protect-ing.de

Produkt- und Know-how-Schutz

Product and Know-how Protection

2. Auflage

2nd Edition

A working group within

VDMA

protect-ing.de

Produkt- und Know-how-Schutz

Product and Know-how Protection

A working group within

VDMA

Editorial

Oliver Winzenried

Sehr geehrter Leser,

36 Mitglieder der 2010 gegründeten Arbeitsgemeinschaft Protect-ing zeigen ihre Lösungen aus den Bereichen Produktkennzeichnung, Detektion, Tracking und Tracing, Embedded Security, technischer Know-how-Schutz sowie Engineering und Beratung. Praxisberichte, Schutz vor Spionage, Patente, Infos zu neuen Publikationen und Standards sowie VDMA Gremien und Ansprechpartner runden die zweite Ausgabe des VDMA-Branchenführer Produkt- und Know-how-Schutz ab.

Original von Plagiat unterscheiden zu können ist wichtig für Kunden und Hersteller. Mit präventiven Maßnahmen kann das Herstellen von Plagiaten erschwert werden. Dazu gilt es auch das Know-how zu schützen, was die deutschen Unternehmen als überlebensnotwendig einstuften.

Verschaffen Sie sich einen Überblick über die verschiedenen Technologien sowie erprobten Lösungen und sprechen Sie die Anbieter gezielt an. Mit einem passenden Mix an Schutzmaßnahmen sind Sie den wachsenden Bedrohungen durch die zunehmende Vernetzung mit Industrie 4.0 gewachsen und nutzen Ihre Wertschöpfungspotentiale.

Ihr

Oliver Winzenried
Vorstandsvorsitzender der AG Protect-ing
Chairman of the Board of Protect-ing

Dear Reader,

36 members of the Protect-ing working group founded in 2010 present their solutions covering the areas of product identification, detection, tracking and tracing, embedded security and technical know-how protection as well as engineering and consulting. Practical reports, protection from espionage, patents, information on new publications and standards together with VDMA bodies and contacts round off the second issue of the VDMA directory „Product and Know-How Protection".

Being able to distinguish between an original and a counterfeit copy is essential for customers and manufacturers. Preventive measures can make it harder to produce counterfeit copies. Such measures also entail protecting the corresponding know-how, an aspect which German companies see as being crucial for survival.

Find out about the various technologies and qualified solutions that are available, and make direct contact with the vendors. A suitable mix of protective measures will help you cope with the growing threat posed by increasing connectivity with Industrie 4.0 and let you make the most of your value-creation potential!

Yours

Inhalt *Contents*

Inhalt

Contents

Arbeitsgemeinschaft „Produkt- und Know-how-Schutz“
Gemeinsam Produkte und Know-how schützen
Working group “Product and Know-how Protection”
Jointly protecting products and know-how

Die Wettbewerbsfähigkeit deutscher Unternehmen, insbesondere im Maschinen– und Anlagenbau, hängt maßgeblich von ihrer Fähigkeit ab, ihr Forschungs- und Verfahrenswissen zu schützen. Der Wettbewerb wird globaler, intensiver und härter. Maschinen und Anlagen werden unternehmensübergreifend digital vernetzt. Für die Unternehmen ist es daher nicht nur eine Herausforderung, sondern eine Verpflichtung, ihre Produkte und das elementare Know-how zu sichern. Die Täter sind oftmals nicht sichtbar, die Bedrohung scheint abstrakt. Ist ein Produkt aber erst einmal gefälscht und auf dem Markt bzw. ist Kern-Know-how abgeflossen, sind die Auswirkungen durch Verlust der Marktführerschaft, den Rückgang von Marktanteilen oder durch fallende Margen im Wettbewerb spürbar.

Der VDMA hat daher im Rahmen seiner Strategie gegen Produktpiraterie und Cyberbedrohungen 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 Plagiateure, Cyberangreifer und Know-how-Diebe.

Sechs Ansätze stehen in der Arbeitsgemeinschaft Protect-ing im Fokus des Interesses:

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

The competitiveness of German companies, particularly on the engineering sector, depends crucially on their ability to protect their research and process knowledge. Competition is getting increasingly global, intensive and tough. Machines and plants are networked digitally on a cross-company scale. Companies are therefore facing not just the challenge but the obligation of protecting their products and their elementary know-how. The perpetrators are often invisible and the threat seems to be abstract. But once a product has been counterfeited and on the market, once core know-how has gone, the impacts on a company’s competition standing will be clearly noticeable in the loss of market leadership, declining market shares or shrinking margins.

The VDMA has therefore set up the working group on product and know-how protection (AG Protect-ing) as part of its strategy against product piracy and cyber threats. It pools the interests of the providers of technologies and services for product and know-how protection and acts as the first contact in the fight against product pirates, cyber attackers and know-how thieves.

The Protect-ing working group focuses on six aspects:

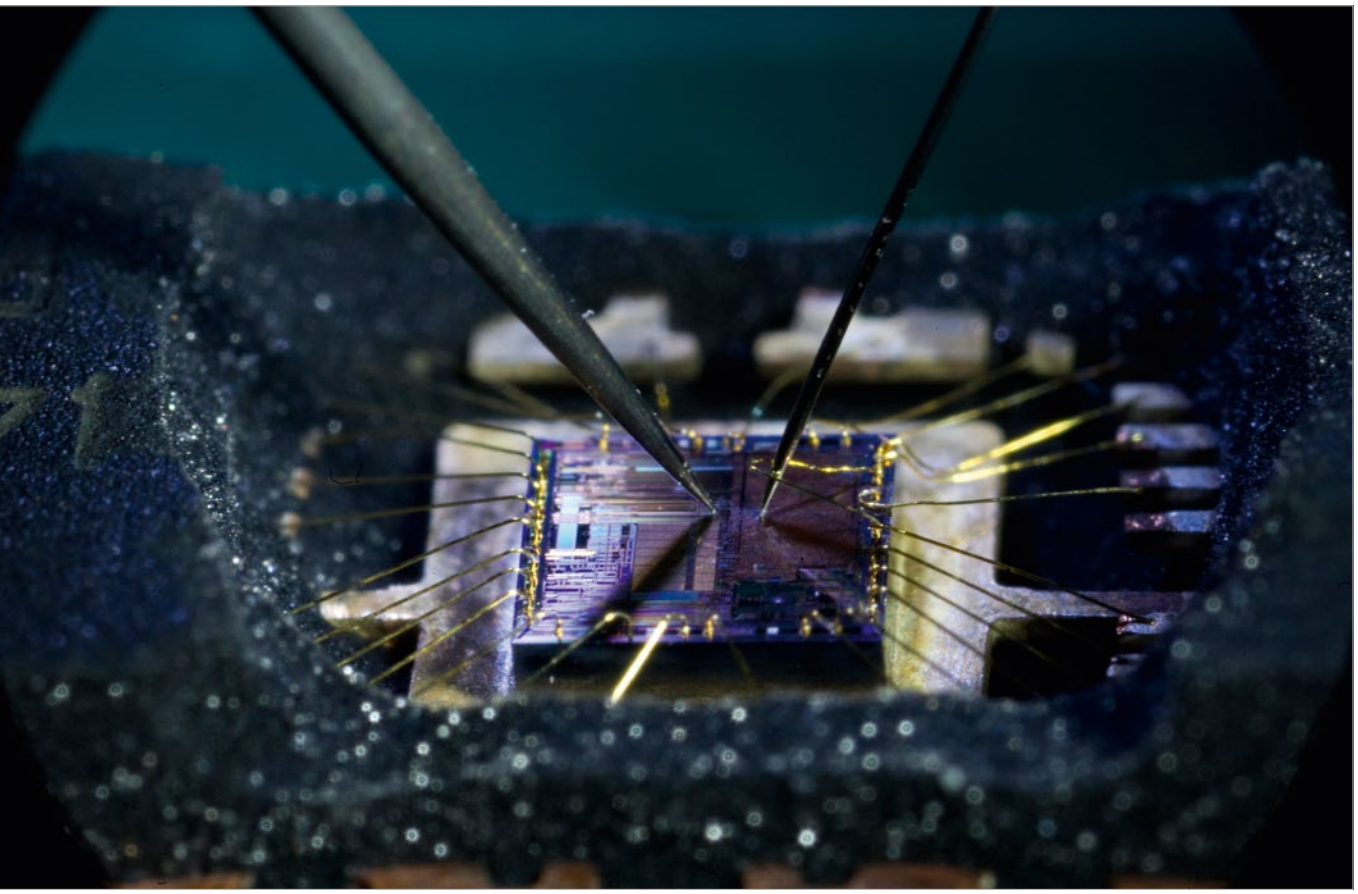
1. Marking products
Marking technologies are visible or invisible security features for verifying product identity, originality and authenticity. Examples include holograms, data matrix codes, RFIDs, special printing methods or material admixtures.

2. Geschützte Produkte authentifizieren
Um Produkte oder Maschinen zu detektieren und eindeutig zu authentifizieren, werden Geräte und IT-Systeme benötigt, mit denen Sicherheitsmerkmale erkannt, identifiziert 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 Produktes soll das Einschleusen von Plagiaten verhindert werden. Technische Basis hierfür bilden IT-Systeme und definierte Überprüfungsstellen wie der Zoll oder Großhändler.

2. Authenticating protected products
The detection and unique authentication of products or machines needs devices and IT systems so that their security features can be detected, identified and their originality checked. Typical devices are RFID readers, opto-sensors or image processing systems which can be connected to online software and databases for checking purposes.

3. Tracking and tracing systems
Tracking and tracing systems aim to monitor and pursue the whole lifecycle of a product on the basis of unique security features. The aim is to prevent any infiltration with counterfeits through close integration with the logistics chain of a product. This whole concept is based on IT systems and defined checking points at customs or wholesalers.



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 auf die industriellen Anforderungen von Embedded Systemen angepasst sind und u.a. vor Reverse Engineering und Manipulation schützen. Beispiele sind Anomaly Detection Systeme in Steuerungsprogrammen, verschlüsselte Software und Kommunikation oder Krypto-RFIDs.

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

4. Embedded security
Embedded security in industrial products and systems aims to protect the know-how concealed in electronic components, software and data in smart technical products. It is based on technologies that have been adapted to the industrial requirements of embedded systems to offer protection above all from reverse engineering and manipulation. Examples include anomaly detection systems in control programs, encrypted software and communication or crypto RFIDs.

5. Controlling know-how transfer
Technical protection from unwanted know-how transfer refers primarily to concepts and technologies to protect sensitive design, production and corporate know-how. Examples include systems for rights management, access protection, encryption and information reduction, as well as organisational concepts to enhance information security in the company.

6. Engineering und Beratung

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

Die Nutzung aktuell verfügbarer Technologien und die Weiterentwicklung neuer, innovativer Werkzeuge zum Schutz von Produkten und Know-how wird, analog zu den Interessen von Staaten und Wettbewerbern, für die industrielle Zukunft notwendig sein. Industrie 4.0 braucht funktionierende Mechanismen zur eindeutigen Identifikation und sicheren Kommunikation. Zudem spielen die Interessen von Verbrauchern eine immer größere Rolle, denen eine einfache Möglichkeit zur Originalitätsprüfung angeboten werden sollte. Insbesondere bei sensiblen Produkten für Endverbraucher wie Pharmazeutika, Medizintechnik und Lebensmittel gibt es entsprechende Forderungen für Echtheits- und Herkunftsnachweissysteme.

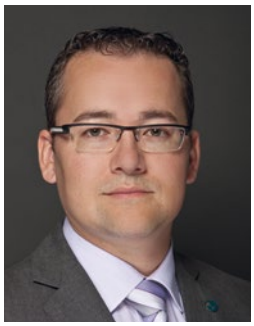
Gemeinsam mit Anwendern, Herstellern, Entwicklern und Behörden wird der VDMA diese Herausforderung annehmen und in der Arbeitsgemeinschaft unterstützen.

6. Engineering and consulting

A whole range of services are available for product and know-how protection in the field of product piracy. Product providers, independent consultants or institutes offer many solutions. These include for example the validation of usability, risk minimisation, profitability or security levels and bringing these aspects together in an individual protection concept.

In the industrial future, it will be necessary to use currently available technologies and to develop new, innovative tools for protecting products and know-how, parallel to the interests of countries and competitors. Industrie 4.0 needs functioning mechanisms for unique identification and secure communication. Furthermore, consumer interests play an ever growing role with the need to offer simple possibilities for authenticity verification. There are corresponding demands for authenticity and origin verification systems particularly for sensitive final consumer products such as pharmaceuticals, medical technology and food.

The VDMA will work together with users, manufacturers, developers and the authorities to take up this challenge and support the working group.



Steffen Zimmermann
Geschäftsführer
Managing Director

VDMA Verband Deutscher
Maschinen- und Anlagenbau e.V.
Arbeitsgemeinschaft Produkt- und Know-how-Schutz
Working group „Product and Know-how Protection“

www.protect-ing.de
pks.vdma.org

protect-ing.de

WOLLEN KÖNNEN DÜRFEN – Know-how-Schutz verschiebt Handlungsoptionen vom Wettbewerb zum eigenen Unternehmen

WILLINGNESS ABILITY PERMISSION – know-how protection shifts the action focus from the competition back to your own company

Patentschutz, IT-Sicherheit und Mitarbeiterbindung haben nichts gemein? Daher werden diese Aufgaben auch in verschiedenen Abteilungen erledigt. Und doch handelt es sich in allen drei Fällen um Maßnahmen des Know-how-Schutzes. Grund genug, mögliche Zielrichtungen eines schlagkräftigen Know-how-Schutzes in Technologieunternehmen einmal genauer zu betrachten. Was soll Know-how-Schutz eigentlich bringen?

Allgemein gesagt: einen weiteren oder länger andauernden Vorsprung gegenüber dem Wettbewerb hinsichtlich Technologie, Marketing oder Organisation. Ein solcher Vorsprung zielt auf bessere Handlungsoptionen im Vergleich zum Wettbewerb, sei es durch bessere, günstigere oder flexiblere Produkte. Hier setzt Know-how-Schutz an.

Vereinfacht gesagt: die Mannschaft eines technologiegetriebenen Unternehmens muss handeln WOLLEN, KÖNNEN und DÜRFEN.

WOLLEN heißt, den Willen zu haben, in Märkte einzutreten und diese auszubauen. KÖNNEN heißt, dazu durch Wissen und praktische Fähigkeiten in der Lage zu sein. DÜRFEN heißt, einen Markteintritt oder eine Bewegung im Markt auch im Rahmen der einschlägigen Gesetze und Normen zu erreichen.

Know-how-Schutz fördert das WOLLEN, KÖNNEN und DÜRFEN im eigenen Unternehmen und erschwert es beim Wettbewerb, wobei unterschiedliche Mittel des Know-how-Schutzes dazu unterschiedliche Ansätze verfolgen und dementsprechend organisatorischen, technischen oder rechtlichen Maßnahmen zugeordnet werden.

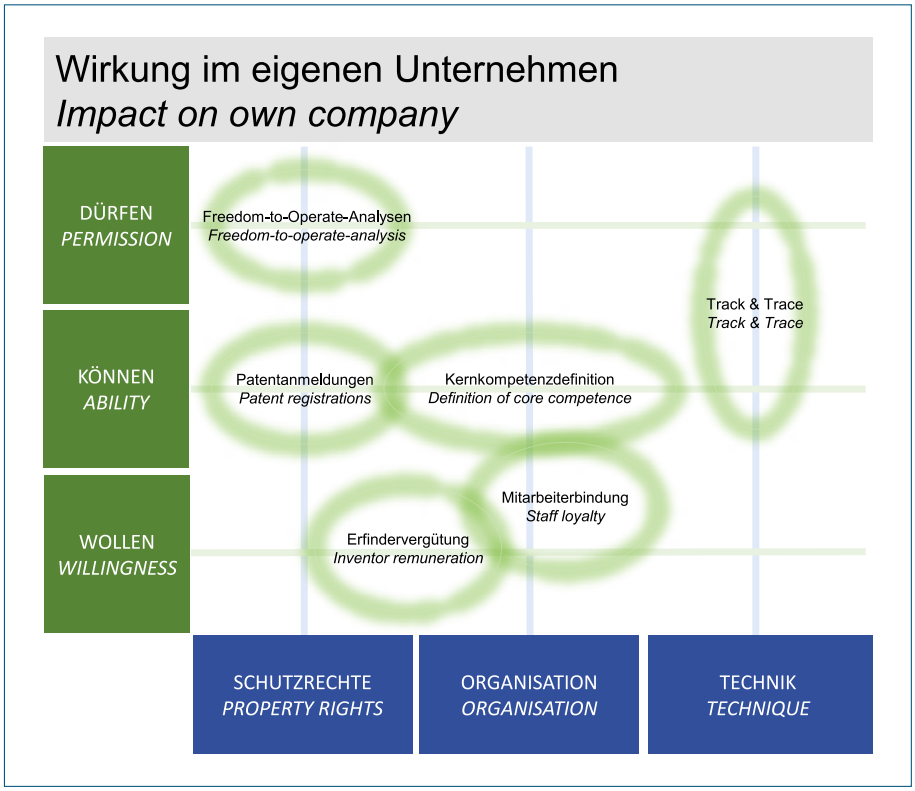
Patent protection, IT security and staff loyalty have nothing in common? It would appear so, and as a result, these tasks are handled in different departments. And yet they all refer to measures for know-how protection. Reason enough to take a closer look at possible objectives for powerful know-how protection in technology companies. What does know-how protection intent to achieve anyway?

