

## Der unsichtbare Feind

Von Lothar Lochmaier

**Der Maschinen- und Anlagenbau verliert durch Raubkopierer jährlich Umsätze in Milliardenhöhe. Auch sensible Geschäftsbereiche sind oft kaum abgesichert - der technische Schutz vor Plagiaten sollte daher bereits in der Produktentwicklung verankert sein.**

Hamburg - Jährlich erstellt das US-Magazin "Forbes" das Ranking der reichsten Menschen der Welt. Auf Platz 79 landeten im vergangenen Jahr die Eigentümer des Automobilzulieferers INA, Maria-Elisabeth Schaeffler und Sohn Georg Schaeffler, mit einem geschätzten Vermögen von 6,8 Milliarden Dollar.

Zum Firmenimperium gehört auch der Wälzlagerhersteller INA Schaeffler KG. Wälzlager sind Produkte, die wenig sexy sind und nicht im Rampenlicht der Öffentlichkeit stehen. Aber sie sorgen dafür, dass die Endprodukte unterschiedlicher Branchen von der Automobil-, über die Druck- bis hin zur Konsumgüterindustrie reibungslos funktionieren. Das Know-how steckt im Innern. Wälzlager sind robuste Hightech und halten enormen Kräften stand. Originalteile sind nur über zertifizierte und lizenzierte Händler erhältlich. Produktfälschungen sind in der Regel von außen kaum erkennbar.

Kürzlich ging der in Schweinfurt angesiedelte Wälzlagerhersteller Schaeffler KG an die Öffentlichkeit und sagte den Produktpiraten den Kampf an. Die Zukunft des Unternehmens und seiner Hightech-Produkte hängt auch davon ab, ob es gelingt, den schwunghaften Handel mit Fälschungen und Nachahmerprodukten wirksam einzudämmen.

Rund 40 Tonnen gefälschte Wälzlager vernichteten die Schaeffler Gruppe, die SKF GmbH und das FAG-Werk in Schweinfurt - mit einem geschätzten Marktwert von acht Millionen Euro. "Mit dieser gemeinsamen Aktion machen wir darauf aufmerksam, dass Marken- und Produktpiraterie kein Phänomen ist, das sich auf China oder Südosteuropa beschränkt, sondern hier vor unserer Haustür stattfindet", erklärt Hans-Jürgen Goslar, Mitglied der Schaeffler-Geschäftsleitung.

Längst seien es nicht mehr ausschließlich gefälschte Luxus- oder Konsumgüter, die den deutschen und europäischen Markt überschwemmen, sondern zunehmend auch sicherheitsrelevante Industrieprodukte wie eben Wälzlager, bekräftigt Goslar. Pikant an dem Fall ist, dass die vom Unternehmen beauftragten Wirtschaftsdetektive die gefälschten Produkte mit den Markenaufdrucken INA, FAG und SKF nicht nur im fernen Osten aufspürten, sondern auch bei einem fränkischen Wälzlagerhändler dingfest machten.

Doch sind derartige Erfolge nur ein schwacher Trost. Raubkopierer und Produktpiraten scheuen kaum mehr den offenen Konflikt, beispielsweise, indem sie für kopierte Produkte sogar das Recht auf Patentschutz einklagen. Angesichts der drohenden Eskalation auf dem internationalen Parkett nützt es wenig, wenn das Thema wieder einmal ganz oben auf politischer Ebene diskutiert wird, etwa im Juni beim G8-Gipfel in



cirosec GmbH  
Edisonstraße 21  
74076 Heilbronn  
Tel: 07131 / 59455-0  
Fax: 07131 / 59455-99  
info@cirosec.de  
[www.cirosec.de](http://www.cirosec.de)

Heiligendamm oder beim "3. Weltkongress gegen Produktfälscherei", der im Januar in Genf stattfand.

