Adobe Acrobat DC met Adobe Document Cloud-services – Beveiligingsoverzicht

Inhoudsopgave

Hoewel Adobe Sign deel uitmaakt van Document Cloud PDF-services, staat de beveiligingsfunctionaliteit los daarvan.

Samenvatting

Adobe neemt de beveiliging van je digitale ervaring heel serieus. Beveiligingspraktijken zijn diep geworteld in onze interne softwareontwikkeling, operationele processen en tools. Deze praktijken worden strikt door onze multidisciplinaire teams gevolgd om incidenten te voorkomen, te detecteren en daar op een zinvolle manier op te reageren. We blijven op de hoogte van de laatste bedreigingen en kwetsbaarheden via onze samenwerking met partners, vooraanstaande onderzoekers, onderzoeksinstellingen op het gebied van beveiliging en andere branche-organisaties. We voegen regelmatig geavanceerde beveiligingstechnieken toe aan de producten en diensten die we aanbieden.

Adobe-services die betrekking hebben op content van klanten hebben tal van branche-certificeringen gekregen. Een uitvoerig overzicht van alle nalevingscertificeringen en -standaarden, alsook de overheidsvoorschriften die door Adobe-producten en -oplossingen worden ondersteund, kun je vinden in de actuele lijst met certificeringen, standaarden en voorschriften. Zie de pagina over AVG-gereedheid voor informatie over de AVG.

Dit artikel gaat in op de meerlagige verdedigingsaanpak en beveiligingsprocedures die Adobe heeft geïmplementeerd om de beveiliging van Adobe Acrobat DC, Acrobat Reader DC, Document Cloud, Document Cloud-services en bijbehorende data te verbeteren.

Overzicht van Acrobat DC met Document Cloud-services

Adobe Acrobat DC combineert de nieuwste Acrobat-desktopsoftware met premium functies in de mobiele Acrobat Reader-app en de online services van Adobe Document Cloud om organisaties te helpen eindgebruikers op elk apparaat de gewenste connectiviteit en productiviteit te geven, terwijl de beveiliging op alle apparaten wordt gewaarborgd. Met Adobe Acrobat DC en Document Cloud-services kunnen klanten content omzetten in een elektronisch document dat ze met anderen kunnen delen en kunnen ze eenvoudig vanuit elke Adobe-cloudservice, Adobe-desktopapplicatie of mobiele Adobe-app PDF-bestanden genereren, bewerken en transformeren.

Documentbeveiligingsvoorzieningen in Acrobat

Bescherming van inhoud

Adobe Acrobat DC biedt een reeks redactietools waarmee klanten gevoelige of vertrouwelijke informatie kunnen beschermen, en onder andere tekst en afbeeldingen in een document permanent onleesbaar kunnen maken voordat ze het document verspreiden. Bovendien kunnen gebruikers content zoeken en onleesbaar maken op basis van patronen, zoals telefoonnummers, creditcardnummers en e-mailadressen. De onleesbaar gemaakte informatie wordt volledig uit het bestand verwijderd; niet alleen maar gemaskeerd zoals bij andere tools of methoden het geval is. Met de documentopschoningsfunctie kunnen klanten ook verborgen informatie en niet-grafische objecten verwijderen, zoals metadata die in de PDF aanwezig kan zijn.

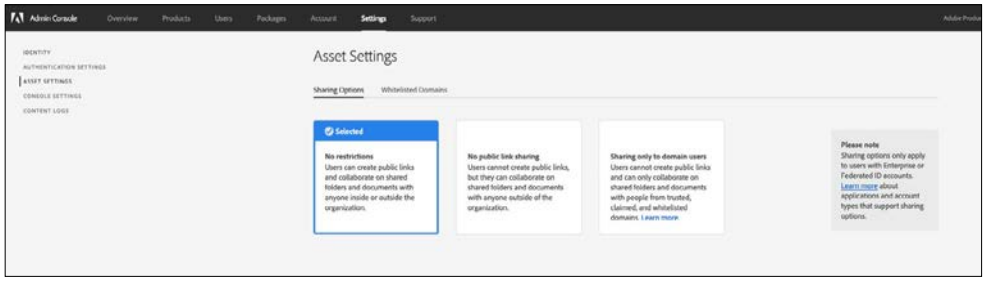
Bestandsdeling

Alle Document Cloud-bestanden die in de cloud zijn opgeslagen, worden automatisch als “Privé” aangemerkt, wat inhoudt dat de content alleen zichtbaar is voor de eindgebruiker die deze heeft geüpload. Een eindgebruiker moet expliciet actie ondernemen om die content te delen; anders blijft deze privé. Alle Document Cloud-content wordt gedeeld door via e-mail, een tekstbericht of samenwerkingssoftware een koppeling naar de Document Cloud-content naar de ontvangers te sturen.

Gebruikers van Document Cloud-services kunnen bestanden op twee manieren delen: Alleen bekijken of Reviewen. Als de gebruiker de koppeling verstuurt met de beperking Alleen bekijken, kan de ontvanger de content alleen bekijken. Als de gebruiker het document echter ter review verstuurt, kan de ontvanger het document van commentaar voorzien, maar kan hij het document niet wijzigen.

Assetinstellingen en deelbeperkingen

Assetinstellingen geven een organisatie controle over de manier waarop medewerkers assets met mensen buiten de organisatie delen. De IT-beheerder kan een beperking selecteren om bepaalde deelfuncties binnen Document Cloud te blokkeren voor medewerkers. Daarbij kunnen ze ook het delen van content via uitnodigingen met ontvangers in de geclaimde, vertrouwde en op de witte lijst geplaatste domeinen beperken. Wanneer dit beleid is ingesteld, kunnen gebruikers geen assets van de organisatie delen met externe gebruikers die niet op de lijst met toegestane domeinen staan.



Assetinstellingen in de Admin Console

Microsoft Information Protection (MIP)

Klanten die Acrobat DC of Acrobat Reader DC gebruiken om bestanden te openen die zijn beveiligd met MIP-oplossingen (Microsoft Information Protection), waaronder Azure Information Protection (AIP) en gegevensbescherming bij Microsoft Office 365, kunnen dit document raadplegen.

Beveiligde modus in Adobe Reader DC

Om klanten te beschermen tegen kwaadaardige code die probeert de PDF te gebruiken om naar het bestandsysteem van een computer te schrijven of om het te lezen, biedt Adobe een implementatie van sandboxing-technologie, de "Beveiligde modus" genaamd, die in Adobe Reader X is geïntroduceerd.

