PLM IT REPORT

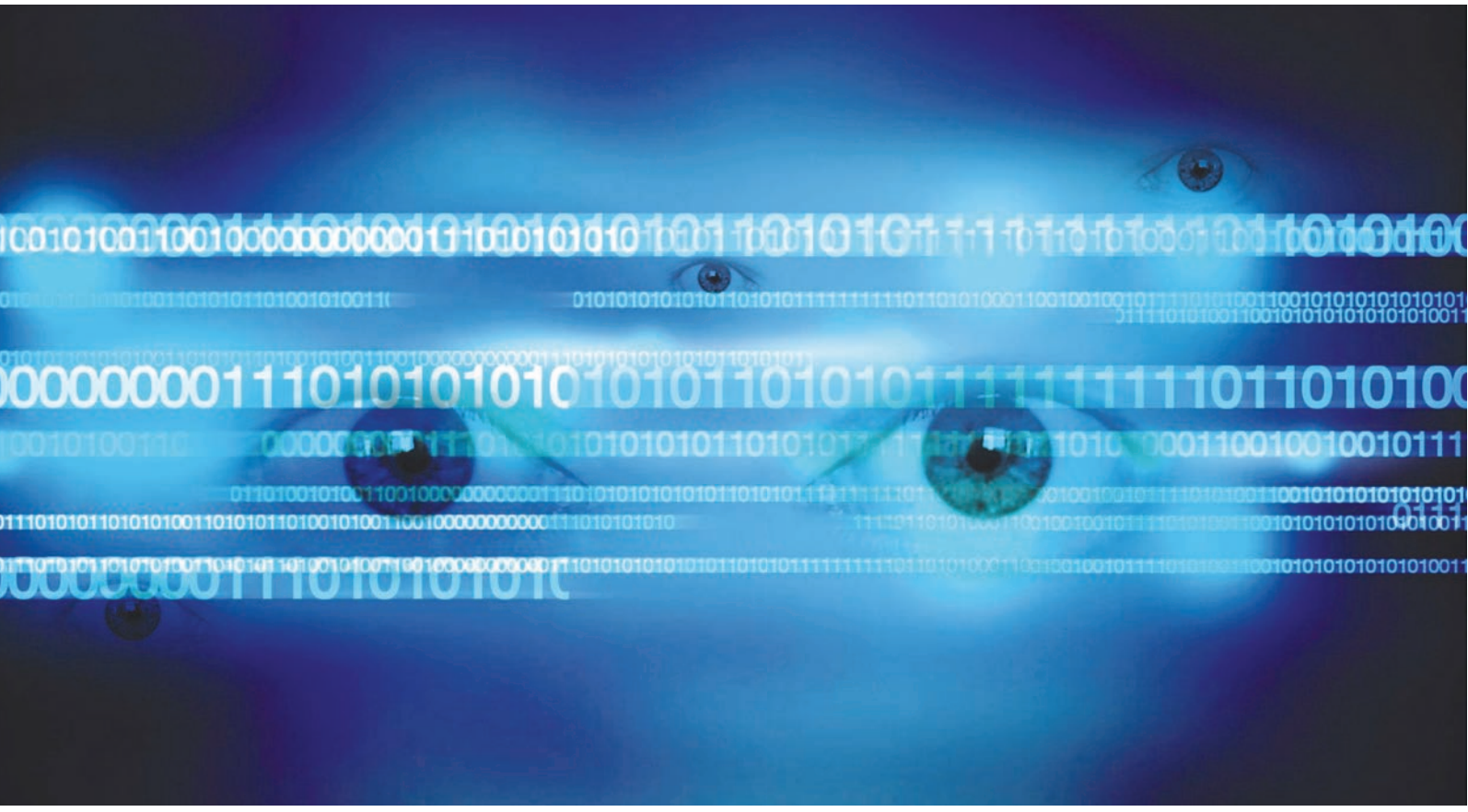
Sonderdruck aus Nr. 3 | Mai 2014 |

Produktdaten haben mehr **Schutz** verdient

www.plm-it-business.de

PROSTEP
integrate the future

Produktdaten haben mehr **Schutz** verdient

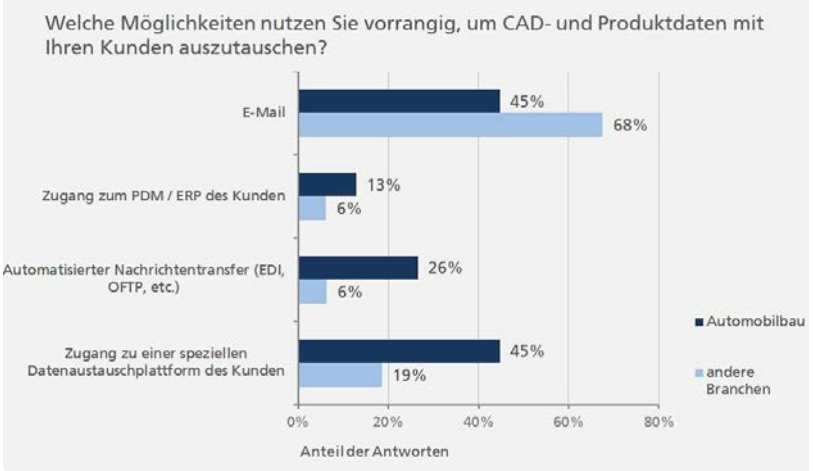


Nicht Gold, nicht Geld - die wahren Werte eines Unternehmens sind seine Daten. Sie enthalten das geistige Eigentum, das den Vorsprung im Wettbewerb ausmacht. Das haben nicht nur die Chinesen erkannt. Auch westlichen Geheimdiensten scheint jedes Mittel recht zu sein, um sich unter dem Deckmantel der Terrorismusbekämpfung Zugang zu vertraulichen Informationen zu verschaffen. Der Know-how-Schutz ist in Zeiten der globalen Zusammenarbeit zu einer echten Herausforderung geworden.

Geld und Daten haben eines gemeinsam - um sich vermehren zu können, müssen sie zirkulieren. Obwohl die Bedeutung des Know-how-Schutzes (Intellectual Property Protection oder kurz IPP) hinlänglich bekannt ist, sind die sensiblen Produktinformationen beim Datenaustausch meist schlechter geschützt als das Geld bei finanziellen Transaktionen. Die Enthüllungen des Whistleblowers Edward Snowden haben deutlich gemacht, wie leicht Daten auf ihrem Transportweg durch die weltweiten Datennetze abgegriffen werden können und wie einfach wir es den Datenspionen machen, indem wir sie ohne jegliche Schutzmechanismen austauschen. Eine Einladung zur Industriespionage.

Ungeachtet aller Sicherheitsbedenken und der in vielen Unternehmen existierenden Datenschutzbestimmungen werden immer noch erschreckend viele Produktdaten per E-Mail

versandt. Das belegt eine vom Fraunhofer IPK zusammen mit dem PLM-Hersteller Contact Software und dem VDI durchgeführte Studie, an der über 1.400 Ingenieure aus den unterschiedlichsten Branchen teilnahmen. Selbst in der Automobilindustrie mit ihren hohen Anforderungen in puncto Know-how-Schutz gaben 45 Prozent der Befragten an, CAD- und Produktdaten mit Kunden und Zulieferern per E-Mail auszutauschen. Das heißt ohne jede Verschlüsselung. Die in den Mailprogrammen enthaltenen Verschlüsselungsmechanismen erfassen nämlich nur den Mail-Body, nicht aber die Dateianhänge.