### **Illegales Reengineering als Kavaliersdelikt**

Firmenchefs halten sich ohnehin lieber an Fakten als an Absichtserklärungen. Experten des Verbandes Deutscher Maschinen- und Anlagenbau (VDMA) schätzen den jährlichen Umsatzverlust für ein Industrieunternehmen durchschnittlicher Größe auf 3 bis 5 Prozent. Der jährliche Schaden für die Investitionsgüterindustrie liegt demnach bei rund 4,5 Milliarden Euro. Nach Angaben einer Erhebung des VDMA vom vergangenen Jahr sind bereits mehr als zwei Drittel der Unternehmen von Produktpiraterie betroffen.

Überwiegend kopiert werden nicht nur Ersatzteile, sondern komplette Maschinen und Anlagen. Global aufgestellte Konzerne mögen dies vielleicht noch verkraften. Bei mittelständischen Zulieferern, bei denen die Gewinnmargen ohnehin permanent unter Druck sind, kann dies leicht die eigene Existenz infrage stellen. Experten nennen nicht nur aufstrebende Schwellenländer wie China und Russland als Urheber, sondern auch die USA und andere Hightech-Staaten.

"Ohne Marken- und Produktpiraterie gäbe es in Deutschland 70.000 Arbeitsplätze mehr", bilanziert Doris Möller, geschäftsführendes Vorstandsmitglied im Aktionskreis deutsche Wirtschaft gegen Produkt- und Markenpiraterie (APM). Nicht nur Arbeitsplätze seien gefährdet, sondern auch die Sicherheit der Menschen und Mitarbeiter, etwa wenn Plagiate in sicherheitssensiblen Anwendungen wie im Automobilbau eingebettet sind.

Nach Angaben des Fachverbandes Werkzeugindustrie sind allein im gewerblichen Bereich rund 3500 Arbeitsunfälle pro Jahr in Deutschland auf Plagiate zurückzuführen. Den Urhebern allein mit den Mitteln der Strafverfolgung beizukommen, entpuppt sich meist als wertloser Papiertiger. Patente und Markenschutz stehen zwar auch im Maschinen- und Anlagenbau ganz oben auf der Agenda. Rechtliche Maßnahmen lösen das Problem indes nur an der Oberfläche. "Die rechtliche Absicherung bietet nur eine Grundlage, Verstöße juristisch zu verfolgen", bestätigt Jens Geissmann, beim VDMA für Fragen zur IT-Sicherheit in den Unternehmen zuständig.

Geissmann setzt neben rechtlichen auch auf technische und organisatorische Maßnahmen, wie die Sensibilisierung der Mitarbeiter, um die Schätze des Unternehmens gegen soziale Schwachstellen (Social Engineering) abzusichern: "Gut informierte und für die Sicherheit sensibilisierte Mitarbeiter tragen dazu bei, dass Know-how-Verlust vermieden wird." Sind die Mitarbeiter darüber informiert, welche Daten und Informationen schützenswert sind, achteten diese verstärkt auf die Sicherheit. "Die Verantwortung ist dabei auf mehrere Schultern verteilt", empfiehlt Geissmann.

### **Defizite beim IT-Management**

Doch auch bei organisatorischen Maßnahmen ist der Grat zwischen effektiver Absicherung und blindem Aktionismus äußerst schmal. Denn das Risiko zum Opfer gezielter Angriffe von innen zu werden, lässt sich mithilfe von organisatorischen Direktiven kaum minimieren. Schließlich

benötigt der Angreifer nur eine kleine Sicherheitslücke im IT-System. Der Verteidiger hingegen müsste alle erdenklichen Szenarien und Katastrophenfälle 100-prozentig absichern.

Für den IT-Sicherheitsexperten Stefan Strobel präsentiert sich so manches global agierende Unternehmen mit einem permanenten "Tag der offenen Tür". Die einfachsten Dinge blieben oftmals unbeachtet, wie gesicherte und verschlüsselte Notebooks zu benutzen, sagt der Geschäftsführer des IT-Dienstleisters Cirosec.

