

WIRTSCHAFT & POLITIK

## Neue Serie Umwelt

FORSCHUNG & INNOVATION

## Fokus Technik: Vom Werkzeuglieferanten zum Produktionsoptimierer

# Produkte und Know-how schützen

Mit Hightech gegen Wissensabfluss,  
Produkt- und Markenpiraterie

IM BLICKPUNKT → SEITE 06

# Produkte und Know-how schützen

Juristische Maßnahmen alleine können Produktpiraterie nicht verhindern. Der Blickpunkt zeigt die Möglichkeiten auf, die sich durch den Einsatz innovativer Technologien zum Produkt- und Know-how-Schutz ergeben.

**Kennzeichnung:** Originale erkennen und wertschätzen

→ SEITE 9

**Conlmit:** Produkte präventiv schützen

→ SEITE 10

**Sick:** Qualitätssicherung hört nicht am Werktor auf

→ SEITE 12

**Siemens:** Embedded Security für intelligente Maschinen

→ SEITE 14

**Weitere Beiträge:** Track & Tracing, Embedded Security, Authentication

→ SEITEN 16-25



„Be sure it's original technology“ ist der Slogan der VDMA-Kampagne Pro-Original. Gefälschte Wasserturbinen wären für einen Staudamm fatal.

Fotos: ETIEN / Fotolia, Hadm / iStockphoto.

→ Das geistige Eigentum, das in neuen Produktideen oder Fertigungstechnologien steckt, ist ein entscheidender Faktor für den dauerhaften wirtschaftlichen Erfolg der VDMA-Mitglieder. Deshalb hat der VDMA im Rahmen seiner Strategie gegen Produktpiraterie die Arbeitsgemeinschaft Produkt- und Know-how-Schutz (AG Protect-ing) gegründet.

Diese bündelt die Interessen der Anbieter von Technologien und Dienstleistungen zum Produkt- und Know-how-Schutz und ist dabei erster Ansprechpartner im Kampf gegen Produktpiraten. Sechs Ansätze stehen in der Arbeitsge-

meinschaft Protect-ing im Fokus des Interesses:

### 1. Produkte kennzeichnen

Kennzeichnungstechnologien sind sichtbare oder unsichtbare Sicherheitsmerkmale, mit denen Produktoriginalität und -echtheit nachgewiesen werden können. Beispiele sind Hologramme, Data-Matrix-Codes, RFIDs, spezielle Druckverfahren oder Materialbeimischungen.

### 2. Geschützte Produkte authentifizieren

Um Originalprodukte zu detektieren und zu authentifizieren, sind Geräte und Sys-

teme in Entwicklung, mit denen Sicherheitsmerkmale erkannt, gelesen und auf Originalität überprüft werden. Typische Geräte sind RFID-Leser, Optosensoren oder Bildverarbeitungssysteme, die teilweise zur Überprüfung mit Online-Software und Datenbanken gekoppelt sind.

### 3. Tracking- und Tracingsysteme

Den gesamten Lebenszyklus eines Produktes anhand eines eindeutigen Sicherheitsmerkmals zu überwachen und zu verfolgen, ist das Ziel von Tracking- und Tracingsystemen. Über die enge Anbindung an die logistische Kette eines →

Foto: Fotosearch



Gemeinsamer Schutz ist wesentlich effektiver als Schutz im Alleingang.

Produktes soll das Einschleusen von Plagiaten verhindert werden. Technische Basis hierfür bilden IT-Systeme und definierte Überprüfungsstellen wie der Zoll oder Großhändler.

#### 4. Embedded Security

Das Ziel von Embedded Security in industriellen Produkten und Systemen ist der Schutz des Know-hows, das in Form von Elektronik, Software und Daten in intelligenten technischen Produkten verborgen ist. Grundlage bilden Technologien, die bereits im klassischen IT-Bereich eingesetzt und auf die industriellen An-

forderungen angepasst werden. Beispiele sind Virens Scanner und Firewalls in Steuerungsprogrammen, verschlüsselte Software und Kommunikation oder Kryptorfid's.

#### 5. Know-how-Transfer kontrollieren

Beim technischen Schutz vor unerwünschtem Know-how-Transfer geht es vor allem um IT-basierte Technologien zum Schutz von sensiblen Konstruktions-, Fertigungs- und Unternehmens-Know-how. Beispiele sind IT-Systeme zum Rechtemanagement, Zugriffsschutz, Verschlüsselung, Informationsreduktion, aber auch organisatorische Konzepte zur Erhöhung der Informationssicherheit im Unternehmen.

#### 6. Engineering und Beratung

Dienstleistungsangebote im Umfeld der Produktpiraterie sind der sechste Ansatz für den Produkt- und Know-how-Schutz. Produkthanbieter, unabhängige Berater oder Institute bieten eine Vielzahl technischer Lösungen. Für den geplanten Einsatzfall sind die Lösungsansätze etwa hinsichtlich Nutzbarkeit, Risikominimierung, Wirtschaftlichkeit oder Sicherheitsgrad zu validieren.

#### Infotag im VDMA

Die Technologien und deren innovative Entwickler sind keine Allheilmittel für jedwedes Piraterieproblem. Eine Analyse

der Anforderungen geht jeder Technologieauswahl voraus. Ob nun zur Produktverfolgung, Produkthaftung oder Kundenbindung – jede Technologie hat ihre Stärken und Schwächen, die auch vom jeweiligen Einsatzort und nicht zuletzt vom Preis abhängen.

Am 16. Februar 2011 findet in Frankfurt zum zweiten Mal der VDMA-Infotag „Technologien gegen Produktpiraterie“ statt. Dort werden die Ideen, Technologien und Lösungen für erfolgreichen Produkt- und Know-how-Schutz aus diesem Blickpunkt vorgestellt. Die begleitende Fachausstellung ist die beste Möglichkeit, sich mit den Experten und Integratoren zu vernetzen. ■

#### KONTAKT

##### Steffen Zimmermann

VDMA Produkt- und Know-how-Schutz  
Telefon +49 69 6603-1978  
steffen.zimmermann@vdma.org

#### INFO

Ein VDMA-Infotag findet am 16. Februar 2011 in Frankfurt statt (siehe dazu auch Seite 15).

#### LINK

[www.protect-ing.de](http://www.protect-ing.de)

#### STECKBRIEF



**Steffen  
Zimmermann**

#### Zuständig im VDMA für:

Produktpiraterie, Produktschutztechnologien, Know-how-Schutz, Informationssicherheit, IT-Sicherheit sowie die Arbeitsgemeinschaft Protect-ing.

#### Ausbildung/Studium:

Diplom-Wirtschaftsinformatiker,  
CISSP (Certified Information Systems Security Professional)

„Das Know-how in Produkten und Technologien ist ein entscheidender Erfolgsfaktor und deshalb sehr schützenswert.“

**Steffen Zimmermann**  
VDMA

## KENNZEICHNUNG

# Originale erkennen und wertschätzen

Um sich im Markt gegen Imitatoren zu positionieren, ist es für Hersteller wichtig, die Sicht ihrer Kunden bei der Kaufentscheidung für oder gegen ein Originalprodukt anzunehmen.

→ Heutige Kennzeichnungstechnologien ermöglichen es, Originalprodukte gerichtsfest zu identifizieren und Fälschungen nachzuweisen. Das ist sehr hilfreich, zumal sich Kunden und Anwender beim Kauf häufig unsicher sind, was sie erwerben. Oft ist auch der Mehrwert des Originals nicht direkt erkennbar. Hersteller sollten sich daher Gedanken darüber machen, welche Faktoren eine Kaufentscheidung beeinflussen.

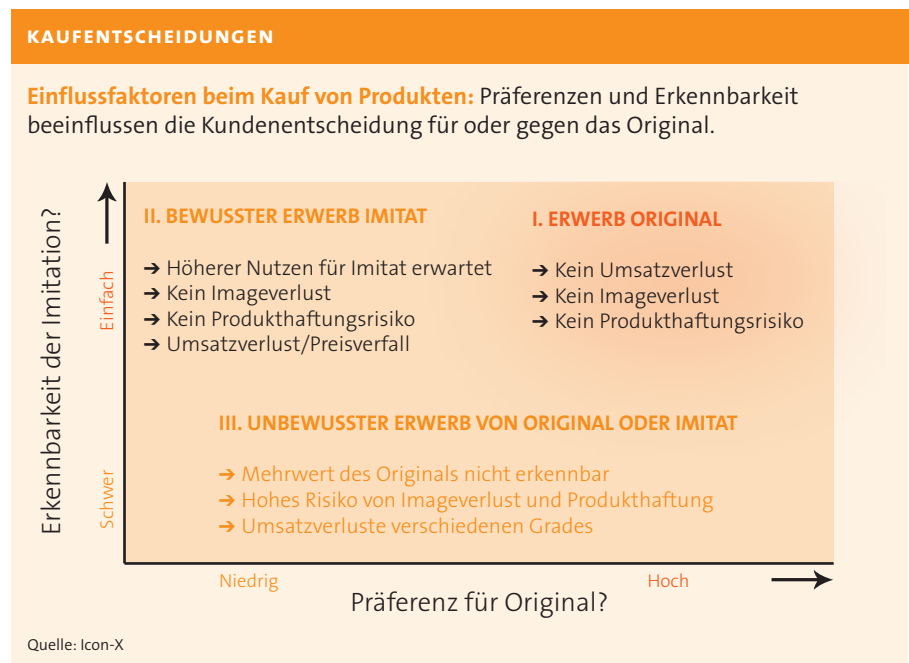
## Die Sicht des Kunden annehmen

Beim Kauf eines Produkts sind – in Abhängigkeit der Kundenpräferenzen und der Erkennbarkeit von Originalen – folgende Situationen zu unterscheiden:

- bewusster Kauf von Originalen
- bewusster Kauf von Imitationen
- unbewusster Kauf von Original oder Imitat.

