

Oppgave 1)

Informasjonssikkerhet handler om å sikre informasjonen, som gjør at den ikke stjeles eller modifiseres utilsiktet av angriperen. Samtidig skal man ha tilgang på informasjonen når du har behov for det. Eksempler kan være å sikre passordet på kontoene dine eller maskinen din. Siden det finnes ulike farenivåer når informasjonen faller i hendene på angriperen, må det definitivt være ulike nivåer for sikring av informasjonen. Det er helt ok om foreldrene dine leser meldingene dine på telefonen din, men om informasjonen til etterretningsagentene lekkes ut på nettet kan dette medføre store konsekvenser. Derfor er det utviklet sikkerhetsmodeller som har til hensikt i å forhindre slike angrep. Vi kan ta i utgangspunktet CIA- modellen som beskriver hvordan informasjonen skal sikres best mulig.

CIA står for (Confidentiality, Integrity, Availability)

Confidentiality:

Konfidensialitet går ut på å beskytte informasjonen mot uvedkommende og dermed sier vi at informasjonen skal være konfidensiell, og måten man gjør dette er for eksempel ved å kryptere dataen som skal sendes, og det finnes ulike metoder for å kryptere dataen på, men det består hovedsakelig av en melding som krypteres før den sendes til mottakeren og deretter dekrypteres av en nøkkel til klartekst for å få tilgang til teksten.

En annen måte å holde informasjonen konfidensiell på er å gi begrenset tilgang til informasjonen din ved å at du gir andre brukere tilgang til informasjonen din. Et eksempel kan være å gi informasjonen sin til datasystemer og tjenester som krever at du oppgir sensitiv informasjon for at de skal brukes som i nettbanken som har kun tilgang til spesifikke områder til informasjonen din. Eller så kan det være at du gir kollegaene din autorisert tilgang til dokumentene dine på jobben. I tillegg er det mulig å sikre informasjonen sin fysisk som dørlåser, vinduer, bygninger eller andre steder hvor gjenstander skal oppbevares som f.eks. gullsmed butikker der denne typen sikring er dominerende.

En tredje måte som sikrer konfidensialiteten på er benytte seg av verktøy som avgjør rollen eller identiteten til en person:

Noe en person **har**:

Mobil, nøkler, smartklokke, adgangskort , bankID- kodebrikke

Noe personen **vet**:

Passord, eller informasjon som ingen andre har tilgang til.

Noe personen **er** :

Fingeravtrykk, DNA-test, iris og ansiktsskanning

Integrity:

Integritet går ut på at informasjonen ikke blir utilsiktet endret av personen som ikke skal ha autorisert tilgang til informasjonen din. Det kan være at en person er inne på Facebook profilen din og informasjonen din endres utilsiktet eller det kan være f.eks. når du sender en epost til en annen person så må man vite at det ikke være en tredje person som leser og modifiserer mailen på veien til mottakeren i transitt. Her tar man i bruk sjekksummer som sammenligner dataen som sendes mot dataen som er mottatt og om dataen er ulike på veien er sjekksummen ulik. Det er også mulig å ta backup av dataen som observerer endringene som ble gjort for å sikre integriteten av dataen din.

Availability:

Tilgjengelighet er den siste delen av CIA – modellen som går ut på at de som har autorisert tilgang til informasjonen din , skal ha mulighet til å endre på informasjonen de har fått tilgang på. Det kan være at du gir fysiske papirer til sjefen din som skal ha mulighet til å endre på dem uten at en tredje person overfører informasjonen din i f.eks. i en harddisk og legger det et i en sikker plass f.eks. en safe og deler denne koden med noen andre, som gir dem uautorisert tilgang til informasjonen de ikke skal ha tilgang på.

