Emnekode: TK2100

Emnenavn: Informasjonssikkerhet

Innleveringsdato: 08.06.2022

Eksamen

Høyskolen Kristiania

Semester Vår 2022

Oppgave 1.

Informasjonssikkerhet er et bred emne som omhandler all sikkerhet både digitalt og det fysiske mediet som verter det digitale. Man kan fort gå dypere ned i forskjellige områder for å gi mer klartekst til hva en mener. Eksempler kan være fysisk sikring av servere som lagrer og drifter kritisk data, nettverkssikring fra hackere som prøver å finne hull på nettverk til bedrift eller sosial angrep mot ansatte. Som foreleser Østby har skrevet, basere mye av lærebøker og sikkerhetsbransjen opp mot CIA-modellen; konfidensialitet, integritet og tilgjengelighet (Østby, u.å., 40).

Konfidensialitet er å unngå uautorisert tilgjengeliggjøring av informasjon. I andre ord å beskytte data og kun gi tilgang til riktige personer. Noen tiltak man aktivt kan gjøre er å kryptere dataen. Kryptert data krever ofte mye tid og ressurser for å dekryptere dataen en prøver å beskytte. Adgangskontroll sørger for at kun riktige personer skal kunne vite og finne dataen. Dette kan være eks. Bell-La Padula modellen som ofte militære og statlige organisasjoner basere seg på(«Bell–LaPadula Model» 2021, avsn. 1). Autentisering for å bekrefte vedkommende, det kan være enkle metoder som å gi riktig person et adgangskort til mer sofistikerte metoder som ratina-skann. For det mer digitale er det standard i dag å ha brukernavn og passord.

Integritet betyr at informasjon ikke har blitt endret på av uautorisert måte. Mulige metoder for å sikre integritet på er å ta periodisk arkivering. Sjekksummer av dataen etter autorisert endringer som kan benyttes som kvittering av endringer.

Tilgjengelighet er for hvor lett en kan nå dataen og gjøre en endring på dem. Her er det ikke direkte noen verktøy man benytter, men mer å vurdere hvor lett det er å nå ønske data for autorisert personell kontra hvor vanskelig det er for uønskede.

CIA-modellen er den mest brukte når det kommer til informasjons sikkerhet, men man har andre mer spissede modeller som IAM-modellen (Østby, u.å., 41) og andre begrep som A.A.A.; Assurance, Authenticity og Anonymity. Alt dette er prinsipper og modeller som bygger på informasjonssikkerhet som privatpersoner, bedrifter og større organisasjon som stater og militær bør følge.

Oppgave 2.

Din epostkonto er hacket og har havnet i verste sitasjon mulige. Uten å tenke over det så benyttes gjerne denne eposten til alt en gjør på internett i større grad. Sosiale medier, nyheter, underholdning, økonomi og profilkontoer som Microsoft eller Apple osv.

Nå som all sosiale og økonomiske informasjon er tilgjengelig og kan nås meget enkelt for hackeren med å sende epost for a endre passord. Majoritetene av kontoer bruker epost som en løsning for å tilbakestille passord. Hackeren kan nå gå inn på siden man ønsker å endre passord på, med å sende epost til epostkonto. Dette skaper farlige senarioer hvor hacker kan stjele identitet og penger.

Fra dette punktet vill hacker prøve å finne informasjon som gjør det mulig for et ID-tyveri av offeret. Det trengs ikke mye mer enn fult navn, mobilnummer, fødselsnummer og bilde. For muligheten for å skaffe falsk legitimasjon etterfulgt av opprettelser av nye kredittkort, mobilnummer, og annen form for kreditt.

I Norge er det meget vanlig å benytte seg av BankID som en offisiell metode å signere kontrakter og bevise sin identitet. Så det å skaffe seg kreditt uten dette er trolig ikke umulig uten BankID, men utfordrerne. Skulle BankID være ute på løpet så har nå gjerningspersonen full kontroll på ditt digitale fotspor på internett og full tilgang til å gjøre alt en kan med Norske tjenester.

Hvorfor er det farlig å miste BankID? Her er BankID sin forklaring på elektronisk signering: «Hva menes med elektronisk signering? Ved hjelp av din BankID kan du elektronisk signere avtaler, dokumenter, kontrakter og lignende. Denne signaturen er med noen få unntak (for eksempel testament) like juridisk bindende som en avtale signert med penn.» («Ofte stilte spørsmål - BankID» u.å., avsn. 17). Ved en bindene kontrakt som dette er det meget vanskelig å komme seg ut av kreditt som er signert med BankID etter skaden er gjort.

Hvordan kan vi forebygge at noe så trasig og farlige kan hende? Vi kan først starte med passord. Passord lekkasjer skjer støtt og stadig og er primærkilden for at noen kommer seg in på dine kontoer. Ved å benytte seg av flere passord på de forskjellige stedene man er påkoblet. Redusere man til et domene hvor skaden kan skje og ikke hele digitale fotspor. Det aller viktigste er at passord benyttet til epostkontoen din er unikt og sikkert.