Der unbewusste Erwerb von Imitaten ist für Hersteller von Originalteilen besonders schwerwiegend: Kundenerwartungen an die positiven Eigenschaften von Originalen wie Qualität und Funktion werden enttäuscht. Das Image der Marke leidet. Produkthaftungsklagen sind die Folge. Auch der umgekehrte Fall des unbewussten Kaufs von Originalen ist schädlich – der Anwender spricht dem vermeintlichen Imitat positive Eigenschaften zu und tendiert zukünftig eher zum Kauf von Imitaten.

Entscheidet sich der Kunde dagegen bewusst für den Nachbau, so verspricht er sich hiervon einen höheren wirtschaftlichen Nutzen. Ursachen sind ein zu hoher Mehrpreis oder fehlende Transparenz in den positiven Eigenschaften des Originals. Möglich ist ebenso, dass gewisse Funktionen oder Varianten des



Originals vom Kunden nicht benötigt und folglich auch nicht gewürdigt werden. Das Imitat „tut es auch“.

## Nutzen bewusst machen

Soll die Kaufentscheidung aktiv in Richtung Original gesteuert werden, müssen beide beschriebenen Fälle berücksichtigt werden. Ansätze sind:

- Produkt- und Preisgestaltung: Zu hohe Preisauflagen ohne erkennbaren Mehrwert forcieren Imitatoren. Deshalb sollten Originalteilhersteller die Anforderungen ihrer Kunden berücksichtigen, hinterfragen und einen sichtbaren Nutzen erzeugen.
- Kennzeichnung: Hersteller sollten Produkt und Verpackung an geeigneter Position kennzeichnen und die Informationen zur Authentifizierung aktiv an ihre Kunden kommunizieren.

→ Prozesse in Produktion, Beschaffung und Vertrieb sollten so gestaltet sein, dass ein unkontrollierter Abfluss von Kennzeichnungsmaterial und hiermit verbundenem Know-how verhindert wird. Zu schützen sind diese äußerst wertvollen Informationen vor jeglicher Weitergabe.

Ziel ist es, die mit dem Original verbundenen Eigenschaften zu visualisieren und den Kunden aktiv einzubeziehen. Anfänglicher Mehraufwand in der Produktentwicklung rechnet sich langfristig in einem erkennbaren Produktwert und Image. ■

## AUTORIN

**Alexandra Schulz**

ist Geschäftsführerin bei Icon-X, Detmold



Exponate auf der begleitenden Fachausstellung brachten Farbe in die Veranstaltung.

## CONIMIT

# Produkte präventiv schützen

Zehn Forschungsprojekte haben in den vergangenen drei Jahren innovative Maßnahmen für den Schutz vor Produktpiraterie entwickelt. Die Forschungsergebnisse wurden nun vorgestellt und der Industrie zur Anwendung übergeben.

„Plagiate sind eine der größten Herausforderungen für den deutschen Maschinen- und Anlagenbau.“

Dr. Hannes Hesse  
VDMA

→ Zum Schutz innovativer Ideen und Technologien startete das Bundesministerium für Bildung und Forschung (BMBF) auf Initiative des VDMA Anfang 2008 die Forschungsoffensive „Innovationen gegen Produktpiraterie“. Im Verbund aus Industrieunternehmen, Dienstleistern und Forschungseinrichtungen sollten technische und organisatorische Maßnahmen erforscht werden, um der Nachahmung von Maschinen und Ersatzteilen Einhalt zu bieten.

Am 16. November 2010 stellten die zehn Forschungsprojekte ihre Projektergebnisse im Haus der Deutschen Wirtschaft in Berlin vor. Über 300 Teilnehmer aus Industrie, Forschung und Politik nahmen an der Veranstaltung teil und informierten sich über aktuelle sowie zukünftige Möglichkeiten, aber auch Grenzen des präventiven Produktschutzes.

## Aktiv gegen Plagiate kämpfen

Ministerialrat Hermann Riehl vom BMBF und VDMA-Hauptgeschäftsführer Dr. Hannes Hesse eröffneten die Veranstaltung. Sie wiesen auf die nach wie vor wachsende Gefahr durch Produktpiraterie hin. Hesse: „Selbst in der Wirtschafts- und Finanzkrise ist der relative Umsatzverlust auf vier Prozent gestiegen. Dies entspricht etwa 6,4 Milliarden Euro Schaden. Ein Umsatz in dieser Schadenshöhe würde unserer Branche knapp 40 000 Arbeitsplätze sichern. Plagiate sind somit neben Fachkräftemangel und Ressourceneffizienz eine der größten Herausforderungen für den deutschen Maschinen- und Anlagenbau.“

Dr. Rüdiger Stihl, Vorsitzender des Aktionskreises Deutsche Wirtschaft gegen Produkt- und Markenpiraterie (APM), zeigte in seinem Vortrag mit dem plakativen Titel „Produkt- und Markenpiraterie – Krebsgeschwür der Globalisierung“ Ursachen und Auswirkungen der Produktpiraterie für die Investitionsgüterindustrie auf. „Wenn Sie bereit sind, eine Quote von fünf bis zehn Prozent Fälschungen Ihrer Produkte zu akzeptieren, setzen Sie ein falsches Zeichen. Plagiatoren müssen damit rechnen, dass ihre Taten nicht toleriert werden“, motivierte Stihl die Zuhörer, sich aktiv am Kampf gegen Plagiate zu beteiligen.

Im Mittelpunkt der Veranstaltung standen jedoch die zehn Forschungspro-



Über 300 Teilnehmer aus Industrie, Forschung und Politik nahmen an der Veranstaltung teil.

jekte sowie ihre Innovationen in den folgenden drei Handlungsfeldern:

→ Reengineering verhindern: Während des eigentlichen Produktionsprozesses, aber auch bereits in der Entwicklungsphase muss der Nachbau von Produkten und der Abfluss von kritischem Know-how verhindert werden. Mit diesem Thema beschäftigten sich die Projekte Pirat-Pro, Pro-Protect und Proactive.

→ Originalität prüfen: Sollten Plagiate in die Wertschöpfungskette einfließen oder den Endkunden erreichen, ist die Überprüfung der Originalität des vorliegenden Produkts entscheidend. Eine Möglichkeit ist es, den Produktlebenszyklus per RFID zu verfolgen, um Imitation zu verhindern. EZ-Pharm, MobilAuthent und O-Pur haben sich mit dieser Aufgabe beschäftigt.

→ Schutzkonzepte umsetzen: Erst im Verbund auf verschiedenen Ebenen lässt sich wirksamer Schutz realisieren – sei es durch rechtliche, prozessbezogene, arbeitsablaufspezifische oder organisatorische Schutzmaßnahmen. Damit haben sich die Projekte KoPiKomp, KoPira, ProAuthent und ProOriginal beschäftigt.

Im Projekt Pro-Protect ist beispielsweise ein Soft- und Hardware-Schutzkonzept entwickelt worden, mit dem Innovationen während des kompletten Produktentstehungsprozesses geschützt werden können. MobilAuthent hat eine fälschungssichere Kennzeichnung mit RFID-Tags realisiert.

Die Produktauthentifizierung lässt sich mit ortsfesten und mobilen Lesegeräten realisieren. KoPilot ist eine Software zur ersatzteilspezifischen Gefährdungsanalyse und Maßnahmenauswahl, die im Rahmen des Projektes KoPiKomp entwickelt wurde.

In drei anwenderorientierten Parallelveranstaltungen wurden die entwickelten Lösungen detaillierter vorgestellt und diskutiert. Die Inhalte der Parallelveranstaltungen orientierten sich an den drei bereits genannten Handlungsfeldern.

#### Hundertprozentiger Schutz unmöglich

Die Forschungsprojekte hatten Demonstratoren und Exponate zur Darstellung ihrer Ergebnisse mit nach Berlin gebracht, die die Teilnehmer in einer begleitenden Fachausstellung auf rund 500 Quadratmetern begutachten konnten. Die Pausen der Veranstaltung wurden für einen intensiven Erfahrungsaustausch zwischen den Projekten und den Teilnehmern der Veranstaltung genutzt.

