Översikt över säkerheten i Adobe Acrobat DC med Document Cloud-tjänster

Innehållsförteckning

Även om Adobe Sign är en del av pdf-tjänsterna i Document Cloud så är dess säkerhetsfunktion fristående.

Överblick

På Adobe tar vi den digitala säkerheten på mycket stort allvar. Säkerhetsrutinerna är djupt integrerade i vår programvaruutveckling, våra operativa processer och våra verktyg. Rutinerna följs noga av våra funktionsövergripande team för att vi ska kunna förebygga, upptäcka och bemöta incidenter på ett ändamålsenligt sätt. Vi håller oss uppdaterade med de senaste hoten och sårbarheterna genom vårt samarbete med partners, ledande forskare, säkerhetsinstitut och andra branschorganisationer. Vi implementerar regelbundet avancerade säkerhetstekniker i våra produkter och tjänster.

Adobe-tjänster som hanterar kundinnehåll uppfyller även kraven för ett stort antal branschcertifieringar. En utförlig lista över alla certifieringar, standarder och regelverk som för närvarande stöds av Adobes produkter och lösningar finns i Current List of Certifications, Standards, and Regulations. Information om GDPR finns här.

I den här rapporten beskrivs ingående det försvar och de säkerhetsprocesser som Adobe infört för att öka säkerheten i Adobe Acrobat DC, Acrobat Reader DC, Document Cloud, Document Cloud-tjänsterna och för data som är knutna till dessa applikationer.

Översikt över Acrobat DC med Document Cloud-tjänster

Adobe Acrobat DC är en kombination av den senaste Acrobat-versionen, premiumfunktionerna i mobilappen Acrobat Reader och onlinetjänsterna i Adobe Document Cloud. Lösningen gör det möjligt för användare inom företag och organisationer att vara uppkopplade och produktiva på vilken enhet som helst, samtidigt som säkerheten upprätthålls på alla enheter. Kunder som använder Adobe Acrobat DC och Document Cloud-tjänsterna kan förvandla innehåll till ett elektroniskt dokument som går att dela med andra, och enkelt skapa, ändra och omforma pdf-filer via dator, mobilapp eller Adobes molntjänster.

Dokumentsäkerhetsfunktioner i Acrobat

Bortredigering

Adobe Acrobat DC har flera bortredigeringsverktyg för skydd av känslig eller konfidentiell information, bland annat kan man permanent avlägsna textavsnitt eller bilder i ett dokument innan man distribuerar det. Dessutom går det att söka på och ta bort innehåll med mönstermatchning, t.ex. telefonnummer, kreditkortsnummer och e-postadresser. Den information som markeras avlägsnas helt och hållet från filen, den täcks inte bara över som med andra verktyg eller metoder. Med dokumentsaneringsfunktionen kan man också ta bort dold information och icke-grafiska objekt, t.ex. metadata som kan finnas i pdf:en.

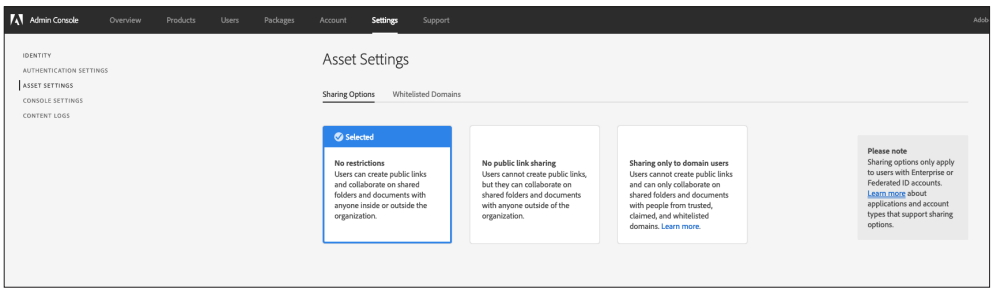
Fildelning

Alla Document Cloud-filer som lagras i molnet märks automatiskt som ”Private”, vilket innebär att innehållet endast är synligt för den användare som laddade upp det. Användaren måste aktivt vidta åtgärder för att dela innehållet, annars förblir det privat. Delning av Document Cloud-innehåll sker genom att en länk till innehållet skickas till mottagaren via e-post, sms eller någon annan programvara för samarbete.

Med Document Cloud-tjänsterna kan filer delas med två visningsalternativ: Endast visning eller Granskning. Om länken skickas med restriktionen Endast visning har mottagaren enbart läsbehörighet. Om dokumentet skickas för granskning kan mottagaren kommentera dokumentet, men inte ändra det på annat sätt.

Resursinställningar och delningsrestriktioner

Med resursinställningar får en organisation kontroll över hur de anställda delar dess resurser utanför organisationen. IT-administratören kan välja en restriktiv inställning som begränsar de anställdas möjlighet att använda vissa delningsfunktioner inom Document Cloud, till exempel förhindra att delningar görs till andra mottagare än inom ianspråktagna domäner, betrodda domäner och godkända domäner. Med en sådan inställning hindras användarna från att dela resurser som ägs av organisationen med externa användare som inte finns med på listan över tillåtna domäner.



Microsoft Information Protection (MIP)

Kunder som använder Acrobat DC eller Acrobat Reader DC för att öppna filer som skyddas med MIP-lösningar (Microsoft Information Protection), inklusive Azure Information Protection (AIP) och Information Protection med Microsoft 365 kan läsa mer i detta dokument.

