Cloud security (T19)

av

Nicklas M. Hamang (kandidat #359),

Huy B. Nguyen (kandidat #418)

&

Dana Zangana (kandidat #488)

som hjemme eksamen i INF3510 (v15)

Innholdsfortegnelse:

1. Introduksjon: 3
1.1 Presentasjon av oppgaven om Cloud Security 3
1.2 Bakgrunn for oppgaven 3
2 Cloud 3
2.1 Hva er Cloud'en? 3
2.2 De forskjellige Cloud typene. 4
2.2.1 Public Cloud 4
2.2.2 Private Cloud 4
2.2.3 Hybrid Cloud 4
2.3 Tjenester i Cloud 4
2.3.1 Infrastrukture as a Service (IaaS) 5
2.3.2 Platform as a Service(PaaS) 5
2.3.3 Software as a Service (Saas) 5
2.2.3.1 E-post servicer 6
2.2.3.2 Social Media. 6
2.2.3.3 Storage. 6
3. Bekymringer og trusler 6
3.1 Digitale beskymeringer. 6
3.2 Fysiske bekymringer. 6
3.2.1 Steg for å beskytte seg mot de fysiske beskymringer 7
3.3 Trusler 7
3.3.1 Data lekkasje 7
3.3.2 Tap av data 8
3.3.3 Kapring av konto eller service trafikk 8
3.3.4 Usikker API'er 8
3.3.5 Service nekt 8
3.3.6 Ondsinnet insidere 9
3.3.7 Missbruk av service 9
3.3.8 Utilstrekkelige tiltak 9
3.3.9 Sårbarheter i delt teknologi 9
4. Sikkerhetsprotokoller 9
4.1 HTTPS - Hyper Text Transfer Protocol Secure 9
4.2 SSL - Secure Sockets Layer 9
4.2.1 TLS - Transport Layer Security 10
4.3 PFS - Perfect Forward Secrecy 10
4.3.1 Diffie–Hellman key exchange 10

5 Kryptering 10
6 Informasjons lagring. 11
6.1 Innlogging informasjon 11
6.1.1 Ren tekst 11
6.1.2 Simpel krypering 11
6.1.3 Hashet passord 11
6.1.4 Hashet passord med “salt” 12
6.1.5 Treg hashing 12
7 Ekstra sikkerhets muligheter 12
7.1 To-faktor innlogging 12
7.2 CAPTCHA 12
8 Kontroll og autorisering organisasjoner 13
8.1 organisasjoner 13
8.2 kontroller og revisjoner. 13
9 Konklusjon 13
Referanse Liste 14

1. Introduksjon:

1.1 Presentasjon av oppgaven om Cloud Security

Denne hjemmeeksamen vil vi gå gjennom de forskjellige sikkerhets systemer og protokoller i Cloud. I tillegg så skal vi drøfte hva som er bra med Cloud og dårlig, forskjellige typer systemer og tjenester i Cloud. Vi starter litt smått om hva en Cloud er, de forskjellige type Cloud systemer tjenester og deretter går vi da dyperer inn i de sikkerheten rundt Cloud. Vi er også litt nysgjerrig på hva de forskjellige firmaer bruker sikkerheten rundt Cloud tjenesten de har valgt.

1.2 Bakgrunn for oppgaven

Cloud i seg selv er jo ganske stort. Man kan tenke seg at Cloud er egentlig internett og all mulig service funksjoner som for eksempel Cloud storage, Cloud Computer etc.
Bare for å nevne noen eksempler i Cloud Storage har vi Apple iCloud, Dropbox, Google Drive etc. og i Cloud computing har vi Citrix etc. Alle de forskjellige Cloud service bruker forskjellige sikkerhet fordi Cloud er jo tilgjengelig på hvilken som helst enhet via internett tilgang og da er det viktig at sikkerheten er på plass på de forskjellige servicene som er tilgjengelig. Mer om sikkerhet kommer vi tilbake senere i rapporten.

En av grunnene til at vi valgte dette temaet er fordi selve tema sier litt om hvordan sikkerhet er i de forskjellige servicene, hva de bruker og hvorfor har vi det. “Security” på norsk er sikkerhet men da tenker vi på back up og hvordan vi tar vare på ting. Men egentlig betyr “Security” er hvordan vi skal beskytte oss og data-en vår.