Sandboxing is een beveiligingsmethode waarmee een besloten uitvoeringsomgeving wordt gecreëerd waarin programma's met beperkte rechten of machtigingen kunnen worden uitgevoerd. Sandboxen bieden gebruikerssystemen bescherming tegen beschadiging door niet-vertrouwde documenten die uitvoerbare code bevatten. Bij Acrobat Reader DC zou de niet-vertrouwde content bestaan uit een PDF-bestand en eventuele processen die daarmee worden aanroepen. Acrobat Reader DC beschouwt alle PDF-documenten als potentieel schadelijk en beperkt alle bewerkingen die door het PDF-bestand worden aangeroepen tot de sandbox.

In Acrobat Reader DC voorkomt de Beveiligde modus dat malware op een computersysteem wordt geïnstalleerd. Zo kunnen organisaties voorkomen dat kwaadwillenden toegang krijgen tot gevoelige gegevens en intellectueel eigendom op hun netwerk. De Beveiligde modus is standaard ingeschakeld wanneer een gebruiker Acrobat Reader DC start. Omdat het programma een lager toegangsniveau krijgt toegewezen, worden Microsoft Windows-systemen beschermd tegen schadelijke PDF-bestanden die proberen gegevens naar of van het bestandssysteem van de computer te schrijven of te lezen, bestanden te verwijderen of op andere wijze systeeminformatie aan te passen.

De Beveiligde modus in Windows 8 en hoger kan ook worden uitgevoerd in een Windows-AppContainer, wat een nog beter afgesloten omgeving waarborgt voor klanten die de Beveiligde modus inschakelen.

Beveiligde weergave in Acrobat DC

De Beveiligde weergave, die vergelijkbaar is met de Beveiligde modus in Adobe Reader, is een implementatie van sandboxing-technologie voor de uitgebreide Adobe Acrobat-functionaliteit. In Acrobat DC gaat de Beveiligde modus verder dan het blokkeren van schrijfaanvallen waarmee wordt geprobeerd om via de PDF-bestandsindeling schadelijke code op een computersysteem uit te voeren: ook leesaanvallen worden geblokkeerd om te voorkomen dat kwaadwillenden via PDF-bestanden gevoelige gegevens of intellectueel eigendom stelen.

Net als in de Beveiligde modus wordt de uitvoering van niet-vertrouwde programma's (bijvoorbeeld een PDF-bestand en de processen die daarmee worden aangeroepen) in de Beveiligde weergave beperkt tot een sandbox, om te voorkomen dat kwaadwillenden via de PDF-indeling gegevens naar of van het bestandssysteem van de computer schrijven of lezen. Bij de Beveiligde weergave wordt ervan uitgegaan dat alle PDF-bestanden potentieel schadelijk zijn en wordt de verwerking beperkt tot de sandbox, tenzij de gebruiker specifiek aangeeft dat hij of zij het bestand vertrouwt.

De Beveiligde weergave wordt ondersteund in de twee scenario's waarin gebruikers PDF-documenten openen, namelijk in de autonome Acrobat DC-toepassing én in een browser. De Beveiligde weergave in Windows 8 en hoger wordt altijd uitgevoerd in een AppContainer. Dit biedt een nog specifiekere, afgesloten omgeving voor klanten die de Beveiligde weergave inschakelen.

Wanneer een gebruiker een niet-vertrouwd bestand opent binnen de Beveiligde weergave, geeft Acrobat DC boven in de balk in het weergavevenster een bericht weer. Dit bericht geeft aan dat het bestand niet wordt vertrouwd en maakt de gebruiker erop attent dat de Beveiligde weergave actief is, waarin veel Acrobat DC-functies uitgeschakeld zijn en er maar beperkte gebruikersinteractie met het bestand mogelijk is. In feite is het bestand in de alleen-lezenmodus geopend, waarmee wordt voorkomen dat eventuele ingesloten of meegestuurde content schade aan het systeem kan toebrengen.

Als de gebruiker het bestand vertrouwt en alle functies van Acrobat DC wil inschakelen, klikt hij of zij op de knop 'Enable All Features' (Alle functies inschakelen) op de berichtenbalk. Hiermee wordt de Beveiligde weergave beëindigd en wordt het bestand permanent vertrouwd doordat het wordt toegevoegd aan de lijst met gemachtigde locaties van Acrobat. De volgende keren dat het vertrouwde PDF-bestand wordt geopend, worden de beperkingen van de Beveiligde weergave automatisch uitgeschakeld.

Architectuur van Document Cloud-services

De Adobe Document Cloud-services zijn onder andere:

- **Organize PDF** – Pagina's invoegen, verwijderen, verplaatsen of roteren in een PDF
- **Create PDF** – Word-, Excel- en PowerPoint-documenten en afbeeldingen of foto's omzetten in PDF-bestanden
- **Export PDF** – Eenvoudig PDF's omzetten in bewerkbare Microsoft Word-, Excel-, PowerPoint- of RTF-bestanden
- **Edit PDF** – Moeiteloos bestaande PDF's bewerken op je mobiele apparaat of laptop
- **Combine PDF** – Overal meerdere bestanden combineren tot één PDF-bestand en documentpakketten maken
- **Send & Track** – Documenten versturen, volgen en de levering ervan bevestigen
- **Adobe Scan** – Informatie vastleggen en omzetten in een doorzoekbare, hoogwaardige PDF
- **Adobe Sign** – Documenten opstellen en versturen om ze op een veilige, vertrouwde en juridisch bindende manier elektronisch te laten ondertekenen, op welk apparaat dan ook

Beveiliging van Document Cloud-services

Toegangs- en identiteitbeheer

IT-beheerders geven eindgebruikers via de Adobe Admin Console op basis van gebruikersgebonden licenties toegang tot Adobe Document Cloud-services. Acrobat Document Cloud ondersteunt drie soorten gebruikersgebonden licenties:

- **Adobe ID** – Voor door Adobe gehoste en door gebruikers beheerde accounts die door afzonderlijke gebruikers worden gemaakt en eigendom van die gebruikers zijn. Adobe ID-accounts hebben alleen toegang tot Acrobat Document Cloud-services als een IT-beheerder die toegang inschakelt.
- **Enterprise ID** – Een door Adobe gehoste, door bedrijven beheerde optie voor accounts die vanuit de organisatie van het bedrijf door IT-beheerders worden gemaakt en beheerd. De gebruikersaccounts en alle daaraan gekoppelde assets zijn eigendom van, en worden beheerd door, de organisatie.
- **Federated ID** – Een door ondernemingen beheerde account waarbij alle identiteitsprofielen worden aangeleverd door het SSO-identiteitbeheersysteem (single sign-on) van de klant. De accounts worden gemaakt en beheerd door, en zijn eigendom van, de IT-infrastructuur van de klant. Adobe biedt integraties met de meeste identiteitsaanbieders die aan de eisen van SAML 2.0 voldoen.