Skyddat läge i Adobe Reader DC

För att skydda kunder mot skadlig kod som försöker utnyttja pdf-formatet för att skriva eller läsa i datorns filsystem har Adobe utvecklat Skyddat läge, en implementering av sandlådeteknologin som lanserades i Adobe Reader X.

Sandlådan är en säkerhetsmetod som skapar en avgränsad exekveringsmiljö för körning av program med låga rättigheter eller behörigheter. Sandlådan kan skydda användarens system mot att skadas av otillförlitliga dokument som innehåller körbar kod. I Adobe Reader DC är det otillförlitliga innehållet pdf-filer och de processer de anropar. Acrobat Reader DC behandlar alla pdf-filer som potentiellt skadliga och begränsar all körning som anropar en pdf-fil till sandlådan.

I Acrobat Reader DC är Skyddat läge ett försvar mot angripare som försöker installera skadlig kod i datorn och ett stöd för organisationer som vill förhindra att illasinnade aktörer får åtkomst till känsliga data och immateriell egendom via deras nätverk. Skyddat läge är aktiverat som standard när en användare startar Acrobat Reader DC. Det begränsar den åtkomstnivå som beviljas programmet och skyddar Microsoft Windows-system mot skadliga pdf-filer som kan försöka skriva till eller läsa i datorns filsystem, ta bort filer eller på annat sätt ändra systeminformationen.

Skyddat läge på Windows 8 och senare versioner kan också köras i en Windows AppContainer. Detta ger en ännu starkare skyddad miljö för kunder som har aktiverat Skyddat läge.

Skyddad vy i Acrobat DC

Precis som Skyddat läge i Acrobat Reader DC är Skyddad vy en implementering av sandlådeteknologin i Acrobats DC:s många funktioner. I Acrobat DC har Adobe utsträckt funktionaliteten Skyddat läge till något mer än att bara blockera skrivbaserade attacker som använder pdf-formatet för att försöka exekvera illasinnad kod i datorn. Skyddad vy inkluderar även läsningsbaserade attacker där syftet är att stjäla känsliga data eller immateriell egendom via pdf-filer.

Liksom Skyddat läge begränsar Skyddad vy också körningen av otillförlitliga program (t.ex. pdf-filer och de processer de anropar) till en begränsad sandlåda för att undvika att skadlig kod försöker utnyttja pdf-formatet till att skriva eller läsa i datorns filsystem. Skyddad vy hanterar alla pdf-filer som potentiellt skadliga och begränsar körningen av dem till sandlådan om inte användaren särskilt anger att en fil är säker.

Skyddad vy kan användas både när en användare öppnar PDF-dokument i Adobe Acrobat DC och i webbläsaren. Skyddad vy på Windows 8 och senare körs alltid i en AppContainer. Detta ger en ännu starkare skyddad miljö för kunder som har aktiverat Skyddad vy.

När man öppnar en otillförlitlig fil i Skyddad vy visas ett meddelandefält överst i fönstret i Acrobat DC. Meddelandefältet anger att filen är otillförlitlig och påminner om att man befinner sig i Skyddad vy, vilket innebär att många av Acrobats DC:s funktioner är avaktiverade och möjligheterna till interaktion med filen är begränsade. Filen visas i praktiken i skrivskyddat läge, och Skyddad vy förhindrar inbäddat eller bifogat skadligt material från att manipulera systemet.

Om man litar på filen och vill aktivera alla funktioner i Acrobat DC klickar man på Aktivera alla funktioner i meddelandefältet. Då avslutas Skyddad vy och filen får permanent status som tillförlitlig och läggs till i Acrobats lista över behöriga platser. Varje gång den säkra pdf:en därefter öppnas avaktiveras begränsningarna i Skyddad vy.

Arkitekturen för Document Cloud-tjänsterna

I Adobe Document Cloud-tjänsterna ingår följande funktioner:

- **Ordna pdf** – Ta bort, sortera om eller rotera sidorna i en pdf
- **Skapa pdf** – Konvertera Word-, Excel- eller PowerPoint-dokument och bilder eller foton till pdf-filer
- **Exportera pdf** – Konvertera enkelt pdf:er till redigerbara Microsoft Word-, PowerPoint- eller RTF-filer
- **Redigera pdf** – Redigera enkelt befintliga pdf:er via mobil enhet eller dator
- **Kombinera pdf** – Slå ihop flera olika filer till en pdf, och sätt ihop dokumentpaket var som helst
- **Send & Track** – Skicka, spåra och bekräfta leverans av dokument
- **Adobe Scan** – Skanna och konvertera nästan vad som helst till en sökbar och högkvalitativ pdf
- **Adobe Sign** – Förbered och skicka dokument för säker och juridiskt bindande e-signering på vilken enhet som helst

Säkerheten hos Document Cloud-tjänsterna

Hantering av behörigheter och identiteter

IT-administratörer ger användare tillgång till Adobe Document Cloud-tjänsterna genom att använda personliga licenser i Adobe Admin Console. Acrobat Document Cloud har stöd för tre olika typer av personliga licenser:

- **Adobe ID** – För Adobe-hostade och användarhanterade konton som skapas, ägs och kontrolleras av enskilda användare. Adobe ID-konton har bara tillgång till Acrobat Document Cloud-tjänsterna om en IT-administratör ger åtkomst till dem.
- **Enterprise ID** – Ett Adobe-hostat alternativ för företag där kontona skapas och kontrolleras av kundens IT-administratörer. Företaget äger och hanterar användarkontona och alla resurser som är knutna till dem.
- **Federated ID** – Ett företagshanterat konto där alla identitetsprofiler tillhandahålls av kundens identitetshanteringssystem för samlad inloggning (SSO) och skapas, ägs och kontrolleras via kundens IT-infrastruktur. Adobe kan integreras med de flesta identitetsleverantörer som följer SAML 2.0.

