Adobe Creative Cloudin tietoturvaan liittyvät usein kysytyt kysymykset IT-henkilöstölle

Adoben Creative Cloudia koskevat yleisimmät kysymykset liittyvät tietoturvaan, yksityisyyteen ja vaatimustenmukaisuuskäytäntöihin. Creative Cloudia käyttävät organisaatiot ovat huolestuneita tietojensa turvallisuudesta ja luotettavasta käytöstä. Tämän dokumentin tarkoituksena on vastata IT-resurssien turvallisuudesta vastaavien käyttäjien aihetta koskeviin, Creative Cloudin hankkimista harkittaessa esitettyihin usein kysyttyihin kysymyksiin.

1 Missä Creative Cloudia ylläpidetään?

Creative Cloudia ylläpidetään Amazon Web Services (AWS) -palveluissa, mukaan lukien Amazon Elastic Compute Cloud (Amazon EC2) ja Amazon Simple Storage Service (Amazon S3), Yhdysvalloissa, Euroopan unionissa sekä Aasian ja Tyynenmeren alueella. AWS on ohjelmistopalveluiden luotettava ympäristö, jolla on tuhansia yrityskäyttäjiä ympäri maailmaa. AWS sertifioidaan ja tarkastetaan alalla yleisesti hyväksytyllä tavalla ja sen palvelut perustuvat parhaisiin tietoturvakäytäntöihin. (aws.amazon.com/security/). Tämä tarkoittaa, että Creative Cloudin jäsenet voivat nauttia Amazonin tallennettuihin resursseihin sovellettavien tietoturvakäytäntöjen jatkuvasta noudattamisesta.

2 Minne asiakkaan tiedot tallennetaan?

Asiakkaan tiedot tallennetaan Amazon S3:een, ja Adobe määrää, millä fyysisellä alueella yksittäisten asiakkaiden tiedot ja palvelimet sijaitsevat. Amazon S3:n dataobjektien replikointi suoritetaan siinä alueellisessa klusterissa, jonne tiedot on tallennettu, eikä tietoja replikoida muilla alueilla oleviin tietokeskusklustereihin. Adobe ylläpitää Creative Cloudia kolmella alueella: Yhdysvalloissa, Euroopan unionissa sekä Aasian ja Tyynenmeren alueella.

Esimerkki: oletusarvoisesti kaikkien Euroopan unionissa asuvien Creative Cloud -asiakkaiden pilvessä olevat tiedot tallennetaan Euroopan unionissa sijaitsevaan AWS:n tietokeskukseen eikä tietoja siirretä Euroopan unionin ulkopuolella sijaitseviin tietokeskuksiin.

3 Kuka valvoo Creative Cloud -tietokeskuksia?

AWS:ssä käytettävien Creative Cloudin osien fyysisiä komponentteja valvoo Amazon. AWS:n valvontamenetelmien ja niiden tehokkaan toiminnan selventämiseksi AWS on julkaissut Service Organization Controls 1 (SOC 1), Type 2 -nimisen raportin. (aws.amazon.com/security/), jossa on määritetty Amazon EC2:n, Amazon S3:n ja Virtual Private Cloudin (VPC) valvontamenetelmät, kuten myös fyysiseen tietoturvaan ja ympäristönsuojeluun liittyvät yksityiskohtaiset valvontamenetelmät. Nämä valvontamenetelmät on määritetty useimpien asiakkaiden tarpeita ajatellen erittäin yksityiskohtaisesti.

4 Antaako Amazon asiakkaille luvan käydä AWS:n tietokeskuksissa?

Ei. AWS:n tietokeskuksissa on useiden asiakkaiden tietoja, joten asiakaskäynnit AWS:n tietokeskuksissa eivät ole mahdollisia, sillä tällöin kolmannet osapuolet voisivat päästä käsiksi monien asiakkaiden tietoihin. Riippumaton ja pätevä tarkastaja tarkistaa valvontamenetelmien olemassaolon ja toiminnan asiakkaan puolesta osana SOC 1, Type 2 -raporttia. Tämä yleisesti hyväksytty kolmannen osapuolen tarkastus antaa asiakkaille riippumattoman näkemyksen käytettävien valvontamenetelmien tehokkuudesta. Adobe on solminut AWS:n kanssa salassapitosopimuksen ja voi hankkia kopion SOC 1, Type 2 -raportista (aws.amazon.com/security/). AWS ISO 27001 -tarkastukseen, PCI-arviointiin ja ITAR-tarkastusprosessiin sisältyy myös tietokeskuksen fyysistä tietoturvaa koskevia riippumattomia arviointeja.