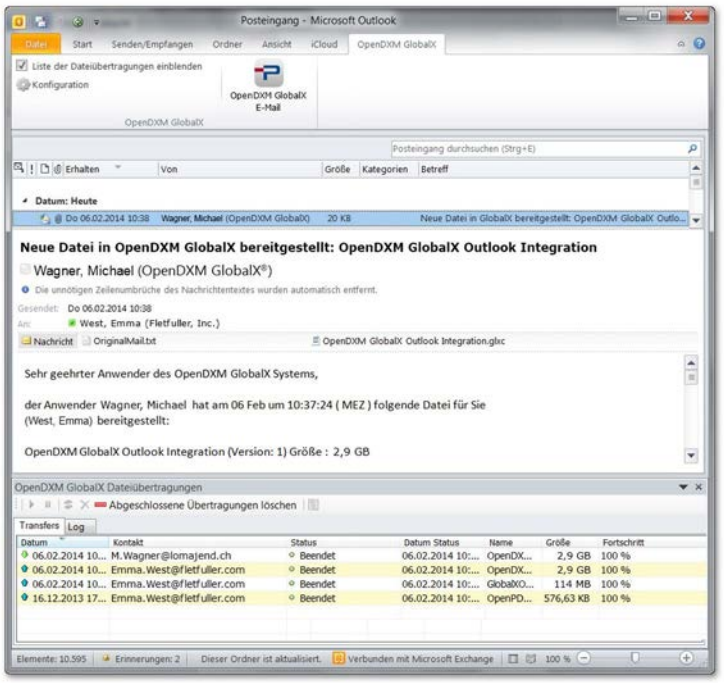
Aus der Studie „Kollaborative Produktentwicklung und digitale Werkzeuge. Defizite heute – Potenziale morgen" von Contact Software, Fraunhofer IPK und VDI.

Sicherer Datenaustausch per E-Mail

Dabei ginge es auch anders, zum Beispiel mit einer vollständig in Outlook integrierten beziehungsweise integrierbaren Datenaustauschlösung wie OpenDXM GlobalX. Der Anwender verschickt seine Daten zwar mit dem gewohnten E-Mail-Programm, aber die Dateianhänge einer bestimmten Größe, mit bestimmten Endungen und/oder an Adressaten in bestimmten Ländern werden automatisch über eine Austauschplattform umgeleitet und dort verschlüsselt zum Download bereitgestellt. Die Regeln dafür legt das betreffende Unternehmen fest und hinterlegt sie zusammen mit den Verschlüsselungsmechanismen auf einem zentralen Server, der im Bedarfsfall auch weitere Verarbeitungsprozesse wie den Virencheck oder die Konvertierung übernehmen kann.

Die auszutauschenden Daten werden beim Upload nach dem Public-Private-Key-Verfahren mit bis zu 4.096 Bit verschlüsselt, was ein hohes Maß an Sicherheit gewährleistet. Im Unterschied zu dem vermeintlich sicheren SSL-Verfahren für die Datenübertragung zu Webservern, das relativ leicht geknackt werden kann. Presseberichten zufolge haben die NSA und der britische Geheimdienst GCHQ ein ganzes Arsenal an Maßnahmen und Techniken entwickelt, um die Verschlüsselung von SSL-Verbindungen oder Virtual Private Networks (VPN) auszuhebeln und die noch unverschlüsselten oder schon wieder entschlüsselten Daten abzugreifen. Die Verschlüsselung lässt sich flexibel mit anderen Schutzmechanismen kombinieren, beispielsweise dem Versand der Daten über eine sichere OFTP-Verbindung, was besonders für die Unternehmen in der Automobilindustrie interessant ist. Außerdem kann der Anwender einzelnen Dateien eine höhere Sicherheitsstufe zuweisen beziehungsweise sie nur für einen bestimmten Zeitraum freigeben oder die Freigabe nachträglich wieder rückgängig machen.