Många företag använder Enterprise ID eller Federated ID för anställda, leverantörer och frilansare, under förutsättning att e-postadressen är knuten till företagsdomänen, eftersom det då blir möjligt att behålla kontrollen över både behörigheter och användargenererat innehåll som lagras under ett ID. På Adobes kundsupportsida finns mer information om de olika identitetstyperna.

För lösenordslagringen till Adobe ID och Enterprise ID används hashalgoritmen SHA-256 i kombination med saltade lösenord och ett stort antal hashiterationer. Adobe övervakar dessa konton kontinuerligt för att upptäcka ovanlig eller avvikande kontoaktivitet och utvärderar informationen så att säkerhetshot snabbt ska kunna åtgärdas. Adobe hanterar inte användarlösenord för Federated ID-konton. Mer information finns i Adobe Identity Management Services Security Overview.

Elektroniska och digitala signaturer

I Document Cloud-tjänsterna kan man välja mellan två olika verktyg för att arbeta säkert med signaturer:

- **Fyll i och signera** – Ett verktyg i Adobe Sign som låter användaren hantera underskriftsprocesser från start till mål och som underlättar efterlevnaden av lagar för e-signaturer i USA, EU och de flesta industriländer i världen. Med detta verktyg kan man begära in signaturer från andra, hålla koll på underskriftsprocessen och automatiskt arkivera underskrivna dokument med verifieringskedjan. Hela processen hanteras säkert, och dokument samt verifieringskedja certifieras av Adobe med en kryptografisk stämpel.

Spårning via mobil är inte möjligt.

Mer information om Adobe Sign och dess säkerhetsfunktioner finns i den tekniska översikten för Adobe Sign.

- **Certifikatverktyg** – Gör det möjligt att underteckna dokument med certifikatbaserade digitala signaturer från betrodda tjänsteleverantörer i Adobe Approved Trust List (AATL) eller European Union Trusted List (EUTL). Att underteckna med ett certifikat-ID som utfärdats av en betrodd certifikatutfärdare från tredje part anses allmänt vara en säker metod att skriva under dokument elektroniskt. ID:t är unikt kopplat till och kan identifiera undertecknaren. Undertecknarens certifikat är kryptografiskt kopplat till dokumentet under underskriftsfasen med den privata nyckel som innehas av undertecknaren.

Acrobat DC validerar undertecknarens signatur – och det undertecknade dokumentets äkthet – genom att automatiskt koppla upp sig till certifikatutfärdaren för verifiering. Denna typ av signaturer följer PDF Advanced Electronic Signature (PAdES) Parts 2, 3 och 4 liksom det amerikanska försvarsdepartementets JITC användning av kryptografi och PKI med AES-256, RSA-4096, SHA-512 och RSA-PSS. Med Certifikatverktyget kan man också lägga till tidsstämplar i dokumenten och certifiera dem med en säkerhetsförsegling.

Innehållslagring med Document Cloud-tjänster

Även om administratörer tilldelar lagringsutrymmen i molnet för Enterprise ID- och Federated ID-konton via Adobe Admin Console har de inte direktåtkomst till några filer i enskilda användares lagringsutrymmen. Om ett Enterprise ID eller Federated ID raderas blir eventuella data i molnlagringen oåtkomliga för användaren, och efter 90 dagar raderas filerna.

Administratörer kan också använda Admin Console för att tilldela lagringsutrymme till Adobe ID-konton. Administratörer kan visserligen inte radera Adobe ID-konton, men de kan återkalla såväl det tilldelade lagringsutrymmet som åtkomsten till applikationer och tjänster. Data som är knutna till dessa konton raderas efter 90 dagar.

Adobe Document Cloud-tjänsterna använder sig av multitenancy-lagring. Kundinnehåll processas av en instans av Amazon Elastic Compute Cloud (Amazon EC2) och lagras i en kombination av hinkar i Amazon Simple Storage Services (Amazon S3) och en MongoDB-instans på Amazon Elastic Block Store (Amazon EBS). Själva innehållet lagras i Amazon S3-hinkar, och metadata om innehållet lagras i Amazon EBS via MongoDB – allt skyddas av regler för identitets- och åtkomsthantering (IAM) inom den aktuella AWS-regionen.

Metadata och stödresurser som lagras i Amazon EBS krypteras med 256-bitars AES-kryptering med godkända kryptografiska FIPS 140-2-algoritmer som följer rekommendationerna i standarden 800-57 från National Institute of Standards and Technology (NIST).

Data lagras redundant i flera datacenter och på flera enheter i respektive datacenter. All nätverkstrafik genomgår systematisk dataverifiering och kontrollsummeberäkningar för att förhindra förvanskning och säkerställa integriteten. Slutligen replikeras allt innehåll synkront och automatiskt till andra datacenter i kundens region så att dataintegriteten upprätthålls även vid förlust av data på två olika platser.

