Adobe Creative Cloud Veelgestelde vragen over beveiliging voor ICT

Beveiliging, privacy en nalevingsbeleid zijn onderwerpen waarover Adobe met betrekking tot Creative Cloud veelvuldig vragen ontvangt. Organisaties die Creative Cloud gebruiken, vinden de veiligheid van hun gegevens zeer belangrijk en willen betrouwbare toegang tot hun gegevens. Dit document is bedoeld om een groot aantal van de veelgestelde vragen te beantwoorden die ICT-beveiligingsmedewerkers hebben als ze de aanschaf van Creative Cloud overwegen.

1 Waar wordt Creative Cloud gehost?
Creative Cloud wordt gehost op Amazon Web Services (AWS), waaronder Amazon Elastic Compute Cloud (Amazon EC2) en Amazon Simple Storage Service (Amazon S3), in de Verenigde Staten, de Europese Unie en de regio Azië en Stille Oceaan. AWS biedt een betrouwbaar platform voor softwareservices die worden gebruikt door duizenden bedrijven over de hele wereld. AWS levert services conform de aanbevolen beveiligingsprocedures en wordt onderworpen aan door de branche erkende certificerings- en controleprogramma's (aws.amazon.com/security/). Dit betekent dat Creative Cloud-leden profiteren van de voortdurende inzet en toewijding van Amazon om te blijven voldoen aan de aanbevolen beveiligingsprocedures voor opgeslagen middelen.

2 Waar worden de klantgegevens bewaard?
Klantgegevens worden opgeslagen in Amazon S3 en Adobe bepaalt de fysieke regio waarin de gegevens en servers van afzonderlijke klanten zich bevinden. Gegevensreplicatie voor Amazon S3-gegevensobjecten wordt uitgevoerd binnen de regionale cluster waar de gegevens zijn opgeslagen. Gegevens worden niet gerepliceerd naar datacenters in andere regio's. Adobe verzorgt Creative Cloud vanuit drie regio's: de Verenigde Staten, de Europese Unie en Azië en Stille Oceaan.

Voorbeeld: de cloudgegevens van alle Creative Cloud-klanten binnen de Europese Unie worden standaard opgeslagen in het AWS-datacenter in de Europese Unie en gegevens worden niet overgedragen naar datacenters buiten deze regio.

3 Wie beheert de Creative Cloud-datacenters?
Voor onderdelen van Creative Cloud die in AWS zijn geïmplementeerd, beheert Amazon de fysieke componenten. Om klanten meer inzicht te geven in de controlemechanismen die AWS hanteert en hoe effectief deze werken, publiceert AWS een SOC 1 Type 2-rapport (Service Organization Controls) (aws.amazon.com/security/) waarin de controlemechanismen voor Amazon EC2, Amazon S3 en Virtual Private Cloud (VPC) zijn gedefinieerd, samen met fysieke beveiligings- en omgevingscontrolemechanismen. Deze controlemechanismen zijn uiterst specifiek gedefinieerd om te voldoen aan de meeste klanteisen.

4 Staat Amazon rondleidingen voor klanten toe in de AWS-datacenters?
Nee. Omdat in AWS-datacenters gegevens van meerdere klanten worden gehost, staat AWS geen datacenterrondleidingen voor klanten toe omdat hierdoor veel klanten worden blootgesteld aan het risico dat derden fysiek toegang krijgen tot de datacenters. Om aan deze klanteis te voldoen, worden de aanwezigheid en werking van controlemechanismen gecontroleerd door een onafhankelijke en competente auditor als onderdeel van het SOC 1 Type 2-rapport. De algemeen geaccepteerde validatie door derden biedt klanten een onafhankelijke visie op de effectiviteit van de geïmplementeerde controlemechanismen. Adobe heeft een geheimhoudingsverklaring met AWS ondertekend en kan een exemplaar opvragen van het SOC 1 Type 2-rapport (aws.amazon.com/security/). Onafhankelijke controles van de fysieke datacenterbeveiliging zijn ook onderdeel van de ISO 27001-audit van AWS, het PCI-assessment en de ITAR-auditprocedure.

