BT için Adobe Creative Cloud Güvenliği Hakkında SSS

Güvenlik, gizlilik ve uyumluluk ilkeleri, Adobe'nin Creative Cloud ile ilgili aldığı sorular arasında en yaygın olanlardan birkaçıdır. Creative Cloud'u kullanan kuruluşlar verilerinin güvenliği ve verilerine erişimin güvenilir olup olmadığı konusuyla ilgilenmektedir. Bu belgede, Creative Cloud'u kullanmayı düşünen BT güvenlik çalışanları tarafından bu konularla ilgili olarak sıklıkla sorulan birçok soruya ilişkin cevaplar sunmak amaçlanmıştır.

1 Creative Cloud nerede barındırılmaktadır?
Creative Cloud; Amerika'da, AB'de ve Asya Pasifik'te Amazon Elastic Compute Cloud (Amazon Elastik Bulut Bilişimi) (Amazon EC2) ve Amazon Simple Storage Service (Amazon Basit Depolama Servisi) (Amazon S3) dahil olmak üzere Amazon Web Servisleri'nde (AWS) barındırılır. AWS, dünya çapında binlerce işletme tarafından kullanılan yazılım hizmetleri için güvenilir bir platform sunar. AWS, güvenlik açısından en iyi uygulamalara uygun şekilde hizmet sunar ve sektörde tanınan sertifikalardan ve denetlemelerden geçer (aws.amazon.com/security/). Bu, Creative Cloud üyelerinin Amazon'un depolama varlıklarına yönelik güvenlik uygulamalarına ilişkin kesintisiz bağlılığından yararlandığı anlamına gelir.

2 Müşteri verileri nerede bulunur?
Müşteri verileri, Amazon S3'te depolanır. Adobe, bireysel müşteri verilerinin ve sunucuların hangi fiziksel bölgede bulunacağını belirler. Amazon S3 veri nesneleri için veri kopyalama işlemi, verilerin depolandığı bölgesel kümede gerçekleştirilir ve diğer bölgelerdeki veri merkezi kümelerine kopyalanmaz. Adobe, Creative Cloud'u üç bölgede çalıştırır: Amerika, AB ve Asya Pasifik.

Örneğin: Varsayılan olarak, AB'deki Creative Cloud müşterilerinin tüm verilerine ilişkin bulut verileri, AB'deki AWS veri merkezinde depolanır ve bu veriler AB dışındaki veri merkezlerine aktarılmaz.

3 Creative Cloud veri merkezlerini kim denetler?
Creative Cloud'un AWS dahilinde dağıtılan kısımları için Amazon, fiziksel bileşenleri denetler. Müşterilerin, AWS'nin ne tür denetimlere sahip olduğunu ve bunların ne kadar etkili çalıştığını daha iyi anlamasına yardımcı olmak için AWS bir Service Organization Controls 1 (Servis Organizasyon Denetimleri (SOC 1)), Tip 2 raporu (aws.amazon.com/security/) ile birlikte Amazon EC2, Amazon S3 ve Sanal Özel Bulut (VPC) ve ayrıntılı fiziksel güvenlik ve ortam denetimleri çerçevesinde belirlenen denetimler yayınlar. Bu denetimler, birçok müşteri ihtiyacını karşılayacak şekilde yüksek kapsam düzeyinde belirlenir.

4 Müşterilerin AWS veri merkezinde gezinmesine Amazon tarafından izin verilir mi?
Hayır. AWS veri merkezlerinin birden fazla müşterinin verilerini barındırması nedeniyle AWS, müşterilerin veri merkezlerinde gezinmesine izin vermez. Aksi takdirde, birçok müşterinin bilgileri üçüncü taraflarca fiziksel olarak erişilecek şekilde savunmasız kalır. Bu müşteri ihtiyacını karşılamak üzere, bağımsız ve yetkin bir denetçi SOC 1, Tip 2 raporunun bir parçası olarak denetimlerin mevcut olduğunu ve çalıştığını doğrular. Yaygın olarak kabul edilen bu üçüncü taraf doğrulaması, müşterilere yerinde denetimlerin etkinliği ile ilgili bağımsız bir perspektif sağlar. Adobe, AWS ile bir gizlilik sözleşmesi imzalamıştır ve SOC 1 Tip 2 raporunun bir kopyasını alabilir (aws.amazon.com/security/). Veri merkezi fiziksel güvenliğine ilişkin bağımsız incelemeler de AWS ISO 27001 denetiminin, PCI değerlendirmesinin ve ITAR denetim sürecinin bir parçasıdır.