Generally speaking, it should give the company a broader and longer lasting lead over the competition in terms of technology, marketing or organisation. This kind of lead has better action options of action than the competition, through improved, cheaper or more flexible products. This is where know-how protection comes in.

To put it simply, the team of a technology-driven company must have the WILLINGNESS, ABILITY and PERMISSION to act.

WILLINGNESS means having the will to enter into markets and work at expanding them. ABILITY means having the knowledge and practical skills to do so. PERMISSION means achieving market entry or moving market within the framework of pertinent legislation and standards.

Know-how protection promotes WILLINGNESS, ABILITY and PERMISSION in your own company and makes it more difficult for the competition. Different methods for know-how protection take different approaches and can therefore be classified as organisational, technical or legal measures.



Quelle: Innovation IP GbR
Source: Innovation IP GbR

Organisatorischer Know-how-Schutz setzt an den Dokumenten und an den Menschen an, also den klassischen Know-how-Trägern. Typische Maßnahmen sind Varianten der Mitarbeiterbindung, ein reges betriebliches Vorschlagswesen und IT-Sicherheit.

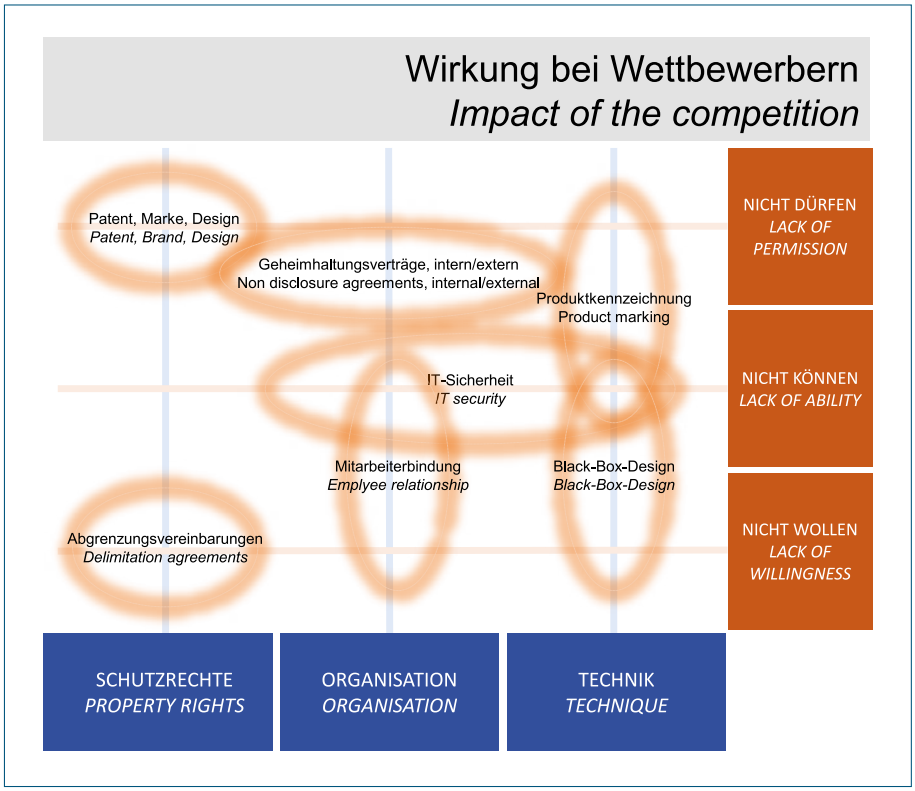
Technischer Know-how-Schutz kümmert sich um einen anderen Know-how-Träger: das verkaufte Produkt oder den angebotenen Service selbst. Typische Maßnahmen sind eine Verschlüsselung der Steuerung, eine Kapselung von kritischer Hardware oder tamper-evidente Etiketten.

Rechtlicher Know-how-Schutz umfasst neben der Anmeldung und Durchsetzung von Schutzrechten auf Technologie (Patent, Gebrauchsmuster), Ästhetik (Design) und Marktleistung (Marke) auch andere Instrumente wie ein Vorgehen gegen unlauteren Wettbewerb oder die Gestaltung von Geheimhaltungs- oder Abgrenzungsverträgen.

Organisational know-how protection addresses the documents and the people, i.e. the classic know-how carriers. Typical measures are variations in promoting staff loyalty, a lively company suggestions scheme and IT security.

Technical know-how protection deals with another know-how carrier: the sold product or the actually provided service. Typical measures include encryption of the controller, encapsulating critical hardware or tamper-evident labels.

Legal know-how protection includes registering and asserting property rights to technology (patent, utility model) appearance (design) and market performance (brand) together with other instruments such as taking action against unfair competition or drawing up non-disclosure or delimitation agreements.



Quelle: Innovation IP GbR
Source: Innovation IP GbR

Einzelne Maßnahmen aus diesen drei Kategorien leisten unterschiedliche Beiträge zu einem „WOLLEN KÖNNEN DÜRFEN“ im eigenen Unternehmen und zu einem „NICHT WOLLEN KÖNNEN DÜRFEN“ beim Wettbewerb, wie für einige weit verbreitete Maßnahmen in den beiden Darstellungen gezeigt wird.

Letztlich wird deutlich, dass Know-how-Schutz zwei grundsätzlich unterschiedliche Ziele verfolgen kann:

Ziel Nr. 1 ist, den Wettbewerbern wertvolles Know-how real vorzuenthalten. Niemand außerhalb des eigenen Unternehmens soll dieses Know-how beherrschen KÖNNEN.

Individual measures from these three categories make different contributions to WILLINGNESS, ABILITY and PERMISSION in the company and to a lack thereof in the competition, as the two diagrams show for a number of wide-spread measures.

In the end, it becomes quite clear that know-how protection can address two fundamentally different goals:

Goal No. 1 is to ensure that valuable know-how is really kept from the competitors. No-one outside your company should have the ABILITY to use this know-how.

Ziel Nr. 2 ist, die Wettbewerber davon abzuhalten, wertvolles Know-how zu verwenden, obwohl sie es bekommen haben oder bekommen könnten. Niemand außerhalb des eigenen Unternehmens soll dieses Know-how nutzen WOLLEN oder nutzen DÜRFEN.

Im Optimalfall würde Ziel Nr. 1 vollständig erreicht, indem die Mitarbeiter, die Dokumente und die Produkte das Kern-Know-how nicht preisgeben. Dieser Fall ist für fast alle Unternehmen utopisch, weil Know-how-Schutz nie perfekt ist (und in vernetzten Wertschöpfungsnetzwerken gar nicht sein soll).

Daher muss auch Ziel Nr. 2 verfolgt werden: Wenn sich Wettbewerber oder Wertschöpfungspartner wertvolles Know-how aneignen können, ist man dann zumindest in der Lage, dessen Nutzung zu erschweren, indem man diese Nutzung verbieten lässt oder unangenehme Konsequenzen in Aussicht stellt.

Um abzustimmen, was wie geschützt wird, ist ein schlagkräftiger Know-how-Schutz daher immer „weit oben aufgehängt“ und verzahnt die Beiträge, die die relevanten Unternehmensfunktionen (u.a. Entwicklung, Service, Marketing, Vertrieb, IT, Personal, Recht und IP) dazu leisten können.

Goal No. 2 consists in preventing the competitors from using valuable know-how, although they have already obtained it or could obtain it. No-one outside your company should have the WILLINGNESS or PERMISSION to use this know-how.

Ideally, goal No. 1 is achieved fully by ensuring that the know-how is revealed by neither employees, documents nor products. But this is unrealistic for nearly all companies because know-how protection is never perfect (nor should it be in connected value networks).

And so goal No. 2 also has to be pursued. If competitors or value partners are able to acquire valuable know-how, you are at least in a position to make it much harder to use by consistently prohibiting such use or showing how unpleasant the consequences thereof would be.

When agreeing what is protected and how, powerful know-how protection therefore always aims as high as possible and combines the contributions made by relevant company functions (including Development, Service, Marketing, Sales, IT, HR; Legal and IP).

Autor:
Dr. Markus Petermann,
European Patent Attorney,
Innovation IP GbR, München
www. innovation-ip.de

Author:
Dr. Markus Petermann,
European Patent Attorney,
Innovation IP GbR, Munich
www. innovation-ip.de

Mit Standards gegen Produktpiraterie
Standards for preventing product piracy

Im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA) widmet sich der Arbeitsausschuss NIA-02-01 „Maßnahmen gegen Produktpiraterie“ seit seiner Gründung in 2009 der Entwicklung von Normen zur Verhinderung von Produktpiraterie. Das schließt beispielsweise Maßnahmen zur Fälschungssicherheit, Authentifizierungswerkzeuge aber auch Managementstandards und spezifische Schutzkonzepte mit ein.

Der NIA-02-01 spiegelt auf nationaler Ebene das internationale Normungsgremium ISO/TC 292 „Security and Resilience“ Working Group 4 „Authenticity, integrity and trust for products and documents“ und stellt seit Mitte 2015 mit Hrn. Dr. Wolfgang Klasen (Siemens) sowohl den Vorsitz als auch das Sekretariat (Hr. Roman Grahle, DIN) dieser Arbeitsgruppe. In ISO/TC 292/WG 4 sind neben deutschen Experten vor allem Experten aus Österreich, Schweiz, Frankreich, Japan, Korea, USA und Großbritannien, aber zunehmend auch aus Schweden, Mexiko und Südafrika aktiv.

Die laufenden Aktivitäten der internationalen Standardisierung sind die folgenden Projekte:

- ISO 34001 Security management system – Fraud countermeasures and controls
- ISO 19564 Product fraud countermeasures and control – General principles
- ISO 19998 Requirements for the content, security and issuance of excise tax stamps
- ISO 20229 Guideline for establishing interoperability among object identification systems to deter counterfeiting and illicit trade

Autor:
Wolfgang Klasen
Obmann NIA-02-01
DIN Normenausschuss
Informationstechnik und
Anwendungen (NIA)
http://www.nia.din.de

In the DIN Standards Committee Information Technology and Selected IT Applications (NIA), the technical committee NIA-02-01 “Measures against product piracy” which was set up in 2009 is dedicated to developing standards for preventing product piracy. This includes for example measures for forgery protection and authentication tools, as well as management standards and specific protection concepts.

The NIA-02-01 is the national counterpart for the international standards body ISO/TC 292 “Security and Resilience” Working Group 4 “Authenticity, integrity and trust for products and documents”. Since mid 2015, the NIA-02-01 has provided both the chairman (Dr. Wolfgang Klasen, Siemens) and the secretary (Roman Grahle, DIN) for this working group. ISO/TC 292/WG 4 is made up of German experts together with experts from Austria, Switzerland, France, Japan, Korea, the USA and the UK, with increasingly active participation also from Sweden, Mexico and south Africa.

International standardisation activities are currently focusing on the following projects:

- *ISO 34001 Security management system – Fraud countermeasures and controls*
- *ISO 19564 Product fraud countermeasures and control - General principles*
- *ISO 19998 Requirements for the content, security and issuance of excise tax stamps*
- *ISO 20229 Guideline for establishing interoperability among object identification systems to deter counterfeiting and illicit trade*

Furthermore, the standardisation body is also responsible for updating the following already published standards:

Author:
Wolfgang Klasen
Obmann NIA-02-01
DIN Standards Committee
Information Technology and
Selected IT Applications (NIA)
http://www.nia.din

Quelle: Zerbor - Fotolia.com
Source: Zerbor - Fotolia.com

„Der Schutz geistigen Eigentums kann nur im Rahmen internationaler Zusammenarbeit realisiert werden. Daher wächst die Bedeutung global anwendbarer und akzeptierter Standards gegen Produktpiraterie“.

„Intellectual property can only be protected in the framework of international cooperation. Globally applicable and acceptable standards against product piracy are therefore growing in significance.“

Desweiteren obliegt dem Standardisierungsgremium die Pflege der bereits veröffentlichten Standards:

- ISO 12931 Performance criteria for authentication solutions used to combat counterfeiting of material goods
- ISO 16678 Guidelines for interoperable object identification and related authentication systems to deter counterfeiting and illicit trade

Bisher nur nationales Projekt aber durchaus mit dem Ziel dieses mittelfristig auch in das international Gremium einzubringen ist eine DIN-Norm mit dem Titel DIN 66405 „Leitfaden für die Erstellung von Schutzkonzepten gegen Produktpiraterie, unlauteren Nachbau und Handel illegaler Waren“. Vor dem Hintergrund, dass unabgestimmte Einzelmaßnahmen nicht ausreichen, einen umfassenden Schutz zu gewährleisten, ist es Ziel dieser Norm, Anforderungen und Vereinbarungen für den Prozess der Erstellung, Umsetzung und Evaluierung eines solchen Schutzkonzeptes festzulegen. Hierbei ist unter anderem zu berücksichtigen dass sich die Maßnahmen in ihren Nutzen nicht gegenseitig einschränken sondern im Gegenteil ergänzen.

Die Zusammensetzung des NIA-02-01 mit Vertretern von Herstellern sowie Anwendern von Produktschutztechnologien sowie Prüfinstituten, Verbänden, Hochschulen und Verbraucherschutz ist derzeit gut aufgestellt um die internationalen Standardisierungsaktivitäten aktiv mitzugestalten. Auch vor dem Hintergrund eines zu erwartenden Zuwachses an internationalen Projekten werden aber jederzeit gerne neue Mitarbeiter begrüßt. Besonders die Projekte ISO 19998, ISO 20229 und ISO 19564 befinden sich derzeit in einem frühen Entwicklungsstadium, so dass noch grundlegend inhaltlich Einfluss genommen werden kann.

- *ISO 12931 Performance criteria for authentication solutions used to combat counterfeiting of material goods*
- *ISO 16678 Guidelines for interoperable object identification and related authentication systems to deter counterfeiting and illicit trade*

A currently national project which in the medium term will also be introduced to the international body consists in a DIN standard entitled DIN 66405 “Guideline for producing protection concepts for fighting product piracy, unfair replication and illicit trade.” Given that uncoordinated isolated measures simply aren’t enough to offer comprehensive protection, the aim of this standard is to stipulate requirements and agreements for the process of producing, implementing and evaluating this kind of protection concept. Here consideration also has to be given to the fact that the measures should supplement each other, rather than having a mutually restrictive effect on the benefits.

The composition of NIA-02-01 with representatives from manufacturers and users of product protection technology together with testing institutes, associations, universities and consumer protection organisations is currently well suited for playing an active role in shaping international standardisation activities. New participants are always welcome, particularly in view of the expected growth in international projects. ISO 19998, ISO 20229 and ISO 19564 are projects currently in an early development stage where there is still scope for influencing the contents.

Piraterie 4.0 – eine Erfindung aus China?
Piracy 4.0: a Chinese invention?

China weiter auf der Überholspur

Spannt man einen Kreis über China und Indien, schlupfen noch ein paar Länder mit in die Fläche, und man hat den Bevölkerungs-Hotspot der Erde: Es wohnen mehr Menschen innerhalb dieses Kreises als außerhalb. Der Drang nach westlichem Wohlstand war dort historisch der Motor für die Wirtschaft, der Westen ein Vorbild, diese Area war bisher das Billiglohnquartier. Das hat sich gewandelt: China begreift sich zunehmend als Macht, welche sich ausdehnt und wirtschaftlich absichert. Es werden große Flächen nicht nur auf Madagaskar eingekauft, sondern auch größere Unternehmenszukäufe und Übernahmen weltweit getätigt. Westliche Märkte werden inzwischen mehr als Potential denn als Vorbild betrachtet. Man sieht hier Möglichkeiten, die etwas nachlassende Binnennachfrage zu kompensieren, schaut sich das Land an und besichtigt neben den Einkäufen von Luxusartikeln gerne Firmen, um hier speziell auch vom Ausbildungssektor noch etwas zu lernen.

In anderen Bereichen hat man längst aufgeholt, Insider vieler Märkte bekennen heimlich, man sei wohl überholt worden. Nicht nur Huawei zeigt was geht.

Andere verweisen auf die aktuelle Wirtschafts- und Finanzlage gerne mit dem Wort „Krise“, verweisen darauf, dass China „noch nicht so weit sei“, alles etwas überschätzt worden sei. Dies erinnert an Aussagen einiger ähnlicher Abteilungen von vor 20 Jahren, welche auch meinten „Das mit dem Internet geht auch wieder vorbei“. Finanzinvestoren sprechen eher auch von einer überfälligen Anpassung der Währung im Sommer 2015, da der Motor zu lange zu hoch drehte und man sich nun den Drehzahlen von anderen Wirtschaftsnationen einfach angleiche. Schlussendlich befindet sich das Wirtschaftswachstum Chinas immer noch in Höhen, z. B. einem BIP von über 6%, wovon die meisten Länder nicht einmal träumen.

China still in the fast lane

A circle drawn around China and India also includes a few other countries which, taken altogether, feature all the population hot spots in the world: more people live inside the circle than outside it. In historical terms, here the urge for western prosperity has been the motor that drives business, with the west as a role model. In the past, this whole area was one big low-wage region. But things have changed. China increasingly sees itself as a power that is on expansion course and seeks to put its economy on a sound footing. It is purchasing huge areas of land, not just on Madagascar; it is also purchasing companies and pursuing takeovers on a global scale. Western markets are meanwhile seen more as potential than role model. They offer scope to compensate for the slight decline in domestic demand; visitors come to take a look, and while purchasing luxury goods they also like to go round companies and factories to see what can be learnt, particularly on the training sector.

