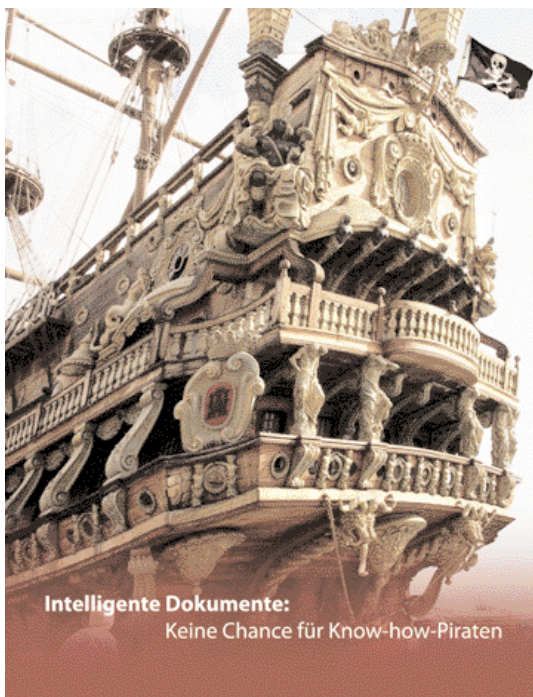


EXPERTEN DISKUTIEREN IM WIN-VERLAG

Entwürfe und Konzepte besser schützen

ANDREAS MÜLLER

Produktplagiate: da denkt man oft reflexartig an den Fernen Osten, an Gucci oder Rolex. Aber auch Maschinen, Ersatzteile und selbst Produktionsprozesse sind vor den Fälschern schon lange nicht mehr sicher – zum Schaden für Unternehmen, Beschäftigte und nicht zuletzt auch Käufer. Das Digital Engineering Magazin und das Inventor Magazin befragten deshalb sechs Experten, worauf sich Fertigungsunternehmen hier gefasst machen müssen und wie sie ihr geistiges Eigentum im Engineering-Umfeld besser schützen können.



Intelligente Dokumente:
Keine Chance für Know-how-Piraten

Ausgewogene Strategien im Kampf gegen den Diebstahl geistigen Eigentums sind gefragt.
Bild: pixelio

Mehr als 600 Bestellungen, die Werke ausgebucht bis 2013 – der neue Passagierjet Boeing 787, genannt Dreamliner, scheint schon eine Erfolgsgeschichte zu sein, bevor er überhaupt flugplanmäßig abhebt. Ein Grund: Boeing hat bei der Entwicklung des Flugzeugs konsequent auf Collaborative Engineering und Web-2.0-Strategien gesetzt. Insgesamt rund 100 Partner und Zulieferer in sechs Ländern arbeiteten in Echtzeit an einem von Boeing außerhalb der eigenen Firewall online bereitgestellten, virtuellen Modell, das zunächst nur die wichtigsten Konturen und Maße enthielt.

Der Flugzeugbauer trat nicht mehr nur als ein Hersteller, sondern vielmehr als Integrator und Organisator von Wissen auf. Unter seiner Kontrolle wurden im CAD-Modell tausende Teile und Baugruppen der neuen Passagiermaschine Schritt für Schritt auf einer einheitlichen PLM-Plattform in einheitlichen Datenformaten zusammenführt, das ursprüngliche Design immer weiter verfeinert und die notwendigen Berechnungen vorgenommen. Die Kenntnisse und Erfahrungen von Piloten, Sicherheitsfachleuten, Flugbegleitern und Kunden flossen frühzeitig

in die Spezifikationen ein. Wissen zu teilen und damit auch Risiken und Kosten mehreren Schultern aufzulasten, hat sich offenbar gelohnt, nicht nur für Boeing, sondern auch für die Zulieferer.

Aber das funktioniert nicht immer und überall so gut. Geht es um weniger komplexe Produkte mit geringerem Entwicklungsaufwand, hat das Teilen von Wissen oft einen bitteren Beigeschmack. Es passiert nämlich vielfach, ohne dass die Schöpfer dieses Wissens es wollen, und diese Aneignung verstößt gegen Rechtsnormen wie das Urheber-, das Patent-, das Muster-, das Marken- oder das Wettbewerbsrecht.