De meeste ondernemingen gebruiken Enterprise ID's of Federated ID's voor hun werknemers, aannemers en freelancers, mits het e-mailadres zich in het bedrijfsdomein bevindt, omdat ze op die manier controle houden over zowel de rechten als de gebruikerscontent die namens die ID wordt opgeslagen. Meer informatie over de verschillende identiteitstypen kun je vinden op de klantenondersteuningswebsite van Adobe.

Voor de opslag van de wachtwoorden voor Adobe ID's en Enterprise ID's wordt gebruikgemaakt van het hash-algoritme SHA-256 in combinatie met wachtwoord-salt en een groot aantal hash-iteraties. Adobe controleert de door Adobe gehoste accounts voortdurend op ongebruikelijke of afwijkende accountactiviteit, en evalueert deze informatie om snel de beveiligingsrisico's te beperken. Voor Federated ID-accounts worden de gebruikerswachtwoorden niet door Adobe beheerd. Raadpleeg voor meer informatie het beveiligingsoverzicht voor Adobe Identity Management Services.

Elektronische en digitale handtekeningen

Met Document Cloud-services kunnen gebruikers op twee manieren veilig met handtekeningen werken:

- **Tool Fill & Sign** – Met deze tool, die wordt aangestuurd door Adobe Sign, kunnen gebruikers volledige ondertekeningstrajecten beheren die voldoen aan de wetten inzake elektronische ondertekening die in de Verenigde Staten, de Europese Unie en de meeste geïndustrialiseerde landen over de gehele wereld gelden. Met deze tool kunnen ze documenten laten ondertekenen, het ondertekeningstraject volgen en ondertekende documenten en controlesporen automatisch archiveren. Op het hele traject worden beveiligingsmaatregelen toegepast, terwijl de documenten en controlesporen door Adobe worden gecertificeerd met een onvervalsbaar-zegel.

- **Tool Certificates** – Hiermee kunnen gebruikers documenten ondertekenen met op certificaten gebaseerde digitale handtekeningen van vertrouwde providers die op de Adobe Approved Trust List (AATL) of de European Union Trusted List (EUTL) staan. Ondertekening met een certificaat-ID die is afgegeven door een vertrouwde, externe certificeringsautoriteit (CA) wordt algemeen als een veilige manier gezien om documenten elektronisch te ondertekenen. De ondertekenaar kan worden geïdentificeerd aan de hand van deze ID, die op unieke wijze aan de ondertekenaar is verbonden. Het certificaat van de ondertekenaar wordt tijdens de ondertekeningsstap cryptografisch verbonden aan het document, op basis van de persoonlijke sleutel die exclusief in het bezit van de ondertekenaar is.

  Acrobat DC valideert de handtekening van de ondertekenaar – en de authenticiteit van het door hem of haar ondertekende document – door die automatisch te laten verifiëren bij de certificeringsautoriteit. Dit type ondertekening voldoet aan diverse PDF-standaarden voor elektronische ondertekening, waaronder PDF Advanced Electronic Signature (PAdES) deel 2, 3 en 4, alsook aan de vereisten van JITC-gebruik van cryptografische beveiliging van het Amerikaanse Ministerie van Defensie en Public Key Infrastructure (PKI) met AES-256, RSA-4096, SHA-512 en RSA-PSS. Met de Certificates-tool kunnen gebruikers ook tijdstempels toevoegen aan documenten, en deze documenten certificeren met een onvervalsbaar zegel.

Tracking is niet mogelijk op mobiele apparaten.

Meer informatie over Adobe Sign en de beveiligingsfunctionaliteit daarvan kun je vinden in het technische overzicht van Adobe Sign.

Opslag van content voor Document Cloud-services

Hoewel beheerders via de Adobe Admin Console afzonderlijke cloudopslag aan Enterprise ID- en Federated ID-accounts toewijzen, hebben ze geen rechtstreekse toegang tot de bestanden in de opslagruimte die gebruikers voor Document Cloud-services ter beschikking staat. Wanneer een Enterprise ID of Federated ID, inclusief de bestaande gedeelde services-opslag, wordt verwijderd, heeft de eindgebruiker geen toegang meer tot de data in de cloudopslag en wordt de data van die gebruiker na 90 dagen verwijderd.

Beheerders kunnen ook via de Admin Console opslag toewijzen aan Adobe ID-accounts. Hoewel ze geen Adobe ID-accounts kunnen verwijderen, kunnen beheerders wel het toegekende bedrijfs-opslagquota en de toegang tot applicaties en services intrekken. De data die aan deze accounts is gekoppeld, wordt na 90 dagen verwijderd.

Adobe Document Cloud-services maken gebruik van multitenant-opslag. De content van klanten wordt verwerkt door een instantie van Amazon Elastic Compute Cloud (Amazon EC2), en opgeslagen op een combinatie van Amazon S3-buckets (Amazon Simple Storage Services) en via een MongoDB-instantie op een Amazon Elastic Block Store (Amazon EBS). De content zelf wordt opgeslagen in Amazon S3-buckets, en de metadata over de content wordt opgeslagen in Amazon EBS via MongoDB – allemaal beveiligd door IAM-rollen (Identity and Access Management) binnen die AWS-regio (Amazon Web Services).

Metadata en ondersteuningsassets die in Amazon EBS worden opgeslagen, worden versleuteld met 256-bits AES-versleuteling op basis van door FIPS 140-2 (Federal Information Processing Standards) goedgekeurde cryptografische algoritmen die aansluiten op de aanbevelingen van National Institute of Standards and Technology (NIST) 800-57.

Data wordt redundant opgeslagen in meerdere datacentra en op meerdere apparaten in elk datacentrum. Al het netwerkverkeer ondergaat systematische dataverificatie en checksumberekeningen om corruptie te voorkomen en de integriteit te waarborgen. Tot slot wordt opgeslagen content synchroon en automatisch gerepliceerd naar andere datacentrafaciliteiten binnen de regio van de klant, zodat de data-integriteit behouden blijft, zelfs als data op twee verschillende locaties verloren gaat.

Zie voor meer informatie over de onderliggende Amazon-services:

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

Toegewezen versleutelingssleutel

Standaard worden de content en assets die in Amazon S3 zijn opgeslagen, versleuteld met 256-bits symmetrische AES-beveiligingssleutels, die voor iedere klant en het door hem geclaimde domein uniek zijn. Als beheerders een extra controle- en beveiligingslaag willen toevoegen voor bepaalde of alle domeinen in hun organisatie, kunnen ze een toegewezen versleutelingssleutel gebruiken die door de AWS KMS wordt beheerd en automatisch jaarlijks wordt vernieuwd.