2 Cloud

2.1 Hva er Cloud’en?

Ordet Cloud er egentlig et buzzword og en forkortelse av termologien “cloud computing”. Første bruken av dette kan spores tilbake til Compaq i 1996. Reuven Cohen, cofounder of Cloud Camp forklarer det best som “The Cloud is a metaphor for the Internet. It’s a rebranding of the Internet”[1].
Dette innebærer da overføringen av prosesser og prosedyrer fra din egen desktop til nett baserte serviser. Den dag idag vil dette innebære alt fra data prosessering til data lagring og sikkerhetskopiering av informasjon.

2.2 De forskjellige Cloud typene.

Det finnes ulike typer Cloud men det er litt avhengig av hvordan Cloud er blitt plassert. Blant dem har vi Public Cloud, Private Cloud og Hybrid Cloud.

2.2.1 Public Cloud

Er en Cloud service og infrastruktur som da drifter av en nett tjeneste, delt gjennom deres klientens base og aksessert av disse klientens offentlige nettverk som internett. Infrastructure as a service(IaaS), Plattform as a service(PaaS) og Software as a service henger sammen med Public Cloud. Dette brukes mye i privatpersoner som er mindre sannsynlighet at de trenger infrastruktur og sikkerhets. Men for bedrifter så kan de også benytte offentlige Cloud for å gjøre sine operasjoner med effektive. for eksempel lagring av ikke-sensitive innhold, online dokumentarbeid og webmail.

2.2.2 Private Cloud

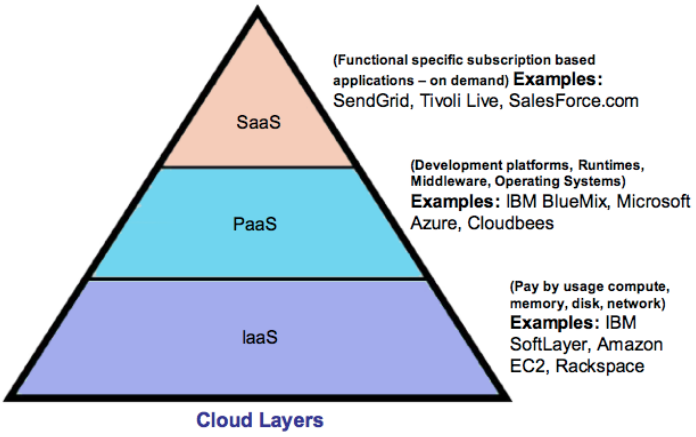
Private Cloud bruker sammenslåtte tjenester og infrastrukturer lagres og vedlikeholdes på en private nettverk enten det er fysisk eller virtuelt. Den åpenbare fordelen er større-grad av sikkerhet og kontroll. Ofte så må kostnadsfordeler ofres til en viss grad som vedkommende av virksomheten blir nødt til å kjøpe eller leie og vedlikeholde all nødvendige programvare og maskinvare.

2.2.3 Hybrid Cloud

Hybrid Cloud er en integrert Cloud service som kombinerer både private og den offentlig delen av Cloud. En slik Cloud tillater å maksimerer sin effektivitet ved å utnytte offentlig Cloud for ikke-sensitive operasjoner og en private oppsett for sensitive eller kritiske operasjoner som gjøre at bedrifter kan sikre at deres data behandling uten at man risikerer å bruke noe mer enn det som er nødvendig.

2.3 Tjenester i Cloud

Tjenestene kan fordeles i 3 forskjellige Cloud systemer Infrastructure as a Service (IaaS) også kjent som Hardware as a Service, Platform as a Service (PaaS) og til slutt Software as a Service (SaaS). Disse tre systemene gir brukere forskjellige bruksrettigheter og begrensninger. Kategoriseringen av servicer inn i disse er bestemt av hvor



stor del av systemet som er styrbart av bruker eller utvikler. De “lagene” som bestemer dette er networking, storage, servers, Virtualization, OS, middleware, runtime, data, application.