5 Voivatko kolmannet osapuolet päästä AWS:n tietokeskuksiin?

AWS valvoo tietokeskusten käyttöoikeuksia tarkasti jopa sisäisten työntekijöiden osalta. Kolmannet osapuolet eivät pääse AWS:n tietokeskuksiin, paitsi jos AWS:n tietokeskuksen johtaja on sallinut tämän erikseen AWS:n käyttöoikeuskäytännön mukaisesti. Lisätietoja fyysiseen käyttöön liittyvistä valvontamenetelmistä, tietokeskusten käyttövaltuuksista ja muista valvontamenetelmistä on SOC 1, Type 2 -raportissa (aws.amazon.com/security/).

6 Kuka on vastuussa korjauksista?

Adobe vastaa AWS:ssä käytettävän oman vieraskäyttöjärjestelmänsä, ohjelmistojensa ja sovellustensa korjaamisesta. AWS vastaa AWS-palveluiden tuottamiseen käytettävien järjestelmien, kuten hypervisor- ja verkkopalveluiden, korjaamisesta. Tämä suoritetaan AWS:n käytännön sekä ISO 27001-, NIST- ja PCI-vaatimusten mukaisesti.

7 Valvotaanko ja hallitaanko etuoikeutettujen tehtävien suorittamista?
Käytössä olevat valvontamenetelmät rajoittavat järjestelmien ja tietojen käyttöä tai tietoja valvotaan ja niiden käyttö estetään. Tämän lisäksi asiakkaan tiedot ja palvelinesiintymät eristetään oletusarvoisesti ja loogisesti muista asiakkaista. Riippumaton tarkastaja tarkistaa etuoikeutettujen käyttäjien pääsynvalvonnan AWS SOC 1-, ISO 27001-, PCI, ITAR- ja FISMA-tarkastusten aikana.

8 Estääkö pilvipalveluiden tarjoaja asiakkaan tietoihin ja sovelluksiin kohdistuvan asiattoman sisäpiirin käytön?
AWS antaa erityisiä SOC 1 -ohjeita SOC 1, Type 2 -raportissa (aws.amazon.com/security/). Tämän lisäksi Adobe suorittaa ajoittain riskien arvioinnin selvittääkseen, miten sisäpiirin käyttöä hallitaan ja valvotaan.

9 Miten Creative Cloud eristää asiakkaan tiedot?
Kaikkiin Adoben asiakkaiden puolesta tallentamiin tietoihin sovelletaan vuokraajan eristämiseen tarkoitettuja vahvoja suojaus- ja hallintatoimintoja. Creative Cloud Storage perustuu Amazon S3:een, jossa on kehittyneitä pääsynvalvontamenetelmiä.

10 Onko asiakkaiden eristäminen toteutettu turvallisesti?
AWS on usean vuokraajan virtualisoitu ympäristö. AWS:ssä käytetään tietoturvan hallintaprosesseja, PCI-valvontamenetelmiä ja muita tietoturvaan liittyviä valvontamenetelmiä, joiden tarkoituksena on eristää asiakkaat toisistaan. AWS-järjestelmät on suunniteltu estämään asiakkaita käyttämästä fyysisiä palvelimia tai esiintymiä ilman lupaa virtualisointiohjelmiston avulla toteutetun suodatuksen avulla. Riippumaton PCI Qualified Security Assessor (QSA) -tarkastaja on tarkistanut tämän arkkitehtuurin ja todennut sen vastaavan kaikkia PCI DSS 2.0 -standardin vaatimuksia (aws.amazon.com/security/pci-dss-level-1-compliance-faqs/).

11 Onko AWS puuttunut tunnettuihin hypervisorin haavoittuvuuksiin?
Amazon EC2 käyttää tällä hetkellä Xen-hypervisorin erittäin mukautettua versiota. Riippumattomat tarkastajat määrittävät AWS:n Xen-hypervisorin turvallisuuden säännöllisesti arviointien ja tarkastusten aikana. Lisätietoja Xen-hypervisorista ja esiintymien eristämisestä on AWS:n tietoturvaa käsittelevässä tutkimusraportissa (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf).

12 Tukevatko palvelut salausta?
Creative Cloud salaa siirrettävät tiedot SSL-protokollan avulla.

13 Mitä oikeuksia pilvipalveluiden tarjoajalla on asiakkaan tietoihin?
Tietojen hallinta- ja omistusoikeudet säilyvät Creative Cloud -asiakkailla. Lisätietoja saat perehtymällä Adoben käyttöehtoihin (www.adobe.com/go/gffooter_terms_of_use) ja tietosuojakäytäntöön (www.adobe.com/privacy/policy.html).