Det andre er å benytte flere epostkontoer til forskjellige nivå av betydning. En sosial media konto har ikke samme vekt i verdi som din bankkonto. Ved å benytte et hierarki av epostkontoer kan man gjøre seg mer sikker for passord lekkasje. Siden majoriteten av kontoer benytter epost som brukernavn gir dette samme effekt som flere passord på forskjellige tjenester. Man deler opp fotsporet til epost domener som innad har passord domener.

Det siste en burde gjøre er å sette opp to-faktorisering på alle kontoer som benyttes. Det betyr at kun brukernavn og passord er ikke nok for pålogging, men en verifisering fra en tredjepart må benyttes, oftest epost. Fra mine erfaringer på internett er ikke alle som støtter det, men å slå av epost og kun benytte SMS og/eller autoriserings applikasjoner på mobil tryggest.

Oppgave 3.

Som nevnt i oppgaven så deler man opp skadevare opp i forskjellige egenskaper, men hva innebære i de forskjellige kategoriene (Østby, u.å., 5).

Spredning:
- **Virus:** Som et biologisk virus er den avhengig av en eksisterende programvare (vertsprogram) å infisere og spre seg til andre maskiner og systemer på.
- **Orm:** Selvstendig programvare som kan gjør hele livssirkelen som et selvstendig program og sprer seg selv oftest igjennom nettverk og benytter sikkerhetsfeil for å gjøre dette.

Skjuling:
- **Rootkit:** Endrer OS, lagrer og viser endret informasjon for dekke sitt tilstedevære.
- **Trojaner:** Et nytteprogram som gjør ondsinnede handlinger i bakgrunnen, men vises som troverdig.

Nyttelast:
- Alt fra ondsinnede handlinger til å ha gode intensjoner som humor.

- ILOVEYOU: Denne skadevaren startet sin spredning mai 2000 og spredde seg igjennom eposter når brukere nedlastet vedlegg. Siden Windows på denne tiden brukte å skjule filutvidelsen, trodde de fleste at dette var et kjærlighetsbrev i from av et tekstdokument og prøvde å åpne det. Dette installerte skadevaren som samlet inn passord og sendte seg selv videre som epost til kontaktlisten til offeret («ILOVEYOU» 2022).
  Dette høres veldig ut som et virus som infisere mailprogrammet og sender epost. Men som jeg tolker beskrivelsen så er dette et selvstendig program som henter data fra mailprogrammet og sender epost via det uten å endre på selve mailprogrammet. Derfor kategorisere jeg dette som en Orm.

- Stuxnet: I meget korte trekk ble dette skadevaren laget av USA og benyttet fire zero-day exploits og skjulte seg selv på SCADA systemer ved å manipulere data vist på maskinene. Den ble først oppdaget i 2010 på maskiner som kontrollerte sentrifuger for å utvikle raffinert uran. Spredningen skjedde trolig hvis igjennom minnepenner som ble plugget inn og kjørte koder med adminrettigheter og gjemte seg ved å manipulere vist data.
  Dette vill jeg beskrive som en orm og rootkit siden den først kjøre kode for å aktivere nyttelastet og gjemmer seg i ettertid med å endre vist data fra OS («Stuxnet» 2022).

- Brain: Et skadevare fra 1986 som ble brukt på floppydisker på IBM PC. Den endret på oppstarts sektoren på disken og la den originale oppstarts koden i en såkalt «bad sector». Ved oppstart ville nå vise sin egen tekst og som jeg tolket det sperret av minnet til maskinen hvis BIOS ikke var registrert. Dette var ifølge forfatteren laget for å hindre pirat kopiering.
  Denne koden har endret/fjernet originalkilden av et oppstarts program og vil kalle dette et virus («Brain (Computer Virus)» 2022).