Die Austauschplattform unterstützt verschiedene Verschlüsselungsstufen. Bei der normalen Verschlüsselung verwaltet die Software die öffentlichen und die privaten Schlüssel und sorgt dafür, dass die Daten während des Downloads beim Empfänger automatisch entschlüsselt werden, so dass der autorisierte Empfänger sie lesen kann. Wenn der Versender der Daten sich 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 erlaubt es, nicht nur neue Austauschpartner, sondern auch das gewünschte Sicherheitsniveau ad hoc zu definieren. Im Falle einer persönlichen Verschlüsselung fordert ein Software-Assistent den Empfänger auf, im Rahmen einer Online-Sitzung einen Speicherort für den privaten Schlüssel festzulegen und mit einem separaten Passwort zu schützen.



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

Entscheidend ist der Schlüsselbund

Die Frage, wo die Schlüssel liegen, ist alles andere als trivial. Mehr noch als das undifferenzierte Absaugen von Daten am transatlantischen Glasfaserkabel hat die europäischen Unternehmen aufgeschreckt, dass große amerikanischen IT-Konzerne wie Amazon, Google oder Microsoft der NSA beim Ausspionieren ihrer Kunden aktiv geholfen haben oder helfen mussten. Nach dem USA 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. Aufgrund der Geheimniskrämerei der amerikanischen Geheimdienste weiß niemand so genau, ob sie die Daten wirklich nur nachrichtendienstlich oder nicht doch auch wirtschaftsdienlich auswerten.

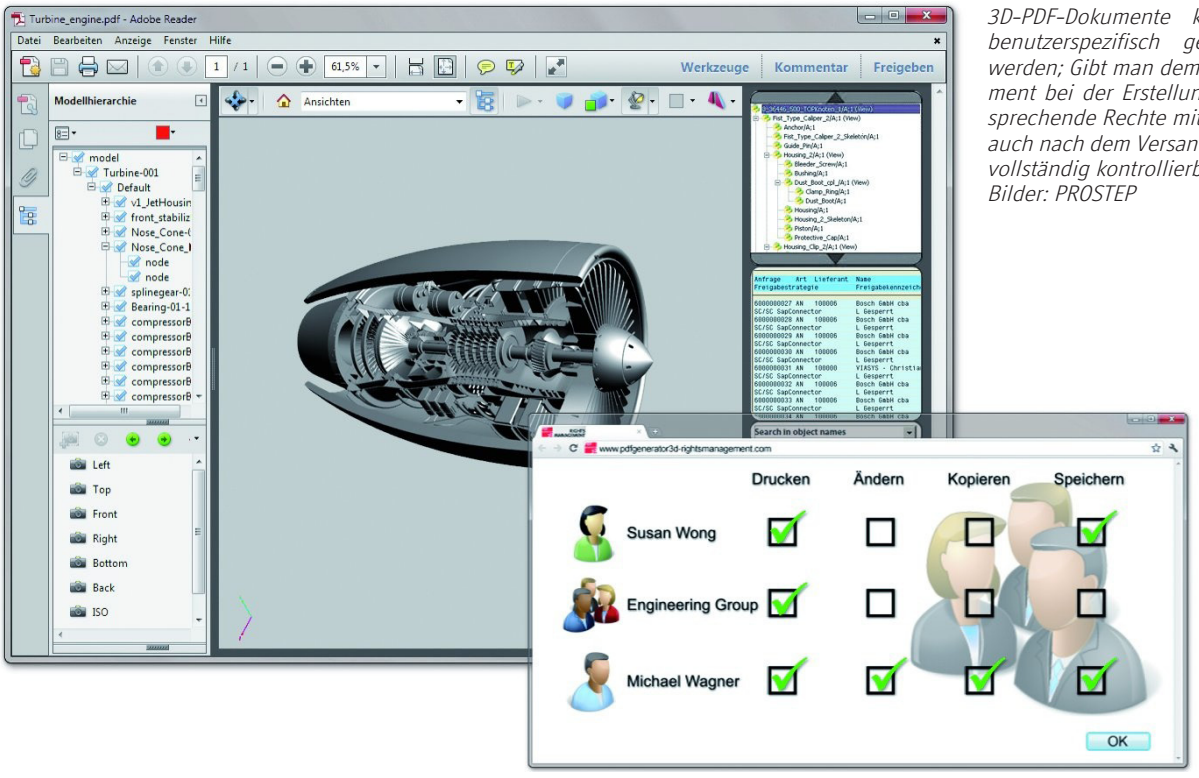
Das Kuriose an der Sache ist, dass das US-Gesetz nicht neu ist - es wurde kurz nach den Terroranschlägen auf das World Trade Center am 11. September 2001 verabschiedet. Seine dramatischen Auswirkungen sind jedoch erst durch die Enthüllungen über Machenschaften von NSA und Co. richtig deutlich geworden. Ein Dolchstoß für amerikanische Anbieter von Cloud-basierten Lösungen. Seitdem können sich die Telekom und andere Provider nicht vor Anfragen von Firmen retten, die ihre Datenwolken gerne nach Europa verschieben möchten, wo wesentlich strengere Datenschutzrichtlinien gelten. Konkret die Richtlinie 95/46EG, die allerdings nach einem Urteil des Europäischen Gerichtshofs in Deutschland nicht korrekt umgesetzt wurde.

