Ofte stillede spørgsmål om sikkerheden i Adobe Creative Cloud (til it)

Spørgsmål til områderne politikker for sikkerhed, beskyttelse af personlige oplysninger og overensstemmelse er nogle af dem, Adobe oftest modtager om Creative Cloud. Organisationer, der bruger Creative Cloud, bekymrer sig om sikkerheden for deres data, og om der er pålidelig adgang til dataene. Dette dokument forsøger at besvare mange af de ofte stillede spørgsmål fra it-sikkerhedsmedarbejdere om disse emner, som bliver stillet, når de overvejer Creative Cloud.

1 Hvor hostes Creative Cloud?
Creative Cloud hostes hos Amazon Web Services (AWS), herunder Amazon Elastic Compute Cloud (Amazon EC2) og Amazon Simple Storage Service (Amazon S3), i USA, Europa og Asien og Stillehavsområdet. AWS tilbyder en pålidelig platform for softwaretjenester, der bruges af tusindvis af virksomheder i hele verden. AWS leverer tjenester, der overholder de bedste fremgangsmåder for sikkerhed og er underlagt brancheanerkendte certificeringer og gennemgange (aws.amazon.com/security/). Det betyder, at Creative Cloud-medlemmer drager fordel af Amazons vedvarende arbejde med sikkerhedsrutiner for lagrede oplysninger.

2 Hvor opbevares kundedataene?
Kundedata lagres i Amazon S3, og Adobe angiver, i hvilket fysisk område den enkelte kundes data og servere skal placeres. Datareplikering af Amazon S3-dataobjekter sker i den områdeklynge, hvor dataene lagres, og de replikeres ikke til datacenterklynger i andre områder. Adobe driver Creative Cloud fra tre områder: USA, EU og Asien og Stillehavsområdet.

Eksempel: Som standard vil alle data fra Creative Cloud-kunder i EU være lagret i AWS-datacentret i EU, og disse data vil ikke blive overført til datacentre uden for EU.

3 Hvem styrer Creative Cloud-datacentrene?
Hvad angår de dele af Creative Cloud, der er installeret hos AWS, så styrer Amazon de fysiske komponenter. For at give kunderne en bedre forståelse af, hvilke kontrolfunktioner AWS har implementeret, og hvor effektivt de fungerer, udgiver AWS en Service Organization Controls 1 (SOC 1), Type 2-rapport (aws.amazon.com/security/) med kontrolfunktionerne, der er defineret for Amazon EC2, Amazon S3 og VPC (Virtual Private Cloud), samt med detaljerede kontrolfunktioner for fysisk sikkerhed og miljø. Disse kontrolfunktioner er defineret på et højt specifikationsniveau, der skulle opfylde de fleste kundebehov.

4 Tillader Amazon kunderundvisninger i AWS-datacentre?
Nej. Med udgangspunkt i det faktum, at AWS-datacentre hoster data for flere kunder, tillader AWS ikke rundvisninger af kunder, da det udsætter en lang række kunder for fysisk adgang af en tredjepart. For at opfylde dette kundebehov validerer en uafhængig og kvalificeret auditor tilstedeværelsen og driften af kontrolfunktionerne som en del af en SOC 1, Type 2-rapport. Denne tredjepartsvalidering, der er bredt accepteret, giver kunderne en uafhængig vurdering af effektiviteten af de implementerede kontrolfunktioner. Adobe har underskrevet en aftale om hemmeligholdelse med AWS og kan få en kopi af SOC 1 Type 2-rapporten (aws.amazon.com/security/). Uafhængige gennemgange af datacentrets fysiske sikkerhed er også en del af AWS ISO 27001-revisionen, PCI-vurderingen og ITAR-revisionsprocessen.

5 Har tredjeparter adgang til AWS-datacentre?
AWS fører en streng kontrol med adgangen til datacentrene, selv for egne ansatte. Tredjeparter har ikke adgang til AWS-datacentre med undtagelse af, når det udtrykkeligt er godkendt af den relevante AWS-datacenterchef i henhold til adgangspolitikken for AWS. Se SOC 1, Type 2-rapporten (aws.amazon.com/security/) for at få oplysninger om specifikke kontrolfunktioner med hensyn til fysisk adgang, autorisation af adgang til datacenter og andre relaterede kontrolfunktioner.

6 Hvem er ansvarlig for opdateringer?
Adobe er ansvarlig for opdatering af vores egne gæsteoperativsystemer (OS), software og programmer, der kører i AWS. AWS er ansvarlig for opdatering af de systemer, der understøtter leveringen af AWS-tjenester, f.eks. hypervisor- og netværkstjenester. Dette sker efter behov i henhold til AWS-politik og i overensstemmelse med kravene i ISO 27001, NIST og PCI.

7 Overvåges og kontrolleres handlinger, der kræver særlig tilladelse?
De implementerede kontrolfunktioner begrænser adgangen til systemer og data, eller der er begrænset og overvåget adgang til dataene. Desuden er kundedata og serverforekomster som standard isoleret fra andre kunder. Adgangskontrollen for brugere med særlige rettigheder til AWS-infrastrukturen kontrolleres af en uafhængig revisor i forbindelse med AWS SOC 1-, ISO 27001-, PCI-, ITAR- og FISMA-gennemgangene.

8 Er skyudbyderen opmærksom på truslen om upassende insideradgang til kundedata og -programmer?
AWS sørger for specifik SOC 1, der er dækket i SOC 1, Type 2-rapporten (aws.amazon.com/security/). Desuden gennemfører Adobe periodevise risikovurderinger af, hvordan insideradgangen kontrolleres og overvåges.

