IN1020: Løsningsforslag gruppetime 12 (uke 46)

Oppgave 1: Case-oppgave

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 integritetsangrep typisk gjør.

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

Oppgave 2: 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.

Oppgave 3: HTTP-cookies

En HTTP-cookie hjelper nettsider med å holde på info om brukere, slik at preferanser ikke tilbakestilles og brukeren logges ut hver gang de går til en annen del av siden. F.eks. at handlekurven din i en nettbutikk ikke slettes. Det finnes persistente cookies og session cookies. Førstnevnte lagres i brukerens sekundærminne, som kan være slitsomt ettersom de tar plass. Nettsider bruker cookies til å samle mye ekstra info om de besøkende. Hvilke knapper de trykket på, hvor lenge de var der. I tillegg har vi third party cookies, som er det vi ofte tenker på når vi snakker om reklame og cookies. Disse er fra andre domener, som kan plante cookiene sine på andre nettsider, ved at sistnevnte brukes ressursene deres, slik som bilder, scripts, etc. Det er ofte disse som gjør at andre nettsider får nyss om hva du har sett på. Man har mulighet til å skru av third-party cookies i browseren sin.

Oppgave 4:

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

b) Sende tilpasset phishing-epost med skadevare vedlagt Sende tilpasset phishing-epost med lenke til webside som inneholder en exploit for en zero-day-sårbarhet som finnes på direktørens maskin.

Oppgave 5:

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.

Oppgave 6:

a) Tips: Kommandoen exiftool på en Unix-maskin på Ifi (feks. login.ifi.uio.no). Google maps el. for å plassere GPS-koordinatorer på kartet.

b) Informasjon om enheten benyttet til å ta fotoet, inkludert OS-versjon. Er dette noe som potensielt kan utnyttes? Tidspunkt bildet er tatt.

Oppgave 7: 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.

Oppgave 8: 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

Oppgave 9: Enkel trusselmodellering

1. Innsidebrukeren, f.eks. en tidligere ansatt som har fått sparken. Ønsker hevne seg på konsulentselskapet, og siden vedkommende forsatt har tilgang til systemet logger vedkommende seg inn og sletter alle data hen kommer over. Sikkerhetstiltak som kan hindre denne type hendelser: Umiddelbart deaktivere brukerkontoer når ansatte slutter. Sørge for en policy for tilgang som sikrer at ansatte aldri har tilgang til flere ressurser enn det som er nødvendig for utførsel av jobben deres. Gode backuprutiner, som gjør det enkelt og raskt å gjenopprette fra denne type hendelser. Teknisk konsekvens er at data/informasjon slettes fra datasystemet. Konsekens for virksomheten kan være at ansatte ikke får gjort jobben sin fordi data er forsvunnet, som igjen fører til økonomisk tap pga. stillstand.
2. Angriper med et litt rettet mål, som sender phishing-epost som utgir seg fra å komme fra ledelsen, for å få tak i brukerkontoer/passord. Sårbarheten er dårlig opplæring av brukere med dertil dårlig sikkerhetskultur. Sikkerhetstiltak kan være bedre opplæring, eller kanskje å bruke 2-faktor-autentisering ved innlogging. Kan det i tillegg finnes tekniske tiltak i en epost-tjener, som stopper denne typen angrep? Tekniske konsekvenser vil være at uvedkommende har tilgang til systemet som en vanlig ansatt, med mulighet for å stjele, endre eller slette dokumenter, timelster i timeføringssystemet, osv. Konsekvenser for virksomheten kan være tapt omdømme som følge av (muligens virksomhetskritisk) informasjon på avveie, også om kunder. Mulige juridiske konsekvenser?
3. Tilfeldig angriper som kommer over og utnytter en sårbarhet i web-applikasjonen, f.eks. ved SQL-injisering. Sikkerhetstiltak vil være hyppige sikkerhetsoppdateringer av programvare, kreve bruk av VPN eller annen sikker tunnell i all kommunikasjon med web-tjeneren. Teknisk konsekvens kan være datalekkasje. Konsekvenser for virksomheten kan være tapt omdømme som følge av (muligens virksomhetskritisk) informasjon på avveie, også om kunder. Mulige juridiske konsekvenser?
4. Konkurrent til en av konsulentfirmaets kunder som ønsker opplysninger om et større IT-prosjekt kunden er i ferd med å innføre. Angrepsvektor kan være svindelepost som lurer en ansatt til å utlevere informasjonen, eller kanskje bestikke en ansatt til å utlever informasjonen. Bevissthetstrening, opplæring, ha policyer som sørger for at en ansatt ikke har tilgang til informasjon om andre prosjekter enn de hen jobber på. Teknisk konsekvens er datalekkasje, for virksomheten vil det være juridiske konsekvenser, i tillegg til sannsynlig tapt omdømme.
5. Kun fantasien setter grenser...