Oppgave 2)

Brute force angrep er en teknikk som angriperen benytter seg av som går ut på at angriperen prøver å logge seg inn på med ulike IP adresser eller forsøker å taste inn ulike passord. Dette er en indikasjon på at vedkommende ikke skal ha autorisert tilgang til denne informasjonen. Hvis en hacker får kontroll på den private epost kontoen min vil han/hun mest sannsynlig utnytte kontoen min til å få uautorisert tilgang på sensitive opplysninger om meg. Dette kan forhindres ved at man tar i bruk input

begrensninger som for eksempel at man kan taste inn brukernavnet og passordet 4 ganger og hvis inntastningen er feil så må man prøve på nytt om 1 minutt og hvis man gjentar denne feilen, kan man øke ventetiden med 5 minutter som kan forhindre i at hackeren eller angriperen får kontroll over kontoen min og får uautorisert tilgang til informasjon om meg.

Vi lever i en digitalisert verden der internett har blitt en dominerende faktor for oss mennesker i dag. Og siden vi mennesker benytter seg av internett gjelder det får oss som brukere å være bevisst på at det finnes nettbaserte trusler som kan gi oss alvorlige konsekvenser. Smarttelefoner og datamaskiner har økt i popularitet og vi har stadig blitt avhengige av disse enhetene på jobb , skole eller privatbruk. Vi bruker blant annet sosiale medier og andre tjenester hvor dataen er lagret på mobiltelefonen eller datamaskinen våre, men vi må være oppmerksom på at det finnes hackere og svindlere som skjuler seg bak skjermene våre som er ute etter informasjonen om oss. Siden vi er på internett , så betyr det at vi er alltid tilgjengelige for hackere. Derfor er datasikkerheten viktig for at vi skal kunne beskytte oss mot trusler på nettet slik at risikoen for å bli utsatt for angrep skal være minimal som mulig. Det største trusselen for oss som brukere er egentlig oss selv. Det er dessverre uaktsomheten vår som gjør det enklere for hackere å få tilgang til informasjonene våre.

Så lenge vi ikke styrker informasjonssikkerhets kunnskapene våre og er tilkoblet på nettverkene er dette et økende problem, som kan være en stor risikofaktor for oss i fremtiden. Det er også viktig at flere folk får opplæring i etisk hacking som skal kunne beskytte oss mot malware ved at de tetter sikkerhetshull før de blir funnet og misbrukes av hackere. Det er vi mennesker som er den største trusselen mot malware angrep, derfor er det viktig for oss å prioritere å styrke kunnskapen om informasjonssikkerhet som kan bistå med å minimere risikoen for å bli utsatt for virus og andre typer malware. Men dessverre er det fremdeles slik at folk trykker på en epost-link som ikke bare infiserer dem selv, men også de andre på kontaktlisten.

Det er dessverre mange som har blitt utsatt for slike svindelmetoder der svindlere har klart å manipulere brukerne til å oppgi informasjon om seg selv. Dette er et økende problem for oss mennesker som ikke kan unngås med mindre vi klarer å skille mellom hva som kan være ekte eller falskt.

Oppgave 3)

Malware eller malicious software er skadeprogram som er laget for å utføre uautoriserte og ondsinnede handlinger, det finnes ulike typer av malware som for eksempel ormer, virus, trojaner og rootkits. De som utvikler slike programmer har som hovedformål å få tak i penger , informasjon eller spionasje av relevant data til ofrene som er utsatt for et malware angrep på pc-en sin. Skadevarene ønsker å være anonyme for antivirusprogrammene for å utføre oppgavene sine og spre seg videre til

andre maskiner og infisere dem. (Østby, 2022). Malware kan deles inn i tre hovedkategorier som er spredning , Sjulung og nyttelast som være programmer som kan forstyrre datamaskinen.

