Adobe Acrobat DC med Document Cloud-tjenester – sikkerhetsoversikt

Innholdsfortegnelse

Adobe Sign er en del av Document Cloud PDF-tjenestene, men har en uavhengig sikkerhetsfunksjonalitet.

Innledning

Vi hos Adobe tar sikkerheten i den digitale opplevelsen på alvor. Sikkerhetsrutiner er dypt innarbeidet i den interne programvareutviklingen, driftsprosessene og verktøyene. Disse rutinene følges nøye av de tverrfunksjonelle arbeidsgruppene, slik at de kan forhindre, registrere og reagere på hendelser på en formålstjenlig måte. Vi holder oss oppdatert på de nyeste truslene og sårbarhetene via samarbeidet med partnere, ledende forskere, sikkerhetsforskningsinstitusjoner og andre bransjetilknyttede organisasjoner. Vi innlemmer regelmessig avanserte sikkerhetsteknologier i produktene og tjenestene vi tilbyr.

Adobe-tjenester som involverer kundeinnhold, har gjennomgått en rekke bransjesertifiseringer. Hvis du vil ha en detaljert liste over alle sertifiseringer og standarder for kravoverholdelse samt offentlige forskrifter som støttes av Adobe-produkter og -løsninger, kan du se den gjeldende listen over sertifiseringer, standarder og forskrifter. Hvis du vil ha informasjon om GDPR, kan du se siden om GDPR-tilrettelegging.

Dette tekniske dokumentet beskriver "defense in depth"-tilnærmingen og sikkerhetsprosedyrene som er implementert av Adobe for å forbedre sikkerheten til Adobe Acrobat DC, Acrobat Reader DC, Document Cloud, Document Cloud-tjenestene og tilknyttede data.

Acrobat DC med Document Cloud-tjenester – oversikt

Adobe Acrobat DC kombinerer de nyeste Acrobat-skrivebordsprogrammene med premiumfunksjoner i Acrobat Reader-mobilapplikasjonen og Adobe Document Cloud-nettjenester for å hjelpe organisasjoner med å oppfylle sluttbrukernes krav om konnektivitet og produktivitet på alle enheter samtidig med at sikkerheten ivaretas på tvers av enhetene. Ved hjelp av Adobe Acrobat DC og Document Cloud-tjenestene kan kundene gjøre innhold om til et elektronisk dokument som kan deles med andre, og de kan enkelt generere, manipulere og omforme PDF-filer fra alle Adobe-nettskytjenester, -skrivebordsprogrammer og -mobilapplikasjoner.

Acrobat-dokumentsikkerhetsfunksjoner

Redaksjon

Adobe Acrobat DC inneholder et sett med redaksjonsverktøy som hjelper kundene med å beskytte sensitiv eller konfidensiell informasjon, blant annet ved å slette både tekst og grafikk permanent i et dokument før det distribueres. Brukerne kan også søke etter og slette innhold basert på mønstre, for eksempel telefonnumre, kredittkortnumre og e-postadresser. Informasjonen du sletter, fjernes fullstendig fra filen. Den blir ikke bare maskert, slik tilfellet er med andre verktøy og metoder. Med funksjonen for dokumentrensing kan kundene også fjerne skjult informasjon og ikke-grafiske objekter, for eksempel metadata som kan finnes i PDF-filen.

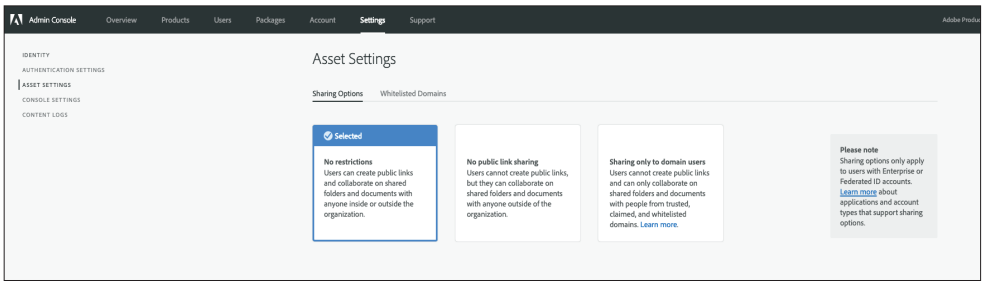
Fildeling

Alle Document Cloud-filer som lagres i nettskyen, merkes automatisk som "privat", noe som betyr at innholdet kun er synlig for sluttbrukeren som laster dem opp. En sluttbruker må foreta eksplisitte handlinger for å dele innholdet, ellers forblir det privat. All Document Cloud-innholdsdeling fullføres ved å sende en kobling til Document Cloud-innholdet til mottakerne via e-post, SMS eller et hvilket som helst samarbeidsprogram.

Brukere av Document Cloud-tjenester kan velge mellom to alternativer når de skal dele filer: skrivebeskyttet eller til gjennomgang. Hvis brukeren sender koblingen med begrensningen for skrivebeskyttelse, kan mottakeren kun vise innholdet som et skrivebeskyttet dokument. Hvis brukeren velger å sende dokumentet til gjennomgang, kan mottakeren kommentere dokumentet, men har ikke mulighet til å redigere/endre det.

Ressursinnstillinger og delingsbegrensninger

Ressursinnstillinger gir en organisasjon kontroll over hvordan de ansatte deler ressurser utenfor organisasjonen. IT-administratoren kan velge en begrensningsinnstilling som hindrer de ansatte i å bruke bestemte delingsfunksjoner i Document Cloud, blant annet begrensning av invitasjonsbasert deling til mottakere i forespurte, klarerte og hvitelistede domener. Når denne begrensningen er angitt, er brukerne forhindret fra å dele organisasjonseide ressurser med eksterne brukere som ikke finnes på listen over tillatte domener.



Ressursinnstillinger i Admin Console

Microsoft Information Protection (MIP)

Kunder som bruker Acrobat DC eller Acrobat Reader DC til å åpne filer som er beskyttet med Microsoft Information Protection-løsninger (MIP-løsninger), blant annet Azure Information Protection (AIP) og informasjonsbeskyttelse med Microsoft Office 365, bør lese dette dokumentet.