Beheerders kunnen deze toegewezen versleutelingssleutel ook via de Admin Console intrekken. Dit maakt alle gegevens die met die sleutel zijn versleuteld, ontoegankelijk voor eindgebruikers en voorkomt dat er content kan worden geüpload of gedownload totdat de versleutelingssleutel weer is geactiveerd.

Opmerking: Hoewel Adobe Document Cloud-bestanden met de toegewezen versleutelingssleutel kunnen worden versleuteld, kan metadata niet met de sleutel worden versleuteld.

Meer informatie over het beheren van versleuteling met een toegewezen sleutel kun je vinden op de Help-pagina's van Adobe:

- Versleuteling beheren
- Toegewezen versleutelingssleutels | Veelgestelde vragen

Amazon Web Services

Zoals eerder aangegeven, worden alle onderdelen van de Adobe Document Cloud-services gehost op AWS, waaronder Amazon EC2 en Amazon S3, in de Verenigde Staten. Amazon EC2 is een webservice die automatisch schaalbare computercapaciteit in de cloud biedt, wat het gebruik van computertoepassingen op webschaal gemakkelijker maakt. Amazon S3 wordt algemeen erkend als een uiterst betrouwbare infrastructuur voor het opslaan en opvragen van elke hoeveelheid data.

Het AWS-platform biedt services conform in de branche gangbare praktijken en wordt regelmatig onderworpen aan in de branche erkende certificeringen en audits. Meer informatie over AWS en de beveiligingsvoorzieningen van Amazon kun je vinden op de website AWS Cloud Security.

Operationele verantwoordelijkheden van AWS en Adobe

AWS bedient, beheert en regelt de verschillende onderdelen, van de hypervisor-virtualisatielaag tot en met de fysieke beveiliging van de faciliteiten waar de Adobe Document Cloud-services worden uitgevoerd. Adobe is op haar beurt verantwoordelijk voor (het beheer van) het gastbesturingssysteem (inclusief updates en beveiligingspatches) en de applicatiesoftware, alsook voor de configuratie van de door AWS beschikbaar gestelde beveiligingsgroepfirewall.

AWS beheert ook de cloudinfrastructuur die door Adobe wordt gebruikt om diverse algemene computerresources te bieden, zoals verwerking en opslag. De AWS-infrastructuur omvat faciliteiten, een netwerk, hardware en de operationele software (zoals hostbesturingssysteem en virtualisatiesoftware) die de terbeschikkingstelling en het gebruik van deze resources ondersteunt. Amazon ontwerpt en beheert AWS overeenkomstig in de branche gangbare praktijken en diverse normen op het gebied van beveiligingsnaleving.

Veilig beheer

Adobe gebruikt Secure Shell (SSH) en Secure Sockets Layer (SSL) voor beheerverbindingen om de AWS-infrastructuur te beheren.

Geografische locatie van klantdata in het AWS-netwerk

Alle gebruikerscontent die naar Document Cloud wordt geüpload, wordt opgeslagen in de regionale datacentra van AWS in het oosten van de VS (Virginia). Ten behoeve van taakverdeling en redundantie wordt binnen elk datacenter en in andere datacentra in de regio een back-up van content gemaakt.

Geografische locatie van identiteitsgegevens in het AWS-netwerk

Identiteitsgegevens worden opgeslagen in multiregionale, voor taakverdeling gebruikte AWS-datacentra die zich in Virginia (VS-Oost), Oregon (VS-West), Ierland (EU-West) en Singapore (AP-Zuidoost) bevinden. Identiteitsgegevens worden in alle datacentra gerepliceerd. Adobe voldoet aan de geldende wetten met betrekking tot grensoverschrijdende dataoverdrachten, zoals wordt toegelicht op https://www.adobe.com/nl/privacy/eudatatransfers.html.

Afscherming van klantdata/scheiding van klanten

AWS maakt gebruik van sterke voorzieningen voor tenant-afscherming en beveiliging. Als gevirtualiseerde multitenant-omgeving implementeert AWS beveiligingsbeheerprocessen en andere beveiligingsvoorzieningen om de AWS-klanten van elkaar af te schermen. Adobe gebruikt de IAM-voorziening van AWS (Identity and Access Management) om de toegang tot computer- en opslaginstanties verder te beperken.

Beveiligde netwerkarchitectuur

AWS maakt gebruik van netwerkapparaten, waaronder firewalls en andere grensapparaten, om de communicatie op de buitengrens van het netwerk en op de belangrijkste interne grenzen binnen het netwerk te bewaken en te regelen. Voor deze grensapparaten worden regelsets, toegangsbeheerlijsten (access control lists, afgekort tot "ACL's") en configuraties gebruikt om de informatiestroom naar specifieke informatiesysteemservices te leiden. Toegangsbeheerlijsten, of beleidsbepalingen voor verkeersstromen, bestaan op elke beheerde interface om de verkeersstroom te beheren en aan te sturen.

Amazon Information Security keurt alle ACL-beleidsbepalingen goed en pusht die automatisch met behulp van de tool AWS ACL-Manage naar elke beheerde interface. Zo wordt ervoor gezorgd dat voor deze beheerde interfaces de meest actuele ACL's worden toegepast.

Netwerkbewaking en -bescherming

AWS gebruikt verschillende geautomatiseerde bewakingssystemen om hoge serviceprestaties en een hoge beschikbaarheidsgraad te waarborgen. Met behulp van bewakingstools worden ongebruikelijke of ongeautoriseerde activiteiten gedetecteerd, en worden bepaalde condities op punten voor inkomende en uitgaande communicatie gesignaleerd. Het AWS-netwerk biedt een goede bescherming tegen de traditionele risico's voor de netwerkbeveiliging:

- DDoS-aanvallen (Distributed denial-of-service)
- MITM-aanvallen (Man-in-the-middle)
- IP-spoofing
- Poortscans
- Packetsniffing door andere tenants

Meer informatie over netwerkbewaking en -bescherming kun je vinden op de website AWS Cloud Security.

Inbreukdetectie

Adobe bewaakt actief de Adobe Document Cloud-services met behulp van in de branche gangbare inbreukdetectiesystemen (IDS) en inbreukpreventiesystemen (IPS).