Spredning (ILOVEYOU ,Stuxnet og Brain):

Brain var et av verdens første virus og ble utviklet av to brødre som drev en databutikk i Pakistan i 1986. Dette viruset var utviklet for å kunne forhindre kunder i å kopiere programvaren deres ulovlig. Dette virus innholdet en melding som bestod av telefonnummeret som var lagt inn av brødrene. Brain stoppet oppstartssektoren i diskett og gjorde ingen andre skade på maskinen en det og spredde seg via disketter . (Hasan, 2019)

Dette er et eksempel på et virus som er to vanligste typene skadeprogrammer som kan spre seg ved at brukeren trykker på en fil for at maskinen skal kunne infiseres. Virus fungerer på den måten at den består av en programkode i filen som aktiveres etter at maskinen er infisert og den infiserte filen vil deretter aktiverer viruskoden i tillegg til å utføre handlingen sin. Virus krever en menneskelig handling for å kunne kjøre eller spre seg, som betyr at brukeren må aktivt trykke på fila for at viruset skal kunne utføre handlingen sin. De vanligste metodene som virus infiserer en maskin på er ved å laste ned filer eller vedlegg fra en epost , laste ned programmer eller filer eller linker fra utroverdige og utrygge nettsider .

Hackere eller utviklerne benytter seg av teknikker for å manipulere en person til å laste ned og kjøre et virus , det gjør de ved å sende for eksempel en mail som inneholder et vedlegg der de forsøker å skrive en mail som skal manipulere brukeren til å laste ned skadeprogrammet. De pakistanske brødrene benyttet seg av disketter og det er pga uaktsomheten til folk som gjorde at den spredde seg fordi de satt inn disketten inn i maskinene sine som forårsaket spredningen.

ILOVEYOU ormen inntok den 4 mai for 22 år siden (Winder, 2020) og spredde seg via epost, som bestod seg av et vedlegg . Denne fungerte ved at en brukeren trykket på en fil i eposten som videre medførte til at ormen spredde seg videre til andre maskiner. Den spredde seg så raskt og infiserte rundt 50 millioner maskiner på 10 dager. Denne ormen gjorde ingen skade på maskinene som ble infisert , men bare spredde seg.

Stuxnet var også ormen som hadde sitt opphav i Iran for 10 år siden. Dette var ormen som var utviklet av amerikanerne i samarbeid med Israel for å sabotere atomprogrammet i frykt for at det kunne utløse en krig. (Gregersen, 2021). Den spredde seg uten at datamaskinene var tilkoblet til internett og infiserte kun maskinene som kjørte Siemens SCADA systemene. Denne ormen påvirket ikke bare Iran og spredde seg overtid til nabolandene som India , Pakistan og Indonesia. Det var anslått at ca.

100 000 maskiner var infisert med Stuxnet ormen , og dette anses som et av historiens verste cyber angrep fordi den var utviklet for å sabotere et system som gav store konsekvenser for et helt land.

Ormer er et av de andre typene malware som er kan minne mye om et virus, men skiller seg ved at den ikke krever menneskelige handlinger for å spre seg. Ormer inneholder kode som gjør at de er i stand til å spre seg automatisk ved å for eksempel kontakte ofre fra kontaktlisten din eller vennene dine på sosiale medier.

Ormen klassifiseres i spredningskategorien siden de spres hovedsakelig gjennom et lokalt nettverk eller internett. Når ormen først har kommet seg inn i et nettverk, så vil den kunne spre seg videre uten noe problem og kan spres seg raskt. De kan spre seg på mange ulike måte ved at man for eksempel plugges inn en minnepinne (USB) på maskinen , en CD trykker på en link i en epost eller en nettside, trykker på en reklame på nettsiden , laster ned et program, eller ved at man trykker på et innlegg på sosiale medier. Noen ormer benytter som oftest seg av sikkerhetshullene den finner på operativsystemet, nettleseren og ser om maskinen ikke inneholder antivirusprogram for å kunne infisere den og spre seg.

Nyttelast og spredning (WannaCry):

WannaCry var et løsepenge virus som antas å være utviklet i Nord- Korea (Wikipedia, 2022) som rammet brukere ved å låse eller kryptere hele datamaskinen. Dette viruset ble utviklet for å kunne tvinge brukere til å betale for å få tilgang til maskinene sine. For å få tilgang til innholdet ble det ble brukt Bitcoin som betalingsmåte. Dessverre var det slik at mange brukere ble infiserte av dette løsepengeviruset. WannaCry kan klassifiseres i både spredning og nyttelast. Selve løsepenge viruset er nyttelasten fordi den utførte en ondsinnet handling som forårsaket en konsekvens for dem som var rammet og spredde seg gjennom et nettverk og infiserte bare Windows Maskinene. Siden WannaCry spredde seg gjennom et nettverk er dette teknisk sett en orm ikke et virus selv om den blir definert som et virus.

