PROSTEP
integrate the future

Whitepaper

# DATENSICHERHEIT
# UND KNOW-HOW-SCHUTZ

Unsere Daten sind auf ihrem Weg durch die globalen Datennetze ständig der Gefahr des Ausspähens ausgesetzt. Maßnahmen zur Datensicherheit und zum Schutz des geistigen Eigentums dürfen jedoch nicht erst beim Datenaustausch ansetzen – die Grundlagen dafür müssen Unternehmen in der eigenen Organisation legen. Erforderlich ist ein umfassendes Sicherheitskonzept, das – ausgehend von der Analyse der möglichen Bedrohungen und ihrer Eintrittswahrscheinlichkeit – die Schutzziele und die zu ergreifenden Maßnahmen spezifiziert. Dabei sollten beide Dimensionen der Sicherheit berücksichtigt werden, nämlich sowohl die Sicherheit vor böswilligen Angriffen als auch der Schutz vor menschlichem oder technischem Versagen.

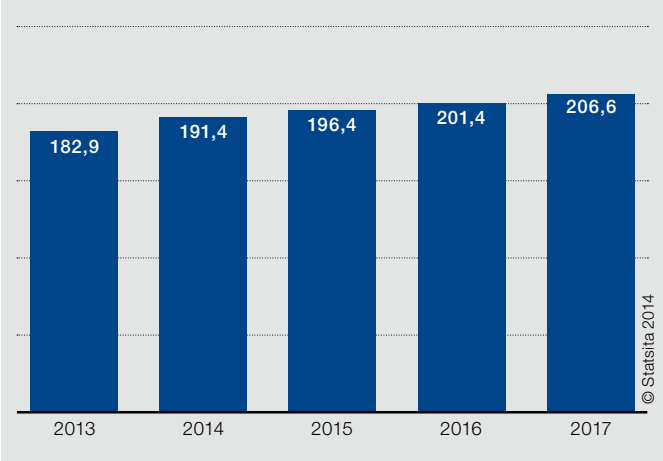
# Inhalt

# Einleitung/Abstract

Der Skandal um die Ausspähung der Internetkommunikation durch die NSA hat deutlich gemacht, wie anfällig unsere Daten auf ihrem Weg durch die globalen Datennetze sind. Maßnahmen zur Datensicherheit und zum Schutz des geistigen Eigentums (IPP oder Intellectual Property Protection in der englischen Schreibweise) dürfen jedoch nicht erst beim Datenaustausch ansetzen – die Grundlagen dafür müssen die Unternehmen in der eigenen Organisation legen. Erforderlich ist ein umfassendes Sicherheitskonzept, das – ausgehend von der Analyse der möglichen Bedrohungen und ihrer Eintrittswahrscheinlichkeit – die Schutzziele und die zu ergreifenden Maßnahmen spezifiziert. Dabei sollten beide Dimensionen der Sicherheit berücksichtigt werden, nämlich sowohl die Sicherheit vor böswilligen Angriffen (security) als auch der Schutz vor menschlichem oder technischem Versagen (safety). Die Umsetzung eines solchen Sicherheitskonzeptes erfordert integrierte Werkzeuge und Dienstleistungen aus der Hand eines vertrauenswürdigen Software- und Systemhauses, das die Prozesse seiner Kunden kennt.

# Die Herausforderung der globalen Datenkommunikation

Ein Großteil der geschäftlichen Kommunikation läuft heute über E-Mail. Dadurch hat das Risiko von unbeabsichtigten Datenverlusten oder gezieltem Diebstahl deutlich zugenommen. Die Veruntreuung brisanter Firmeninterna kann verheerende Folgen haben – so soll der Einbruch des Aktienkurses von Lehman Brothers im Vorfeld der globalen Finanzkrise durch die unautorisierte Weitergabe einer internen E-Mail ausgelöst worden sein. Für die IT-Verantwortlichen heißt das, dass sie E-Mails und E-Mailsysteme nicht nur vor Bedrohungen von außen (Viren, Trojaner etc.) schützen, sondern gleichzeitig die Integrität der versandten Informationen sicherstellen, den ungewollten Abfluss vertraulicher Informationen unterbinden und die Nachvollziehbarkeit der Datenkommunikation bei Rechtsstreitigkeiten gewährleisten müssen. Keine leichte Aufgabe angesichts des wachsenden Volumens an digitalen Informationen.




*Prognose zur Anzahl der täglich versendeten E-Mails weltweit von 2013 bis 2017 (in Milliarden)*

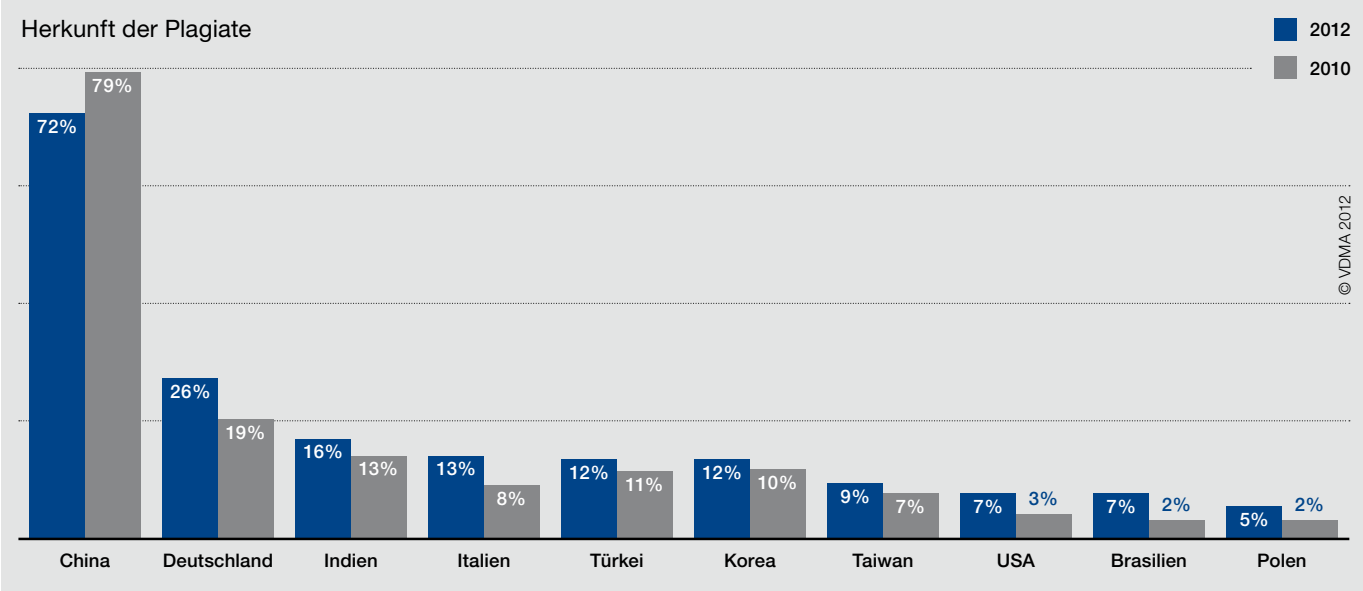
Rund 191 Milliarden E-Mails werden aktuellen Erhebungen zufolge täglich um den Globus geschickt. Schätzungsweise nicht mehr als drei Prozent davon sind verschlüsselt, selbst wenn sie vertrauliche Informationen und/oder Dateianhänge wie Finanzdaten, juristische Unterlagen, Patientendaten, urheberrechtlich geschützte Bild- und Musikdaten oder sensible Produktdaten enthalten. Im Prinzip ist eine E-Mail nicht sicherer als eine Postkarte, weil ihr im Unterschied zum klassischen Geschäftsbrief Unterschrift und Umschlag fehlen, die für die Authentizität des Absenders und die Vertraulichkeit der Informationen bürgen. Selbst wenn sie verschlüsselt sind, erfassen die Verschlüsselungsmechanismen der Mailprogramme nur den so genannten Mailbody und nicht die Anhänge; außerdem lassen sie sich – wie die Enthüllungen des Whistleblowers Edward Snowden bewiesen haben – recht einfach knacken.

