Vanliga frågor om säkerheten i Adobe Creative Cloud Security för IT

Säkerhet, sekretess och efterlevnadspolicyer hör till de vanligaste ämnena för de frågor som Adobe får om Creative Cloud. Företag som använder Creative Cloud har funderingar kring hur säkra deras data är och om tillgången till dessa data är pålitlig. I detta dokument försöker vi besvara många av de vanliga frågor som ställs av IT-säkerhetspersonal när företaget överväger att börja använda Creative Cloud.

1 Var befinner sig de servrar där Creative Cloud lagras?

Creative Cloud har Amazon Web Services (AWS) som värd, däribland Amazon Elastic Compute Cloud (Amazon EC2) och Amazon Simple Storage Service (Amazon S3), i USA, EU och Asien/Stillahavs-regionen. AWS erbjuder en tillförlitlig plattform för programvarutjänster som används av tusentals företag över hela världen. AWS tillhandahåller sina tjänster i enlighet med de bästa metoderna för säkerhet och genomgår certifieringar och granskningar som är erkända inom branschen (aws.amazon.com/security/). Det innebär att Creative Cloud-medlemmarna kan dra fördel av Amazons kontinuerliga säkerhetsarbete för de tillgångar som de har lagrade.

2 Var befinner sig kundernas data?

Kundernas data lagras i Amazon S3 och Adobe anger i vilken fysisk region som enskilda kunders data och servrar ska finnas. Datareplikering för Amazon S3-dataobjekt görs inom det regionala kluster där de aktuella data lagras, och replikeringen sker inte till datacenterkluster i andra regioner. Adobe driver Creative Cloud från tre regioner: USA, EU och Asien/Stillahavs-regionen.

Exempel: Som standard lagras alla data som härrör från Creative Cloud-kunder inom EU som molndata i AWS-datacentret i EU och dessa data kommer inte att överföras till datacenter utanför EU.

3 Vem kontrollerar Creative Cloud-datacentren?

För de delar av Creative Cloud som distribuerats i AWS kontrollerar Amazon de fysiska komponenterna. För att kunderna lättare ska kunna förstå vilken typ av kontroller som AWS har och hur effektivt de fungerar publicerar AWS en Service Organization Controls 1 (SOC 1), Type 2-rapport (aws.amazon.com/security/) med de kontroller som definierats kring Amazon EC2, Amazon S3 och VPC (Virtual Private Cloud), samt ingående information om fysisk säkerhet och miljökontroller. Dessa kontroller är noggrant specificerade på en nivå som bör uppfylla de flesta kunders behov.

4 Tillåter Amazon visningar för kunderna på AWS datacenter?

Nej. Eftersom AWS datacenter är värd för data för flera olika kunder tillåter AWS inte visningar för kunder, eftersom detta skulle utsätta många olika kunder för risken att en tredje part skulle få fysisk åtkomst till data. För att uppfylla detta kundbehov validerar en oberoende och behörig granskare att kontrollerna finns och fungerar som en del av en SOC 1, Type 2-rapport. Denna allmänt accepterade tredje parts-validering ger kunderna en oberoende insyn i hur effektiva de implementerade kontrollerna är. Adobe har undertecknat ett sekretessavtal med AWS och kan få en kopia av SOC 1 Type 2-rapporten (aws.amazon.com/security/). Oberoende granskningar av den fysiska säkerheten på datacentren ingår också i AWS ISO 27001-granskningen, PCI-utvärderingen och ITAR-granskningsprocessen.

5 Har tredje part tillträde till AWS datacenter?

AWS kontrollerar mycket noggrant tillträdet till datacentren, även för de egna anställda. Tredje part ges inte tillträde till AWS datacenter när detta inte uttryckligen godkänts av rätt AWS-datacenterchef i enlighet med AWS åtkomstpolicy. Se SOC 1, Type 2-rapporten (aws.amazon.com/security/) för mer information om specifika kontroller som rör fysiskt tillträde, auktorisering för tillträde till datacenter och andra relaterade kontroller.

6 Vem ansvarar för korrigering av filer?

Adobe ansvarar för korrigeringar av våra egna gästoperativsystem (OS) och program som körs i AWS. AWS ansvarar för korrigeringar i de system som levererar AWS tjänster, till exempel hypervisor- och nätverkstjänsterna. Detta sker i enlighet med kraven i AWS policy och i ISO 27001, NIST och PCI.

7 Övervakas och kontrolleras behöriga åtgärder?
De implementerade kontrollerna begränsar åtkomsten till system och till data, eller så är data begränsade och övervakade. Dessutom är en kunds data och serverinstanser som standard logiskt isolerade från andra kunders. Åtkomstkontroll för behöriga användare till AWS-infrastrukturen granskas av en oberoende granskare i samband med granskningarna SOC 1, ISO 27001, PCI, ITAR och FISMA.

8 Tar molnleverantören hänsyn till hotet om otillbörlig insideråtkomst till kundernas data och program?
AWS tillhandahåller specifika SOC 1-kontroller som tas upp i SOC 1, Type 2-rapporten (aws.amazon.com/security/). Dessutom utför Adobe regelbundna riskbedömningar av hur insideråtkomst kontrolleras och övervakas.

9 Hur isolerar Creative Cloud kundernas data?
Alla data som lagras av Adobe för kundernas räkning har kraftfulla säkerhets- och kontrollfunktioner för isolering av innehavarna. För Creative Cloud-lagringen används Amazon S3, som ger avancerade kontroller för dataåtkomst.