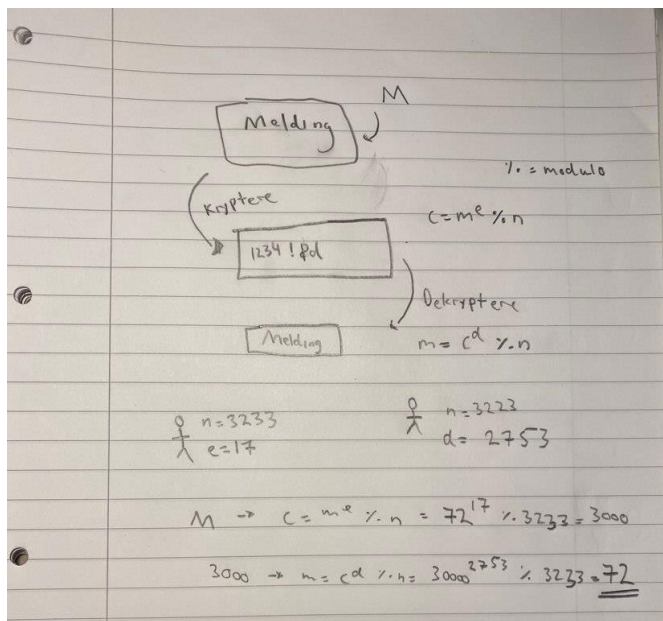
Oppgave 4)

Asymmetrisk kryptering eller public- key kryptering som det også kalles. Her benytter man to nøkkelpar: en privat og en offentlig nøkkel, den offentlige nøkkelen er tilgjengelig for alle i mens den private tilhører en person og skal forbli hemmelig. Et eksempel er når Alice sender en melding til Bob , må hun bruke den offentlige nøkkelen for å kryptere den og sender den til bob, og bob må bruke den

private nøkkelen for å dekryptere den for å lese den. Det er ved matematiske metoder som muliggjør dette.

RSA kryptering er en metode for å utveksle krypteringsnøkkelen, men har utviklet seg til å bli en faktisk krypteringsmetode. Denne metoden fungerer ved at man har en kryptert melding(m), offentlig nøkkel og en offentlig krypteringsnøkkel. For å kunne kryptere denne meldingen benytter man seg av utregningen $c=(m^e)\%n$. Hvis man krypterer hvert tegn i meldingen vil de ha ulike verdier, og hver gang det er et nytt tegn i meldingen betyr det at det er en ny verdi som videre betyr at dette tegnet er kryptert og ikke lesbar. Hvis motsatt, altså dekryptere meldingen, må man ha en privat nøkkel og en dekrypteringsnøkkel. Siden dette er en motsatt operasjon av krypteringen må det definitivt være en annen formel som skal benyttes for dekrypteringen. Formelen som man skal ta i bruk er $m=(c^d)\%n$, og hvis man benytter seg av denne formelen under utregningen, vil den krypterte meldingen, dekrypteres i klartekst form. (Østby, TK2100_01-Kryptering.pdf, 2022)

Tegning:



RSA signering er en matematisk metode som brukes for å kunne verifisere at det er bare avsenderen kunne ha sendt melding og ingen andre. Signeringen blir brukt for å autentisere meldingen for å bekrefte at den ble sendt av avsenderen Alice og ingen andre. Med tanke på CIA sikkerhetsmodellen, blir denne brukt til å kunne beskytte integriteten og konfidensialiteten til melding som gjør at mottakeren Bob kan dekryptere meldingen med den offentlige nøkkelen.

