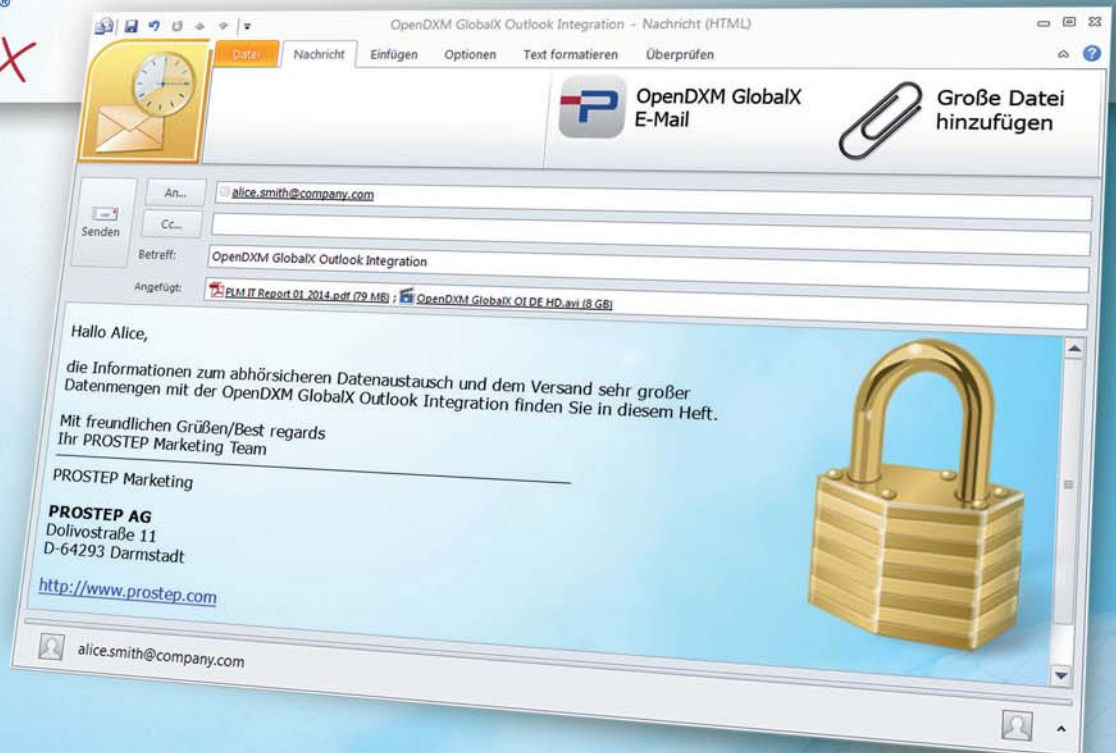


PLM IT REPORT

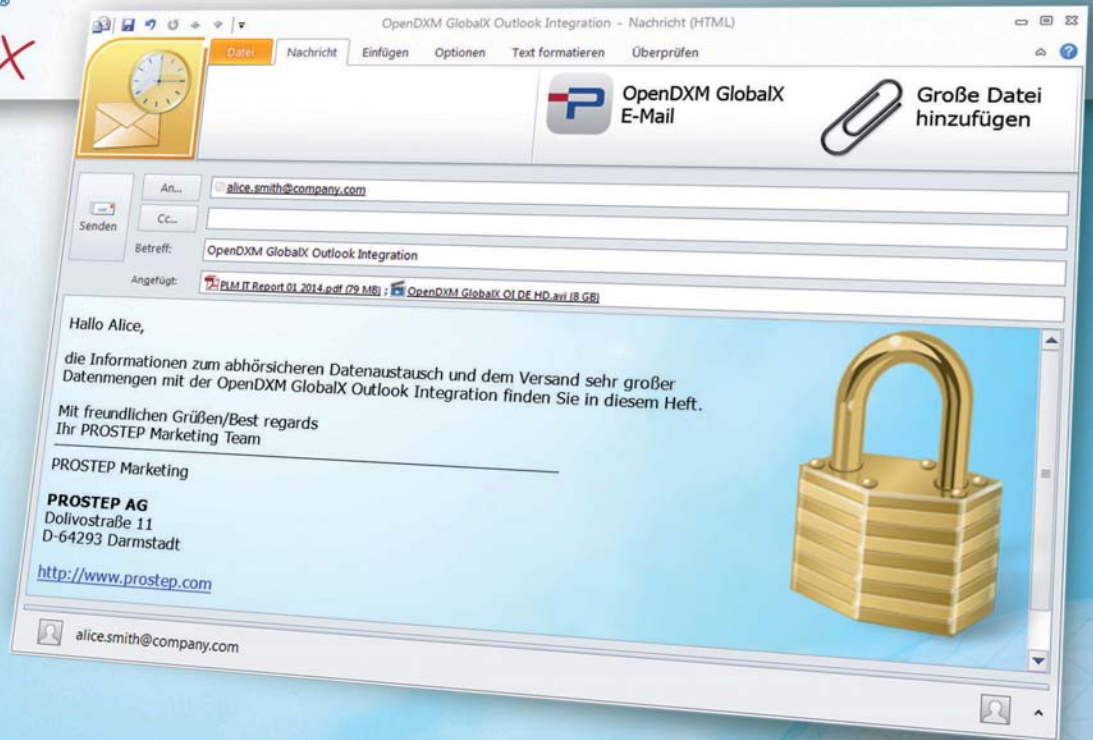
Sonderdruck aus Nr. 1 | Januar 2014 |

OPENDXM[®]
GLOBALX



Mit Sicherheit Kommunizieren

Mit Sicherheit Kommunizieren



*Einfach aber sicher:
Mit OpenDXM GlobalX von PROSTEP ist
der verschlüsselte Datenaustausch so
einfach wie der Versand einer E-Mail.*

Der Fall Edward Snowden hat uns zwei Dinge vor Augen geführt: Erstens, wie nachlässig wir mit vertraulichen Informationen umgehen und, zweitens, wie schamlos neugierige Spionagedienste das ausnutzen. Ob sie die abgelaugten Informationen wirklich nur nachrichtendienstlich oder auch wirtschaftlich auswerten, sei dahin gestellt. Fest steht, dass die E-Mail-Verschlüsselung allein nicht ausreicht, um das Know-how von Unternehmen zu schützen – hier sind in E-Mail-Programme integrierte Schutzmechanismen notwendig.

Hand aufs Herz – verschlüsseln Sie Ihre E-Mails? Wenn nicht, befinden Sie sich in guter Gesellschaft. Rund 144 Milliarden E-Mails werden jeden Tag um den Globus geschickt (1), von denen schätzungsweise nicht mehr als drei Prozent verschlüsselt sind. Ein gefundenes Fressen für