Logboekregistratie

Aan de serverkant houdt Adobe logboeken bij van de activiteiten van de klanten van de Adobe Document Cloud-services, om onderbrekingen in de service, specifieke problemen van klanten en gemelde bugs te diagnosticeren. In de logboeken worden alleen Adobe-ID's opgenomen om de specifieke problemen van de klant te diagnosticeren; er worden geen combinaties van gebruikersnaam en wachtwoord opgeslagen. Alleen geautoriseerde technische ondersteuningsmedewerkers, de belangrijkste engineers, en bepaalde ontwikkelaars van Adobe hebben toegang tot de logboeken om specifieke kwesties te diagnosticeren.

Servicebewaking

AWS bewaakt de elektrische, mechanische en levensreddende systemen en apparatuur om service-problemen zo snel mogelijk te identificeren. Om de doorlopende werking van de apparatuur te verzekeren, voert AWS voortdurend preventief onderhoud uit.

Dataopslag en -back-up

Adobe slaat alle data van de Adobe Document Cloud-services op in Amazon S3, dat een opslag-infrastructuur met een hoge duurzaamheid biedt. Met het oog op de duurzaamheid worden met de Amazon S3-bewerkingen PUT en COPY synchroon klantdata opgeslagen in verschillende faciliteiten en worden objecten redundant opgeslagen op meerdere apparaten in meerdere faciliteiten in een Amazon S3-regio.

Amazon S3 berekent checksums voor al het netwerkverkeer om corrupte datapakketten te detecteren wanneer data wordt opgeslagen of opgehaald. Datareplicatie voor de dataobjecten van Amazon S3 vindt plaats binnen het regionale cluster waarin de data is opgeslagen en wordt niet gerepliceerd naar datacentrumclusters in andere regio's.

Metadata wordt gerepliceerd door momentopnamen te maken van Amazon EBS-volumes en wordt opgeslagen op een manier die vergelijkbaar is met Amazon S3. Uitgebreide informatie over de beveiliging van AWS kun je vinden op de website AWS Cloud Security.

Wijzigingenbeheer

Terugkerende, nood- en configuratiewijzigingen in de bestaande AWS-infrastructuur worden door AWS geautoriseerd, in een logboek vastgelegd, getest, goedgekeurd en gedocumenteerd conform de branchestandaarden voor vergelijkbare systemen. Amazon plant updates voor AWS om de gevolgen daarvan voor de klant tot een minimum te beperken. AWS informeert klanten via e-mail of via het AWS Service Health Dashboard als updates het gebruik van de services kunnen verstoren. Adobe houdt ook een Adobe System Status voor Adobe Document Cloud bij.

Patch-beheer

AWS blijft verantwoordelijk voor de installatie van patches voor systemen die worden gebruikt voor de aanlevering van AWS-services, zoals de hypervisor- en netwerkservices. Adobe verzorgt de patches voor de gastbesturingssystemen, de software en de applicaties die in AWS worden uitgevoerd. Als er patches nodig zijn, levert Adobe een nieuwe, vooraf geharde instantie van het besturingssysteem en de applicatie aan in plaats van een feitelijke patch.

Fysieke en omgevingsbeveiliging van AWS

De kenmerken van de fysieke en omgevingsbeveiliging van AWS worden specifiek vermeld in de SOC Type 1- en SOC Type 2-rapporten. In het volgende gedeelte worden enkele van de beveiligingsmaatregelen en -mechanismen genoemd die wereldwijd in de datacentra van AWS worden gebruikt. Meer informatie over de beveiliging van AWS kun je vinden op de website AWS Cloud Security.

Fysieke beveiliging van faciliteiten

In de datacentra van AWS worden branchestandaard architectuur- en engineering-benaderingen gehanteerd. De AWS-datacentra bevinden zich in onopvallende faciliteiten, en Amazon regelt de fysieke toegang bij zowel de perimeter als de gebouwingangen met behulp van professioneel beveiligingspersoneel, videobewaking, IDS's en andere elektronische middelen. Geautoriseerd personeel moet zich minimaal twee keer legitimeren met een tweeledige verificatiemethode om toegang tot de datacentrumvloer te krijgen. Alle bezoekers en aannemers moeten zich legitimeren, worden ingeschreven en worden voortdurend vergezeld van geautoriseerd personeel.

AWS verleent alleen datacentratoegang en -informatie aan medewerkers en aannemers die daarvoor een legitieme zakelijke noodzaak hebben. Wanneer een medewerker niet langer een dergelijke zakelijke noodzaak heeft, wordt zijn of haar toegang onmiddellijk ingetrokken, zelfs als hij of zij bij Amazon of AWS in dienst blijft. Alle fysieke toegang tot de datacentra door AWS-medewerkers wordt geregistreerd en regelmatig gecontroleerd.

Brandbestrijding

AWS heeft in alle AWS-datacentra automatische branddetectie- en brandbestrijdingsapparatuur geïnstalleerd. Het branddetectiesysteem maakt gebruik van rookdetectiesensoren in alle datacentrum-omgevingen, ruimten met mechanische en elektrische infrastructuur, koelruimten en ruimten met generatorapparatuur. Deze ruimten worden beveiligd met een natte sprinklerinstallatie, een double-interlock pre-action-installatie of een met blusgas werkende sprinklerinstallatie.

Klimaatregeling

AWS gebruikt een klimaatbeheersingssysteem om een constante bedrijfstemperatuur voor servers en andere hardware aan te houden, zodat oververhitting wordt voorkomen en de kans op service-uitval wordt beperkt. In de datacentra van AWS worden de atmosferische omstandigheden op optimaal niveau gehouden. De medewerkers en systemen van AWS bewaken en regelen zowel de temperatuur als de luchtvochtigheid, zodat die op het juiste niveau blijven.

Noodstroom

De elektriciteitsvoorzieningssystemen in de AWS-datacentra zijn volledig redundant en zonder operationele invloed te onderhouden – 24 uur per dag, zeven dagen per week. UPS-eenheden (Uninterruptible Power Supply) zorgen voor noodstroom in geval van een elektrische storing voor kritieke en essentiële activiteiten in de faciliteit. In de datacentra voorzien generatoren noodstroom voor de hele faciliteit.

Calamiteitenherstel

De datacentra van AWS bieden een hoge beschikbaarheidsgraad en kunnen met minimale operationele impact systeem- of hardwarestoringen aan. Omdat alle datacentra in clusters in verschillende regio's over de hele wereld zijn gebouwd, blijven ze 24x7x365 online om klanten te bedienen. In geval van een storing wordt klantdataverkeer automatisch van het getroffen gebied weggeleid.

Kernapplicaties worden ingezet in een N+1-configuratie, zodat er in geval van een storing in een datacentrum voldoende capaciteit is om het verkeer te verdelen over de overige locaties. Meer informatie over de AWS-protocollen voor calamiteitenherstel kun je vinden op de website AWS Cloud Security.