For å signere en melding M så må man først kryptere meldingen med den private nøkkel d . Deretter benytter du deg av formelen $M^d \bmod N = \text{signatur}$. Man kan ta i bruk den offentlige nøkkel for å finne hvem som signerte meldingen ved å ta i bruk denne formelen : $\text{signatur}^e = (M^d)^e = M \bmod N$. Så hvis Alice vil finne ut av om Bob signerte denne meldingen må hun Sjekke om at det resultatet hun får er lik meldingen M . Det er slik hun kan verifisere at bob signerte denne meldingen.

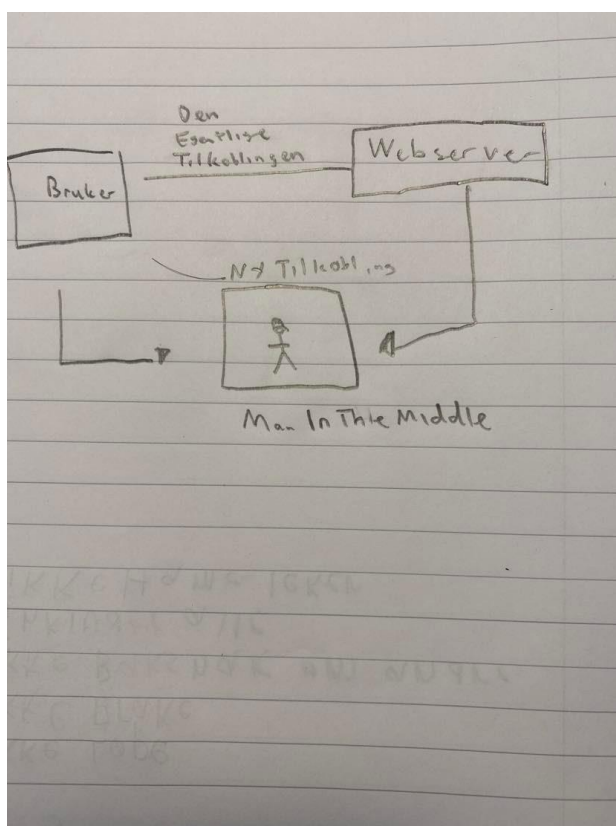
Oppgave 6)

Helt siden internett eller WWW ble oppfunnet har den vår sårbar får internett trusler og spredning av malware og årsaken til det er at den ikke var utviklet for å ha sikkerhet. Så det er egentlig oss som brukere å ivareta sikkerheten på egenhånd, og må ha selv ansvaret å følge som for eksempel ikke laste ned programmer , filer og linker for å redusere risikoen for å bli utsatt for et malware angrep.

TCP/IP modellen er den som overfører data til riktig destinasjon i riktig rekkefølge, disse protokollene har også vært standard helt siden internetts eksistens. Men dessverre er det slik at TCP/IP protokollene i likhet med internett ikke har noe form for integrert sikkerhet. Dette kan blant annet resultere til at den kan misbrukes og siden TCP benytter seg av SYN-ACK eller «Three way handshake» som fungerer på den måten at tjeneren sender en SYN og venter på en ACK eller et svar fra klienten, kan det utføre et såkalt DOS angrep (Denial of Service). Og hvis man aldri får en respons fra klienten kan dette resultere i at meldingen blir hengende og tjenesten blir oppbrukt, applikasjonene vil dermed heller ikke være i stand ta imot flere henvendelser fra tjeneren.

Et annet problem er at man kan bli utsatt for et angrep som heter «Session -hijacking» som er en metode som lar angriper stjele cookie fremdriftene til brukeren, og siden cookie er serverens måte å skille brukere på , kan angriperen kopiere cookie fremdriftene og overføre dem til en annen maskin som manipulerer serveren til å tro at det er den opprinnelige maskinen som betyr at TCP sender pakkene til angriperen fremfor brukeren. Dette er også på grunn av de sårbarhetene Internett består av.

Angriperen eller uvedkommende kan også utføre en Man In The Middle angrep, som er mulig når angriperen er tilkoblet til samme switch som brukeren.. Dette er et angrep som utføres av angriperen der han/hun videresender meldinger som manipulerer to parter til å tro at de kommuniserer med hverandre. Det kan være for eksempel når en person er på en webserver. (Lynch, 2022)



Man In The Middle angrep utføres ved at en angriper avkjærer dataen mellom klienten og serveren .