In other areas, deficits have already been made good, while insiders on many markets admit in secret that they have probably been overtaken. Huawei is not the only example of progress. Others like to refer to the current economic and financial situation as a “crisis” and say that China “simply isn’t that far yet”, with everything having been somewhat exaggerated. It all bears a striking resemblance to statements coming from similar sources 20 years ago, to the effect that “the internet is just a passing trend”. Financial investors also speak of an overdue currency adjustment in summer 2015 as the motor had been running too fast for too long and it was now a case of simply adapting the revs to other economic powers. After all, China’s economic growth with a GDP of more than 6% is still on a level most countries can’t even dream of.

Plagiarius 2009: Sonderpreis für eine Fälschung
Plagiarius 2009: special counterfeit award

Plagiarius 2014: Sonderpreis „Fälschung“
Plagiarius 2014: special “counterfeit” award

Tatsache ist: Mit der wirtschaftlichen Entwicklung haben sich auch die Strategien verändert: War man früher am Kopieren, so ist man heute in vielen Technologiefeldern Vorreiter, und wandelt seine Strategien:

In fact, economic development has also transformed the approach. While they used to be copycats, today they have become pioneers in many areas of technology, bringing about a change in strategy.

Mit der Entwicklung des Patentwesens schob man die Innovation zusätzlich an: Mit Subventionierung von Anmeldungen und Reduzierung der Unternehmenssteuer bei Erlangung einer Mindestanzahl von Anmeldungen führte man die Unternehmen an das Patent- und Innovationswesen heran. In einer zweiten Stufe wird jetzt die Benutzung der Erfindungen gefördert.

Development of the patent system also gave a boost to innovation. Companies were encouraged to use the patent and innovation system with the introduction of subsidies for registrations and reductions in corporate taxation on achieving a minimum quantity of registrations. In a second stage, they are now promoting the use of inventions.

Gleichzeitig etabliert sich die Rechtsprechung durch den Umstand, dass sich immer mehr Firmen innerchinesisch um Schutzrechtsverletzungen streiten. Damit stieg auch der Druck einer ordentlichen Patentprüfung und Erteilung, welche sich zunehmend dem Stand von USPTO, EPA angleicht.

At the same time, jurisprudence is become established by the increasing number of domestic Chinese legal disputes for infringements of property rights. There is therefore growing pressure to have proper procedures to review and grant patients, which are increasingly achieving the same standard as USPTO or EPA.

Dies ist auch erfreulicherweise für andere Themen - wie das Markenrecht - zu entdecken, wenn westliche Firmen gegen Nachahmer vorgehen, aber auch bei innerchinesischen Streitigkeiten, welche heute den Großteil ausmachen. Auch wenn wieder leicht zunehmend eine Abschottung und Limitierung von Märkten von Regierungsseite betrieben wird – man will schließlich auch eigene Marken weiter voranbringen, dem westlichen Vorbild folgend zukünftig weltweit bekannt und etabliert sein ... und vor allem erfolgreich. Gleichsam bleiben die chinesischen Kleinbetriebe auch auf anderen Sektoren kreativ.

The same also applies to other areas as well, such as brand law, when western companies take action against imitators and also to domestic Chinese disputes, which account for the bulk of cases today. Even if the government shows a slight trend to close off and limit markets, with the aim of letting its own brands grow in future and become globally known, established and, above all, successful like the western role models before them, at the same time small Chinese companies still remain creative on other sectors.

Mit dem Negativ-Preis „Plagiarius“ gegen dreisten Ideenklau sensibilisiert die Aktion Plagiarius e.V. mit Hilfe der Medien die Öffentlichkeit bezüglich der Problematik der Produkt- und Markenpiraterie.

The “anti-prize Plagiarius” against the flagrant theft of ideas, Aktion Plagiarius e.V. involves the media to draw public attention to the problems of product and brand piracy.

Betrachtet man das Nachahmen von westlichen Produkten noch als Piraterie 2.0, war man spätestens mit dem Nachbau des Transrapid in Shanghai bei Piraterie 3.0 - dem Transfer von Knowhow und die Etablierung von Qualität und Funktion - auf Westniveau angekommen. Hierfür wird also nicht nur nachgemacht, sondern zunehmend auch immer mehr von eigenen Ingenieuren entwickelt. Insgesamt aber wurde das Geschäft adaptiert, indem zunehmend nicht nur der Look von außen stimmen sollte, sondern auch die Qualität der Funktion.

Als folgerichtig kann man nun den aktuellen neuen Trend als „Piraterie 4.0“ einordnen, welcher immer öfter zu beobachten ist, um den Umsatz weiter anzukurbeln: Findige Firmen oder Händler betreiben Webseiten, welche Markenprodukte anbieten und sich in den Suchmaschinen kontinuierlich nach oben arbeiten. Ist man in oberen Rängen angelangt, erfreut man sich der Nachfrage nach Produkten, die man gar nicht hat. Fragt der Kunden nach der Marke oder dem Produkt gibt es ja vielfältige Möglichkeiten, wie nun Umsatz gemacht werden kann:

A. Man antwortet, ja man sei Händler, dieses Produkt sei aber gerade nicht lieferbar, aber man habe ein anderes verbessertes Produkt, welches auch noch etwas günstiger sei.
B. Man teilt mit, die Produktion dieses Produkt sein eingestellt worden und bietet nun das Ersatzprodukt an, also z.B. die Eigenmarke.
C. Man bietet natürlich dieses Produkt an, aber als Plagiat.

Insbesondere mit Blick auf C. erscheint naheliegend, dass die Piraterie 4.0 eine Business-Erweiterung im Zuge des Internets aus China sei. Allerdings muss leider darauf verwiesen werden, dass dies auch schon seit einiger Zeit in anderen Ländern angewendet wird, wie z.B. Russland, Südamerika, usw. und somit mitnichten eine Erfindung Chinas ist. Zusätzlich ist zu sagen, dass in diesen anderen Ländern es mitunter wesentlich schwieriger ist, Markenrechte durchzusetzen und beispielsweise eine Löschung oder Übertragung

While the copying of western products was still known as piracy 2.0, western levels in terms of quality and function were reached at the latest with piracy 3.0, embodied by the reconstruction of the Transrapid in Shanghai and the transfer of know-how. It was no longer just a case of imitation but also of increasing development work by China’s own engineers. Altogether, business was adapted by putting an increasing focus on getting functional quality right as well as just the outside appearance.

It is therefore only logical to call the current new trend “piracy 4.0” with its increasing urge to boost sales. Resourceful firms or dealers run websites that offer brand products and keep making their way up to the top of the search engines. Once they’ve got there, they enjoy the demand for products that they simply don’t have.

When customers ask for the brand or product, there are many ways of making a sale.

A. For example, they answer yes, they do business with this product but unfortunately it’s not available at present, but they can offer another improved product, which is actually costs less too.
B. They say that production of this product has just been discontinued and then offer the substitute product, e.g. their own brand.
C. They naturally offer the product, but in fact it’s a counterfeit.

A glance at C in particular tends to indicate that piracy 4.0 is a business development from China brought about by the internet. Unfortunately, here it must be said that for some time now other countries have been following suit, such as Russia, South America etc., so that this is by no means a Chinese invention. It must also be said that in these other countries it can be far more difficult to assert brand rights and for example to get a domain deleted or transferred. In China at least it is possible to follow court proceedings being automatically recorded on a TFT screen in the courtroom, while typewriters can still be heard here and

REFCO Vakuumpumpe: links Original, rechts Fälschung.
REFCO Vacuum pump: left original, right fake.

einer Domain zu erlangen. In China jedenfalls kann man den Mitschrieb des Prozessprotokolls meistens groß auf einem TFT im Gerichtssaal mitlesen, wohingegen hier und da in der ersten Instanz Markenrechte fast unbekannt erscheinen, noch Schreibmaschinen klappern.

Als Schlüssel zur Durchsetzung solcher Rechte bleibt in jedem Land eine eingetragene Marke. Je nach Sprache, Schrift und Bild auch eventuell dreifach angemeldet. Hat man diese nicht, hat man schon verloren, bevor man anfangen will. Dies gilt gleichsam auch für die herkömmliche Produktpiraterie: Marke oder Design sind Rechte, welche man auch beim Zoll und auf Messen eher schnell versteht.

Hierzu geht auch eine jährliche „Schulung" durch die Presse, wenn auf der „Ambiente" wieder der Plagiarius verliehen wird: Er benennt nicht nur den Kopierer, sondern zeigt, dass man vorbereitet sein soll. Zumindest mit einer eingetragenen Marke in den wichtigsten Ländern, Märkten. Interessant ist auch, dass die industrielle Messtechnik Platz 3 der kopierten Produkte belegt, allerdings ermöglicht insbesondere die Piraterie 4.0 durch Suchdienste auch ein tagesaktuelles Auffinden von Plagiaten und ermöglichst so ein konsequentes Vorgehen im Frühstadium: Wenn die Umsätze noch schwach sind, lässt sich meistens der Chinese auch außergerichtlich auf Unterlassung ein. Diese gilt es zu überwachen, aber frühes Einschreiten hat sich insbesondere bei WIKA als wichtigsten Faktor herausgestellt, um die Distribution von Plagiaten auf dem Markt zu vermeiden. Gleichwohl muss in Einzelfällen – am besten vor Gericht in den Großstädten – auch gerichtlich hin und wieder eingeschritten werden.

Autor:
Ulrich Demuth,
Dipl-Ing. (FH), Head of IP,
WIKA SE, Klingenberg

Author:
Ulrich Demuth,
Dipl-Ing. (FH), Head of IP,
WIKA SE, Klingenberg

there at first instance level, where brand rights seem to be practically unknown.

The key to asserting such rights is and remains having one's own brand registered in every country. Possibly even in triple registration, depending on language, font and picture. Without this, companies will be lost before they've even begun. The same also applies to conventional product piracy: brands or designs are rights that are probably best understood at customs and trade-fairs. Annual "training" for the press takes place in this respect when the Plagiarius is awarded at the Ambiente consumer goods trade fair in Frankfurt, Germany. It not only names the copier but also shows the need to be prepared. At least by having a registered brand in the key countries and markets.

It is also interesting to note that industrial metrology comes in third place of the copied products. On the other hand, piracy 4.0 in particular with its use of search engines also permits daily discoveries of counterfeit products and plagiarism so that it is possible to take consistent action already at an early stage. While sales are still on a low level, the Chinese are usually willing to reach an out-of-court agreement to desist. This needs to be monitored, but early intervention has proven the key factor particularly at WIKA to avoid counterfeit products from spreading through the market. Even so, in specific cases there will still be a need now and then to take legal action in court - preferably at courts in the major cities.

Wirtschaftsspionage – Herausforderungen gemeinsam annehmen
Industrial espionage: facing the challenges together

Spionage ist Realität

Das ist keine überraschende Aussage. Dennoch halten viele Unternehmen Spionage nach wie vor eher für ein Problem von „Global Playern". Wirtschaftsspionage und Konkurrenzausspähung sind jedoch ein reales und häufig unterschätztes Risiko, auch für eine Vielzahl innovativer und wettbewerbsstarker mittelständischer Unternehmen; unter ihnen nicht wenige sog. „Hidden Champions".

Neben klassischen Spionage-Methoden der „human intelligence" hat die Cyberspionage die Möglichkeiten der Angreifer erheblich ausgeweitet. Beispielhaft hierfür sind elektronische Angriffe mittels E-Mails bzw. Internetangebote, die auf Zielrechner und -netzwerke Schadsoftware installieren, die zum anschließenden Informationsverlust führen können.

Elektronische Angriffe sind meist schnell umsetzbar, können eine Vielzahl von Opfern betreffen und verursachen einen vergleichsweise nur geringen Kostenaufwand. Sie sind zudem leicht anonymisierbar, erschweren daher die Täterzuordnung und bleiben für das Opfer meist unerkannt. Die zunehmende elektronische Vernetzung der Wirtschaft und zukünftig auch von ganzen Wertschöpfungsketten – Stichwort Industrie 4.0 – führt zu neuen Chancen und Perspektiven, jedoch auch für konkurrierende Unternehmen und fremde Nachrichtendienste. Das Risiko der Spionage, auch der Sabotage, wird also weiter steigen.

In einer aktuellen Umfrage des Bundesverbands der Informationswirtschaft, Telekommunikation und neue Medien e.V. BITKOM gaben 51% der befragten Unternehmen an, in den vergangenen zwei Jahren von Datendiebstahl, Spionage und Sabotage betroffen gewesen zu sein.

Espionage really happens

That is no great surprise. And yet many companies still think espionage is only a problem for the global players. But industrial espionage and spying on the competition are a frequently underestimated and real risk also for a large number of innovative, highly competitive SME companies, including not just a few "hidden champions".

Together with the classical spying methods of "human intelligence", cyber espionage has given attackers a far greater range of possibilities. Examples here include electronic attacks by e-mail or internet services that install malware on target computers and networks with a resulting loss of information.

Electronic attacks usually happen quickly, hit a large number of victims and generate only comparatively low costs. It is also easy to make them anonymous so that it is harder to identify the perpetrators, and such attacks usually remain undetected by the victim.

The increasing electronic interconnection of the business sector, which in future will also extend to entire value chains under Industrie 4.0, generates new chances and prospects, but this also applies to competing companies and foreign news services. The risk of espionage and also sabotage will therefore continue to grow.

A current survey by the BITKOM (Federal Association for Information, Telecommuni-cation and New Media) revealed that 51% of the interviewed companies have been affected by data theft, espionage and sabotage over the last two years.

Quelle: JiSign - Fotolia.com
Source: JiSign - Fotolia.com

Das unbekannte Risiko – der Innentäter.

Die Unternehmensmitarbeiterinnen und -mitarbeiter sind ein wesentlicher Faktor für den Erfolg eines Unternehmens. Mitarbeiterinnen und Mitarbeiter können jedoch ebenso – als Innentäter – auch zu einem Sicherherheitsrisiko werden. Sie kennen in aller Regel die „Kronjuwelen" des Unternehmens und verfügen über Zugangs- und Aneignungsmöglichkeiten.

So „verkaufte" bei einem Hersteller für Windenergieanlagen ein Ingenieur den Quellcode für den Betrieb solcher Anlagen an ein ausländisches Unternehmen. In einem Strafprozess gab er als Motivation berufliche Zurücksetzung durch seinen Arbeitgeber an.

Dieser Vorfall führte zu einem deutlichen Rückgang der Verkaufszahlen und in der Konsequenz auch zu Arbeitsplatzverlusten in dem betroffenen Unternehmen.

Mitarbeiter sind eher selten schon bei Einstellung „Innentäter". Sie können sich aber aufgrund privater und/oder betrieblicher Umstände dazu entwickeln. Eine Prävention in diesem Bereich sollte daher nicht nur aus innerbetrieblichen Sicherheitsmaßnahmen, sondern auch aus sozialen Angeboten und einer integrativen Unternehmenskultur bestehen.

Das BfV: Dienstleister für Spionageabwehr

„Prävention durch Dialog und Information" ist das Leitmotiv für ein umfangreiches Security-Awareness-Angebot des Bundesamtes für Verfassungsschutz.

The unknown risk: the inside perpetrator.

The employees in the workforce are a crucial factor in the success of a company. However, employees can also become a security risk as inside perpetrators.

They usually know all about the company's "crown jewels" and have corresponding possibilities for accessing and appropriating all that is necessary. For example, an engineer working for a company producing wind turbines "sold" the source code for operating the turbines to a foreign company. The motivations he stated in court referred to having been passed over by his employer on the career ladder.

This incident led to a clear decline in sales figures; in the long term, jobs were also lost in the affected company.

Employees will rarely already be "inside perpetrators" on joining the company. But they may slip into this role as a result of private and/or work-related circumstances. Prevention in this area should consist not just in interior security measures but also in appropriate social amenities and in an integrative corporate culture.

Bilaterale Sicherheitsgespräche, Sensibilisierungsvorträge, umfangreiche Informationsmaterialien und Veranstaltungen sind Zeichen eines zielgruppenorientiertes Wirtschaftsschutzes. Dahinter steht eine langjährige Erfahrung und Expertise in der Einschätzung von Risiken, Schadensvorfällen und Möglichkeiten zum präventiven Schutz.

Neben Abwehr von Spionage umfasst ein proaktiver Wirtschaftsschutz u.a. auch Aspekte des Schutzes vor Sabotage- und proliferationsrelevanten Handlungen sowie die Aufklärung über Risiken durch politischen Extremismus und Terrorismus. Das Wirtschaftsschutzreferat des BfV ist Ihr Ansprechpartner im Wirtschaftsschutz und erreichbar unter der E-Mail-Adresse: **wirtschaftsschutz@bfv.bund.de**

Wirtschaftsschutz ist Teamwork

Für ein zielgruppengerechtes Angebot im Wirtschaftsschutz arbeitet das BfV seit Jahren eng mit Partnern aus der Wirtschaft zusammen. Denn: Wirtschaftsschutz ist kein Selbstzweck. Sichere und wettbewerbsfähige Unternehmen sind auch eine Voraussetzung für soziale Sicherheit und gesamtgesellschaftliche Stabilität und damit im allgemeinstaatlichen Interesse.
Zur Teamwork im Wirtschaftsschutz zählt u.a. eine seit 2014 bestehende Kooperation mit dem Verband Deutscher Maschinen- u. Anlagenbau VDMA. Eine Vielzahl an gemeinsamen Aktivitäten kennzeichnet das gemeinsame Zusammenwirken für einen effektiven Schutz der meist mittelständisch geprägten Unternehmen des Maschinen- u. Anlagenbaus und darüber hinaus.