Hochrangige Vertreter aus Wirtschaft und Wissenschaft fassten die Erkenntnisse aus den Erfahrungen der Projekte zusammen und diskutierten darüber. Es wurde herausgestellt, wie erfolgreich die Forschungsprojekte gearbeitet haben. „Einen hundertprozentigen Schutz vor Produktpiraterie wird

es wohl nicht geben“, schlussfolgerte Prof. Dr. Jürgen Gausemeier, Koordinator des Transferprojektes ConImit. „Mit den Ergebnissen der Forschungsprojekte liegen aber nun Methoden und Werkzeuge vor, mit denen jedes Unternehmen seinen eigenen Schutz vor Produktpiraterie erhöhen und das Risiko, Opfer von Plagiatoren zu werden, verringern kann“, war sein positives Resümee. Und er appellierte an die Teilnehmer der Veranstaltung: „Die deutsche Investitionsgüterindustrie ist

„Jetzt ist es an der Zeit, dass die entwickelten Lösungen zur Anwendung kommen.“

Prof. Dr. Jürgen Gausemeier  
Heinz Nixdorf Institut

hinreichend sensibilisiert für die Gefahren durch Produktpiraterie. Jetzt ist es an der Zeit, dass die entwickelten Lösungen zur Anwendung kommen.“ ■

#### AUTOREN

Martin Kokoschka und Oliver Köster

Heinz Nixdorf Institut, Universität Paderborn

#### INFO

In der Buchreihe „Innovationen gegen Produktpiraterie“ werden die Forschungsergebnisse kompakt vorgestellt. Die Bücher können über den VDMA-Shop bezogen werden. Einen Überblick über alle Forschungsprojekte gibt die ConImit-Informationsbroschüre „Produktschutz kompakt“.

#### LINKS

[www.vdma.org/produktpiraterie](http://www.vdma.org/produktpiraterie)  
[www.vdmashop.de/piraterie](http://www.vdmashop.de/piraterie)



Rainer Glatz (am Mikrofon), Geschäftsführer der VDMA-Arbeitsgemeinschaft Produkt- und Know-how-Schutz, war der Initiator der Forschungsinitiative. In einer begleitenden Fachausstellung (Bild rechts) auf 500 Quadratmetern konnten die Teilnehmer Demonstratoren und Exponate begutachten.



Foto: Sick

Kennzeichnung im Produkt: Verdeckt angebrachte Sicherheitsmerkmale erzeugen eine relativ hohe Sicherheitsstufe gegen Plagiatoren.

SICK

## Qualitätssicherung hört nicht am Werktor auf

Plagiate werden inzwischen so perfekt nachgemacht, dass sie selbst für Experten kaum noch vom Original zu unterscheiden sind. Dies macht Maschinen- und Anlagenbauern zu schaffen, denn neben finanziellem Schaden steht auch ihr Ruf auf dem Spiel.

→ Unternehmen sollten alles tun, um ihre Produkte, Komponenten und Ersatzteile eindeutig zu kennzeichnen. Dabei gilt: Je komplizierter eine Markierung zu imitieren ist, desto sicherer ist das System. Entsprechende Technologien gibt es bereits, man muss sie nur einsetzen.

### Mehrstufigen Schutzwall errichten

Schutz vor Nachahmern und Produktpiraterie ist Teil der Qualitätssicherung von Unternehmen. Mit einem mehrstufigen Schutzwall aus Sicherheitsmerkmalen können Unternehmen ihre Produkte, Komponenten und Ersatzteile schützen. Wichtigstes Ziel dabei ist es, den Aufwand für die Verifizierung so gering und für den Plagiator so hoch wie möglich zu halten. Gleichzeitig sollten alle Maßnahmen gegen Piraterie in den gesamten Produktlebenszyklus eingebunden und die Sicherheitsrichtlinien im Unternehmen gelebt werden.

Den Grad der Sicherheitsstufe kann der Maschinenbauer selbst definieren. In der niedrigsten Sicherheitsstufe kommen als Sicherheitsmerkmale Hologramme und Sicherheitsetiketten zum Einsatz. Zur Erfassung dienen Sensoren, die Farbe, Struktur und Form erkennen. Bei entsprechender Anforderung finden auch Kamerasysteme Verwendung.

Eine höhere Sicherheitsstufe wird durch eine Kombination von offenen und verdeckt angebrachten Sicherheitsmerkmalen erreicht. Neben Hologrammen und Sicherheitsetiketten können die Produkte durch UV-Farbpigmente gekennzeichnet werden. Speziell dafür ausgerichtete Sensoren können auch diese dem Kunden und Anwender nicht bekannte Kennzeichnung sicher identifizieren. So lässt sich etwa mit einem

Lumineszenzmaßstab schon bei der Produktion der Verpackung ein gewünschter Pigmentanteil einfach definieren. Im Verpackungsprozess kann damit der Empfindlichkeitswert von Lumineszenzsensoren eingestellt werden. Die Sensoren prüfen innerhalb der gesamten Logistikkette, ob das Produkt markiert ist. Eine individuelle Pigmentzusammensetzung gibt zusätzliche Sicherheit, weil es dadurch sehr aufwendig wird, die Plagiate zu erstellen.

„Bei perfekt abgestimmten Merkmalen sind Fälschungen so gut wie unmöglich.“

Detlef Deuil  
Sick

### Kombination am sichersten

Die höchste Sicherheitsstufe kombiniert technische und organisatorische Merkmale. So macht zum Beispiel ein Data-Matrix-Code mit einer nach dem Zufallsprinzip erzeugten und in einer Datenbank hinterlegten Seriennummer Produkte, Verpackungen und Ersatzteile unverwechselbar.

## PROFIL

**Sick AG, Waldkirch**

Der Hersteller von Sensoren und Sensorlösungen für industrielle Anwendungen in der Fabrik-, Logistik- und Prozessautomation zählt mit weltweit über 40 Tochtergesellschaften, zahlreichen Vertretungen sowie mehreren Beteiligungen zu den Technologie- und Marktführern seiner Branche. Umsatz (2009): 596,8 Millionen Euro, Mitarbeiter: 5 000

## LINK

[www.sick.com](http://www.sick.com)

Jeder Code wird weltweit nur einmal vergeben. Zoll und Servicemitarbeiter können die geheimen Herstellerinforma-

tionen bei Bedarf mit mobilen 2-D-Handscannern auslesen und über Funk oder USB-Schnittstelle mit der Datenbank vergleichen.

Für die Produktion bedeutet dies aber auch eine Umstellung. Entgegen der bisherigen Praxis müssen bei der Verpackung jetzt überall Einzelprodukte statt Paletten gekennzeichnet und registriert werden. Bei Produktionsraten von zuweilen 300 bis 400 Verpackungen pro Minute schaffen dies nur kamerabasierte Codeleser. Hier erfasst eine Matrixkamera in Kombination mit intelligenten Dekodieralgorithmen noch Objekte sicher, die sich mit einer Geschwindigkeit von vier bis sechs Metern pro Sekunde am Sensor vorbeibewegen. Ist der Code fehlerhaft aufgedruckt, wird die Maschinensteuerung informiert und das Produkt ausgeschleust. Die 2-D-Scanner haben inzwischen eine Lesesicherheit von mindestens 99,97 Pro-

zent, je nach Produktions- und Umgebungsbedingungen ist diese sogar noch besser.

Wenn alle Sicherheitsmerkmale auf die Anforderungen perfekt abgestimmt sind, ist es kaum noch möglich, das Original 100-prozentig zu imitieren. Kunden oder Servicemitarbeiter können die Sicherheitsmerkmale von Tools, Komponenten oder Ersatzteilen per Handscanner oder halbautomatisch an der Maschine erkennen. So verifizieren sie die Echtheit der Bauteile schnell und unterbrechen die Produktion nur kurz. ■

## AUTOREN

**Detlef Deuil**

Leiter 2D-Code Reader & Hand-held-Line,

**Danny Mangelschots**

Sales Engineer, und

**Simone Klausmann**

Produktmanagerin Automatisierungstechnik bei der Sick AG, Waldkirch

## Komplett kombinierbar

### Bohr-, Reib-, Gewinde- und Fräswerkzeuge für ihre Teile- und Komponentenbearbeitung

- Intelligent kombinierte Standard- und Sonderwerkzeuge
- Aufeinander abgestimmte und optimierte Arbeitsschritte
- Einsparung von Nebenzeiten durch möglichst wenige Werkzeugwechsel



**KOMET**<sup>®</sup>  
GROUP

**Bearbeitungsbeispiel:**  
Optimierte Komplettbearbeitung eines LKW-Kupplungsgehäuses aus Aluminium

Entdecken Sie weitere Komplettbearbeitungsbeispiele unter [www.kometgroup.com/branchenloesungen](http://www.kometgroup.com/branchenloesungen)

## Unser PLUS.

Sie kennen die KOMET GROUP als Hersteller von Premium-Werkzeugen und Sie kennen die Ideen in unseren Lösungen. Entdecken Sie ein unvergleichliches Mehr, das Ihnen dauerhafte und nachhaltige Vorteile bietet. Wir nennen es TOOLS+IDEAS. Zukunftsweisende Dienstleistungen, einzigartiger technischer Support und praxisorientierte Fachseminare.

TOOLS+IDEAS™



Fotos: Siemens

Um auch künftig sichere und verlässliche Automatisierungslösungen zu gewährleisten, hat Siemens ein konsequentes Security-Programm installiert.