9 Hvordan isolerer Creative Cloud kundedata?
Alle data, der lagres af Adobe på kundernes vegne, har stærke sikkerheds- og kontrolfunktioner, der isolerer lejeren. Creative Cloud-lagring benytter Amazon S3, der sørger for avancerede dataadgangskontrolfunktioner.

10 Er kundeopdeling implementeret sikkert?
AWS-miljøet er et virtualiseret miljø med flere lejere. AWS har implementeret processer til sikkerhedsstyring, PCI-kontrolfunktioner og andre sikkerhedskontrolfunktioner, der skal isolere den enkelte kunde fra de andre. AWS-systemer er designet til forhindre kunder i at få adgang til fysiske værter eller forekomster, der ikke er tilknyttet til dem, gennem filtrering i virtualiseringssoftwaren. Denne arkitektur er blevet valideret af en uafhængig PCI Qualified Security Assessor (QSA), og resultatet var, at den var i overensstemmelse med alle krav i PCI DSS 2.0 (aws.amazon.com/security/pci-dss-level-1-compliance-faqs/).

11 Har AWS løst kendte hypervisor-sårbarheder?
Amazon EC2 benytter i øjeblikket en meget tilpasset version af Xen-hypervisoren. Sikkerheden i AWS' Xen-hypervisor vurderes med jævne mellemrum af uafhængige revisorer i forbindelse med gennemgange og revisioner. Se AWS-hvidbogen om sikkerhed (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf) for at få flere oplysninger om Xen-hypervisoren og isolering af forekomster.

12 Understøtter den leverede tjeneste kryptering?
Creative Cloud krypterer data i overførsel med SSL.

13 Hvilke rettigheder har skyudbyderen over kundedataene?
Creative Cloud-kunder bevarer kontrollen over og ejerskabet til deres data. Læs Adobes vilkår for brug (www.adobe.com/go/gffooter_terms_of_use) og politik for beskyttelse af personlige oplysninger (www.adobe.com/privacy/policy.html) for at få flere oplysninger.

14 Offentliggør AWS oplysninger om deres fysiske og miljømæssige kontrolfunktioner?
Ja. De fysiske og miljømæssige kontrolfunktioner er specifikt beskrevet i en SOC 1, Type 2-rapport (aws.amazon.com/security/). Desuden understøtter AWS ISO 27001- og FISMA-certificeringer, og det kræver fysiske og miljømæssige kontrolfunktioner, der følger de bedste fremgangsmåder.

15 Kan kunderne sikre og administrere adgang til Creative Cloud fra klienter som pc'er og mobile enheder?
Ja. Creative Cloud tillader kunderne at styre adgangen fra klienter og mobile enheder efter deres egne krav.

16 Tillader AWS, at kunderne sikrer deres virtuelle servere?
Ja. Adobe har implementeret sin egen sikkerhedsarkitektur oven på AWS på basis af de bedste fremgangsmåder i branchen, herunder SANS Top 20 Controls for Internet Security, Consensus Audit Guidelines, NIST-retningslinjer og internet-standarder.

17 Omfatter AWS funktioner til styring af identitet og adgang (IAM)?
AWS har en række tilbud til identitets- og adgangsstyring, der tillader Adobe at styre brugeridentiteter, tildele legitimationsoplysninger, organisere brugere i grupper og administrere tilladelser på en centraliseret måde.

18 Lukker Adobe Creative Cloud-systemerne for at foretage vedligeholdelse?
Creative Cloud er implementeret på en sådan måde, at det praktisk taget eliminerer nedetid. Tjenester skulle være tilgængelige og brugbare under nye installationer på grund af brugen af A/B-miljøer og andre mekanismer, der tillader overgange under drift uden nedetid, der er synlig eksternt.

19 Hvordan beskytter AWS mod angreb af distribueret denial-of-service (DDoS)?
AWS-netværket giver en væsentlig beskyttelse mod traditionel netværkssikkerhed. Se AWS-hvidbogen om sikkerhed (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf) for at få flere oplysninger om dette emne, herunder en diskussion af DDoS.

20 Har Adobe en beredskabsplan for Creative Cloud?
AWS tilbyder en beredskabsplan (media.amazonwebservices.com/AWS_Disaster_Recovery.pdf), og Creative Cloud er designet til at køre fra flere områder og flere tilgængelighedszoner eller datacentre. Adobe designede, konstruerede og implementerede Creative Cloud til at bruge dataredundansreplikering og installationsarkitekturer med flere områder/tilgængelighedszoner.

21 Angiver AWS dataholdbarhed?
Creative Cloud lagrer data på Amazon S3, der sørger for en holdbar lagringsinfrastruktur. Objekterne lagres redundant på flere enheder på tværs af flere steder i et Amazon S3-område. Når data er lagret, opretholder Amazon S3 holdbarheden af objekterne ved hurtigt at registrere og reparere enhver mistet redundans. Amazon S3 kontrollerer også jævnligt integriteten af data, der er lagret ved hjælp af kontrolsummer. Hvis der registreres en beskadigelse, repareres den ved hjælp af redundante data.

22 Planlægger Adobe at opnå overensstemmelse med Federal Information Security Management Act (FISMA)?
Adobe har ingen umiddelbare planer om at opnå overensstemmelse med Federal Information Security Management Act (FISMA) for Creative Cloud.

23 Er Creative Cloud HIPAA-kompatibel?
Adobe har ingen plan om at certificere Creative Cloud som kompatibel med Health Insurance Portability and Accountability Act of 1996 (HIPAA), da Creative Cloud ikke er beregnet til at behandle poster, der vedrører sundhedspleje.

Referencer

Oversigt over AWS Security Practices Whitepaper, marts 2013
(media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf)

AWS Risk and Compliance Whitepaper, januar 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/dk