Datendiebe. Der Grund ist schlicht und einfach der, dass die Einrichtung der Verschlüsselung den meisten Anwendern viel zu kompliziert ist. Anders ist die Vielzahl an Internet-Seiten zum Thema „E-Mail-Verschlüsselung leicht gemacht“ nicht zu erklären. Wenn der Anteil verschlüsselter E-Mails dennoch steigt, dann deshalb, weil paradoxerweise immer mehr Spam-Nachrichten verschlüsselt werden. Der Spam-Anteil am weltweiten E-Mail-Verkehr liegt laut Pingdom inzwischen bei 68,8 Prozent.

Viele Anwender werden sich nach den jüngsten Skandalen zu Recht fragen, ob sich der Aufwand für die Verschlüsselung überhaupt lohnt. Einem Bericht des Guardian zufolge hat sich ausgerechnet Microsoft als „Bock mit Gärterschürze“ entpuppt und der NSA, Amerikas geheimstem aller Geheimdienste, dabei geholfen, die Verschlüsselung von Daten durch Nutzer seiner Dienste auszuhebeln (2). Als ob MS Outlook nicht schon genug Sicherheitslücken (gehabt) hätte – vor einigen Jahren sah sich sogar das deutsche Bundesamt für Sicherheit genötigt, vor der Nutzung der Mailprogramme des amerikanischen Softwaregiganten zu warnen (3). Der Popularität von MS Outlook hat das nicht geschadet.