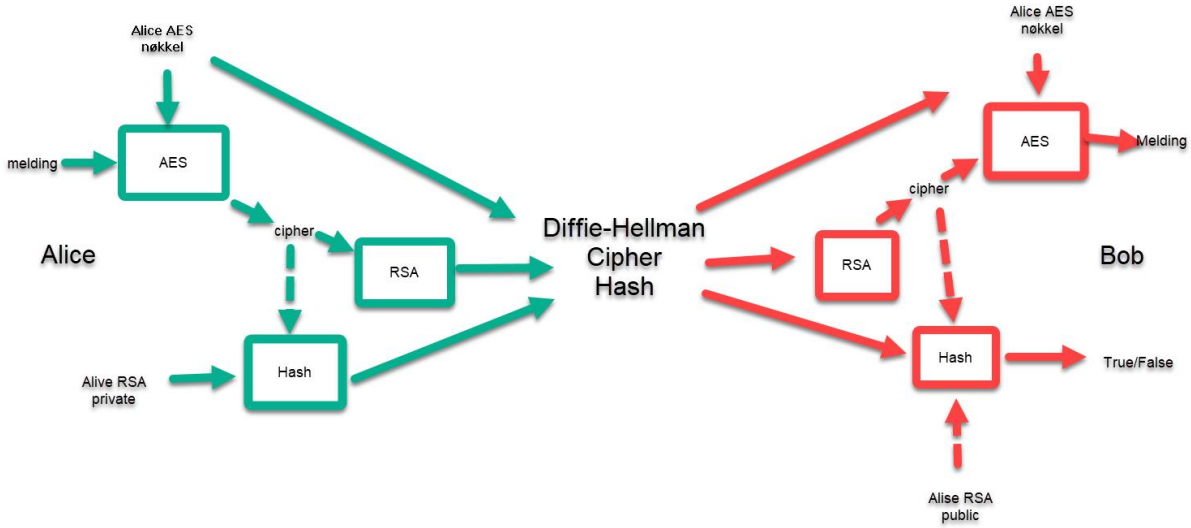
- WannaCry: Skadevare som benyttet en exploit stjelt fra NSA som kun fungerte på en eldre versjoner av Windows. Selv om nyere versjonen av Windows hadde fikset dette problemet var det fortsatt mange bedrifter som benyttet denne eldre versjonen som var utenfor sin livstid og ble påvirket. I 2017 spredde dette skadevaren seg igjennom nettverket og begynte å kryptere filer og date på maskinen. Når disken var kryptert, krevde man penger for å dekryptere disken.
  Denne koden spredde seg selv over nettverk av maskiner og benyttet egen kode for å kryptere diskene på maskinene så vill jeg kategorisere dette som en orm. Skal sies at dette blir en subklasse kalt ransomware og har hele sitt formål å kryptere disken og spørre etter penger eller informasjon for å dekryptere disken («WannaCry Ransomware Attack» 2022).

Oppgave 4.

RSA kryptering eksempelvis er å bruke felles nøkkel til Alice og kryptere den og Alice benytter sin private nøkkel for å hente ut meldingen.

RSA signering er at Alice bruker sin private nøkkel for å lage en hash av meldingen. Sender meldingen og hashen til Bob hvor han dekryptere meldingen og bruker Alice sin offentlige nøkkel til å lage en hash. Hvis både Alice og Bob sin Hash fra meldingen stemmer så er meldingen godkjent.

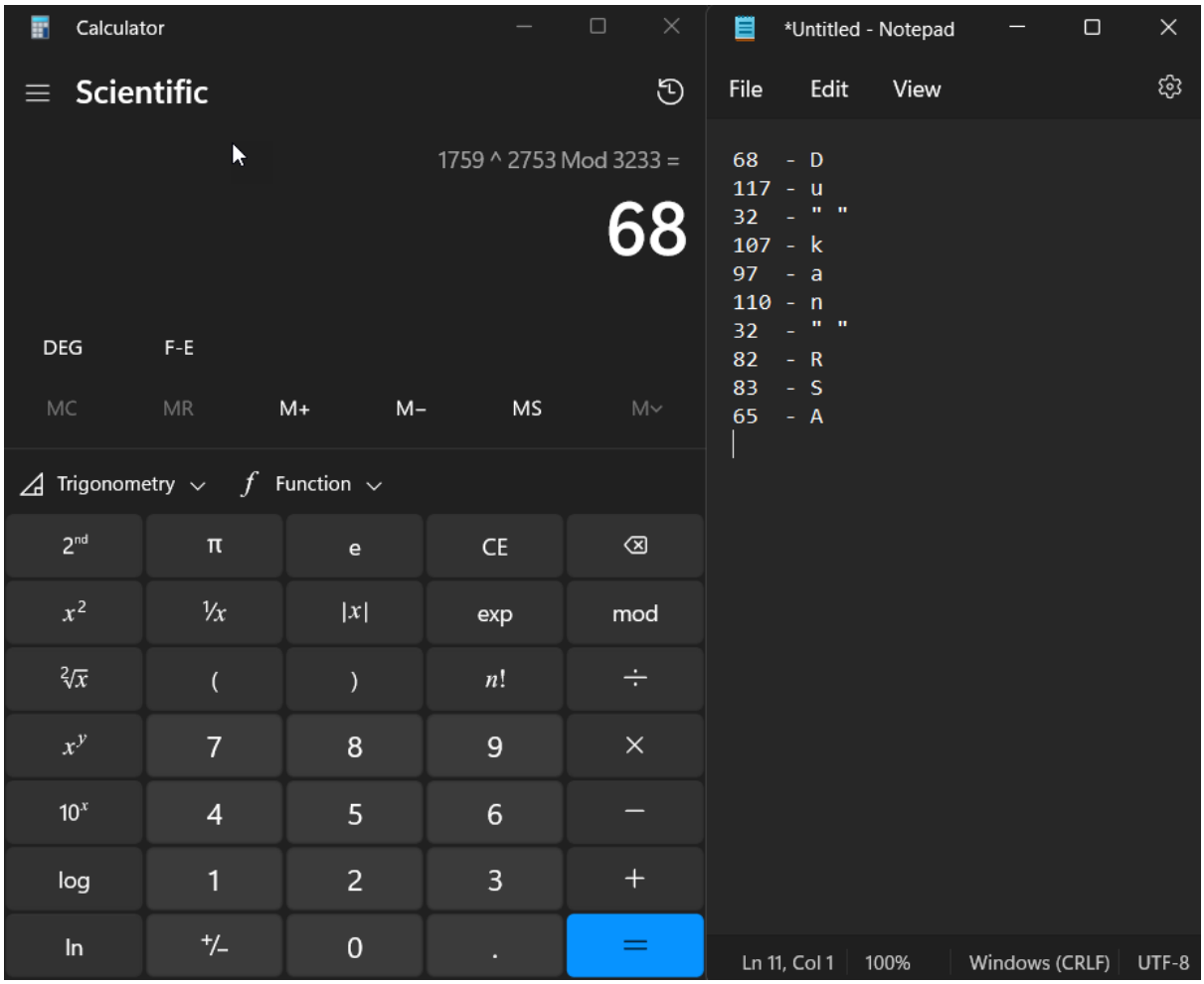
For å sende en epost som ikke kan tukles med tenker jeg man bruker en blanding av AES, Diffie-Hellman og RSA signering. Tanken vill se noe som dette, hvordan det skal fungere i detaljer klare jeg ikke å ordlegge meg.