Für den Sicherheitsexperten zaubert oftmals schon die erste Analyse der aktuellen Sicherheitslage überraschende Erkenntnisse hervor, etwa wenn Outsourcing-Partner vom deutschen Auftraggeber mit automatischen Zugriffsrechten auf sensible Informationsbestände ausgestattet seien. "Wenn das indische Callcenter ungewollt Zugriff auf wichtige Daten erhält, sollte man sich schon vorher fragen, ob der Partner ähnliche Wertvorstellungen wie das eigene Unternehmen hat", so Strobel.

Auch vor der Chefetage machen die Versäumnisse nicht halt. Hat der Vorstand immer darüber Kenntnis, ob der Fileserver mit sensiblen Powerpoint- und Excel-Dateien als geheim klassifiziert ist oder nicht? Selbst probate Schutzmaßnahmen sind wirkungslos, wenn der Angreifer in sensiblen Bereichen wie Hotels oder Flughäfen illegalen Zugriff auf die Daten erhält.

"Die passenden IT-Werkzeuge sollten aber nicht auf die Rundum-Absicherung aller Systeme ausgerichtet sein, sondern auf die als schützenswert klassifizierten Dokumente und Prozesse", gibt Strobel zu bedenken.

### **Erhöhtes Risiko von Insider-Attacken**

Social Engineering, das gezielte Ausnutzen von inneren Sicherheitslücken, stellt nach Auffassung von Experten weiterhin das größte Risiko dar. Patentrezepte dagegen gibt es keine. Der spektakulärste Fall einer Attacke von innen ereignete sich im Februar 2005. Eine chinesische Studentin begann ein Praktikum beim französischen Automobilzulieferer Valeo in Paris. Den Kollegen fiel auf, dass sie häufig mit einem privaten Notebook im Unternehmen anzutreffen war. Die Betriebsspionage flog auf, nachdem die Polizei bei einer Wohnungsdurchsuchung gleich mehrere Computer mit vertraulichen Daten vorfand.

Von ähnlich gelagerten Fällen berichtet der Verfassungsschutz Baden-Württemberg auf seiner Homepage. Insider-Attacken jedoch allein mit einer groß angelegten "Blockade der Kommunikationskanäle" zu begegnen, greift zu kurz. Wie also lassen sich relevante Datenbanken oder Zeichnungen vor dem Ausspionieren schützen?

Zunächst einmal gelte es bei der Klassifizierung schützenswerter Bestände den jeweiligen Produktverantwortlichen und die in den Produktionsprozess eingebundenen Fachabteilungen einzubeziehen, empfiehlt Sicherheitsberater Strobel: "Besser ist es, das Schutzniveau pragmatisch bei 80 Prozent anzusetzen und dann weiter zu verbessern, als alle denkbaren Szenarien künstlich hochzurechnen."

Technisch gesehen gehören etwa eine eindeutig geregelte Passwortvergabe, die Verschlüsselung sensibler Daten sowie transparente

Berechtigungskonzepte zu den Standards. Jeder Mitarbeiter sollte nur Zugriff auf die für seine Aufgabe relevanten Daten und Informationen erhalten. Allerdings schützt dies nicht vor "Datenklau" durch autorisierte Personen. Hier kann das Unternehmen durch Protokollierung der Datenzugriffe höchstens nachvollziehen, auf welche Daten die berechtigten Mitarbeiter zugegriffen haben. Zudem gilt es, die Grundlagen des Datenschutzgesetzes bei der Protokollierung zu beachten.

### **Automatischer Schutzriegel**

Bei Lösungen im Bereich der automatischen Einbruchsabwehr - Intrusion Detection beziehungsweise Prevention – liegt der Schwerpunkt bislang auf der Absicherung des Datenverkehrs von außen nach innen. Die Abwehr konzentriert sich darauf, den Angreifer so gut wie möglich an der virtuellen Eingangstüre abzufangen oder durch auffällige Verhaltensmuster proaktiv zu erkennen, möglichst bevor ein größerer Schaden entstanden ist.