Mer information om underliggande Amazon-tjänster finns här:

- MongoDB
- Amazon S3
- AWS Key Management Service (KMS)
- Amazon EC2 service

Dedikerad krypteringsnyckel

Lagrat innehåll i Amazon S3 krypteras som standard med 256-bitars symmetriska AES-säkerhetsnycklar som är unika för kunden och kundens domän. Om administratörer vill lägga till ytterligare ett kontroll- och säkerhetslager för vissa eller alla domäner i organisationen, kan de använda en dedikerad krypteringsnyckel som hanteras av AWS KMS och som roteras automatiskt på årsbasis.

Administratörer kan också återkalla denna dedikerade krypteringsnyckel via Admin Console, och det leder till att alla data som krypterats med nyckeln blir otillgängliga för användarna. Även uppladdning och nedladdning av innehåll förhindras tills krypteringsnyckeln aktiveras på nytt.

Obs! Adobe Document Cloud-filer kan krypteras med den dedikerade krypteringsnyckeln, men inte metadata.

Mer information om kryptering med dedikerad nyckel finns på dessa Adobe-hjälpsidor:

- Krypteringshantering
- Dedikerade krypteringsnycklar | Vanliga frågor

Amazon Web Services

Det är alltså AWS i USA som är värd för alla komponenter i Adobe Document Cloud-tjänsterna, inklusive Amazon EC2 och Amazon. Amazon EC2 är en webbtjänst som erbjuder automatiskt skalbar datakapacitet i molnet. Amazon S3 anses allmänt vara en mycket tillförlitlig datainfrastruktur för lagring och hämtning av data.

AWS-plattformen tillhandahåller tjänster i enlighet med branschpraxis och genomgår regelbundet branscherkända certifieringar och revisioner. Mer information om AWS och Amazons säkerhetskontroller finns på webbplatsen AWS Cloud Security.

AWS och Adobes driftsansvar

AWS driftar, hanterar och kontrollerar komponenterna från hypervisorvirtualiseringen och hela vägen till den fysiska säkerheten på de anläggningar där Adobe Document Cloud-tjänsterna körs. Adobe ansvarar för gästoperativsystemet (inklusive uppdateringar och säkerhetspatchar) och programvaran, samt konfigureringen av brandväggen som tillhandahålls av AWS.

AWS driftar även molninfrastrukturen som Adobe använder för att kunna erbjuda en rad olika grundläggande resurser för databearbetning och -lagring. AWS-infrastrukturen omfattar anläggningar, nätverk och hårdvara samt driftprogramvara (värdoperativsystem, virtualiseringsprogram osv.) som gör det möjligt att tillhandahålla och använda dessa resurser. Amazon utformar och hanterar AWS i enlighet med branschpraxis och ett antal olika säkerhetsstandarder.

Säker hantering

Adobe använder Secure Shell (SSH) och Secure Sockets Layer (SSL) för att ansluta till AWS-infrastrukturen.

Geografisk placering av kunddata på AWS-nätverket

Allt användargenererat innehåll som laddas upp till Document Cloud lagras i AWS regionala datacenter i Virginia (US-East). Innehållet säkerhetskopieras inom varje datacenter och i andra datacenter i regionen för lastbalansering och redundans.

Geografisk plats för identitetsdata på AWS-nätverket

Identitetsdata lagras i flera regioner i lastbalanserade AWS-datacenter i Virginia (US-East), Oregon (US-West), Irland (EU-West) och Singapore (AP-Southeast). Identitetsdata replikeras till alla datacenter. Adobe uppfyller alla gällande lagar om gränsöverskridande dataöverföringar. Detta beskrivs mer ingående här: https://www.adobe.com/se/privacy/eudatatransfers.html.

Isolering av kunddata/kundsegregering

AWS använder starka säkerhets- och kontrollfunktioner för isolering av kunderna. AWS-miljön är en virtualiserad multitenant-miljö och har integrerade processer för säkerhetshantering och andra säkerhetskontroller som utformats för att isolera kunder från varandra. Adobe använder AWS identitets- och åtkomsthantering för att ytterligare begränsa åtkomsten till beräknings- och lagringsinstanser.

Säker nätverksarkitektur

AWS utnyttjar olika nätverksenheter, bland annat brandväggar, för att övervaka och kontrollera kommunikationen som sker dels via nätverkets yttre gränslinje, dels via viktiga interna gränser inom nätverket. Dessa enheter använder regeluppsättningar, åtkomstlistor och olika konfigurationer för att hantera flödet av information till specifika informationssystemtjänster. Åtkomstlistor, eller riktlinjer för trafikflöden, finns för varje hanterat gränssnitt och används för att hantera och styra trafikflödet.

Amazon Information Security godkänner alla åtkomstlistor och skickar dem automatiskt till varje hanterat gränssnitt med hjälp av AWS ACL-Manage-verktyget, vilket säkerställer att gränssnitten tillämpar de mest aktuella åtkomstlistorna.

Övervakning och skydd av nätverk

AWS använder en rad olika automatiserade övervakningssystem för att skapa hög tillgänglighet och prestanda. Övervakningsverktygen upptäcker avvikande eller otillåtna aktiviteter och villkor för ingående och utgående kommunikation. AWS-nätverket ger starkt skydd mot vanliga säkerhetsproblem i nätverk:

- Distribuerade överbelastningsattacker (DDoS)
- Man-in-the-middle-attacker (MITM)
- IP-adressförfalskning
- Portskanning
- Packet sniffing av andra klienter

Mer information om nätverksövervakning och nätverksskydd finns på webbplatsen AWS Cloud Security.