Det er ARP protokollen (Address Resolution Protocol) bruker en IP adresse for å kommunisere med andre enheter. ARP finner MAC adressen til enheten den vil kommunisere med. Angriper kan ta i bruk teknikker som ARP spoofing som gjør at man kan sende falske ARP meldinger. Dette gir angriper muligheten til å utgjøre seg for å være en troverdig bruker som gjør at angriperens MAC adresse kobler seg til nettsidens IP adresse som gjør at angriper får tilgang til meldingene som går til og fra IP adressen. Dette gjør at angriper kan avskjære , modifisere og slippe inn falske meldinger i forbindelsen mellom klienten og serveren.

På denne måten manipulerer hackeren klienten og serveren til å tro at de sender informasjon til hverandre, deretter fanger angriperen opp dataen som går mellom forbindelsen til klienten og serveren. Og Angriperen oppretter videre en ny forbindelse til nettsiden og setter inn falsk informasjon i kommunikasjonen.

Cashe poisoning er en type MIM angrep som gjør det mulig for angriperen å avlytte all nettverkstrafikk når han/hun er koblet til samme switch. (Yasar, 2022)

Oppgave 7)

Phishing er metoder angriperen tar i bruk får å få tak i sensitiv informasjon. (Wikipedia, Wikipedia, 2022). phishing metoder som for eksempel å sende falske meldinger eller eposter hvor de utgjør seg for å være fra banken eller en nettbutikk. Noen pleier også å ringe opp til deg som har til hensikt å manipulere oss til å oppgi sensitiv informasjon om oss, eksempelvis kan det være at de ringer opp til deg og utgjør seg å være fra banken og trenger bankID og passordet til bankkontoen din. Det er dessverre mange som har blitt utsatt for slike svindelmetoder der svindlere har klart å manipulere brukerne til å oppgi informasjon om seg selv. Dette er et økende problem for oss mennesker som ikke kan unngås med mindre vi klarer å skille mellom hva som kan være ekte eller falskt.

Dette rammer ikke bare enkelt personer, men også selskaper for mange selskaper i dag gir opplæring til ansatte om hvordan man skal håndtere og detektere slike svindelepost eller meldinger, men allikevel så faller de fleste i den fella som risikerer dem i å miste sine rettigheter til å bruke epost og liknende.

For å sikre seg selv mot slike metoder er det lurt å tenke seg om og hvis man blir oppringt av noen eller man får en melding eller epost med en lenke er det lurt å ikke trykke seg inn på lenken eller oppgi sensitiv info som kan være et sikkerhetstiltakene som dermed minimerer risikoen for å bli utsatt for angrep som kan gi deg alvorlige konsekvenser. Andre tiltak man kan ta i bruk for å redusere disse angrepene er å sjekke om f.eks. eposten som ble sendt til deg er fra en troverdig avsender, dette kan dermed gjøre at du unngår å bli manipulert og reduserer risikoen for at du blir utsatt for identitetstyveri. Andre tiltak man kan ta i bruk for å øke informasjonssikkerheten sin er å ikke bruke samme passord på flere av tjenestene eller kontoene sine, hvis hackeren kommer seg inn på et av kontoene dine kan det dermed øke sjansen for at han kan komme seg inn på de andre også. Derfor kan det lønne seg å ha lange og litt kompliserte passord ved å kombinere både bokstaver og tall som du klarer å huske, dette gjør at risikoen for hackerangrep blir mindre og sikkerheten øker.