Produktplagiate, aber auch kopierte Produktionsprozesse und Vermarktungsstrategien sind die sichtbaren Folgen. Und das betrifft zunehmend auch Investitionsgüter wie Maschinen, dazugehörige Komponenten oder Auto-Ersatzteile. Der Schaden durch Produktpiraterie beläuft sich nach Angaben der OECD (Organisation for Economic Cooperation and Development) auf rund 200 Milliarden US-Dollar, wobei diese Summe noch nicht einmal die über das Internet gehandelten Produkte enthält [1].



Wolfgang Straßer, @yet:

„Angriffe finden immer statt, 7 mal 24 Stunden. Das erfordert einen entsprechenden Schutz, und zwar organisatorisch, physisch und in der IT.“

Eine Studie des DIHK und des APM (Aktionskreis deutsche Wirtschaft gegen Produkt- und Markenpiraterie e. V.) stellt fest: „Das vorhandene Instrumentarium zum Schutz geistigen Eigentums wird nicht genutzt.“

Schutzrechte anmelden

Unternehmen, die nicht schon von Produktpiraterie betroffen seien, meldeten überwiegend keine Schutzrechte an. Die Studie macht dafür vor allem Informationsdefizite besonders bei kleineren Unternehmen verantwortlich [2].

Aber von den rechtlichen Gesichtspunkten einmal abgesehen: Wie können Fertigungsunternehmen ihr Wissen mit technischen und organisatorischen Mit-

ternehmens: „Ein Kollege wandert zur Konkurrenz ab und lädt in seinen letzten Arbeitswochen gigabyteweise Daten herunter. Über ein PDM-System können wir nachweisen, was von wem heruntergeladen und angeschaut wurde. Abgesehen davon gibt es natürlich das Szenario, dass sich ein Experte abwerben lässt. Das ist immer noch die einfachste Methode, Know-how abzuziehen.“ Ebenfalls häufig ist die Kombination aus Tätern innerhalb und außerhalb des Unternehmens, die Konstruktionsunterlagen gemeinsam entwenden und verwerten.

Während all das auch schon vor den Zeiten von CAD und PLM möglich war, bergen heterogene IT-Landschaften, unterschiedliche CAX- und PLM-Systeme



GM Daewoo Matiz und Chery QQ. Bilder: GM Daewoo, Chery



mit aber der Gefahr des Datendiebstahls unmittelbar aus. Dieser Spagat zwischen effizienten, schnellen und kostengünstigen Fertigungs- und Entwicklungsprozessen einerseits und wirksamen Schutzmaßnahmen andererseits stellt für viele Firmen eine kaum lösbare Aufgabe dar.

Wo das Vertrauen fehlt, werden die Prozesse oft unnötig kompliziert, selbst, wie Ulrich Isermeyer feststellt, in eigentlich gut kontrollierbaren Prozessen wie der technischen Dokumentation. Isermeyer, Business Development Manager Acrobat bei Adobe Systems, schildert das am Beispiel eines mittelständischen Unternehmens: „Es gibt dort nur eine einzige Stelle, die an einem geschützten Arbeitsplatz das volle 3D-CAD-Modell hat. Man hat Angst, dass sich die Mitarbeiter in der technischen Dokumentation irgendwelche 3D-Modelle extrahieren und nach außen geben.“

Abwehrstrategien im Unternehmen

Auch wenn man die Erfolgsmeldungen lange suchen muss: Die Unternehmen



Chris J. Nicolaes, ENOVIA:

„Unternehmen können Prozesse so segmentieren, dass kein einzelner Fertiger den Überblick über die gesamte Produktentwicklung und Fertigung hat.“

teln schützen, ohne dabei auf die Vorteile der verteilten Produktentwicklung und Fertigung zu verzichten, wie können sie eine geeignete IT-Sicherheitsinfrastruktur etablieren?

Um dies aus der Sicht des Engineering zu klären, hat der WIN-Verlag Vertreter von Softwareanbietern, Engineering-Dienstleistern und dem Autozulieferer Autoliv an den runden Tisch gebeten.