5 Üçüncü tarafların, AWS veri merkezlerine erişmesine izin verilir mi?
AWS, şirket içi elemanlar için bile veri merkezlerine erişimi sıkı bir şekilde denetler. Üçüncü tarafların, uygun AWS veri merkezi yöneticisi tarafından AWS erişim ilkelerine uygun şekilde açıkça onaylanmadığı sürece AWS veri merkezlerine erişmesine izin verilmez. Fiziksel erişim, veri merkezi erişim yetkisiyle ilgili belirli denetimler ve diğer ilgili denetimler için SOC 1, Tip 2 raporuna (aws.amazon.com/security/) bakın.

6 Düzeltme eki uygulama işleminden kim sorumludur?
AWS'de çalışan kendi misafir işletim sistemlerimiz (OS), yazılım ve uygulamalarımıza düzeltme eki uygulama işleminden Adobe sorumludur. AWS, hipervizör ve ağ hizmetleri gibi AWS hizmetlerinin sunumunu destekleyen sistemlere düzeltme eki uygulama işleminden sorumludur. Bu işlem, AWS ilkelerinin gerektirdiği şekilde ve ISO 27001, NIST ve PCI gerekliliklerine uygun şekilde gerçekleştirilir.

7 Ayrıcalıklı eylemler izlenip denetlenir mi?
Yerinde denetimler, sistemlere ve verilere erişimi sınırlar veya veriler kısıtlanır ve izlenir. Ayrıca, müşteri verileri ve sunucu örnekleri varsayılan olarak diğer müşterilerden mantıksal bir şekilde yalıtılır. AWS altyapısına ilişkin ayrıcalıklı kullanıcı erişimi denetimi AWS SOC 1, ISO 27001, PCI, ITAR ve FISMA denetimleri sırasında bağımsız bir denetçi tarafından incelenir.

8 Bulut sağlayıcısı, müşteri verilerine ve uygulamalarına yönelik uygun olmayan iç erişim tehdidini ele alır mı?
AWS; SOC 1, Tip 2 raporunda özel SOC 1'i sağlar (aws.amazon.com/security/). Ayrıca Adobe, iç erişimin nasıl denetlendiği ve izlendiği ile ilgili periyodik risk değerlendirmeleri gerçekleştirir.

9 Creative Cloud, müşteri verilerini nasıl yalıtır?
Adobe tarafından müşteriler adına depolanan tüm veriler, güçlü kiracı yalıtım güvenliği ile denetim özelliklerine sahiptir. Creative Cloud Depolama Alanı, gelişmiş veri erişimi denetimleri sağlayan Amazon S3'ü kullanır.

10 Müşteri ayrılığı güvenli bir şekilde gerçekleştirilir mi?
AWS ortamı sanallaştırılmış, birden çok kiracı bulunduran bir ortamdır. AWS, her bir müşteriyi diğer müşterilerden yalıtma amacıyla tasarlanmış güvenlik yönetimi işlemleri, PCI denetimleri ve diğer güvenlik denetimlerini gerçekleştirmiştir. AWS sistemleri, müşterilerin kendilerine atanmamış fiziksel ana bilgisayarlara veya örneklere erişmesini sanallaştırma yazılımı ile filtreleme yoluyla önler. Bu mimari, bir PCI Qualified Security Assessor (Yetkili Güvenlik Denetçisi (QSA)) tarafından doğrulanmıştır ve mimarinin tüm PCI DSS 2.0 gerekliliklerine uyduğu belirlenmiştir (aws.amazon.com/security/pci-dss-level-1-compliance-faqs/).

11 AWS, bilinen hipervizör zayıf noktalarına değinmiş midir?
Amazon EC2, şu anda Xen hipervizörünün oldukça özelleştirilmiş bir sürümünü kullanmaktadır. AWS Xen hipervizör güvenliği, değerlendirmeler ve denetimler sırasında bağımsız denetçiler tarafından düzenli olarak değerlendirilir. Xen hipervizörü ve örnek yalıtım ile ilgili daha fazla bilgi için AWS güvenliği teknik incelemesine (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf) bakın.

12 Sağlanan hizmetler şifrelemeyi destekler mi?
Creative Cloud, verileri aktarım sırasında SSL ile şifreler.

13 Bulut sağlayıcısının müşteri verileri üzerindeki hakları nelerdir?
Creative Cloud müşterileri, verilerinin denetimini ve sahipliğini korur. Daha fazla ayrıntı için Adobe'nin Kullanım Koşullarını (www.adobe.com/go/gffooter_terms_of_use) ve Gizlilik İlkesi'ni (www.adobe.com/privacy/policy.html) inceleyin.

