bitsec

2014-06-27

Dokument ID: AJP131126-001

Er referens:
SecureMailbox
Mats Enocson

Säkerhetsgranskning

SecureMailbox

bitsec

Kungsbron 21 111 22 Stockholm 08-411 90 10 info@bitsec.se www.bitsec.se

1. Exekutiv summering

Bitsec har som oberoende part, på uppdrag av SecureMailbox, granskat krav samt prövat hur väl tjänsteprodukten uppfyller kraven. Kravställningen för denna säkerhetsgranskning har satts samman för att adressera en kombination av vanligt förekommande tekniska frågeställningar vid utvärdering av molntjänster. Detta rör framförallt hanteringen av information skyddad av Persondatalagen (PUL), Patientdatalagen (PDL) samt allmänna krav rörande säkerhet och tillgänglighet.

Sammantaget uppfyller SecureMailbox samtliga av de uppsatta kraven.

2. Bakgrund

Detta dokument redogör för de krav som ställs på tjänsteprodukten SecureMailbox. Varje krav redovisas även med hur väl tjänsteprodukten uppfyller det. Kraven har utformats av Bitsec och representerar aspekter som är viktiga för:

- Skydda personlig information och integritet.
- Säkerställa säker kommunikation.
- Verifiera partnerna i kommunikationen.
- Säkerställa driftskontinuitet och åtkomst till informationen.

Kraven som är uppsatta följer ingen standard utan är utformade för att ge högsta möjliga säkerhet för användarna. Med detta sagt innebär det att uppsatta krav i vissa fall är hårdare än någon standard fastställer.

3. Beskrivning av tjänsteprodukten

SecureMailbox är en säker kommunikationsplattform som hjälper företag, myndigheter, sjukvård och privatpersoner runt om i världen att säkert utbyta och lagra meddelanden, dokument och bilder på ett enkelt och legalt korrekt sätt.

SecureMailbox är lätt att använda, väl integrerad med användarens vanliga e-post, och ser till att viktig information alltid är krypterad, säkert lagrad och juridiskt korrekt hanterad.

4. Krav

För att säkerställa ovan aspekter av säkerhet samt att tjänsteprodukten kan uppfylla ovan funktioner till användaren har följande krav ställts;

4.1 Kryptering

4.1.1 Krav
Meddelanden i sin helhet inklusive eventuella bilagor ska lagras krypterat.

4.1.1.1 Kravuppfyllelse
SecureMailbox uppfyller kravet.

Genom kodgranskning har Bitsec verifierat att filerna, där meddelanden i sin helhet samt eventuella bilagor lagras, är krypterade med AES 256 symetrisk kryptering.

4.1.2 Krav
Kommunikationen mellan användare och SecureMailbox sker krypterat.

4.1.2.1 Kravuppfyllelse
SecureMailbox uppfyller kravet.

Kommunikationen mot SecureMailbox sker genom HTTPS[1] samt med PFS[2]. Funktionaliteten fungerar på samtliga framstående webbläsare. Upprättas inte HTTPS anslutning fungerar tjänsten inte, detta då kommunikationen inte sker krypterat.

4.1.3 Krav
Användarens lösenord ska lagras krypterat.

4.1.3.1 Kravuppfyllelse
SecureMailbox uppfyller kravet.

Användarens lösenord krypteras genom en hash algoritm med salt[3]. Detta gör att lösenordet inte kan läsas som klartext av någon part, inte heller SecureMailbox.

[1] Hypertext Transfer Protocol Secure – Krypterad transport av data för http-protokollet
[2] Perfect Forward Secrecy – Nyckelbaserad säkerhet för transport av data
[3] Ett slumpmässigt tillägg till ett lösenord som förstärker skyddet

4.2 Autentisering

4.2.1 Krav
Meddelanden som skickas av användare (avsändaren) ska bara kunna öppnas av menad mottagare.

4.2.1.1 Kravuppfyllelse
SecureMailbox uppfyller kravet.

Genom tester har Bitsec verifierat att meddelanden skickade med funktionaliteten ”ID-kontroll” aktiverad kräver stark autentisering av mottagaren för att kunna läsas. Autentiseringen är stark då den kräver två faktorer, dels att mottagaren måste kunna presentera sitt användarnamn och lösenord, men även att användaren måste bekräfta sin identitet genom att ange en kod som skickats till det mobiltelefonnummer som angetts.

4.3 Redundans

4.3.1 Krav
Användarens information ska lagras med minst trippel redundans.

4.3.1.1 Kravuppfyllelse
SecureMailbox uppfyller kravet.

SecureMailbox använder AWS S3[4] för att lagra användarens krypterade information. Denna tjänst omfattar redundans och replikering genom tre olika datacenters.

SecureMailbox använder AWS RDS[5] för att lagra sin databas. Tjänsten omfattar redundans och replikering genom tre olika datacenter.