Entscheidend für den Know-how-Schutz ist aber nicht, wo die verschlüsselten Daten liegen, sondern ob die langen Finger der neugierigen Nachrichtenagenturen und anderer Datenspione an den Schlüsselbund heranreichen. Um den Datenverkehr über große Entfernungen zu optimieren, können die Daten auf lokalen Servern in den USA oder anderswo abgelegt sein beziehungsweise an sie repliziert werden - sie sind ja zu jedem Zeitpunkt verschlüsselt. Um sie öffnen zu können, muss der Empfänger sich jedoch am zentralen Datenaustauschserver anmelden, der zweckmäßigerweise in einem Land mit strengeren Datenschutzrichtlinien steht, in dem die Geheimdienste nicht mal eben die Herausgabe der Schlüssel verlangen können. Wenn die Daten darüber hinaus persönlich verschlüsselt werden, müssten sie zusätzlich den privaten Schlüssel der Empfänger auftreiben.

Schutz auch hinter der Firewall

Es reicht allerdings nicht aus, die Gefahren für die Datensicherheit immer nur bei den Hackern und Produktpiraten vor der Firewall zu suchen. Der Fall Snowden hat auch gezeigt, dass der größte Risikofaktor für die Datensicherheit der Mensch beziehungsweise der eigene Mitarbeiter sein kann, was die Mitarbeiter von Partnerfirmen einschließt. Es war schließlich der Systemadministrator einer externen Beratungsfirma der NSA, der die Geheimnisse des geheimsten aller amerikanischen Geheimdienste offenbarte. Der Schutz des geistigen Eigentums kann sich deshalb nicht allein auf den Datenaustausch beschränken, sondern muss beim Umgang mit den sensiblen Daten im Unternehmen und im erweiterten Unternehmensverbund ansetzen.

Unternehmen mit global verteilten Entwicklungsstandorten müssen sich heute darüber Gedanken machen, welche Projektdaten an welchen Standorten benötigt werden und im Zweifelsfalle auch nur diese Daten bereitstellen. In den aufstrebenden Ländern Asiens ist die Personalfluktuation höher, so dass man nicht immer auf die Loyalität der Mitarbeiter bauen kann. Um genau steuern zu können, welche Mitarbeiter an welchen Standorten beziehungsweise von welchen Partnerfirmen auf welche Daten zugreifen dürfen, ist ein



3D-PDF-Dokumente können benutzerspezifisch gestaltet werden; Gibt man dem Dokument bei der Erstellung entsprechende Rechte mit, ist es auch nach dem Versand noch vollständig kontrollierbar. Bilder: PROSTEP

ausgefeiltes Rollen- und Rechtemanagement mit einer mehrstufigen Authentifizierung der Benutzer erforderlich. Die Kombination vorhandener ADS/LDAP-System mit der Datenaustauschlösung reduziert den Aufwand für die Definition der Benutzerrechte und ermöglicht die Authentifizierung im Single-Sign-On-Verfahren.