14 Julkaiseeko AWS fyysiset ja ympäristönsuojeluun liittyvät valvontamenetelmänsä?
Kyllä. Fyysiset ja ympäristönsuojeluun liittyvät valvontamenetelmät on esitetty SOC 1, Type 2 -raportissa (aws.amazon.com/security/). Tämän lisäksi AWS tukee ISO 27001- ja FISMA-sertifiointeja, jotka edellyttävät fyysisten ja ympäristönsuojeluun liittyvien valvontamenetelmien parhaiden käytäntöjen noudattamista.

15 Voivatko asiakkaat suojata ja hallita Creative Cloudin käyttöä asiakaslaitteista, kuten tietokoneista ja mobiililaitteista?
Kyllä. Creative Cloud antaa asiakkaille mahdollisuuden hallita asiakas- ja mobiililaitteiden käyttöä omien vaatimustensa mukaan.

16 Antaako AWS asiakkaiden suojata virtuaaliset palvelimensa?
Kyllä. Adobe on lisännyt AWS:n päälle oman tietoturva-arkkitehtuurinsa, joka perustuu alan parhaisiin käytäntöihin, muun muassa SANS:n Internet-tietoturvan 20 tärkeimpään valvontamenetelmään, Consensus Audit Guidelinesiin, NIST:n ohjeisiin ja Internet-standardeihin.

17 Sisältääkö AWS käyttäjätietojen hallinta- ja pääsynvalvontatoimintoja (IAM)?
AWS:ssä on useita käyttäjätietojen hallinta- ja pääsynvalvontatoimintoja, joiden avulla Adobe pystyy hallitsemaan käyttäjätietoja, määrittämään suojausvaltuuksia, järjestämään asiakkaita ryhmiin ja hallitsemaan käyttäjien käyttöoikeuksia keskitetysti.

18 Sammuttaako Adobe Creative Cloud -järjestelmät ylläpidon vuoksi?
Creative Cloud on toteutettu niin, että käyttökatkoja ei käytännössä ole. Palveluiden pitäisi olla käytettävissä ja tavoitettavissa myös uusien käyttöönottojen aikana, sillä A/B-ympäristöt ja muut mekanismit mahdollistavat reaaliaikaiset siirtymät ilman ulkoisesti näkyviä käyttökatkoja.

19 Miten AWS on suojattu Distributed Denial Of Service (DDoS) -hyökkäyksiä vastaan?
AWS-verkko on suojattu tehokkaasti verkossa piileviä perinteisiä tietoturvauhkia vastaan. Lisätietoja tästä aiheesta, myös DDoS-hyökkäyksistä, on AWS:n tietoturvaa käsittelevässä tutkimusraportissa (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf).

20 Onko Adobella toiminnan jatkuvuussuunnitelmaa Creative Cloudille?
AWS:llä on toiminnan jatkuvuussuunnitelma (media.amazonwebservices.com/AWS_Disaster_Recovery.pdf), ja Creative Cloud on suunniteltu toimimaan useilla alueilla ja useilla käytettävyysalueilla tai tietokeskuksissa. Adobe on suunnitellut ja toteuttanut Creative Cloudin niin, että siinä hyödynnetään redundanttien tietojen replikointia sekä useaan alueeseen ja käytettävyysalueeseen perustuvia käyttöönottoarkkitehtuureja.

21 Määrittääkö AWS tietojen säilyvyyden?
Creative Cloud tallentaa tiedot Amazon S3:een, joka on kestävä tallennusinfrastruktuuri. Objektit tallennetaan Amazon S3:n alueella useisiin laitteisiin ja toimipisteisiin. Tietojen tallennuksen jälkeen Amazon S3 varmistaa objektien säilyvyyden menetetyn redundanttisuuden nopealla tunnistuksella ja korjauksella. Amazon S3 tarkistaa säännöllisesti myös tietojen eheyden tarkistussummien avulla. Jos se havaitsee tietojen vioittuneen, se korjaa ne redundanttien tietojen avulla.

22 Aikooko Adobe hankkia Federal Information Security Management Act (FISMA) -sertifioinnin?
Adobella ei ole välittömiä suunnitelmia hankkia Federal Information Security Management Act (FISMA) -sertifiointia Creative Cloudille.

23 Vastaako Creative Cloud HIPAA-määräyksiä?
Adobe ei aio sertifioida Creative Cloudia vuoden 1996 Health Insurance Portability and Accountability Act (HIPAA) -säädösten mukaan, sillä Creative Cloudia ei ole tarkoitettu potilastietojen käsittelyyn.

Viittaukset

Overview of AWS Security Practices -tutkimusraportti, maaliskuu 2013 (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf)

AWS Risk and Compliance -tutkimusraportti, tammikuu 2013 (media.amazonwebservices.com/AWS_Risk_and_Compliance_Whitepaper.pdf)

Adobe

Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
Yhdysvallat
www.adobe.com