Risico- en kwetsbaarhedenbeheersing van Adobe

Adobe streeft naar een flexibel en zorgvuldig proces voor risico- en kwetsbaarhedenbeheersing, incidentenrespons, risicobeperking en de implementatie van oplossingen. We houden voortdurend de bedreigingen in de gaten, delen kennis met beveiligingsexperts over de gehele wereld, lossen snel incidenten op, en koppelen deze informatie terug naar onze ontwikkelteams om de hoogst mogelijke beveiliging voor alle Adobe-producten en -services te waarborgen.

Penetratietesten

Door Adobe worden vooraanstaande, externe beveiligingsbedrijven goedgekeurd en ingeschakeld om penetratietesten uit te voeren waarmee potentiële beveiligingsproblemen aan het licht kunnen worden gebracht en de algehele beveiliging van Adobe-producten en -services kan worden verbeterd. Na ontvangst van het rapport van deze externe partij documenteert Adobe de kwetsbaarheden, beoordeelt zij de ernst en prioriteit ervan, en stelt zij vervolgens een beperkingsstrategie of herstelplan op. Adobe voert elk jaar een volledige penetratietest uit en voert maandelijks kwetsbaarhedenscans uit.

Intern voert het Adobe Document Cloud-beveiligingsteam elk kwartaal en vóór elke release een risicobeoordeling uit met betrekking tot alle Document Cloud-onderdelen en -services. Het Document Cloud-beveiligingsteam werkt samen met de leiders van de technische en ontwikkelteams om ervoor te zorgen dat alle risicovolle kwetsbaarheden vóór elke release worden beperkt. Meer informatie over de Adobe-procedures voor penetratietesten kun je vinden in het overzicht van veilige engineering bij Adobe.

Incidentenrespons en -melding

Elke dag komen er nieuwe kwetsbaarheden en dreigingen bij. Adobe streeft ernaar om actie te ondernemen op nieuw ontdekte dreigingen en om die te beperken. Adobe heeft zich niet alleen aangemeld voor sectorbrede informatielijsten voor kwetsbaarheden, zoals het United States Computer Emergency Readiness Team (US-CERT), Bugtraq en SANS, maar ook voor de nieuwste lijsten met beveiligingswaarschuwingen die door belangrijke beveiligingsaanbieders worden uitgegeven.

Meer informatie over Adobe's processen voor incidentenrespons en -meldingen kun je vinden in het overzicht van de incidentenrespons van Adobe.

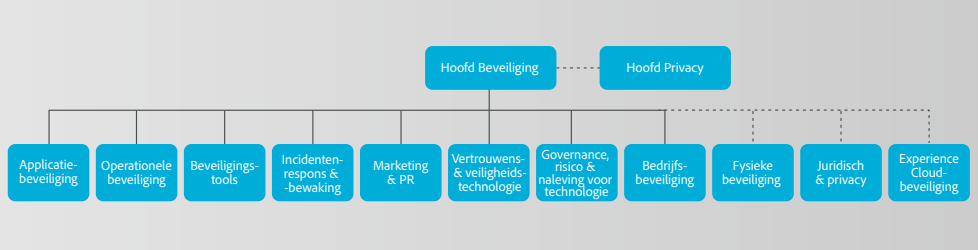
Forensische analyse

Voor incidentenonderzoeken volgt het Document Cloud-team het Adobe-proces voor forensische analyses. Hierbij gaat het onder andere om vastlegging van de volledige dataopslag of geheugendump van de getroffen computers, bewaring van bewijs, en registraties ten behoeve van de bewijsvoeringsketen.

De beveiligingsorganisatie van Adobe

In het kader van Adobe's inzet voor de beveiliging van haar producten en services zijn alle beveiligingsactiviteiten ondergebracht bij de Chief Security Officer (CSO). Het kantoor van de CSO coördineert alle initiatieven op het gebied van product- en servicebeveiliging, alsook de implementatie van de Adobe Secure Product Lifecycle (SPLC).

De CSO geeft bovendien leiding aan het Adobe Secure Software Engineering Team (ASSET). Dit speciaal opgezette, centrale team bestaat uit beveiligingsdeskundigen die als consultants fungeren voor de belangrijkste product- en operationele teams van Adobe, waaronder het Adobe Document Cloud-team. De ASSET-onderzoekers werken samen met de afzonderlijke product- en operationele teams van Adobe om ervoor te zorgen dat producten en services de juiste beveiliging bieden. Daarnaast adviseren zij deze teams over beveiligingspraktijken voor duidelijke en herhaalbare processen voor ontwikkelings-, implementatie- en operationele taken en incidentrespons.



Beveiligingsorganisatie van Adobe

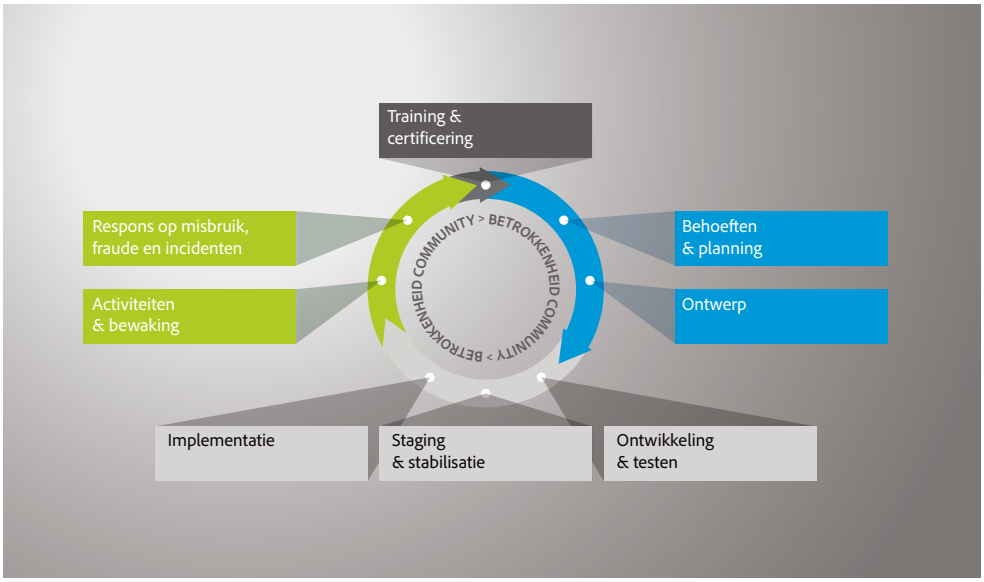
Adobe Secure Product Development

Net als bij de andere belangrijke product- en serviceorganisaties van Adobe maakt de Adobe Document Cloud-organisatie gebruik van het Adobe SPLC-proces. De Adobe SPLC omvat honderden specifieke beveiligingsactiviteiten voor softwareontwikkeling, processen en tools en is geïntegreerd in meerdere fasen van de productlevenscyclus, van ontwerp en ontwikkeling tot en met kwaliteitsborging, test-werkzaamheden en implementatie. ASSET-beveiligingsonderzoekers bieden specifiek SPLC-advies voor alle kernproducten en -services op basis van een beoordeling van de potentiële beveiligingsproblemen. Dankzij de doorlopende bijdragen vanuit de community blijft de Adobe SPLC actueel terwijl de technologie, de beveiligingspraktijken en de bedreigingen veranderen.