Gefährdet sind vor allem die Dateianhänge, die oft besonders schützenswerte Informationen enthalten. Das gilt nicht nur, aber eben auch für die Produktdaten und das in ihnen steckende Know-how. Ungeachtet der Gefahren für den Schutz des geistigen Eigentums und der in vielen Unternehmen geltenden Sicherheitsbestimmungen werden immer noch erschreckend viele Produktdaten per E-Mail ausgetauscht. Das belegt eine im Jahr 2011 vom Fraunhofer IPK zusammen mit dem PLM-Hersteller CONTACT Software und dem VDI durchgeführte Studie, an der über 1.400 Ingenieure aus unterschiedlichen Branchen teilnahmen. Selbst in der Automobilindustrie mit ihren hohen Anforderungen in punkto Know-how-Schutz gaben 45% der Befragten an, CAD- und Produktdaten mit Kunden und Zulieferern per E-Mail auszutauschen.

Der sorglose Umgang mit den Produktdaten ist nicht der einzige Grund, aber sicher einer der Gründe dafür, dass die Produktpiraterie so dramatisch zunimmt. Aktuellen Schätzungen des Deutschen Industrie- und Handelskammertags (DIHK) zufolge entsteht allein der deutschen Wirtschaft durch Produktpiraterie jedes Jahr ein Schaden von 50 Milliarden Euro – mehr als doppelt so viel wie noch vor ein paar Jahren. Zwei Drittel aller Fälschungen kommen laut DIHK aus China und Hongkong, mit leicht sinkender Tendenz, aber dafür mehren sich die Fälle von Fälschungen aus Singapur und Indien. Gerade für mittelständische Unternehmen ohne mächtige Rechtsabteilung stellt der Diebstahl ihres geistigen Eigentums eine große Bedrohung dar: sie verlieren im globalen Wettbewerb ihren Wissensvorsprung, erhalten als Zulieferer vielleicht trotz erfolgreicher Konzeptentwicklung keinen Serienauftrag oder erleiden als Markenhersteller durch schlechte Raubkopien Imageverluste.

# Innere und äußere Gefahrenherde für die Datensicherheit

Die oben genannten Zahlen des DIHK belegen, dass die Produktpiraterie in einigen Ländern weiter verbreitet ist als in anderen. Nachzügler der Industrialisierung wie China, die ein berechtigtes Interesse am Transfer von Wissen und Technologie haben, räumen dem Schutz des geistigen Eigentums einen anderen Stellenwert ein. Oft müssen westliche Unternehmen Joint Ventures mit lokalen Firmen eingehen, um den jeweiligen Markt beliefern zu können. Damit stehen sie vor der Frage, wie sie diese Standorte und Tochtergesellschaften IT-technisch einbinden, ohne ihr geistiges Eigentum möglichen Angriffen auszusetzen. Einige Automobilhersteller lassen Standorte in Ländern mit Gefahrenpotential zum Beispiel gar nicht mehr direkt auf ihre IT-Systeme zugreifen, sondern stellen ihnen die Produktdaten über eine separate Plattform zur Verfügung.




*Die Volksrepublik China ist weiterhin auf Platz eins der Herkunftsländer bei Produkt- und Markenpiraterie. Deutschland als Herkunftsland wurde von einem Viertel der betroffenen Unternehmen genannt.*

Man braucht aber gar nicht so weit in die Ferne zu schweifen, um die heimlichen Häfen der Produktpiraten aufzuspüren. Zahlen des VDMA zufolge rangieren im Maschinen- und Anlagenbau deutsche Unternehmen als Plagiatoren hinter China an zweiter Stelle. Schlimmer noch: Während der Anteil Chinas an den Fälschungen von Komponenten, Ersatzteilen etc. in den letzten zwei Jahren gefallen ist, hat der Anteil deutscher Plagiatoren zugenommen.

## Gefahrenpotential durch illoyale Mitarbeiter

Innerhalb der Unternehmen ist der Zugang zu sensiblen Produktdaten meist durch ein (rollenbasiertes) Berechtigungskonzept geregelt, das normalerweise in einer Produktdaten (PDM)- bzw. Product Lifecycle Management (PLM)-Lösung abgebildet wird. Wie gut sensible Daten dadurch geschützt sind, hängt auch davon ab, wie sorgfältig die Mitarbeiter mit den Berechtigungen und Passwörtern umgehen. Die Umsetzung des Sicherheitskonzeptes erfordert in jedem Fall eine Sensibilisierung der Mitarbeiter, um sie über die Gefahren für die Datensicherheit aufzuklären und den Blick für das eigene Verhalten und das der Kollegen zu schärfen.

Die größere Gefahr für die Datensicherheit und das geistige Eigentum geht nicht unbedingt von Nachrichtendiensten, Hackern oder anderen Datenpiraten aus, sondern von unzufriedenen, illoyalen Mitarbeitern. Insbesondere an Auslandsstandorten mit vielen neuen Mitarbeitern und an Standorten mit einer hohen Personalfluktuation ist Vorsicht geboten. Eine besondere Risikogruppe sind dabei die IT-Systemadministratoren, die als Superuser nicht dem Berechtigungskonzept unterliegen und direkten Zugang zu den in der Datenbank gespeicherten Informationen haben. Nicht von ungefähr war es der Systemadministrator einer externen Beratungsfirma der NSA, der die Geheimnisse des geheimsten aller amerikanischen Geheimdienste offenbarte. Einige Automobilzulieferer haben für ihre sensiblen Styling-Daten die Regel geschaffen, dass sie nur auf Anfrage eines autorisierten Projektmitglieds an andere Standorte repliziert werden.

## Achillesferse Engineering Collaboration

Besonders wichtig für die Wettbewerbsfähigkeit ist der Schutz des geistigen Eigentums während der Produktentwicklung, weil der Diebstahl oder Missbrauch von Informationen in diesem frühen Stadium dazu führen kann, dass ein Unternehmen seinen Time-to-Market-Vorsprung verliert. Und dieser Vorsprung entscheidet gerade bei schnelllebigen Konsumgütern über den Erfolg oder Misserfolg eines Produktes. In keiner Phase des Produktlebenszyklus ist das geistige Eigentum so gefährdet, weil aufgrund der Digitalisierung der Produktentwicklung immer mehr produktrelevante Daten erzeugt und anderen Abteilungen, Standorten oder sogar externen Partnern in digitaler Form bereit gestellt werden müssen, um die Folgeprozesse zu bedienen.