En annen måte å sikre seg selv på er å ta i bruk to-faktor- autentisering , dette er en metode som kan benyttes for å gjøre det enklere for nettsidene å bekrefte identiteten din på ved å sende en 6 sifret kode på SMS som bare du mottar som skal brukes for at du autentiserer deg for nettsiden, det finnes også touch Id ,eller ansiktsgjenkjenning som noen applikasjoner på mobiltelefonene bruker, får å bekrefte identiteten til brukeren for å logge deg inn. Et tiltak for å beskytte passordene sine er at hvis man skal lagre passordene sine burde man skrive dem ned på et ark og legge dem i et hemmelig sted som er ganske sikkert så lenge det ikke tilgjengelig for andre . Ikke ha det tilgjengelig på pc-en eller på mobilen for hvis man blir utsatt for hacking vil angriperen ha disse passordene i sine hender som kan gi store konsekvenser for deg , så dette er med andre ord ikke sikkert. Et siste tiltak som kan bidra med å redusere risikoen for angrep er å ikke oppgi mye informasjon om seg selv på nettet, som kan øke risikoen for at noen lager falske profiler om deg eller bruker informasjonen og bildene du delte på nettet til noe ondsinnet. Dette er de viktigste sikkerhetstiltakene som kan benyttes for å redusere risikoen for angrep eller identitetstyveri.

Oppgave 8)

Siden verden har blitt utsatt for en pandemi, har det vært innført hjemmekontorer for både ansatte og arbeidsgivere hos selskapene. Dette medførte at man benyttet seg mer av internettet ,og dette har vært en gyldig mulighet for hackere å utføre angrep mot systemet og stjele sensitive opplysninger, som økte risikoen for sikkerhetstrusler. Bedriftene måtte også innføre noen sikkerhetstiltak for ansatte som skulle gi en optimal beskyttelse av informasjonen i bedriftene. Som for eksempel strengere påloggings og passordkrav ved innlogginger på nettet. Her var det viktig for ansatte å ikke lagre passordene på nettsiden som kan medføre store konsekvenser hvis de blir utsatt for et hackerangrep.

Hjemmekontor innføringen gjorde at man f.eks. ikke kunne surfe på nettet uten å bruke VPN for å sikre informasjonen sin og at man skulle få en sikker surfing . Det at man jobbet hjemmefra gjorde at ansatte benyttet seg av hjemmemaskinene og utstyr som er mindre sikre og skyløsninger var mindre sikre ved fildeling, enn de maskinene på jobben som var godt beskyttet mot angrep fordi man utførte pentesting på dem.

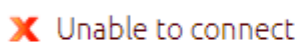
Det medførte også til at man ved video møter for nyansettelse av folk, konferanser og private samtaler kunne avlyttes, dette ble et stort problem ettersom hjemmekontor ble dominerende løsning for arbeid under pandemien.


Med tanke på at hjemmekontorer har blitt den nye normalen og at hverdagen har blitt mer digitalisert er den største sikkerhetstrusselen oss selv, for de fleste av oss har ingen kjennskap til hvordan man skal øke sin egen datasikkerhet. Det at vi ikke har nok kunnskap til datasikkerheten gjør at man blir utsatt for blant annet dataangrep og phishing metoder som for eksempel at svindleren ringer opp og utgjør seg selv for å være fra en tjeneste, eller skrive en svindel SMS eller epost som har til formål å stjele informasjonen din for å utnytte det til noe ondsinnet. Det at vi jobber hjemmefra gjør at vi måtte ta med oss fysiske dokumenter som inneholder sensitive opplysninger, og det er ikke alle som har en form for sikkerhet i huset for eksempel sikkerhetskameraer og andre utstyr som bidrar til å øke sikkerheten i huset er også viktig med tanke på tyveri. Så det er ikke bare den digitale sikkerheten som må styrkes, men også den fysiske.