Sogenannte Extrusion-Prevention-Systeme gehen einen Schritt weiter. Sie unterbinden den ungehinderten Datenfluss von innen nach draußen. In erster Linie lassen sich damit also Attacken von Insidern verhindern. Technisch gesehen gibt es zwei grundlegende Ansätze: Zum einen lässt sich der Datenfluss direkt an den Servern regeln und kontrollieren, zum anderen auf der Ebene des Anwenders, der sogenannten hostbasierten Einbruchsabwehr.

Im Idealfall bedeutet die Absicherung mit Hilfe eines automatischen Schutzriegels von innen nach außen, dass entsprechende Programme auf jedem PC oder Endgerät im Betrieb installiert sind. Ein Agent regelt den Zugriff auf sensible Daten - und erkennt jeden illegalen Zugriff darauf, egal ob per E-Mail oder mithilfe eines externen Speichergeräts.

Die Marktanalysten von IDC haben für den Markt zum Schutz sensibler Unternehmensdaten einen weiteren Begriff definiert - Information Leakage Detection and Prevention (ILD&P) -, das Aufdecken und Schließen von "Informationslecks" in den Computersystemen.

Darunter sind auch konzeptionelle Schwachstellen in webbasierten Anwendungen zu verstehen, die einem Angreifer helfen, die Schwachstellen der Kommunikation übers Internet zu missbrauchen. Ähnlich wie bei der klassischen Einbruchsabwehr (Intrusion Detection), die eine Brandschutzmauer von außen nach innen bildet, lassen sich dabei Ansätze auf der Anwender- und auf der Netzwerkebene unterscheiden.

### **Klare Spielregeln für die Nutzung**

Sicherheitsexperte Strobel empfiehlt nicht nur auf ein Pferd zu setzen, sondern plädiert für einen mehrschichtigen Ansatz, der Desktop- und Netzlösungen kombiniert, um den Schutz nachhaltig zu optimieren. Denn allein das Netzwerk auf Anomalien zu überprüfen, reiche nicht aus, da der Datenabfluss häufig über externe Geräte wie USB-Memory-Stick, CD, iPod oder Notebook erfolge.

Den Vorteil der hostbasierten Extrusion Prevention gegenüber dem klassischen serverbasierten Ansatz sieht Strobel darin, sowohl den

Datenfluss im Unternehmen als auch aus dem Unternehmen heraus zu kontrollieren. Das System unterscheidet dabei zwischen "sensiblen" Daten und öffentlichen beziehungsweise als unkritisch eingestuften Daten.

Auch Infowatch, ein auf die Gefahrenabwehr von Unternehmen spezialisierter Ableger des russischen Virenabwehrspezialisten Kaspersky, favorisiert ein kombiniertes Lösungskonzept. In Kürze will das Unternehmen aufgrund der steigenden Nachfrage eine deutsche Niederlassung eröffnen. So überwacht bei Infowatch zum einen ein "Mail- und Webmonitor" den Internetverkehr von innen nach außen.

Des Weiteren ist ein sogenannter Netmonitor im Einsatz, der mit seinen Clients an die Fileserver und Arbeitsstationen angedockt ist und dort die Aktivitäten des Nutzers kontrolliert, sobald dieser eine Datei öffnet, kopiert oder druckt. Ein dritter Bestandteil "Device Monitor" trägt dafür Sorge, dass das illegale Kopieren der Kronjuwelen aus dem Computersystem nicht über externe Speichermedien wie USB-Sticks, MP3-Player oder CD-Brenner erfolgt -, ohne derartige Geräte gleich gänzlich zu verbieten.

Bei Code Green Networks ist der Schutz direkt am Ausgang des Firmennetzes postiert. Dort überwacht die Lösung den Datenfluss aus dem Unternehmen wie Mail, Webverkehr, Instant Messaging, FTP oder Peer-to-Peer-Filesharing. Dadurch sollen nach eigenem Bekunden keine wichtigen Memos, Kundenlisten, Verträge, Konstruktionsdaten oder andere Quellcodes nach draußen gelangen.