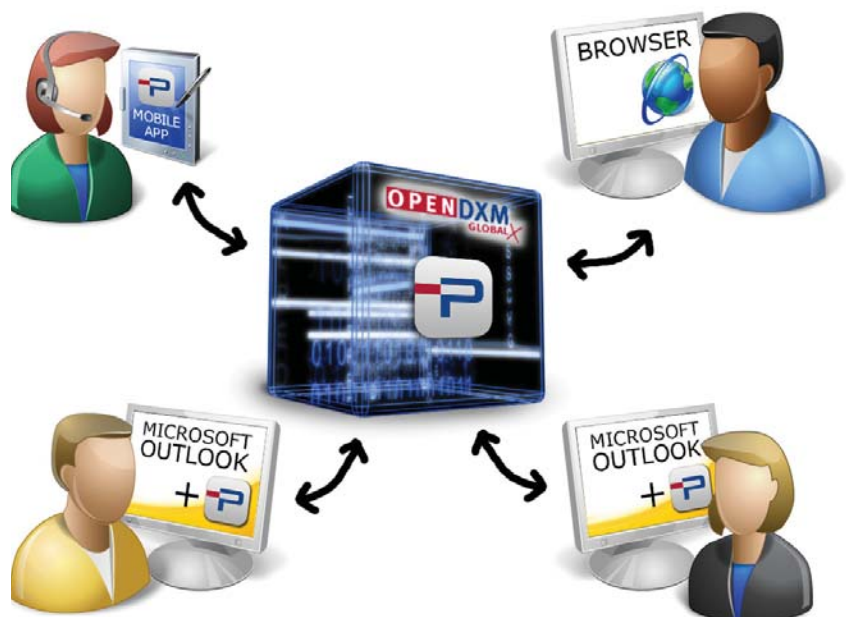
Ungeachtet aller Sicherheitsbedenken sind Outlook und Co. aus unserem Arbeitsleben nicht mehr wegzudenken. Sogar Ingenieure, die eigentlich kreativeren Arbeiten nachgehen sollten, verbringen einer vom Fraunhofer IPK zusammen mit Contact Software und VDI durchgeführten Studie zufolge mehr Zeit mit der Kommunikation und Koordination von Entwicklungsprojekten als mit ihren Kernaufgaben (4). Ihr wichtigstes IT-Werkzeug ist deshalb nicht das CAD-System, sondern das E-Mail-Programm, das viele von ihnen trotz strenger Sicherheitsauflagen in den Unternehmen auch immer noch für den Austausch von sensiblen Informationen wie etwa CAD- und Produktdaten, aber auch Unternehmenskennzahlen nutzen.

Einfache Lösung gefragt

Was viele Anwender vielleicht nicht wissen ist, dass selbst die Verschlüsselung der E-Mails ihr intellektuelles Eigentum nicht aus-

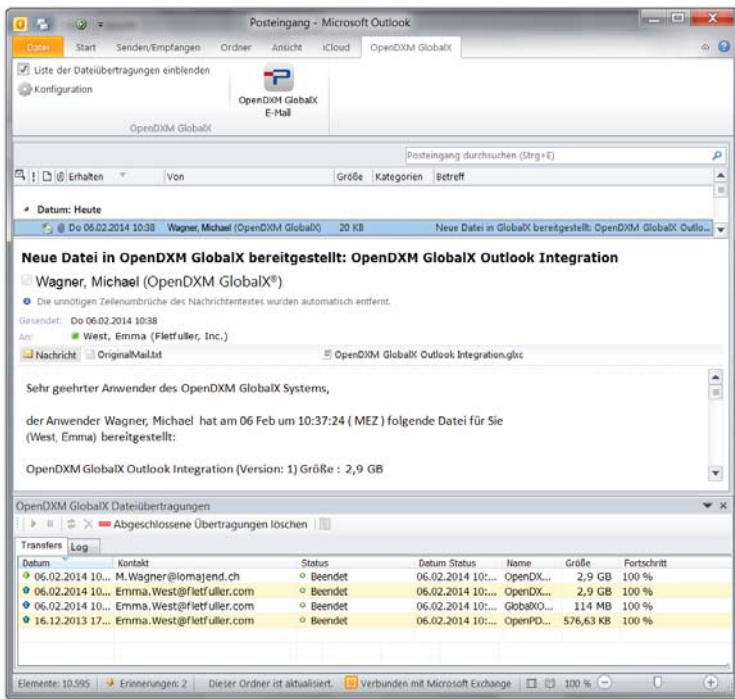
reichend schützt. Die in den Mailprogrammen enthaltenen Verschlüsselungsmechanismen erfassen normalerweise nur den Mail-Body, nicht aber die Anhänge, die oft die geheim zu haltenden Informationen enthalten. Das gilt nicht nur für CAD-Daten, in denen schützenswertes Konstruktions-Know-how steckt, sondern auch für sensible Simulationsdaten (z.B. von Crashtests) oder autorenrechtlich geschützte Grafik-, Bild-, Musik- und Videodateien. Oft erreichen diese Dateien eine Größe, die jedes Mailprogramm in die Knie zwingt, das heißt sie lassen sich entweder überhaupt nicht als Anhang verschicken oder nur verteilt auf mehrere Mails.