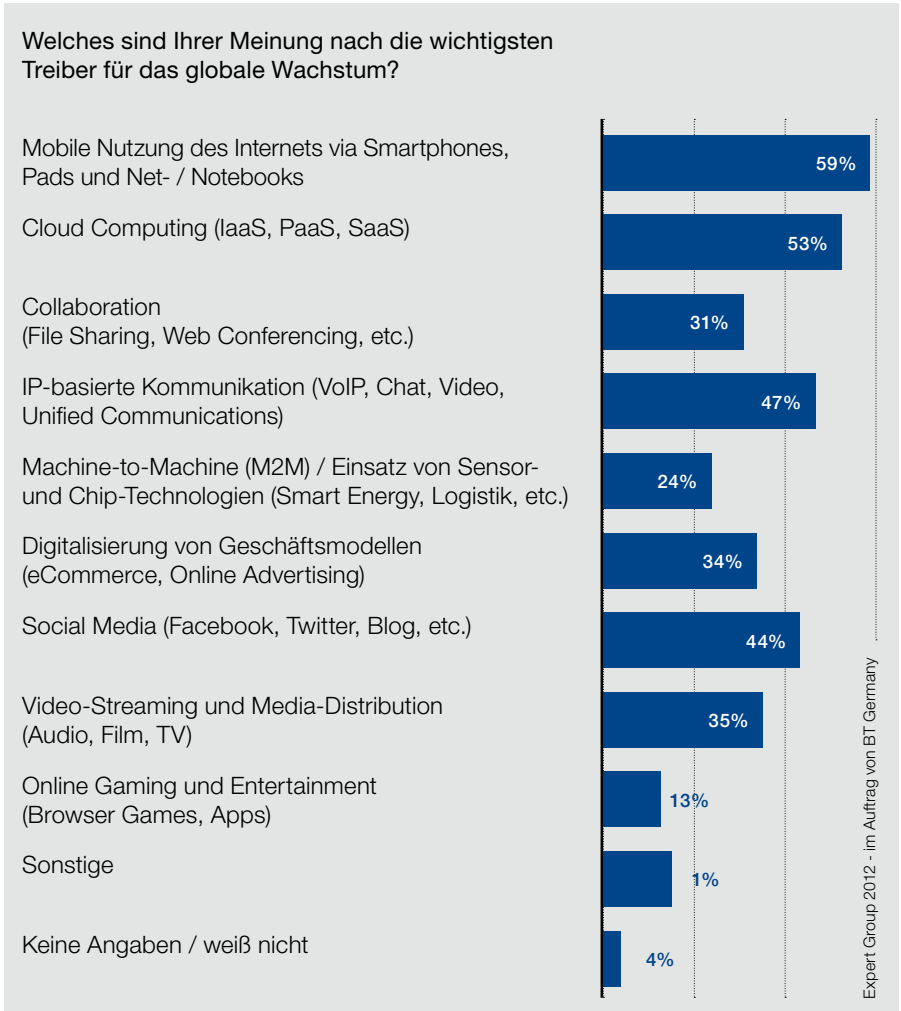
Im Zuge der digitalen Produktentwicklung fallen nicht nur immer mehr Daten an, sie enthalten auch immer mehr schützenswerte Informationen. Parametrische CAD/CAM-Systeme bieten die Möglichkeit, das in den Köpfen der erfahrenen Ingenieure steckende Konstruktions- und Fertigungs-Know-how in Form von Regeln oder intelligenten Features abzubilden, um es jüngeren Anwendern leichter zugänglich zu machen und für die Automatisierung von bestimmten Folgeprozessen zu nutzen. Dadurch stecken in den auszutauschenden CAD-Modellen zwangsläufig immer mehr Inhalte, die nicht in falsche Hände gelangen dürfen. Vielfach verlangen die Auftraggeber von ihren Zulieferern jedoch die Bereitstellung der nativen CAD-Daten, um mit ihnen effizient weiter arbeiten zu können.

Die Zusammenarbeit mit externen Partnern ist in doppelter Hinsicht eine Achillesferse für die Datensicherheit: zum einen, weil CAD-Daten und andere Dokumente über die globalen Datennetze ausgetauscht werden müssen und damit der Neugier von Nachrichtendiensten und anderen nicht zugriffsberechtigten Personen ausgesetzt sind; zum anderen, weil auch ein Missbrauch der Informationen durch Kooperationspartner, die zum Zugriff berechtigt sind, nicht immer ausgeschlossen werden kann. Die für die Datensicherheit verantwortlichen Personen müssen sich also darüber Gedanken machen, welche Daten in welchen Formaten und in welcher Informationstiefe mit welchen Partnern ausgetauscht werden sollen. Ein wichtiges Kriterium dabei ist, für welche Folgeprozesse sie benötigt werden. Gleichzeitig müssen die Verantwortlichen dafür sorgen, dass die Daten mit möglichst wenig Aufwand entsprechend diesen Regeln aufbereitet werden können.

Der Trend zum Outsourcing und die globale Collaboration haben dazu geführt, dass das Volumen an Produktdaten, das tagtäglich über die weltweiten Datennetze ausgetauscht wird, in den letzten Jahren und Jahrzehnten dramatisch zugenommen hat. Insbesondere in Branchen wie der Automobil- oder der Flugzeugindustrie verteilt sich die Produktentwicklung heute über eine lange Kette von Systemlieferanten, Entwicklungsbüros und anderen Zulieferern. Um ihre Arbeit aufeinander abstimmen zu können, müssen sie in kurzen Zeitabständen enorme Mengen an Daten und Informationen austauschen oder den anderen Partnern im Entwicklungsverbund den direkten Zugang zu ihren Datenbanken öffnen. Insbesondere für die Zulieferer ist das eine gefährliche Gratwanderung, denn manche Projektpartner können schon beim nächsten Projekt Mitbewerber sein.

## Datenexplosion durch Cloud-Computing

Neben der Collaboration trägt das Cloud-Computing dazu bei, dass die Datenmenge in den weltweiten Datennetzen explodiert und neue Sicherheitslücken auftauchen. Treiber für das globale Datenwachstum sind nach Einschätzung hochrangiger IT-Experten die mobile Internet-Kommunikation, das Cloud-Computing und die internetbasierte Kommunikation via VoIP, Video, Chat etc., wie eine von BT Germany in Auftrag gegebene Studie ergeben hat. Durch den mobilen Datenzugriff ergeben sich zusätzliche Anforderungen in puncto Datensicherheit, die beim Aufbau der IT-Architektur berücksichtigt werden müssen. Zugleich stellt sich mit der Verlagerung von Daten in die Cloud die Frage, wie sicher sie dort vor dem Zugriff von Geheimdiensten, Hackern und anderen Datenpiraten sind.