Adobe Secure Product Lifecycle

De activiteiten van de Adobe SPLC omvatten (afhankelijk van het specifieke Adobe Document Cloud-onderdeel) enkele of alle van de volgende aanbevolen best practices, processen en tools:

- Beveiligingstraining en -certificering voor productteams
- Analyse van productstatus, risico's en bedreigingen
- Richtlijnen, regels en analyses voor veilig programmeren
- Serviceschema's, beveiligingstools en testmethoden die het Adobe Document Cloud-beveiligingsteam helpen om het hoofd te bieden aan de Top 10 van de meest kritieke beveiligingsrisico's voor webapplicaties van het Open Web Application Security Project (OWASP) en de Top 25 van de gevaarlijkste softwarefouten van CWE/SANS
- Controle van beveiligingsarchitectuur en penetratietesten
- Controles van broncode om bekende fouten weg te nemen die tot beveiligingsproblemen zouden kunnen leiden
- Validatie van gebruikerscontent
- Applicatie- en netwerkscans
- Volledige gereedheidsbeoordeling, responsplannen en vrijgave van educatief materiaal voor ontwikkelaars



Adobe Secure Product Lifecycle

Adobe Software Security Certification Program

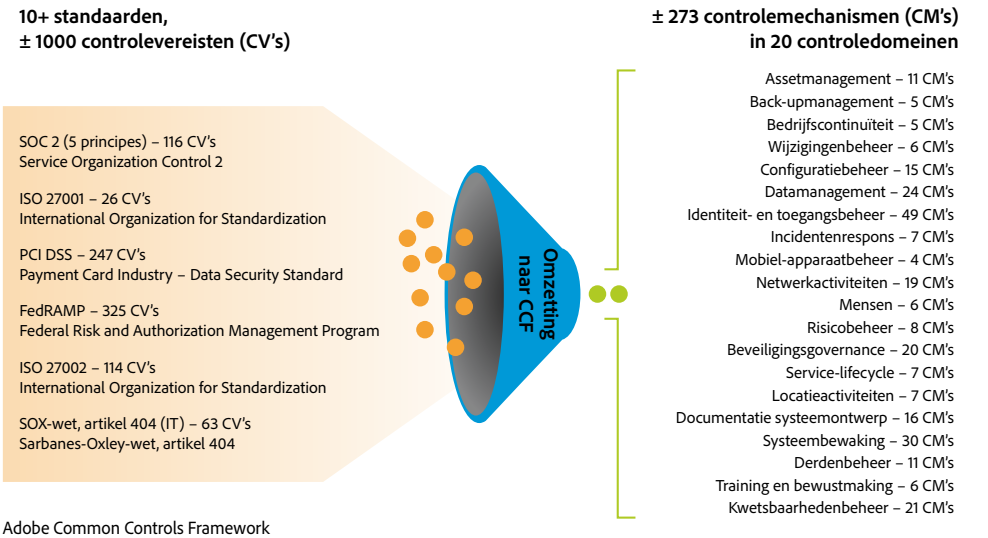
In het kader van de Adobe SPLC verzorgt Adobe doorlopend beveiligingstraining binnen de ontwikkelteams om de beveiligingskennis in het hele bedrijf te vergroten en de algehele beveiliging van onze producten en services te verbeteren. Werknemers die aan het Adobe Software Security Certification Program deelnemen, kunnen verschillende certificeringsniveaus behalen door beveiligingsprojecten af te ronden. Meer informatie over onze productbeveiligingspraktijken kun je vinden in het overzicht van veilige engineering bij Adobe.

Meer informatie over het Adobe Software Security Certification Program kun je vinden in het artikel over de beveiligingscultuur bij Adobe.

Naleving van voorschriften en standaarden door Document Cloud-services

Het Adobe Common Controls Framework (CCF) is een pakket beveiligingsactiviteiten en nalevingscontroles die worden geïmplementeerd binnen onze productactiviteitteams, alsook in diverse onderdelen van onze infrastructuur- en applicatieteams.

Bij de opzet van het CCF heeft Adobe de criteria voor de meest gangbare beveiligingscertificeringen voor cloudbedrijven geanalyseerd en de ruim 1000 vereisten teruggebracht tot Adobe-specifieke controlemechanismen die aansluiten bij zo'n tiental branchestandaarden.



Adobe Common Controls Framework

Huidige voorschriften en naleving voor Adobe Document Cloud-services

SOC 2 omvat een reeks beveiligingsprincipes met algemeen aanvaarde controlemechanismen voor beveiliging, vertrouwelijkheid en privacy. Adobe Document Cloud-services voldoen aan de vereisten van SOC 2 Type 2 (beveiliging en beschikbaarheid).

ISO 27001 is een reeks wereldwijd geaccepteerde standaarden die strenge beveiligingseisen aangeven en een systematische aanpak bieden om de vertrouwelijkheid, integriteit en beschikbaarheid van klantgegevens te waarborgen. Adobe Document Cloud-services voldoen aan de vereisten van ISO 27001:2013.

De Payment Card Industry Data Security Standard (PCI DSS) is een beveiligingsstandaard voor organisaties die betaalkaartgegevens, zoals creditcardnummers, verwerken. Omdat Adobe een PCI DSS-conforme serviceprovider is, kan Adobe klanten helpen om aan de PCI-vereisten voor de veilige verwerking van persoonsgegevens van kaarthouders te voldoen.

De Amerikaanse Gramm-Leach-Bliley Act (GLBA) schrijft voor dat financiële instellingen de persoonlijke gegevens van hun klanten moeten beschermen. Adobe Document Cloud-services zijn klaar voor de GLBA, wat inhoudt dat onze financiële klanten aan de GLBA-vereisten voor het gebruik van dienstverleners kunnen voldoen.

Het Amerikaanse Federal Risk and Authorization Management Program (FedRAMP) is een overheidsbreed programma dat een gestandaardiseerde aanpak biedt voor de inventarisatie, autorisatie en doorlopende controle van de beveiliging van cloudproducten en -services. Adobe Document Cloud-services voldoen aan de vereisten van het FedRAMP, wat inhoudt dat onze klanten aan de FedRAMP-vereisten kunnen voldoen.