Beskyttet modus i Acrobat Reader DC

For å hjelpe kundene med å beskytte seg mot skadelig kode som forsøker å bruke PDF-formatet til å skrive til eller lese fra filsystemet i en datamaskin, tilbyr Adobe Beskyttet modus, en implementering av sandkasseteknologien som ble introdusert i Adobe Reader X.

Sandkasseteknologien er en sikkerhetsmetode som oppretter et begrenset miljø der programvare kan kjøres med lave rettigheter. Sandkassen bidrar til å beskytte brukernes systemer mot å bli skadet av ikke-klarerte dokumenter som inneholder kjørbar kode. Når det gjelder Acrobat Reader DC, betyr ikke-klarerte dokumenter alle PDF-filer og prosessene de eventuelt aktiverer. Acrobat Reader DC behandler alle PDF-filer som potensielt skadde og avgrenser all kjøring PDF-filen aktiverer, til sandkassen.

Beskyttet modus i Acrobat Reader DC bidrar til å beskytte mot angripere som prøver å installere skadelig programvare på en datamaskin. Dette støtter opp om ulike organisasjoners tiltak for å hindre ondsinnede aktører i å få tilgang til og trekke ut sensitive data og åndsverk fra nettverkene. Beskyttet modus aktiveres som standard hver gang en bruker åpner Acrobat Reader DC. Modusen begrenser tilgangsnivået som er tilordnet applikasjonen, og systemer som kjører Microsoft Windows®, beskyttes mot skadelige PDF-filer som forsøker å skrive til datamaskinens filsystem, slette filer eller på annen måte endre systeminformasjonen.

Beskyttet modus på Windows 8 og nyere kan også kjøres i en Windows AppContainer, noe som gir et enda sterkere låst miljø for kunder som aktiverer Beskyttet modus.

Beskyttet visning i Acrobat DC

På samme måte som Beskyttet modus i Acrobat Reader CD er Beskyttet visning en implementering av sandkasseteknologi for det avanserte Acrobat DC-funksjonssettet. I Acrobat DC utvider Adobe funksjonaliteten til Beskyttet modus fra kun å gjelde blokkering av skrivebaserte angrep som forsøker å kjøre skadelig kode på en datamaskin ved hjelp av PDF-filformatet, til også å gjelde lesebaserte angrep som forsøker å stjele sensitive data eller åndsverk via PDF-filer.

På samme måte som Beskyttet modus vil Beskyttet visning begrense kjøringen av ikke-klarerte programmer (for eksempel en PDF-fil og prosessene den aktiverer) til en begrenset sandkasse, for på den måten å unngå at skadelig kode bruker PDF-formatet til å skrive til eller lese fra datamaskinens filsystem. Beskyttet visning antar at alle PDF-filer potensielt er skadelige, og begrenser behandlingen av dem til sandkassen med mindre brukeren spesifikt angir at en fil er klarert.

Beskyttet visning støttes i begge scenarioer der brukere åpner PDF-dokumenter – med frittstående Adobe Acrobat DC og i en nettleser. Beskyttet modus på Windows 8 og nyere kjører alltid i en AppContainer. Dette gir et enda sterkere låst miljø for kunder som aktiverer Beskyttet visning.

Når en bruker åpner en ikke-klarert fil i Beskyttet visning, vises det en gul meldingslinje øverst i vinduet i Acrobat DC. Meldingslinjen angir at filen ikke er klarert, og minner brukeren på at vedkommende er i Beskyttet visning, noe som deaktiverer mange Acrobat DC-funksjoner og begrenser brukerens interaksjon med filen. Filen er i bunn og grunn skrivebeskyttet, og Beskyttet visning beskytter mot innebygd eller medfølgende ondsinnet innhold som kan utføre uautoriserte endringer i systemet.

Brukeren kan klarere filen og aktivere alle Acrobat DC-funksjonene ved å klikke på knappen for aktivering av alle funksjoner på meldingslinjen. Denne handlingen avslutter Beskyttet visning og gir filen permanent klarering ved å legge den til på Acrobats liste over privilegerte plasseringer. Når du åpner den klarerte PDF-filen i fremtiden, er begrensningene i Beskyttet visning deaktivert.

Document Cloud-tjenester – arkitektur

Adobe Document Cloud-tjenestene omfatter følgende:

- **Organize PDF** – Sett inn, slett, endre rekkefølgen på eller roter sider i en PDF-fil
- **Create PDF** – Konverter Word-, Excel- og PowerPoint-dokumenter og bilder til PDF-filer
- **Export PDF** – Konverter PDF-filer enkelt til redigerbare Microsoft Word-, Excel-, PowerPoint- eller RTF-filer
- **Edit PDF** – Rediger eksisterende PDF-filer på en enkel måte fra mobilenheten eller den bærbare datamaskinen
- **Combine PDF** – Slå sammen flere filer til én PDF-fil og sett sammen dokumentpakker fra hvor som helst
- **Send & Track** – Send, spor og bekreft levering av dokumenter
- **Adobe Scan** – Fang inn hva som helst og konverter det til en søkbar PDF-fil av høy kvalitet
- **Adobe Sign** – Klargjør dokumenter og send dem til signering med sikre og pålitelige og rettsgyldige e-signaturer på en hvilken som helst enhet

Document Cloud-tjenester – sikkerhet

Håndtering av rettigheter og identiteter

IT-administratorer gir sluttbrukere tilgang til Adobe Document Cloud-tjenester ved å ta i bruk lisensiering for navngitte brukere i Adobe Admin Console. Acrobat Document Cloud støtter tre (3) ulike typer lisensiering for navngitte brukere:

- **Adobe ID** – For brukeradministrerte kontoer som driftes av Adobe, og som opprettes, eies og styres av enkeltbrukere. Adobe ID-kontoer har kun tilgang til Acrobat Document Cloud-tjenester hvis en IT-administrator aktiverer tilgang.
- **Enterprise ID** – Et bedriftsadministrert alternativ som driftes av Adobe, og som brukes for kontoer som er opprettet og styres av IT-administratorer fra kundens bedriftsorganisasjon. Organisasjonen eier og håndterer brukerkontoene og alle tilknyttede ressurser.
- **Federated ID** – En bedriftsadministrert konto der alle identitetsprofilene leveres av kundens system for identitetsadministrasjon med enkel pålogging (SSO), og som er opprettet av og eies og styres av kundens IT-infrastruktur. Adobe integreres med de fleste SAML 2.0-kompatible identitetsleverandører.

