INNEO®
That's IT.

Wie sicher sind Ihre CAD Daten?

Warum Onshape Ihr geistiges Eigentum besser vor Hackern und Datenlecks schützt

Deutschland
Rindelbacher Straße 42
73479 Ellwangen

Tel. +49 (0) 7961 890-0
inneo@inneo.de
www.inneo.de

Schweiz
Ruchstuckstrasse 21
8306 Brüttisellen

Tel. +41 (0) 44 805 1010
inneo@inneo.ch
www.inneo.ch

Inhalt

1. Warum Ihnen die Sicherheit Ihrer Daten am Herzen liegen sollte

Betrachtet man persönliche Daten wie Sozialversicherungsnummern und Kreditkartendetails, so ist offenkundig, dass diese Daten schützenswert sind. Mit einem Zugang zu solch privaten Daten ist es einfach, Betrugshandlungen zu begehen, doch leider gehört dies heute dennoch zum Alltag: Ein Computersystem existiert, um gehackt zu werden. Ob die Täter dies aus Spaß oder zum finanziellen Gewinn tun, spielt keine Rolle. Wer über genügend technisches Know-how und Hartnäckigkeit verfügt, kann potenziell jedes System knacken. Kein Unternehmen ist davor geschützt.

Im Gegensatz zu den Datenschutzverletzungen die man in den Nachrichten verfolgen kann, befasst sich dieses eBook mit der Sicherheit von Geschäftsdaten – insbesondere dem Diebstahl oder Verlust von Konstruktions- und CAD-Daten. Wenn dieses geistige Eigentum (IP) in die falschen Hände gerät, können Ideen kopiert oder Patente für ungültig erklärt werden, bevor sie eingereicht wurden, oder schlimmstenfalls kann die Konkurrenz auf Grundlage Ihrer Arbeit und Innovation zuerst auf den Markt kommen.

Der Großteil der Wirtschaftsspionage beinhaltet nicht das Hollywood-Drama von Spionen und Geheimagenten. Geschäftsgeheimnisse werden ständig preisgegeben, manchmal absichtlich und manchmal aus Versehen oder aufgrund von Fahrlässigkeit.

Wie kann es zu diesen Datenlecks kommen und mit welchen Schritten können sie vermieden werden? Im Grunde gilt, dass alle Daten, die Ihren Computer verlassen, gefährdet sind. Die sichere Umgebung des Computers verlassen Daten entweder auf physischem Weg (durch Kopieren auf ein externes Medium wie einen USB-Stick) oder durch eine Verbindung mit einem anderen Computersystem (über einen Server oder das Internet). Letzteres lässt den Ansatz der Cloud keinesfalls Sicher erscheinen, da hierbei ebenfalls Daten in ein anderes System verschickt werden. Zusätzlich hat Microsoft enthüllt, dass seine Cloud-Systeme täglich von 1,5 Millionen Hackerangriffen heimgesucht werden.

Wie soll ausgerechnet in einem System wie Onshape, das die Daten ausschließlich in der Cloud speichert, eine höhere Sicherheit erreicht werden, als in On-Premise Lösungen?

Bevor wir uns dieser Frage widmen, ist es notwendig zu beleuchten, was die Cloud überhaupt ist.

2. Kurzüberblick Cloud

Die „Cloud“ ist ein Begriff aus der Informatik, der schon seit vielen Jahren bekannt ist. Grundsätzlich handelt es sich bei der Cloud um ein Netzwerk von Servern, die über den gesamten Erdball verteilt sind. Für diejenigen, die mit dem Begriff vertraut sind, ist er ein Synonym für Datei- und Foto-Sharing-Dienste wie Dropbox, OneDrive und Google Drive. Nutzt man einen dieser Cloud-Storage-Dienste weiß man nie, wohin genau die eigenen Dateien gehen oder wo sie gespeichert werden. Aber das ist ein Vorteil der Cloud; es ist nicht notwendig zu wissen, wo die Daten liegen, da im Gegenzug ermöglicht wird, trotz minimalem Einrichtungsaufwand und ohne IT-Kenntnisse auf „unendliche“ Ressourcen in Bezug auf Rechenleistung und Speicherplatz zugreifen zu können. Der Zugriff auf die Cloud ist jederzeit möglich, wenn ein Webbrowser oder ein Smartphone verfügbar ist.

Natürlich ist die Cloud nicht nur eine Sache oder Einheit, auf die alle gleichzeitig zugreifen. Sie ist ein Oberbegriff für Computer-dienste und -speicher, die von einem Drittanbieter über das Internet gehostet und kontrolliert werden. Jeder Dienst, auf den Sie über einen Webbrowser zugreifen, kann als „Cloud“ bezeichnet werden. Er muss nicht von einem multinationalen Unternehmen stammen, dessen Daten über mehrere Rechenzentren in mehreren Zeitzonen verbreitet sind (z.B. Server die auf Amazon Web Services, Microsoft Azure oder Google Cloud gehostet werden). Es könnte sich auch um ein kleines Unternehmen handeln, das einen Dienst anbietet, der von dem Computer in seinem Serverraum aus gehostet wird.

Jeder nutzt die Cloud, ob er sich dessen bewusst ist oder nicht. Wenn Sie schon einmal Online-Banking oder einen webbasierten E-Mail-Dienst, Facebook oder Instagram genutzt haben, dann haben Sie die Cloud benutzt.

Wie sicher sind diese Dienste also und kann man dem Prinzip der Cloud vertrauen?

3. Sicherheit in der Cloud vs. On-Premise

Wenn alle Ihre Daten auf Ihrem eigenen persönlichen Computer/Laptop oder auf dem Server Ihres Unternehmens im feuerfesten Serverraum gespeichert sind, wie kann dann das Senden von Daten über das Internet sicherer sein?

In der Vergangenheit haben sich streng geheime Regierungsbehörden auf diese Methode verlassen, um ihre Verteidigungslinie zu ziehen. In der Realität wurde die Datensicherheit hergestellt, indem externe Netzwerkverbindungen, USB-Anschlüsse oder andere beschreibbare Medien an den Computern entfernt wurden. Zusätzlich waren keine Kameras oder Mobiltelefone vor Ort erlaubt und ohne strenge Durchsuchungen durch das Pförtnerpersonal war der Zutritt von vornherein untersagt.

Aber in Wirklichkeit garantierten selbst diese aufwändigen Schutzmaßnahmen keine Sicherheit. Ein Beispiel hierfür sind die Affären rund um die WikiLeaks Plattform. Zwar stellt der Diebstahl immer ein Negativbeispiel dar, doch auch im Guten müssen Sie letzten Endes Ihre Daten aus dem sicheren Hafen entlassen, um mit Ihren Kunden und Lieferanten kommunizieren zu können. Während Regierungsbehörden immer noch diese strengen Sicherheitsmaßnahmen anwenden, wird die Datenkommunikation zwischen Behörden und zugelassenen Lieferanten jetzt in der Cloud verwaltet.

Täglich wird von böswilligen Hackerangriffen berichtet, um Daten zu stehlen und bösartige Computerviren einzuschleusen. Obwohl die Hacker mit diesen Angriffen einen Großteil der Ängste und Aufmerksamkeit im Zusammenhang mit Sicherheitsverletzungen erzeugen, sind sie nicht die einzigen Schuldigen. Unbeabsichtigte oder unvorsichtige Mitarbeiteraustritte können ebenfalls großen Schaden anrichten. Mitarbeiter nehmen Laptops mit nach Hause, speichern Daten auf austauschbaren USB-Laufwerken oder senden unverschlüsselte vertrauliche Informationen per E-Mail. Mit diesem Verhalten werden weitere Sicherheitslücken geöffnet. Es passiert zu leicht, dass Computer mit Viren infiziert werden, dass Laptops und USB-Sticks verloren gehen oder gestohlen werden und dass E-Mails abgefangen oder sogar an den falschen Empfänger gesendet werden. Selbst alltägliche Aktivitäten, die für den Betrieb Ihres Unternehmens notwendig sind, machen Sie für viele potenzielle Sicherheitsbedrohungen anfällig.

Für eine gute Sicherheitspolitik im Unternehmen ist es wichtig sich auf die zentrale Botschaft zu besinnen: das wertvollste Kapital eines Unternehmens ist sein geistiges Eigentum. Demzufolge ist die Durchsetzung strenger Datenverwendungs- und Sicherheitsrichtlinien innerhalb traditioneller Computerausstattung von entscheidender Bedeutung. Doch so lange auf der Hardware allgemein erhältliche Software installiert ist, sind die Daten immer gefährdet – egal welche Richtlinie aufgestellt wird.