Womit zu rechnen ist

Bevor das Produkt- und Prozesswissen in den Produktionsbetrieben in Billiglohnländern ankommt, hat es oft schon einen langen und verwirrenden Weg zurückgelegt. Die Sicherheitslücken im eigenen Unternehmen zu finden, stellt häufig den ersten und noch vergleichsweise einfachen Schritt zu Gegenmaßnahmen dar. Denn ein großer Teil der Angriffe geht von innen aus, wie Wolfgang Straßer bestätigt. Straßer ist Gründer und Geschäftsführer der @-yet GmbH, die sich auf das Thema IT-Risikomanagement spezialisiert hat. „Wir versuchen aufzuklären, wer was gestohlen hat, wer wo und wie auf Daten zugegriffen hat und wer auf die Daten nicht hätte zugreifen dürfen.“

Einen typischen Fall, der sich überall ähnlich abspielen kann, schildert Sven Kleiner. Er ist einer der Gründer und Geschäftsführer der :em engineering methods AG, eines CAX-Dienstleistungsun-

und auf höchste Produktivität getrimmte, segmentierte Prozessketten nicht nur für die Unternehmen, sondern auch für Datendiebe wirtschaftliches Potenzial. Diese Widersprüchlichkeit bringt Ralf Fellner, PLM Business Process Manager beim Autozulieferer Autoliv, auf den Punkt: „Grundsätzlich sollten alle unsere Designs in CATIA gemacht werden. Wenn es eine Anforderung ist, das auch noch im Kundensystem zu haben, gibt es eine Übersetzung, die nur auf der Schnittstelle zum Kunden hin funktional sein wird. Der Kunde würde nie einen Gasgenerator aufgedröseln in Unigraphics-Strukturen bekommen, sondern immer nur eine Blackbox“, veranschaulicht Fellner die Vorgehens-



Ulrich Isermeyer, Adobe:

„Ein wichtiger Bestandteil im Sicherheitskonzept von Adobe ist der Policy Server: Hier kann der Anwender dem Datenaustauschpartner Rechte zuteilen und auch nachträglich entziehen.“

weise. „Sie müssen mit vielen zusammenarbeiten und als Schutz einen kleinen gemeinsamen Nenner finden, um ihre Prozesse nicht stillzulegen“, bestätigt Burkhard Hörnig, Marketing Solution Manager für die Mechanik-Software von Autodesk.

Unternehmen verlagern Teile ihrer Fertigung in Billiglohnländer, um Kosten zu sparen und lokale Märkte zu erschließen, gleichzeitig setzen sie sich da-

stehen der Produktpiraterie keineswegs wehrlos gegenüber. So gelang es den etablierten Herstellern von DVD-Playern, Billiganbieter fast komplett aus dem Markt zu drängen, indem sie Druck auf die Händler ausgeübt haben, nichtlizenzierte Geräte aus den Regalen zu verbannen, und sich gegenseitig Lizenzen erteilt haben. Ein solches Vorgehen im großen Maßstab bleibt den meisten kleinen und mittelständischen Unternehmen ver-

schlossen, aber auch sie können sich gegen den Datendiebstahl schützen. Im Gespräch haben sich dabei zwei Ansatzpunkte herausgestellt: Einer betrifft die Ebene der Prozesse und der Unternehmensorganisation, der andere die Ebene der IT, der Software und der Daten.



Burkhard Hörnig, Autodesk:

„Sie müssen mit vielen zusammenarbeiten und als Schutz einen kleinen gemeinsamen Nenner finden, um ihre Prozesse nicht stillzulegen.“

Firmen, die zum Beispiel in China oder in Osteuropa technologisch anspruchsvoll produzieren wollen, müssen damit rechnen, dass ihre Produkte früher oder später kopiert werden. Chris J. Nicolaes, Director Central Europe und Geschäftsführer von ENOVIA Germany, führt mehrere Möglichkeiten an, wie sich dies erschweren lässt. Einerseits könne man technisch weniger komplexe Teile in Billiglohnländern fertigen lassen, andererseits ließen sich die Prozesse so segmentieren, dass kein einzelner Fertiger den Überblick über die gesamte Produktentwicklung und Fertigung habe. Und schließlich könne man bereits länger auf dem Markt eingeführte Produkte etwa in China fertigen lassen, während die technologisch anspruchsvollsten Lösungen nach wie vor in Deutschland hergestellt würden.