So können Messebesucher beispielsweise die Experten des BfV und Vertreter des VDMA auch 2016 (25. – 29. April) an einem gemeinsamen Stand auf der HANNOVER-Messe antreffen.

Autor:
Bodo W.Becker M.A.,
Bundesamt für Verfassungsschutz

The BfV: counter-espionage provider

"Prevention through dialogue and information" is the leitmotiv behind a comprehensive security awareness service offered by the BfV (Federal Office for the Protection of the Constitution).

Bilateral security talks, awareness lectures, comprehensive information material and related events are the signs of target group-oriented business protection. It is backed up by many years of experience and expertise in assessing risks, harmful incidents and preventive protection possibilities.

Together with counter-espionage, proactive business protection also includes protection from sabotage and proliferation-related activities as well as an improved understanding of the risks posed by political extremism and terrorism.
The business protection department of the BfV is your contact for business protection and can be contacted at: ***wirtschaftsschutz@bfv.bund.de***

Business protection is teamwork

For years the BfV has been working together closely with partners in business and industry to offer target group-oriented business protection. After all, business protection is not an end in itself. Secure, competitive companies are also a prerequisite for social safety and overall stability in society, and therefore also in the general state interest.
Since 2014, the teamwork activities for business protection have also included cooperation with the VDMA (German Engineering Federation).
A large number of common activities illustrate the joint striving towards effective protection for the mainly SME companies of the German engineering sector and beyond.

Visitors to the HANNOVER-Messe (25 to 29 April 2016) will once again find experts from the BfV and VDMA representatives at a joint stand.

Author:
Bodo W.Becker M.A.,
Federal Office for the Protection of the Constitution

Bildung

VDMA

Dein Start in die Berufswelt
talentmaschine.de

Du bewegst Technik. Technik bewegt die Welt.

Ausbildungsplätze | Praktika | Duale Studienplätze |
spannende Jobs & attraktive Arbeitgeber im Maschinenbau |

DesignStudio

IUNO: IT-Sicherheit in der Industrie 4.0 hat einen neuen Namen
IUNO: IT security in Industrie 4.0 has a new name

Der deutsche Maschinen- und Anlagenbau kann ein wesentlicher Nutznießer der Industrie 4.0 werden. Der Begriff meint eine Vision, nach der das Internet Einzug in die Produktionsanlagen erhält und so intelligente Fabriken erzeugt: Maschinen kommunizieren mit anderen Maschinen ebenso wie mit den Werkstücken und tauschen so permanent Informationen über den Stand des Fertigungsprozesses aus. Durch diese Verfügbarkeit aller Daten in Echtzeit lässt sich zu jedem Zeitpunkt der Wertschöpfungsfluss optimieren, Kunden und Geschäftspartner können direkt in die Prozesse eingebunden werden und die Produktionssysteme werden hoch wandlungsfähig und ermöglichen die Losgröße 1.

Vor der Realisierung dieser Vision sind jedoch noch Hürden zu überwinden. Eine besonders große Herausforderung ist es, die IT-Sicherheit dieser hochgradig vernetzten Produktionssysteme zu gewährleisten. Wenn das Internet in die Maschinen wandert, überträgt sich die zunehmende Bedrohung von IT-Systemen automatisch auch auf die industriellen Anlagen. Bisher ist die in der Produktion eingesetzte IT nur unzureichend auf Security-Anforderungen hin ausgerichtet. Eine VDMA-Studie zeigte bereits 2013 auf,

The German engineering sector can become an essential beneficiary of Industrie 4.0. The term refers to a vision in which the internet becomes integrated in production machinery to generate smart factories. Machines communicate with other machines and also with the workpieces, permanently exchanging information about the status of the production process. Realtime availability of all data makes it possible to optimise the value chain; customers and business partners can be directly integrated in the process, and production systems become highly adaptable and facilitate batch size 1.

However, there are still hurdles to be overcome before the vision can become reality. One particular challenge consists in warranting IT security for such highly connected production systems. Once the internet moves into the machine, the increasing threat faced by IT systems is automatically also transferred to the industrial machinery. Up to now, IT used in the production process is only inadequately aligned to security requirements. A VDMA study back in 2013 already showed that insufficient use is made of security standards in the German engineering sector, with production stoppages caused by security incidents occurring in 29% of the interviewed companies.

dass Security-Standards bei den deutschen Maschinen- und Anlagenbauern nur unzureichend zum Einsatz kommen, wodurch es bei 29 Prozent der befragten Unternehmen bereits zu Produktionsausfällen durch Security-Vorfälle kam.

Um die Potenziale der Industrie 4.0 voll auszunutzen, braucht es also Wissen und erprobte Lösungen. Aus diesem Grund hat das Bundesministerium für Bildung und Forschung (BMBF) im vergangenen Juli gemeinsam mit der Wirtschaft IUNO gestartet, das Nationale Referenzprojekt für IT-Sicherheit in der Industrie 4.0, das bis Sommer 2018 einen Werkzeugkasten mit erprobten und dokumentierten Umsetzungen von Lösungen für IT-Sicherheitsprobleme in der Industrie 4.0 erstellen wird.

Das Projekt vereint 14 Industriepartner und sieben Forschungseinrichtungen. Hersteller von IT-Security-Lösungen wie Infineon, Siemens oder Phoenix Contact treffen auf Anwender wie Bosch, Trumpf, VW oder Rexroth. Unter den Forschungspartnern sind allein drei Fraunhofer-Institute mit IT-Sicherheitsfokus. Das vielfältige Themenfeld der Industrie 4.0 wird in IUNO in vier Anwendungsfälle aufgeteilt, die zusammen ein repräsentatives Bild der Herausforderungen ergeben und aus denen die erprobten und dokumentierten Lösungen in den Werkzeugkasten einfließen.

Der VDMA hat IUNO aktiv in der Entstehung begleitet und moderiert und wird das Projekt auch weiter begleiten, etwa durch eine Mitgliedschaft im Beirat sowie die Unterstützung der Transfermaßnahmen des Projektes. Denn gerade die kleinen und mittelständischen Unternehmen etwa des Maschinen- und Anlagenbaus sollen von den Projektergebnissen profitieren.

www.iuno-projekt.de

Ansprechpartner:
- IUNO-Koordinierungsstelle (Bernd Hartmann, bernd.hartmann@cs.tu-darmstadt.de)
- VDMA (Steffen Zimmermann, steffen.zimmermann@vdma.org)

Contact:
- *IUNO coordination office (Bernd Hartmann, bernd.hartmann@cs.tu-darmstadt.de)*
- *VDMA (Steffen Zimmermann, steffen.zimmermann@vdma.org)*

And so know-how and proven solutions are needed to make full use of the potential offered by Industrie 4.0. For this reason, the Federal Ministry of Education and Research (BMBF) launched IUNO last July in cooperation with the business sector: this is the national reference project for IT security in Industrie 4.0. It aims to put together a toolbox to be ready by summer 2018 with proven and documented implementations of solutions for IR security problems in Industrie 4.0.

The project combines 14 partners from industry and seven research institutions. Manufacturers of IT security solutions such as Infineon, Siemens or Phoenix Contact meet users such as Bosch, Trumpf, VW or Rexroth. The research partners also include three Fraunhofer Institutes with an IT security focus. IUNO breaks down the diverse range of topics in Industrie 4.0 into four application cases; taken together, these give a representative picture of the challenges resulting in the proven, documented solutions that will be featured in the toolbox.

The VDMA has played an active role in accompanying and moderating the emergence of IUNO and will continue to accompany the project through being a member of the advisory board and also by supporting the project's transfer measures. After all, the aim is particularly for the small and medium-sized companies for example on the German engineering sector to benefit from the project results.

www.iuno-projekt.de

Traceability im Wertschöpfungsnetzwerk – Die Basis für Industrie 4.0
Traceability in the value-creation network – the basis for Industrie 4.0

Die „Traceability“ (Rückverfolgbarkeit) von Produkten und Prozessen hat auch für den Maschinen- und Anlagenbau sowie andere Industriezweige eine wachsende Bedeutung. Aber was muss dabei berücksichtigt werden und welchen Nutzen haben Kunden und Hersteller?

Die Realisierung der Traceability von Produkten und Prozessen über den gesamten Lebenszyklus ist eine der Voraussetzungen für Industrie 4.0. Nur mit der entsprechenden Kennzeichnung ist auch die digitale Identifikation von Maschinen, Baugruppen oder Komponenten möglich. Doch dabei steht nicht bloß die Erhöhung der Transparenz und Sicherheit in den Abläufen im Vordergrund.

Vor allem die folgenden Bereiche können in unterschiedlicher Art und Weise von einer entsprechenden Identifikation profitieren:

- Qualitätsmanagement
- Produktion
- After Sales / Wartung
- Logistik

Der bekannteste Anwendungsfall im Qualitätsmanagement ist mit Sicherheit die Rückrufeingrenzung. Mit vorhandenen Traceabilitydaten können so nicht nur der organisatorische Aufwand sondern auch die anfallenden Kosten deutlich gesenkt werden. Darüber hinaus lassen sich beispielsweise aber mit entsprechenden Kennzeichnungen am Produkt oder über eine gezielte Verlinkung ins Internet auch Zusatzinformationen für Instandhaltung, Servicetechniker oder Anlagenbetreiber bereitstellen, der Kundensupport im Gewährleistungsfall optimieren oder die Garantie- und Gewährleistungsabgrenzungen eindeutiger vornehmen.

The traceability of products and processes is of growing significance for both the engineering sector and also other branches of industry. But what does this involve, what has to be taken into account, and what is the benefit for customers and manufacturers?

Implementing the traceability of products and processes throughout the entire life cycle is one of the prerequisites for Industrie 4.0. Digital identification of machines, assemblies or components depends on having the right kind of corresponding marking. However, this is not just about enhancing transparency and security.

The following areas in particular can benefit in varying ways from corresponding identification:

- *Quality management*
- *Production*
- *After sales / maintenance*
- *Logistics*

Without any doubt, the best known application in quality management consists in limiting the scope of recall measures. When traceability data are available, it is possible to make cutbacks in both organisational workload and incurred costs. Furthermore, corresponding markings on the product or a direct internet link can provide additional information for maintenance, ensure that service engineers or machinery operators are at the ready, optimise customer support in case of warranty claims or make it easier to differentiate between guarantee and warranty situations.

Dafür muss allerdings die Möglichkeit geschaffen werden, dass im Bedarfsfall die relevanten Traceabilitydaten wie Stücklistenstand, Softwareversion, Informationen zu verbauten Komponenten, Prozessdaten oder Prüfdaten auch digital zur Verfügung stehen.

Produktkennzeichnung

Abhängig von den umzusetzenden Anforderungen an die Rückverfolgbarkeit ergeben sich ie notwendigen Produktkennzeichnungen. Für manche Anwendungen ist eine Hersteller und Typ Kennung bereits ausreichend, in anderen Fällen wird zusätzlich noch eine Chargenkennzeichnung benötigt. Wird allerdings eine eindeutige Identifizierung des Produktes gewünscht, dann ist die Aufbringung einer Seriennummer erforderlich. Wer seine Produkte nicht nur eindeutig identifizieren, sondern auch noch authentifizieren (hinsichtlich Originalität überprüfen) will, muss darüber hinaus zusätzliche Echtheitsmerkmale anbringen. Denn eine serialisierte Nummer allein bietet keinen Schutz vor Fälschern, weil auch sie kopiert und nachgemacht werden kann.

However, in this case it must be possible to ensure that the relevant traceability data such as valid parts lists, software version, information about fitted components, process data or test data are provided in digital form when necessary.

Product marking

The necessary product marking depends on the specific traceability requirements in each case. Sometimes it will suffice for the marking to state the manufacturer and type; in other cases, a batch marking is also required. A serial number will also be needed for unique identification of the product. If in addition to unique identification a manufacturer also wants to authenticate his products (for checking that they are original), the marking needs to be supplemented by additional authenticity attributes. After all, a serial number on its own offers no counterfeit protection because it can also be copied and replicated.

Autor:
Guido Reimann
VDMA Software und Digitalisierung

Author:
Guido Reimann
VDMA Software and Digitalization

„Risikoschutz für das Unternehmen – Produkte und Know-how für Patente und Marken“
“Risk prevention for the company: products and know-how for patents and brands”

Die Bedeutung von Patenten und Marken im internationalen Wettbewerb

Zur Absicherung der Investitionen in Forschung und Entwicklung und damit zur Absicherung der eigenen Marktposition haben die Industrieunternehmen über alle Branchen hinweg bereits seit den Neunziger Jahren vermehrt Schutzrechte (Intellectual Property, IP) angemeldet. Die zunächst defensive Ausrichtung im Umgang mit den eigenen Schutzrechten entwickelte sich zunehmend zu einer offensiveren Handhabung und damit weltweit zu stetig steigenden Zahlen an schutzrechtsbegründeten Rechtsstreitigkeiten. Die Folgekosten hieraus stellen insbesondere für klein- und mittelständische Unternehmen ein erhebliches Risiko dar. Daher gewinnt gerade auch im Zuge der Globalisierung eine kosteneffiziente IP-Strategie, die sowohl aktive als auch passive Maßnahmen beinhaltet, weiter an Bedeutung.

Proaktiver Risikoschutz: Nur werthaltige Patente und Marken zählen

Die aktiven Maßnahmen beinhalten insbesondere Aktivitäten zur Generierung durchsetzbarer Verbietungsrechte. Dies umfasst nicht nur den Schutz des eigenen geistigen Eigentums durch die sinnvolle Kombination aller Arten von Schutzrechten, sondern auch die zweckmäßige Ergänzung des eigenen IP-Portfolios mit Schutzrechten von Dritten, die entweder einlizensiert oder vollständig akquiriert werden. Der Aufbau und Umfang des IP-Portfolios richtet sich hierbei nach der IP-Strategie des Unternehmens.

Der alleinige Schutz von Technologien ist hierfür nicht immer ausreichend. Um die Kosten für den Aufbau und die Aufrechterhaltung des eigenen IP-Portfolios in maßvollen Grenzen zu halten sollte hierbei zum einen dem Grundsatz „Qualität vor Quantität“ gefolgt werden. Zum anderen kann das eigene IP durch eine Lizenzvergabe

The significance of patents and brands in international competition

In order to protect their investment in research and development, thus also shoring up their own market position, since the 1990s industrial companies have increasingly registered intellectual property rights (IP) right across all branches. The initially defensive purpose to protect proprietary intellectual property rights has increasingly turned into a more offensive approach, with growing numbers of legal disputes addressing intellectual property rights all over the world. The resulting costs pose a considerable risk particularly for small and medium-sized companies. Globalisation in particular is making it increasingly important to have a cost-efficient IP strategy with both active and passive measures.

Proactive risk prevention: only valuable patents and brands count

The active measures include especially activities for generating enforceable prohibition rights. This includes not just protective proprietary intellectual property with an appropriate combination of all kinds of intellectual property rights but also adequately supplementing the company’s own IP portfolio with third-party property rights either on the basis of licences or full acquisition. The structure and scope of the IP portfolio is geared to the company’s IP strategy.

Protecting technologies alone is not always adequate. On the one hand, the principle of “quality before quantity” should be observed to put reasonable limits on the costs for setting up and maintaining the company’s IP portfolio. On the other hand, proprietary IP can be monetised by issuing licences or IP box models to safeguard investment in R&D and generate corresponding returns (Fig. 1).

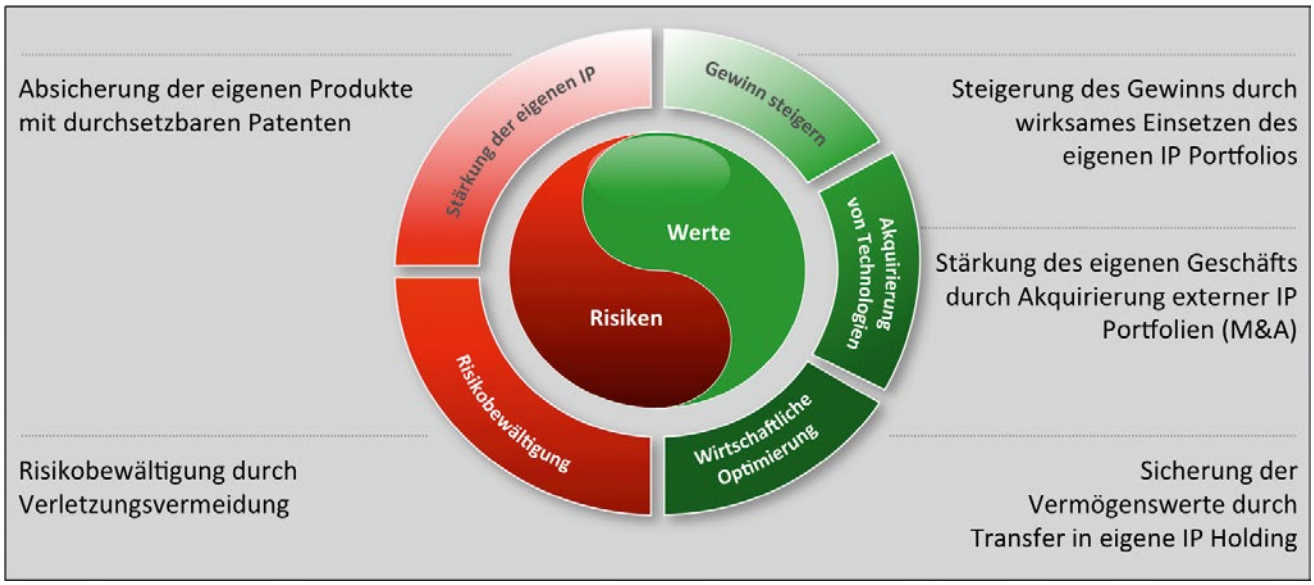


Abbildung 1: Management von Risiken und Werten bei Schutzrechten
Figure 1: *Management of risks and values with intellectual property rights*

Quelle: PATEV
Source: PATEV

monetarisiert oder durch IP-Box-Modelle eine Absicherung der Investitionen in FuE und der hieraus erzielten Rückflüsse erlangt werden (Abb. 1).