14 AWS, kendisine ait fiziksel denetimleri ve ortam denetimlerini yayınlar mı?
Evet. Fiziksel denetimler ve ortam denetimleri SOC 1, Tip 2 raporunda özellikle özetlenmiştir (aws.amazon.com/security/). Ayrıca AWS, en iyi fiziksel ve ortam denetimlerini gerektiren ISO 27001 ve FISMA sertifikasını destekler.

15 Müşteriler, PC ve mobil aygıt gibi istemcilerden Creative Cloud'a erişimi güvenceye alıp yönetebilir mi?
Evet. Creative Cloud, müşterilere istemci ve mobil erişimi kendi ihtiyaçlarına göre yönetme olanağı tanır.

16 AWS, müşterilerin kendi sanal sunucularını güvenceye almasına izin verir mi?
Evet. Adobe; İnternet Güvenliğine Yönelik En İyi SANS 20 Denetimi, Consensus Audit Guidelines, NIST kılavuzları ve İnternet standartları dahil olmak üzere sektördeki en iyi uygulamaları temel alan AWS'ye dayalı kendi güvenlik mimarisini uygulamıştır.

17 AWS, kimlik ve erişim yönetimi (IAM) özelliklerini içerir mi?
AWS, kimlik ve erişim yönetimine ilişkin bir paket sunar. Bu, Adobe'nin kullanıcı kimliklerini yönetmesini, güvenlikle ilgili kimlik bilgileri atamasını, kullanıcıları gruplar halinde düzenlemesini ve kullanıcı izinlerini merkezi şekilde yönetmesini sağlar.

18 Adobe, Creative Cloud sistemlerini bakım için durduracak mı?
Creative Cloud, çalışmama süresini neredeyse ortadan kaldıracak şekilde hayata geçirilmiştir. Dışarıdan görünen bir çalışmama süresi olmadan A/B ortamlarının ve canlı fiziksel değişime olanak tanıyan diğer mekanizmaların kullanımı sayesinde yeni dağıtımlar sırasında hizmetlere erişilebilmeli ve ulaşılabilmelidir.

19 AWS, Dağıtılmış Hizmet Engelleme (DDoS) saldırılarına karşı nasıl korur?

AWS ağı, geleneksel ağ güvenliğine göre önemli koruma sağlar. Bu konuyla ilgili daha fazla bilgi ve DDoS'ye ilişkin bir tartışma için AWS Güvenliği Teknik İncelemesine (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf) bakın.

20 Adobe'nin, Creative Cloud'a ilişkin bir iş devamlılığı planı var mı?

AWS, bir iş devamlılığı programı sunmaktadır (media.amazonwebservices.com/AWS_Disaster_Recovery.pdf) ve Creative Cloud birden fazla bölgede ve kullanılabilir alanda veya veri merkezlerinde çalışacak şekilde tasarlanmıştır. Adobe, veri artıklığını kopyalama özelliğini ve birden fazla bölgede/kullanılabilir bölgede dağıtım mimarilerini kullanmak için Creative Cloud'u tasarlamış, düzenlemiş ve hayata geçirmiştir.

21 AWS, veri kalıcılığını belirtir mi?

Creative Cloud verileri, kalıcı depolama alanı alt yapısı sunan Amazon S3'te depolar. Nesneler, bir Amazon S3 bölgesinde birden fazla özellikte birden çok aygıtta fazladan depolanır. Veriler depolandıktan sonra, Amazon S3 kaybolan fazlalıkları hızlı bir şekilde algılayıp onararak nesnelerin kalıcılığını sağlar. Amazon S3 ayrıca sağlama toplamlarını kullanarak depolanan verilerin bütünlüğünü de düzenli olarak doğrular. Bozulma algılanması durumunda bunlar, fazla veriler kullanılarak onarılır.

22 Adobe, Federal Bilgi Güvenliği Yönetimi Yasası (FISMA) Uyumluluğunu almayı planlıyor mu?

Adobe'nin, Creative Cloud için yakın zamanda Federal Bilgi Güvenliği Yönetimi Yasası (FISMA) uyumluluğunu alma planı bulunmamaktadır.

23 Creative Cloud, HIPAA uyumlu mudur?

Adobe'nin, Creative Cloud'un sağlık hizmeti kayıtlarını işlemeye yönelik bir planı bulunmadığından Creative Cloud için 1996 Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası (HIPAA) uyumluluk sertifikasını alma niyeti bulunmamaktadır.

Referanslar

AWS Güvenlik Uygulamaları Teknik İncelemesine Genel Bakış, Mart 2013 (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf)

AWS Risk ve Uyumluluk Teknik İncelemesi, Ocak 2013 (media.amazonwebservices.com/AWS_Risk_and_Compliance_Whitepaper.pdf)

Adobe

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