Eine große Gefahr für die Datenintegrität lauert in den globalen Entwicklungsnetzen der Automobil- oder der Flugzeugindustrie, deren Zusammensetzung sich oft von Projekt zu Projekt ändert. Um ihre Arbeit aufeinander abstimmen zu können, müssen die Partner große Mengen an Daten und Informationen austauschen. Damit steigt die Gefahr, dass Daten in die falschen Hände gelangen. Die Unternehmen benötigen deshalb Werkzeuge, mit denen sie auch die Informationstiefe der bereitgestellten Daten beeinflussen können.

Der Einsatz von „intelligenten" Entwicklungswerkzeugen hat dazu geführt, dass in den CAD-Modellen sehr viel Konstruktions- und Fertigungs-Know-how steckt. Die Lösung kann nicht darin bestehen, sie pauschal zu „verdummen"; vielmehr müssen die Austauschpartner in der Lage sein, bestimmte Informationen gezielt und abgestuft zu unterdrücken, je nachdem für welchen Empfänger die Daten bestimmt sind beziehungsweise für welche Prozesse sie benötigt werden. Für die Abstimmung reicht in der Regel die Konvertierung der Daten in ein leichtgewichtiges Neutralformat wie 3D-PDF aus. Serverlösungen wie der PROSTEP PDF Generator 3D können dies dann vollautomatisiert und mit umfangreichen Schutzfunktionen. Um die Daten dann wieder in Folgeprozessen nutzen zu können, sind vielfach die nativen Daten erforderlich, die dann entsprechend verschattet werden müssen.