Oppgave 5.

Fremgangsmetoden er meget fremover. (Østby, u.å., 56) Benyttet lært formel for RSA:

m = message
c = cipher
(n, e) = public key
(n, d) = private key
1. For å kryptere: c = m^e mod n
2. For å dekryptere: m = c^d mod n



Ved å benytte formel beskrevet over, dekrypterte jeg gitt sett med tall fra oppgaven og fikk en melding skrevet i ASCII og oversatt til «Du kan RSA».

Oppgave 6.

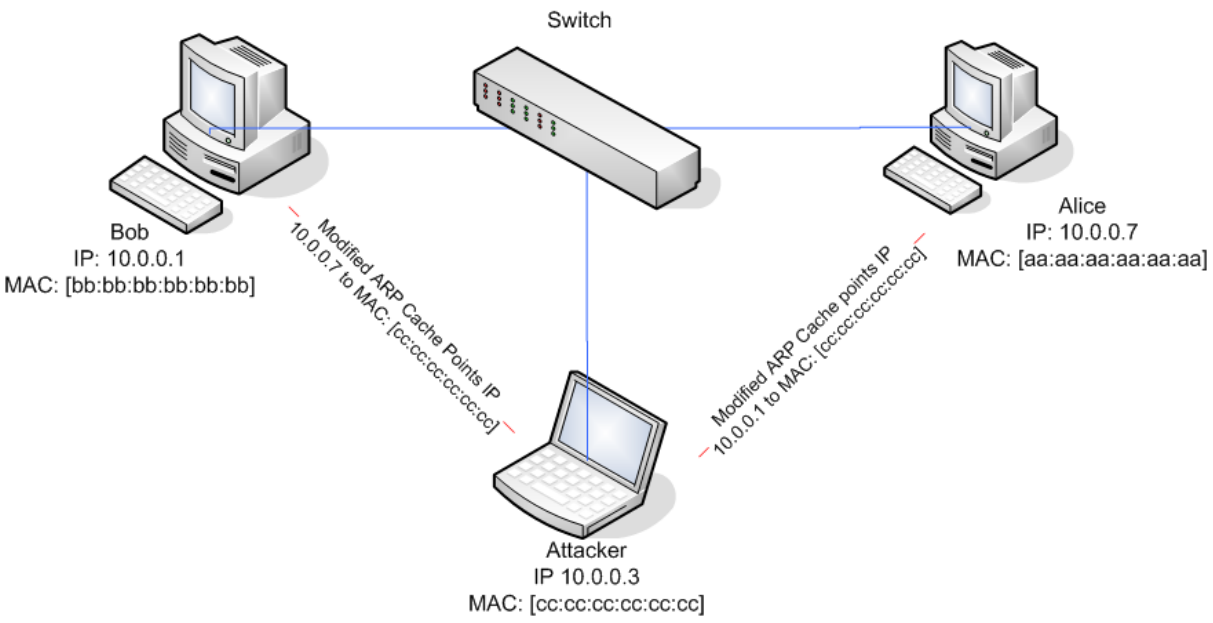
TCP/IP-modellen ble laget og designet tidlig i sine dager hvor man ikke tenkte på sikkerhet. Modellen ble et resultat av ARPANET som blir utviklet på 1970-tallet. Målet var for at internett skal være troverdig og stabilt. Pakker skal fram uansett hvilken vei den dro selv om et led ble borte.

Som skjent så er det forskjellige protokoller som benyttes i det forskjellige lagende i TCP/IP. I linklaget benyttes det noe som heter ARP (Address Resolution Protocol). Denne protokollen sin jobber å kartlegge hvilken maskin som eier hvilken IP-adresse.