Passiver Risikoschutz: Effiziente Wettbewerbsüberwachung & Vermeidung von Patentverletzung

Infolge der Entwicklung zu einer Wissensgesellschaft kommt dem Zugang zu Informationen und dem Umgang damit, sowie den daraus abgeleiteten Maßnahmen eine immer größere Bedeutung zu. Schwerpunkte der Überwachung sind die Schutzrechte Dritter aber auch die Produkte der Wettbewerber.

Überwachung Marken und Patente

Das Monitoring von Schutzrechten Dritter ist im Hinblick auf zwei bedeutsame Effekte von großer Bedeutung: Zum einen bei der Vermeidung der Verletzung von Schutzrechten Dritter. Aus einer regelrechten Flut von Anmeldungen die wirklich relevanten Schutzrechte automatisiert auszufiltern und dann effizient zu bearbeiten ist eine große Herausforderung. Im Falle des frühzeitigen Entdeckens relevanter Schutzrechte von Dritten kann eine Problemlösung oft auch durch Kooperation statt Konfrontation herbeigeführt werden (Abb. 2).

Passive risk prevention: efficient competition monitoring and preventing patent infringements

The development towards a knowledge-based society puts ever growing significance on the access to information and how it is handled, together with correspondingly derived measures. Monitoring activities focus on third-party intellectual property rights as well as competing products.

Monitoring brands and patents

Great importance is given to monitoring third-party intellectual property rights with regard to two significant effects: on the one hand by avoiding infringements of third-party intellectual property rights. Automatically filtering the relevant intellectual property rights from the sheer flood of applications is a great challenge, as is dealing with them efficiently. When relevant third-party intellectual property rights are detected early on, it is often possible to solve the problem through cooperation instead of confrontation (Fig. 2).

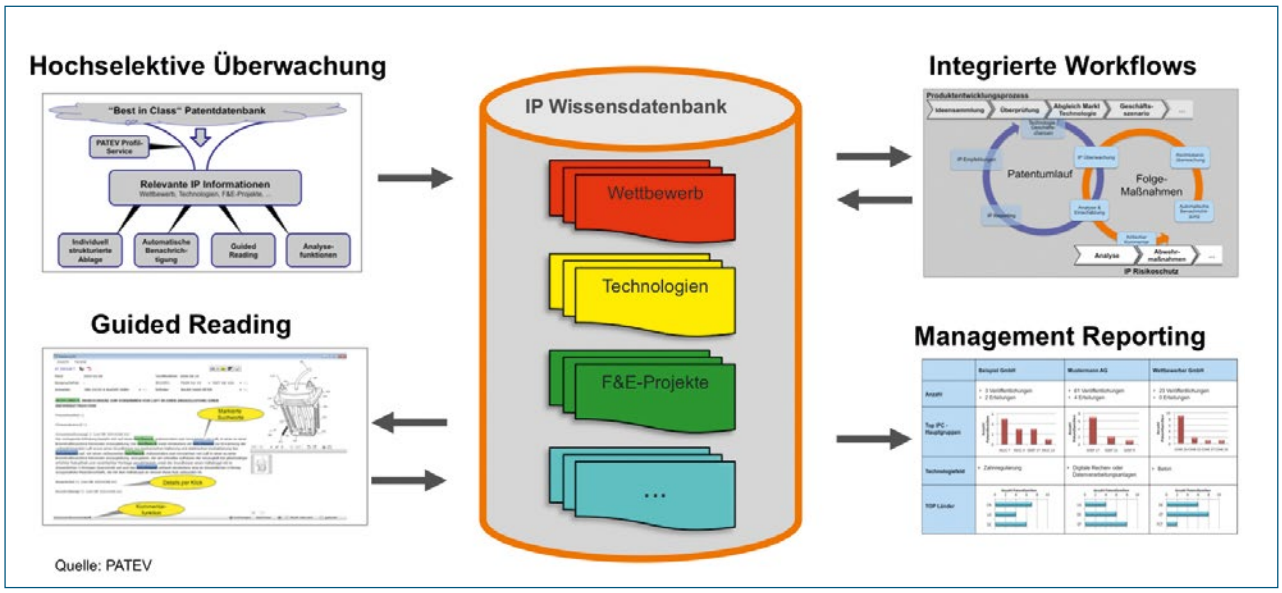


Abbildung 2: Überwachung von Marken und Patenten
Figure 2: Monitoring brands and patents

Quelle: PATEV
Source: PATEV

Aus den Rechercheergebnissen können aber auch wertvolle Informationen hinsichtlich der FuE-Aktivitäten und damit ggfs. auch über die Geschäftsstrategien der Wettbewerber gewonnen werden.

Hilfreich sind hierbei zum Beispiel semantische Recherchen, integrierte Workflows, die Arbeits-, Erfassungs-, Bewertungs- und Archivierungsab-

The research results can also generate valuable information about the competitors' R&D activities and possibly also about their business strategies.

Semantic research can be helpful here for example, or integrated workflows with working, recording, evaluating and archiving processes and aids for processing the researched contents, including guided reading, for example.

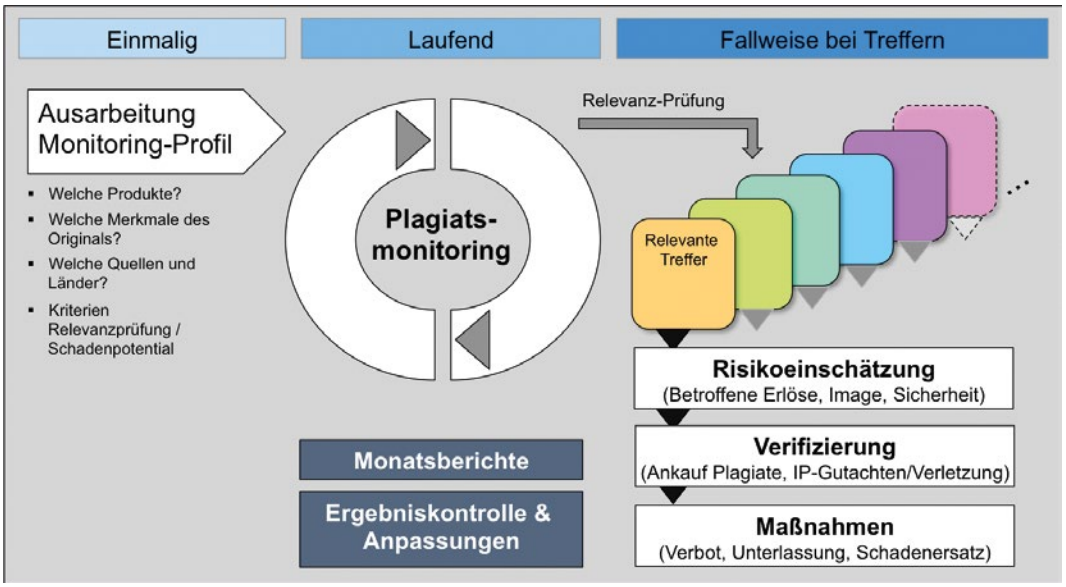


Abbildung 3: Ganzheitliches Plagiatsmonitoring
Figure 3: Holistic counterfeit monitoring

Quelle: PATEV
Source: PATEV

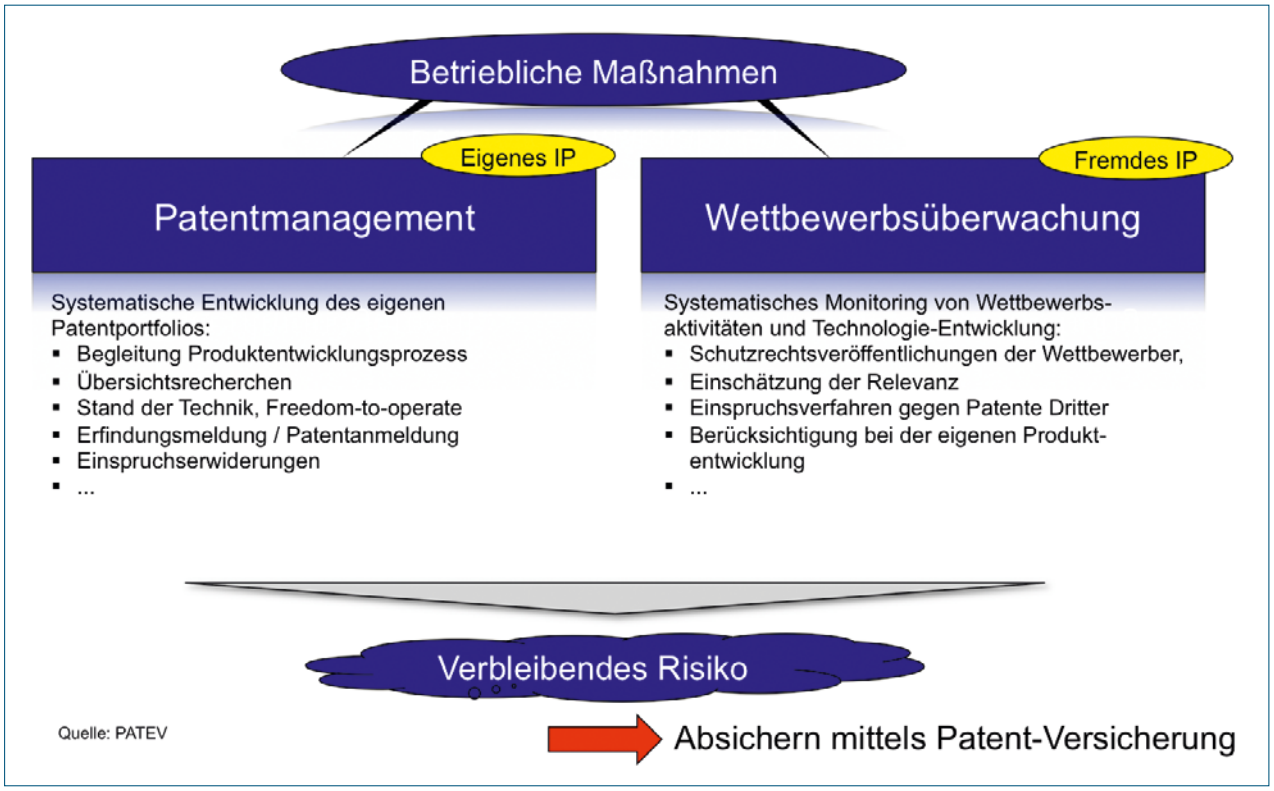


Abbildung 4: Betriebliche Maßnahmen zum IP Risikoschutz
Figure 4: Operational measures for IP risk prevention

Quelle: PATEV
Source: PATEV

läufe beinhalten, Hilfsmittel zur Verarbeitung der recherchierten Inhalte, wie beispielsweise das sogenannte Guided-Reading. Auch sollten die aufbereiteten Inhalte als recherchierbares Wissen insbesondere auch für späteren Zugriff verfügbar gehalten werden. Besonderer Bedeutung kommt auch dem gesetzeskonformen, regelmäßigen Reporting an das Management zu.

Eine weitere wichtige Form der Wettbewerbsüberwachung ist das Plagiatsmonitoring (Abb. 3). Entgangene Gewinne und Imageverlust durch qualitativ minderwertige Nachahmungen sind hier von besonderer Bedeutung. Der weltweite Schaden infolge von Schutzrechtsverletzungen liegt im Multi-Milliarden-Bereich. Daher ist es auch wichtig Plagiate durch regelmäßige Prozesse frühzeitig zu erkennen, zu bewerten und ggfs. Maßnahmen einzuleiten, um diese wieder vom Markt zu entfernen, den Schadenersatz einzufordern und weiteren Schaden vom Unternehmen abzuwenden.

The prepared contents should also be kept available as researchable knowledge particularly also for later access. Special significance is also attributed to regular, legally compliant reporting to the management.

Counterfeit monitoring is another important form of keeping an eye on the competition (Fig. 3). Special significance is given to lost profits and a loss of image brought about by poor quality replicas. The global damage caused by intellectual property rights infringements amounts to many billions. It is therefore also important to ensure that regular processes will detect counterfeit products early on, assessing them and possibly introducing measures to remove them from the market again, demand compensation and avert further damage from the company.

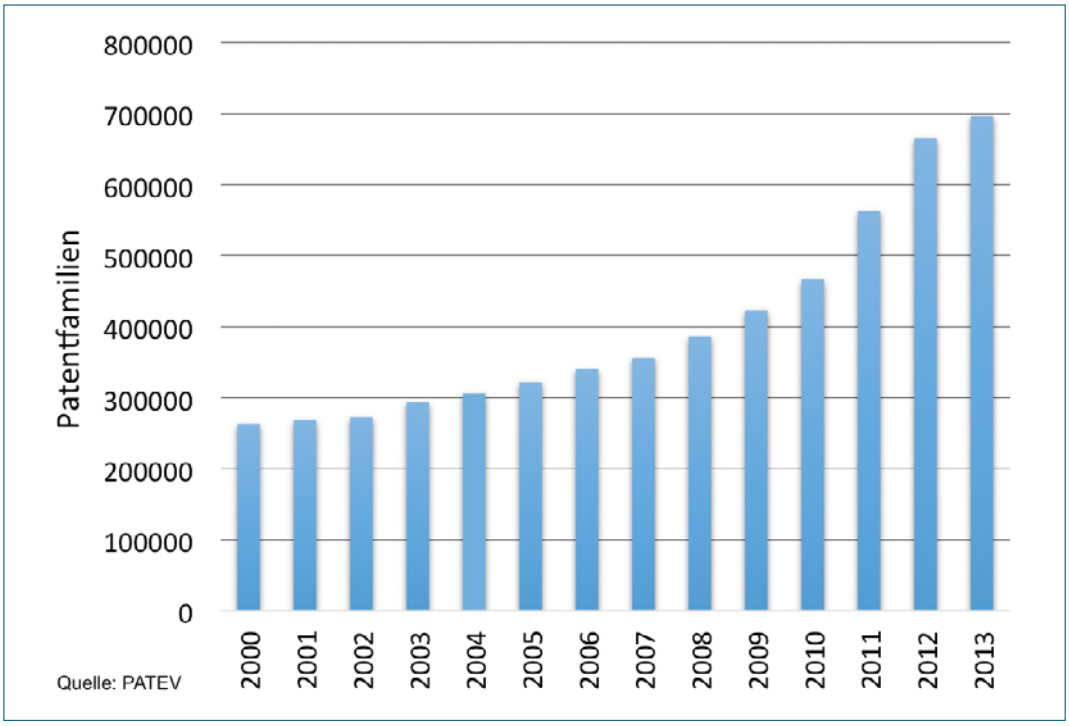


Abbildung 5: Internationale Anmeldungen im Maschinen- und Anlagenbau
Figure 5: International registrations in the engineering sector

Quelle: PATEV
Source: PATEV

Best Practice Lösungen für die betriebliche Praxis

Jegliches Risikomanagement führt nicht automatisch und vollständig zur Eliminierung sämtlicher Risiken. Bewährt hat sich in der betrieblichen Praxis insbesondere für Unternehmen mit US Export die IP-Versicherung, mit deren Hilfe sowohl Haftpflichtrisiken, beispielsweise zur Abdeckung von Schadenersatzzahlungen, als auch den Rechtsschutz zur Durchsetzung von Patenten absichern lassen. In der Kombination der systematischen Weiterentwicklung des eigenen Schutzrechtsportfolios, der Überwachung der Wettbewerbsaktivitäten und der Absicherung des verbleibenden Risikos über die IP-Versicherung ist ein Unternehmen bestens positioniert (Abb. 4).

Best practice solutions for operational practice

Not every kind of risk management automatically and completely eliminates all risks. IP insurance has proven useful in operational practice particularly for companies exporting to the USA. This kind of insurance includes both liability risks, such as covering compensation payments, and also legal protection for covering legal and court costs. By combining the systematic further development of your own intellectual property rights portfolio with the monitoring of competition activities while also hedging the remaining risk with IP insurance puts your company in the best possible position (Fig. 4).

Die besondere Rolle des Mittelstands am Beispiel des Maschinen- und Anlagenbaus

Beim internationalen Technologiewettlauf kommt den mittelständischen Unternehmen eine besondere Bedeutung zu. Während die Patentanmeldungen der weltweit zehn größten Unternehmen im Maschinen und Anlagenbau zwischen 2005 und 2013 um ca. 40% sank, verdoppelte sich die Gesamtzahl der Patentanmeldungen der im VDMA organisierten Unternehmen (Abb. 5; Abb. 6). Insbesondere der Mittelstand ist also die treibende Kraft, dem es gelingt sich mit Patenten in neuen Technologiefeldern zu positionieren und mit neuen Produkten nachhaltig Wachstum zu generieren.