SIEMENS

## Embedded Security für intelligente Maschinen

Die unterschiedlichen Sparten von Siemens haben verschiedene Sicherheitsanforderungen und müssen demnach individuelle Lösungen verfolgen – viele sind bereits erfolgreich im Einsatz.

→ In der modernen Fertigungs- und Prozessindustrie tragen intelligente Maschinen und durchgängige Automatisierungssysteme entscheidend dazu bei, dass die Produktivität nachhaltig steigt und sich die Wettbewerbsfähigkeit hinsichtlich Zeit, Kosten und Qualität nach-

haltig verbessert. Siemens setzt hier seit vielen Jahren Maßstäbe mit Lösungen, die sich flexibel an die gegebenen Anforderungen anpassen.

### Gestiegene Security-Anforderungen

Hinsichtlich der Systemsicherheit bringt die zunehmende IT-Integration in der Automatisierung allerdings erhebliche Herausforderungen mit sich; Angriffspunkte ergeben sich durch die steigende Komplexität und Vernetzung der Systeme. Zudem werden Hackerattacken gegen Industriesysteme immer professioneller und zielgerichteter. Das Schadenspotenzial wächst weiter, wenn kritische Infrastrukturen und Kontrollsysteme wie im Fall des Coputerwurms Stuxnet angegriffen werden.

Auch aus Sicht des Markts sind die Anforderungen an Security in der Automatisierung stark gestiegen. Vor allem der Schutz proprietären Know-hows

muss gewährleistet werden, und zwar sowohl für Siemens als auch für OEM (Original Equipment Manufacturer), Systemintegratoren und Endkunden mit ihrem spezifischen Fachwissen. Nachgewiesene Integrität der Systeme und Authentifizierung von Systemkomponenten ermöglichen einen wirksamen Schutz gegen Plagiate; insbesondere für die Einhaltung der funktionalen Sicherheit kann dies unerlässlich sein. Darüber hinaus ist die sichere Kommunikation einschließlich der Machine-to-Machine-Communication auf allen Ebenen von entscheidender Bedeutung.

Um die Ziele Systemintegrität, Authentizität und Vertraulichkeit sicherzustellen, wird ein umfassendes Security-Konzept mit angepassten kryptografischen Methoden und geeigneten organisatorischen Prozessen benötigt. Wesentlicher Bestandteil ist dabei adäquate „Embedded Security“ in den Systemkomponenten – ein Tool-

„Die zunehmende IT-Integration in der Automatisierung bringt große Herausforderungen mit sich.“

Dr. Ariane Sutor  
Siemens



## VDMA-INFOTAG

**Technologien gegen Produktpiraterie  
am 16. Februar 2011**

Auf dem Infotag zeigen Technologieanbieter ihre Lösungen aus der Praxis. Eine begleitende Fachausstellung lädt zum „Anfassen“ ein.

Ein umfassender Schutz vor Produktpiraterie und Know-how-Abfluss ist nur durch eine Integration von konstruktiven, produktionsbezogenen und IT-basierten Ansätzen zu erreichen. Die Möglichkeiten, aber auch die Grenzen von technischen Schutzmaßnahmen sind oft noch nicht bei den Unternehmen bekannt. Deshalb informieren sie sich über präventive Schutzmaßnahmen gegen Produktpiraterie und ungewollten Know-how-Transfer, um eine eigene Abwehrstrategie zu finden und den Kampf gegen die Kopierer für sich zu entscheiden.

Die Tagungsteilnehmer erhalten die Möglichkeit, sich mit Lösungsanbietern gezielt zu vernetzen. Die Technologien und Lösungen stammen etwa aus den Bereichen Produktkennzeichnungen, Track & Trace, RFID, Know-how-Schutz und Embedded Security. Alle Produkte sind bereits erfolgreich im Einsatz. Die begleitende Ausstellung bietet Gelegenheit, die klugen Köpfe hinter den Ideen näher kennenzulernen.

Die Teilnehmerzahl ist begrenzt. Programm und Anmeldung sind erhältlich bei [biljana.gabric@vdma.org](mailto:biljana.gabric@vdma.org).

## KONTAKT

**Steffen Zimmermann**

VDMA Produkt- und Know-how-Schutz  
Telefon +49 69 6603-1978  
[steffen.zimmermann@vdma.org](mailto:steffen.zimmermann@vdma.org)

## LINK

[www.protect-ing.de](http://www.protect-ing.de)

set aus Hardware und Software mit sicherem Speicher, Konzepten für Public-Key-Kryptografie, Blockchiffren, Hash-Funktionen und Zufallszahlen. Eine spezielle Security-Hardware ermöglicht das höhere Sicherheitsniveau; reine Softwarelösungen haben dagegen das Problem, dass geheime Schlüssel gegebenenfalls im Code „versteckt“ werden müssen.

Die jeweiligen Randbedingungen einer Anwendung bestimmen die spezielle Wahl eines Konzepts und der einzusetzenden Methoden. Entscheidend sind insbesondere Kosten, Performance und Flexibilität, aber auch die Usability während des kompletten Lebenszyklus wird

immer wichtiger. Bestandteile eines individuellen Toolsets sind beispielsweise eine umfangreiche Softwarebibliothek mit kryptografischen Verfahren, ein Security-Controller und ein Low-Cost-Chip zur Authentisierung.

**Datenänderungen unmöglich machen**

Siemens setzt bei der Implementierung des Toolsets bei Public-Key-Kryptografie auf Elliptic Curve Cryptography (ECC) als konzernweiten Blueprint. Hierbei kommt unter anderem ein patentiertes ECC-Verfahren der Siemens AG Corporate Technology zum Einsatz, das eine unbemerkte Änderung von Systemkonfigurationen unmöglich macht.

Um auch künftig sichere und verlässliche Automatisierungslösungen zu gewährleisten, hat Siemens eine durchgehende Security Roadmap für seine Lösung erstellt. Darüber hinaus installiert das Unternehmen ein konzernweites Security-Programm. Ein übergreifendes Programm stellt harmonisierte und ganzheitliche Lösungen sicher – für eine umfassende Sicherheit. ■

## AUTORIN

**Dr. Ariane Sutor**

Program Manager Cryptography Corporate Technology bei der Siemens AG, München

## PROFIL

**Siemens AG, Berlin und München**

Weltweit entwickelt und fertigt das Unternehmen Systeme und Anlagen und bietet so seinen Kunden maßgeschneiderte Lösungen an. Mit seinen Aktivitäten auf den Gebieten Industrie, Energie und Gesundheit ist Siemens weltweit führend.

Umsatz 2009: 76,65 Milliarden Euro,  
Mitarbeiter: rund 400 000

## LINK

[www.siemens.com](http://www.siemens.com)



Foto: Tailorlux

Gewusst wie: Leuchtstoffe können eingesetzt werden, um Produkte eindeutig zu kennzeichnen.

#### KENNZEICHNUNG

## Mit Leuchtstoffen schützen

Eine Kennzeichnung, die langlebiger als Granit und bis 1 700 Grad Celsius unzerstörbar ist, macht den gerichtsfesten Nachweis von Originalität und Herkunft von Produkten möglich.

→ Wer durch ein Teleskop ferne Sterne und Planeten beobachtet, sieht die Himmelskörper in den unterschiedlichsten Farben leuchten. Astronomen nutzen das Leuchten der Sterne zur sicheren Identifizierung ihres Beobachtungsobjektes. Um diesen Effekt für den gerichtsfesten Produktschutz zu nutzen, haben die Forscher der Tailorlux GmbH ein zum Patentschutz

angemeldet Verfahren entwickelt. Mit Hilfe von speziellen Markierungsstoffen lässt das Verfahren Ersatzteile, Komponenten und sogar ganze Maschinen als Originale erstrahlen.

#### Schutz durch Leuchtstoffe

Genutzt werden dafür keine extraterrestrischen Materialien, sondern ein Gemisch mehrerer Leuchtstoffe, sogenannter Pigmente, die in Kombination eine charakteristische und eindeutige Leuchtspur auf einem Spektrometer hinterlassen. Dank Milliarden von Kombinationsmöglichkeiten ergibt sich so ein sicherer und unverfälschlicher Herkunftsnachweis. Eine Veränderung der Eigenschaften des zu schützenden Produkts ist dabei ausgeschlossen. Das Produkt selbst wird nun zum Träger der untrennbaren Originalitätskennzeichnung. Zudem sind die Leuchtpigmente toxikologisch unbedenklich, was den Einsatz nicht nur in Maschinenteilen erlaubt.

„Mit wenigen Gramm des Pulvers lassen sich mehrere Kilogramm Werkstoff schützen.“

Prof. Dr. Thomas Jüstel  
Tailorlux

#### Auf der Messe identifizieren

Ein Original kann man mit preiswerten Standard-Spektrometern identifizieren. Dazu nutzt man das Spektrum des von den Pigmenten ausgesendeten Lichts. Dank der Leuchtstoffe wird für jedes Produkt ein eindeutiger Lichtcode empfangen, der weder gefälscht noch mit den gleichen Leuchtstoffen erneut produziert werden kann, denn auch jede Charge des Markierungspulvers ist ein Unikat des chemischen Herstellungsprozesses.