„Aus Produktsicht ist das auch eine Strategie in unserem Unternehmen“, konkretisiert Ralf Fellner. „Die Schlüsselkomponenten, die Know-how erfordern, im Airbag-Bereich zum Beispiel ist das der Gasgenerator, die werden nicht nach China vergeben.“



KIA Opirus,
Mercedes-Benz E-Klasse.
Bilder: KIA, Mercedes-Benz

Dienstleister zeigen Sicherheitsdefizite auf

Als Alternative zu eigenen Überlegungen, ihre Sicherheitsinfrastruktur gegen Angriffe zu wappnen, können Unternehmen auch auf Dienstleister zurückgreifen, die Schwachstellen aufdecken und Lösungs-

möglichkeiten für Sicherheitsdefizite vermitteln. Denn solange noch nichts passiert ist, lassen sich potenzielle Datenlecks oft nicht ohne professionelle Hilfe von außen erkennen. Assessments und Testangriffe auf die IT-Infrastruktur legen die Lücken offen. Dabei arbeitet etwa @-yet falls erforderlich auch mit einer internationalen Anwaltssozietät sowie der Kriminalpolizei zusammen.



Ralf Fellner, Autoliv:

„Der Kunde würde nie einen Gasgenerator aufgedröseln in Unigraphics-Strukturen bekommen, sondern immer nur eine Blackbox.“

em engineering methods konzentriert sich eher auf das Handling und den Schutz der Dateien selbst: „Wir beschäftigen uns mit Knowledge Based Engineering und entwickeln seit drei Jahren Lösungen für den Wissensschutz im Engineering“, sagt Sven Kleiner. Doch diese nützen natürlich überhaupt nichts, wenn beispielsweise Automobilzulieferer noch vor der Auftragsvergabe parametrische CAD-Daten mit Constraints und Automatismen oder gar schon komplette Produkte in 3D aus freien Stücken für verschiedene OEM-Plattformen bereitstellen, um bei der Ausschreibung bessere Karten zu haben.

Was die Software leisten kann

Die Softwareanbieter stellen verschiedene Möglichkeiten bereit, die Intelligenz der Daten mit Automatismen oder händisch zu reduzieren. „Man muss das Skalpell anset-

zen, um Wesentliches von Unwesentlichem zu trennen, ohne dass die Datenqualität leidet“, umschreibt Sven Kleiner die Aufgabe. Das Wissen in 3D-CAD-Modellen, also die Features, die Parametrik, die Historie und die Abhängigkeiten, müssen sich vor dem Datenaustausch reduzieren lassen, und zwar abgestuft und entsprechend dem Kooperationsmodell, das mit dem Kunden vereinbart wurde. Die Verschlüsselung kann noch als zusätzlicher Schutz hinzukommen.

„Dann haben wir immer noch ein natives 3D-Modell, das sich auch noch begrenzt variieren lässt, wie es der Kunde möchte“, sagt Sven Kleiner. Für Autodesk führt Burkhard Hörnig aus: „Zum einen kann man ein 3D-Modell eindampfen. Es behält dann zwar die Exaktheit, verliert aber den Strukturbaum, ähnlich wie ein STEP- oder IGES-File, es bleibt jedoch ein natives Format.“ Um die Abhängigkeiten und damit die Wirkmechanismen baugruppenübergreifend zu beseitigen, sei

schon etwas mehr händische Arbeit notwendig. DWG-Daten ließen sich passwortgeschützt weitergeben. Mit Design-Review könne der Anwender darüber hinaus ein kompaktes, webbasierendes Format erzeugen, das skalierbar sei, und sich zudem mit seinen Viewing- und Mark-up-Funktionen für die Designkommunikation eigne.

Je mehr Beteiligte in einem Projekt zusammenarbeiten, desto wichtiger wird die Verbindung von ausgefeilten Rechte- und Rollenkonzepten mit schlanken und sicheren Datenformaten. Chris Nicolaes nennt hier 3DLive von Dassault Systèmes als Beispiel. Auf dieser Collaboration-Plattform arbeiten die Projektbeteiligten mit abgepackten CATIA- oder DELMIA-Modellen, die sich mit Anmerkungen versehen und bemaßen lassen, und mit denen die Anwender zum Beispiel den Aufbau von Komponenten interaktiv erproben können.