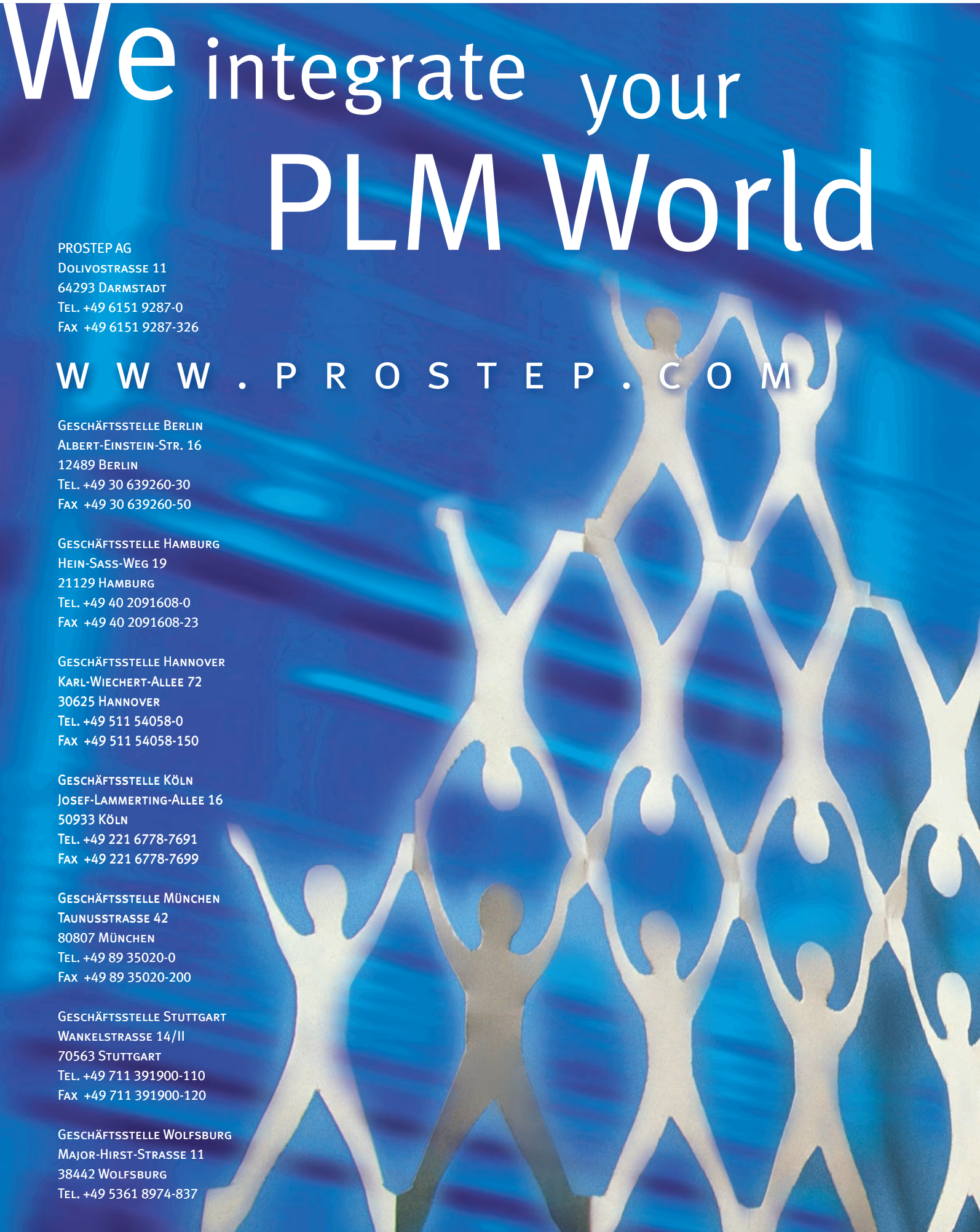
Bei den Datenmengen, die heute in den Entwicklungsnetzen der Automobil- oder der Luftfahrtindustrie bewegt werden, kann die Auswahl der auszutauschenden Informationsumfänge und die Aufbereitung der Daten nicht mehr von Hand erfolgen. Entscheidend für die Datensicherheit ist deshalb, dass sich die Werkzeuge für die Konvertierung oder Verschattung der Daten vollständig in die Datenaustauschprozesse integrieren lassen. Nur so lassen sich die Verarbeitungsprozesse automatisieren und Fehler der Anwender bei der Auswahl der auszutauschenden Informationsumfänge vermeiden. Mit anderen Worten: Maximaler Datenschutz erfordert die Kombination unterschiedlicher Technologien und ein umfassendes Paket von Maßnahmen, das nicht nur die äußeren Gefahren berücksichtigt. -sg-

Michael Wendenburg, Sevilla
(www.wendenburg.net)

PROSTEP AG, Darmstadt,
Telefon +49 6151 9287-0,
www.prostep.com

PROSTEP
integrate the future

We integrate your PLM World



PROSTEP AG
Dolivostrasse 11
64293 Darmstadt
Tel. +49 6151 9287-0
Fax +49 6151 9287-326

WWW.PROSTEP.COM

Geschäftsstelle Berlin
Albert-Einstein-Str. 16
12489 Berlin
Tel. +49 30 639260-30
Fax +49 30 639260-50

Geschäftsstelle Hamburg
Hein-Sass-Weg 19
21129 Hamburg
Tel. +49 40 2091608-0
Fax +49 40 2091608-23

Geschäftsstelle Hannover
Karl-Wiechert-Allee 72
30625 Hannover
Tel. +49 511 54058-0
Fax +49 511 54058-150

Geschäftsstelle Köln
Josef-Lammerting-Allee 16
50933 Köln
Tel. +49 221 6778-7691
Fax +49 221 6778-7699

Geschäftsstelle München
Taunusstrasse 42
80807 München
Tel. +49 89 35020-0
Fax +49 89 35020-200

Geschäftsstelle Stuttgart
Wankelstrasse 14/II
70563 Stuttgart
Tel. +49 711 391900-110
Fax +49 711 391900-120

Geschäftsstelle Wolfsburg
Major-Hirst-Strasse 11
38442 Wolfsburg
Tel. +49 5361 8974-837