Intrångsdetektering

Adobe övervakar aktivt Adobe Document Cloud-tjänsterna med system för intrångsdetektering och intrångsskydd som är branschstandard.

Loggning

Adobe loggar kundaktiviteter på serversidan av Adobe Document Cloud-tjänsterna för att diagnostisera serviceavbrott, specifika kundproblem och rapporterade fel. I loggarna sparas Adobe ID:n endast i syfte att diagnostisera kundproblem – inga kombinationer av användarnamn och lösenord lagras. Det är bara behöriga servicetekniker, specialistingenjörer och utvalda utvecklare från Adobe som har tillgång till loggarna för att kunna åtgärda eventuella problem.

Tjänstövervakning

AWS övervakar elektriska, mekaniska och kritiska system och utrustningar för att snabbt identifiera problem med tjänsterna. För att kunna upprätthålla en kontinuerlig drift utför AWS löpande förebyggande underhåll av utrustningen.

Datalagring och backup

Adobe lagrar alla data för Adobe Document Cloud-tjänsterna i Amazon S3 som har en hållbar lagringsinfrastruktur. Denna hållbarhet åstadkoms genom att PUT- och COPY-processer i Amazon S3 synkront lagrar kunddata på flera anläggningar och även lagrar objekt med redundans på flera enheter i flera olika anläggningar i en Amazon S3-region.

Amazon S3 utför kontrollsummeberäkningar på all nätverkstrafik för att identifiera förvanskade datapaket när data lagras eller hämtas. Datareplikering för Amazon S3-dataobjekt görs inom det regionala kluster där aktuella data lagras, och replikeringen sker inte till datacenterkluster i andra regioner.

Metadata replikeras genom snapshots av Amazon EBS-volymer och lagras på liknande sätt i Amazon S3. Mer information om AWS-säkerhet finns på webbplatsen AWS Cloud Security.

Ändringshantering

AWS auktoriserar, loggar, testar, godkänner och dokumenterar rutinmässiga, akuta och konfigurationsrelaterade ändringar i befintlig AWS-infrastruktur enligt branschstandarderna för liknande system. Amazon schemalägger uppdateringar av AWS på ett sätt som orsakar minsta möjliga störning för kunderna. AWS meddelar kunder antingen via mejl eller via AWS Service Health Dashboard om det finns risk för att en tjänst skulle kunna påverkas negativt. Adobe har även en statuslista för Adobe Document Cloud: Adobe System Status.

Patchhantering

AWS ansvarar för korrigeringar i de system som levererar AWS tjänster, till exempel hypervisor- och nätverkstjänsterna. Adobe ansvarar för korrigeringar av våra egna gästoperativsystem (OS) och program som körs i AWS. När det krävs korrigeringar levererar Adobe en ny, härdad instans av operativsystemet och applikationen i stället för en faktisk patch.

AWS kontroller av anläggningar och miljö

AWS kontroller av anläggningar och miljö redovisas specifikt i SOC Type 1- och SOC Type 2-rapporterna. Nedan beskrivs några av de säkerhetsåtgärder och kontroller som genomförs på AWS datacenter runt om i världen. Mer information om AWS säkerhet finns på webbplatsen om AWS Cloud Security.

Anläggningssäkerhet

AWS datacenter är arkitektoniskt och tekniskt utformade enligt branschstandard. De är inrymda i diskreta anläggningar. Amazon kontrollerar det fysiska tillträdet till både det omgivande området och byggnadens entréer med professionell säkerhetspersonal, videoövervakning, system för intrångsdetektering och annan elektronisk utrustning. Behörig personal måste passera kontroller med tvåfaktorsautentisering minst två gånger för att komma in i datacentret. Alla besökare och leverantörer måste uppvisa identitetshandlingar. De registreras vid ankomst och eskorteras alltid av behörig personal.

AWS ger endast tillträde till och information om datacenter till anställda och entreprenörer som behöver detta av arbetsskäl. När en anställd inte längre har behov av sådana behörigheter återkallas tillträdet omedelbart, även om personen fortfarande är anställd hos Amazon eller AWS. AWS-anställdas fysiska besök i datacenter loggas och granskas rutinmässigt.

Brandbekämpning

AWS har installerat automatisk branddetektering och undertrycksutrustning i alla datacenter. Branddetekteringssystemet inkluderar röksensorer i alla datacenter samt i utrymmen för mekanisk och elektrisk infrastruktur, kylrum och generatorrum. Dessa områden skyddas av våt-, preaction- eller gassprinklersystem.

Kontrollerad miljö

AWS använder en klimatanläggning för att upprätthålla en konstant driftstemperatur för servrar och annan hårdvara så att överhettning förhindras och risken för driftsavbrott minimeras. Luftförhållandena i AWS datacenter är optimala. AWS-personal och -system övervakar och håller både temperatur och fuktighet på lämpliga nivåer.