De Amerikaanse Family Educational Rights and Privacy Act (FERPA) is bedoeld om de vertrouwelijkheid van de opleidingsdocumenten en adreslijstgegevens van Amerikaanse scholieren te beschermen. Op grond van de FERPA-richtlijnen kan Adobe er contractueel mee instemmen om als "schoolbestuurder" op te treden wat betreft de verwerking van leerlinggegevens, waardoor onze klanten in het onderwijs aan de FERPA-vereisten kunnen voldoen.

In de SAFE-BioPharma-standaard zijn de vereisten opgenomen voor gestandaardiseerd identiteits-vertrouwen voor identiteitauthenticatie of digitale ondertekening. Adobe Document Cloud is gecertificeerd volgens de SAFE-BioPharma-standaard voor digitale identificatie. Adobe Acrobat DC is veilig te gebruiken in, en is compatibel met, SAFE-BioPharma-workflows. Bovendien voldoen Adobe Document Cloud-services en Adobe Sign aan de vereisten van SOC 2 Type 2.

Informatie over de huidige nalevingspositie voor Adobe Sign kun je vinden in het technische overzicht van Adobe Sign.

Uiteindelijk zijn het de klanten die verantwoordelijk zijn voor de inachtneming van hun wettelijke verplichtingen en die ervoor moeten zorgen dat onze oplossingen aan hun nalevingsbehoeften voldoen en op passende wijze zijn beveiligd.

Adobe-medewerkers

Adobe heeft medewerkers en vestigingen over de gehele wereld, en hanteert de volgende bedrijfsbrede processen en procedures om het bedrijf te beschermen tegen beveiligingsrisico's.

Toegang van medewerkers tot klantgegevens

Adobe hanteert gescheiden ontwikkel- en productieomgevingen voor Adobe Document Cloud, waarbij technische controlemechanismen worden gebruikt om de toegang op netwerk- en applicatieniveau tot live productiesystemen te beperken. Medewerkers krijgen specifieke toegangsautorisatie voor ontwikkel- en productiesystemen; medewerkers die geen legitieme zakelijke reden hebben om toegang tot deze systemen te hebben, hebben geen toegang tot deze systemen.

Achtergrondonderzoeken

Bij indienstneming van nieuwe werknemers maakt Adobe gebruik van achtergrondonderzoeken. Het rapport dat Adobe doorgaans opvraagt, omvat informatie over de opleiding, het arbeidsverleden en gerechtelijke stukken, waaronder strafrechtelijke veroordelingen en referenties van bedrijven en personen, voor zover het toepasselijke recht dit toestaat. Dit achtergrondonderzoek is verplicht voor nieuwe vaste Amerikaanse medewerkers, waaronder voor degenen die systemen zullen beheren of toegang tot klantgegevens zullen hebben. Voor nieuwe uitzendmedewerkers in de Verenigde Staten wordt via het desbetreffende uitzendbureau een achtergrondonderzoek uitgevoerd overeenkomstig de richtlijnen die Adobe daarvoor hanteert. Buiten de Verenigde Staten verricht Adobe achtergrondonderzoeken naar bepaalde nieuwe werknemers overeenkomstig het Adobe-beleid inzake achtergrondonderzoeken en de geldende lokale wetgeving.

Uit dienst tredende medewerkers

Wanneer een werknemer vertrekt bij Adobe, dient zijn of haar manager een vertrekformulier voor de werknemer in. Nadat dat formulier is goedgekeurd, zet de afdeling Personeelszaken van Adobe een e-mailworkflow in gang om de betrokkenen te vragen om tot en met de laatste werkdag van de werknemer specifieke maatregelen te treffen. Als Adobe een werknemer ontslaat, stuurt de afdeling Personeelszaken van Adobe een vergelijkbaar e-mailbericht naar de betrokkenen, met vermelding van de datum en tijd waarop het dienstverband eindigt.

De afdeling Concernbeveiliging van Adobe plant vervolgens de volgende maatregelen in om ervoor te zorgen dat de werknemer na afloop van zijn of haar laatste werkdag geen toegang meer heeft tot de vertrouwelijke bestanden of de vestigingen van Adobe:

- Het intrekken van e-mailtoegang
- Het intrekken van externe VPN-toegang
- Het ongeldig maken van kantoor- en datacentrumbadges
- Het beëindigen van de netwerktoegang

Op verzoek kunnen managers de gebouwbeveiliging vragen om de ontslagen werknemer naar buiten te begeleiden.

Beveiliging van faciliteiten

Op elke concernvestiging van Adobe zijn bewakers aanwezig om het gebouw en het terrein 24 uur per dag, 7 dagen per week te beveiligen. Adobe-medewerkers dragen een keycard-ID-badge die hun toegang tot het gebouw geeft. Bezoekers komen via de vooringang binnen, schrijven zich in en uit bij de receptiemedewerker, dragen een tijdelijke bezoekers-ID-badge en worden altijd vergezeld van een medewerker. Adobe houdt alle serverapparatuur, ontwikkelcomputers, telefoonsystemen, bestands- en e-mailservers en andere gevoelige systemen te allen tijde achter slot en grendel in klimaatgeregelde serverruimten die alleen toegankelijk zijn voor geautoriseerde medewerkers.

Virusbescherming

Adobe scant alle inkomende en uitgaande zakelijke e-mail op bekende malwarerisico's.

Geheimhouding van klantgegevens

Adobe gaat altijd vertrouwelijk om met alle klantgegevens. De gegevens die namens een klant worden verzameld, worden niet door Adobe gebruikt en gedeeld, behalve voor zover dat wordt toegestaan op grond van een overeenkomst die met die klant is aangegaan en zoals in de gebruiksvoorwaarden van Adobe en het privacybeleid van Adobe wordt aangegeven.

Conclusie

Adobe's proactieve beveiligingsaanpak en strenge procedures die in dit artikel worden beschreven, houden niet alleen Adobe Acrobat DC, Acrobat Reader DC en Document Cloud-services, maar ook uw vertrouwelijke gegevens veilig. Adobe neemt de beveiliging van je digitale ervaring heel serieus. We houden doorlopend nieuwe bedreigingen in het oog om schadelijke activiteiten voor te blijven en de gegevens van onze klanten veilig te houden.

Ga voor meer informatie naar het Adobe Trust Center.

Adobe Inc.
345 Park Avenue
San Jose, CA 95110-2704 USA
www.adobe.com
www.adobe.com/nl
www.adobe.com/be

5/19