Dateien können leicht gelesen und Daten leicht extrahiert werden. Die Nutzung der Cloud stellt einen Weg aus dieser Unsicherheit dar.

4. Cloud-Software in Unternehmen

Viele Unternehmen sind der Ansicht, dass sie keine Cloud-Software in ihrem Unternehmen nutzen. Doch häufig sind bereits solche Tools im Einsatz. Stellen Sie sich einmal die Frage: Welche unserer Geschäftsanwendungen lassen sich mit dem Webbrowser oder dem Smartphone bedienen?“

Es ist sehr wahrscheinlich, dass die Vertriebsabteilung einen Service wie Salesforce nutzt, um jederzeit und von jedem Ort aus auf die Informationen über Kunden oder Interessenten zugreifen zu können. Die Marketingabteilung kann eine Plattform wie HubSpot für webbasierte Kampagnen und die Überwachung des Website-Traffics nutzen, während die Personalabteilung wahrscheinlich auch die Gehaltsabrechnung und die Leistungen online verwaltet. Warum? Weil die Einrichtung, Verwaltung und Bereitstellung einer Cloud-basierten Lösung so viel einfacher ist als alle bisherigen Tools – und nebenbei ist sie auch viel billiger.

Schauen wir uns zum Beispiel die Personalabteilung an. Jahrelang war HR-Software nur für Unternehmen mit großen Budgets rentabel. Die Produkte waren zwar datenbankgesteuert, aber es handelte sich um On-Premise-Lösungen (d.h. auf Ihren eigenen internen Servern gehostet). Diese Art von Lösungen sind in der Regel nicht sofort einsatzbereit, sondern erfordern aufwändiges Customizing in dem Datenbankprogrammierer den Code an Ihr Unternehmen anpassen, bevor das System eingeführt wird. Die meisten Unternehmen können sich dies heutzutage nicht leisten, vor allem dann nicht, wenn praktikable Systeme online verfügbar sind, die zudem flexible Bezahlmodelle bereithalten.

Demgegenüber ist die Cloud eine Win-Win-Situation sowohl für Kunden als auch für Anbieter. Der Kunde profitiert von der Einfachheit und den Einsparungen, die die Nutzung einer Cloud-Lösung mit sich bringt, während der Anbieter seine Logistikkosten für Softwarelieferung, -verfolgung, -debugging und -upgrades stark reduziert. Immer mehr Unternehmen verlagern nun alle ihre Geschäftssysteme in die Cloud. Laut Forrester Research wird der Cloud-Computing-Markt bis 2020 auf 236 Milliarden Dollar anwachsen, bis 2022 sogar auf bis zu 411 Milliarden. Die Analysten führen das Wachstum auf eine schnell wachsende Nachfrage nach Software-as-a-Service (SaaS)-Anwendungen zurück.

Wenn nun bereits mehrere Abteilungen in Firmen von der Cloud profitieren, warum sollte die Entwicklungsabteilung hinten anstehen?!

5. Der Verlust von Konstruktionsdaten auf vier Wegen

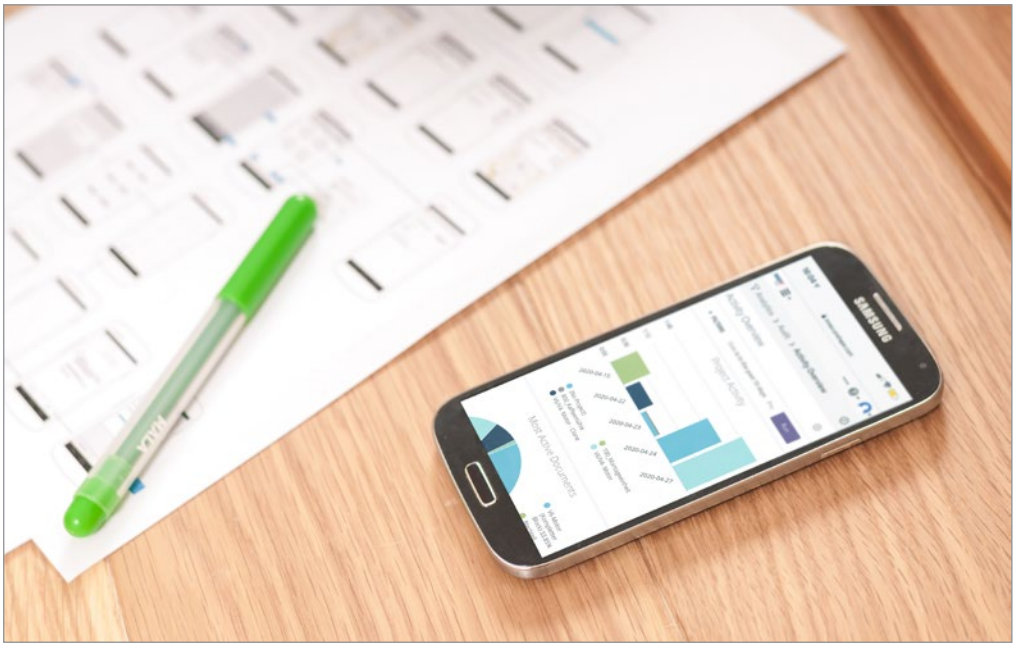
Konstruktionsdaten werden seit den Anfängen von Computern und CAD in unverschlüsselten Dateien auf Festplatten von Desktopcomputern gespeichert. Alternativ befinden sie sich auf Servern, innerhalb der Mauern des Gebäudes, in dem die Konstrukteure arbeiten. Diese Designdateien sind Ihr geistiges Eigentum und das Herz Ihres Unternehmens. Aus diesem Grund gibt es einen Widerstand der technischen Abteilungen, gegen die Speicherung von Daten außerhalb der Firmen-Firewall.

Diese Bedenken sind verständlich, wenn man die ständigen Nachrichtenmeldungen über Hacking betrachtet. Gegenstand der Berichterstattung ist zwar hauptsächlich der Diebstahl persönlicher Verbraucherdaten, doch nur weil die Allgemeinheit durch den Verlust von Konstruktionsdaten wenig betroffen ist. Dennoch gehen bei weniger bekannten Unternehmen täglich Millionen von Daten verloren oder werden gestohlen. Dies spielt sich teilweise direkt vor den Augen der Akteure ab, ohne dass die es bemerken würden. Leider ist auch Ihr Unternehmen davor nicht gefeit.

Arbeitscomputer werden heutzutage nicht nur für CAD verwendet, sondern auch zum Lesen von E-Mails und zum Surfen im Internet. Die Designer von heute teilen sich beliebig viele, unkontrollierte Kopien von CAD-Daten mit anderen Konstrukteuren, Herstellern und Zulieferern. Die Workstations werden teils von mehreren Mitarbeitern genutzt. Wo auch immer wir hingehen, Laptops reisen mit uns und verbinden sich häufig mit unsicheren Netzwerken.

Dies sind alles Wege für Viren, Netzwerkangriffe, Datenverlust und den Diebstahl von IP. Während Hacker, die in ein Online-System einbrechen, Spuren hinterlassen, haben gestohlene Daten keine Möglichkeit sich bemerkbar zu machen. Bei Online Angriffen ist es viel einfacher, einen Angriff zu entdecken und Schritte zu unternehmen, um eine Wiederholung zu verhindern. Dateien verfügen jedoch nicht über einen solchen Schutz oder eine solche Verfolgung – sie verschwinden einfach.

Hier sind 4 Wege, wie dies passieren kann.



5.1. Versenden von Daten an Zulieferer oder Kunden

Jedes Mal, wenn Sie eine Datei per E-Mail oder FTP an einen Kunden oder Lieferanten versenden, erzeugen Sie Kopien. Dies trifft sogar beim Versenden über einen sicheren Dateiaustauschdienst wie Dropbox (der während der Übertragung und Speicherung sicher ist) auf. Damit sind Sie nicht alleine, denn de facto alle Unternehmen wählen E-Mails als bevorzugte Kommunikationsmethode.