Allerdings gilt es, durch interne Eingriffe die Arbeitsabläufe der Mitarbeiter sowie deren produktives Arbeiten nicht zu sehr einzuschränken. Denn das Management sollte dem in Einzelfällen durchaus begründeten Misstrauen durch klare und transparente Regeln entgegenwirken. Das Ziel besteht schließlich in der Know-how-Absicherung und nicht in der Innenüberwachung. Hier sind die Verantwortlichen im Unternehmen bei der Auswahl der passenden Produkte gefragt, die Spielregeln für deren Nutzung genau festzulegen.

Grundsätzlich soll die hostbasierte Extrusion Prevention nur das Öffnen, Umbenennen oder Kopieren von Dokumenten erfassen, nicht aber die Inhalte der Dokumente. "Ob ein Mitarbeiter am Morgen fünf Dateien öffnet und den Rest des Tages mit Spielen verbringt, ist aus den Protokollen des Extrusion Prevention Systems auf der Anwenderbene nicht ersichtlich", argumentiert Sicherheitsberater Strobel. Damit die Lösung funktioniert, kommt es aber auch auf ein reibungsloses Zusammenspiel mit möglicherweise im Unternehmen verankerten Konzepten zum Digital Rights Management (DRM) an.

### **Plagiatsschutz schon in der Entwicklung**

Um das eigene Unternehmen in Zukunft noch wirkungsvoller und umfassend gegen den Verlust geistigen Eigentums zu schützen, ist nach Auffassung von Experten eine weitergehende technische Vision notwendig. Um das geistige Eigentum nämlich effektiv vor illegalem Reengineering zu schützen, müsste der technische Schutz vor Plagiaten unmittelbar in der Entwicklung und Produktion verankert sein, bestätigt Rainer Glatz, Geschäftsführer des VDMA-Fachverbandes Software.

Entsprechende Lösungskonzepte unterstützt bereits das

Bundesministerium für Bildung und Forschung (BMBF), sie stecken allerdings teilweise noch in den Kinderschuhen. Aktuell diskutiert ist eine ganze Armada von IT-basierten Schutzkonzepten, wie produktindividuelle Buchstaben-Zahlen-Kombinationen, Hologramme, Mikropartikel, molekulare Markierungssysteme, Funkchips oder zusätzliche Hardware, ohne die ein Produkt gar nicht benutzbar ist. Immerhin, einige Betriebe setzen derartige innovative Konzepte ein, halten sich aber in der Öffentlichkeit aus plausiblen Gründen eher bedeckt.

Forscher der Universität Würzburg arbeiten in einer noch weiter entfernten Galaxie, der Vision einer abhörsicheren Methode zur künftigen Datenübertragung. "Der chaotische Laserstrahl wird dazu mit einer Nachricht moduliert", erklärt Professor Wolfgang Kinzel vom Lehrstuhl für Theoretische Physik III der Universität Würzburg. Bei einem "Lauschangriff", der den Strahl abhorcht, bliebe die Botschaft verborgen, denn sowohl mit oder ohne Nachricht sei die Intensität des Laserstrahls nicht kalkulierbar. Somit wäre die Kommunikation für den Eindringling nicht nur unberechenbar, sondern auch abhörsicher.

Der synchronisierte Laser des Kommunikationspartners dagegen kennt die Dynamik des sendenden Lasers, und könnte deshalb den geheimen Text rekonstruieren. Bevor dieses physikalische Prinzip allerdings für eine sichere Nachrichtenübertragung die Marktreife erlangt, ist noch intensive Grundlagenforschung erforderlich. Es kann also noch Jahre oder Jahrzehnte dauern, um tatsächlich dem Fernziel einer vollständig geheimen Nachrichtenübertragung mithilfe der Lasertechnologie näherzukommen.

***Spiegel Online / manager-magazin.de 06.02.07***