*Datenexplosion durch mobile Nutzung und Cloud Computing.*

Viele Unternehmen in Deutschland stehen der Nutzung der Cloud als Speicherort für schützenswerte Daten skeptisch gegenüber oder akzeptieren sie nur in Form einer privaten Cloud, die durch einen vertrauenswürdigen Provider betrieben werden kann. Die Tatsache, dass große amerikanische IT-Konzerne wie Amazon, Google oder Microsoft der NSA beim Ausspionieren ihrer Kunden aktiv geholfen haben oder helfen mussten, hat ihre Skepsis noch verstärkt. Nach dem US-amerikanischen Patriot Act sind Unternehmen amerikanischen Rechts und ihre ausländischen Tochtergesellschaften, aber auch nichtamerikanische Firmen mit Servern in den USA verpflichtet, den Sicherheitsbehörden den Zugang zu vertraulichen Daten zu gewähren, was im Zweifelsfall auch die Hilfsmittel zur Entschlüsselung dieser Daten einschließt. Sicherheitshalber suchen viele Unternehmen deshalb nach deutschen oder zumindest kontinentaleuropäischen Providern für ihre Cloud-basierten Dienste.

# Definition eines umfassenden Sicherheitskonzeptes

Ausgangspunkt für ein umfassendes Sicherheitskonzept ist die Analyse der Bedrohung und der möglichen Auswirkungen eines Datenverlustes oder -diebstahls: Welche Daten im Unternehmen sind besonders schützenswert und welche sind besonders gefährdet? Ausgehend von dieser Fragestellung sind zunächst einige grundsätzliche Dinge zu klären, zum Beispiel welche Daten grundsätzlich im Hause verwaltet werden sollen, welche an alle Standorte repliziert werden dürfen (z. B. Normteile) und welche nicht, welche gegebenenfalls in die Cloud gestellt werden dürfen, welche Sicherheitsanforderungen die Betreiber einer Cloud-Infrastruktur erfüllen müssen und welche Dienstleister zum Beispiel bei Datenkonvertierung und Datenaustausch Zugang zu den Daten haben dürfen etc.

## Assessment zum Informationsschutz

Um diese und andere Fragen im Zusammenhang mit Datensicherheit und Know-how-Schutz zu klären und die notwendigen Schutzmaßnahmen zu definieren, empfehlen IT-Experten ein einleitendes Assessment mit einem externen Beratungsunternehmen. Wesentliche Zielsetzung eines solchen Assessments ist neben der Abschätzung der Risiken und der Definition der Schutzziele die Sensibilisierung der beteiligten Personen und vor allem des Managements, das die Mittel für die Schutzmaßnahmen bewilligen muss. Mittel, deren Return on Investment schwer zu kalkulieren ist, weil ihr Ziel gerade darin besteht, quantifizierbaren Schaden abzuwenden.

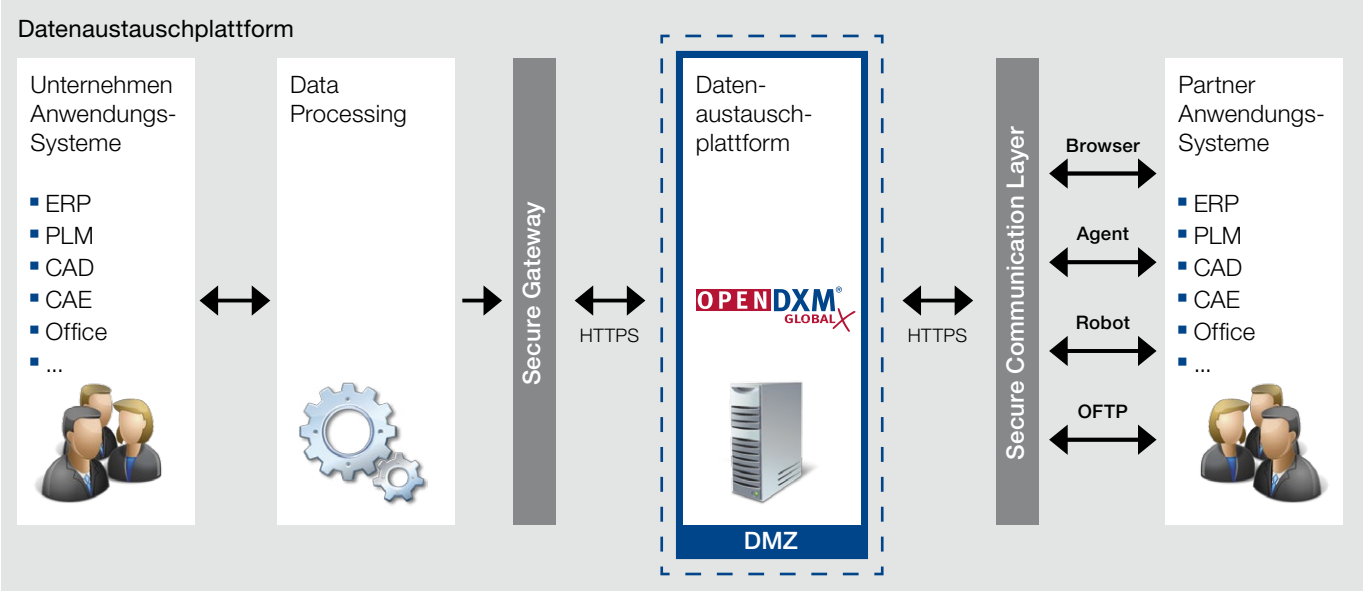
Ansatzpunkte für Schutzmaßnahmen gibt es so viele wie Gefahrenherde. Deshalb sollten im Rahmen des Assessments zunächst die Schwerpunkte des Sicherheitskonzepts festgelegt werden, bevor dann in Workshops mit Schlüsselpersonen qualitative und quantitative Schutzziele für die einzelne Anwendungsfälle erarbeitet werden. Nach der Analyse und Aufbereitung der Ergebnisse können die Berater dem Kunden klare Handlungsempfehlungen an die Hand geben und Vorschläge für das weitere Vorgehen unterbreiten.

## Umsetzung eines Sicherheitskonzeptes

Das weitere Vorgehen kann zum Beispiel darin bestehen, nach Sichtung der Wissensträger und Wissenstransferwege sowie der Typologisierung von Risikobereichen und Schutzklassen ein Grobkonzept für den Soll-Prozess zu erarbeiten. Um die Machbarkeit des Konzepts sicherzustellen und um zu prüfen, wie sich die Schutzmaßnahmen in die Unternehmensabläufe einfügen, empfiehlt sich eine Pilot-Implementierung von bestimmten Schlüsselszenarien, die mit den Anwendern durchgespielt werden können. Ausgehend davon kann dann ein Fachkonzept für die Implementierung der Abläufe und ihre Unterstützung im operativen Betrieb erarbeitet werden. Wichtig bei der Implementierung ist, dass die Anwendung der neuen Regeln zum Know-how-Schutz geschult wird und dass Mechanismen entwickelt werden, um ihre Einhaltung und Wirksamkeit nachzuverfolgen. Gegebenenfalls kann der Betrieb der Sicherheitslösung an einen externen Partner outgesourct werden.

