Často kladené dotazy na téma bezpečnosti služby Adobe Creative Cloud pro odborníky z oblasti IT

Otázky na téma služby Creative Cloud se nejčastěji týkají zásad zabezpečení, soukromí a souladu. Organizace využívající službu Creative Cloud se zajímají o zabezpečení svých dat a o to, zda je přístup k nim spolehlivý. V tomto dokumentu jsou zodpovězeny mnohé dotazy, které často kladou pracovníci IT oddělení při zvažování, zda jejich firma má využívat službu Creative Cloud.

1. Kde je služba Creative Cloud hostována?
Služba Creative Cloud je hostována na serverech služby Amazon Web Services (AWS), včetně serverů služeb Amazon Elastic Compute Cloud (Amazon EC2) a Amazon Simple Storage Service (Amazon S3), ve Spojených státech amerických, Evropské unii a asijsko-tichomořské oblasti. Služby AWS jsou spolehlivou platformou pro softwarové služby, kterou využívají tisíce firem po celém světě. Služby AWS využívají špičkové zabezpečení, disponují uznávanými osvědčeními a jsou na nich prováděny pravidelné audity. (aws.amazon.com/security/). Uživatelé služby Creative Cloud tedy mohou těžit ze snahy pracovníků společností Amazon o neustálé zdokonalování zabezpečení.

2. Kde jsou data zákazníků uložena?
Data zákazníků jsou uložena v úložištích služby Amazon S3. Společnost Adobe určí, ve které fyzické oblasti budou data a servery zákazníka umístěny. Replikace datových objektů služby Amazon D3 probíhá v rámci datových center v místě uložení. Data tedy nejsou replikována do datových center v jiných oblastech. Společnost Adobe provozuje zázemí služby Creative Cloud ve třech oblastech: Spojených státech amerických, Evropské unii a asijsko-tichomořské oblasti.

Příklad: Podle základního principu budou mít všichni uživatelé služby Creative Cloud sídlící v Evropské unii uložena data v datových centrech AWS v Evropské unii a tato data nebudou přenášena do datových center nacházejících se mimo Evropskou unii.

3. Kdo dohlíží na datová centra služby Creative Cloud?
U částí služby Creative Cloud implementovaných v rámci služeb AWS se o fyzické komponenty stará společnost Amazon. Provozovatelé služeb AWS vydali zprávu Service Organization Controls 1 (SOC 1) typu 2, ve které jsou popsána bezpečnostní opatření služeb AWS a jejich efektivita. (aws.amazon.com/security/). Dále jsou zde popsány služby Amazon EC2, Amazon S3 a Virtual Private Cloud (VPC) a uvedeny podrobné informace o fyzickém a softwarovém zabezpečení. Toto zabezpečení je na velmi vysoké úrovni, takže by mělo vyhovět většině požadavků zákazníků.

4. Mohou se zákazníci přijít podívat do společnosti Amazon na datová centra služby AWS?
Ne. Vzhledem k tomu, že v datových centrech služeb AWS jsou uložena data více zákazníků, nejsou prohlídky datových center povoleny. Fyzický přístup osob třetích stran není možný. Na zavedení a dodržování bezpečnostních standardů popsaných ve zprávě SOC 1 typu 2 dohlíží nezávislý odborný auditor. Jedná se o široce uznávanou třetí stranu, takže si naši zákazníci mohou být jisti, že efektivitu implementovaných bezpečnostních opatření hlídá nezávislá organizace. Společnost Adobe podepsala dohodu o mlčenlivosti s provozovatelem služeb AWS a může obdržet kopii zprávy SOC 1 typu 2 (aws.amazon.com/security/). Nezávislé hodnocení fyzického zabezpečení datového centra je součástí auditu ISO 27001, vyhodnocení PCI a auditu ITAR prováděného provozovatelem služeb AWS.