Die Vorteile der Technologie sind immens: Mit wenigen Gramm des Markierungspulvers lassen sich mehrere Kilogramm Werkstoff schützen – je nach Anwendungsgebiet mehr als das 1 000-Fache des Ausgangsmaterials. Im Bereich der hochwertigen und herstellerbezogenen Ersatzteile kann der Schutz direkt in Kunststoffbauteilen, Keramiken, Farben und gegebenenfalls Lacken eingebracht werden. Für eine erste Beurteilung der Originalität reicht schon eine Spezialtaschenlampe. So können Anwender auf Messen mit bloßem Auge eine Fälschung erkennen.

#### Gerichtsfesten Nachweis erbringen

Zur gerichtlichen Verwertbarkeit besitzt jedes verwendete Leuchtpigment weitere Eigenschaften, die mit größeren Messgeräten überprüft werden können. Hierzu gehört zum Beispiel das thermische oder zeitliche Verhalten der eingesetzten Pigmente. Diese Methode eignet sich so nicht nur zur sicheren Identifizierung eines bestimmten Produkts, sondern kann vielmehr auch als Prüfsubstanz zur Sicherstellung der Herkunft eingebrachter Materialien benutzt werden. Dies ist insbesondere für den Schutz vor unbegründeten Reklamationen sinnvoll. Der Nachweis der Leuchtpigmente gelingt auch noch nach Brand, Abrieb oder mutwilliger Zerstörung. ■

#### AUTOR

Alex Deitermann

ist Geschäftsführer der Tailorlux GmbH, Steinfurt

## TRACK &amp; TRACING

# Ersatzteile fälschungssicher zurückverfolgen

Mikro-Farbcodes kombinieren zwei Funktionen: Fälschungssicherheit und Rückverfolgbarkeit von Ersatz- und Verschleißteilen, die besonders anfällig sind.

→ Die Lieferkette von Ersatzteilen ist oft lang und führt über viele verschiedene Zwischenhändler. Auch wenn Container, Verpackungen, Einzelteile und sogar Lieferpapiere auf den ersten Blick genau gekennzeichnet sind, können sich dahinter minderwertige Plagiate verbergen. Denn Fälscher befinden sich technisch häufig auf dem gleichen Stand wie die produzierenden Unternehmen: Sicherheitsmerkmale werden fast genauso schnell gefälscht, wie sie auf den Markt gelangen.

## Besonders anfällige Ersatzteile

Fälschungen reichen von Erzeugnissen aus Überproduktion, die mit dem Logo

des Originalherstellers versehen werden, über gänzlich nachgemachte Teile bis hin zu gefälschten Verpackungen und Etiketten. Besonders anfällig sind Ersatz- und Verschleißteile, die häufig ausgetauscht werden müssen. Mit ihnen werden im Maschinenbau die größten Margen erzielt. Fehlerhafte Lenkungssysteme, Lager und Getriebe, poröse Dichtungen, Zylinder, Ventile, Filter und Kolben sind nur einige Beispiele von Ersatzteilen, die in großen Mengen nachgebaut und in die Lieferkette eingeschleust oder über das Internet vertrieben werden.

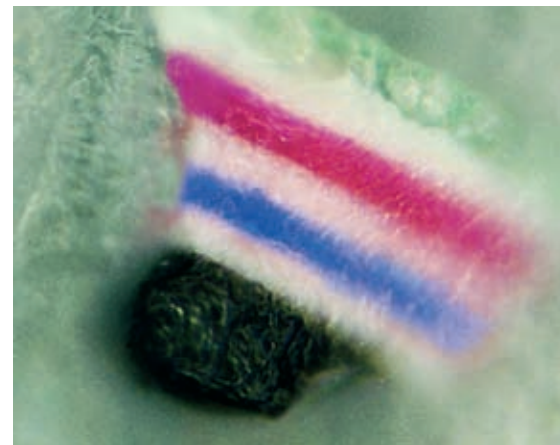
Der Leidtragende ist zuallererst der Kunde, der die Teile einbaut und dem durch minderwertige Qualität Schäden an seinen Maschinen entstehen können.

## Unternehmen in der Pflicht

Erfahrungen aus dem Maschinenbau zeigen, dass Plagiate um 40 bis 70 Prozent unter dem Preis der Originalartikel vertrieben werden. Für den Hersteller bedeutet das immense Umsatzeinbußen. Ebenfalls teuer kommen ihn langwierige Produkthaftungsprozesse zu stehen.

Gelangen gefälschte Teile unter dem Namen des Originalherstellers in den Handel, haftet jener für entstandene Schäden, sofern sich nicht eindeutig zurückverfolgen lässt, dass die gefälschten Teile nicht von ihm produziert oder vertrieben werden. Gelingt dies nicht, muss der Hersteller mit zusätzlichen Schadenersatzzahlungen rechnen.

1. Gesicherte Ersatzteile werden anhand ihres Mikro-Farbcodes eindeutig als Originale identifiziert.
2. Die Kombination aus Rückverfolgbarkeit und fälschungssicheren Mikro-Farbcodes legt Fälscherbanden das Handwerk.



Ein Mikro-Farbcodes ermöglicht es, kleinste Teile rechtssicher zu schützen.

## Fälschungssichere Traceability

Vor diesem Hintergrund wird es für Unternehmen immer wichtiger, eine Sicherheitsstrategie zu implementieren, die sowohl die Fälschungssicherheit als auch die Rückverfolgbarkeit gewährleistet. Zwar wird die Rückverfolgbarkeit (Traceability) etwa durch Data-Matrix-Codes und RFID möglich. Doch diese Merkmale sind nicht per se fälschungssicher. Deshalb hat die 3S GmbH, Nottuln auf der Grundlage ihrer Mikro-Farbcodes eine Systemlösung entwickelt, die Fälschungssicherheit und Rückverfolgbarkeit kombiniert. Die Hinterlegung der Informationen in Datenbanken gewährleistet eine leichte Überprüfung sowie, eine eindeutige Identifizierung und hilft den Zollbehörden bei der Durchführung von Grenzbeschlagnahmeverfahren. ■

## AUTOR

### Rolf Simons

Geschäftsführer der 3S Simons Security Systems GmbH, Nottuln

Foto: 3S



1



2

## TRACK &amp; TRACING

# Der Ware mit integriertem RFID auf der Spur

Ein individueller Code auf jedem einzelnen Produkt in Verbindung mit einem fälschungssicheren Kennzeichnungsetikett ermöglicht es, auf mehreren Ebenen Informationen zu speichern, die zum Teil mit dem bloßen Auge, der Lupe oder nur maschinell ausgelesen werden können.

→ 600 Milliarden US-Dollar Umsatz machen Fälscher jährlich weltweit mit Produktplagiaten, schätzt die Internationale Industrie- und Handelskammer – Tendenz steigend. Die Fälschungen schmälern Image und Gewinn der Originalhersteller und gefährden – etwa bei Medikamenten oder Autoersatzteilen – auch Leib und Leben der Endkunden. Für Originalhersteller sind wirksame Schutzmaßnahmen wichtig, um das Eindringen von Fälschungen in die Lieferkette auszuschließen, indem die Echtheit der Ware für jedermann eindeutig sichtbar gemacht wird.

Hier treffen klassische Logistikansprüche auf Anforderungen des Produktschutzes. Für Logistiker ist es ent-

scheidend, den Weg jedes einzelnen Produkts von der Herstellung bis zum Vertriebspartner genau verfolgen zu können.

### Produktherkunft wichtig

Für die Maschinen- und Anlagenbauer ist die Frage der Produktherkunft beziehungsweise der Nachweis der Originalität wichtig, da Haftungsfragen zunehmend in den Vordergrund treten und den Unternehmen viel Geld kosten können. Logistiker und Maschinenbauer sind deshalb daran interessiert, Originale schnell und sicher von Fälschungen zu unterscheiden und Graumarktware zu erkennen.

„Die Produktkennzeichnung macht nur einen Teil des Produktschutzes aus.“

Volker Hahn  
tesa scribos

Die tesa scribos GmbH, Spezialist für Produktschutz und -identifikation, hat ein Konzept entwickelt, das Produktverfolgung und Originalitätsnachweis verbindet.

### Individueller Code

Kern ist eine physisch gesicherte Codierung. Jedes Produkt bekommt einen individuellen Code zugewiesen und wird mit einem fälschungssicheren Kennzeichnungsetikett versehen. Dieses speichert auf mehreren Ebenen Informationen, die zum Teil mit dem bloßen Auge, der Lupe oder nur maschinell ausgelesen werden können. Sicherheit wird direkt auf dem Produkt oder der Verpackung angebracht – zur sofortigen Überprüfung der Echtheit sowie Produktverfolgung.

Eine andere Möglichkeit ist die sichere Produktkennzeichnung per RFID (Radio Frequency Identification), wie sie der Sensorspezialist Balluff GmbH anbietet. Hierbei geht es speziell im Maschinen- und Anlagenbau weniger um den Plagiatschutz ganzer Anlagen, sondern um die Kennzeichnung von oft gefälschten Einzelkomponenten oder Ersatzteilen. Dabei lassen sich dann neben der Identifikation auch noch zusätzliche Informationen wie Einstelldaten oder Serviceinformationen hinterlegen.