5 Krijgen derden toegang tot AWS-datacenters?
AWS hanteert strenge regels voor toegang tot datacenters, zelfs voor interne werknemers. Derden krijgen geen toegang tot AWS-datacenters, tenzij ze expliciet zijn goedgekeurd door de juiste manager van het AWS-datacenter conform het toegangsbeleid van AWS. Raadpleeg het SOC 1 Type 2-rapport (aws.amazon.com/security/) voor specifieke controlemechanismen met betrekking tot fysieke toegang, autorisatie voor datacentertoegang en verwante controlemechanismen.

6 Wie is verantwoordelijk voor patching?
Adobe is verantwoordelijk voor patching van onze eigen gastbesturingssystemen (OS), software en toepassingen die worden uitgevoerd in AWS. AWS is verantwoordelijk voor patching van systemen die de levering van AWS-services ondersteunen, zoals de hypervisor- en netwerkservices. Dit wordt gedaan conform de vereisten van het AWS-beleid en van ISO 27001, NIST en PCI.

7 Hoe worden handelingen met verhoogde gebruikersbevoegdheden bewaakt en beheerd?
Er zijn controlemechanismen ingesteld waarmee toegang tot systemen en gegevens of alleen gegevens wordt beperkt en bewaakt. Daarnaast worden de gegevens- en serverinstanties van de klant standaard logistiek afgeschermd van die van andere klanten. Voor de AWS-infrastructuur wordt de toegangscontrole voor bevoegde gebruikers gecontroleerd door een onafhankelijke auditor tijdens de SOC 1-, ISO 27001-, PCI-, ITAR- en FISMA-audits van AWS.

8 Heeft de cloudaanbieder het risico van ongeoorloofde toegang tot gegevens en toepassingen van klanten door insiders afgedekt?
AWS hanteert specifieke SOC 1-maatregelen die zijn uiteengezet in het SOC 1 Type 2-rapport (aws.amazon.com/security/). Daarnaast voert Adobe periodiek risicobeoordelingen uit voor de wijze waarop toegang door insiders wordt beheerd en bewaakt.

9 Hoe isoleert Creative Cloud de klantgegevens?
Voor alle gegevens die door Adobe worden opgeslagen namens klanten, worden krachtige beveiligings- en beheerfuncties voor isolatie van tenants gebruikt. Voor Creative Cloud-opslag wordt Amazon S3 gebruikt, dat geavanceerde functionaliteit voor toegangscontrole van gegevens biedt.

10 Is de scheiding van klanten veilig geïmplementeerd?
De AWS-omgeving is een gevirtualiseerde omgeving met meerdere tenants. AWS heeft beveiligingsbeheerprocessen, PCI-besturingselementen en andere controlemechanismen voor beveiliging geïmplementeerd waarmee elke klant wordt gescheiden van de overige klanten. AWS-systemen zijn ontworpen om te voorkomen dat klanten toegang kunnen krijgen tot fysieke hosts of instanties die niet aan hen zijn toegewezen. Hiervoor worden filters in de virtualisatiesoftware gebruikt. Deze architectuur is gevalideerd door een onafhankelijke PCI Qualified Security Assessor (QSA) en voldoet aan alle vereisten van PCI DSS 2.0 (aws.amazon.com/security/pci-dss-level-1-compliance-faqs/).

11 Heeft AWS een oplossing voor de bekende hypervisorkwetsbaarheden?
Amazon EC2 gebruikt momenteel een sterk aangepaste versie van de Xen-hypervisor. De beveiliging van de Xen-hypervisor van AWS wordt periodiek geëvalueerd door onafhankelijke auditors tijdens assessments en audits. Raadpleeg het AWS-beveiligingsdocument (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf) voor meer informatie over de Xen-hypervisor en isolatie van instanties.

12 Ondersteunen de geleverde services codering?
Creative Cloud codeert gegevens tijdens overdracht met SSL.

13 Welke rechten heeft de cloudaanbieder met betrekking tot klantgegevens?
Creative Cloud-klanten behouden de controle over en eigendom van hun gegevens. Lees de gebruiksvoorwaarden (www.adobe.com/go/gffooter_terms_of_use) en het privacybeleid (www.adobe.com/privacy/policy.html) van Adobe voor meer informatie.