5. Mají do datových center služeb AWS přístup zástupci třetích stran?
Provozovatel služeb AWS přísně omezuje přístup do datových center a tato opatření se týkají i jeho vlastních zaměstnanců. Žádný zástupce třetích stran nemá do datových center služeb AWS přístup. Výjimky jsou možné pouze po výslovném schválení vedoucím datového centra na základě přístupových zásad. Více informací o fyzickém přístupu, oprávnění ke vstupu do datových center atd. naleznete ve zprávě SOC 1 typu 2 (aws.amazon.com/security/).

6. Kdo zodpovídá za opravy chyb?
Za opravy v našem vlastním operačním systému, softwaru a aplikacích spuštěných v rámci služeb AWS zodpovídá společnost Adobe. Provozovatel služeb AWS zodpovídá za opravy chyb ve svých podpůrných službách, například hypervizoru nebo síťového zázemí. Tyto opravy splňují zásady služeb AWS a odpovídají standardům ISO 27001, NIST a PCI.

7. Jsou privilegované činnosti sledovány a řízeny?
Řídicí prvky hlídají přístup k systémům a datům a sledují operace prováděné s daty. Data a instance serverů zákazníků jsou navíc logicky izolovány od dat ostatních zákazníků. Řízení uživatelského přístupu na základě privilegií implementované v infrastruktuře služeb je kontrolováno nezávislým auditem SOC 1, ISO 27001, PCI, ITAR a FISMA.

8. Řeší poskytovatel cloudových služeb hrozbu neoprávněného vnitřního přístupu k datům a aplikacím zákazníků?
Provozovatel služeb AWS zavedl opatření popsaná ve zprávě SOC 1 typu 2 (aws.amazon.com/security/). Společnost Adobe navíc pravidelně vyhodnocuje rizika spojená s řízením a sledováním vnitřního přístupu.

9. Jakým způsobem jsou ve službě Creative Cloud oddělena data zákazníků?
Všechna data uložená v zastoupení společností Adobe jsou dobře zabezpečena a oddělena od ostatních. Úložiště služby Creative Cloud využívá službu Amazon S3, která disponuje pokročilými možnostmi řízení přístupu k datům.

10. Je oddělení zákaznických dat implementováno bezpečně?
Prostředí služeb AWS je virtualizované a určené pro více klientů. Provozovatel služeb AWS implementoval bezpečné procesy správy, řídicí prvky PCI a další bezpečnostní řídicí prvky, takže data jednotlivých zákazníků jsou od sebe dokonale oddělena. Systémy AWS jsou navrženy tak, aby zákazníci neměli přístup k fyzickým zařízením nebo instancím, které jim nejsou přiřazeny. O filtrování se stará virtualizační software. Tato architektura byla ověřena nezávislým odborným bezpečnostním auditorem (QSA = Qualified Security Assessor) podle standardu PCI a byla shledána jako vyhovující standardu PCI DSS 2.0 (aws.amazon.com/security/pci-dss-level-1-compliance-faqs/).

11. Jak se provozovatel služeb AWS staví ke známým zranitelným místům hypervizorů?
Služba Amazon EC2 v současnosti využívá velmi upravenou verzi hypervizoru Xen. Zabezpečení hypervizoru AWS Xen je pravidelně vyhodnocováno nezávislými auditory. Více informací o hypervizoru Xen a oddělení instancí naleznete v oficiální zprávě o zabezpečení služeb AWS (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf).

12. Podporují poskytované služby šifrování?
Služba Creative Cloud šifruje data v rámci přenosu podle protokolu SSL.

13. Jaká práva má provozovatel cloudu ohledně dat zákazníků?
Vlastníkem dat jsou zákazníci služby Creative Cloud a je jim dána kontrola nad přístupem. Více podrobností naleznete v dokumentech Podmínky použití (www.adobe.com/go/gffooter_terms_of_use) a Zásady ochrany osobních údajů (www.adobe.com/privacy/policy.html) vydaných společností Adobe.