E-Mail-Anhänge sind jedoch wahrscheinlich die unsichersten aller Dateiverteilungsmethoden. Sobald Sie eine Datei zur Herstellung an Ihren Lieferanten schicken, besitzen Sie keine Kontrolle über die weitere Verteilung und Vervielfältigung der Kopien. Meist entsteht eine Unmenge an Kopien:

Ihre Nachricht landet im Posteingang der Empfänger (**Kopie 1**). Ab diesem Zeitpunkt haben Sie keine Garantie, dass ihre Sicherheitsprotokolle mit deren Sicherheitsprotokolle übereinstimmen. Eventuell verwenden die Empfänger keine Firewalls oder gar Passwortschutz für ihre Computer, so dass Sie keine Ahnung haben, wie einfach es für jemanden wäre, sich in das System zu hacken und auf die E-Mails zuzugreifen. Um den Anhang zu öffnen, laden die Empfänger ihn auf ihren lokalen Computer herunter (**Kopie 2**). Möglicherweise müssen sie ihn an einen Kollegen weiterleiten (**Kopie 3**) oder in der Produktion auf die Datei zugreifen (**Kopie 4**). Wenn ein Empfänger am Wochenende daran arbeiten möchte, kopiert er die Datei auf einen USB-Stick (**Kopie 5**) und dann auf seinen persönlichen Computer zu Hause (**Kopie 6**). Kopien von Kopien von Kopien von Kopien. Selbst wenn Sie FTP oder Dropbox verwenden, wird Ihr Lieferant das oben beschriebene Verfahren befolgen, so dass es dort keine zusätzlichen Vorteile gibt.

Erscheinen Kopien vielleicht auf den ersten Blick harmlos, so stellen sie ein eklatantes Sicherheitsrisiko dar. Einerseits erhöht die im Umlauf befindliche Anzahl an Dateien die Wahrscheinlichkeit, dass Daten verloren gehen oder abgefangen werden. Andererseits verbleibt eine Kopie fast nie an dem gleichen Ort, wie ihr Original. Die kopierte Datei wird an einen neuen Ort gebracht, der anderen Sicherheitsrisiken ausgesetzt ist. Beispielsweise greift der Virenschutz des Unternehmens noch auf der Workstation des Mitarbeiters, jedoch ist der Privatrechner lediglich mit kostenloser Virenabwehr ausgestattet. Besonders wenn Daten an Dritte weitergegeben werden, hat die IT-Abteilung keine Chance mehr, die Datei in irgendeiner Weise zu schützen.

Neben diesen Bedenken werden die lästigen Größenbeschränkungen für E-Mail-Anhänge und die Sorge, ob Ihr Lieferant die neueste Kopie der Datei für die Herstellung Ihres Teils verwendet, eher nebensächlich. Beunruhigender ist mehr die Frage, wohin all diese Kopien gehen (könnten). Sie könnten versehentlich an die anderen Kunden Ihres Lieferanten weitergeleitet werden, von denen einer sogar Ihr Konkurrent sein könnte!

5.2. Daten mithilfe von externen Transportmedien übermitteln

Wenn USB-Sticks, externe Festplatten oder Laptops verwendet werden, um Daten an verschiedene Computersysteme zu übertragen, ist das genauso unsicher wie E-Mails zu versenden. Jegliche Hardware, die zum Transport von Daten nach außerhalb des Unternehmens verwendet wird, stellt ein großes Risiko dar. Die Transportmedien können versehentlich an einem öffentlichen Ort vergessen und zurückgelassen, leicht aus Ihrem Auto oder Hotelzimmer gestohlen, oder auf verschiedene Weise zerstört werden.

Des Weiteren gilt hier die gleiche Kopie-Problematik, wie sie bei der Verwendung von E-Mail, FTP oder Dropbox auftritt. Selbst beim Versuch dies zu beheben (z.B. durch die Verwendung von VPN, um sich per Fernzugriff auf Ihren Server einzuloggen), müssen trotzdem Dateien lokal auf Ihren Laptop heruntergeladen werden.

Ohne, dass Sie dies beabsichtigen, werden Sie mehrere unkontrollierte Kopien derselben Datei generieren – alle anfällig für Diebstahl oder Verlust. Darüber hinaus kann es vorkommen, dass Sie ohne strenge Versionskontrolle an einem veralteten Design arbeiten.

5.3. Verlust durch verärgerte Mitarbeiter

Unvorsichtiges menschliches Verhalten stellt eines der größten Risiken gegen Cyberattacken dar. Da gelegentlich Vorgesetzte und Mitarbeiter nicht im Guten auseinander gehen, bergen verärgerte oder ehemalige Mitarbeiter eines der größten Risiken für die Datensicherheit von Unternehmen. Die physische und softwareseitige Absicherung der Daten ist nur effektiv, wenn sie auf der menschlichen Seite mit durchdachten Prozessen unterstützt werden. Diese sind besonders wichtig, wenn Mitarbeiter das Unternehmen verlassen.

Tatsächlich hat eine Umfrage der Ostermann Research ergeben, dass 69% der Mitarbeiter einen privaten Account von file-sharing Diensten wie Dropbox verwenden, um unternehmenskritische Daten zu speichern. Weiterhin fand die Umfrage heraus, dass 89% der Mitarbeiter Login Informationen für mindestens ein Unternehmenssystem aufbewahren, selbst nachdem sie das Unternehmen verlassen hatten. Dies schließt den privaten Dropbox Ordner nicht mit ein. Am erschreckendsten ist, dass 6% der Befragten, angaben, die zurückbehaltenen Daten mit ihrem neuen Arbeitgeber geteilt haben.

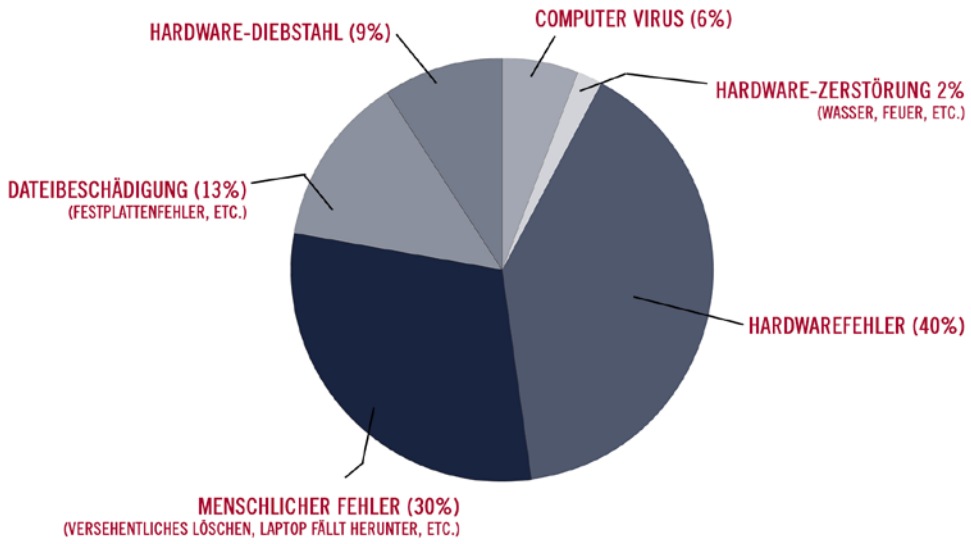
Abgesehen von diesen Risiken gibt es stets die Möglichkeit, dass Mitarbeiter die kurz vor dem Unternehmensaustritt stehen, Daten von Servern löschen – ein Vorfall der möglicherweise nicht direkt auffällt und nicht nachverfolgt werden kann.

5.4. Hardwareausfall und menschliches Versagen

Datenverlust muss nicht immer mit böswilliger Absicht geschehen. Es gibt Probleme, die in der Natur von Dateibasierten Systemen liegen, beispielsweise beschädigte oder gelöschte Daten. Diese können tausende Euro Schaden in Form von vergeudeter Zeit und verpasstem Umsatz anrichten. Die Gründe hierfür sind vielfältig, meistens jedoch zufällig und kaum zu verhindern.

Schätzungsweise 30% aller Daten von traditionellen CAD Systemen werden entweder beschädigt oder gehen im Laufe der Zeit verloren. Eine Lösung stellen die PDM Systeme der Softwarehersteller dar, jedoch sind die Kosten für Lizenz, Administration und IT Infrastruktur meist so hoch, dass sich viele Firmen dies nicht leisten können.
Aus diesem Grund ist häufig die Datenverwaltung im Windows Explorer und in Netzwerken das Mittel der Wahl. Wie kommt es dann, dass bei einer eigenverantwortlichen Verwaltung trotzdem 30% der Daten verloren gehen oder beschädigt werden? Die häufigste Ursache von beschädigten Daten ist, dass die Software abstürzt, wenn die Datei gespeichert werden soll. Die Ordner, in denen die beschädigten und intakten Dateien gespeichert sind gehen selten wirklich verloren, jedoch werden sie unerreichbar durch Versagen der Hardware oder menschliches Versagen. (Bsp. Versehentliches Löschen)

Die Firma SOLIDWORKS® hat eine Infografik veröffentlicht, die den Verlust von Daten genauer unterteilt. Folgende Grafik fasst die enthaltenen Kernaussagen zusammen:
Da diese Probleme bei traditionellen Systemen vorprogrammiert sind, bringt auch eine PLM Lösung an der Stelle wenig. So lange CAD Daten in Dateien und Ordnern gespeichert werden, bestehen diese Probleme weiter.