The special role played by mid-sized businesses, exemplified by the engineering sector

SME companies play an especially important role in the international technology race. While patent registrations from the world's ten largest engineering companies decreased by approx. 40% between 2005 and 2013, the total number of patent registrations by companies organised in the VDMA doubled (Fig. 5; Fig. 6). Mid-sized businesses are therefore the driving force: they use patents to establish a secure position in fields of technology, generating sustainable growth with new products.

Autor:
Dr. Dirk Dantz
dantzhoehne.
PATENT & RECHT, Berlin
http://www.dantzhoehne.de

Author:
Dr. Dirk Dantz
dantzhoehne.
PATENT & RECHT, Berlin
http://www.dantzhoehne.de

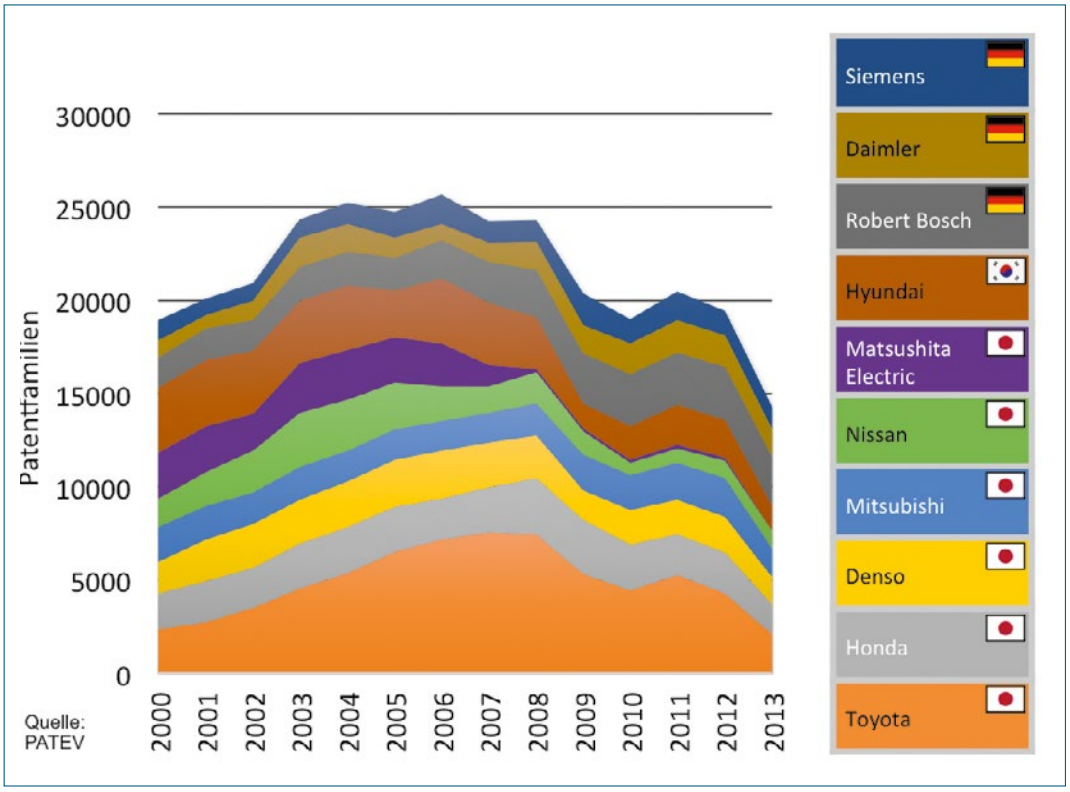


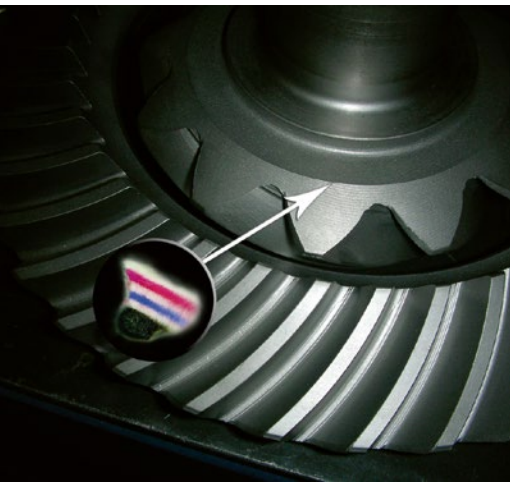
Abbildung 6: Internationale TOP 10 Unternehmen im Maschinen- und Anlagenbau
Figure 6: International top 10 companies in the engineering sector

Quelle: PATEV
Source: PATEV

Know-how in Security-Themen
Corporate expertise for industries

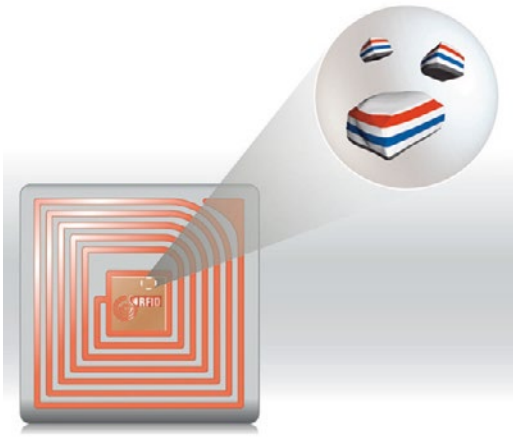
	Unternehmen / *Company*													
	3S	add-yet	Balluff	BORRIES Markiersysteme	Brainloop	Diagramm Halbach	Fraunhofer AISEC	Fraunhofer IPT	GS1 Germany	Hans Turck	HiSolutions	Hoffmann Engineering	Hologram Company RAKO	Innovation IP
Produktkennzeichnung und Produktschutz Kennzeichnungstechnologien sind sichtbare oder unsichtbare Sicherheitsmerkmale, mit denen die Originalität und Echtheit von Produkten nachgewiesen werden können. ***Product identification and product protection*** *Identification technologies are visible or invisible security features that allow the proof of originality and authenticity of products.*	●		●	●		●			●	●			●	
Detektion und Authentifizierung geschützer Produkte Hierbei handelt es sich um Geräte und Systeme, mit denen Sicherheitsmerkmale erkannt, gelesen und auf Originalität überprüft werden. ***Detection and authentication of protected products*** *Devices and systems that detect and identify security features and proof originality.*	●		●	●		●			●	●			●	
Tracking- und Tracingsysteme zur Produktverfolgung Systeme zur Überwachung und Verfolgung von Produkten anhand eindeutiger Sicherheitsmerkmale in der Lieferkette und dem Produktlebenszyklus. ***Track & Trace Systems*** *Systems for monitoring, tracking and tracing of products by unique security features in the supply chain and product life cycle.*	●			●		●			●				●	
Embedded Security in industriellen Produkten und Systemen Schutz des Know-hows, das in Form von Steuerungssoftware, Elektronik und Daten in intelligenten technischen Produkten verborgen ist. ***Embedded Security in industrial goods and systems*** *Protection of know-how that is hidden in control software, electronics or data inside of smart products.*						●	●			●				
Technischer Schutz vor unerwünschtem Know-how-Transfer IT-basierte Technologien zum Schutz von sensiblem Konstruktions-, Fertigungs- und Unternehmens-Know-how. ***Technical Know-how protection solutions*** *IT-based technologies to protect sensitive design, production and business know-how.*	●				●		●				●			
Engineering u. Beratung zum Produkt- u. Know-how-Schutz Für den geplanten Einsatzfall sind Schutztechnologien und Lösungsansätze unabhängig hinsichtlich Nutzbarkeit, Wirtschaftlichkeit und Sicherheitsgrad auf Wirksamkeit zu prüfen. ***Engineering and consulting in product and know-how protection*** *For the intended application, technologies and solutions should be independently checked for effectiveness in terms of usability, efficiency and protection level.*		●				●		●		●		●		●

			●	●	●	Innovent
			●	●	●	KURZ
			●	●	●	OCS Checkweighers
			●	●	●	OpSec Security
●						PATEV
	●					PROSTEP
●			●	●	●	Schreiner ProSecure
			●	●	●	Securikett Ulrich & Horn
	●					SEEBURGER
				●	●	Sensor Instruments
				●		SICK
	●	●	●	●		Siemens
●						Steinbeis Hochschule Berlin
			●	●	●	swiss authentication
			●	●	●	Tailorlux
			●	●	●	tesa scribos
	●					Trend Micro
				●	●	TRUMPF Laser Marking Systems
			●	●	●	U-NICA Solutions
●						UNITY
●						VICCON
	●	●				WIBU-SYSTEMS



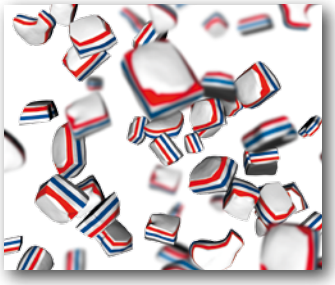
SECUTAG®: Fälschungsschutz für die Automobil- und Maschinenbauindustrie
SECUTAG®: Counterfeit protection for the automotive industry and for mechanical engineering

SECUPACK® sichert Blister, Fläschchen, Tuben und Faltschachteln
SECUPACK® secures blisters, phials, tubes and folded boxes



SECUDATA® kombiniert Rückverfolgbarkeit und Fälschungssicherheit
SECUDATA® combines traceability and counterfeit protection

Fälschungsschutz ist Verbraucherschutz
Counterfeit protection is consumer protection



Mikro-Farbcodes zum Nachweis der Echtheit von Produkt und Marke
Micro colour codes prove authenticity of products and brands

Kennzeichnungssysteme für den rechtssicheren Plagiatschutz

Auf Basis der weltweit kleinsten Mikro-Farbcodes SECUTAG® hat 3S™ mehrere Branchenlösungen für den Fälschungsschutz entwickelt. Damit können u.a. Produkte aller Industriezweige, Ersatzteile, Werkzeuge, Medikamente, Sport- und Lifestyleartikel, Verpackungen und Warenwirtschaftsdaten gesichert werden. Durch die Kombination mit Rückverfolgungssystemen (wie Datamatrix, RFID) kann die gesamte Produktions- und Lieferkette vor Plagiaten geschützt werden.

Komplette Sicherheitslösung aus einer Hand

Die Mikro-Farbcodetechnologie ist vor Gericht als Beweismittel anerkannt und bewahrt vor ungerechtfertigten Schadenersatzansprüchen. Vom Konzept über die Produktion und Auslieferung bis hin zu nachgelagerten Dienstleistungen liefert der Komplettanbieter 3S™ Unternehmen aller Branchen die optimale Strategie in Sachen Produkt- und Knowhow-Schutz.

Labelling systems for legally binding counterfeit protection

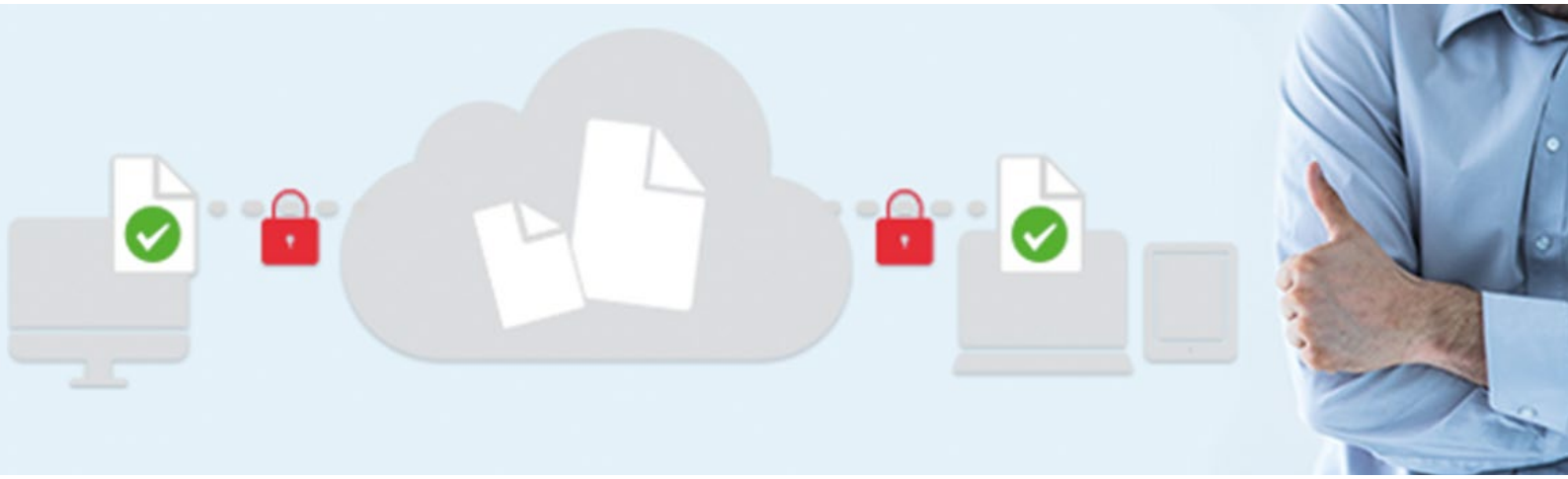
On the basis of the world's smallest micro colour codes SECUTAG®, 3S™ has developed industry-specific solutions for brand and product protection. This reliable security concept protects products from all industry sectors, including spare parts, tools, drugs, sporting goods, lifestyle articles, packaging and ERP data, among others. In combination with traceability systems (such as data matrix, RFID), the entire production and supply chain can reliably be secured against counterfeiting.

Full range of security solutions from one source

The micro colour code technology is accepted as evidence by court and protects businesses from unjustified claims. From the concept stage to production and from supply to downstream services, the full-service supplier 3S™ provides the optimal product and IP protection strategy for companies of all sizes in all industries.

3S Simons Security Systems GmbH • Lise-Meitner-Str. 6 • 48301 Nottuln • Germany
Phone +49 2502 2333-0 • E-Mail info@secutag.com
Internet www.secutag.com

Vertrauliche Informationen vor unbefugtem Zugriff schützen
Protect your confidential information from unauthorised access



Die Digitalisierung erfordert neue Konzepte für die Zusammenarbeit im Unternehmen und darüber hinaus. Brainloop ermöglicht einen kontrollierten Informationsaustausch für den Schutz von Geschäftsgeheimnissen und Know-how.

Digital transformation requires new concepts for collaboration within the company and beyond. Brainloop provides a controlled environment for information sharing – for the protection of your trade secrets and expertise.

Informationsaustausch und Zusammenarbeit

Die Gefahr, dass Informationen in falsche Hände geraten, ist größer als je zuvor. Brainloop Lösungen verbinden Security mit Usability und ermöglichen es Mitarbeitern, verantwortungsbewusst zu arbeiten: Sie verschieben Dateien, die sie mit anderen Teams, Partnern oder Lieferanten austauschen wollen, einfach in die Cloud-basierten Lösungen. Dort können sie einzig von berechtigten Personen angeschaut oder bearbeitet werden.

Information sharing and collaboration

The danger of your information falling into the wrong hands is greater than it has ever been. Brainloop solutions combine security with usability, making it easier for your staff to work in a responsible way. All they need to do is move the files they want to share with other teams, business partners and suppliers into the cloud-based solution. Once there, the files can only be viewed or worked on by people with the relevant permissions.