Ulrich Isermeyer erläutert: Mittlerweile ließen sich in PDF-Dateien auch native CAD-Files wie CATIA-Part-Dateien und DWGs unterbringen. Das PDF diene dabei als Container. 2D-Zeichnungen und 3D-Modelle könnten zudem in 3D-PDFs umgewandelt werden. Ein wichtiger Be-





Interior-Entwurf für die 787: Boeing hat bei der Entwicklung der 787 konsequent auf Collaborative Engineering und Web-2.0-Strategien gesetzt und trat als Integrator und Organisator von Wissen auf. Bild: Boeing

standteil im Sicherheitskonzept von Adobe sei der Policy Server: „Hier kann der Anwender dem Datenaustauschpartner Rechte zuteilen und auch nachträglich entziehen. Die Lösung gilt für sämtliche Arten von Dokumenten und als Client braucht es nur den Adobe Reader. Für CAD-Files gibt es aber noch weitere Funktionen: Mit einem nativen Plug-in in CATIA V5 R16 lassen sich komplette Baugruppen oder einzelne CAD-Parts verschlüsseln. So kann man ein komplettes Assembly verschicken, dabei aber zum Beispiel drei sensible Bauteile schützen“, erklärt Isermeyer.

So umfassend einzelne Lösungen auch sein mögen, sie können sich doch als ungenügend erweisen gegenüber der Heterogenität der Engineering-Software-Landschaft in den Unternehmen. Ralf Fellner beschreibt: „Wir nutzen eine PLM-Plattform im Unternehmen. Es klappt gut, solange ich mich auf dieser Metadatenebene bewege, aber wenn ich mit unter-

schiedlichen Dateien arbeite, wird es problematisch. Wenn ich mit einem Joint-Venture-Produktionswerk zu tun habe, rede ich über einen Satz an CAD-Modellen, Strukturen, FEM-Dateien, Excel-Sheets. Hier muss nun der Ingenieur in Zeitnot versuchen, die Dokumente herunterzuziehen und an die Partnerfirmen weitergeben.“ Zwar wisse das PLM-System, was derjenige, der die Daten herunterlade, sehen darf, aber es könne dem Excel-Sheet nicht sagen, dass es einzelne Spalten herausfiltern soll.

Einfache, transparente Richtlinien

„Angriffe finden immer statt, 7 mal 24 Stunden. Das erfordert einen entsprechenden Schutz, und zwar organisatorisch, physisch und in der IT“, erklärt Wolfgang Straßer und vergleicht Sicherheitskonzepte mit dem Arbeitsschutz, wo zum Beispiel Bekleidung und bestimmte Verhaltensweisen vorgeschrieben sind. Die Richtlinien müssten jedoch übersichtlich und knapp gehalten sein. Dass Einfachheit und Transparenz den Schutz der eigenen Daten verbessern, bestätigt auch Ralf Fellner: „Der Ingenieur darf nicht

noch mehr Aufwand haben, weil er erst einmal mit 35 Klicks jede Datei verschlüsseln muss.“

Trotz aller Möglichkeiten, Sicherheitsmechanismen zu implementieren, bleibt somit immer noch der Mensch die Schwachstelle, zumal der Druck auf die Ingenieure durch immer kürzere Innovationszyklen wächst. Fellner schlägt vor, ein dichtes Netz aus Vertrauenspersonen aufzubauen, denn: „Wir erfahren nicht durch eine Software, dass ein bestimmter Kollege Daten stiehlt, sondern von Kollegen, die ihn verdächtigen.“ Und schließlich sind sich alle darin einig: Ein Sicherheitskonzept muss gelebt werden. Von der Geschäftsleitung, vom Auftraggeber und von denen, die es dann in die Praxis umsetzen.

to ■

KENNZIFFER: DEM13028

Anmerkungen:

[1] *The Economic Impact of Counterfeiting and Piracy, Executive Summary* unter: www.oecd.org/dataoecd/13/12/38707619.pdf, Stand 03.08.2007

[2] *Studie des DIHK und des APM zu Produkt- und Markenpiraterie in China* unter: <http://www.markenpiraterie-apm.de/files/standard/China%20Studie.pdf>



Sven Kleiner, :em engineering methods:

„Man muss das Skalpell ansetzen, um Wesentliches von Unwesentlichem zu trennen, ohne dass die Datenqualität leidet.“ Bilder: WIN-Verlag

1/3 Anzeige
quer