10 Har kundsegregeringen implementerats på ett säkert sätt?
AWS-miljön är en virtualiserad multi-innehavarmiljö. AWS har implementerat säkerhetshanteringsprocesser, PCI-kontroller och andra säkerhetskontroller som utformats för att isolera alla kunderna från varandra. AWS system har utformats för att förhindra kunderna från att få åtkomst till fysiska värdar eller instanser som inte tilldelats dem genom filtrering via virtualiseringsprogramvaran. Denna arkitektur har validerats av en oberoende PCI Qualified Security Assessor (QSA) och befunnits uppfylla alla kraven i PCI DSS 2.0 (aws.amazon.com/security/pci-dss-level-1-compliance-faqs/).

11 Har AWS hanterat kända svagheter i hypervisorn?
Amazon EC2 använder för närvarande en mycket specialanpassad version av Xen-hypervisorn. Säkerheten i AWS Xen-hypervisor utvärderas regelbundet av oberoende granskare vid utvärderingar och granskningar. Se AWS whitepaper om säkerhet (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf) om du vill ha mer information om Xen-hypervisorn och instansisolering.

12 Har de levererade tjänsterna stöd för kryptering?
Creative Cloud krypterar data som överförs med SSL.

13 Vad har molnleverantören för rätt till kundernas data?
Creative Cloud-kunderna behåller kontrollen över och ägarskapet av sina data. Läs Adobes användarvillkor (www.adobe.com/go/gffooter_terms_of_use) och integritetspolicy (www.adobe.com/privacy/policy.html) om du vill ha mer information.

14 Publicerar AWS sina fysiska kontroller och miljökontroller?
Ja. Fysiska kontroller och miljökontroller beskrivs i en SOC 1, Type 2-rapport. (aws.amazon.com/security/). Dessutom har AWS stöd för ISO 27001- och FISMA-certifiering, och för det krävs det fysiska kontroller och miljökontroller som är bästa metoder.

15 Kan kunderna säkra och hantera åtkomsten till Creative Cloud från klienter som PC-datorer och mobilenheter?
Ja. Creative Cloud låter kunderna hantera klient- och mobilåtkomst efter sina egna behov.

16 Tillåter AWS kunderna att säkra sina virtuella servrar?
Ja. Adobe har implementerat sin egen säkerhetsarkitektur ovanpå AWS i enlighet med branschens bästa metoder, däribland SANS Top 20 Controls for Internet Security, Consensus Audit Guidelines, NIST-riktlinjer och Internetstandarder.

17 Har AWS inkluderat funktioner för identitets- och åtkomsthantering (IAM – Identity and Access Management)?
AWS erbjuder en serie funktioner för identitets- och åtkomsthantering som låter Adobe hantera användaridentiteter, tilldela säkerhetsautentiseringsuppgifter, organisera användare i grupper och hantera användarbehörigheter centralt.

18 Kommer Adobe att ta ned Creative Cloud-systemen för underhåll?
Creative Cloud har implementerats för att mer eller mindre helt eliminera driftavbrott. Tjänsterna ska gå att nå under nydistributioner, tack vare användandet av A/B-miljöer och andra mekanismer som möjliggör en live-snabbmigrering med så gott som inget driftavbrott som syns externt.

19 Hur skyddar AWS sig mot DDoS-angrepp (Distributed Denial Of Service)?
AWS-nätverket har ett betydande traditionellt nätverksskydd. Se AWS whitepaper om säkerhet (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf) för mer information om detta ämne, med bland annat en diskussion om DDoS.

20 Har Adobe en affärskontinuitetsplan för Creative Cloud?
AWS erbjuder ett affärskontinuitetsprogram (media.amazonwebservices.com/AWS_Disaster_Recovery.pdf) och Creative Cloud har utformats för att köras från flera regioner och flera tillgänglighetszoner, eller datacenter. Adobe har utformat och implementerat Creative Cloud till att använda replikering för dataredundans och zondistributionsarkitekturer för multiregion/tillgänglighet.

21 Har AWS specificerat datahållbarheten?
Creative Cloud lagrar data i Amazon S3, som ger en hållbar lagringsinfrastruktur. Objekt lagras på ett redundant sätt på flera enheter i flera olika anläggningar i en Amazon S3-region. När data väl har lagrats gör Amazon S3 objekten hållbara genom att snabbt känna av och reparera eventuell förlorad redundans. Amazon S3 verifierar också regelbundet integriteten för lagrade data med hjälp av kontrollsummor. Om skador upptäcks repareras de med hjälp av redundanta data.

22 Planerar Adobe att efterleva Federal Information Security Management Act (FISMA)?
Adobe har för närvarande inga planer på att efterleva Federal Information Security Management Act (FISMA) för Creative Cloud.

23 Efterlever Creative Cloud HIPAA?
Adobe har ingen avsikt att certifiera Creative Cloud för efterlevnad av Health Insurance Portability and Accountability Act of 1996 (HIPAA) eftersom Creative Cloud inte är avsett för bearbetning av patienthandlingar.

Referenser

Overview of AWS Security Practices Whitepaper, mars 2013
(media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf)

AWS Risk and Compliance Whitepaper, januari 2013
(media.amazonwebservices.com/AWS_Risk_and_Compliance_Whitepaper.pdf)

Adobe

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