Auf Nummer sicher

Zahlreiche Unternehmen vertrauen auf die führende Sicherheitstechnologie: Ende-zu-Ende-Verschlüsselung, 2-Faktor-Authentifizierung, Administrator-/Provider-Abschirmung, Verschlüsselung auf allen Endgeräten, Nachvollziehbarkeit, Datenspeicherung in Deutschland oder anderen europäischen Ländern. **Brainloop.einfach.sicher.**

Top-flight security

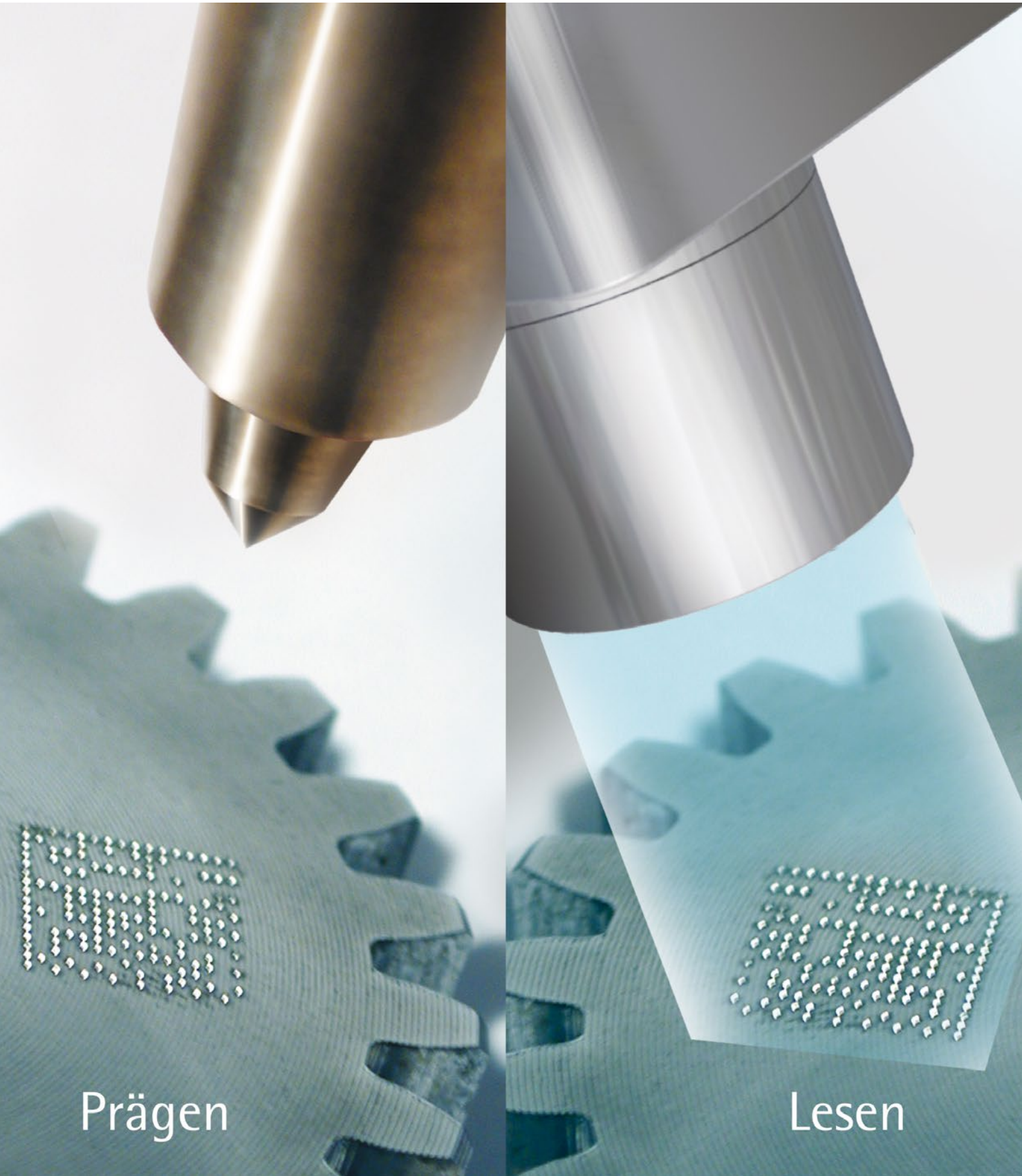
Many companies trust Brainloop's leading security technology, which features end-to-end encryption, 2-factor authentication, administrator and provider shielding, file encryption on all user devices, traceability, and data storage in Germany or other European countries. ***Brainloop. simple. secure.***

SecurITy made in Germany
TeleTrusT Quality Seal www.teletrust.de/itsmig

brainloop

Brainloop AG • Franziskanerstr. 14 • 81669 München • Germany
Phone +49 89 444699-0 • E-Mail info@brainloop.com
Internet www.brainloop.com

Dauerhafte Produktkennzeichnung – Produkt und Marke verteidigen
Permanent product marking – defending product & label



Die Produktpiraterie ist heute weit verbreitet und ihre Formen sind vielfältig. Sie reichen vom plumpen Formennachbau bis zu professionellen Plagiaten, bei denen selbst Experten das Original kaum von der Fälschung unterscheiden können.

Nowadays piracy of products is very common and their forms are multifaceted. They can be just a simple replica of the product's form but also be professional rip-offs, which sometimes even experts cannot differ in original and the fake.

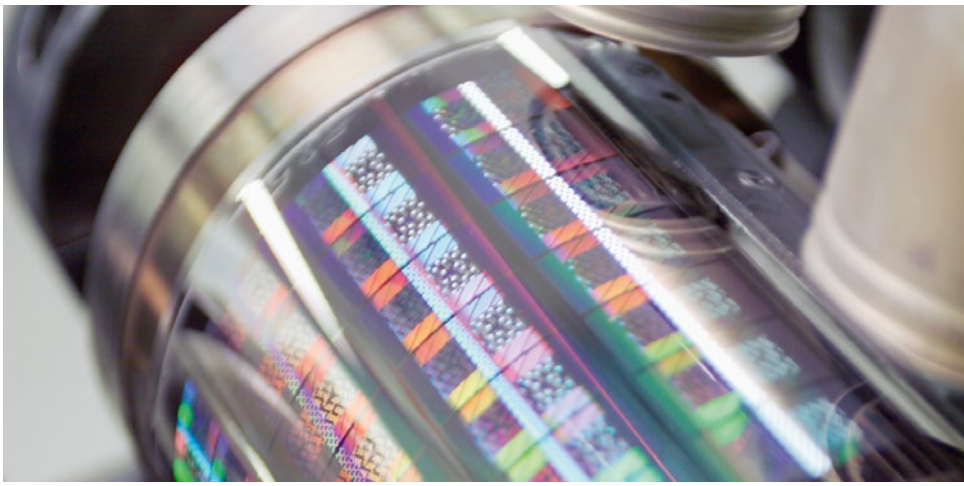
Prävention statt Reaktion: Produktkennzeichnung
Prävention ist der beste Schutz. Denn ist der Schaden erst einmal angerichtet und das Plagiat im Umlauf, wird es aufwendig, sich das Recht am eigenen Produkt und der eigenen Marke zurück zu erobern. Bei den technischen Kopierschutzmaßnahmen sind Produktkennzeichnungen das am häufigsten eingesetzte Mittel. Dazu gehören Identifikationssysteme wie der DataMatrix-Code. Mit dieser fehlerredundanten Kennung lässt sich die Originalität der Produkte beweisen und die Nachverfolgbarkeit sichern.

Der DataMatrix-Code wird in Sekundenschnelle per Nadelprägung direkt auf den Bauteilen angebracht. Eine digitale Kamera erfasst die Informationen. Alle weiteren Produktionsschritte werden dann über den Code erfasst. Fälscher können ein Bauteil, nicht aber den Code-Algorithmus kopieren. Der Originalcode ist ein Unikat und alle dazugehörigen Informationen beim Hersteller hinterlegt. BORRIES Markier-Systeme produziert Maschinen und Werkzeuge für die direkte, materialverdrängende und dauerhafte Kennzeichnung, die in jeder Branche eingesetzt werden kann.

Prevention instead of reaction: Product marking
Prevention is the best protection. Because if the damage is done and the plagiarism is in circulation, it will be hard to get back the rights of the own product and the own label. Product marking is the most common instrument for technical copy protection. This includes identification systems like the DataMatrix-code. This fault redundant identification will help to prove the originality of products and secure the traceability.

Within seconds the DataMatrix-Code will be placed on the component part with help of a Stylus marker. A digital camera will register the information. All the following production stages will be registered within this code. Counterfeits can copy the component parts but won't be able to copy the code algorithm. The original code is a unique copy and all the information is secured at the producer's. BORRIES Marking Systems produces machines and tools for direct and permanent marking. You can find our marking systems worldwide: in the automobile industry as well as their suppliers, aerospace industry, manufacturing systems engineering, electronic and steel industry as well as medical engineering.

BORRIES MARKIER-SYSTEME
BORRIES Markier-Systeme GmbH • Siemensstraße 3 • 72124 Pliezhausen • Germany
Phone +49 7127 9797-0 • E-Mail info@borries.com
Internet www.borries.com



Die RAKO Group – Vorsprung durch Sicherheit.
The RAKO Group – Lead Through Security.

Die RAKO Group ist einer der führenden Hersteller von Haftetiketten. 90 der modernsten Druckmaschinen und über 1.500 Mitarbeiter verteilen sich auf 13 Standorte weltweit. Mehr als 1.000 Kunden vertrauen auf die Expertise, Kreativität und Innovationskraft des Unternehmens.

The RAKO Group is one of the leading manufacturers of self- adhesive labels. 90 state-of-the-art printing presses and over 1,500 employees distributed among 13 production facilities worldwide. More than 1,000 customers rely upon the expertise, creativity and innovative capacity of the company.

Führend im Digital Druck

Die RAKO Group bietet den größten und modernsten digitalen Druckmaschinenpark für Haftetiketten und flexible Verpackungen.

Leaders in the field of digital printing

The RAKO Group has the largest and state-of-the-art digital machine pool for self- adhesive labels, and flexible packaging.

Elektronische Etiketten aus erster Hand

Die RAKO Security-Label Produktsicherungs GmbH entwickelt, produziert und vertreibt Produkte aus dem Bereich RFID/NFC und der elektronischen Artikelsicherung (EAS) für ein breites Anwendungsspektrum der kontaktlosen Identifikation.

Electronic labels from one source

RAKO Security-Label Produktsicherungs GmbH develops, produces and sells products for the field of electronic article surveillance (EAS) and radio frequency identification (RFID) for a wide range of applications of contacless identification.

Sicherheitsetiketten auf höchstem Niveau

Ein führender Hersteller im Bereich des Produkt- und Markenschutzes ist die Hologram Company. Weltweit setzen namhafte Kunden das Nanogram erfolgreich zum Schutz gegen Fälschungen und Nachahmungen ein.

Security labels of the highest level

Leading manufacturer in the field of product and brand protection is Hologram Company. Reputable customers worldwide successfully use the Nanogram against counterfeits and forgeries.

RAKO GROUP®

RAKO Group
Möllner Landstraße 15 • 22969 Witzhave • Germany
Phone +49 4104 693-100 • E-Mail info@rako-etiketten.com
Internet www.rako-gruppe.de

INDUSTRIE 4.0
Das RAKO LABEL 4.0 zeigt die einzigartige Kompetenz- und Produktionsvielfalt sowie Innovationskraft der RAKO Group für die Industrie 4.0.

INDUSTRIE 4.0
The RAKO LABEL 4.0 shows the unique variety of competence, innovative capacity and production skill of the RAKO Group for the industrie 4.0.

digital · smart · secure

DIGITAL
Die digitale Drucktechnologie bietet mit hochqualitativer Bildwiedergabe, variablem Datendruck, Inline-Farbregelsystem und 100% Kontrolle inklusive Code-Verifizierung einzigartige Gestaltungsmöglichkeiten sowie die Kombination mit offenen und versteckten Sicherheitsmerkmalen.

DIGITAL
The digital printing technology offers high quality printing with variable data, Inline color control system and 100%-camera inspection including code-verification as well as the combination with overt and hidden security features.

SMART
Durch Kombination von zwei RFID-Technologien wird das Etikett intelligent. Logistik, Authentifizierung und Kundeninteraktionen werden dank neuester Chips mit integrierten Verschlüsselungsverfahren abgesichert.

SMART
By the RFID combination of EPC and NFC your label will be intelligent. Logistic, authentification and customer interaction will be secured through cutting-edge chip technologies, containing cryptographic security techniques.

SECURE
Hochsicherheitsschutz gegen Fälschungen bietet das Nanogram mit 1,5 Mio dpi und einer hoch entwickelten Prägetechnik.
Garantiert nicht kopierbar und optisch eindrucksvoll sind Originale von Kunden, Zoll und Kontrolleuren sofort zu erkennen.

SECURE
The Nanogram offers the highest level of security against forgeries with a resolution of 1,500,000 dpi and a high- end recording technique.
Guaranteed forgery-proofed and the eye-catching appearance makes it easy to identify the original for customers, customs and internal inspectors.

Scan this code for more information!

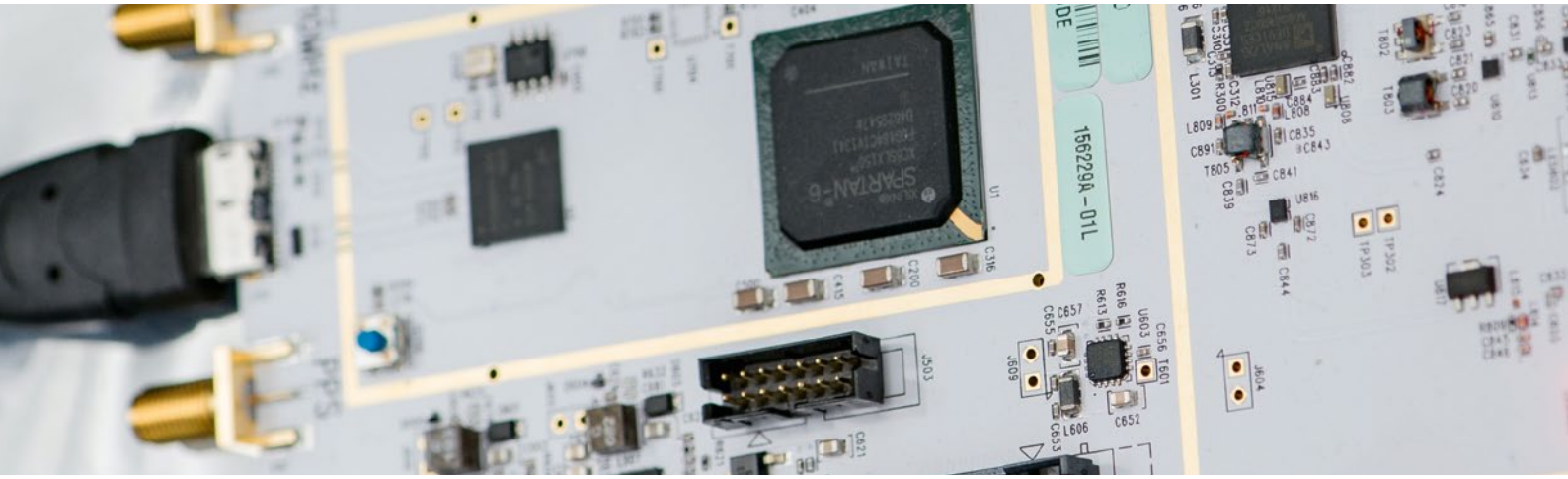
Setzen auch Sie auf DAS ETIKETT der Zukunft, und auf einen starken, kompetenten und verlässlichen Partner – die RAKO Group.

Rely on THE LABEL of the future and on a strong, professional and reliable partner – the RAKO Group.

HOLOGRAM COMPANY®
MEMBER OF THE RAKO GROUP

Hologram Company RAKO GmbH
Möllner Landstraße 15 • 22969 Witzhave • Germany
Phone +49 4104 693-250 • E-Mail info@hologram-company.com
Internet www.hologram-company.com

Firmware-Schutz ist Pflicht
Firmware Protection is a Must



Die Absicherung eingebetteter Systeme (Steuerungselektronik und Firmware) bildet beim Schutz von Investitionsgütern wie Maschinen und Anlagen das wichtigste Bollwerk gegen Produktpiraten. Technische Lösungen verhindern das Auslesen und die Analyse und somit den Nachbau der Komponenten. Eine Kombination aus Hardware- und Software-basierten Maßnahmen bietet den besten Schutz.

Securing embedded Systems (electronic control units and firmware) is a decisive factor in protecting capital goods such as machines and plants against piracy. Technical solutions hinder extraction and analysis and thus prevent copying of components. A combination of hardware-based and software-based measures provides comprehensive protection.

Firmware-Verschlüsselung verhindert einen vollständigen Nachbau von Maschinen und Anlagen. Die zugehörige Entschlüsselung kann nur mit Original-Hardware erfolgen. So fehlen Nachbauten wichtige Schlüsselwerte – deren Steuerungselektronik funktioniert nicht. Fraunhofer AISEC bietet praxiserprobte Lösungen für den Schutz von Firmware-Code an. Die Schlüsselwerte kennt nur der Produkthersteller selbst. Die verschlüsselte Datei kann gefahrlos verteilt werden. Ein Angreifer kann ohne den geheimen Schlüssel nicht den ursprünglichen Inhalt rekonstruieren oder die Firmware mit gefälschter Hardware betreiben. Die Implementierung zusätzlicher Verschleierungstechniken erhöht das Schutzniveau.

Firmware encryption effectively prevents the copying of machines and plants. The associated decryption is only possible with original hardware so the copies lack the essential keys and their control units do not work properly. Fraunhofer AISEC offers practically proven solutions for the protection of firmware. Only the product manufacturer knows the associated keys. The encrypted files can be distributed with no risk. Without the secret key, attackers cannot reconstruct the original content or use the firmware to operate forged hardware. The protection level can be enhanced by implementing additional obfuscation methods.

Fraunhofer AISEC

Fraunhofer AISEC • Parkring 4 • 85748 Garching bei München • Germany
Phone +49 89 322 9986-0 • E-Mail product-protection@aisec.fraunhofer.de
Internet www.aisec.fraunhofer.de

KURZ ist ein internationaler Hersteller funktionaler und dekorativer Beschichtungen. Die Heißprägetechnologie von KURZ ist allgegenwärtig: auf Verpackungen, Elektronik- und Haushaltsgeräten, auf Kosmetikartikeln, Textilien, Möbeln, Kraftfahrzeugteilen und vielem mehr.

KURZ is an international manufacturer of functional and decorative coatings. KURZ's hot stamping technology is widely used: it can be found on packaging, electronic devices and household appliances, on cosmetics, textiles, furniture, automotive parts and many more applications.

BRAND ENHANCEMENT BY KURZ®
Protect – Decorate – Communicate

Markenschutz, Markendekoration, Markenkommunikation

Im Produktschutzbereich ist KURZ ein weltweit renommierter Lieferant optischer Sicherheitslösungen. Das Unternehmen bietet umfassende Konzepte für Markenschutz, Markendekoration und Markenkommunikation. Schwer kopierbare holografische Echtheitskennzeichen vom Typ TRUSTSEAL® werten Marken optisch auf, geben dem Verbraucher Sicherheit und bieten hohen Fälschungsschutz.