[4] Amazon Simple Storage
[5] Amazon Relational Databas Service

4.4 Lagring

4.4.1 Krav
Användaren ska själv kunna styra i vilken region dennes information lagras.

4.4.1.1 Kravuppfyllelse
SecureMailbox uppfyller kravet.

SecureMailbox använder AWS S3[6] för att lagra användarens krypterade information. Denna tjänst lagrar informationen enligt EU-standard på Irland. För SecureMailbox företagskunder finns valet att själv styra lagringen till en annan region. De regioner som i nuläget finns som val är:

US-East-1:	USA, Norra Virginia
US-West-1:	USA, Norra Kalifornien
US-West-2:	USA, Oregon
EU-West-1:	EU, Irland
AP-Southeast-1:	Asien/Stillahavsregionen, Singapore
AP-Southeast-2:	Asien/Stillahavsregionen, Sydney
AP-Norhteast-1:	Asien/Stillahavsregionen, Tokyo
SA-East-1:	Sydamerika, Sao Paulo

4.4.2 Krav
Användarens lagrade information ska inte gå att härleda tillbaka till dem.

4.4.2.1 Kravuppfyllelse
SecureMailbox uppfyller kravet.

SecureMailbox lagrar all användardata i krypterade filer vars namn slumpmässigt blir satta genom UUID[7]. Detta har validerats genom tester där användardata skapats och de filer som lagrar information har granskats.

4.4.3 Krav
Informationsradering i form av tömning av papperskorgen utförd av användaren ska betyda att den krypterade meddelandefilen raderas permanent från SecureMailbox servrar.

4.4.3.1 Kravuppfyllelse
SecureMailbox uppfyller kravet.

När en användare tömmer papperskorgen raderar SecureMailbox den krypterade meddelandefilen genom att skriva över den med en tom fil. På så sätt går inte den raderade informationen att återskapa. Tillvägagångsättet har verifierats av Bitsec genom kodgranskningar.

[6] Amazon Simple Storage
[7] Universally unique identifier

4.4.4 Krav

SecureMailbox har funktioner som möjliggör att meddelanden i sin helhet raderas hos mottagaren efter läsning (Burn After Reading) eller efter ett visst datum (Expiration Date).

4.4.4.1 Kravuppfyllelse

SecureMailbox uppfyller kravet.

Funktionerna är verfierade av Bitsec genom kodgranskningar. Den skickade meddelandefilen skrivs över med en tom fil, på så sätt går inte informationen att återskapas.

4.5 Säkerhetsvalidering

4.5.1 Krav

Tjänsteprodukten SecureMailbox ska regelbundet säkerhetsgranskas av tredje part. Detta för att säkerställa att samtliga kravställningar kontinuerligt uppfylls.

4.5.1.1 Kravuppfyllelse

SecureMailbox uppfyller kravet.

SecureMailbox genomför säkerhetsgranskningar, inkluderar penetrationstester och kodgranskningar, var sjätte (6e) månad. Säkerhetsgranskningarna utförs av Bitsec.

4.5.1 Krav

Tjänsteprodukten SecureMailbox ska ha en certifierad driftsmiljö. Certifieringarna ska säkerställa driftsmiljöns säkerhet, redundans och kontinuitetsplanering.

4.5.1.1 Kravuppfyllelse

SecureMailbox uppfyller kravet.

SecureMailbox driftsmiljö är hos Amazon AWS[8] som har följande certifieringar;

HIPAA	US Health Insurance Portability and Accountability Act
SOC 1/SSAE 16/ISAE 3402	Service Organization Controls 1
SOC 2	Service Organization Controls 2
SOC 3	Service Organization Controls 3
PCI DSS Level 1	Payment Card Industry Data Security Standard
ISO 27001	International Organization for Standardization, LIS (Ledningssystem för informationssäkerhet)
FedRAMP	Federal Risk and Authorization Management Program
DIACAP	Department of Defence Information Assurance Certification and Accreditation Process
FISMA	Federal Information Security Management Act
ITAR	International Traffic in Arms Regulation
FIPS 140-2	Federal Information Processing Standard Publication 140-2
CSA STAR	Cloud Security Alliance. Security, Trust & Assurance Registry
MPAA	Motion Picture Association of America. Best practice for securely storing, processing and delivering protected media and content.

[8] http://aws.amazon.com/compliance/

bitsec

4. Om Bitsec

Bitsec är ett företag som stödjer organisationer genom att tillhandahålla djup teknisk kompetens, lång erfarenhet av IT-säkerhet samt Informationssäkerhet, och med djup förståelse och erfarenhet av vilka risker som finns och vilka hot som olika aktörer utgör. Vi är vana att arbeta i känsliga miljöer och att hantera konfidentiell information. Vi arbetar kontinuerligt enligt tydliga processer för att säkerställa säkerhet och sekretess i vårt arbete, och samtlig personal är säkerhetsprövad.

Bitsec arbetar i samtliga nivåer med säkerhetsgranskningar, penetrationstester, kodgranskningar, härdning och säker arkitektur.

Gällande säkerhetsgranskningar levererar Bitsec på samtliga nivåer, från enkla penetrationstester med automatiserade verktyg, till manuell penetrationstestning, samt till djupaste kodgransking. Bitsec kan även bygga kod för att testa eller bevisa sårbarheter (exploitutveckling).

För Bitsec, den 5 juni 2014

……
Jonas Persson
Senior IT-säkerhetskonsult