Reservströmförsörjning

Elsystemen i AWS datacenter är konstruerade för att vara helt redundanta och kunna fungera utan driftspåverkan dygnet om, alla dagar veckan. Enheter för avbrottsfri strömförsörjning (UPS) fungerar som backup om kritiska funktioner skulle drabbas av strömavbrott. Det finns generatorer som ger reservkraft åt hela anläggningen vid behov.

Katastrofåterställning

AWS datacenter har hög tillgänglighet och klarar system- och hårdvarufel utan att detta påverkar driften i någon större grad. De ligger i kluster i olika regioner runt om i världen och alla är online dygnet runt, året runt – inget datacenter är någonsin ”inaktivt”. Om ett fel skulle uppstå flyttas kunddatatrafiken automatiskt bort från det drabbade området.

Kärnapplikationer driftsätts i en N+1-konfiguration så att det i händelse av ett datacenterhaveri finns tillräcklig kapacitet för att flytta över trafiken till övriga anläggningar. Mer information om AWS protokoll för katastrofåterställning finns på webbplatsen för AWS Cloud Security.

Adobes risk- och sårbarhetshantering

På Adobe strävar vi efter att vår risk- och sårbarhetshantering, incidentrespons och våra processer för att mildra och lösa problem ska vara smidiga och precisa. Vi övervakar kontinuerligt hotlandskapet, utbyter kunskap med säkerhetsexperter runt om i världen, löser snabbt incidenter när de uppstår och återkopplar informationen till våra utvecklingsteam för att nå högsta möjliga säkerhetsnivå för alla våra produkter och tjänster.

Penetrationstestning

I samarbete med ledande tredjeparts säkerhetsföretag utför Adobe penetrationstester för att upptäcka potentiella säkerhetsproblem och göra Adobes produkter och tjänster ännu säkrare. När rapporten kommer från tredje part dokumenterar Adobe sårbarheterna, bedömer allvarlighetsgraden och prioritetsnivån, och tar sedan fram en begränsningsstrategi eller åtgärdsplan. Adobe genomför ett fullständigt penetrationstest varje år och utför sårbarhetsskanningar varje månad.

Internt genomför säkerhetsteamet för Adobe Document Cloud en riskbedömning av alla komponenter och tjänster i Document Cloud kvartalsvis och före varje ny release. Säkerhetsteamet för Dokument Cloud samarbetar med tekniker och utvecklare för att eliminera alla sårbarheter som kan innebära hög risk. Läs mer om Adobes rutiner för penetrationstestning i Adobe Secure Engineering Overview.

Incidentrespons och säkerhetsvarningar

Nya sårbarheter och hot uppstår varje dag, och Adobe strävar efter att hantera och minska risken som nyupptäckta hot innebär. Förutom att prenumerera på branschövergripande sårbarhetsmeddelanden, bland annat från United States Computer Emergency Readiness Team (US-CERT), Bugtraq och SANS, så får Adobe också de senaste listorna med säkerhetsmeddelanden som ges ut av större säkerhetsleverantörer.

Mer information om Adobes incidentrespons och meddelandeprocesser finns i rapporten Adobe Incident Response Overview.

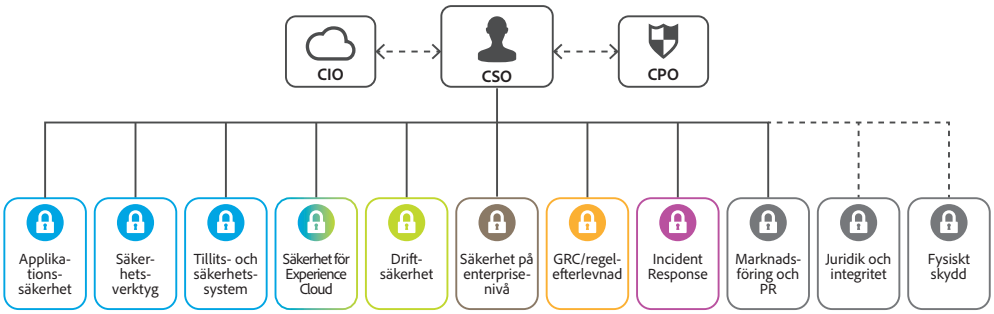
Forensisk analys

Vid incidentutredningar följer Document Cloud-teamet Adobes process för forensisk analys som innefattar en komplett avbildning eller minnesdump från aktuell utrustning, bevissäkring och spårbarhetsregistrering.

Adobes säkerhetsorganisation

Arbetet med att stärka säkerheten hos produkter och tjänster samordnas av Adobes Chief Security Officer (CSO). CSO-avdelningen koordinerar alla säkerhetsinitiativ för produkter och tjänster, liksom implementeringen av Adobe Secure Product Lifecycle (SPLC).

CSO leder Adobes Secure Software Engineering Team (ASSET), ett dedikerat centralt team med säkerhetsexperter som fungerar som konsulter till Adobes produkt- och driftteam. ASSET:s forskare arbetar med individuella produkt- och driftsteam på Adobe för att uppnå rätt säkerhetsnivå för produkter och tjänster och förordar säkerhetsrutiner för tydliga och repeterbara processer för utveckling, driftsättning, körning och incidentrespons.