Man fragt sich, warum selbst in größeren Unternehmen immer noch so viele Daten ohne jegliche Sicherheitsvorkehrungen ausgetauscht werden? Vermutlich, weil es meistens schnell gehen muss und alle anderen Mechanismen aufwendiger zu handhaben sind als das E-Mailprogramm, das jeder von uns im (Halb-)Schlaf bedienen kann. Eine wesentliche Anforderung an eine sichere Datenaustauschlösung ist deshalb, dass sie für den Endanwender genau so einfach zu bedienen ist wie sein E-Mail-Programm. Oder besser noch, dass sie sich wie das E-Mailprogramm bedienen lässt. Das ist der Anspruch, dem die PROSTEP AG mit der neuen OpenDXM GlobalX Outlook Integration gerecht werden möchte.



OpenDXM GlobalX erlaubt eine flexible Nutzung – aber immer hochsicher.
Alle Bilder: PROSTEP AG

Vollständig in MS Outlook integriert



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

Aus Anwendersicht ist der Datenaustausch-Client vollständig in die Outlook-Benutzeroberfläche integriert. Einziger Unterschied sind zwei zusätzliche Tasten, eine für den Versand von großen Dateien und die andere, um den Versand von Dateien jeglicher Größe über OpenDXM GlobalX zu erzwingen. Die erste Funktion ist eigentlich überflüssig, weil im Regelwerk der Datenaustauschplattform hinterlegt ist, dass Daten ab einer bestimmten Größe automatisch über OpenDXM GlobalX ausgetauscht werden. Das Problem ist nur, dass Outlook über die Standardfunktion „Datei anhängen“ Minuten braucht, um überhaupt festzustellen, dass eine mehrere Gigabyte große Datei viel zu groß für den normalen E-Mail-Versand ist. Mit der Funktion „große Datei versenden“ kann der Anwender diese Grenze direkt überwinden.

Mit der OpenDXM GlobalX Outlook Integration können aber nicht nur Dateien ab einer bestimmten Größe automatisch über die Datenaustauschplattform „umgeleitet“ werden. Der Systemadministrator kann mit wenig Aufwand beliebige Regeln definieren, zum Beispiel, dass Dateien mit einer bestimmten Endung grundsätzlich über OpenDXM GlobalX, das heißt verschlüsselt verschickt werden. Oder Dateien an Empfänger in Ländern, die es mit dem Know-how-Schutz nicht so genau nehmen. Zusätzlich

hat der Anwender dank der zweiten Funktionstaste die Möglichkeit, beliebige Dateien an beliebige Anwender über OpenDXM GlobalX zu versenden, auch wenn keine der spezifizierten Regeln automatisch greift.

Aktivierung von spontanen Empfängern

Aus Empfängersicht gestaltet sich der Download der Daten unterschiedlich, je nachdem ob er ebenfalls die OpenDXM GlobalX Outlook Integration einsetzt oder nicht. In beiden Fällen erhält er eine Benachrichtigung, dass Daten für ihn bereitstehen. Diese Benachrichtigung kann den Body der ursprünglichen Mail enthalten oder nicht – je nachdem wie das betreffende Unternehmen die Lösung konfiguriert hat. Wenn der Empfänger keine Outlook-Integration einsetzt, muss er sich für den Download mit seinem Passwort am OpenDXM GlobalX-Portal anmelden, das sich beim Klicken auf den Link in der Nachricht automatisch öffnet. Arbeitet er ebenfalls mit der OpenDXM GlobalX Outlook Integration, ist der Download noch einfacher – er braucht nur den Dateianhang in der OpenDXM GlobalX-Benachrichtigung anzuklicken und kann dann die Datei wie gewohnt mit Outlook herunterladen und speichern. Eine zusätzliche Authentisierung am OpenDXM GlobalX-Portal ist in diesem Falle nicht notwendig.

Eine interessante Frage ist, was passiert, wenn der Anwender Dateien an einen Empfänger verschickt, der der OpenDXM GlobalX-Datenbank noch nicht bekannt ist. Für diese spontanen oder Ad-hoc-Austauschprozesse kann jedes Unternehmen eine einheitliche Vorlage definieren, die für den Empfänger automatisch einen zeitlich limitierten Account, eventuell mit eingeschränkten Nutzerrechten erzeugt. Der Empfänger erhält in diesem Fall neben der Benachrichtigung über die zum Download bereitstehenden Daten zwei weitere E-Mails, eine mit seiner User ID und eine zweite mit einem zeitlich begrenzten Aktivierungslink, die ihn auffordert, ein Passwort für den Zugang anzulegen.