Hovedproblemet med denne protokollen at den har ingen form for autorisering som gjør det meget lett å spoofe inn feil MAC-adresse inn i det lokale nettverket. Siden dette systemet er meget basert på tillit så er det vanlig når en maskin kobler seg på nettverket om hvem som har hvilken MAC-adresser og hvilken IPv4 adresser dem tilhører.

1. Alice sin maskin gjør en ARP broadcast for å fylle sin tabell. Eve sender ut sin MAC-adresse og bruker Bob sin IPv4-adresse.
2. Bob sin maskin gjør også en ARP broadcast for å fylle/oppdatere sin tabell og Eve sender ut sin MAC-adresse og Alice sin IPv4 adresse.
3. Alice beholder de originale og riktige MAC og IPv4-adressene.

Nå som Alice skal sende noe til Bob eller Bob skal sende til Alice vill data gå igjennom Eve sin maskin.



(SRJanel [2017] 2022, fig. 1)

Oppgave 7.

Phising er praksisen hvor en hacker sender epost eller andre meldinger for å skaffe personlig informasjon og passord. I majoritetene av tilfellene masker hackeren seg bak noe troverdig som en offentlig tjeneste, bank eller store skjente selskap. I denne eposten ligger det gjerne en URL som offeret skal klikke inn på for å aktivere fellen. Avhengig av nettsiden kan den kjøre scripts for å hente data fra maskinen eller være så enkel at bruker selv skriver inn informasjon i et felt. Skal sies at det finnes flere metoder som prinsipielt gjøre det samme; vishing som er å ringe ut direkte til offeret og smishing som er å sende ut SMS med URL.

Videre i denne drøftingen kommer perspektivet å være orientert fra et bedriftsfokus.
Det viktigste forsvaret mot et slikt angrep er at ansatte vet hva at disse truslene eksistere. Opplæring blir hovedfokuset når man skal kunne forsvare seg selv. Det å ha kurs hvor man går igjennom fremgangsmåten en phising prosess fungere og klargjør hvilke sårbarheter man setter seg selv og bedriften i.

Et problem i å kun stole på ansatte at de kan alt og aldri vill gjøre feil blir meget ignorant og medføre man ender opp med phisinghendelse. Så å ha et system i ettertid som tester ansatte med eposter en gang i uken eller å ringe dem med jevne mellomrom ruster opp de ansatte med kunnskap om hva dem ikke skal gjøre. For at dette skal ha full effekt må det være noe nedsider som at man eks. mister epost rettigheter eller redusere tilganger til ansatte.

Et annet punkt i forsvaret er IT-teamet som kan fikse gode og solide epostfilter som fjerner majoriteten av spam/phising. Problemet er å finne en god balanse mellom å kunne ha en fungerende epost system hvor man kan motta eposter som faktisk er gyldige, men samtidig fjerner søplet. Derfor ligger mye av ansvaret på de ansatte å faktisk vite hva som er farlig å klikke på.

Et meget viktig punkt er at privat personer er like åpne for angrep som bedrifter, men i mye mindre grad har en privatperson mulighet å bli kurset, ha et IT-team for testing og oppfølgning og gjør de forebyggende metodene irrelevante. Her går det mer på selvutdanning, nettfornuft og forhåpentlig hvis en jobb som kan bringe hjem viten om phising truslene som finnes.

Oppgave 8.

Hjemmekontor har blitt en helt ny utfordring for bedrifter som i større grad har aldri møtt på dette problemet. Man har nå to fysiske arenaer hvor sikkerhetsbrudd kan oppstå samt det digitale kommunikasjonsplattformen som må bli integrert til hverdagen.

Mange bedrifter har en større digital plass hvor man ønsker å lagre, endre og lese dokumenter og data mellom ansatte. Fram til nå har det vært en meget lett løsning å ha et eget nett på kontoret som når dette digitale området. Hvordan løser man at en bruker plutselig må nå dette hjemmefra? Bedrifter nå må raskt og mest sannsynlig hoppe ut i et område dem ikke har stor kjennskap til og skapte en helt ny arena for hackere å leke seg i.

VPN (Virtual Private Network) ble en av mange løsninger man benyttet seg av. Dette er programvare som skaper en sikker tilkobling mellom deg og et lukket nettverk. På din maskin er det et program som sender og mottar krypterte meldinger med en VPN-server på jobben som gir tilgang til resten. VM (Virtual Machines) som eks. Citrix ble benyttet. Hvor man kobler seg på en virtuell maskin som har tilgang til jobbnettet. Siste som jeg kan komme på ble ren sky løsning både for bedrift og ansatte hvor all data blir lagret igjennom en tredjepart som Microsoft Azure som basere seg på skylagring og kontotilgang.

Alle tre gir ulemper og fordeler, men har hovedsakelig i de fleste løsninger ett ledd for å bryte seg inn. Brukernavn og passord. Som jeg tolker situasjonen var det mer viktig å kunne komme seg inn på nettverket på et hvis, men nå har spillet endret seg. Hvis man bare fikk tak i et brukernavn og passord kunne man komme seg direkte på bedriftsnettet og få et lett utgangspunkt for en hacker.