2.3.1 Infrastrukture as a Service (IaaS)

Denne servicen gir deg grunnleggende database resurser som trengs for å utplassere bedriftssystemer på internett. Dette inkluderer lagringsplass, hardware, servere og nettverkskomponenter. Typisk for IaaS er at den fysiske delen av infraskrukturen til IT systemer er plassert et eksternt sted og tjenesteleverandøren gir tilgang til et virtualisert miljø av dataresursene til kunden[2]. Med denne type service er fordele mange og store. Kunden trenger ikke lenger tenke på mangel på fysisk plass til alt hardware. Eller kanskje det plutselig trengs ekstra lagringsplass på kort tid. Med IaaS tilbyr de fleste tjenesteleverandører veldig fleksible løsninger til alle kundenes behov. Kunden betaler kun for resurser som blir brukt, og på veldig kort tid kan det også gjøres endringer for kunden[2]. Denne løsningen kan kutte kostnader dramatisk, spesielt for mindre bedrifter eller kunder med liten behov. Her slipper man all innkjøpskostnader, driftskostnader, reparasjonskostnader og ikke minst, sikkerhet og backup av all data. De fleste IaaS systemer bruker sikre protokoller for å holde data til kunder sikkert og trygt. Secure File Transfer Protocol (SFTP), Hyper Text Transfer Protocol Secure (HTTPS) er eksempler på sikkerhetsprotokoller som blir brukt i IaaS.

2.3.2 Platform as a Service(PaaS)

Denne servicen er en kategori av Cloud Computing som tilbyr en plattform og et miljø som tillater utviklere til å lage applikasjoner og service over nettet. PaaS servicene er en host i Cloud og brukere har da tilgang via nettleseren deres. Dette tillater brukeren til å lage programvarer applikasjon ved å bruke verktøy fra leverandører. Servicen kan bestå av forhåndskonfigurerte funksjoner som kunden kan abonerer på. De kan velge å inkludere de funksjonene som oppfyller deres krav og kaste de som ikke gjør det. Følgelig kan pakkene variere fra å tilby en enkel pek-og-klikk-rammeverk der ingen på klient siden trenger å levere en alternativ infrastruktur. Eksempler på protokoller som blir brukt er HTTPS og SSL

2.3.3 Software as a Service (Saas)

Dette er den mest kjente formen av Cloud. Cloud servicer som faller under denne kategorien er nett baserte “programmer” hvor alle lagene er bestemt av utgiveren av servisen og brukeren ikke har bestemmelse over noen av dem. Disse er vanligvis ekle å bruke, de krever ingen nedlasting og absolutt ingen installering. Noen av de mest kjente formene for disse Cloud applikasjonene blant annet e-post (gmail, hotmail, yahoo etc.), sosial media (facebook, myspace, twitter etc.) og Cloud storage (google

drive, skydrive, dropbox etc.). Ettersom disse er hovedsaklig kjørt direkte i nettleseren din så bruker de protokoller som HTTPS, ALS og TCP. [3]

2.2.3.1 E-post servicer

Disse Cloud applikasjonene bruker flere lag av sikkerhets protokoller. De beskytter innlegging informasjon med HTTPS og enten bruken av to faktor's innlogging eller en CAPTCHA. Dette gjøres for å begrense tilgang til din informasjon til deg og beskytte mot innlogging ved bruken av brute force angrep. Det brukes da også en kryptering under overføring mellom servere og mellom forskjellige data senter.

2.2.3.2 Social Media.

Sosial media som e-post bruker HTTPS via SSL og TLS og muligheten for to faktor's innlogging. En veldig populær funksjon brukt av sidene under denne kategorien er engangs passord. [4]

2.2.3.3 Storage.

Disse servicene tilbyr brukeren x antall mega- eller gigabyte som de kan bruke til lagring av filer. Disse filene blir sendt til, fra og mellom serverene med Perfect Forward Secrecy. Mens file blir lagret på selve serveren uten noe ekstra kryptering. Sikkerheten her blir utvidet med at serverene kjører sin egne spesifikke hardware og OS

3. Bekymringer og trusler

Når det kommer til Cloud service er det mange sikkerhets bekymringer og trusler både vi som kunden og utviklerene tenker på. Når det kommer til bekymringer kan dette gjelde sikkerhet for både det fysiske planet og det digitale. De største truslene mot Cloud er informasjons tyver, hackere og cyber angrep.