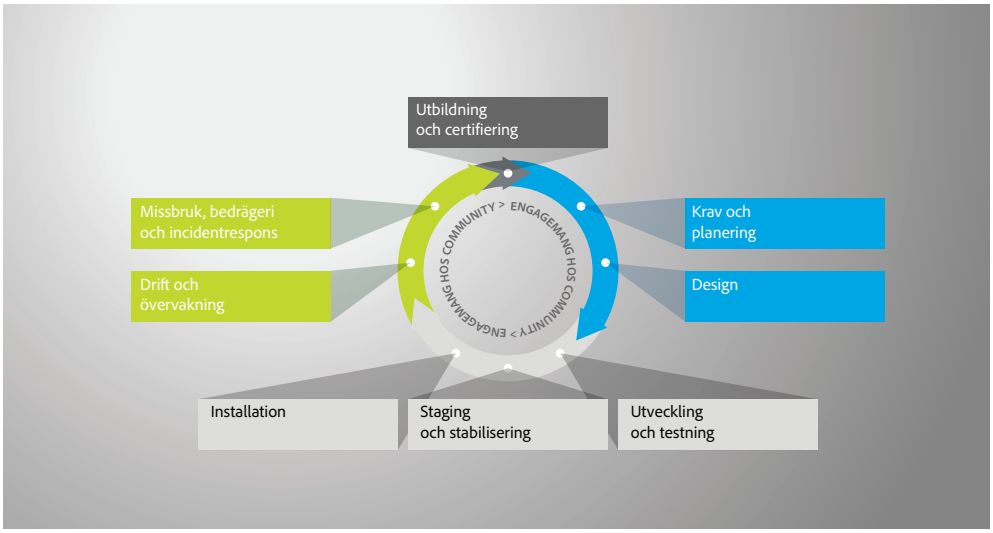
Adobe och säker produktutveckling

Precis som Adobes andra stora produkt- och tjänsteorganisationer så arbetar även Adobe Document Cloud-organisationen enligt Adobes SPLC-process. Adobe SPLC utgörs av flera hundra specifika säkerhetsaktiviteter som omfattar utvecklingsmetoder, processer och verktyg, och är integrerat i flertalet steg i produktlivscykeln, från design och utveckling till kvalitetssäkring, testning och implementering. ASSET:s säkerhetsforskare ger specifik SPLC-vägledning för varje nyckelprodukt eller -tjänst baserat på en bedömning av potentiella säkerhetsproblem. Adobe SPLC kompletteras av en engagerad community och utvecklas hela tiden för att förbli aktuellt i takt med att teknik, säkerhetspraxis och hotlandskap förändras.

Adobe Secure Product Lifecycle

Beroende på vilken Adobe Document Cloud-komponent det handlar om innefattar Adobes SPLC-aktiviteter några eller alla följande rekommenderade arbetsmetoder, processer och verktyg:

- Säkerhetsutbildning och certifiering av produktteam
- Analys av produkthälsa, risker och hotlandskap
- Säker kodning med riktlinjer, regler och analyser
- Färdplaner, säkerhetsverktyg och testmetoder som underlättar för Adobe Document Cloud-säkerhetsteamet att hantera Open Web Application Security Project (OWASP) som listar de 10 mest kritiska riskerna i webbapplikationer och CWE/SANS som lister de 25 farligaste programfelen
- Översyn av säkerhetsarkitektur och penetrationstestning
- Källkodsgranskningar för att eliminera kända brister som kan leda till sårbarheter
- UGC-validering
- Applikations- och nätverksskanning
- Fullständig driftstest, responsplaner och framtagning av utbildningsmaterial för utvecklare



Adobe Software Security Certification Program

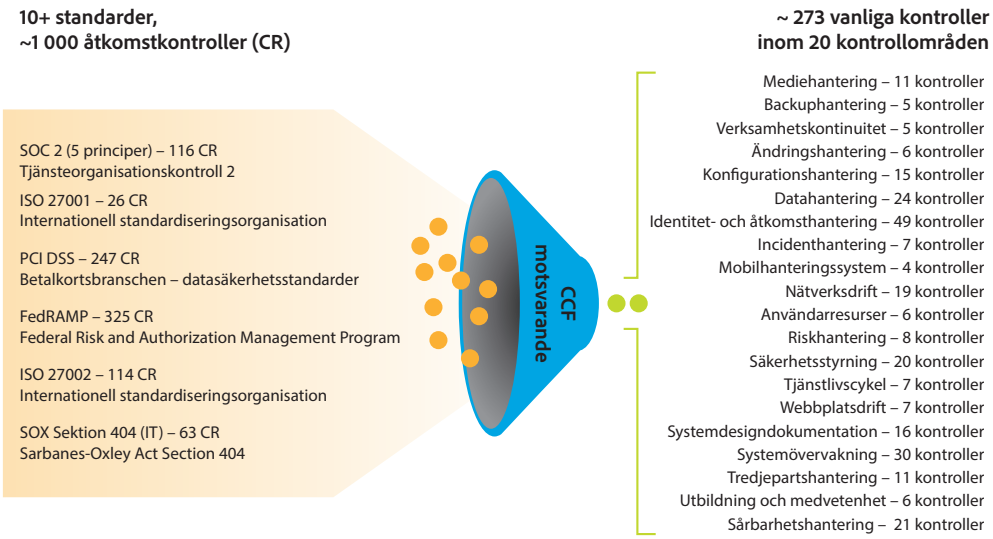
Som en del av Adobe SPLC håller Adobe kontinuerligt säkerhetsutbildningar med utvecklarteamen för dels förbättra säkerhetskunskaperna i hela företaget, dels höja den allmänna säkerhetsnivån på produkter och tjänster. Medarbetare som deltar i Adobe Software Security Certification Program uppnår olika certifieringsnivåer genom att utföra säkerhetsprojekt. Mer information om våra produktsäkerhetsrutiner finns här: Adobe Secure Engineering Overview.