Det andre problemet blir fysisk sikring av bygget og kontorene. Nå som det er ingen tilgjengelig er det vanskelig å vite om noen kommer seg inn. Ingen ansatte som kan spørre hvorfor fremmede folk er i kontoret eller intimidere innbrudds folk. Nå som kontorene er meget tomme skaper det en lett tilgang å kunne finne en nettverksport i veggen et sted og sette seg ned å hacke.

Tredje problemet er den reduserte sikkerheten et privathjem bringer forskjell til et stort firma sitt internettsikkerhet med eget dedikert IT-team. Hvis en privatmaskin får et skadevare, kan det fort spre seg igjennom privatnettet og inn i arbeidsmaskinen. Eller at privatpersoner benytter private maskiner uten god og streng Antivirus eller restriksjoner på maskinene så det lett kan komme skadevare på dem.

Håndtering av dette må gjøres på et hvis og vi kan starte med konto problemet. Første en kan gjøre er å sette på to-faktorisering. Viktig her at man bruker gode lange koder så man slipper problemet med bursdags paradokset. Et annet tiltak er å benytte begrenset pålogging basert på region. Så noen fra Asia ikke kan logge på, men jeg i Norge kan. Eller ha en maskin med sertifikat som er registrert som gjør en blir godkjent via pålogging. Det viktigste er at man ikke kun bruker en, men flere for å skape et solid forsvar som gjør en sikret mot flere angrepsmetoder.

Tiltak som kan benyttes for kontoret er å begrense hvilken porter som er aktive og sikkerhetstiltak som alarm til sikkerhetsselskap. Annet virkemiddel er å slå av tråløst nett eller slå av SSID. Dette hindrer lett tilgang for fremmed å koble seg på kontornettet og gjør det vanskeligere å bryte inn. Noe som er meget undervurdert men meget viktig er faktisk fysisk låser. Hvis selskapet investere i låser som tar lang tid å pirke opp øker det sjansen for de få som er på kontoret til å se dem eller kamera overvåkning fanger dem på video.

Hjemmekontor løsningene blir litt mer problematisk, men viktigste blir en blanding av policys for de ansatte. Det å kun bruke jobbmaskin til jobb og ha den oppdatert med antivirus program og Active Directory policy på maskinen for å begrense hva bruker får lov til å ha på maskinen. Dette forbygger farlig installasjon som kan potensielt inneholde skadevare. Opplæring av trygt passord, phising og andre trusler blir enda mer relevant nå som kontor sikkerheten forsvinner.

Som nevnt over blir dette en helt ny måte å tenke på med masse utfordringer, men skal man oppsummere på en fin måte er det viktigste å blande alle tiltakene for å skjerme seg godt for forskjellige mulige angrep. Man må få tilpasset sin løsning som gir best mulig sikkerhet og muligheten for ansatte å komme på. Så her finnes det ikke en løsning, men mange små som danner et solid grunnlag.

Oppgave 9.

Det beskrives at vi skal benytte standard verktøy for SSL/TLS. Jeg kommer å bruke gratis online verktøy https://www.ssllabs.com/ (Østby, u.å., 79).

Det første vi kan ta en titt på er scoren til denne nettsiden. Den får en score T av A – F scoring. T betyr i denne situasjonen at siden sin sertifisering ikke kan stoles på og får automatisk scor T. Hvis vi ser bort fra automatisk T så ville denne siden scoret en B.

Rot problemet til denne siden er at den til nylig har hatt et gyldig sertifikat, men har utløpt den 22.05.2022. Dette problemet gjør at siden automatisk får karakter T pga. HTTPS ikke vill fungere og går over til HTTP. En annen feil som oppstår relevant til sertifikat: «Chain issue: Incomplite, Contains anchor». Fra min forståelse er dette enten en følge feil av utdatert gyldighet eller verre at ordrene på alle sertifikatene er feil.

Et annet viktig problem som tas opp i rapporten er at siden bruker en svak Diffie-Hellman nøkkelparametere som begrenser maks scor til B. Dette skaper en svakhet til det som heter Logjam Attack («Weak Diffie-Hellman and the Logjam Attack» u.å.) I korte trekk betyr dette at man kan nedgradere til en eldre TLS protokoll og gjøre en man-in-the-middle angrep.