# Grundlagen für eine sichere Datenkommunikation

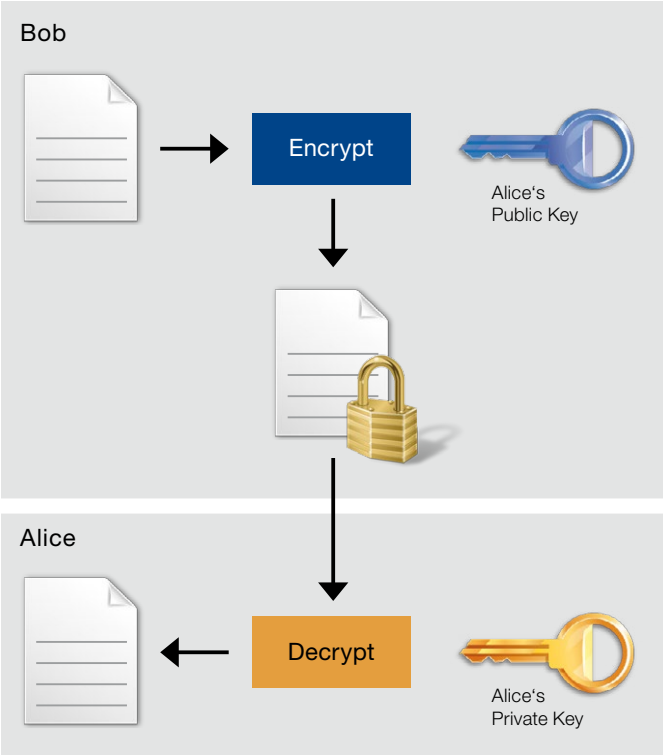
Voraussetzung für den sicheren Datenaustausch ist eine kontrollierte Datenhaltung in den Unternehmen selbst, beispielsweise durch den Einsatz einer PDM/PLM-Lösung oder eines integrierten PDM/ERP-Systems. Solange Daten noch in einem normalen Dateiverzeichnis ohne abgestufte Zugangsberechtigung verwaltet werden, lässt sich nicht mit letzter Sicherheit ausschließen, dass falsche Versionsstände oder Daten ohne entsprechende Autorisierung das Unternehmen verlassen. Wesentliche Anforderung an eine sichere Datenaustauschplattform ist deshalb, dass sie sich über entsprechende Schnittstellen nahtlos in die bestehende IT-Landschaft integrieren lässt. Dem trägt die Datenaustauschplattform OpenDXM GlobalX durch Konnektoren zu gängigen PDM/PLM- und ERP-Systemen und durch die Microsoft Outlook-Integration Rechnung.




Eine Datenaustauschplattform wird zweckmäßigerweise auf einem separaten Server in der demilitarisierten Zone (DMZ) des Unternehmens installiert, die als Projekteigner fungiert; sie kann aber auch von einem externen Provider gehostet werden. Unabhängig von der Verschlüsselung der Daten selbst sollte auch die Datenübertragung zur Plattform und zwischen Plattform und Empfänger über eine verschlüsselte https-Verbindung erfolgen. Für Unternehmen der Automobilindustrie kann es interessant sein, die Verschlüsselung mit anderen Schutzmechanismen zu kombinieren, beispielsweise dem Versand der Daten über eine sichere OFTP-Verbindung.

## Mehrstufige Verschlüsselung der Daten

Um ein Maximum an Sicherheit zu bieten, sollte die Austauschplattform ein mehrstufiges Verschlüsselungskonzept unterstützen. Idealerweise werden die auszutauschenden Daten beim Upload nach dem Public-Private-Key-Verfahren stark, z. B. mit bis zu 4.096 Bit, verschlüsselt und erst beim Download durch den Empfänger wieder entschlüsselt, so dass sie grundsätzlich verschlüsselt auf dem Server der Austauschplattform liegen. Vorteilhaft ist es darüber hinaus, jedes einzelne Dokument oder Datenpaket mit einem separaten, individuell erzeugten Schlüssel schützen zu können. Dann kann der Anwender bestimmten Dateien eine höhere Sicherheitsstufe zuweisen bzw. sie nur für einen bestimmten Zeitraum freigeben oder die Freigabe nachträglich wieder rückgängig machen.



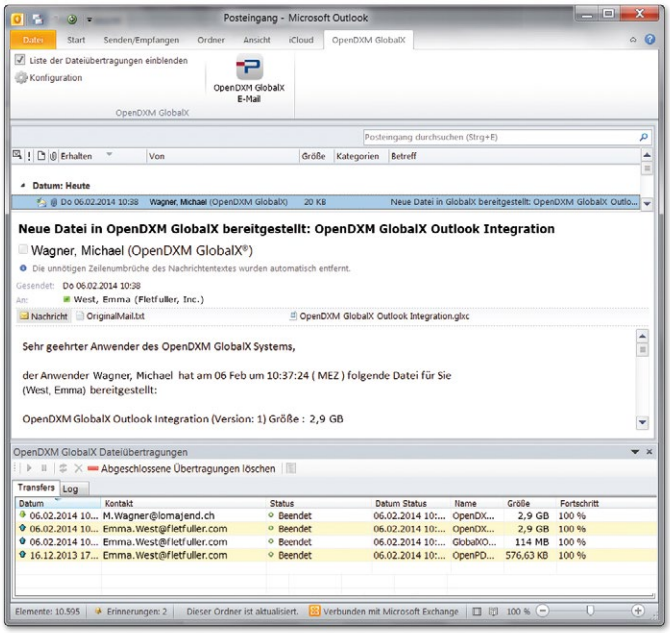

*Mehrstufige Verschlüsselung von Daten.*

Die Wahl der Verschlüsselungsstufe hat Einfluss auf die Frage, wer die ultimative Schlüsselgewalt hat. Bei der normalen Verschlüsselung verwaltet die Software die öffentlichen und die privaten Schlüssel und sorgt dafür, dass die Daten beim Download automatisch entschlüsselt werden, so dass der autorisierte Empfänger sie lesen kann. Wenn der Versender der Daten sich hingegen für die maximale Sicherheitsstufe der persönlichen Verschlüsselung entscheidet, muss der Empfänger einen privaten und nur ihm zugänglichen Schlüssel haben, um die Daten öffnen zu können. Die Austauschlösung sollte Hilfen bieten, um das gewünschte Sicherheitsniveau ad hoc definieren zu können. Voraussetzung dafür ist, dass neue Empfänger im Rahmen einer Online-Sitzung festlegen können, wo sie den privaten Schlüssel speichern möchten (z. B. auf dem eigenen Rechner, einem USB-Stick, einer Speicherkarte etc.) und mit welchem Passwortschutz.

Eine wichtige Anforderung mit Blick auf die Datensicherheit ist die Möglichkeit, die verschlüsselten Daten getrennt von den Schlüsseln auf dezentralen Servern zu verwalten. Diese Trennung minimiert nicht nur den Datenverkehr über große Entfernungen, sondern hat außerdem den Vorteil, dass man die Datenaustauschplattform mit der Schlüsselverwaltung in einem Land betreiben kann, in dem die Nachrichtendienste nicht mal eben die Herausgabe der Schlüssel verlangen können. Ohne die Schlüssel können sie mit den verschlüsselten Daten in den FileVaults (Datentresoren) nicht viel anfangen. Im Falle der persönlichen Verschlüsselung müssten sie ohnehin die einzelnen Empfänger zur Herausgabe der Schlüssel auffordern.