De fleste bedriftsorganisasjoner bruker Enterprise ID-er eller Federated ID-er for sine ansatte, underleverandører og frilansere, forutsatt at e-postadressen er innenfor bedriftsdomenet. Grunnen er at dette gir dem kontroll over både rettighetene og det brukergenererte innholdet som lagres

på vegne av den aktuelle ID-en. Hvis du vil ha mer informasjon om hver identitetstype, kan du se området for Adobes kundestøtte.

Adobe ID- og Enterprise ID-passordlagring bruker begge SHA-256-nummeralgoritmen i kombinasjon med salt-koder for passord og et stort antall hash-iterasjoner. Adobe overvåker kontinuerlig kontoer som driftes av Adobe, for å se etter uvanlig eller avvikende kontoaktivitet. Denne informasjonen blir så evaluert, slik at det raskt kan iverksettes tiltak for å redusere forekomsten av sikkerhetstrusler. For Federated ID-kontoer håndterer ikke Adobe brukernes passord. Hvis du vil ha mer informasjon, kan du se sikkerhetsoversikten for Adobes identitetshåndteringstjenester.

Elektroniske og digitale signaturer

Med Document Cloud-tjenester kan brukerne velge mellom to ulike verktøy for sikkert arbeid med signaturer:

Sporing er ikke tilgjengelig på mobilenheter.

Hvis du vil ha mer informasjon om Adobe Sign og tilhørende sikkerhetsfunksjoner, kan du se den tekniske oversikten for Adobe Sign.

- **Utfyllings- og signeringsverktøyet** – Drevet av Adobe Sign og lar brukerne håndtere komplette signeringsprosesser som er utviklet for å bidra til overholdelse av e-signaturlovene i USA, EU og de fleste industrialiserte land verden over. Med dette verktøyet kan de be om signaturer fra andre, spore signeringsprosessen og arkivere signerte dokumenter og revisjonsspor automatisk. Sikkerhetstiltak iverksettes i hele prosessen, og dokumentene og revisjonssporene sertifiseres av Adobe med en forsegling som hindrer andre i å utføre uautoriserte endringer.
- **Sertifikater-verktøyet** – Gir brukerne mulighet til å signere dokumenter med sertifikatbaserte digitale signaturer fra klarerte tjenesteleverandører på enten Adobe Approved Trust List (AATL) eller European Union Trusted Lists (EUTL). Signering med en sertifikat-ID utstedt av en klarert, ekstern sertifiseringsinstans (CA – Certificate Authority) er generelt anerkjent som en av de sikreste metodene for elektronisk signering av dokumenter. ID-en er unikt knyttet til og i stand til å identifisere signataren. Signatarens sertifikat knyttes kryptografisk til dokumentet under signeringstrinnet ved hjelp av den private nøkkelen som er unikt tilordnet den aktuelle signataren.

  Acrobat DC validerer signatarens signatur – og ektheten til det signerte dokumentet – ved å koble seg automatisk til CA-en for å få bekreftelse. Denne signaturtypen overholder standardene for elektronisk signering av PDF-dokumenter, blant annet PDF Advanced Electronic Signature (PAdES) del 2, 3 og 4 samt det amerikanske forsvarsdepartementets Joint Interoperability Test Command-bruk (JITC-bruk) av kryptografi og Public Key Infrastructure (PKI) med AES-256, RSA-4096, SHA-512 og RSA-PSS. Sertifikater-verktøyet gir brukerne også mulighet til å legge til tidsstempler i dokumentene og sertifisere dem med en forsegling som hindrer andre i å utføre uautoriserte endringer.

Document Cloud-tjenester – innholdslagring

Selv om administratorer tildeler individuell skybasert lagring for Enterprise ID- og Federated ID-kontoer via Adobe Admin Console, har de ikke direkte tilgang til filer i brukerens lagringplass for Document Cloud-tjenester. Sletting av Enterprise ID eller Federated ID med eksisterende lagring for delte tjenester gjør alle data i den skybaserte lagringen utilgjengelig for sluttbrukeren. Brukerens data blir slettet etter 90 dager.

Administratorer kan også bruke Admin Console til å tildele lagring til Adobe ID-kontoer. Administratorer kan ikke slette Adobe ID-kontoer, men de kan trekke tilbake både tildelt enterprise-lagringskvote og applikasjons- og tjenestetilgang. Dataene som er tilknyttet disse kontoene, blir slettet etter 90 dager.

Adobe Document Cloud-tjenester bruker lagring med flere leietakere (multitenant-lagring). Kundeinnholdet håndteres av en Amazon Elastic Compute Cloud-forekomst (Amazon EC2-forekomst) og lagres på en kombinasjon av Amazon Simple Storage Services-samlinger (Amazon S3-samlinger) og via en MongoDB-forekomst på Amazon Elastic Block Store (Amazon EBS). Selve innholdet blir lagret i Amazon S3-samlinger, og metadataene om innholdet blir lagret i Amazon EBS via MongoDB. Alt er beskyttet av IAM-roller (Identity and Access Management – identitets- og tilgangsbehandling) i den aktuelle Amazon Web Services-regionen (AWS-regionen).

Metadata og støtteressurser som lagres i Amazon EBS, krypteres med AES 256-bits kryptering med kryptografiske algoritmer godkjent av Federal Information Processing Standards (FIPS) 140-2 og i overensstemmelse med anbefalingene fra National Institute of Standards and Technology (NIST) 800-57.

Data lagres redundant i flere datasentre og på flere enheter i hvert datasenter. All nettverkstrafikk gjennomgår systematisk dataverifisering og kontrollsumberegninger for å forhindre ødeleggelser og sikre integriteten. Til slutt må det nevnes at lagret innhold replikeres synkront og automatisk til andre datasentertjenester innenfor den aktuelle kundens område, slik at dataintegriteten opprettholdes selv ved tap av data på to forskjellige steder.