Ähnliches gilt auch für das bereits erwähnte „Trust-&-Trace“-Konzept, das sich problemlos in bestehende Logistikprozesse einbinden lässt. Warenverfolgungssysteme auf der Basis von Kennzeichnungstechnologien wie 2-D-Matrix-Codes, Barcodes oder RFID- und NFC-Technologie werden dabei einfach in den Produktschutz integriert.



Jedes Produkt bekommt einen individuellen Code zugewiesen und wird mit einem fälschungssicheren Kennzeichnungsetikett versehen.



Foto: Balluff

Eine sichere Produktkennzeichnung mittels RFID funktioniert auch in rauer Umgebung (Beispiel Tool-ID).

Egal, für welche Kennzeichnungstechnologie man sich entscheidet, es lassen sich Aufträge durch die Anbindung zusätzlicher IT-Systeme wie SAP oder Zolldatenbanken einzeln zuordnen und nachverfolgen. In der Logistik liefern die Systeme verlässliche Daten für Qualitätskontrolle und Rückrufaktionen. Auch die Vorteile für den Produktschutz liegen auf der Hand: Alle Beteiligten in der Logistik, Mitarbeiter der Zollbehörden, Vertriebspartner oder auch Endverbraucher, können die Echt-

„Die Anbindung zusätzlicher IT-Systeme liefert verlässliche Daten für eine Qualitätskontrolle und Rückrufaktionen.“

Ralf Pfisterer  
Balluff

heit, Herkunft und Vertriebswege eines Produkts jederzeit feststellen.

#### Schützenswerte Teile richtig wählen

Die Produktkennzeichnung macht jedoch nur einen Teil des Produktschutzes aus. Ein anderer wichtiger Part ist die richtige Auswahl der zu schützenden Komponenten und Teile, unabhängig davon, für welches Verfahren man sich entscheidet. Geklärt sein muss dabei auch, mit welchen Maßnahmen man auf derartige Verstöße reagieren will.

Im Maschinen- und Anlagenbau ist dies bei der Nutzung des RFID-Systems von Balluff beispielsweise eine automatische Drosselung der Maschinenleistung oder ein Logfile zur Dokumentation der gefälschten Komponenten. Besonders wichtig ist dies vor allem dann, wenn durch den Einsatz von Plagiaten die Qualität der Produkte leidet oder gar Menschen zu Schaden kommen können.

Ähnliche Lösungen sind auch mit einem selbstklebenden Fälschungsschutzetikett realisierbar, das sich mit Kundenbindungsprogrammen verknüpfen lässt. Kunden, die sich mit dem Code des Sicherheitsetiketts auf einer Internetseite registrieren, bekommen die Echtheit des Produkte bestätigt und eine Garantieverlängerung eingeräumt. ■

#### PROFIL

##### Balluff GmbH, Neuhausen

Der 1921 gegründete Hersteller von Sensortechnik für die industrielle Automatisierung sowie von Connectivity- und Networking-Lösungen bietet ein komplettes Sortiment an hochwertigen Sensoren, Wegmess- und RFID-Systemen, Zubehör und anwendungsspezifischen Kundenlösungen für alle Bereiche der Fabrikautomation an. Das Unternehmen unterhält 30 Vertretungen weltweit. Umsatz: 250 Millionen Euro, Mitarbeiter: 2 200

LINK  
[www.balluff.com](http://www.balluff.com)

#### AUTOREN

##### Volker Hahn

Marketing Manager bei der tesa scribos GmbH, Hamburg

##### Ralf Pfisterer

Referent RFID und Produktschutz bei der Balluff GmbH, Neuhausen

## CHINA

# Chancen und Risiken im Chinageschäft

China gilt als einer der stärksten „Know-how-Sammler“ weltweit und ist zugleich auch Betroffener. Diese Ausgangslage bietet eine Lern- und Entwicklungsplattform für deutsche Maschinen- und Anlagenbauer – an erster Stelle steht aber weiterhin die Absicherung des eigenen Wissens.



Fotos: Onitjij / Fotolia, Luca di Filippo, Doug Berry / iStockphoto

Auch chinesische Hersteller sind an deutschen Produkten zum Know-how- und Produktschutz interessiert.

→ Die guten Beziehungen zwischen der Volksrepublik China und der Bundesrepublik sowie die exportorientierte deutsche Wirtschaft begünstigen seit Jahren einen intensiven, in aller Regel einseitigen Abfluss von Know-how aus allen innovativen Technologien in Richtung China. Das Bestreben Chinas, bis zum Jahr 2020 den USA wirtschaftlich und militärisch auf Augenhöhe gegenüberzutreten zu können, soll auch durch Beschaffung von Spitzentechnologie aus dem Westen gelingen.

Daher versucht das Land, auf diversen Wegen entsprechendes Know-how zu beschaffen, um die Technologielücken zu schließen, die in vielen Bereichen noch bestehen. Besonders betroffen ist der Maschinen- und Anlagenbau: Zwei Drittel aller befragten Mitgliedsunternehmen des VDMA beschwerten sich über Produkt-

piraten; 75 Prozent der Geschädigten zeigen dabei mit dem Finger nach China.

## Risiken im Chinageschäft

Als konkrete Bedrohungen in diesem Zusammenhang sind zu nennen:

- die Gefahr des Know-how-Abflusses durch chinesische Mitarbeiter – die Loyalität von Chinesen zu ihrem Heimatland ist in der Regel stärker als die zum Arbeitgeber, weswegen sich eine enge Bindung an das Unternehmen nur schwer erreichen lässt
- die Verpflichtung zur Offenlegung von Prozess- und Maschineninformationen bei verschiedenen chinesischen Behörden, zum Beispiel bei Planungs- und Umbaumaßnahmen



- der Zwang, Importwaren einem Zertifizierungsverfahren zu unterwerfen und bei technischen Projekten detaillierte Dokumentationen an sogenannte chinesische Design-Institute weiterzugeben
- internetbasierte Angriffe auf Computersysteme und mobile Kommunikation.

## Chancen für deutsche Unternehmen

Die beschriebene Ausgangslage kann jedoch auch Chancen für deutsche Unternehmen eröffnen. Beispielsweise kann es von Vorteil sein, sich im Rahmen von Überlegungen zum Know-how-Schutz der hauseigenen „Kronjuwelen“ bewusst zu werden und sich in der Folge strategischer am Markt zu positionieren.

Darüber hinaus sind chinesische Unternehmen in zunehmendem Maße selbst von Produktfälschungen beziehungsweise Know-how-Verlust betroffen. Somit eröffnen sich Möglichkeiten, den chinesischen Markt für deutsche Produkte zum Know-how- und Produktschutz zu nutzen. Hier wäre unter anderem an lernende Know-how-Schutz-Systeme (gebunden an interkulturelle Kompetenzen) und Technologien zum Schutz der chinesischen Wirtschaft vor Nachahmern zu denken. ■

## AUTOR

**Peter Mnich**

Senior Consultant bei der Viccon GmbH, Ettlingen

## EMBEDDED SECURITY

## Vom Wurm Stuxnet lernen

Der Schutz von Produktionsdaten gewinnt an Bedeutung. Moderne IT beziehungsweise Schutzsysteme können helfen, Produktpiraterie zu reduzieren und den Know-how-Vorsprung länger vor dem globalen Wettbewerb zu schützen.

→ Immer mehr Funktionalität in Maschinen und Anlagen wird durch Software realisiert, die in fest integrierten Embedded-Systemen und Industrie-PCs steckt. Nach einer aktuellen VDMA-Studie sind 45 Prozent der deutschen Hersteller vom Nachbau kompletter Maschinen betroffen. Auch Serviceunterlagen und digitale Maschinentagebücher enthalten schützenswertes Know-how.

### Fünf Ziele für die nahe Zukunft

→ Schutz des geistigen Eigentums vor Reverse Engineering: Wertvolles Know-how in Algorithmen und Verfahren wird so geschützt, dass die Steuerung den Programmcode zwar ausführen, aber nicht analysieren oder disassemblieren kann.

→ Nachbau von Maschine und Geräten erschweren: Die eingebaute „Embedded Software“ läuft nur, wenn die passende Lizenz in der Steuerung oder dem Industrie-PC vorhanden ist. Eine Programmkopie von einer Festplatte oder Speicherkarte dagegen funktioniert in einem anderen System nicht.

→ Neue Geschäftsmodelle im Maschinenbau ermöglichen: Durch flexible und modulare Lizenzierung der Embedded-Software werden neue Geschäftsmodelle möglich, wie Pay-per-Use oder Feature-on-Demand. Oft müssen Maschinen aufgrund des Preisdrucks in einer sehr günstigen Basisversion angeboten werden. Einzigartige und zusätzliche Leistungsmerkmale und Funktionen werden zusätzlich verkauft. Auch Miet- und Leasingmodelle sind möglich, indem die Nutzung verschiedener Funktionen gemessen oder einfach nur nach

Zeit lizenziert wird. So muss der Nutzungsvertrag alle drei Monate verlängert werden. Nach der Zahlung wird die Funktion der Maschine wieder aktiviert.

