IN1020 - Operativsystemer og datasikkerhet: Løsningsforslag oppgaver gruppetime 5 (uke 39)

1. Operativsystemer:

   (a)
   - Portable programmer, som fungerer på datamaskiner med forskjellig maskinvare. Det gjør at det blir enklere å forholde seg til.
   - Abstrahere bort maskinvaredetaljer. Detaljer om hvordan lagre filer? Hvordan sende data til nettverket? Hvordan bruke grafikkort.
   - Deling av ressurser mellom tjenester og programmer som kjører (scheduling, allokering). Operativsystemet sørger for rettferdig fordeling av tid mellom prosesser, tjenester og programmer.
   - Sikkerhet. Programmer skal ikke kunne se og forandre hverandres minneområder.

   (b) Dette er noen av stedene hvor det finnes: datamaskiner, biler, smarte enheter (IoT), konsoller, mobiler, Nesten alle digitale enheter har et operativsystem, selv om de i mange tilfeller kan være veldig enkle.

   (c)
   - Extended machine (utvidet maskin): Gjemmer unna detaljene om maskinvare slik at den blir enklere å bruke å bruke datamaskinen
   - Resource manager (Ressurshåndterer): Deler ressursene mellom programmene som kjører på datamaskinen.

2. Hvilke hovedkomponenter finner man i et operativsystem?

   - Filhåndtering
   - Brukergrensesnitt (grafisk og tekst)
   - Prosesshåndtering
   - Enhetshåndtering (Device management)
   - Kommunikasjon (Internt mellom programmer og over datanettverk)
   - Minnehåndtering (allokering, aksess)

3. Diskuter hvilke mekanismer et operativsystem bruker for å ivareta sikkerhet, og sørge for at et program ikke får tilgang til data fra andre programmer?

   Her er noen av momentene man kan være innom:

   - Operativsystemet kar et klart skille mellom «user mode / brukermodus» og «kernel mode / kjernemodus».
   - Vanlige programmer kjører i brukermodus, og har da begrenset tilgang til prosessoren, samt kan kun se sitt eget minne. Interne komponenter i operativsystemet kjører i kjernemodus har vil da kunne kjøre alle typer instruksjoner på prosessoren og se hele minne.
   - Det er innebygd maskinvare i alle prosessorer som sørge for at disse modellene håndheves. Man bør derfor være veldig forsiktig med å gi programmer man ikke kjenner til tilgang til kjernemodus. (sudo på Linux eller Administrator på Windows)
   - Snakk eventuelt i gruppen om noen har hørt om noe i media hvor noen har brukt sikkerhetshull i operativsystemet for å få tilgang til maskiner/data.

4. Sosial manipulasjon:

   (a) Phishing-angrep utnytter menneskelige svakheter: Uvitenhet, godtroendehet, mangel på bevissthet rundt farene ved også digital svindel.

   (b) Sikkerhetstiltak for å forebygge phishing angrep: Opplæring, slik at folk kan klare å identifisere potensielle farer, f.eks. personer som utgir seg for å være legitime personer, og falsk epost. Praktiske sikkerhetstiltak kan være god filtrering av epost, benytte epost-autentisering, samt forsøke å avdekke og deretter tydelig varsle om falske tjener-sertifikater.

   (c) i. Snike seg inn etter andre ("tailgating"). Bære store esker og få hjelp til å åpne døra. Produsere og benytte et falskt tilgangskort.

   ii. Først samel mest mulig informasjon om direktøren, for å se om noe av edt kan brukes til å lure vedkommende. Reretter sende en tilpasset phishing-epost med skadevare vedlagt, eller kanskje med lenke til webside som inneholder en *exploit* for en nulldagssårbarhet som du etter litt forundersøkelser mistenker at finnes på direktørens maskin.

5. Ingen fasit. Tips til hvordan finne ut informasjon om bildet: Kommandoen exiftool på en Unix-maskin på Ifi (feks. login.ifi.uio.no). Google maps el. for å plassere GPS-koordinatorer på kartet. Du kan også finne informasjon om enheten benyttet til å ta fotoet, inkludert OS-versjon. Er dette noe som potensielt kan utnyttes? Tidspunkt bildet er tatt.

   Brukernavn kan f.eks. brukes i phishing, eller kanskje brute-force-angrep.

6. Bruk av HTTPS som sikkerhetstiltak:

   https med digitale sertifikater hindrer falske nøkler og falske tjenester. Den offentlige nøkkelen til en entitet inngår i en ubrutt kjede av sertifikater (med nøkler) som går god for hverandre, helt opp til det øverste nivået, rot-sertifikatet. Det er vanskelig for svindlere å generere og spre falske nøkkelpar til allerede etablerte tjenester.

   Digitale sertifikater hindrer ikke svindler i å opprette et gyldig domene, f.eks. sparebnak1.com, generere privat/offentlig nøkkelpar, og få dette signert av en tiltrodd sertifikatutsteder. Denne fremgangsmåten benyttes ofte i svindel-angrep.

   HTTPS bidrar altså **kun** til å krypterer kommunikasjonen og verifiserer motparten.

7. Tjenestenektangrep:

   (a) Tjenestenektangrep berører sikkerhetsmålet tilgjengelighet, i og med at tjenester som utsettes for angrepet blir utilgjengelig for den som har legitimt behov for tjenesten.