Du finner mer informasjon om de underliggende Amazon-tjenestene her:

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

Dedikert krypteringsnøkkel

Som standard er innholdet og ressursene som er lagret i Amazon S3, kryptert med AES 256-bits symmetriske sikkerhetsnøkler som er unike for hver kunde og hver kundes domene. Hvis administratorer ønsker å legge til ytterligere et lag med kontroll og sikkerhet for noen av eller alle domenene i organisasjonen, kan de bruke en dedikert krypteringsnøkkel som administreres av AWS KMS og automatisk roteres årlig.

Administratorer kan også trekke tilbake denne dedikerte krypteringsnøkkelen via Admin Console. Dette gjør alle dataene som er kryptert med den nøkkelen, utilgjengelig for sluttbrukerne og hindrer både opplasting og nedlasting av innhold inntil krypteringsnøkkelen aktiveres på nytt.

Merk: Adobe Document Cloud-filer kan krypteres med den dedikerte krypteringsnøkkelen, men ikke metadata.

Du finner mer informasjon om krypteringsadministrasjon med dedikert nøkkel på disse Adobe-hjelpesidene:

- Administrere kryptering
- Vanlige spørsmål om dedikerte krypteringsnøkler

Amazon Web Services

Som tidligere nevnt er alle komponenter i Adobe Document Cloud-tjenestene driftet på AWS, inkludert Amazon EC2 og Amazon S3, i USA. Amazon EC2 er en webtjeneste som leverer automatisk skalerbar databehandlingskapasitet i skyen, noe som gjør webskalert databehandling enklere. Amazon S3 er generelt anerkjent som en svært pålitelig infrastruktur for datalagring og henting av alle mengder data.

AWS-plattformen leverer tjenester i overensstemmelse med fremgangsmåter av bransjestandard og gjennomgår regelmessige bransjeanerkjente sertifiseringer og kontroller. Du finner mer detaljert informasjon om AWS og Amazons sikkerhetskontroller på webområdet for AWS Cloud Security.

Driftsansvaret til AWS og Adobe

AWS drifter, administrerer og kontrollerer komponentene fra hypervisor-virtualiseringslaget ned til den fysiske sikkerheten til lokalene der Adobe Document Cloud-tjenestene kjører. Adobe har ansvar for og administrerer gjesteoperativsystemet (inkludert oppdateringer og sikkerhetsoppdateringer) og applikasjonsprogramvaren samt konfigurasjonen av sikkerhetsgruppebrannmuren fra AWS.

AWS drifter også den skybaserte infrastrukturen som Adobe bruker til å klargjøre ulike grunnleggende databehandlingsressurser, deriblant behandling og lagring. AWS-infrastrukturen omfatter lokaler, nettverk og maskinvare samt driftsprogramvaren (blant annet vertsoperativsystem og virtualiseringsprogramvare) som støtter klargjøringen og bruken av disse ressursene. Amazon utformer og administrerer AWS i overensstemmelse med fremgangsmåter av bransjestandard samt ulike sikkerhetsmessige krav.

Sikker administrasjon

Adobe bruker Secure Shell (SSH) og Secure Sockets Layer (SSL) for administrasjonstilkoblinger for å administrere AWS-infrastrukturen.

Geografisk plassering av kundedata på AWS-nettverket

Alt brukergenerert innhold som lastes opp til Document Cloud, blir lagret i AWS' datasentre i regionen US-East (Virginia). Innholdet blir sikkerhetskopiert i hvert datasenter samt i andre datasentre i samme region for å gi lastfordeling og redundans.

Geografisk plassering av identitetsdata på AWS-nettverket

Identitetsdata blir lagret i lastfordelte AWS-datasentre basert på flere regioner som er plassert i Virginia (US-East), Oregon (US-West), Irland (EU-West) og Singapore (AP-Southeast). Identitetsdata blir replikert på tvers av alle datasentre. Adobe overholder relevant lovgivning når det gjelder dataoverføring over grenser. Du finner en detaljert oversikt på https://www.adobe.com/no/privacy/eudatatransfers.html.

Isolering av kundedata / fordeling av kunder

AWS bruker sterke sikkerhets- og kontrollfunksjoner for leietakerisolasjon. Som et virtualisert miljø med flere leietakere implementerer AWS sikkerhetsadministrasjonsprosesser og andre sikkerhetskontroller som er utformet for å isolere hver kunde fra andre AWS-kunder. Adobe bruker AWS Identity and Access Management (IAM) til ytterligere å begrense tilgang til databehandlings- og lagringsforekomster.

Sikker nettverksarkitektur

AWS bruker nettverksenheter, blant annet brannmurer og andre grenseenheter, til å overvåke og kontrollere kommunikasjon i nettverkets ytre grense samt i viktige interne grenser i nettverket. Disse grenseenhetene bruker regelsett, tilgangskontrollister (ACL-er – Access Control Lists) og konfigurasjoner til å fremtvinge flyten av informasjon til spesifikke informasjonssystemtjenester. ACL-er, eller retningslinjer for trafikkflyt, finnes på hvert administrerte grensesnitt for å administrere og fremtvinge flyten av trafikk.

Amazon Information Security godkjenner alle ACL-retningslinjer og sender dem automatisk til hvert administrerte grensesnitt via verktøyet AWS ACL-Manage for å bidra til å sikre at disse administrerte grensesnittene bruker de nyeste ACL-ene.

Overvåking og beskyttelse av nettverk

AWS bruker ulike automatiserte overvåkingssystemer for å levere tjenesteytelse og -tilgjengelighet på et høyt nivå. Overvåkingsverktøy bidrar til å påvise uvanlig eller uautorisert aktivitet samt betingelser på punkter for inngående og utgående kommunikasjon. AWS-nettverket gir betydelig beskyttelse mot tradisjonelle problemer knyttet til nettverkssikkerhet:

- DDoS-angrep (distribuert tjenestenekt)
- MITM-angrep (mellommannbaserte angrep)
- IP-forfalsking
- Portskanning
- Pakkesniffing utført av andre leietakere

Du finner mer informasjon om overvåking og beskyttelse av nettverk på webområdet til AWS Cloud Security.