Die Lösung ist so flexibel, dass es sogar möglich ist, persönliche Verschlüsselungen mit einem Public und einem Private Key ad hoc zu definieren. In diesem Fall werden die Dateien mit dem öffentlichen Schlüssel des Empfängers verschlüsselt. Den privaten Schlüssel, um sie zu entschlüsseln, besitzt einzig und allein der Empfänger. Im Rahmen einer Online-Session wird er durch einen



Höchste Datensicherheit auch beim Datenaustausch mit Outlook.

entsprechenden Assistenten unterstützt, um den Private Key zu erzeugen. Das Applet fordert ihn auf, einen so genannten Key Store zu definieren und den Speicherort für den privaten Schlüssel festzulegen, zum Beispiel auf einem USB-Stick, sowie den Zugriff auf den Key Store noch einmal mit einem separaten Passwort zu schützen. Die persönliche Verschlüsselung mit bis zu 4.096 Bit bietet ein Höchstmaß an Datensicherheit.

Sichere Datenaustauschplattform

OpenDXM GlobalX ist eine sehr sichere Datenaustauschplattform, die normalerweise von der Firma eingerichtet wird, die Eigner der Collaboration-Projekte ist; sie kann aber auch von PROSTEP AG oder einem anderen Provider gehostet werden. Installiert wird sie normalerweise in der so genannten demilitarisierten Zone, also zwischen internen und externen Firewalls des betreffenden Unternehmens auf einem zentralen Server, auf den nur Systemadministratoren Zugriff haben, um die Profile der Austauschpartner und die Regeln für den Datenaustausch zu definieren. Außerdem sind die Verschlüsselungsmechanismen auf dem Server hinterlegt, der auch mögliche Verarbeitungsprozesse, wie beispielsweise Viren-Checks, Weiterleiten von Daten an Back-End Systeme oder Konvertierung übernimmt.

Die zu jedem Zeitpunkt verschlüsselten Daten können auf dezentralen Servern in einem OpenDXM GlobalX Filevault liegen, um den Datenverkehr über große Entfer-

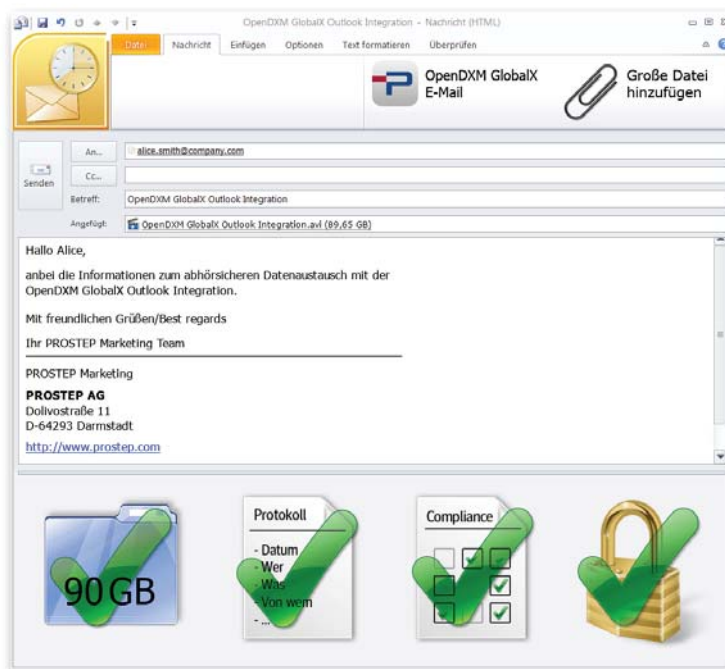
nungen zu optimieren. Das heißt zum Beispiel, dass die amerikanische Tochtergesellschaft eines deutschen Unternehmens die Daten für einen Projektpartner in den USA lokal bereitstellt, auch wenn dieser sich für den Download am zentralen Server in Deutschland anmelden muss. Diese Architektur hat den Vorteil, dass man den OpenDXM GlobalX-Server in einem Land mit strengeren Datenschutzrichtlinien betreiben kann, in dem die Nachrichtendienste nicht mal eben die Herausgabe der Schlüssel verlangen können - wie zum Beispiel in den USA. Ohne die Schlüssel können sie mit den verschlüsselten Daten in den Remote Filevaults nichts anfangen.