   (b) Å spre skadevaren løsepengevirus (kryptevirus/ransomware) er en vanlig angrepsform. Skadevarer virker ved å kryptere sentrale (ofte alle) filer i et IT-system (på f.eks. en datamaskin), med en for offeret ukjent krypteringsnøkkel, slik at systemet ikke fungerer og blir utilgjengelig. En annen form er tradisjonelle DDoS-angrep, som består i å "bombardere" tjenester med nettverktrafikk på en slik måte at tjenestene/serverne overbelastes og dermed ikke er tilgjengelige for andre . I DDoS-angrep bruker hackerne ofte såkalte *botnett*, som er nettverk av maskiner de har tatt kontroll over med f.eks. skadevare, uten av eier/bruker av maskinen er klar over det. Det skal som regel ganske store mengder samtidig nettverkstrafikk til for å kjøre en tjeneste i senk. En annen form for tjenestenektangrep (nevnt i læreboka) er f.eks. å bombardere en bruker med så mye søppel-epost (spam) at vedkommende ikke får tak i og lest epost som er reell.

   (c) Tiltak mot løsepengevirus er nevnt i oppgave 1 c). Mot DDoS-angrep kan det være vanskelig å beskytte seg, men et tiltak er å ha tilstrekkelig robuste systemer, men f.eks. redundans, samt mulighet til avvis en del trafikk fra spesielle domener/IP-ranger i f.eks. en brannmur. Internettleverandører kan også gjøre tiltak for å stanse denne typen skadelig trafikk på et nivå utenfor selve virksomheten som er målet for angrep. For søppel-epost kan spamfiltrering være et godt tiltak.

8. Se fasit til eksamensoppgaver 3.5 og 3.6 fra eksamenssettet m/fasit H22.

9. Se fasit til eksamensoppgaver 11, 12 og 13 fra eksamenssettet m/fasit H20.

10. Case-oppgave:

    Mulige scenarier: Brukere havner på en falsk nettside (følger en falsk lenke, Googler bankens navn istedenfor å huske adressen el.). Bruker må selv vite forskjell på www.dnb.no, www.d-nb.com, d-nb.org, osv. TLS-basert autentisering er syntaktisk, og gir ikke brukeren bevis for at en nettside er ekte. Bruker benytter et åpent trådløst nett: DNS-forfalskning i et kompromittert eller falskt aksesspunkt kan også sende brukeren til en falsk nettside.

11. Case-oppgave:

    Nei. Kanksje brukeren har forlatt maskinen sin for å få en kaffe eller gå på toalettet? Om maksinen da ikke er låst kan en annen person bruke denne, utgi seg for å være brukeren og sende data til tjeneren. En annen mulighet er at brukerens datamaskin er infisert med en trojaner som genererer og sender data til serveren uten at brukeren vet om det (til tross for at brukeren fysisk sitter foran datamaskinen og aktivt utfører transaksjoner, f.eks. til en nettbank).

    Hvis sesjonen mellom klient og server ikke er beskyttet med TLS (Transport Layer Security) eller f.eks. VPN (Virtual Private Network), kan sesjonen også være et offer for et Man-in-themiddel-angrep. I et Man-in-the-middle-angrep bryter uvedkommende inn i kommunikasjonen og kan endre eller slette data utvekslet mellom klienten (brukerens datamaskin) og tjener

12. Dataangrep:

    (a) Dette er selvsagt basert på WannaCry, så hovedpersonen hadde nok ikke gjort noe galt her. Det som sikkert er skjedd er at en av kollegaene har åpnet en mail der ransomware-en lå. WannaCry er en orm, så denne kunne derfra infisere andre maskiner i nettverket. Hvis studentene mener hovedpersonen er skyldig selv kan årsakene være mange.

    (b) Det riktige svaret er kryptovirus/løsepengevirus/ransomware.

    (c) Arbeidsplassen kunne tatt regelmessige backup av dataene sine og lagret dem adskilt fra arbeidsstasjonene. De kunne også fokusert på opplæring om hvilke e-post man bør åpne og hvilke som er mistenkelige. Dette er ikke en garanti, siden mennesker ikke klarer å ha fullt fokus og ta gode valg absolutt hele tiden. De kunne også hatt en form for spam-filter i epost-tjeneren sin, som kanksje kunne klart å filtrere vekk også denne typen skadevare. Arbeidsplasser bør også oppdatere operativsystemene de benytter med alle tilgjengelige sikkerhetsoppdateringer, siden slike type angrep svært ofte utnytter kjente sårbarheter i f.eks. operativsystem. En seriøs arbeidsplass bør ikke bruke operativsystemer som er så gamle at OS-leverandøren ikke lengre støtter operativsystemet, og dermed heller ikke bruker ressurser på f.eks. sikkerhetsoppdateringer. Når angrepet først er i gang og man ser skadevare spre seg kan det faktisk være lurt å bare skru av alle maskinene. Dra ut kontakten. Selv om krypteringen har startet tar det litt tid å komme gjennom alle filene, så noe kan reddes på denne måten. I etterkant bør man ikke betale. Det er svært sjelden man får data tilbake, dekryptert, ved å betale utpresserne, i tillegg kan det være usolidarisk ettersom man da er med på å oppfordrer angriperne til å fortsette siden det tydeligvis er vellykket.

    (d) Tilgjengelighet. Ikke integritet, siden den ikke fjerner eller endrer filene, slik et integritets-angrep typisk gjør.

    (e) wannaCrypt0r fra mai 2017, som rammet helsetjenester, banker og en rekke andre selskaper over hele verden.