Påvisning av inntrengingsforsøk

Adobe overvåker aktivt Adobe Document Cloud-tjenester ved å bruke systemer for påvisning av inntrengingsforsøk (IDS-er) og systemer for å hindre inntrenging (IPS-er) av bransjestandard.

Logging

Adobe utfører logging på serversiden av kundeaktivitet knyttet til Adobe Document Cloud-tjenestene for å diagnostisere tjenesteavbrudd, spesifikke kundeproblemer og rapporterte feil. I loggene lagres kun Adobe ID-er for å bidra til å diagnostisere spesifikke kundeproblemer. Kombinasjoner av brukernavn og passord lagres ikke. Det er bare autorisert personell hos Adobes tekniske kundestøtte, nøkkelteknikere og utvalgte utviklere som har tilgang til loggene når de skal diagnostisere spesifikke problemer.

Tjenesteovervåking

AWS overvåker elektriske, mekaniske og overlevelsesrelaterte systemer og utstyr for å bidra til å identifisere tjenesteproblemer umiddelbart. AWS driver hele tiden forebyggende vedlikehold for å opprettholde kontinuerlig drift av utstyret.

Lagring og sikkerhetskopiering av data

Adobe lagrer alle Adobe Document Cloud-tjenestedata i Amazon S3, som leverer en lagringsstruktur med høy slitestyrke. For å bidra til økt slitestyrke lagrer PUT- og COPY-operasjoner i Amazon S3 synkront kundedata på flere steder og lagrer objekter redundant på flere enheter på flere steder i en Amazon S3-region.

Amazon S3 utfører kontrollsumberegninger på all nettverkstrafikk for å påvise skadede datapakker ved lagring eller henting av data. Datareplikering for Amazon S3-dataobjekter skjer i den regionale klyngen der dataene er lagret. Det blir ikke replikert til datasenterklynger i andre regioner.

Metadata replikeres ved å ta øyeblikksbilder av Amazon EBS-volumer og lagres på lignende måte som Amazon S3. Du finner mer informasjon om AWS-sikkerhet på webområdet til AWS Cloud Security.

Endringsadministrasjon

AWS autoriserer, logger, tester, godkjenner og dokumenterer rutinemesige endringer, endringer i nødstilfeller samt konfigurasjonsendringer i eksisterende AWS-infrastruktur i samsvar med bransjestandardene for lignende systemer. Amazon planlegger oppdateringer av AWS på en slik måte at kundene berøres i minst mulig grad. AWS kommuniserer med kunder via e-post eller AWS Service Health Dashboard i tilfeller der bruk av tjenesten kan få negativ innvirkning. Adobe oppdaterer også Adobe-systemstatus for Adobe Document Cloud.

Administrasjon av oppdateringer

AWS har ansvar for å oppdatere systemer som støtter leveringen av AWS-tjenester, blant annet hypervisor- og nettverkstjenestene. Adobe har ansvar for å oppdatere gjesteoperativsystemene, programvaren og applikasjonene som kjører i AWS. Når en oppdatering er påkrevd, leverer Adobe en ny, forhåndsherdet forekomst av operativsystemet og applikasjonen i stedet for å levere en oppdatering.

Fysiske og miljømessige kontroller i AWS

Fysiske og miljømessige kontroller i AWS er spesifikt beskrevet i SOC Type 1- og SOC Type 2-rapportene. Følgende del beskriver noen av sikkerhetstiltakene og -kontrollene som er på plass på AWS-datasentre verden over. Du finner mer informasjon om AWS-sikkerhet på webområdet til AWS Cloud Security.

Fysisk sikkerhet i lokalene

AWS-datasentre bruker arkitektoniske og tekniske tilnærminger av bransjestandard. AWS-datasentrene er plassert i anonyme lokaler, og Amazon kontrollerer den fysiske tilgangen både på utsiden og ved inngangene til bygningen ved hjelp av profesjonelt sikkerhetspersonell, videoovervåking, systemer for påvisning av inntrengingsforsøk og andre elektroniske tiltak. Autorisert personell må gå gjennom autentisering med to faktorer minst to ganger for å få tilgang til datasenteretasjene. Alle besøkende og underleverandører må vise legitimasjon, og de blir skrevet inn og eskortert hele veien av autorisert personell.

AWS gir tilgang til og informasjon om datasenterne kun til ansatte og underleverandører som har behov for disse rettighetene. Når ansatte ikke lenger har behov for disse rettighetene, blir tilgangen deres umiddelbart trukket tilbake, selv om de forsatt er ansatt hos Amazon eller AWS. All fysisk tilgang som AWS-ansatte har til datasentrene, blir rutinemessig logget og kontrollert.

Brannvern

AWS installerer utstyr for automatisk brannvarsling og -slukking i alle AWS-datasentre. Brannvarslingssystemene har røyksensorer i alle datasentermiljøer, steder med mekanisk og elektrisk infrastruktur, kjølerom og rom med generatorutstyr. Disse områdene er beskyttet av ulike typer sprinkleranlegg.

Kontrollert miljø

AWS bruker et klimastyringssystem for å opprettholde en konstant driftstemperatur for servere og annen maskinvare, noe som hindrer overoppheting og reduserer muligheten for avbrudd i tjenesten. AWS-datasentrene har optimale luftforhold. Både personell og systemer hos AWS overvåker og kontrollerer at temperatur og fuktighet holder rett nivå.

Reservestrøm

Strømsystemene i AWS-datasentrene er utformet for å være fullt redundante og mulige å vedlikeholde uten at det går ut over driften på noe tidspunkt. UPS-enheter (avbruddsfri strømforsyning) leverer reservestrøm til kritiske og viktige belastninger i lokalene i tilfelle strømbrudd. Datasentrene har generatorer for reservestrøm for hele anlegget.

Gjenoppretting

AWS-datasentrene har høyt tilgjengelighetsnivå, og system- eller maskinvarefeil har minimal innvirkning på driften. Alle datasentre er bygd i klynger i ulike globale regioner, slik at de er tilkoblet døgnet rundt, hele året. Det er ingen "kalde" datasentre. Hvis det oppstår feil, sørger automatiserte prosesser for at kundedatatrafikken flyttes bort fra det berørte området.