## Integration in die E-Mail-Prozesse

Die beste Verschlüsselung nützt nichts, wenn sie im Tagesgeschäft nicht verwendet wird. Deshalb ist es sinnvoll, den Austausch verschlüsselter Daten mit den normalen E-Mail-Prozessen zu verbinden. Die Client-Anwendung der Datenaustauschplattform sollte vollständig in die Benutzeroberfläche des E-Mail-Programms integriert sein, so dass der Anwender den Versand großer Dateien oder von Dateien mit schützenswertem Inhalt aus seiner gewohnten Arbeitsumgebung veranlassen kann. Wichtig ist, dass das Unternehmen bzw. der Systemadministrator einheitliche Regeln dafür definieren kann, welche Dateien automatisch über die Plattform versand werden sollen. Ein Kriterium ist zweifellos die Dateigröße, um die Grenzen von Outlook beim Versand großer Datenmengen zu überwinden. Es kann aber auch zweckmäßig sein, Dateien mit bestimmten Endungen oder für Empfänger in bestimmten Ländern immer verschlüsselt bereitzustellen. Neben der Möglichkeit, dem Anwender bestimmte Regeln vorzugeben, sollte er aber auch die Flexibilität haben selbst zu entscheiden, welche Daten er über die Plattform verschicken möchte.




Aus Empfängersicht muss die Datenaustauschplattform unterschiedliche Szenarien unterstützen. Unternehmen, die selbst keine entsprechende Datenaustauschlösung einsetzen, bevorzugen für den Download ein einfach zu bedienendes Webportal, das sich beim Klick auf den Link in der Benachrichtigungsmail öffnet, sodass sie nur noch ihr Passwort eingeben müssen; Unternehmen mit einer eigenen OpenDXM GlobalX Outlook-Integration wollen die Daten wie alle anderen Anhänge direkt in ihrer E-Mail-Umgebung öffnen können. Für die Akzeptanz der Lösung ist es wichtig, Daten auch an Empfänger schicken zu können, die noch nicht mit einem Profil im System hinterlegt sind. Das heißt es muss möglich sein, ad hoc einen Account mit eingeschränkten Rechten einzurichten und das möglichst automatisiert.

*Mit der OpenDXM GlobalX Outlook Integration ist der verschlüsselte Datenaustausch so einfach wie der Versand einer E-Mail.*

## Kontrollierter Datenzugriff auch von unterwegs

Um den Zugriff auf die Daten kontrollieren zu können, empfiehlt sich ein mehrstufiges Authentifizierungskonzept. Wenn Kennwort und Schlüssel nicht ausreichen, kann zusätzlich eine Chipkarte für die Authentifizierung eingesetzt werden, was software- und hardwareseitig unterstützt werden muss. Sofern der betreffende Kunde für die Anmeldung und Authentifizierung der Anwender bereits ein ADS/LDAP-System einsetzt, sollte er dieses System auch zusammen mit der Datenaustauschplattform nutzen können, um beispielsweise Single-Sign-On-Verfahren einzurichten. Die Identität des Empfängers muss mit zuverlässigen Verfahren überprüfbar sein – bevor er Zugriff auf die Daten erhält, sollte er dem Versender beispielsweise den Empfang der Daten bestätigt haben.

Neue Anforderungen ergeben sich durch die Popularität mobiler Eingabegeräte wie iPad oder iPhone, die der Anwender auch für den Zugang zur Datenaustauschplattform nutzen will. Deshalb sind entsprechende Anwendungen oder Apps erforderlich, um auf die Benutzerkonten zugreifen, Office-, PDF- und Grafikdateien herunterladen und offline betrachten zu können. Auch beim mobilen Zugriff muss die Datensicherheit jederzeit durch eine eindeutige Authentifizierung und Verschlüsselung der Daten gewährleistet sein.

## Steuerung und Protokollierung der Austauschvorgänge

In bestimmten Branchen sind die Unternehmen heute gesetzlich und/oder vertraglich verpflichtet zu dokumentieren, welche Informationen und Unterlagen wann mit welchen Partnern ausgetauscht wurden. Die Austauschplattform sollte deshalb in der Lage sein, alle Informationen zu den Austauschvorgängen revisionssicher in einer Datenbank zu speichern, so dass sie beispielsweise für Audit-Zwecke genutzt werden können. Das erleichtert den Unternehmen die Einhaltung der Compliance-Anforderungen. Die Integration der Datenaustauschplattform in die E-Mail-Anwendung bietet dabei den Vorteil, dass die Textkörper der Original-Mails zusammen mit den Informationen über die Austauschvorgänge in der Datenbank gespeichert werden können, so dass Volltextrecherchen nach Absender, Empfänger, Betreff oder nach anderen Suchkriterien möglich sind.

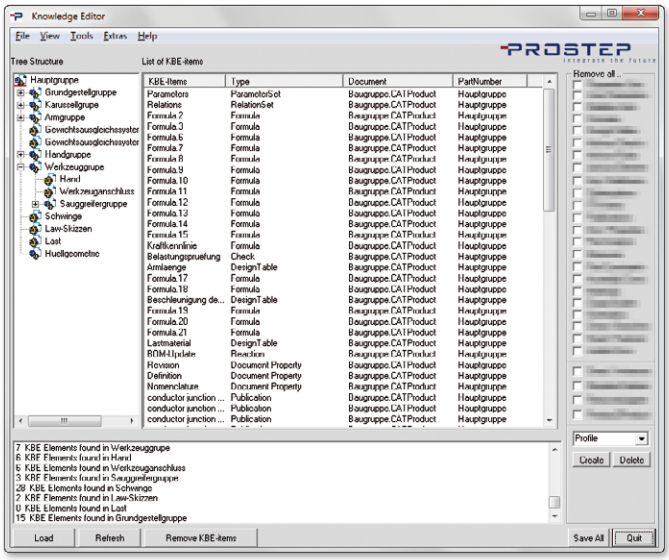
Neben der Protokollierung der Austauschvorgänge für Audits sollte die Anwendung aber auch die Steuerung des täglichen Betriebs unterstützen. Das kann beispielsweise durch eine übersichtliche grafische Oberfläche geschehen, in der alle Transfervorgänge mit Datenvolumen, Anzahl der Nutzer, Übertragungs-Threads etc. aufgelistet sind. Um einen reibungslosen Betrieb zu gewährleisten, sollte das System den Administrator darüber informieren, welche Schlüssel bald ablaufen, welche Speicherkontingente von Anwenderkonten erschöpft sind oder ähnliche Dinge. Vorteilhaft sind außerdem zeitgesteuerte Wartungsfunktionen, um beispielsweise Nutzerkonten zu sperren, Archivierungs- und Löschzeitpunkte festlegen und die Operationen automatisch ausführen zu können, was den Administrationsaufwand reduziert.

# Mehr Sicherheit durch automatische Datenaufbereitung

Mit Blick auf den Schutz des geistigen Eigentums spielt neben der Kontrolle der Austauschvorgänge die Kontrolle der auszutauschenden Informationen eine wichtige Rolle. Idealerweise sollten immer nur die Informationsumfänge bereitgestellt oder ausgetauscht werden, die für die Erledigung der jeweiligen Folgeoperationen unbedingt notwendig sind. Für viele Arbeitsschritte braucht der Empfänger keine nativen CAD-Daten - Neutralformate mit reduziertem Informationsgehalt oder sogar leichtgewichtige Viewing-Formate reichen völlig aus. Die manuelle Selektion der Informationsumfänge wäre jedoch für die Anwender viel zu umständlich und zeitaufwendig, weshalb in den Austausch bestimmte Automatismen für die Datenaufbereitung implementiert werden müssen. Die Definition dieser Automatismen erfordert eine genaue Kenntnis der unternehmensinternen und -übergreifenden Prozesse. Ein kompetentes Beratungsteam kann hier wertvolle Hilfestellung leisten.