Überraschenderweise sichert fast die Hälfte der Unternehmen selbst bei so viel Datenverlust ihre Daten nicht regelmäßig. Dies ist im Wesentlichen auf die IT-Administration, die vorhandene Infrastruktur und die Kosten zurückzuführen. Wenn Dateien verloren gehen oder beschädigt werden, ist die IT-Abteilung mit ihrer Datensicherung die erste Anlaufstelle. Jedoch können Backups auch schief gehen, in diesem Fall sind die Backup-Daten selbst bis zur Hälfte nicht wiederherstellbar. Selbst wenn Sie Ihre Ziel erreichen und die verlorenen Daten wiederherstellen, kann dieser Prozess mehrere Stunden dauern.

Diese Punkte summieren sich schnell auf und resultieren in verlorener Zeit und verpasstem Umsatz.
Wie viel Zeit wird vergeudet, während Ihr gesamtes Projektteam, den ganzen Tag darauf wartet, dass die IT-Abteilung die Daten wiederherstellt? Oder schlimmer noch, wie viele Tage oder Wochen dauert es, von Grund auf neu zu beginnen und alle fehlenden Daten wiederherzustellen?

All diese Probleme werden irrelevant, wenn Sie eine datenbankgesteuerte Cloud-native CAD Lösung wie Onshape einsetzen.

6. Cloud-Washing, Hybrid Cloud-, und Cloud-basierte Lösungen

Viele Softwarehersteller haben das enorme Potenzial der Cloud bereits erkannt. Sowohl aus finanzieller und logistischer Sicht als auch zur Verbesserung der Kundenakquise und –bindung stellt die Cloud ein mächtiges Werkzeug dar. Das Angebot an Cloud Produkten wächst, doch betrachtet man die Anwendungen die „Cloud“ im Namen tragen näher, so fallen erhebliche Unterschiede auf.

Einige Anbieter haben einfach ein bestehendes Produkt mit einem „Cloud“ im Namen versehen - eine Praxis, die auch als „**Cloud-Washing**“ bezeichnet werden kann. Während diese Produkte zwar mit einem zusätzlichen Cloud-Storage-Element ausgestattet sind, ist die Software selbst unverändert. Es handelt sich nach wie vor um eine Anwendung, die heruntergeladen, installiert und aktualisiert werden muss, die jetzt aber möglicherweise zum Kauf und zur Nutzung als wiederkehrende Abonnementmiete zur Verfügung steht. De facto ist die größte Änderung also nur das neue Bezahlmodell.

Ein zur Unterstützung häufig verwendetes Promo-Mittel ist, dass eine Reihe von Software-Titeln zu einer „Suite“ gebündelt wird. Eine Änderung die den Umfang der enthaltenen Software zwar aufbläht, aber kaum Mehrwert generiert. Traditionelle CAD-Anbieter, die sich diese Taktik zu Nutze machen verwenden in ihren Anwendungen immer noch Ordner um Dateien abzuspeichern und unterliegen somit immer noch allen Sicherheitsfragen, die in diesem eBook beleuchtet werden. Hinter der neuen „Cloud-Suite“ verbirgt sich immer noch dieselbe Software.

Mit den „**Hybrid Cloud**“ Lösungen und „**Cloud-basierten**“ Lösungen verhält es sich ähnlich. Sie gehen einen Schritt über das Re-branding hinaus und werden mit neuer Software assoziiert. Tatsächlich ist jedoch nur die standardmäßige Speicherung der Daten in der Cloud neu. Die Software basiert immer noch auf „fat clients“ (voll ausgestatteter Rechner, der ein vollwertiges Betriebssystem, lokale Software und eigene Ressourcen wie Rechenleistung, Speicher und Netzwerkanbindung besitzt) und nutzt weiterhin Ordner um Daten abzuspeichern. Demzufolge muss sie auch weiterhin heruntergeladen, aktualisiert und gewartet werden.

Die dritte Kategorie von Cloud Lösungen sind gehostete Systeme, die auf einem Server installiert sind und von dort aus auf den Computer gestreamt werden. Dies lässt sich am ehesten damit vergleichen, als würde man sich remote auf einen anderen Computer aufschalten. Diese Anwendungen erfordern immer noch, dass die Software auf dem ausgelagerten Rechner installiert und administriert wird. Der Zugriff für den Benutzer erfolgt über den Login durch einen Browser, dieser erfasst dann die Maus- und Tastatureingaben und stellt die dazugehörigen Ergebnisse des ausgelagerten Rechners grafisch dar. Üblicherweise wird diese Cloud Lösung in Kombination mit einem weiteren Dienst wie z.B. Dropbox umgesetzt, in dem die Daten gespeichert werden und darauf zugegriffen wird.

All diese Lösungen sind zumeist gut und erfüllen die Aufgaben, für die sie gekauft wurden, nicht jedoch aus Sicht der Datensicherheit. Die Produkte müssen allesamt lokal installiert werden und sind dateibasiert, was sie anfällig für alle vorab beleuchteten Sicherheitsrisiken macht. Des Weiteren bedürfen alle dieser Lösungen der Administration durch die IT Abteilung, die Software auf jeden Laptop oder Workstations herunterlädt, installiert und wartet. Hinzu kommen die Verwaltung der Lizenzen und das Datenmanagement.

Onshape bildet mit seinem „**Cloud-nativen**“, datenbankbasierten 3D CAD System als einziges Produkt die vierte Kategorie der Cloud Lösungen ab. Aufgrund der vollkommen neuen Softwarearchitektur, in der es keine Dateien gibt, sind Unternehmen systemimmanent vor Datenverlust, Beschädigung oder Diebstahl geschützt.

Was zeichnet Onshape aus und worin besteht die Einzigartigkeit dieser Lösung?

7. Cloud-natives CAD

Die Gründer von Onshape sind alle Veteranen im CAD Umfeld mit 30 oder mehr Jahren Erfahrung aus der Arbeit mit Firmen verschiedener Größen und aus unterschiedlichen Branchen. In Diskussionen mit den Kunden, wie CAD Systeme verbessert werden könnten waren selten Vorschläge für Features und Funktionen die gefragtesten Punkte. Beschwerden über das Modellieren von Teilen und Baugruppen und über das Erstellen von Zeichnungen kamen lediglich von einer Minderheit. Die maßgeblichen Beschwerden drehten sich um die Administration, die Bereitstellung und die Dateien von CAD Systemen.

Die am meisten geforderte Verbesserung war die nach effektiver Zusammenarbeit mit anderen und besseren Wegen um Daten zu teilen. Der Fortschritt in den Web- und Mobiltechnologien stellte einen Weg dar, diese Wünsche zu adressieren. Die Motivation von Onshape war und ist nicht ein weiteres CAD System zu programmieren – davon gibt es bereits genug. Die Motivation von Onshape ist es ein besseres CAD System bereitzustellen das genau die von Kunden geforderten Anforderungen abbildet. Die Bereitschaft hierbei vollkommen neue Wege zu gehen und alte Paradigmen zu brechen legt den Grundstein für die Einzigartigkeit des Produktes und katapultiert das Potenzial der Software an die Spitze aller CAD-Hersteller.

Onshape wurde von Grund auf neu entwickelt. Den Kern bildet der datenbankbasierte, cloud-native Ansatz. Dieser revolutionäre Ansatz ist der einzige Weg, um die Probleme und Beschränkungen die sich aus einem dateibasierten Ansatz ergeben effektiv zu adressieren. Würde man auf eine bestehende Software mit dateibasiertem Kern zusätzliche Funktionen anbauen, würde man niemals ein so sicheres und flexibles Produkt erhalten, wie mit dem Ansatz von Onshape.

Die Bezeichnung “Cloud-nativ” bedeutet also, dass Onshape vollkommen mit Amazon Web Services (AWS) verschmolzen ist. Vereinfacht kann man sagen, dass das gesamte CAD System und alle CAD Daten in einem zentralen Ort in der Cloud abgelegt werden, der von AWS gehosted wird.