Kjerneapplikasjoner er utrullert i en N+1-konfigurasjon, noe som betyr at hvis det oppstår feil i et datasenter, er det tilstrekkelig kapasitet til å muliggjøre lastfordeling til de gjenstående stedene. Du finner mer informasjon om AWS' protokoller for gjenoppretting på webområdet til AWS Cloud Security.

Risiko- og sårbarhetsadministrasjon hos Adobe

Adobe har som mål å sikre at prosessen vår for administrasjon, respons, reduksjon og løsing av risikoer og sårbarheter er fleksibel og presis. Vi overvåker kontinuerlig trussellandskapet, deler kunnskapen vår med sikkerhetseksperter verden over, løser problemer straks de oppstår, og sender denne informasjonen tilbake til utviklerne våre for å bidra til å oppnå et høyest mulig sikkerhetsnivå for alle Adobe-produkter og -tjenester.

Inntrengingstester

Adobe godkjenner og engasjerer ledende eksterne sikkerhetsselskaper til å utføre inntrengingstester som kan avdekke mulige sikkerhetssårbarheter og forbedre den generelle sikkerheten til Adobes produkter og tjenester. Når Adobe mottar rapporten fra det eksterne selskapet, blir sårbarhetene dokumentert og alvorlighetsgraden og prioriteten vurdert, og det blir deretter utarbeidet en strategi for å redusere eller fjerne sårbarhetene. Adobe utfører en komplett inntrengingstest hvert år samt sårbarhetsskanninger hver måned.

Internt utfører sikkerhetsavdelingen hos Adobe Document Cloud en risikovurdering av alle komponentene og tjenestene til Document Cloud hvert kvartal samt før hver nye utgave. Sikkerhetsavdelingen hos Document Cloud samarbeider med tekniske avdelinger og utviklere for å sikre at alle farene knyttet til høyrisikosårbarheter reduseres før hver nye utgave. Du finner mer informasjon om Adobes prosedyrer for inntrengingstesting i oversikten over Adobe Secure Engineering.

Respons og varsling

Nye sårbarheter og trusler dukker opp hver dag, og Adobe har som mål å reagere på og redusere truslene etter hvert som de oppstår. I tillegg til å abonnere på bransjeomfattende kunngjøringslister over sårbarheter, deriblant United States Computer Emergency Readiness Team (US-CERT), Bugtraq og SANS, abonnerer Adobe også på listene over de nyeste sikkerhetsvarslene fra andre store sikkerhetsleverandører.

Du finner mer informasjon om Adobes prosess for respons og varsling i oversikten over Adobes respons.

Analyser

Ved undersøkelser av hendelser følger Document Cloud-avdelingen Adobes analyseprosess, som omfatter en komplett avbildning eller minnedump av berørte maskiner, trygg oppbevaring av bevis samt dokumentering av prosessen.

Adobes sikkerhetsorganisasjon

Som en del av vårt mål om å levere sikre produkter og tjenester er alt sikkerhetsarbeid hos Adobe samlet under sikkerhetssjefen (CSO). Sikkerhetssjefens kontor koordinerer alle sikkerhetsinitiativer knyttet til produkter og tjenester samt implementeringen av Adobe Secure Product Lifecycle (SPLC).

Sikkerhetssjefen leder også Adobe Secure Software Engineering Team (ASSET), som er en egen gruppe sikkerhetseksperter som fungerer som konsulenter for de viktigste produkt- og driftsarbeidsgruppene hos Adobe, deriblant Adobe Document Cloud-gruppen. ASSET-forskerne jobber med de ulike produkt- og driftsarbeidsgruppene hos Adobe for å oppnå de rette sikkerhetsnivåene for produkter og tjenester og gi råd til gruppene om sikkerhetsløsninger som gir gode og repeterbare prosesser for utvikling, utrullering, drift og respons.

Adobes sikkerhetsorganisasjon

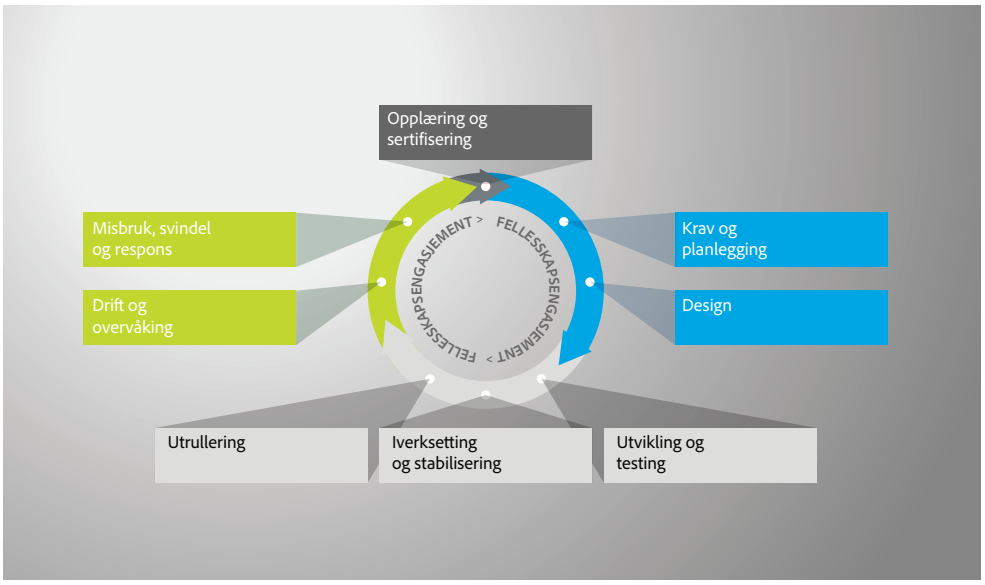
Adobe Secure Product Development

På samme måte som andre viktige Adobe-organisasjoner knyttet til produkter og tjenester bruker Adobe Document Cloud-organisasjonen Adobe SPLC-prosessen. Adobe SPLC er et omfattende sett av flere hundre sikkerhetsaktiviteter som spenner over utviklingspraksis for programvare, prosesser og verktøy, og som er integrert i flere faser av produktlivssyklusen – fra design og utvikling til kvalitetssikring, testing og utrullering. ASSET-sikkerhetsforskerne gir spesifikk SPLC-veiledning for de ulike nøkkelproduktene og -tjenestene basert på en vurdering av mulige sikkerhetsproblemer. Adobe SPLC støttes av et sterkt fellesskapsengasjement og er i stadig utvikling, slik at det alltid er oppdatert på endringer i teknologi, sikkerhetspraksiser og trussellandskap.