## Verschattung von nativen CAD-Daten

Die Einbettung von immer mehr „Intelligenz“ in die Produktdaten macht eine Aufbereitung der auszutauschenden Informationsumfänge zwingend erforderlich. Falls native CAD-Daten ausgetauscht werden müssen, etwa weil der Auftraggeber das verlangt, sollten alle Elemente unterdrückt werden, die schützenswertes Konstruktions- und Fertigungs-Know-how enthalten. Das ist leichter gesagt als getan: „Intelligente“ CAD-Modelle pauschal zu verdummen, indem man diese Elemente komplett entfernt, kann nicht die Lösung sein, weil sie normalerweise als Referenz für andere Objekte dienen. Außerdem kommen die Daten im Laufe der Entwicklung oft mit Änderungen wieder zurück, die dann von Hand in die Ausgangsmodelle übernommen werden müssten.




*Die Projektsoftware Knowledge Editor unterstützt unter anderem die Analyse der CAD-Modelle auf das darin enthaltene Wissen und den Schutz des Unternehmens-Know-hows durch die Bereinigung der CAD-Modelle von Wissenselementen.*

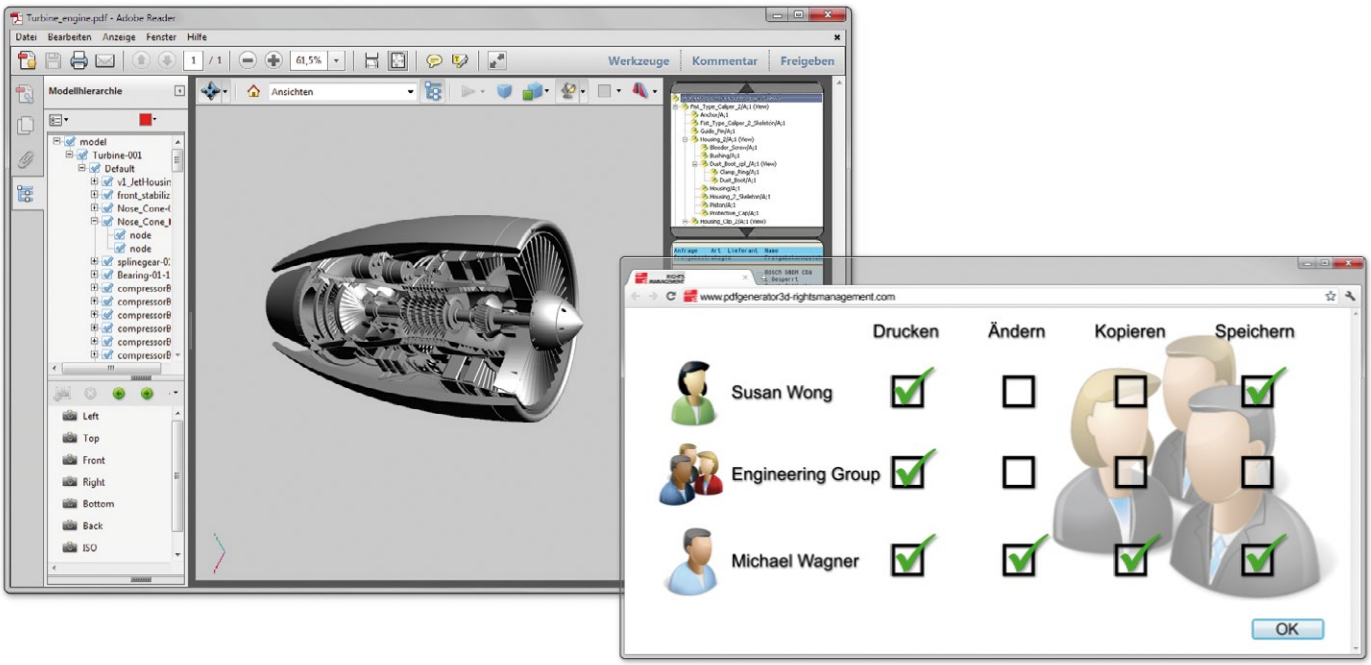
Erforderlich sind deshalb spezielle Werkzeuge wie der PROSTEP Knowledge Editor, mit dem man die Zusammenhänge und Strukturen von CAD-Modellen analysieren und bestimmte Wissensbausteine gezielt herausfiltern und verschatten kann. Um den Aufwand für die Verschattung zu minimieren, empfiehlt es sich, einmal festzulegen, welche Austauschpartner welche Informationsumfänge erhalten sollen bzw. welche Wissensbausteine nie das Haus verlassen dürfen und den Wissensfilter dann als Batchprogramm zu nutzen. Mit Hilfe entsprechender Programmerweiterungen können die Wissensbausteine auch wieder angehängt werden, wenn die ausgetauschten Modelle für Änderungen zurückkommen.

## Automatische Erzeugung von 3D-PDF-Dokumenten

Datensicherheit und Prozessdurchgängigkeit stehen in einem Spannungsverhältnis zueinander: Einerseits sollen Informationsumfänge bedarfsgerecht aufbereitet werden, andererseits sollen sie für alle nutzbar und zugänglich sein. Um diese Spannungsverhältnis aufzulösen, sind flexible Lösungen für die Aufbereitung und Verteilung von CAD- und anderen Produktdaten im Unternehmen und erweiterten Unternehmensverbund erforderlich. Sie sollten sich sowohl in die PDM/PLM- oder PDM/ERP-Lösungen als auch in die Datenaustauschplattform einbinden lassen, um Prozesse wie die Datenbereitstellung mit Hilfe intelligenter Dokumentvorlagen automatisieren zu können. Diese Anforderungen adressiert PROSTEP mit dem PDF Generator 3D.

Eine wesentliche Anforderung bei der unternehmensübergreifenden Kommunikation ist die Bereitstellung der Daten und Informationen in einem Format, das nach Möglichkeit ohne Installation von zusätzlicher Software für alle Beteiligten lesbar ist. 3D-PDF-Dokumente lassen sich mit dem kostenlosen Adobe Reader visualisieren, der praktisch auf jedem Computer-Arbeitsplatz vorhanden ist, und haben darüber hinaus den Vorteil, dass 3D- und 2D-Daten miteinander kombiniert werden können, was für viele Geschäftsprozesse erforderlich ist. Entscheidend ist natürlich, dass 3D-Modelle aus allen gängigen CAD-Systemen eingebettet und interaktiv visualisiert werden können.

Die Darstellung des Funktionsumfangs und der vielfältigen Anwendungsmöglichkeiten der 3D-PDF-Technologie ist nicht Gegenstand dieses Whitepapers (siehe hierzu das Whitepaper 3D-PDF-Technologie). Die 3D-PDF-Technologie kann allerdings einen wichtigen Beitrag zur Datensicherheit und zum Know-how-Schutz leisten. Voraussetzung dafür ist, dass sich die bereit gestellten Informationsumfänge flexibel konfigurieren und auch die weitere Verwendung dieser Informationen nach dem Versand der 3D-PDF-Dokumente noch kontrollieren lassen. Zweckmäßigerweise sollten in der Anwendung entsprechende Regeln hinterlegt werden können, um zum Beispiel festzulegen, mit welchem Detaillierungsgrad und in welcher Auflösung die CAD-Modelle konvertiert und in die 3D-PDF-Dateien eingebettet werden. Wichtig für die Datensicherheit ist auch, dass sich die Daten und Dokumente einzeln durch Passwörter oder digitale Signaturen schützen lassen, auch wenn sie der einfachen Handhabung halber in einem strukturierten PDF-Portfolio zusammengeführt werden.