3.1 Digitale beskymeringer.

Vi vil alle at vår personlige informasjon er sikker. Dette gjør at en av beskymringene våres er hvordan vår opplysninger blir lagret på servicens server. Er utvikleren og servicen til å stole på og hvem burde jeg ikke dele informasjonen min med. Hvordan blir mine personlige filer og data håndtert i servicen og hvordan blir den tatt vare på?

3.2 Fysiske bekymringer.

En av tingene vi frykter er om data'en er trygg mot fysiske skader på hardware. Er informasjonen min trygg hvis det skjer uhell hos leverandøren som f.eks brann, tyveri, strømbrudd, hærverk ol.

3.2.1 Steg for å beskytte seg mot de fysiske beskymringer [5]

De fysiske truslene mot datasentere som nevnt over er en stor risiko. Å tilby Cloud-løsninger til millioner av mennesker rundt om i verden er et stort ansvar for selskaper som tilbyr denne type tjenester. Noen tiltak som er blitt iverksatt av Google blant annet for å beskytte seg mot inntrengere er fysiske gjerder rundt sine datasentere. De har en 24 timers bemannet port som er veldig strenge på å slippe inn besøkede. I tillegg har de overvåkningskameraer plassert overalt rundt senteret som er monitorert live 24 timer i døgnet, 7 dager i uken. For å bli sluppet inn i senteret må en ha adgangskort som er kopi sikret, samt biometrisk innlogging som f.eks iris skanning. Fra innsiden ser sikkerheten annerledes ut. Beskyttelse av selve hardware og kundenes data på innsiden gjøre på følgene måte. Overvåkning av rom og hardware temperatur skjer konstant. Dette er for å minke og også eliminere sannsynligheten for brannfare. Serverne er sammenkoblet via høyhastighets fiber kabler og er koblet til internett med flere nettverkstilganger for at brukerer ikke skal miste kontakt med sitt arbeid hvis en av tilkoblingene feiler. Samme data er også lagret flere steder for backup for å best beskytte data til kunder. I tilfellet en strømsvikt så har senterene til Google flere generatorer som holder serverne gående uten avbrudd. I verste tilfellet hvis hele senteret går offline eller opplever problemer så blir brukere som er koblet til servicen automatisk overført til et annet senter helt flytende uten å legge merke til det og kan fortsette sitt arbeid. Videre er politiresponsen ved senteret veldig korte for sikkerhets grunner.
Levetiden til hardware er ikke evig, og Google har metoder også her for å beskytte brukerdata maksimalt. Først av alt så bruker de spesialtbygd hardware. Dette er for å hindre tap av data i tilfellet tyveri. Selv om noen klarer å få tak i en av deres lagringsenheter, så vil det ikke være mulig å lese noe data av enheten på grunn av mangel på verktøy, noe som bare finnes hos Google. Når en hardisk ikke består tester som de stadig blir utsatt for, så blir de fysisk ødelagt og klippet opp i strimler for at ingen skal kunne lese av daten som var lagret på enheten. De blir så sendt til resirkulering.

3.3 Trusler

Det finnes da mange trusler mot sikkerheten i Cloud men det blir vanligvis satt fokus på 9 spesifikke trusler. Disse har blitt gitt navnet “The Notorious Nine”[n1] av The Cloud Security Alliance (CSA). Hva er disse truslene, hva vil implikasjonene av disse være og hvordan kan du og/eller leverandøren beskyttes mot disse.

3.3.1 Data lekkasje

En data lekkasje vil si når data blir lest og muligens publiser ulovlig av et eller flere pertier som egentlig ikke har rettigheten til å se denne data’en.[6] [7] Dette kan da være et individ, en service eller en organisasjon som har fått tak i denne ulovlige tilgangen.