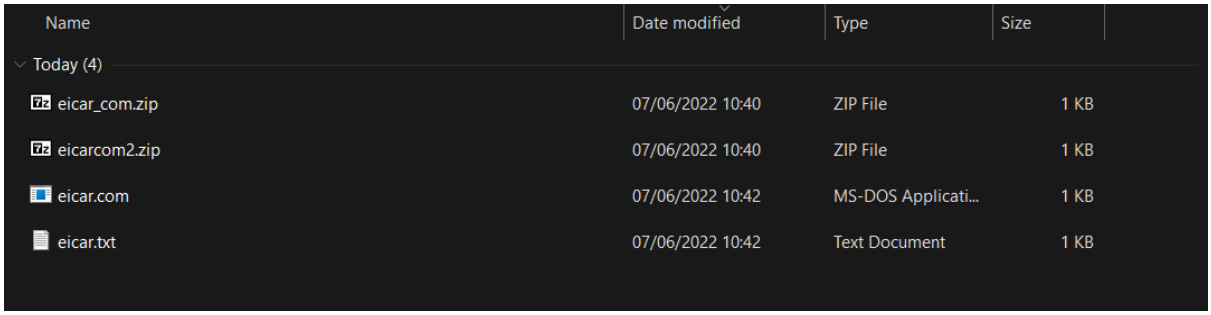
Siste betydelige feil denne siden har er at den støtter eldre versjoner av TLS protokoller som har sine svakheter og utnyttelser. Resten av rapporten kommer med detaljer om andre mulige svakheter som hovedsakelig går i bruk av eldre protokoller, handshakes og svake Cipher Suites.

Fra min tolkning av rapporten kan siden få en scor på A hvis den klare å oppdatere følgende: Sertifikat, begrense til kun nyere protokoller av TLS, høyere Chiper suits som kun kan benyttes og følge resultat blir tryggere handshakes («SSL Server Test: demo.testfire.net (Powered by Qualys SSL Labs)» u.å.).

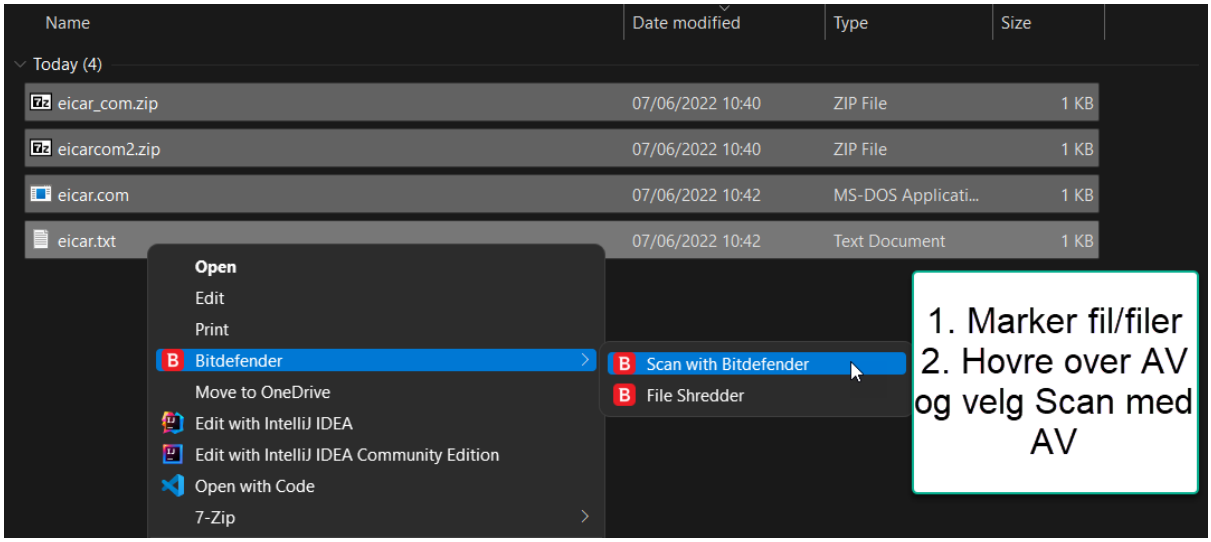
Oppgave 10.

I første steget slo jeg av santidbeskyttelse for min AV (Bitdefender). Grunnen for jeg gjør detter er fordi den vill automatisk skanne og slette skadlig filer den finner på min maskin. Andre steg var å nedlastet tre filer fra referert nettside og laget en .TXT fil med strengen med 64 karakterer som utgjør viruset. Når alt var i download mappen min gjorde jeg følgende:

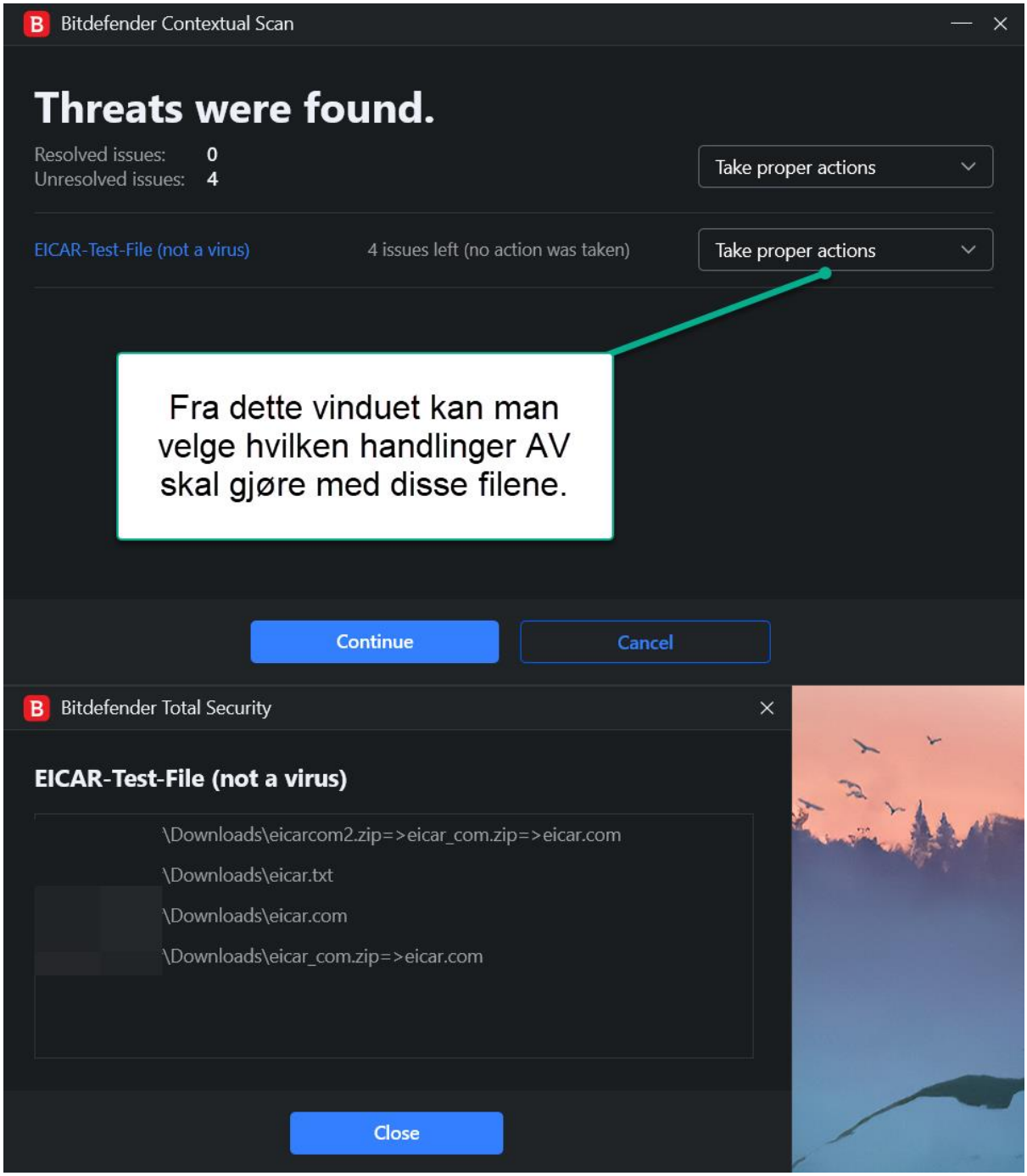
1. Åpnet mappen download fra filutforsker.



2. Markerte alle filene. Høyreklikket og lente pekeren over Bitdefender og ny meny slo ut. I den nye menyen velger man «Scan with Bitdefender»



3. Etter Bitdefender er ferdig skannet får jeg opp dette vinduet som lar meg velge hva jeg skal gjøre: Slette filer, gjøre ingenting eller gjøre riktig handling.
   OBS! Hvis jeg har nedlastet filen mens AV santidbeskyttelse var på så ville den tatt filene i karantene som et valg.



Kildehenvisning:

«Bell–LaPadula Model». 2021. I *Wikipedia*. https://en.wikipedia.org/w/index.php?title=Bell%E2%80%93LaPadula_model&oldid=1053053243.

«Brain (Computer Virus)». 2022. I *Wikipedia*. https://en.wikipedia.org/w/index.php?title=Brain_(computer_virus)&oldid=1083280768.

«ILOVEYOU». 2022. I *Wikipedia*. https://en.wikipedia.org/w/index.php?title=ILOVEYOU&oldid=1091169301.

«Ofte stilte spørsmål - BankID». u.å. Åpnet 7. juni 2022. https://www.bankid.no/privat/los-mitt-bankid-problem/ofte-stilte-sporsmal/.

SRJanel. (2017) 2022. *ARP Poisoning*. C. https://github.com/SRJanel/arp_poisoning.

«SSL Server Test: demo.testfire.net (Powered by Qualys SSL Labs)». u.å. Åpnet 7. juni 2022. https://www.ssllabs.com/ssltest/analyze.html?d=demo.testfire.net.

«Stuxnet». 2022. I *Wikipedia*. https://en.wikipedia.org/w/index.php?title=Stuxnet&oldid=1089678844.

«WannaCry Ransomware Attack». 2022. I *Wikipedia*. https://en.wikipedia.org/w/index.php?title=WannaCry_ransomware_attack&oldid=1086034703.

«Weak Diffie-Hellman and the Logjam Attack». u.å. Åpnet 7. juni 2022. https://weakdh.org/.

Østby, Bengt. u.å. «TK2100_00_Introduksjon.pdf».

———. u.å. «TK2100_01-Kryptering.pdf».

———. u.å. «TK2100_03_Malware.pdf».

———. u.å. «TK2100_07_ModellerMM.pdf».