Die auszutauschenden Daten werden beim Upload auf die Plattform nach dem Public-Private-Key-Verfahren verschlüsselt. Bei der normalen Verschlüsselung ist OpenDXM GlobalX Herr über 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 dagegen für die persönliche Verschlüsselung entscheidet, muss der Empfänger einen privaten und nur ihm zu-

gänglichen Schlüssel haben, um die Daten öffnen zu können. In diesem Fall müssten die Nachrichtendienste noch mehr Aufwand treiben, wenn sie die Verschlüsselung knacken wollen, denn sie benötigen dafür den privaten Schlüssel, der Passwort geschützt auf einem Speichermedium der Anwender gespeichert ist.

Dokumentation der Austauschvorgänge

Der Versand der Daten über die Austauschplattform hat zusätzlich den Vorteil, dass alle Austauschvorgänge protokolliert werden und damit jederzeit für Audit-Zwecke genutzt werden können. OpenDXM GlobalX speichert zwar nicht die anhängende Datei, aber alle anderen Informationen, die zu jedem einzelnen Datenaustauschvorgang gehören. Bei Verwendung der OpenDXM GlobalX Outlook Integration wird sogar zusätzlich der Textkörper der originalen E-Mail archiviert. Der Textkörper wird nicht als Dokument abgelegt, sondern direkt in die Datenbank geschrieben, was Volltextrecherchen nach Sender, Empfänger, Betreff oder anderen Suchkriterien möglich macht. Der Anwender sieht natürlich immer nur die E-Mails, die er selbst über



Die Vorteile: Sehr große Dateien mit Outlook versenden, volle Dokumentation, automatische Einhaltung der Unternehmensregeln, höchste Sicherheit für vertrauliche Dokumente und einfachste Bedienung.

OpenDXM GlobalX empfangen oder verschickt hat - ein Gruppenleiter oder Systemadministrator aber hat die Gesamtsicht auf alle Austauschvorgänge zu einem bestimmten Projekt.

Die Integration der Datenaustauschplattform OpenDXM GlobalX in MS Outlook bietet nicht nur ein Höchstmaß an Datensicherheit und Schutz für die Dateianhänge, sondern macht die Austauschvorgänge außerdem jederzeit nachvollziehbar. Entscheidend für die Akzeptanz der Lösung ist, dass sie für den Endanwender eigentlich nicht in Erscheinung tritt. Die Möglichkeit, unternehmensweit einheitliche Spielregeln für den Umgang mit sensiblen Daten zu definieren, ist im Zweifelsfalle und auf längere Sicht wichtiger als den Datenspionen von NSA und Co. ein Schnippchen zu schlagen. -sg-



Die OpenDXM GlobalX Outlook Integration ist ab sofort verfügbar.

(1) siehe <http://royal.pingdom.com/2013/01/16/internet-2012-in-numbers>

(2) siehe www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data

(3) www.welt.de/wirtschaft/web-welt/article5918620/Bundesamt-warnt-jetzt-auch-vor-Outlook.html

(4) www.ingenieur.de/Arbeit-Beruf/Management/Ingenieure-Freiraum-fuer-Engineering-Konstruktion

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 HANNOVER
KARL-WIECHERT-ALLEE 72
30625 HANNOVER
TEL. +49 511 54058-0
FAX +49 511 54058-150

GESCHÄFTSSTELLE MÜNCHEN
TAUNUSSTRASSE 42
80807 MÜNCHEN
TEL. +49 89 35020-0
FAX +49 89 35020-200

GESCHÄFTSSTELLE WOLFSBURG
MAJOR-HIRST-STRASSE 11
38442 WOLFSBURG
TEL. +49 5361 8974-837

GESCHÄFTSSTELLE HAMBURG
HEIN-SASS-WEG 19
21129 HAMBURG
TEL. +49 40 2091608-0
FAX +49 40 2091608-23

GESCHÄFTSSTELLE KÖLN
JOSEF-LAMMERTING-ALLEE 16
50933 KÖLN
TEL. +49 221 6778-7691
FAX +49 221 6778-7699

GESCHÄFTSSTELLE STUTTART
WANKELSTRASSE 14/II
70563 STUTTART
TEL. +49 711 391900-110
FAX +49 711 391900-120