Aus Cloud-nativen Lösungen resultieren einige Vorteile:

1. Kein Aufwand für die IT Abteilung
Cloud-native Software muss nicht heruntergeladen oder installiert oder aktualisiert werden. Es bedarf einzig eines Webbrowsers wie beispielsweise Chrome, Firefox oder Safari, wie er auf jedem Computer vorhanden ist. Die Updates der Software (bei Onshape im Zyklus von 3 Wochen) werden zentral eingespielt, so dass automatisch und zeitgleich alle Benutzer weltweit auf die neueste Version gehoben werden. Die Probleme durch verschiedene Softwareversionen bei Zuliefern und Kunden existieren nicht mehr.

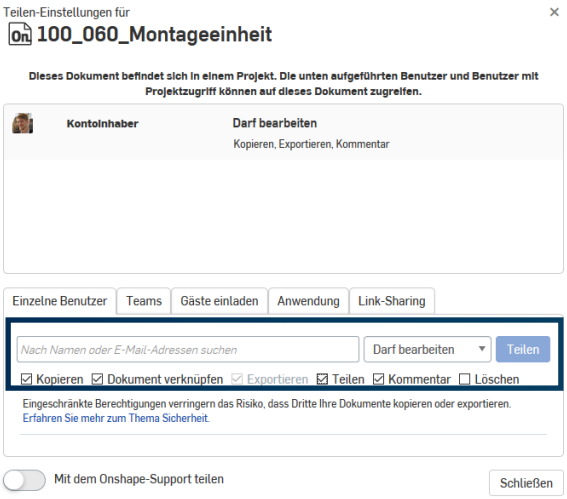
2.Die Daten bleiben wo sie sind
Da sowohl die CAD Daten als auch die Anwendung selbst in der Cloud sind, werden zu keinem Zeitpunkt Daten an lokale Computer gesendet oder heruntergeladen. Lediglich die grafische Information (“ein Bild des Bauteils”) wird im Computer angezeigt. Alle Rechenoperationen werden remote ausgeführt und die Ergebnisse der Berechnungen im Browser angezeigt. Selbst beim Teilen von Daten mit anderen werden keine CAD Dateien übertragen, die geteilte Datei verbleibt an ihrem ursprünglichen Ort, wodurch sie allzeit geschützt ist.

3. Zusätzliche Maßnahmen zur Cybersicherheit
Da Onshape Amazon Web Services nutzt, und die Daten dort speichert, ist es die einzige CAD Plattform, die von so mächtigen Maßnahmen geschützt wird, wie nur ein Großunternehmen wie Amazon sie umsetzen kann. Kleinere Unternehmen hätten niemals die finanziellen Mittel und Ressourcen, um vergleichbare Maßnahmen implementieren zu können. Im Gegensatz zu traditioneller CAD Software, die sich auf die Sicherheitsmaßnahmen des einzelnen Unternehmens stützt, um CAD Daten zu beschützen, bietet Onshape eine erhöhte Sicherheit während des gesamten Designprozesses. Von der Erstellung über die Fertigung bis hin zur Archivierung sind die Daten kontinuierlich geschützt.

8. Sicheres Teilen von CAD Daten

Im Gegensatz zu traditionellen CAD Systemen gibt es bei Cloud-nativen Systemen keine Daten in Ordnern. In Onshape werden Designdaten in „Dokumenten“ gespeichert, die am besten als Container auf Projekt-Ebene beschrieben werden können. Jedes Bauteil, Braugruppe, Zeichnung, Bild, PDF, Video oder andere Projekt-Dateien können in einem einzigen Onshape-Dokument erstellt und aufbewahrt werden. Dadurch werden das Teilen von Projektdaten und die Zusammenarbeit mit anderen erheblich vereinfacht, da alle relevanten Dokumente an einem Ort sind. Des Weiteren ermöglicht der einzigartige Datenbank Ansatz, dass mehrere Nutzer gleichzeitig an demselben Bauteil oder derselben Baugruppe arbeiten können, egal wo sie sich befinden.

Mit den entsprechenden Zugriffsrechten kann jeder auf die aktuellste Version der Designdaten zugreifen – von überall und jedem beliebigen Gerät aus, egal ob ein Webbrowser auf dem Mac, Windows, Linux oder Chromebook ist, auch jedes Android oder iOS Smartphone oder Tablet mit der Onshape APP hat Zugriff auf die Daten.



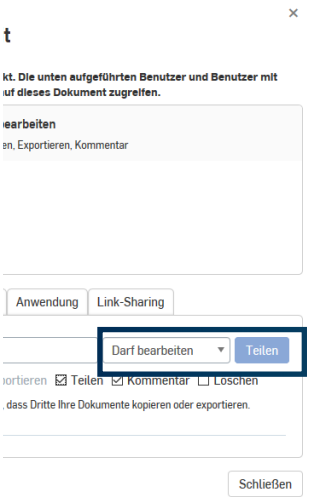
Während bei traditionellen CAD Systemen Daten über E-Mail, FTP oder Dropbox geteilt werden, benötigt Onshape lediglich die E-Mail Adresse des Empfängers. Eine Vereinfachung die nebenbei auch die Sicherheitsrisiken der vorherigen Übermittlungswege aushebelt. Durch einen Klick auf die Schaltfläche “Teilen” öffnet sich ein Dialogfeld in dem die Rechteeinstellungen für das Teilen sehr präzise eingestellt werden können.

Sobald eine andere Person als berechtigter Nutzer in das Dokument aufgenommen wurde, wird sie per E-Mail benachrichtigt. In dieser E-Mail ist ein Link enthalten, der sie direkt in den Browser und zum Dokument führt. Besitzt diese Person keinen Onshape Account, so wird die Datei im „Nur-Anzeigen“ Modus dargestellt, unabhängig der eingestellten Berechtigungen.

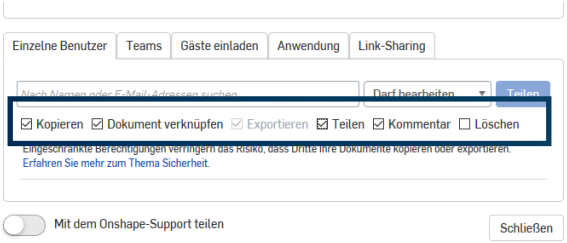
Jedem Benutzer und jedem Team können für jedes Dokument individuelle Berechtigungen zugewiesen werden:

8.1. Rechtevergabe beim Teilen von Daten

“Darf bearbeiten”
Mit dieser Berechtigungseinstellung erhält jeder Benutzer Zugang zum Dokument und kann dieses bearbeiten. Benutzer können innerhalb des Dokuments beliebig Inhalte hinzufügen, ändern und löschen. Damit haben sie dieselben Rechte wie der ursprüngliche Ersteller des Dokuments. Da jeder Vorgang in Onshape dokumentiert wird, stellt auch das versehentliche Löschen von Daten kein Problem dar. Daten können jederzeit zu einem früheren Versionspunkt wiederhergestellt werden. Wenn mehrere Personen gleichzeitig am selben Bauteil oder derselben Baugruppe arbeiten, kann über „Haupt- und Nebenversionen“ die gegenseitige Behinderung umgangen werden.



“Darf anzeigen”
Mit dieser Berechtigungseinstellung erhält jeder Benutzer Zugang zum Dokument und kann dieses anzeigen. Benutzer können Bauteile, Baugruppen und Zeichnungen innerhalb des Dokuments anzeigen, Elemente von Baugruppen verschieben und verbergen und Abmessungen kontrollieren. Diese Berechtigung ist vollkommen ausreichend für Zulieferer, damit sie ein Angebot abgeben können.



Zusätzlich zu diesen groben Einstellungen können die Berechtigungen auch feiner eingestellt werden:

“Kopieren” –
Der Benutzer kann Kopien des Dokuments erstellen. Dabei entsteht eine vollkommen eigenständige Kopie mit keiner Verbindung zum ursprünglichen Dokument. Diese Einstellung sollte nur an vertrauenswürdige Personen vergeben werden.

“Dokument verknüpfen”
Mit dieser Einstellung wird es ermöglicht Elemente eines Dokuments in ein anderes Dokument einzufügen. Ein Beispiel hierfür wäre die Verwendung von Standardteilen in einer Baugruppe. Das Entfernen des Häkchens in der Checkbox deaktiviert diese Funktion.

“Exportieren”
Wird ein Dokument mit dieser Einstellung geteilt, wird die Person dazu berechtigt das Dokument in einem neutralen Format zu exportieren z.B. STL, STEP oder Parasolid. Wenn die Berechtigung für “Dokument verknüpfen“ erteilt ist, dann wird der Export automatisch mit berechtigt.

“Teilen”
Diese Einstellung legt fest, ob die berechtigte Person das Dokument mit einer anderen teilen darf.