14. Zveřejňuje provozovatel služeb AWS informace o fyzických a softwarových bezpečnostních opatřeních?
Ano. Fyzická a softwarová bezpečnostní opatření jsou popsána ve zprávě SOC 1 typu 2 (aws.amazon.com/security/). Služby AWS navíc mají osvědčení ISO 27001 a FISMA, k jejichž obdržení je potřeba splnit nejpřísnější požadavky na fyzická a softwarová bezpečnostní opatření.

15. Mohou zákazníci zabezpečovat a spravovat přístup k službě Creative Cloud z klientských zařízení, například stolních počítačů nebo přenosných zařízení?
Ano. Zákazníci mohou v rámci služby Creative Cloud spravovat přístup z klientských a mobilních zařízení podle vlastních požadavků.

16. Umožňují služby AWS zákazníkům, aby si zabezpečili své virtuální servery?
Ano. Společnost Adobe implementovala vlastní bezpečnostní architekturu a přidala ji ke špičkovému zabezpečení služeb AWS. Zahrnuje 20 nejlepších bezpečnostních opatření SANS, směrnice průběžného auditu, směrnice NIST a internetové standardy.

17. Zahrnují služby AWS možnosti správy identity a přístupu (IAM)?
Provozovatel služeb AWS nabízí několik variant správy identit a přístupu, takže společnost Adobe může centrálně spravovat uživatelské identity, přiřazovat bezpečnostní oprávnění, organizovat uživatele do skupiny a spravovat uživatelská oprávnění.

18. Provádí společnost Adobe odstávky služby Creative Cloud za účelem údržby systému?
Služba Creative Cloud je implementována tak, aby nedocházelo téměř k žádným výpadkům. Služba by měla být dostupná i při zavádění nových systémů, a to díky záložním prostředím a dalším mechanismům, které se starají o to, aby se odstávky nedotkly možností přístupu.

19. Jak jsou služby AWS chráněny proti distribuovanému útoku na odepření služby (DDoS)?
Zabezpečení sítě AWS je mnohem větší než v případě běžných sítí. Více informací a toto téma, včetně diskuze o útocích DDoC, naleznete v oficiální zprávě o zabezpečení služeb AWS (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf).

20. Má společnost Adobe plán kontinuity pro službu Creative Cloud?
Provozovatel služeb AWS nabízí program kontinuity (media.amazonwebservices.com/AWS_Disaster_Recovery.pdf). Služba Creative Cloud je navržena tak, aby byla spuštěna ve více regionech spadajících do různých zón dostupnosti a aby využívala více datových center. Společnost Adobe navrhla a implementovala architekturu služby Creative Cloud tak, aby využívala replikaci dat a byla spouštěna ve více oblastech dostupnosti zároveň.

21. Zaručuje provozovatel služeb AWS stálost uložených dat?
Služba Creative Cloud ukládá data v rámci služby Amazon S3, která využívá infrastrukturu dlouhodobého ukládání dat. Datové objekty jsou duplicitně uloženy na více zařízeních v různých pobočkách v rámci dané oblasti služby Amazon S3. Po uložení dat služba Amazon S3 automaticky rychle rozpoznává a napravuje jakékoliv odchylky v redundanci. Služba Amazon S3 také pomocí kontrolních součtů pravidelně ověřuje integritu uložených dat. Je-li rozpoznáno narušení integrity, je okamžitě sjednána náprava podle duplicitně uložených dat.

22. Plánuje společnost Adobe získat osvědčení FISMA (Federal Information Security Management Act)?
Společnost Adobe v tuto chvíli neplánuje získat osvědčení FISMA (Federal Information Security Management Act) pro službu Creative Cloud.

23. Má služba Creative Cloud osvědčení HIPAA?
Společnost Adobe neplánuje pro službu Creative Cloud získat osvědčení HIPAA (Health Insurance Portability and Accountability Act of 1996), jelikož služba Creative Cloud není určena k zpracovávání lékařských záznamů.

Reference

Přehled oficiálních zpráv o zabezpečení služeb AWS, březen 2013 (media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf)

Oficiální zpráva na téma rizik a souladu služeb AWS, leden 2013 (media.amazonwebservices.com/AWS_Risk_and_Compliance_Whitepaper.pdf)

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