Dette ble oppgradert til å være den største truselen i 2013[6] ettersom dette er den mest relevante av truslene. Dette leder til at folk lagrer sikkerhetskopi av data'en sin på en lokal maskin, dette vil da egentlig lede til at denne data'en blir mindre sikker. Den beste måten for en person å minimere risikoen for dette er å velge et sterkt passord, holde dette passordet hemmelig og unikt for den siden. Leverandører kan beskytte denne data'en med ekstra bruker autorisering, sikre protokoller for sending av data som SSL og PFS. Dette er en trusel som kan true alle cloud modeller

3.3.2 Tap av data

Tap av data vil bety alle mulige måter data kan forvinne. Som en privat person kan jo dette bety missting av lagring media, tyveri, sletting av en tredje part og masse mer. Det samme kan jo da også hende ved bruk av Cloud service. Da via ondsinnede angrep på systemer, naturkatastrofer, uhell og muligens tap av kryptering nøkkel. Dette er noe som kan ramme alle tre modeller.

3.3.3 Kapring av konto eller service trafikk

Ved bruken av Cloud servicer tillates muligheten for a kapre trafikken mellom deg og servicen du bruker eller direkte kapring av din konto. Ved denne kapringen kan da din informasjon bli misbrukt, manipulert, skadet og/eller ødelagt. For å beskytte trafikken brukes metoder som SSL for å sende data'en sikkert mellom deg og serveren. dette er en fare for alle modellene til Cloud.

3.3.4 Usikker API'er

Cloudtjenester tilbyr en rekke av grensesnitt eller APIer (Application Programming Interface) som kundene bruker til å administrere og samhandle med. Disse grensesnittene må ta hånd om autorisering og tilgangskontroll til kryptering og aktivitetsovervåkning. Den skal også hindre all mulig forsøk på å lure systemet og eller komme seg rundt policy.

3.3.5 Service nekt

Veldig mange er koblet til en Cloud service. Om det er noen som vil slippe ut frustrasjonen sin på andre folk, så er Cloud det rette målet for en slik hensikt. Å nekte brukere tilgang til deres data og filer på Cloud er veldig ondt og effektivt for den som angriper for å skape kaos. Dette kan gjøres ved et DDoS attack og veldig mange kommer til å bli påvirket og ingen kommer til å vite hvorfor. Brukere vil bli nektet adgang til Cloud og det kan bety katastrofale konsekvenser for mange, og Cloud servicen vil få skylda.

3.3.6 Ondsinnet insidere

Dette vil da si en nåværende eller tidligere ansatt eller en tidligere ansatt entrepenør av servicen som da har fått tilgang til informasjonen. Denne informasjonen kan da bli misbrukt eller solgt. Dette er en trusel til alle Cloud modellene.

3.3.7 Missbruk av service

En av de største fordelene til Cloud er at det er billig å få tilgang til store mengder med beregningskraft (computing power). Det ville vært vanskelig og veldig dyrt for små organisasjoner kjøpe og opprettholde tusenvis av servere. For noen betyr ikke dette alltid å bruke det til noe godt. Den enorme kraften til Cloud kan f.eks bli brukt til å dele pirat applikasjoner eller utføre en stor DDoS attack på noen.

3.3.8 Utilstrekkelige tiltak

Cloud har blitt veldig stor og for mange betyr dette at de kan flytte all sin virksomhet over på en slik serivce og oppnå kosntnadsreduksjoner, operasjonell effektivitet og økt sikkerhet. Selv om dette er realistisk for organisasjoner som har resurser til å foreta en slik overgang skikkelig, så er det mange som ikke er klar over det fulle omfanget av Cloud. Å dytte applikasjoner og servicer ut i clouden utsetter man seg for mange sikkerhetsrisikoer som man selv ikke er helt klar over.

3.3.9 Sårbarheter i delt teknologi

Ett av risikoene med å lagre ting i Cloud er at all din data er lagret fysisk et eller annet sted, men det betyr ikke at du er alene om det. Andre brukere av samme service kan ha sine filer og data på samme hardisk, men i en annen partisjon. Risikoen er om noen klarer å få uautorisert tilgang til din partisjon og lese av din data[8].