→ Schutz von Daten: Neben der reinen Software können auch Daten geschützt werden. Die Möglichkeit, mit Maschinen auch geschützte Produktionsdaten zu verarbeiten, ist ein Wettbewerbsvorteil für den Maschinenhersteller. Dem späteren Auftraggeber ermöglicht es, seine Produktionsdaten einer Lizenz für die beauftragte Stückzahl zuzuordnen und dem Fertiger geschützt zu übergeben. Nach dem Erreichen dieser Stückzahl kann die Maschine nicht weiterproduzieren – die unbemerkte Herstellung von Graumarktprodukten ist damit ausgeschlossen.

→ Gesteigerte Systemsicherheit und Zuverlässigkeit: Der erstmalige Angriff



Mit den Smart-Card-basierten Hardwarevarianten der Wibu-Lösung können Hersteller ihr Know-how schützen und Produktpiraterie reduzieren.

## PROFIL

### Wibu-Systems AG, Karlsruhe

Das 1989 gegründete Unternehmen hat sich auf Digital-Rights-Management, Softwareschutz, Lizenzmanagement, Dokumentenschutz, Schutz von Mediadaten und Zugangsschutz spezialisiert und ist weltweit vertreten.

## LINK

[www.wibu.de](http://www.wibu.de)

auf Industriesysteme im Sommer 2010 durch den Computerwurm „Stuxnet“ verstärkt die Wünsche nach sicherem Integritätsschutz. Dieser kann durch Schutzsysteme mittels digitaler Signaturen gesichert werden, sogenanntes „Anti-Tampering“. Wichtig ist, dass die Sicherheit nicht an einem einzigen geheimen Schlüssel hängt, der durch Social Engineering ermittelt werden kann. ■

## AUTOR

### Oliver Winzenried

ist Vorstand der Wibu-Systems AG, Karlsruhe und stellvertretender Vorsitzender der VDMA-Arbeitsgemeinschaft Protect-Ing.



Prüfung mit mobilem Endgerät: Produkte werden bereits bei der Herstellung mit einem Code gekennzeichnet.

#### Daten auf Abruf

Die eindeutige Kennzeichnung des Produkts erlaubt nicht nur eine Echtheitsprüfung. Auch komplexe Track- & Trace-Szenarien wie die Nachverfolgung eines Produkts über unterschiedliche Logistikanbieter und Ländergrenzen hinweg sind umsetzbar. Der Hersteller erreicht damit ein Maximum an Transparenz in seiner Lieferkette und erhält die Möglichkeit, den Warenfluss zu optimieren.

#### Direkte Kommunikation mit dem Kunden

Die stückbasierte Datenhaltung bei Produkten öffnet einen direkten Kanal zum Endkunden und liefert damit einen wichtigen Mehrwert in der Kundenkommunikation. Mittels Mobiltelefonen können Informationen aus der zentralen Datenbank ausgelesen werden. Die abgerufenen Daten können Track- & Trace-basiert sein und etwa Nachhaltigkeitsaspekte einer Produktion kommunizieren, indem Lieferwege oder Herstellungsprozesse dargestellt werden. Auch ein Feedbackkanal oder kampagnenbasierte Aktionen wie Rabattangebote sind denkbar.

#### Fachpersonal informieren

Selbst dem Fachpersonal wie Servicetechnikern oder Reparaturteams können aktuelle Informationen übermittelt werden. Wiederum werden vorhandene Kennzeichnungstechnologien dazu verwendet, den Informationsaustausch mit der zentralen Datenbank zu starten und besondere Wartungshinweise, Einbauvorschriften oder Garantiehinweise zu kommunizieren. ■

#### AUTOR

##### Henrik Stammer

ist Mitglied der Geschäftsführung der Original1 GmbH, Frankfurt am Main und Vorstandsvorsitzender der Arbeitsgemeinschaft Protect-ing.

#### TRACK & TRACE

## Aktiv für mehr Produktsicherheit

In Zeiten zunehmender Produktpiraterie stellt eine Lösung zur eindeutigen Produktverfolgung und -authentifizierung einen wertvollen Beitrag zu mehr Produkt- und Markensicherheit dar.

→ Dass Produktfälschungen ein weltweit zunehmendes Problem darstellen, wird häufig in den Medien berichtet. Betroffen ist auch das produzierende Gewerbe mit alarmierenden Folgen für die Verbraucher. Für Unternehmen stellt sich daher die Frage, was sie unternehmen können, um ihre Produkte zuverlässig zu verfolgen.

#### Produktverfolgung anhand von Codes

Die SAP AG, Walldorf hat gemeinsam mit einem großen Hersteller von Mobiltelefonen sowie der Giesecke & Devrient GmbH, München das Joint Venture „Original1“ gegründet. Dank der gebündelten Kompetenz und innovativen Gründertechnologie kann nun ein Komplettservice rund um Registrierung, Nachverfolgung und Echtheitsprüfung von Marken und Produkten angeboten werden.

Eine zentrale Rolle bei der Verfolgung und Authentifizierung von Produkten spielen Kennzeichnungstechnologien wie RFID-Tags, digitale Graubilder (CDP) oder 2-D-Barcodes. Jedes Produkt erhält vom Hersteller eine solche Kennzeichnung mit eindeutig identifizierbarem Code, der direkt bei der Herstellung in einer zentralen Datenbank registriert wird. Ab diesem Zeitpunkt ist das Produkt dem System bekannt, es können zusätzliche Informationen wie Texte, Bilder oder Videos verknüpft werden und das Produkt kann mit mobilen Endgeräten, dem PC oder einem Kassensystem gescannt und auf Echtheit geprüft werden.

„Kennzeichnungstechnologien spielen bei der Verfolgung und Authentifizierung von Produkten eine zentrale Rolle.“

Henrik Stammer  
Original1

## TRACK, TRACE &amp; AUTHENTICATION

# Für eine fälschungssichere Zukunft

Bei Track-, Trace- & Authentication-Lösungen spielen neben Expertise in Consulting und Implementierung auch nachhaltige Technologien eine entscheidende Rolle.

→ Eine aktuelle Studie schätzt, dass der Aufwand zur Bekämpfung von Marken- und Produktfälschungen sowie -manipulationen, illegalen Importen und organisiertem Diebstahl bis 2012 jährlich global um rund zwölf Prozent steigt. Schwer überschaubare Supply-Chain-Strukturen, vernetzte Produktströme sowie die fortschreitende Globalisierung erleichtern Fälschern das Handwerk. Dabei entwickeln diese ihre Methoden ständig weiter: In immer kürzeren Abständen werden sichtbare und unsichtbare Sicherheitsmerkmale kopiert oder Fälschungen in vermeintlich sichere Supply Chains eingeschleust. Im Kampf gegen Fälschungen sind daher maßgeschneiderte Lösungen und nachhaltige Technologien unverzichtbar.

## Maßgeschneiderte Lösungen

Um spezifisches Produkt-Know-how und Markenwerte zu schützen, benötigen Firmen ein auf ihre Bedürfnisse, Workflows und externe Rahmenbedingungen individuell maßgeschneidertes Track-, Trace- & Authentication-(TT & A-)Konzept. Zur Entwicklung dieser Lösung sind nicht nur Kenntnisse von Technologien zur Produktkennzeichnung und IT-Architektur, sondern auch Prozess-Know-how entlang der gesamten Lieferkette nötig. Die Bayer Technology Services GmbH in Leverkusen bietet Unternehmen branchenunabhängig die Erstellung eines Business Case sowie die Evaluierung möglicher Lösungsszenarien an. Anschließend besteht die Möglichkeit, das TT & A-Konzept durch erfahrene Projekt-Ingenieure auch in die Systemlandschaft und Workflows integrieren zu lassen.

„Intrinsische Fingerabdrücke sichern Objekte noch besser als biometrische Verfahren.“

Dr. Markus Gerigk  
Bayer

Dies hat das Unternehmen bereits in verschiedenen Serialisierungsprojekten weltweit bewiesen. Bayer Technology Services konzipierte und realisierte auch TT & A-Konzepte für verschiedene Branchen und Anwendungsfelder außerhalb der Pharmaindustrie. Auf der Suche nach neuen Konzepten entwickeln die Experten von Bayer Technology Services ohne Pause weiter: Seit Mitte 2010 ist eine Lösung am Markt, die garantiert, dass Zufallszahlen tatsächlich einmalig und nicht reproduzierbar sind.

## Nachhaltige Technologien

Weiterhin lässt sich der Erfolg von Investitionen in Sicherheitsmerkmale auch daran messen, wie schnell ein entsprechendes Feature kopiert wird. Mit markierungsfreien Authentifizierungstechnologien hat Bayer Technology Services

nachhaltige fälschungssichere Lösungen entwickelt. Die Lösungen übersteigen durch die Generierung eines intrinsischen Fingerabdrucks des Objekts sogar den Security-Level biometrischer Verfahren. Dies maximiert die Sicherheit, denn Fälscher können zum einen nicht sehen, dass Produkte oder Verpackungen registriert sind. Zum anderen ist es ihnen nicht möglich, die Einzigartigkeit des intrinsischen Fingerabdrucks zu kopieren.