“Kommentar”
Mithilfe dieser Einstellung kann die berechtigte Person Kommentare im Dokument einfügen. Dies ist eine hervorragende Funktion, wenn beispielsweise eine Kommunikation mit dem Zulieferer oder Kunden ermöglicht werden soll.

Das Teilen von Dokumenten in Onshape ist einerseits sicher und gewährt andererseits den sofortigen Zugriff. Dies ist möglich, da geteilte Dokumente Onshape nie verlassen. Die Datei bleibt an ihrem ursprünglichen Platz, lediglich die Anzahl an Personen die darauf zugreifen wird erhöht. Zudem ist es möglich die Berechtigung bestehender Personen jederzeit zu ändern, wie folgendes Beispiel verdeutlicht:

Nehmen wir an, dass ein Dokument mit einem Zulieferer geteilt wird. Dazu eignet sich die Berechtigung „Darf anzeigen“ in Kombination mit „Kommentar“ für eine gute Kommunikation. Wenn nun in einer weiter fortgeschrittenen Projektphase der Zulieferer berechtigt werden soll das Dokument auch bearbeiten zu können oder zu exportieren, dann ist das ebenso einfach möglich, wie einem nicht geeigneten Zulieferer die Berechtigungen wieder zu entziehen. Beide Änderungen sind sofort umgesetzt, während das Dokument sicher in den Servern von AWS ruht.

Die Änderungsgeschwindigkeit bedeutet tatsächlich „sofort“, denn selbst wenn eine Person sich noch im Dokument befindet, wenn ihr die Rechte entzogen werden, schließt sich das angezeigt Dokument einfach. Dokumente in Onshape zu teilen ist keine Garantie, dass sie nie wieder Daten verlieren werden, aber es der sicherste Weg um Daten zu teilen ohne, dass dabei unkontrollierte Kopien entstehen.

8.2. Weitere Risikovermeidung

Die Kommunikation zwischen den Onshape Servern und den Endgeräten der Benutzern (Computer, Smartphone, etc.) ist stets verschlüsselt. Damit gibt Onshape die Regeln vor, mit denen Benutzer in den Dokumenten agieren. Dies wird Benutzern mit böswilliger Absicht zwar den Weg an Ihr geistiges Eigentum erschweren, jedoch hält es sie nicht davon ab beispielsweise Screenshots zu machen oder mittels Reverse Engineering weitere Daten des Dokuments offen zu legen. Vor kriminellen Machenschaften vermeintlich vertrauenswürdiger Personen sind Sie also trotz aller Vorkehrungen nicht geschützt – und werden es aber auch nie sein.

Wie mit jedem geistigen Eigentum des Unternehmens sollten Sie auch bei CAD Daten Vorsicht walten lassen, wem Sie die Daten anvertrauen und Berechtigungen standardmäßig auf ein Minimum beschränken. In Situationen in denen das Vertrauensverhältnis bereits geschädigt ist empfiehlt es sich, Daten in ein weiteres Onshape Dokument zu kopieren. Dort können Sie die Daten von allen Features befreien, nur in tesselierter Form (STL) teilen oder weitere Schritte anwenden, um den Informationsgehalt so gering wie möglich zu halten. Dies stellt selbstverständlich eine gleichartige oder schlimmere Vorgehensweise dar, wie sie es wäre, wenn man die Daten auf konventionelle Weise teilen würde.

9. Der Unterschied zwischen öffentlichen und privaten Dokumenten

Worin liegt der Unterschied zwischen einem Öffentlichen Dokument und einem Privaten Dokument in Onshape?

Dokumente mit der Zuweisung Öffentlich sind für alle Onshape-Benutzer sichtbar und können von ihnen geöffnet und kopiert werden. Das Editieren der öffentlichen Dokumente ist jedoch weiterhin den Benutzern vorbehalten, die über die Teilen-Funktion die entsprechende Zugriffsrechte erhalten haben. Damit sind öffentliche Dokumente besonders für den Einsatz in Open Source Projekten geeignet. Unabhängig davon, ob ein Dokument öffentlich oder privat ist, können beliebig viele öffentliche Benutzer zu einem Projekt hinzugefügt werden, die dann alle zeitgleich am Projekt arbeiten können.

Eine weitere Verwendungsmöglichkeit für öffentliche Dokumente ist, sie in andere Dokumente einzufügen wie z.B. Standardteile. Als Lieferant von Standardteilen könnten beispielsweise alle Teile öffentlich gestellt und von jedem verwendet werden. Je einfacher der Zugang zu Standardteilen eines Lieferanten ist, umso eher werden Konstrukteure diese in ihren Bauteilen verwenden und dann auch eher dort bestellen, wenn es an die Produktion geht.

Ab der kostenpflichtigen Version von Onshape Professional können beliebig viele private Dokumente erstellt werden. Private Dokumente sind bis zum Zeitpunkt an dem sie gezielt mit anderen geteilt werden nur für den Ersteller einsehbar. Dies betrifft alle Onshape Benutzer gleichermaßen wie Angestellte von Onshape. Keine Person kann auf private Dokumente zugreifen oder diese ansehen, ohne dass sie nicht ausdrücklich die Erlaubnis dazu bekommen hat. Um Dokumente mit dem Support von Onshape zu teilen muss das entsprechende Kontrollkästchen aktiviert werden. Im Falle dass eine Subscription ausläuft, werden alle Dokumente in den „Nur-anzeigen“ Zustand versetzt. In diesem Zustand haben Benutzer weiterhin Zugriff auf die Dokumente und können sie auch weiterhin exportieren. Wird die Subscription wieder aktiviert, kehren die Dokumente wieder in den ursprünglichen Zustand zurück und können wie gewohnt bearbeitet werden. Private Dokumente werden durch keine Aktion öffentlich, es sei denn der Besitzer ordnet es so an.

Hinweis	
	Befindet sich dieses Erdball-Symbol auf Ihrem Onshape Dokument, ist es öffentlich. Kein Symbol bedeutet das Dokument ist privat.

10. Ein Überblick zur Sicherheit bei Onshape

Onshape hat zusätzlich zu den eingebauten Sicherheitsmaßnahmen von Amazon Web Services eigene Schutzmechanismen installiert. Diese adressieren Client-seitig den Zugriff auf Daten und schützen im Backend vor Sicherheitslücken und Datenverlust.

Leider nehmen die Risiken durch Angriffe von außen (Phishing, Malware, Verschlüsselungstrojaner) für alle Unternehmen zu. Um diesen, sich ständig weiterentwickelnden Sicherheitsbedrohungen entgegenzuwirken, beschäftigt Onshape eine eigene Sicherheitsabteilung, deren einzige Aufgabe darin besteht, die Daten der Kunden zu schützen. Dieser Aufwand an Ressourcen übertrifft das, was die meisten Unternehmen selbst für den Schutz ihrer CAD-Daten aufwenden (können). Der agile Entwicklungsprozess und die Cloud-Native Architektur von Onshape ermöglichen es, aufkommende Sicherheitslücken innerhalb von Stunden zu schließen. Bei traditionellen Softwareherstellern dauert es meist Monate bis zum nächsten Software-Update.

Aus den sich ändernden Beziehungen zwischen Mitarbeitern und Lieferanten, können zusätzliche Sicherheitsbedenken hinsichtlich des Datenzugriffs entstehen. Genau hier glänzt Onshape mit seinen Echtzeit-Analysen, sowie der Möglichkeit, den Datenzugriff sofort zu widerrufen.

Im Folgenden sind zunächst 8 Maßnahmen aufgeführt, mit denen Onshape dafür sorgt, dass geistiges Eigentum besser geschützt wird. An dieser Stelle sei erwähnt, dass keine Vorsichtsmaßnahme Hacker davon abhalten wird, in Systeme einzubrechen. Jedoch bieten die mehrschichtigen Schutzmaßnahmen von Onshape wahrscheinlich eine deutliche Verbesserung gegenüber den Bemühungen der meisten Unternehmen, um die CAD Daten zu schützen.

Passwortgeschützter Zugang

Bevor jemand auf Design-Daten zugreifen kann, muss derjenige registriert sein und über gültige Anmeldedaten verfügen: eine E-Mail und ein Passwort. Alle Passwörter unterliegen minimalen Komplexitätsanforderungen und dürfen keinem der 5 zuletzt verwendeten Passwörter entsprechen. 5 ungültige Login-Versuche blockieren den Zugang zu diesem Konto für 30 Sekunden. Dies verhindert „Brute-Force“-Passwort-Angriffe, bei denen Hacker systematisch alle möglichen Passwörter und Kombinationen ausprobieren, bis das Richtige gefunden wird.