4. Sikkerhetsprotokoller

4.1 HTTPS - Hyper Text Transfer Protocol Secure

Denne protokollen er en sammensetningen av en vanlig HTTP med en sikkertsprotokoll som f.eks Secure Socket Layer (SSL) eller Transport Layer Security (TLS). Dette gjøres for å skape en sikker kanal over et usikkert nettverk. En nettside kan oppnå dette ved å kjøpe et sertifikat fra en autorisert tredje parti som f.eks Comodo og GlobalSign.

4.2 SSL - Secure Sockets Layer

SSL er en sikkerhetsprotokoll som lar deg sende sensitiv informasjon som f.eks bankkort informasjon (bankkort nr), personlig informasjon (person nr), innloggingsinformasjon osv. over

nett på en sikker måte. Med SSL blir all kommunikasjon mellom nettleser og web server kryptert ved bruken av en symmetrisk sesjonsnøkkel. Denne koblingen opprettes ved at nettleseren ber serveren om å identifisere seg selv, den gir også med informasjon om hvilken versjon av SSL den selv kjører. Serveren gjenkjenner da hvilken versjon av SSL de kan bruke for å kommunisere via. Videre svarer serveren med sitt sertifikat samt en kopi av sin public key gitt via RSA kryptering system. Nettleseren sjekker så med en tredjepart om sertifikatet er til å stole på og lager en forbindelse hvis dette er tilfellet og sender sin en kryptert melding med sin public key. Dette vises som en unik lås ved URLen i nettleseren[9].

4.2.1 TLS - Transport Layer Security

I midten av 90-tallet var Netscape (skaperne av SSL) og Microsoft i konkurranse om å lage beste nettleser. SSL 1.0 ble gitt ut men inneholdt masse feil. SSL 2.0 gjorde forbedringer, men et par år senere ble det klart at den også hadde mange feil. Da kom Microsoft inn på banen og hjalp dem å gjøre den sikrere og slik ble SSL 3.0 til. Videre ble Netscape og Microsoft enige om å la Internet Engineering Task Force (IETF) ta over protokollen og standardisere det som førte til at navnet også ble byttet fra SSL 3.1 til TLS 1.0[10] [11].

4.3 PFS - Perfect Forward Secrecy

Protokollen PFS øker sikkerheten av nett trafikk ved å tvinge bruken av en ny krypteringsnøkkel for hver sesjon mellom nettleseren og nettstedet. Dette kan oppnås ved å bruke en algoritme fra Diffie–Hellman. Når da nøkkelen blir ødelagt etter hver sesjon slutter og skaper ny til neste sesjon så vil dette da beskytte tidligere og fremtidig kommunikasjon fra å bli komprimert hvis noen får tak i sesjonsnøkkelen.

4.3.1 Diffie-Hellman key exchange

Dette er et nøkkel delings system som tillater to systemer å skape en sikker kobling mellom hverandre. Den gjør at de to partene hver for seg kommer frem til samme hemmelige nøkkelen som skal brukes for kryptering. istedenfor å transportere en hemmelig nøkkel fra en til den andre før sesjonen starter.

5 Kryptering

Hva er Kryptering og hvorfor har vi det? Selve ordet er gresk *Kryptos*[12] og det betyr å skjule informasjonen for de som ikke har den riktig nøkkelen eller passord. De-kryptering er det motsatte av kryptering. Dette brukes også for å autentisere informasjon som for eksempel på eposter, at man benytter digitale signaturer for å bekrefte identiteten til en avsender. Et annet eksempel kan være trådløs nettverk. Hvis man ikke har satt opp passord så har alle tilgang til

ditt nettverk. Derfor er kryptering viktig.

Nå finnes det mange typer kryptering men alt krypering basere seg på matematikk. Bare for å nevne noen så er det mest brukte idag er AES, TwoFish [13], TripleDES(DES står får Data Encryption)[14] og IDEA. Advanced Encryption Standard[15] regnes som et at det mest sikker kryptering, men det vil lengre tid å knekke koden til krypteringer. AES bruker symmetric block cipher som vil si at en block med tekster som er i n bits og den biten blir da krypter med en nøkkel i en annen bits [16].