Adobe Secure Product Lifecycle

Adobe SPLC-aktivitetene omfatter noen av eller alle følgende anbefalte fremgangsmåter, prosesser og verktøy, avhengig av den spesifikke Adobe Document Cloud-komponenten:

- sikkerhetsopplæring og -sertifisering for produktgrupper
- analyse av produkttilstand, risiko og trussellandskap
- retningslinjer, regler og analyse for sikker koding
- tjenestekart, sikkerhetsverktøy og testemetoder som veileder sikkerhetsgruppen for Adobe Document Cloud og bidrar til å håndtere de ti største sikkerhetsrisikoene mot webapplikasjoner, som oppgitt av Open Web Application Security Project (OWASP), og de 25 farligste programvarefeilene, som oppgitt av CWE/SANS
- gjennomgang av sikkerhetsarkitektur og inntrengingstesting
- kildekodegjennomganger som bidrar til å fjerne kjente feil som kan føre til sårbarheter
- validering av brukergenerert innhold
- skanning av applikasjoner og nettverk
- fullstendig tilretteleggingsgjennomgang, responsplaner og utgivelse av opplæringsmateriell for utviklere



Adobe Secure Product Lifecycle

Adobe Software Security Certification Program

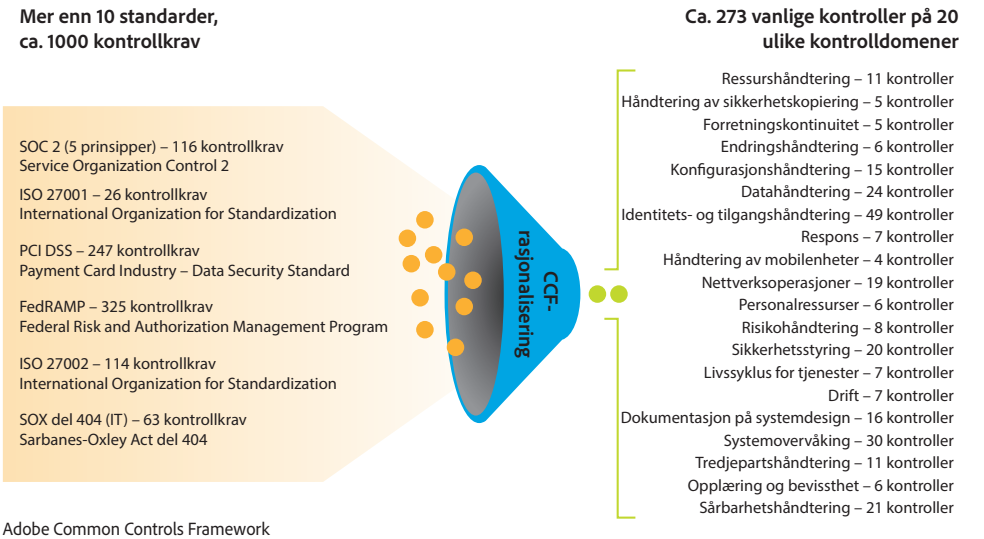
Som en del av Adobe SPLC utfører Adobe kontinuerlig sikkerhetsopplæring i utviklergruppene for å øke kunnskapen om sikkerhet i hele selskapet og forbedre den generelle sikkerheten til produktene og tjenestene våre. Ansatte som deltar i Adobe Software Security Certification Program, får ulike sertifiseringsnivåer ved å fullføre sikkerhetsprosjekter. Du finner mer informasjon om produktsikkerhetspraksisene i oversikten over Adobe Secure Engineering.

Du finner mer informasjon om Adobe Software Security Certification Program i det tekniske dokumentet om Adobes sikkerhetskultur.

Document Cloud-tjenester – overholdelse

Adobe Common Controls Framework (CCF) er et sett av sikkerhetsaktiviteter og samsvarskontroller som er implementert i produktvirksomhetsgruppene samt i ulike deler av infrastruktur- og applikasjonsgruppene.

Under opprettingen av CCF analyserte Adobe kriteriene for de vanligste sikkerhetssertifiseringene for nettskybaserte bedrifter og rasjonaliserte de mer enn 1000 kravene ned til Adobe-spesifikke kontroller som tilordnes en rekke bransjestandarder.



Adobe Common Controls Framework

Gjeldende forskrifter og overholdelse for Adobe Document Cloud-tjenester

SOC 2 er et sett med sikkerhetsprinsipper som definerer ledende praksiskontroller som er relevante for sikkerheten, konfidensialiteten og personvernet. Adobe Document Cloud-tjenestene overholder SOC 2 Type 2 (sikkerhet og tilgjengelighet).

ISO 27001 er et sett med globalt vedtatte standarder som skisserer strenge sikkerhetskrav og gir en systematisk tilnærming til håndtering av konfidensialiteten, integriteten og tillgjengeligheten av kundeinformasjon. Adobe Document Cloud-tjenestene overholder ISO 27001:2013.

Payment Card Industry Data Security Standard (PCI DSS) er en sikkerhetsstandard for bedriftsintern informasjon for organisasjoner som håndterer betalingskortinformasjon, for eksempel kredittkortnumre. Ved å være en tjenesteleverandør som overholder PCI DSS, kan Adobe hjelpe kundene med å overholde PCI-kravene for sikker håndtering av personlig identifiserbare data som er tilknyttet en kortinnehaver.

Gramm-Leach-Bliley Act (GLBA) krever at finansinstitusjoner beskytter kundenes personlige data. Adobe Document Cloud-tjenestene er GLBA-klare, noe som betyr at de gjør det mulig for finanskundene våre å overholde GLBA-kravene for bruk av tjenesteleverandører.

