

EXPERTENGESPRÄCH: SO SCHÜTZEN SIE IHR KNOW-HOW

In Sicherheit wissen

Produktplagiate: da denkt man oft reflexartig an den Fernen Osten, an Gucci oder Rolex. Aber auch Maschinen und selbst Produktionsprozesse sind vor den Fälschern nicht mehr sicher. Wir, die Redakteure des Digital Engineering Magazins und Inventor Magazins, haben uns mit sechs Experten darüber unterhalten, wie Fertigungsunternehmen ihr geistiges Eigentum im Engineering-Umfeld besser schützen können.



Quelle: aboutpixel.de-Kellermeister

Mehr als 600 Bestellungen, die Werke ausgebucht bis 2013 – der neue Passagierjet Boeing 787, der Dreamliner, ist schon eine Erfolgsgeschichte, 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 Flugzeuggigant 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 zusammengeführt, 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 gelohnt, nicht nur für Boeing, auch für die Zulieferer und die Nutzer.

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 ganz anderen Beiklang. Es passiert nämlich vielfach, ohne dass die Schöpfer dieses Wissens es wollen, und dieses unfreiwillige Teilen verstößt



Ulrich Isermeyer, Business Development Manager Acrobat bei Adobe Systems.

gegen Rechtsnormen wie das Urheber-, das Patent-, das Marken- oder das Wettbewerbsrecht. Diebstahl geistigen Eigentums heißt der zugehörige Straftatbestand. Produktplagiate, aber auch kopierte Produktionsprozesse und Vermarktungsstrategien sind die sichtbaren Folgen. Und das betrifft nicht nur die Kreationen von Gucci, Prada oder Rolex, sondern 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]. Der Verlust von Arbeitsplätzen und, schlimmer noch, der Gesundheit, wenn es um minderwertige Ersatzteile oder Medikamente geht, führt zu erheblichen Folgekosten, für die die eigentlichen Verursacher kaum je zur Rechenschaft gezogen werden können. Dabei darf sich China mit dem unrühmlichen Titel der größten Fälscherwerkstatt der Welt schmücken, obschon die chinesische Regierung zunehmend erkennt,

welcher immense Schaden hier für die eigene Glaubwürdigkeit als Investitionsstandort erwächst.

Informieren und Schutzrechte anmelden

Die Bundesregierung und die EU andererseits haben erst kürzlich eine ganze Reihe von Maßnahmen angekündigt und verabschiedet, um geistiges Eigentum wirksamer zu schützen. Dazu gehören eine Verbesserung der Zollarbeit, die verstärkte Kooperation mit Behörden in den USA, der Dialog mit Problemstaaten und eine grenzüberschreitend vereinheitlichte Patentgerichtsbarkeit. Auch Wirtschaftsverbände informieren darüber, wie Unternehmen Schutzrechte an Produkten und Marken geltend machen können und bieten ihnen die Möglichkeit, Rechtsverletzungen zu melden. Gesetze und Informationsangebote allein reichen aber nicht aus. So stellt eine Studie des DIHK und des APM (Aktionskreis deutsche Wirtschaft gegen Produkt- und Markenpiraterie e. V.) fest: „Das vorhandene Instrumentarium zum Schutz geistigen Eigentums wird nicht genutzt.“ 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 Mitteln schützen, ohne dabei auf die Vorteile der verteilten Produktentwicklung und Fertigung zu verzichten, wie können sie eine geeignete IT-Sicherheitsinfrastruktur etablieren? Um das aus der Sicht des Engineering zu klären, hat der WIN-Verlag sechs Vertreter von Softwareanbietern, Engineering-Dienstleistern und Anbietern an den runden Tisch gebeten, die sich aus unterschiedlichen Blickwinkeln mit dem Schutz geistigen Eigentums befassen: Sven Kleiner, einer der Gründer und Geschäftsführer der *em engineering methods AG*, eines CAX-Dienstleistungsunternehmens, Ulrich Isermeyer, Business Development Manager Acrobat bei Adobe Systems, Chris J. Nicolaes, Director Central Europe und Geschäftsführer ENOVIA Germany, Wolfgang Straßer, Gründer und Geschäftsführer der *@-yet GmbH*, die sich auf das Thema IT-Risikomanagement spezialisiert hat, Burkhard Hörnig, als Marketing Solution Manager MSD bei Autodesk für die Mechanik-Software zuständig und auf der Seite der Anwender Ralf Fellner, PLM Business Process Manager beim Autozulieferer Autoliv, der sich auf die Entwicklung von Sicherheitssystemen wie Airbags und Gurtsystemen fokussiert hat.