Hinzufügen und Entfernen von Benutzern zu Onshape ist sehr einfach, wenn es als Unternehmen eingerichtet ist. Bis zum arbeitsfähigen Einsatz neuer Mitarbeiter dauert es nur wenige Minuten. Den einzigen Arbeitsschritt dafür muss der Administrator ausführen, indem er die Email Adresse des Benutzers in die Liste der Mitarbeiter aufnimmt. Daraufhin wird eine Email an die neu hinzugefügte Person gesendet, die lediglich ein Passwort vergeben muss, um den neuen Account anzulegen.

Im Vergleich dazu dauert der Prozess bei traditionellen CAD-Systemen typischerweise deutlich länger:

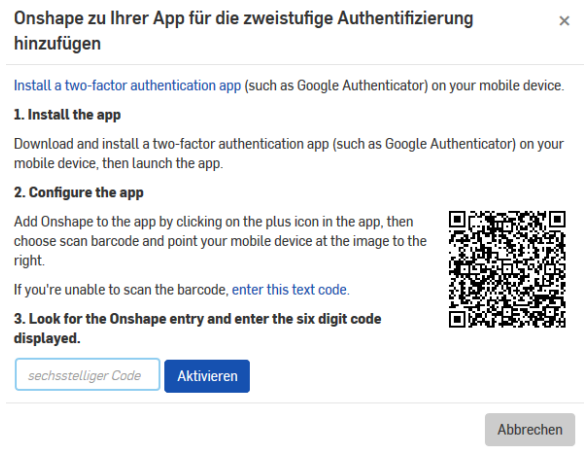
1. Einholen einer Bestellbestätigung und übersenden an den Reseller
2. Wartezeit, bis die Bestellung dort verarbeitet wird und ein Lizenzschlüssel vom Hersteller angefordert wird.
3. Auswählen und Bestellen von neuer Hardware, um das 3D CAD System ausführen zu können.
4. Ausstatten der Hardware mit Virenschutz und anderen Sicherheitsvorkehrungen.
5. Herunterladen, installieren und konfigurieren des CAD Systems und der PDM Software.
6. Verteilen der Hardware an den End User.

Im Falle, dass ein Mitarbeiter ausscheidet, ein Teammitglied zu einem anderen Projekt wechselt oder der Vertrag eines Kunden abläuft, ist es genauso einfach, den Zugriff auf die CAD-Daten zu entziehen. Dazu muss nichts weiter getan werden, als in der Liste der Benutzer einfach auf das „x“ neben dem Namen der Person zu klicken. Die Login-Daten werden somit widerrufen. Bei herkömmlichen CAD-Systemen wird dazu das Systempasswort geändert, aber es ist in keinem Aktionsverlauf dokumentiert, ob der Benutzer vor seinem Austreten Kopien der Daten gemacht haben. Passwörter von Benutzern werden von Onshape nie im Klartext gespeichert. Stattdessen nutzt Onshape starke kryptographische Hashfunktionen, so dass selbst bei Kompromittierung des internen Passwortspeichers das ursprüngliche Passwort nicht ausgelesen werden kann.

2-Faktor Authentifizierung

Ergänzend zum Schutz durch Passwörter kann jeder Benutzer eine zusätzliche Sicherheitsebene für sein Konto aktivieren, die als 2-Faktor-Authentifizierung (2FA) bezeichnet wird. Bei der 2FA handelt es sich um eine weitere Sicherheitsebene, die den Login-Schutz durch ein externes Gerät, das sich nur im direkten Zugriff des Benutzers befindet (z.B. Smartphone), verstärkt. Wenn die 2FA aktiviert ist, muss jeder Benutzer einen 6-stelligen Code eingeben, der von einer Smartphone-Anwendung wie Google Authenticator generiert wird.

Dieser Code ändert sich alle 30 Sekunden, d.h. selbst wenn ein Angreifer das Passwort und den 2FA-Code erhalten würde, hätte er nur 30 Sekunden Zeit, um ihn zu verwenden. Benutzer können ihr Konto so konfigurieren, dass sie auf einem vertrauenswürdigen Computer 30 Tage lang nicht nach Ihrem 2FA-Code gefragt werden. Dies schafft ein praktikables Gleichgewicht zwischen Sicherheit und Bequemlichkeit. Falls das Smartphone verlogen geht, kann der Wiederherstellungscode verwendet werden, der bei der Einrichtung generiert wurde. Andernfalls hilft der Onshape-Support.



Datenbank Sicherungsverfahren

Die Datenbanken von Onshape werden über mehrere, geografisch verteilte Datenzentren repliziert. Dies geschieht durch eine Vervielfältigung der Daten in wenigen Millisekunden, während die Benutzer daran arbeiten. Darüber hinaus werden sämtliche Datenbanken von Onshape alle 3 Stunden gesichert. Im Abstand von mindestens 3 Wochen werden die Daten aus diesen Sicherungen wiederhergestellt und alle Dokumente sogenannten Integritätstests unterzogen. Selbst wenn Benutzer versehentlich ein Dokument löschen und den Papierkorb geleert haben, können sie sich an den Onshape-Support wenden, um es zurückzubekommen.

Dedizierte Server

Auf allen Servern, die den Onshape-Dienst bereitstellen– mehrere hundert an der Zahl – läuft nur Onshape. Auf diesen virtuellen Servern wird ausschließlich die Software installiert, die für die Bereitstellung des Onshape-Dienstes benötigt wird. Jede Installation auf den Servern wird automatisiert durchgeführt. Um sicherzustellen, dass alle Onshape-Dienste die gleichen Versionen jeder Softwarekomponente ausführen, werden die Server regelmäßig ersetzt, manchmal innerhalb weniger Stunden. Wenn die Nachfrage nach dem Onshape-Dienst hoch ist, werden automatisch weitere Server hinzugefügt.

Kommunikationssicherheit

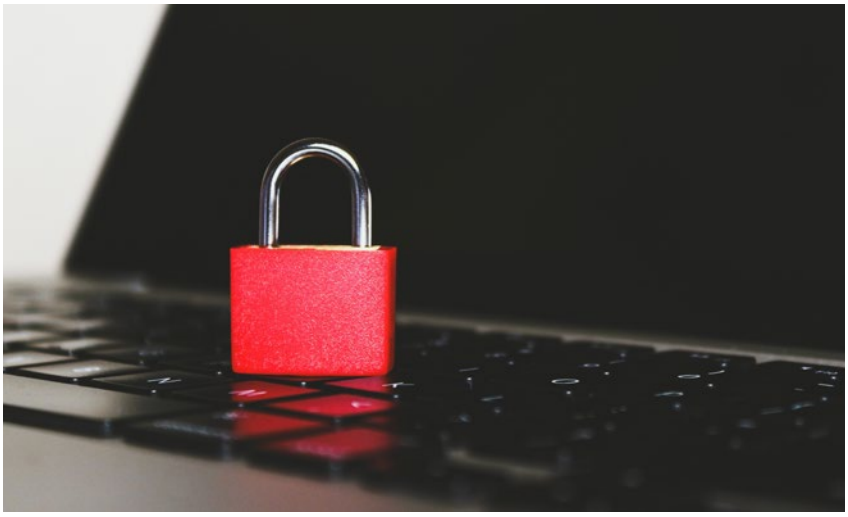
Die Konstruktionsdaten verlassen niemals das sichere Rechenzentrum von Onshape. Die Darstellung im Browser oder im mobilen Client sind nur tesselierte (und verschlüsselte) visuelle Approximationen des Designs. Somit werden zu keinem Zeitpunkt verwertbare Informationen physisch auf dem Computer des Benutzers gespeichert. Darüber hinaus können Onshape-Konten so konfiguriert werden, dass der Benutzer keine CAD-Daten übertragen oder exportieren kann.
Onshape erfordert für alle Dienste, einschließlich der öffentlichen Website und der Onshape-Foren das Kommunikationsprotokoll HTTPS. Die Einzelheiten dieser Implementierung (Zertifikate, Zertifizierungsstellen und unterstützte Chiffren) werden regelmäßig überprüft. Automatisierte Tools testen die Live-Server von Onshape auf ihre Anfälligkeit für neue und bestehende SSL/TLS-Schwachstellen. Um sicherzustellen, dass die Browser mit Onshape nur über HTTPS interagieren, wird HSTS verwendet.