Hvis dette forblir den nye normalen for arbeidshverdagen og med tanke på uaktsomhet vår, kan det hende at man utvikler nye løsninger som bistår for at arbeidsplassen skal øke den digitale sikkerheten for enkelte og ha mer kontroll på arbeidsplassen hjemmefra. Med tanke på at det er mindre sikkerhet i enhetene man benytter seg av hjemme, vil de fleste arbeidsplassene lage løsninger for å holde strengere krav for begrensnig av hjemme utstyr og enheter, som for eksempel løsninger som gjør at ansatte må kjøpe eller benytte seg av utstyr fra arbeidsplassen som er mer sikre for å øke data sikkerheten under arbeidsdagene som holder til for det meste hjemme. For ansatte som jobber med hemmelig sensitiv informasjon, vil få andre krav enn vanlig ansatte som for eksempel å ta i bruk isolerte arbeidsrom eller hjemmekontorer med låste skap og lydisolerte vegger. Siden man jobber mye hjemmefra vil jeg tro at man kommer til å utvikle løsninger for kommunikasjon som f.eks. utvikle tjenester for som benytter kryptering for å ta kontakt med andre ansatte eller utvikle løsninger som gjør at samtaler eller møtene skal holdes anonyme og avlytningsfritt for å øke datasikkerheten deres.


Oppgave 9)

Bruker digicert ssl sjekker og skriver inn : [https:// demo.testfire.net](https://demo.testfire.net) og får opp en liste med sårbarheter:




 **Heartbleed Vulnerability**

Server is not vulnerable to the Heartbleed Bug because heartbeats are not enabled on this server.

 **Protocol Support**

TLSv1.0
TLSv1.1
TLSv1.2

 **TLS ciphers supported by the server**

TLSv1.0


TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLSv1.1

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLSv1.2

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA

 **No known vulnerable Debian keys were found**

Ser at nettsiden støtter tre forskjellige versjoner av TLS protokollen og får opp TLS cypherene som nettsiden støtter

Oppgave 10)

Benytter meg av Bitfender antivirusprogram i denne oppgaven

1. Jeg laster ned filen fra EICAR: https://www.eicar.org/?page_id=3950 velger eicar.com.zip-fil. Ser at filen skannet filen og detekterte dette som en skade.

**Dangerous page blocked for your protection**

https://secure.eicar.org/eicar_com.zip

Dangerous pages attempt to install software that can harm the device, gather personal information or operate without your consent.

[TAKE ME BACK TO SAFETY](#)

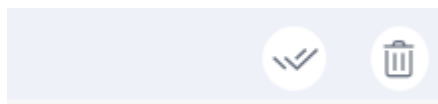
[I understand the risks, take me there anyway](#)

2. Går inn i quarantine og finner zip filen

Infected web page detected
4 minutes ago

Feature: Online Threat Prevention

We blocked this dangerous page for your protection:
https://secure.eicar.org/eicar_com.zip
Dangerous pages attempt to install software that can harm the device, gather personal information or operate without your consent.

3. Deretter sletter jeg zip filen fra karantenen og trykker på søppelkasse ikonet.

Ser at den ble slettet:



You have no critical notifications.

Bibliografi

- Gregersen, E. (2021, Desember 13). *Brittania*. Hentet fra <https://www.britannica.com/technology/Stuxnet>
- Hasan, S. (2019, Desember 18). *Trtworld*. Hentet fra <https://www.trtworld.com/magazine/the-making-of-the-first-computer-virus-the-pakistani-brain-32296>
- Lynch, B. (2022, April 28). *Imperva*. Hentet fra <https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/>
- Wikipedia. (2022, Mai 3). *WannaCry ransomware attack*. Hentet fra https://en.wikipedia.org/wiki/WannaCry_ransomware_attack
- Wikipedia. (2022, Juni 3). *Wikipedia*. Hentet fra <https://en.wikipedia.org/wiki/Phishing>
- Winder, D. (2020, Mai 4). *Forbes*. Hentet fra <https://www.forbes.com/sites/daveywinder/2020/05/04/this-20-year-old-virus-infected-50-million-windows-computers-in-10-days-why-the-iloveyou-pandemic-matters-in-2020/>
- Yasar, K. (2022, April). Hentet fra <https://www.techtarget.com/iotagenda/definition/man-in-the-middle-attack-MitM>
- Østby, B. (2022). TK2100_01-Kryptering.pdf. I B. Østby. Oslo. Hentet fra 48-52
- Østby, B. (2022). TK2100_03_Malware.pdf. Oslo, Norge. Hentet fra 4-5
- <https://www.digicert.com/help/>