14 Publiceert AWS de fysieke en omgevingscontrolemechanismen?
Ja. Fysieke en omgevingscontrolemechanismen zijn uiteengezet in een SOC 1 Type 2-rapport (aws.amazon.com/security/). Daarnaast ondersteunt AWS de ISO 27001- en FISMA-certificering waarvoor de aanbevolen procedures voor fysieke en omgevingscontrolemechanismen vereist zijn.

15 Kunnen klanten de toegang tot Creative Cloud beveiligen en beheren met clients zoals pc's en mobiele apparaten?
Ja. Klanten kunnen mobiele en clienttoegang tot Creative Cloud beheren volgens hun eigen vereisten.

16 Staat AWS toe dat klanten hun virtuele servers beveiligen?
Ja. Adobe heeft zijn eigen beveiligingsarchitectuur geïmplementeerd op AWS op basis van de aanbevolen brancheprocedures, waaronder SANS Top 20 Controls for Internet Security, Consensus Audit Guidelines, NIST-richtlijnen en internetstandaarden.

17 Biedt AWS functionaliteit voor identiteits- en toegangsbeheer (IAM)?
AWS bevat een suite met functies voor identiteits- en toegangsbeheer waarmee Adobe via één centrale methode gebruikersidentiteiten en -machtigingen kan beheren, beveiligingsreferenties kan toewijzen en gebruikers in groepen kan indelen.

18 Gaat Adobe Creative Cloud-systemen offline halen voor onderhoud?
Creative Cloud is zo geïmplementeerd dat de uitvaltijd vrijwel tot nul wordt teruggebracht. Tijdens nieuwe implementaties zouden de services toegankelijk en bereikbaar moeten zijn door het gebruik van A/B-omgevingen en andere mechanismen die ervoor zorgen dat live-cutover kan worden uitgevoerd zonder extern zichtbare uitvaltijd.

19 Welke beveiliging biedt AWS tegen DDoS-aanvallen (Distributed Denial Of Service)?
Het AWS-netwerk biedt geavanceerde bescherming tegen traditionele netwerkbeveiligingsproblemen. Raadpleeg het AWS-beveiligingsdocument (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf) voor meer informatie over dit onderwerp, waaronder een discussie over DDoS.

20 Heeft Adobe een bedrijfscontinuïteitsplan voor Creative Cloud?
AWS biedt een bedrijfscontinuïteitsprogramma (media.amazonwebservices.com/AWS_Disaster_Recovery.pdf) en Creative Cloud is ontworpen om te worden uitgevoerd vanuit meerdere regio's en beschikbaarheidszones of datacenters. Adobe heeft Creative Cloud ontworpen, gebouwd en geïmplementeerd voor gebruik van redundante-gegevensreplicatie en implementatiearchitecturen met meerdere regio's en beschikbaarheidszones.

21 Geeft AWS specificaties voor houdbaarheid van gegevens?
Creative Cloud slaat gegevens op in Amazon S3, dat voorziet in een duurzame opslaginfrastructuur. Objecten worden redundant opgeslagen op meerdere apparaten in verschillende faciliteiten in een Amazon S3-regio. Nadat de gegevens zijn opgeslagen, waarborgt Amazon S3 de houdbaarheid van objecten door redundantiefouten snel op te sporen en te herstellen. Amazon S3 controleert ook regelmatig de integriteit van opgeslagen gegevens met controlesommen. Als er beschadigde gegevens zijn gedetecteerd, worden deze hersteld met redundante gegevens.

22 Is Adobe van plan om FISMA-certificering (Federal Information Security Management Act) te behalen?
Adobe heeft geen directe plannen om FISMA-certificering (Federal Information Security Management Act) te behalen voor Creative Cloud.

23 Voldoet Creative Cloud aan HIPAA?
Adobe is niet van plan voor Creative Cloud een HIPAA-certificering conform de Health Insurance Portability and Accountability Act uit 1996 te behalen, omdat Creative Cloud niet bedoeld is voor verwerking van informatie met betrekking tot de gezondheidszorg.

Referenties

Overzichtsdocument voor beveiligingsbeleid van AWS (Engelstalig), maart 2013
(media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf)

Document over AWS-programma voor risicobeheer en naleving (Engelstalig), 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