Mer information om Adobe Software Security Certification Program finns i rapporten om Adobes säkerhetskultur.

Document Cloud-tjänsternas regelefterlevnad

Adobe Common Controls Framework (CCF) är en uppsättning säkerhetsaktiviteter och efterlevnadskontroller som utförs av våra produkt- och verksamhetsteam, men även av olika delar av våra infrastruktur- och applikationsteam.

När Adobe tog fram CCF analyserades kriterierna för de vanligaste säkerhetscertifieringarna för molnbaserade verksamheter och de mer än tusen kraven kokades ner till Adobe-specifika kontroller som täcker ungefär ett dussin branschstandarder.



Den senaste informationen om certifieringar och regelefterlevnad som rör Adobe Acrobat DC och Document Cloud-tjänsterna finns i Adobe Trust Center.

Information om aktuell efterlevnadsstatus för Adobe Sign finns i säkerhetsöversikten för Adobe Sign.

I slutänden är det dock alltid kundernas ansvar att uppfylla de lagkrav som ställs på dem och att säkerställa att lösningarna de använder tillgodoser deras efterlevnads- och säkerhetsbehov.

Adobes anställda

Adobe har anställda och kontor runt om i världen och använder nedanstående processer och rutiner för att skydda företaget mot säkerhetshot.

Anställdas åtkomst till kunddata

Adobe upprätthåller separata utvecklings- och produktionsmiljöer för Adobe Document Cloud och använder tekniska kontroller för att begränsa åtkomsten från nätverks- och applikationsnivå till livesystem. Tillgång till utvecklings- och produktionssystemen kräver särskild behörighet, och anställda som inte har legitima arbetsskäl har ingen åtkomst till dessa system.

Bakgrundskontroller

Adobe gör bakgrundskontroller av sina anställda. Bakgrundkontrollerna innefattar vanligen utbildningsbakgrund, tidigare anställningar, utdrag ur domstolsregister inklusive belastningsregister, samt personliga och yrkesmässiga referenser, allt i den utsträckning lagen tillåter. Kraven på bakgrundskontroll gäller vid nyanställning i USA och för personer som administrerar system eller har tillgång till kundinformation. När personal anlitas via bemanningsföretag i USA är det bemanningsföretaget som står för bakgrundskontrollen, och den utförs i enlighet med Adobes riktlinjer. Utanför USA genomför Adobe bakgrundskontroller av vissa nya medarbetare i enlighet med Adobes policy för bakgrundskontroll och tillämpliga nationella lagar.

Uppsägning

När en anställd väljer att sluta på Adobe lämnar den anställdes chef in ett formulär om upphörande av anställning. När den har godkänts meddelar Adobes personalavdelning berörda personer via e-post så att dessa kan vidta nödvändiga åtgärder. Om Adobe säger upp en anställd gör Adobes personalavdelning ett liknande e-postutskick till relevanta personer och informerar om datum och tidpunkt för anställningens upphörande.

Därefter schemalägger Adobes säkerhetsavdelning ett antal åtgärder för att säkerställa att den anställde inte kommer att ha åtkomst till Adobes konfidentiella filer eller kontor efter sin sista arbetsdag:

- Borttagning av åtkomst till e-post
- Borttagning av åtkomst till VPN
- Ogiltigförklarande av passerkort till kontor och datacenter
- Avslutande av nätverksåtkomst

På begäran kan chefer ge anläggningens säkerhetspersonal i uppdrag att eskortera den uppsagda medarbetaren ut ur kontoret eller byggnaden.

Anläggningssäkerhet

Adobes samtliga kontor skyddas av väktare på plats dygnet runt, alla dagar i veckan. Adobe-anställda måste bära passerkort för att få tillträde till lokalerna. Besökare går in genom huvudentrén och anmäler sig i receptionen både när de kommer och går. De får ett tillfälligt besöks-ID och åtföljs av en Adobe-anställd. Serverutrustning, utvecklingsmaskiner, telefonsystem, fil- och e-postservrar liksom andra känsliga system står alltid i låsta serverrum med klimatstyrning dit endast behörig personal har tillträde.

Virusskydd

Adobe skannar all inkommande och utgående e-post till företaget för att fånga upp skadlig kod.

Kunddata och konfidentialitet

Adobe behandlar alla kunddata som konfidentiella. Adobe varken använder eller delar information som samlas in å kunders vägnar utom i enlighet med kundavtal och med Adobes användningsvillkor och Adobes integritetspolicy.

Till sist

Adobes proaktiva syn på säkerhet och de strikta rutiner som beskrivs i den här rapporten bidrar till säkerheten i Adobe Acrobat DC, Acrobat Reader DC och Document Cloud-tjänsterna – och till att skydda dina konfidentiella data. På Adobe tar vi den digitala säkerheten på mycket stort allvar. Vi övervakar kontinuerligt det föränderliga hotlandskapet för att ligga steget före så att vi kan skydda våra kunders data.

Mer information finns här: Adobe Trust Center.

Adobe

Adobe Systems Nordic AB
Box 47, 164 93 Kista, Sverige
www.adobe.se, www.adobe.com