Zukunftsweisend ist auch die Weiterentwicklung zur Systemlösung auf Etiketten: Produktetiketten sind bereits registriert und werden in Kombination mit einem Scanner zur Verifikation von Original und Fälschung einsatzfertig an den Kunden ausgeliefert. ■

## AUTOR

Dr. Markus Gerigk

Leiter Authentication Solutions bei der Bayer Technology Services GmbH, Leverkusen



Produktschutz und -identifikation ist zum Beispiel durch Barcodes oder Data-Matrix-Codes möglich.

Foto: Anatoly Vartanov / Stockphoto

## INFORMATIONEN SCHÜTZEN

# Know-how-Schutz mit Methode

Maßnahmen, die den Nachbau eigener Produkte erschweren sollen, laufen ins Leere, wenn der Plagiator statt des Produkts die Konstruktionsunterlagen analysiert. Der Schutz von Bauplänen, CAD-Daten und weiteren Unterlagen steht daher im Fokus jeder Produktschutzstrategie.

→ Gerade im Zuge der zunehmend globalen Entwicklungsprozesse gewinnt der Know-how-Schutz an Bedeutung, da der Austausch von produktdefinierenden Daten innerhalb der Wertschöpfungskette eine selbstverständliche Form der Geschäftskommunikation darstellt. Hierbei helfen Sicherheitstechnologien.

## Sicherung der „Kronjuwelen“

Eine effektive Schutzstrategie setzt eine sorgfältige Planung voraus: Diese beginnt mit einem Überblick über alle Stellen, wo sensible konstruktionsrelevante Daten anfallen, gespeichert oder übertragen werden. Basierend auf einer Grundsicherung dieser IT-Systeme (strenge Zugriffsbeschränkung, dokumentierte Prozesse für die Beantragung, Vergabe und Entziehung von Rechten, Virenschutz und me-

thodisches Einspielen für Sicherheitsupdates), empfehlen sich weitergehende Maßnahmen zur Sicherung der „Kronjuwelen“, also der wirklich sensiblen Konstruktionsdaten.

Ein einfaches und wirksames Mittel ist hier die Trennung von Netzen: Entwicklungspläne gehören nicht in dieselbe Dateiablage wie die allgemeine Korrespondenz, sondern zum Beispiel in ein Teilnetz mit eigener Windows-Domäne und Dateiablage für die Entwicklungsabteilung. Zur Minimierung der Angriffsfläche auf dieses Netz kann auch der Zugriff auf das Worldwide Web von hier gesperrt werden, wenn die Mitarbeiter stattdessen etwa über einen Terminalserver auf das Web zugreifen, ohne ihren eigenen PC zu gefährden.

Noch weiter geht ein Ansatz, der unter dem Namen „Data Leakage Protection“ (DLP) bekannt geworden ist: Dabei handelt es sich um Systeme, die die im Unternehmen verarbeiteten Daten überwachen und anhand eines Regelwerks sicherstellen, dass bestimmte Daten das Unternehmen nicht verlassen. Dazu arbeiten diese Systeme entweder netzbasierend, indem sie an Netzübergängen wie Mail- oder Proxyservern den Datenverkehr überwachen und vertrauliche Inhalte blockieren, oder sie arbeiten hostbasiert mithilfe von Softwareagenten auf den einzelnen PCs, die für jedes geöffnete Dokument kontrollieren, unter welchen Bedingungen eine Speicherung und ein Versand zugelassen sind.

DLP-Systeme können eine sinnvolle Schutzwirkung jedoch nur entfalten, wenn das Regelwerk hinreichend präzise und aktuell ist – sie erfordern daher genaue Aussagen darüber, welche Daten

vertraulich sind, anhand welcher Kriterien diese erkannt werden können (zum Beispiel Formularfelder, Speicherorte) und welche Operationen mit diesen Daten „zugelassen“ sind. Wie so oft liegt auch bei DLP-Projekten die Herausforderung nicht in der Technik, sondern in der guten organisatorischen Vorbereitung.

## Ungewollten Wissenstransfer verhindern

In vielen Geschäftsprozessen müssen die Daten das eigene Haus verlassen, etwa innerhalb von Hersteller-Lieferanten-Beziehungen. Vielfach erfolgt die Herausgabe von vertraulichen Daten wie CAD-Daten an Kooperationspartner zurzeit noch ohne jegliche Schutzmechanismen. Doch gerade mit dem Inhalt der CAD-Modelle erlangt man direkten Zugriff auf das Produktwissen. Deshalb ist es ratsam, den

„Vielfach erfolgt die Herausgabe von vertraulichen Daten an Kooperationspartner noch ohne Schutzmechanismen.“

Dr. Harald Liese  
Prostep

## PROFIL

### Prostep AG, Darmstadt

Das Unternehmen ist ein anerkannter PLM-Integrationspezialist im Bereich Produktdatenintegration. Kunden aus Luft- und Raumfahrt, Automobilindustrie sowie Schiff- und Maschinenbau bietet das Unternehmen die Integration von CAD, PDM und Supplier Communication an, um E-Engineering Realität werden zu lassen. Die Prostep AG hat Niederlassungen in vielen Städten Deutschlands, in Frankreich und den USA.

Mitarbeiter weltweit: mehr als 280

LINK  
[www.prostep.com](http://www.prostep.com)

Piraterieschutz auf die gesamte Wertschöpfungskette auszuweiten mit dem Ziel, einen ungewollten Know-how-Transfer prozesssicher zu vermeiden.

Zunächst ist es dazu notwendig, auf der Dokumentenebene, also das in den CAD-Modellen oder -Zeichnungen enthaltene Produktwissen, bedarfsspezifisch zu filtern oder zu entfernen. Wissen, das bereits vor dem Datenversand derart entfernt wurde, kann später nicht mehr missbraucht werden.

Die softwarebasierte Umsetzung dieser Methodik hat in den vergangenen Jahren die Prostep AG aus Darmstadt vorangetrieben und wird als „Data Filtering“ bezeichnet. Mithilfe von Softwaremodulen wird das Firmen-Know-how automatisiert aus CAD-Modellen entfernt, ohne die hohen Ansprüche des Datenempfängers an die vereinbarten CAD-Lieferumfangfänge und die CAD-Datenqualität zu vernachlässigen. Diese Filterung kann in den täglichen Datenaustausch prozesssicher integriert werden.

### Lösungen für Verschlüsselung

Unabdingbar für den Schutz sensibler Daten ist die Verschlüsselung bei der Übertragung zwischen Partnerunternehmen in der Wertschöpfungskette. Hierfür existieren Lösungsansätze wie abgesicherte „Datenräume“ im Worldwide Web oder Verschlüsselungslösungen für E-Mails. Für den automatisierten und sicheren Austausch von Massendaten mit hoher Austauschfrequenz bieten sich spezielle Plattformen an, die für den Austausch einer Vielzahl von Produktdaten und Informationen zum Einsatz kommen können, zum Bei-

spiel auch als Sourcing-Plattform für den technischen Einkauf. Eine lückenlose Dokumentation der Austauschvorgänge, eine geeignete Datenverschlüsselung und die Automatisierung einer Vielzahl von Prozessen lassen sich damit leicht umsetzen.

Ein weiterer Ansatz ist der Einsatz des Enterprise Rights Managements (ERM), der es ermöglicht, die Nutzung von Daten zu steuern: Nur, wer eine explizite Berechtigung

besitzt, kann Daten lesen, ändern oder speichern. Der ProStep iViP Verein in Darmstadt hat zu diesem Thema die Projektgruppe Secure Product Creation Processes (SP<sup>2</sup>) gegründet. Basierend auf Anwendungsfällen, wurden unter anderem ERM-Referenzprozesse sowie eine ERM-Referenzarchitektur und -infrastruktur in Form einer Empfehlung erarbeitet.

### Sicherheit ist Managementaufgabe

Technische Lösungen und Schutzmaßnahmen müssen dabei durch Schulung und Sensibilisierung der Mitarbeiter, klare Regelungen und die systematische Behandlung und Analyse von Sicherheitsvorfällen

flankiert werden. Damit die Gesamtheit der Schutzmaßnahmen zur Organisation passt und mit ihr wächst, muss Informationssicherheit als Managementaufgabe verstanden und durch ein betriebliches Managementsystem (ISMS) gesteuert werden. Spezialisierte IT-Sicherheitsdienstleister wie die HiSolutions AG in Berlin können helfen, ein insgesamt stimmiges Sicherheitskonzept zu entwickeln, das sich an anerkannten Standards orientiert und ein durchgängig angemessenes Schutzniveau realisiert. ■

„Eine effektive Schutzstrategie setzt eine sorgfältige Planung voraus.“

Frank Rustemeyer  
HiSolutions

### AUTOREN

#### Frank Rustemeyer

ist Director System Security bei der HiSolutions AG, Berlin.

#### Dr. Harald Liese

ist Teamleiter CA-Anwendungen bei der Prostep AG, Darmstadt.



Foto: Yunus Arakon / iStockphoto

Datendieben das Handwerk legen: Mithilfe spezieller Software kann Produktwissen aus CAD-Modellen und -Zeichnungen gefiltert werden.