Kryptering brukes på forskjellige områder der man ønsker at ingen skal ha tilgang til data. kryptering på sikkerhetskopi er et eksempel men noen leverandører tilbyr ikke gode løsninger

6 Informasjons lagring.

6.1 Innlogging informasjon

Det blir brukt flere forskjellige metoder for å lagre innlogging's informasjonen din på serveren med. Disse metodene er da å lagre den som ren tekst, kryptere dem med en enkel kryptering, hashet passord, hashing med "salt og treg hashing. [17]

6.1.1 Ren tekst

Er akkurat som det høres ut, dette er når nettsiden lagrer innlogging informasjonen din rett på serveren i lesbar tekst. Dette er en veldig dårlig måte å gjøre det på ettersom en hacker får da tilgang til all innlogging informasjon til alle brukere hvis de klarer å infiltrere nettsidens server.

6.1.2 Simpel krypering

Dette er en lagrings metode hvor det brukes en nøkkel til å kryptere informasjonen før det lagres på serveren. Dette er da ikke spesielt trygt ettersom krypteringsnøkkelen er da vanligvis lagret på samme server. Med da det kryptert passord og krypteringsnøkkelen kan dette enkelt bli dekryptert.

6.1.3 Hashet passord

Hashing as passordet fungerer litt som en oppgradert version av simple kryptering. Den fungerer da på samme måte med at den gjør om passordet til en streng med tilfeldige tegn. Oppgraderingen denne metoden har er at dette gjøres bare en vei, det vil si at når passordet er gjort til en hashet streng kan den ikke gjøres tilbake til det originale ordet. Minusen med dette er da hvis en tredje part får tak i dette hashede passordet kan det da testet mot andre hashede ord til en match blir funnet. En av måtene dette kan gjøres på er ved bruken av brute force med forkjellige hashings

algoritmer. En til metode er å bruke en liste med tidligere hashet ord bedre kjent som et “Rainbow Table”[18].

6.1.4 Hashet passord med “salt”

Som det høres ut så er dette en utvidelse av Hashet passord. Denne legger til noen ekstra tegn før eller etter passordet før den hasher passordet ditt. Disse tegnene er spesifikk for hvert eneste passord. Dette øker da sikkerheten ved at muligens “crackere” ikke vet hva disse tegnene er eller hvor de er satt som da gjør det vanskeligere å bruke brute force eller et rainbow table.

6.1.5 Treg hashing

Denne sikkerhets metoden funker ved å gjøre hver hash opperasjon saktere en vanlig. Denne er da en veldig fin måte å gjøre det på etter som tid er alt under brute force prosessen. Dette er da den tryggeste av alle disse metodene.

7 Ekstra sikkerhets muligheter

Det er mange muligheter å øke sikkerheten din på. Blant dem har vi To-faktor innlogging, CAPTCHA som vi skal gå nærmere inn på. Hvorfor vi har det er fordi at man ønsker å ha ekstra beskyttelse på klientens data og applikasjoner.

7.1 To-faktor innlogging

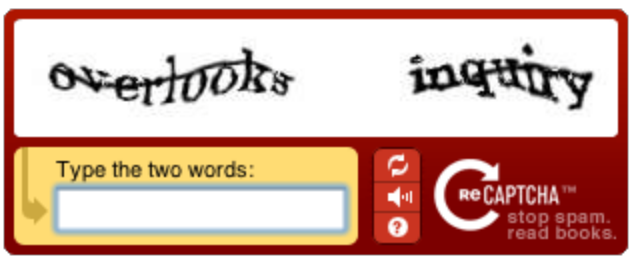
To-faktor vil si at man legger til et ekstra lag av godkjenning til en bruker[19]. Når man logger inn med brukernavn og passord så vil det tilsi at det er 1 faktor innlogging. 2 faktor krever at brukeren har to eller tre av typer identifisering før man kan få tilgang til brukeren.

1. PIN kode
2. Kredittkort, mobiltelefon etc.
3. Noe biometrisk, eksempel fingeravtrykk leser, IRIS skann, stemme godkjenning

Selv om det 2 faktor innlogging har høres sikker ut så det er noen ulemper med det. Blant dem er at det ikke er 100% beskyttet mot crackere. For at dem skal tilgang trenger de noe fysisk komponent(USB etc.) eller tilgang til infromasjonskapsel via nettleseren, og at det kan være vanskelig for brukeren fordi man legger til et ekstra steg i innloggingsprossesen.