Verschlüsselung

Onshape schützt alle Design-Daten mit starken kryptografischen Verschlüsselungsverfahren und durch eine Speicherung mit 256-Bit-AES-Verschlüsselung. Alle Daten werden verschlüsselt, wenn sie gespeichert werden (im Ruhezustand) und während der Kommunikation zwischen den Servern von Onshape und Client des Benutzers (während der Übertragung). Der Zugriff von Kundenrechnern auf die Datenbanken mit den Entwurfsdaten, wird durch das Datenübertragungsprotokoll SSL/TLS abgesichert.

Sicherheits- und Penetrationstests

Die Server von Onshape werden kontinuierlich Penetrationstests unterzogen. Dies wird von einem Drittanbieter durchgeführt, der ein globales Team professioneller Sicherheitsforscher beschäftigt. Diese Forscher haben nur eine Aufgabe; das Entdecken und Melden von Sicherheitslücken. Onshape wird fortlaufend diesen Sicherheitstests unterzogen, um den kontinuierlich Strom der Service-Updates von Onshape gegen bestehende und neu entdeckte Bedrohungen zu validieren. Jegliche Serveraktivitäten und Administratorzugriffe werden von Onshape protokolliert und überprüft. Jede Server-Transaktion wird zur späteren Analyse und Bedrohungserkennung aufgezeichnet.



Zusätzliche Sicherheitsmaßnahmen von Amazon Web Services

Zusätzlich zur bestmöglichen Datensicherheit in der Cloud sind die Rechenzentren von Amazon Web Services in unscheinbaren Einrichtungen untergebracht. Der physische Zugang wird sowohl an der Grenzlinie als auch am Gebäudeeingang durch professionelles Sicherheitspersonal (bewaffnete Wachen) unter Verwendung von Videoüberwachung, Einbruchserkennungssystemen und anderen elektronischen Mitteln streng kontrolliert. AWS gewährt nur Mitarbeitern und Kunden mit triftigem Grund Zugang zu Rechenzentren und Informationen. Autorisiertes Personal muss mindestens zweimal eine Zwei-Faktor-Authentifizierung durchlaufen, um Zugang zu den Serverräumen des Rechenzentrums zu erhalten. Alle Besucher und Kunden müssen sich ausweisen und werden ständig von autorisiertem Personal begleitet. In diesem Whitepaper führt AWS die Einzelheiten zu den Maßnahmen für Sicherheit und Servicekontinuität aus.

AWS wird bereits seit einigen Jahren von amerikanischen Regierungseinrichtungen verwendet (darunter die CIA). Doch seit 2017 ist AWS auch vorläufig autorisiert, Aufgaben des US Verteidigungsministeriums mit der Geheimhaltungsstufe 5 zu handhaben. Die Technologien für die Sicherheit dieser Regierungseinrichtungen sind im Grunde gleich wie die für ihr Public Cloud Angebot.

All diese Sicherheitsprotokolle stellen nur einen Teil aller Maßnahmen dar. Selbst für den Fall, dass sich ein Hacker unbefugt Zugang zu den Daten verschafft wäre er nicht in der Lage sie auszulesen. Hintergrund ist, dass zum Lesen und Bearbeiten der Daten eine funktionsfähige Version von Onshape benötigt wird, da die Daten so verschlüsselt sind, dass nur Onshape sie lesen kann. Zum Öffnen der Daten wäre also das Hacken mehrerer Systeme auf mehreren Servern notwendig.

Um die gestohlenen Daten nutzen zu können, müssten die Hacker nicht nur eine Kopie aller Softwarekomponenten von allen verschiedenen Servern erstellen (einschließlich der Lokalisierung dieser Server und der Umgehung der Sicherheitsvorkehrungen, die sie schützen). Zusätzlich müssten sie auch in der Lage sein, die genaue Konfiguration jedes dieser Server nachzubilden und sie auf genau die gleiche Weise zu verbinden, wie die Produktivversion von Onshape es macht.

Da sich der Hackingprozess theoretisch beschreiben lässt, ist er auch technisch nicht unmöglich – jedoch ist die Wahrscheinlichkeit sehr gering. Die Konstruktionsdaten sind in Onshape also bestmöglich geschützt.

11. Sichern Sie die Zukunft Ihrer CAD-Daten

Wenn Sie bereits ein herkömmliches Desktop-installiertes 3D-CAD-System verwenden, werden Ihnen viele der in diesem eBook behandelten Fragen zur Dateifreigabe und Sicherheit bekannt sein. Wie im Laufe des Buches aufgezeigt kann mit Onshape als primäres CAD-System oder als Ergänzung zu bestehenden Systemen die Möglichkeit von Datenverlust oder -diebstahl drastisch reduziert werden. Neben all den Sicherheitsaspekten bietet Cloud-natives CAD jedoch auch andere entscheidende Vorteile, darunter die Zusammenarbeit, Skalierbarkeit und die Wirtschaftlichkeit. In Kombination machen sie Cloud-natives CAD wie Onshape es bietet zu einem mächtigen Werkzeug für die Produktentwicklung.

Onshape Professional Testversion

Erleben Sie die Unterschiede zu traditionellem CAD selbst und starten Sie Ihr eigenes Projekt in der Onshape Professional Testversion.

Sofortiger Zugriff auf CAD von überall
Onshape ist auf jedes beliebige Endgerät ausgelegt, greifen Sie also ab sofort auf Ihre CAD Daten von dem Computer, Mac, Smartphone oder Tablet aus zu. Sie sind nicht länger an die eine Workstation gebunden, auf der ihr traditionelles CAD System lizenziert ist.

Part Studios
Konstruieren Sie mehrere Bauteile die untereinander referenziert sind in einem Dokument. Onshape erlaubt es mehrere Bauteile auf dieselbe Skizze oder Features zu referenzieren. Nutzen Sie diesen Vorteil, indem sie mehrere Bauteile gleichzeitig konstruieren und editieren.

Baugruppen
Nutzen sie einen neuen Ansatz, um Baugruppen zu erstellen. Verknüpfungspunkte auf einem höheren Level ermöglichen es den Benutzern mit einem Drittel der Verbindungselemente wie in traditionellen CAD Systemen auszukommen. Baugruppen in Onshape sind einfacher zu erstellen, zu verwalten und zu bearbeiten.

Sofortiges Teilen
Arbeiten Sie mit Kollegen und Zulieferern in Echtzeit zusammen, ohne dabei Ihr geistiges Eigentum durch Kopien aus den Händen zu geben. Mit Onshape haben Sie die Möglichkeit Zugriffsrechte sofort zu erteilen und ebenso schnell wieder zu entziehen.

Haupt- und Nebenversionen
Experimentieren sie mit Designideen in beliebig vielen Nebenversionen und fügen Sie später einfach die Elemente in das endgültige Design, die am besten funktionieren.

Designen-im-Kontext
Mit dieser mächtigen Funktion können Sie Bauteile im Kontext von Baugruppen bearbeiten um sicherzustellen, dass sie weiterhin passen und ihre Funktion erfüllen. Das Designen-im-Kontext unterstützt Konstrukteure dabei kaputte Referenzen zu verhindern, ein Problem das bei traditionellen CAD Systemen häufig auftritt, wenn Teile geändert oder gelöscht werden.

Zeitgleiche Blechkonstruktion
Die integrierten Funktionen für parallele Betrachtung von flachen, gefalteten und tabellarischen Ansichten erlaubt es Nutzern Fehler und Überschneidungen schnell zu erkennen, Alterativen zu begutachten und somit den Ausschuss und die Nacharbeit in der Fertigung zu verringern.

Integrierte Cloud Apps für Ingenieure
Der Onshape App Store hält eine Fülle essentieller Ingenieurswerkzeuge bereit: CAM, Simulation, Rendering uvm. Alle Apps besitzen aufgrund der Cloud die gleiche Produktivitätsverbesserung wie Onshape.

Fordern Sie gleich heute Ihre Testlizenz von Onshape Professional an und testen Sie selbst die eingebauten Funktionen für Datenmanagement und Zusammenarbeit. Jetzt anfordern!

INNEO®
That's IT.

Onshape

A PTC Business

Onshape ist die einzige **Software-as-a-Service** (SaaS) Plattform für **Produktentwicklung**, die robuste CAD Werkzeuge mit **Echtzeit Datenmanagement**, **Zusammenarbeit** und **Geschäftsanalysen** vereint.
Vorgesetzte und Führungskräfte können **minutengenaue Berichte** über den Fortschritt und Status von Projekten erhalten. Die eingebaute **Versionskontrolle** verhindert teure Verzögerungen und Fehler in der Fertigung.

Weitere Informationen:
www.inneo.de/onshape
www.inneo.ch/onshape