Um den Zugriff auf die 3D-PDF-Dokumente benutzerspezifisch zu gestalten und die Weitergabe und Verwendung auch nach dem Versand noch kontrollieren zu können, sind abgestufte Sicherheitsmechanismen erforderlich. Dazu können bestimmte Rechte dem 3D-PDF-Dokument bei der Erstellung mitgegeben werden, die auf Empfängerseite die entsprechenden Funktionen im Adobe Reader aktivieren, zum Beispiel die Berechtigung, Schnitte durch die Modelle zu legen und Maße abzugreifen. Andere Rechte können nachträglich aktiviert oder deaktiviert werden. Im Bedarfsfall sollte man die Lösung mit einem umfassenden Digital-Rights-Management-Modul kombinieren,

um individuelle Benutzerrechte zu vergeben. Um das 3D-PDF-Dokument visualisieren, kopieren oder drucken zu können, muss der Empfänger sich mit einem Schlüssel an einem bestimmten Sicherheitsserver anmelden. Die einmal definierten Benutzerrechte können zeitlich befristet oder auch wieder entzogen werden, so dass der Eigner die volle Verfügungsgewalt über sein Dokument behält, auch wenn das Dokument sich nicht in seinem Zugriffsbereich befindet.

Automatismen sind wichtige Hilfsmittel, um unbeabsichtigte Fehler bei der Weitergabe von Daten zu vermeiden und die Datensicherheit zu erhöhen. Eine wichtige Anforderung in diesem Zusammenhang ist die Möglichkeit, einheitliche Vorlagen für die Weitergabe bestimmter Informationen zu definieren, die automatisch mit bestimmten Metadaten befüllt werden können bzw. diese Daten auch wieder in die Backend-Systeme zurückspielen. Voraussetzung dafür sind entsprechende Schnittstellen zu Backend-Systemen und die Möglichkeit, mit Hilfe von Webservices auf diese Informationen zuzugreifen.

## Automatisierung des Datenaustauschs

Eine wesentliche Anforderung aus Prozess-Sicht ist die Möglichkeit, Werkzeuge für die Aufbereitung der Daten bzw. die Ableitung von Neutralformaten in die IT-Infrastruktur einzubinden. Das kann in der Form geschehen, dass die Daten bei einem Statuswechsel automatische konvertiert und in einem Sekundärformat in der PDM/PLM-Lösung gespeichert werden oder aber dadurch, dass die Konvertierungswerkzeuge bei der Auslösung eines Datenaustauschvorgangs aufgerufen werden, um die Daten zur Laufzeit zu konvertieren. Letztere Option hat den Vorteil, dass man die bereitgestellten Informationsumfänge in Abhängigkeit von dem jeweiligen Empfänger bzw. Empfängerland dynamisch steuern kann.

Um die Konvertierung und den Austausch der Daten mit der Datenaustauschplattform steuern zu können, sind entsprechende Roboter-Funktionen erforderlich. Die Anwender brauchen nur den Empfänger und gegebenenfalls das gewünschte Zielformat auszuwählen, alle anderen Operationen erledigt die Software im Hintergrund. Sofern entsprechende Schnittstellen verfügbar sind, können die Daten auch direkt aus der PDM/PLM-Umgebung verschickt werden.

Gegebenenfalls kann es – aus Kapazitätsgründen oder weil spezielles Know-how erforderlich ist – effizienter sein, Datenkonvertierung und Qualitätssicherung an einen externen Dienstleister zu vergeben, zum Beispiel an den cloud-basierten Konvertierungsdienst OpenDESC.com. In diesem Fall muss der Dienstleister wie jeder andere Partner in den Prozess eingebunden werden, damit er die zu konvertierenden Daten über die Plattform verschlüsselt erhält und sie auch wieder verschlüsselt dort abgeben oder gegebenenfalls direkt dem endgültigen Empfänger zur Verfügung stellen kann.

# PROSTEPs Lösungsansatz: Datensicherheit Made in Germany


Die wachsenden Anforderungen in puncto Datensicherheit und Know-how-Schutz machen ein umfassendes Sicherheitskonzept erforderlich, das neben dem Datenaustausch auch die Prozesse der Datenaufbereitung und -bereitstellung berücksichtigt. Um dieses Konzept in die Praxis umsetzen zu können, benötigen Unternehmen neben ihren traditionellen Datenverwaltungssystemen innovative Lösungen für einen sicheren Datenaustausch, die idealerweise in die E-Mail-Anwendung integriert sind. Sie benötigen darüber hinaus ergänzende Lösungen für die Aufbereitung der Daten und die Ableitung von Neutralformaten, um den Umfang der bereit gestellten Informationen kontrollieren zu können. Und sie sind auf die Unterstützung eines kompetenten Software- und Systemhauses angewiesen, das sie bei der Implementierung der verschiedenen Lösungsbausteine unterstützt.

Die PROSTEP AG hat sich zum Ziel gesetzt, mit Datensicherheits-Technologie aus Deutschland weltweit Maßstäbe zu setzen. Das Angebot umfasst folgende Werkzeuge und Dienstleistungen:

- Die Datenaustauschplattform PROSTEP OpenDXM GlobalX ist weltweit bei führenden Unternehmen in Automobilindustrie und anderen Branchen im Einsatz und wird dank der OpenDXM GlobalX Outlook-Integration und der Unterstützung mobiler Endgeräte auch von Anwendern außerhalb des klassischen Engineering-Umfeldes genutzt.
- Der PROSTEP PDF Generator 3D ist eine ideale Ergänzung zur Datenaustauschplattform OpenDXM GlobalX, um Informationen für unterschiedliche Geschäftsprozesse in einem einheitlichen, für alle Beteiligten lesbaren und sicheren Format bereitzustellen.
- Der PROSTEP Knowledge Editor erlaubt die Analyse von CAD-Modellen mit dem Ziel, Wissensbausteine gezielt herauszufiltern, um das Firmen-Know-how bei der Weitergabe von Daten an Auftraggeber und Entwicklungspartner zu schützen.
- Das Beratungsteam der PROSTEP AG berät Kunden bei der Analyse möglicher Sicherheitsrisiken beim Datenaustausch und anderen Geschäftsprozessen und unterstützt sie bei der Integration der verschiedenen PROSTEP-Lösungsbausteine in ihre Unternehmensanwendungen.

PROSTEP AG
Dolivostraße 11
64293 Darmstadt
Deutschland

Telefon +49 6151 9287-0
Telefax +49 6151 9287-326

info@prostep.com
www.prostep.com

## Sie haben Anmerkungen oder Fragen?

Wir freuen uns auf Ihr Feedback an
infocenter@prostep.com


IMPRESSUM

### Herausgeber

PROSTEP AG

### Verantwortlich für den Inhalt

Joachim Christ

Edition 1, 2014