7.2 CAPTCHA

CAPTCHA står for Completely Automated Public Turing[20] test to tell Computer and Humans Apart og er et program som hjelper oss



for å beskytte mot BOTS innlogging, spam og passord kryptering ved å spørre deg om en liten test som beviser at du er et menneske og ikke en datamaskin. Den testen er lagt opp i to deler. Den ene er at den generer et sekvens med bokstaver og eller number som vises i et forvrengt bilde og den andre er en tekt boks. For at man skal komme seg videre så må man skrive inn bokstavene.

8 Kontroll og autorisering organisasjoner

For å kontrollere sikkerheten og påliteligheten til en cloud service har vi flere organisasjoner og deres service så har vi flere organisasjoner. disse organisasjonene kan da utføre flere forskjellige kontroller og revisjoner på er cloud firma. Vi velger å nevne noen av disse revisjonen og kontrollene blir brukt for tidligere nevnte sikkerhets bekymringer.

8.1 organisasjoner

- Comodo[21]
- GlobalSign.[22]
- Cloud Security Alliancen[23]

8.2 kontroller og revisjoner.

- Revisjon:
    - Statement on Standards for Attestation Engagements no. 16 (SSAE 16)
    - International Standard on Assurance Engagements no. 3402 type II (ISAE 3402 type II)

- Kontroller:
    - CCM DG - 04: Data Governance - Retention Policy
    - CCM RS - 06: Resiliency - Equipment Location
    - CCM SA - 03: Security Architecture - Data Security/Integrity
    - CCM RS - 07: Resiliency - Equipment Power Failures

9 Konklusjon

Det er veldig delte meninger om bruk av Cloud. På grunn av dens enorme omfang kan den brukes til veldig mye forskjellige. Alt fra å lagre noen dokumenter og bilder til å legge ut en hel organisasjon og selskap på Cloud. De største fordelene er sparing av fysisk plass, enorm digital plass og at den er tilgjengelige overalt så lenge man er koblet til internett. De negative sidene med Cloud er selfølgelig det faktum at all data er lagret hos noen andre. Du er avhengig av at tjenesten er oppe og går 24/7 365 dager i året. En annen risikofaktor er at det er på internett. Selv om den er beskyttet av leverandøren, så er risikoen fortsatt der. Sikkerhets risikoen er forsatt stor på både det digitale og det fysiske planet. Mensteparten av leverandører har høy beskyttelse av hardware. Mange av bevisene peker til at sikkerheten på

det digitale ikke er helt optimalt enda. så det er da opptil individuelle personer om risikoen er verdt tiljegeligheten Cloud tilbyr

Referanse Liste

1: http://www.technologyreview.com/news/425970/who-coined-cloud-computing/
2: https://www.mulesoft.com/resources/cloudhub/iaas-infrastructure-as-a-service
3: http://www.zurich.ibm.com/~cca/talks/metis2011.pdf
4: www.facebook.com/safty/tools
5: https://www.youtube.com/watch?v=OGVAjEcCHrY
6:https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf
7: http://searchsecurity.techtarget.com/definition/data-breach
8: http://ttajts0.tripod.com/cloud/technology.htm
9: https://www.digicert.com/ssl.htm
10: http://tim.dierks.org/2014/05/security-standards-and-name-changes-in.html
11: http://en.wikipedia.org/wiki/Transport_Layer_Security
12: http://no.wikipedia.org/wiki/Kryptografi
13: https://www.schneier.com/twofish.html
14: http://www.cryptographyworld.com/des.htm
15: http://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard
16: https://www.youtube.com/watch?v=Fo_-azAEAz0
17: http://lifehacker.com/5529133/five-best-password-managers
18: http://en.wikipedia.org/wiki/Rainbow_table
19: http://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/
20: https://support.google.com/a/answer/1217728?hl=en
21: https://www.comodo.com/
22: www.globalSign.com
23: www.cloudsecurityalliance.org