Federal Risk and Authorization Management Program (FedRAMP) er et program som gjelder for alle offentlige organer og gir en standardisert tilnærming til sikkerhetsvurdering, autentisering og kontinuerlig overvåking for nettskybaserte produkter og tjenester. Adobe Document Cloud-tjenestene er FedRAMP-tilpassede, noe som betyr at de gjør det mulig for kundene våre å overholde FedRAMP-kravene.

Family Educational Rights and Privacy Act (FERPA) i USA er utviklet for å ivareta konfidensialiteten til informasjonen i utdanningsjournalene og -registrene knyttet til studenter i USA. I henhold til FERPA-retningslinjene kan Adobe kontraktsmessig samtykke i å fungere som en "skoleansatt" når det gjelder håndtering av regulerte studentdata, noe som gir utdanningskundene mulighet til å overholde FERPA-kravene.

SAFE-BioPharma-standarden beskriver kravene for standardisert identitetstillit for enten identitetsautentisering eller digital signering. Adobe Document Cloud er sertifisert for å overholde den digitale SAFE-BioPharma-identifikasjonsstandarden. Adobe Acrobat DC kan trygt brukes i og er kompatibel med SAFE-BioPharma-arbeidsflyter. I tillegg overholder Adobe Document Cloud-tjenestene og Adobe Sign SOC 2 Type 2.

Hvis du vil ha mer informasjon om de samsvarsrelaterte aspektene ved Adobe Sign, kan du se den tekniske oversikten for Adobe Sign.

Kundene er til syvende og sist selv ansvarlig for å sikre overholdelse av de juridiske forpliktelsene og at løsningene våre dekker overholdelsesbehovene og sikres på en hensiktsmessig måte.

Adobe-ansatte

Adobe har ansatte og avdelinger verden over og implementerer følgende prosesser og prosedyrer i hele selskapet for å beskytte mot sikkerhetstrusler.

Ansattes tilgang til kundedata

Adobe opprettholder segmenterte utviklings- og produksjonsmiljøer for Adobe Document Cloud og bruker tekniske kontroller til å sikre at tilgangen til aktive produksjonssystemer begrenses til nettverks- og applikasjonsnivå. Ansatte har spesifikke tillatelser til å få tilgang til utviklings- og produksjonssystemer, og ansatte uten legitime forretningsformål har ikke tilgang til disse systemene.

Bakgrunnssjekker

Adobe innhenter bakgrunnssjekkrapporter for sysselsettingsformål. Det spesifikke innholdet i og omfanget til rapporten som Adobe vanligvis er ute etter, inneholder forespørsler om utdanningsbakgrunn, jobberfaring og rettsopptegnelser, blant annet politiattester og referanser innhentet fra profesjonelle og personlige medarbeidere, alt tillatt i henhold til gjeldende lov. Disse kravene til bakgrunnssjekk gjelder for vanlige nyansatte i USA, inkludert ansatte som skal håndtere systemer eller ha tilgang til kundeinformasjon. Nye ansatte fra vikarbyråer i USA er underlagt krav til bakgrunnssjekk via det aktuelle vikarbyrået, i samsvar med Adobes retningslinjer for bakgrunnssjekk. Utenfor USA utfører Adobe bakgrunnssjekker av enkelte nyansatte i henhold til Adobes retningslinjer for bakgrunnssjekk og gjeldende lokale lover.

Oppsigelse av ansatte

Når en av de ansatte forlater Adobe, sender lederen til den ansatte inn et oppsigelsesskjema. Når dette er godkjent, setter Adobes personalavdeling i gang en e-postarbeidsflyt for å informere relevante interessenter om å iverksette konkrete tiltak som leder opp til den ansattes siste arbeidsdag. I de tilfellene der Adobe sier opp en av de ansatte, sender Adobes personalavdeling et lignende e-postvarsel til de relevante interessentene, blant annet med det spesifikke tidspunktet for oppsigelsen.

Adobes bedriftssikkerhetsavdeling planlegger deretter følgende tiltak for å sikre at den ansatte ikke har tilgang til Adobes konfidensielle filer eller kontorer etter siste arbeidsdag:

- fjerning av e-posttilgang
- fjerning av ekstern VPN-tilgang
- ugyldiggjøring av kontor- og datasentermerke
- avslutting av nettverkstilgang

På forespørsel kan lederne be sikkerhetsvaktene om å følge den oppsagte ansatte ut fra Adobe-kontoret eller -bygningen.

Sikkerheten i lokalet

Samtlige av Adobes bedriftskontorer har vakter som beskytter lokalene døgnet rundt. Adobe-ansatte har et nøkkelkort med et ID-merke for å få tilgang til den aktuelle bygningen. Besøkende går inn hovedinngangen, sjekker inn og ut ved resepsjonen, viser et midlertidig ID-merke for besøkende og ledsages av en av de ansatte. Adobe holder alt av serverutstyr, utviklingsmaskiner, telefonsystemer, fil- og e-postservere og andre sensitive systemer låst til enhver tid i miljøstyrte serverrom som kun er tilgjengelig for ansatte med riktig autorisasjon.

Virusbeskyttelse

Adobe skanner alle innkommende og utgående e-postmeldinger for å se etter kjente trusler om skadelig programvare.

Kundedatakonfidensialitet

Adobe behandler alltid alle kundedata som konfidensielle. Adobe bruker ikke og deler ikke informasjonen som samles inn på vegne av en kunde, med unntak av det som eventuelt tillates i en kontrakt med den aktuelle kunden, og som angitt i Adobes bruksbetingelser og Adobes retningslinjer for personvern.

Konklusjon

Adobes proaktive tilnærming til sikkerhet og strenge prosedyrer som er beskrevet i dette dokumentet, bidrar til å styrke sikkerheten til Adobe Acrobat DC, Acrobat Reader DC og Document Cloud-tjenestene – og dine konfidensielle data. Vi hos Adobe tar sikkerheten til den digitale opplevelsen på alvor. Vi overvåker kontinuerlig det skiftende trussellandskapet for å ligge i forkant av ondsinnede aktiviteter og styrke sikkerheten til kundedataene.

Hvis du vil ha mer informasjon, kan du gå til Adobe Trust Center.

Adobe Systems Nordic AB
Box 47, 164 93 Kista, Sverige
www.adobe.no, www.adobe.com

6/19