Womit zu rechnen ist

Bevor das Produkt- und Prozesswissen in den Produktionsbetrieben in Russland oder in China ankommt, hat es oft schon einen langen und verwirrenden Weg zurückgelegt. Die Sicherheitslecks 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 aus seiner Erfahrung bestätigt. Einen typischen Fall, der sich überall ähnlich abspielen kann, schildert Sven Kleiner: „Ein Kollege wandert zur Konkurrenz ab und lädt in seinen letzten Arbeitswochen gigabyteweise Daten herunter.

Natürlich können wir über unser PDM-System nachweisen, was von wem heruntergeladen und angeschaut wurde. Und dann 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, selbst in ein und demselben Unternehmen, und auf höchste Produktivität getrimmte, segmentierte Prozessketten nicht nur für die Unternehmen, sondern auch für Datendiebe wirtschaftliches Potenzial. Diese Widersprüchlichkeit bringt Ralf Fellner auf den Punkt: „Eine Firma wie meine muss sich mit mindestens fünf verschiedenen Kunden auseinander setzen, und der Kunde fordert, dass die Daten direkt in sein jeweiliges PDM-System eingestellt werden können.“ Dann habe sich ein Minimalstandard entwickelt, die CAD-Modelle enthalten nur sehr wenige Features. Wir de-



Burkhard Hörnig, Marketing Solution Manager MSD bei Autodesk.

1/2 hoch



Chris J. Nicolaes, Director Central Europe und Geschäftsführer ENOVIA Germany.

signen eine Blackbox. 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 Vorgehensweise.

„Sie müssen mit vielen zusammenarbeiten und als Schutz einen kleinen gemeinsamen Nenner finden, um ihre Prozesse nicht stillzulegen“, bestätigt Burkhard Hörnig. Hinzu kommt, dass Unternehmen Teile ihrer Fertigung in Billiglohnländer verlagern, um Kosten zu sparen und lokale Märkte zu erschließen, sich damit aber gleichzeitig der Gefahr des Datendiebstahls ganz unmittelbar aussetzen. Dieser Trade-off zwischen effizienten, schnellen und kostengünstigen Fertigungs- und Entwicklungsprozessen einerseits und wirksamen Schutzmaßnahmen andererseits stellt für viele Unternehmen 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 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.“

Abwehr im Unternehmen

Auch wenn man die Erfolgsmeldungen lange suchen muss: Die Unternehmen stehen der Produktpiraterie keineswegs wehrlos gegenüber. So gelang es den etablierten Herstellern von DVD-Playern die chinesischen 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 verschlossen, 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.

Firmen, die in China oder in Osteuropa technologisch anspruchsvoll produzieren wollen, müssen damit rechnen, dass ihre Produkte früher oder später kopiert werden. Chris Nicolaes führt mehrere Möglichkeiten an, wie sich dies erschweren lässt. Einerseits könne man technisch weniger komplexe Teile in den entsprechenden Ländern fertigen, andererseits ließen sich die Prozesse so segmentieren, dass kein einzelner Fertiger den Überblick über die gesamte Produktentwicklung und Fertigung hat. Und schließlich könne man bereits länger auf dem Markt eingeführte Produkte zum Beispiel 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, PLM Business Process Manager, Autoliv.

Ralf Fellner. „Die Schlüsselkomponenten, die Know-how erfordern, im Airbag-Bereich zum Beispiel ist das der Inflator oder Gasgenerator, die werden nicht nach China vergeben.“

Als Alternative zu eigenen Überlegungen, ihre Sicherheitsinfrastruktur gegen Angriffe zu wappnen, können Unternehmen auch auf Dienstleister zurückgreifen, die Schwachstellen aufdecken und Lösungsmöglichkeiten für Sicherheitsdefizite vermitteln. Denn solange noch nichts passiert ist, lassen sich potenziellen Datenlecks oft nicht ohne professionelle Hilfe von außen erkennen. Assessments und Testangriffe auf die IT-Infrastruktur legen die Lücken offen. Wolfgang Straßer erklärt: „Wir versuchen aufzuklären, wer was gestohlen hat, wer wo und wie auf Daten zugegriffen hat und wer auf die Daten nicht hätte zugreifen dürfen.“ Dabei arbeitet @-yet, falls erforderlich, auch mit einer internationalen Anwaltssozietät sowie der Kriminalpolizei zusammen.

