beskriv din fremgangsmetode trinn for trinn, i så stor detalj som tiden tillater. Beskriv også eventuelle forutsetninger og antagelser du tar. (Obs; du skal ikke utføre oppdraget i praksis …)

Først blir det å gjøre analyse rundt banken, se hvilke firma som leverer for heisen, om det er noen andre firma som Telenor som har servise punkt inne i lokalet dies. Så blir det å skaffe seg en type for ID kort (RFID/NFC), om det er med en lang distanse skanner og klone et kort. Så blir det gå in lokalet gå inn i en heis åpne kontroll panelet og sette den i individuell modus. Bli der til normal ansatte har dratt. Deretter blir det å komme seg inn på server rommet, da kan man prøve og pike låsen viste det er en lett lås, eller bruke en under dør angrep, eller vist vi var heldig med RFID kortet så har du kanskje tilgang til server rommet. Så blir det å sette opp noen LAN

turtles/wifi pinapples på nettet som spuffer alle pc-ene til å gå gjennom dem. Så blir det å gå rundt og se hvilke pe-cer som er åpne for å bruke noen bash scripts via en bash bunny. så blir det å skaffe noe informasjon da blir det enten vist du kommer deg inn på hoved kontorene til f.eks. CEO så kan du ta pc-en vist du ikke kommer deg inn via enten brut force eller ved hjelp av rainbow table. Der etter blir det og komme seg ut, da kan man bruke den heisen som ikke har funket i hele dag på grunn av deg så da tar du den ned igjen og går ut. Enten med pc-en på en cloud eller på en minnepinne.

OPPGAVE 7

Drøft fordeler og ulemper med patent og kopibeskyttet software. Hvem tjener på det og hvem taper? Kan en aktør både tjene og tape på streng håndheving av kopibeskyttelse?

Patent er en måte og sikre at en konkurrent/forfalsker ikke kan kopiere ditt verk innen en vis tidsramme, dette kan hindre innovasjon innenfor det patenten er laget for, fordi det kommer alltid til å bli hindret av de som har patenten. Det kan også føre til at de som eier patenten setter opp prisen på noe folk tenger for å leve av bare for å få veldig høye inntjenings marginer som f.eks. insulin der man må betale ufattelige mye penger for noe som blir produsert veldig billig, men fordi en medisin selskap eier patenten i produksjon så seller de det til ufattelige høye priser. Men kan også føre til at det er vert å forske fram nye metoder for å være den eneste som kan produsere det i en periode, som eller ikke hadde blitt forsket på. kopibeskyttet software er en måte å sikre at man kan vite hvem som har kjøpt produktet og hva man kan bruke av det. Dette er også et dobbeltsidet sverd der det er program som er gratis å bruke og lære, men når man vil få flere funksjoner/ tjene penger på det så må man enten kjøpe det eller abonnere til tjenesten, dette medfører at noen selskaper vet at det ikke er noe konkurranse innenfor hva de gjør og øker prisene sånn at noen som vil starte med det ikke kan/ har ikke rå. Men det kan også føre til at man kan lage produktet sitt helt ferdig så tar selskapet bare en del av din fortjeneste til en sum. Så det er både positive ting innenfor dette og negative ting, det som er vanskelig er å finne et fint middel bane som får både kunden og produsenten til å få godet av dette, men ingen blir misbrukt. En aktør kan både tjene og tape på å være strenge, vist de er strenge så kan de få flere salg av sitt produkt, men vist de er stenge og en konkret lager et lignende, men dårligere produkt kan mange av kundene hoppe over selv om det er et dårligere produkt fordi de ikke er så strenge. Det er også sånn at et rykte om et firma gjør mye med slag og syn på om du vil ha produktene til det firmaet.

OPPGAVE 8

Forklar hvordan du føler emnet Informasjonssikkerhet har vært, hvordan kan du bruke kunnskaper og ferdigheter fra dette emnet i ditt planlagte yrkesvalg? Våren 2020 har vært preget av tilnærmet unntakstilstand i Norge og resten av verdenen, hvordan har det preget din studiehverdag? Hva har vært positivt og hva har vært negativt med å ha siste del av semesteret i et digitalt klasserom, hvordan føler du det har fungert i dette faget?

Emnet har vært en god oppfølger til TK1100 og har forklart mye av det vi lærte før som kanskje ikke ga så mye mening da, men gir mer mening nå. Det er også temaer inne i dette faget som er veldig viktig til å forstå hvordan IT-verdenen har blitt sånn som den er i dag, men også hva vi vå være obs på i vår framtidige jobb innenfor denne verden. Da dette temaet kommer til å spille mer og mer rolle jo mer penger som er inne i blide, når selskaper ikke klarer å opprettholde «best practice» og du ser på nyhetene at fler og fler selskaper blir saksøkt på brud av personvernet og brudd på flere lover. Så dette er noe alle må tenke på bak i hodet når vi jobber framover. Faget er mer egnet som en normal forelesning, der man kan stille spørsmål og komme med diskusjoner og drøftet ting i øvingstimene, og man kan hjelpe værende med ting man ikke er så gode på. Når vi fikk vite at vi måtte ha timene på nettet midt i sesongen blir det mye endringen som betyr at man ikke får sa mye innspill fra studiekameratene/veiledere og får ikke feilsøkt problemer med øvingsoppgavene som gjør det ekstra vanskelig. Det at det også rammer alle fag gjorde det, i en tøff periode utenom studie ble det virkelig et bytte for mange. Det som har vært positivt med denne delen av semesteret er at vi har fått mer kontakt med lærer på Virtuell after-ski og i zoom har mer av personligheten kommet ut. Det som har vært negativt det er alt samarbeid på øvingstimene ble borte/ vanskeligere å gjennomføre. Også motivasjonen til å studere forsvant litt i noen uker der du må fokusere med på om du fortsatt har en deltids jobb eller ikke og om du klarer å betale regninger eller ikke. Jeg føler selve forelesningene har godt fint på nettet, mere det at vi måtte bytte midt inni. Også det med å få hjelp var mye vanskeligere en i øvingstimene, men det kan jo være positivt og negativt.