em engineering methods konzentriert sich eher auf das Handling und den Schutz der Dateien selbst: „Wir beschäftigen uns mit dem Thema Knowledge Based Engineering, und wenn man über Wissen spricht, dann ist das Thema Innovation und geistiges Eigentum nicht weit. Wir entwickeln seit zwei, drei Jahren Lösungen für das Thema Wissensschutz im Engineering“, sagt Sven Kleiner. Er sieht andererseits die Gefahr, dass zum Beispiel Automobilzulieferer schon in frühen Phasen, noch vor der Auftragsvergabe, parametrische CAD-Daten mit Constraints und Automatismen oder gar schon komplette Produkte in 3D für verschiedene Plattformen bereitstellen, um dann bei der Ausschreibung die besten 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 kann hier nicht mit dem großen Hammer vorgehen, sondern muss eher das Skalpell ansetzen, um Wesentliches von Unwesentlichem zu trennen, ohne dass die Datenqualität leidet“, umschreibt Sven Kleiner die schwierige Aufgabe auf der Seite des Anwenders.

Es besteht ein Konsens in der Gesprächsrunde, dass sich das Wissen in 3D-CAD-Modellen, also die Features, die Parametrik, die Historie und die Abhän-



Wolfgang Strasser, Geschäftsführer der @-yet GmbH.

gigkeiten, sich vor dem Datenaustausch reduzieren lassen muss, 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 aber ein natives Format.“ Um die Abhängigkeiten und damit die Wirkmechanismen baugruppenübergreifend zu beseitigen, sei schon etwas mehr händische Arbeit notwendig.

DWG-Daten lassen sich passwortgeschützt weitergeben. Mit DesignReview kann der Anwender darüber hinaus ein



Sven Kleiner, einer der Gründer und Geschäftsführer der :em engineering methods AG.

kompaktes, webbaserendes Format erzeugen, das vektorbasierend und skalierbar ist, und sich zudem mit seinen Viewing- und Mark-up-Funktionen für die Designkommunikation eignet.

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

Ursprünglich in der Office- und Grafikwelt zu Hause, etabliert sich Adobes Standardformat PDF nun auch im Engineering als Datenaustauschformat. Mittlerweile lassen sich in PDF-Dateien auch native CAD-Files wie CATIA-Part-Dateien und DWGs unterbringen. Das PDF dient dabei als Container. 2D-Zeichnungen und 3D-Modelle können zudem in 3D-PDFs umgewandelt werden. Ein wichtiger Bestandteil im Sicherheitskonzept von Adobe ist der Policy Server. Hier kann der Anwender dem Datenaustauschpartner Rechte zuteilen und entziehen. Die Lösung gilt für sämtliche Arten von Dokumenten, sowohl für native Office- als auch für CATIA- und in Kürze Pro/E-Dateien. 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 Ulrich Isermeyer.

So umfassend und fast schon allgegenwärtig die Lösungen von Adobe oder Autodesk aber auch sind, sie funktionieren am besten, wenn sie als einzige Lösungen im Einsatz sind. Ralf Fellner wendet ein: „Wir nutzen eine PLM-Plattform im Unternehmen. Es klappt gut, solange ich mich auf dieser Metadaten-ebene bewege, aber wenn ich dann mit Files arbeite, dann habe ich ein Problem: die fehlenden Schnittstellen. 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 herunterzustricken und an die Partnerfirmen weitergeben.“ Zwar wisse das PLM-System, was derjenige, der die Daten herunterlade, sehen können sollte, aber es könne dem Excel-Sheet nicht sagen, dass es einzelne Spalten herausfiltert.

Und der Mensch?

„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. Das Werk müsse jedoch knapp sein – 300 Seiten würde sonst niemand lesen. 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 chinesischer 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.

ANDREAS MÜLLER

Anmerkungen:

[1] The Economic Impact of Counterfeiting and Piracy, Executive Summary, unter: www.oecd.org/dataoecd/13/12/38707619.pdf, Stand vom 3. 8. 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>; Stand vom 3. 8. 2007

Anzeige

www.cad-ausbildung.de
CAD-ServiceCenter Klinkenberg