Diese optischen Sicherheitsmerkmale sind mit dem webbasierten Identifikationssystem TRUSTCODE® kombinierbar. Das TRUSTCODE®-System verbindet die reale mit der virtuellen Welt: Über verschiedene Scanprozesse per Smartphone können umfangreiche Produktinformationen für Käufer, Händler, Zoll und Markenartikler abgerufen werden.

Brand protection, brand decoration, brand communication

In the field of product protection, KURZ is a world-renowned supplier of optical security solutions. The company offers comprehensive concepts for brand protection, brand decoration and brand communication. The TRUSTSEAL® range of difficult to copy holographic authenticity features visually enhance the brand, build consumer confidence, and provide a high level of counterfeit protection.

These optical security features can be combined with the web-based TRUSTCODE® identification system. The TRUSTCODE® system connects the real world to the virtual one: detailed product information can be accessed by buyers, retailers, customs officials and brand owners using different smartphone scanning processes.

KURZ

LEONHARD KURZ Stiftung & Co. KG • Schwabacher Str. 482 • 90763 Fuerth • Germany
Phone +49 911 7141-0 • E-Mail sales@kurz.de
Internet www.kurz.de • www.brand-enhancememt.com

Zukunftssicher: Serialisierung und Aggregation von OCS Checkweighers
Future proof: Serialisation and Aggregation from OCS Checkweighers

Inspektionslösungen von OCS Checkweighers für die dynamische, schnelle und hochpräzise Gewichts- und Vollständigkeitskontrolle sind seit Jahren zuverlässiger Standard in den Produktionslinien führender Hersteller in der Pharma-, Kosmetik-, Food- und Chemieindustrie.

Aufbauend auf diesen Erfahrungen mit individuellen Hightech-Applikationen und mit Blick auf die von der Europäischen Kommission geplante Einführung einer verbindlichen Kennzeichnung von Medikamenten hat OCS sein Produktportfolio um eine einzigartige Produktfamilie ausgebaut.

Das Traceable Quality System (TQS) ist eine umfassende Track & Trace-Lösung. Es beinhaltet zum einen die Serialisierung der einzelnen Verpackungseinheit und zum anderen deren durchgängige Aggregation, die Voraussetzung ist für einen nachvollziehbaren Produktfluss vom Pharmahersteller über den Handel bis zum Patienten.

Das Ziel dieser gemeinsamen Anstrengungen ist ein optimierter Verbraucherschutz und die nachhaltige Bekämpfung von lebensbedrohlicher Produktpiraterie.

TQS als Instrument für optimierten Verbraucherschutz

TQS ist ein intuitiv zu bedienendes System, das größtmögliche Flexibilität mit einfachster Handhabung kombiniert. Die Bedienung aller drei Funktionseinheiten (Produkthandling, Codierung und Kamerainspektion) erfolgt vollständig integriert aus nur einer Software heraus. Diese Durchgängigkeit erstreckt sich über alle Aggregationsstufen. TQS steht für höchste Sicherheit und einfachste Handhabung. Es verhindert zuverlässig Fehlbedienungen und Schnittstellenkonflikte.

Serialisierung und Aggregation mittels TQS (Traceable Quality System)
Serialisation and aggregation by means of TQS (Traceable Quality System)

For many years, the dynamic, fast, and highly accurate product inspection systems for weight and completeness checks from OCS Checkweighers have provided the reliable standard for the production lines of the leading manufacturers in the pharmaceutical, cosmetic, food, and chemical industries.

Building on its experience with custom, high tech applications and with an eye towards the European Commission's planned introduction of mandatory labeling of drugs, OCS has expanded its product portfolio by the addition of an extraordinary, new product family.

The Traceable Quality System (TQS) is a comprehensive Track & Trace system. It covers the serialisation of the individual packing units and their continuous aggregation. The requirement is to achieve a traceable product flow – from drug manufacturer, through the distribution chain, to the patient.

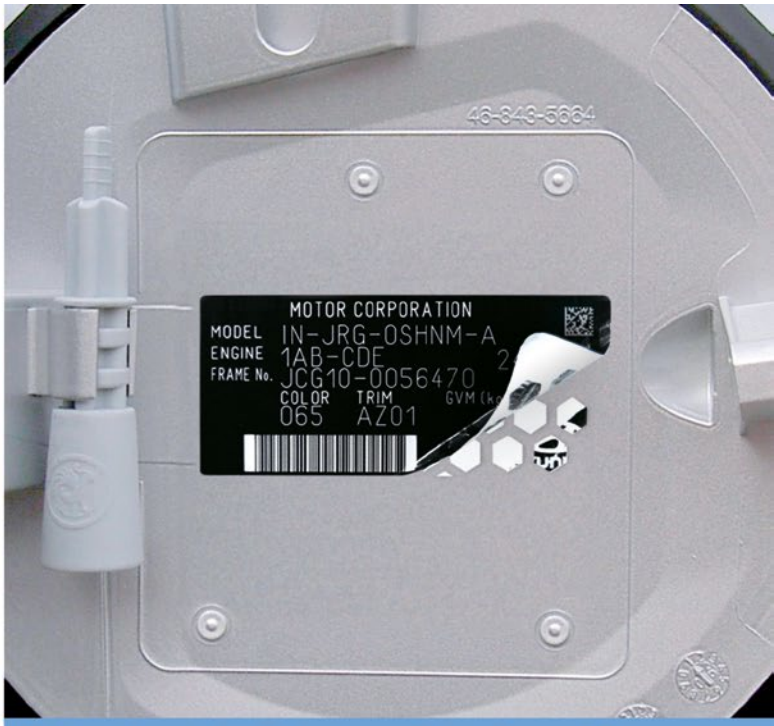
The result of this joint effort is optimal consumer protection and another weapon in the long term fight against life threatening product piracy.

TQS – a tool to optimise consumer protection

TQS is an intuitively operated system, which combines the greatest possible flexibility with easy handling. A fully integrated single software product manages the operation of all three functional units (product handling, coding, and camera inspection). This thorough integration continues across all levels of aggregation. The TQS system reliably prevents operating errors and interface problems, while delivering the maximum safety and the greatest ease of use.

Individuelle Kennzeichnung – zuverlässiger Produktschutz
Customized Marking – Reliable Product Protection

Serialisierung und mobile Echtheitsprüfung
Serialization and mobile authentication



Manipulationsschutz für laserbeschriftbare Typenschilder
Tamper protection for laser-markable labels

Logistiketiketten zur Graumarktüberwachung von Lieferketten
Logistics labels for gray market monitoring of supply chains

Individuelle, verborgene Echtheitsmerkmale – beständig bis 2000°C
Individual, covert authentication features – resistant up to 2000 °C

Hochwertiges Originalteil oder mangelhaftes Imitat? Diese Frage stellt sich zunehmend auch im Maschinen- und Anlagenbau. Als Spezialist für Funktions- und Kennzeichnungslösungen entwickelt und produziert Schreiner ProTech gemeinsam mit den Sicherheitsexperten von Schreiner ProSecure individuelle Produktschutz- sowie Track & Trace-Lösungen für Manipulationsschutz, Echtheitsprüfung und Rückverfolgung entlang der Distributionskette.

A high-grade original component or an inferior copy? This question increasingly arises in machinery and plant engineering as well. As a specialist in functional and marking solutions Schreiner ProTech, together with the security experts from Schreiner ProSecure, develops and produces customized product protection and track & trace solutions for tamper protection, authentication and monitoring of the distribution chain.

Eine ideale Kennzeichnungslösung verbindet einen optischen Fälschungsschutz mit einer Serialisierungslösung wie KeySecure. Bei diesem System erhält jede Verpackung oder jedes Bauteil einen 15-stelligen Code, der in jeder Phase der Distribution die Authentifizierung per Internet, Smartphone oder Hotline erlaubt. Die Serialisierung allein gewährt jedoch keinen Fälschungsschutz, weil sie leicht kopiert werden kann.

An ideal marking solution combines visual counterfeit protection with a serialization solution such as KeySecure. When using this system, every packaging or component is provided with a 15-digit code that enables internet, smartphone or hotline based authentication in any stage of distribution. However, the serialization alone does not guarantee protection against counterfeiting because it is easy to copy.

Kombination mit zuverlässigem Fälschungsschutz
Kosteneffizient, hochsicher und einfach in die Fertigung integrierbar ist BitSecure: Kopiert ein Fälscher das hoch aufgelöste Zufallsmuster werden weniger Details angezeigt. Diese Abweichungen sind mit einem Datamatrix-Scanner oder mobil per Smartphone-App nachweisbar. Auch bietet sich zum Beispiel die Kombination mit einer verborgenen Markierung mit geruchs- und farblosen Spezialpigmenten an, die nur mit speziellen Lesegeräten nachweisbar sind.

Combination with Reliable Counterfeit Protection
The copy detection pattern BitSecure is cost-effective, highly secure and easy to integrate into the production process. When a counterfeiter copies the high-resolution random pattern, the copy will indicate fewer details. These discrepancies are verifiable with a code scanner or by using a smartphone app. The authentication pattern can be inconspicuously integrated into any nameplate. Also the combination with a covert feature containing very durable, odorless and colorless taggants or microparticles that can only be detected by special readers is possible as well.

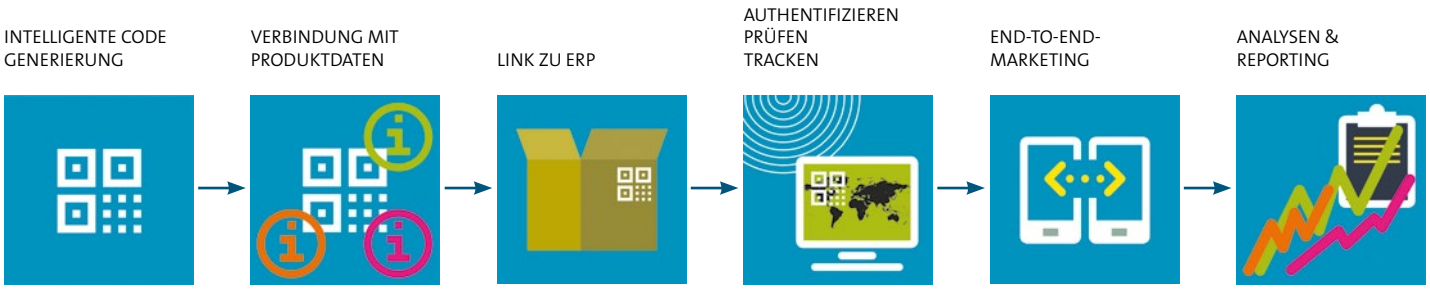
Individuelle Beratung, leistungsstarke Forschung & Entwicklung
Schreiner ProTech und Schreiner ProSecure entwickeln für Sie maßgeschneiderte Sicherheitssysteme, die sich optimal in bestehende Produktions- und Distributionsabläufe integrieren lassen.

Individual Consulting, Powerful Research & Development
Schreiner ProTech and Schreiner ProSecure will develop tailored security systems for you that can be optimally integrated into existing production and distribution processes.

Weitere Infos unter
For more information go to

schreiner ProTech

Schreiner ProTech, a business unit of Schreiner Group GmbH & Co. KG
Bruckmannring 22 • 85764 Oberschleissheim • Germany
Phone +49 89 31584-5251 • E-Mail info@schreiner-protech.com
Internet www.schreiner-protech.com



Schützen Sie Ihre Marke | Erhöhen Sie Ihre Marktanteile | Steigern Sie die Kundenbindung

protect your brand | increase market share | drive customer loyality

CODIKETT®

CODIKETT® ist eine skalierbare und zukunftssichere Lösung für die Produktverfolgung, Graumarkterkennung in globalen Märkten und für den Einstieg in das End-to-End Marketing.

Von der Bereitstellung sicherer Codes über die geeignete Integration in die Lieferprozesse bis hin zur differenzierten Authentifizierung durch alle Beteiligten wird das gesamte Spektrum des Produkt- und Markenschutzes unterstützt.

Das Team von CODIKETT® berät dabei in allen Belangen der Planung und Integration bis zur Betriebseinführung. Die aktive Mitarbeit im ISO Komitee TC292 garantiert die Konformität zu ISO 16678 . SECURIKETT® ist zertifizierter GS1 solution provider und CODIKETT® ist angebunden an das WCO Tool IPM.

CODIKETT® ist als modulare SaaS-Lösung (Software as a Service) in der Einstiegsvariante STANDARD sofort einsatzbereit. Die weiteren Ausbaustufen PROFESSIONAL und ENTERPRISE erhöhen die Wertschöpfung durch weiterführende Mehrwertdienste (Schnittstellen zu ERP, Track & Trace, RFID, Reporting).

CODIKETT® is a scalable, future-proof and cost effective solution that supports the authentication of products, the detection of grey market activities and the entry into end-to-end marketing.

CODIKETT® delivers unique and secure codes that can be applied direct to product, labels or packaging and be seamlessly integrated in to the existing supply chain, with the potential for differentiated authentication by all stakeholders. The entire spectrum of product and brand protection is supported.

The team of CODIKETT® is experienced to advise on all aspects of planning, integration and operation. Active membership and participation in the ISO committee TC292 guarantees conformance to ISO 16678. SECURIKETT® is certified GS1 solution provider and CODIKETT® is linked to the WCO tool IPM.

CODIKETT® is a modular, ready to use SaaS solution (Software as a Service). Beside the entry-level version STANDARD, higher system levels of PROFESSIONAL and ENTERPRISE are available to fulfill more demanding needs and to further enhance the benefits of the CODIKETT® solution (Interfaces to ERP, Track & Trace, RFID, Reporting).

www.codikett.com

MANIPULATIONSSICHERHEIT

TAMPER EVIDENCE

AUTHENTIFIZIERUNG

AUTHENTICATION

IDENTIFIZIERUNG

IDENTIFICATION

SECURIKETT® entwickelt und produziert innovative Sicherheitslösungen, mit denen die Echtheit von Produkten leicht erkennbar und nachweisbar gemacht wird. Diese werden weltweit für zahlreiche Branchen erfolgreich eingesetzt.

Durch proprietäre Technologien ist SECURIKETT® führend in der Umsetzung von Manipulationssicherheit. Kundenspezifisch kombiniert mit variablen Codierungen sowie offenen und verdeckten Sicherheitsmerkmalen ist das die wesentliche Grundlage für:

- Sicheres Versiegeln von Faltschachteln und Verpackungen
- Direktmarkierung von Produkten
- Unterstützung von Dokumentationsabläufen

Sicherheitslösungen mit SECURIKETT®-Etiketten wenden sich gleichermaßen an Kunden, Supply Chain Mitglieder und Markeninhaber, da das Konzept auf verdeckten und offenen bzw. leicht verständlichen Sicherheitsmerkmalen basiert. In Kombination mit CODIKETT® wird das gesamte Spektrum des Markenschutzes und der Graumarktbekämpfung abgedeckt.
Ihre Argumente für SECURIKETT®:

- One-Stop-Shop für den Markenschutz
- "Best in class" in Sicherheitsetiketten
- Spezialisten für Codierung und integriertes Datenmanagement

SECURIKETT® ist Mitglied der Ulrich Gruppe.

SECURIKETT® develops and manufactures innovative security solutions, by which the authenticity of products can be easily proven. These solutions are being used successfully and extensively deployed across various industries globally.

By leveraging proprietary technologies SECURIKETT® continues to be a leading provider of tamper evident identification solutions. Identification solutions are custom made, and combined with variable, unique and secure codes, linked to overt and covert layered security features, this is the important base for:

- *Secure sealing of folding boxes and packaging*
- *Direct marking of products*
- *Support compliance documentation processes*

Security identification solutions by SECURIKETT® may be communicated to both consumers (e.g. marketing purposes) and defined specialist stakeholders (enforcement etc), as the concept builds on a mix of both covert an overt technologies, so ensures that the security features are easily understood. CODIKETT® can protect and support the whole range of brand protection and has the benefit of identifying and deterring grey market activity.
Your arguments for SECURIKETT®:

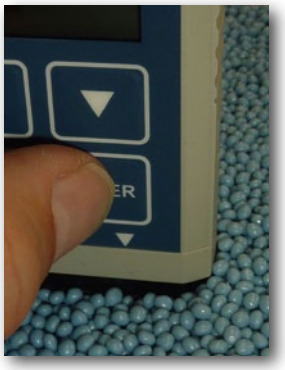
- *One-stop-shop for brand protection*
- *Best in class security labels*
- *Code and integrated data management specialists*

SECURIKETT® is a member of the Ulrich Group.

Securikett Ulrich & Horn GmbH • Strasse 10, Objekt 48
2355 Wiener Neudorf • Austria
Phone +43 2236 677925 • E-Mail office@securikett.com
Internet www.securikett.com

Wirtschaftliche Lösungen für die Einfache Produktauthentifizierung
Cost-effective Solutions for Simple Product Authentication

Detektion eines verdeckten Merkmals im Druck
Detection of a hidden characteristic in print



Rohstoffkontrolle am Wareneingang
Inspection of raw materials on receipt of goods

Sensor Instruments ist ein innovatives deutsches Unternehmen im Bereich der optischen Sensortechnologien. Seit mehr als 10 Jahren entwickeln wir Detektoren für den Schutz gegen Produktpiraterie.

Sensor Instruments is an innovative German company which operates in the area of optical sensor technology. We have been working with optical technologies for anti-counterfeiting applications for more than 10 years.

Zusammen mit unseren Netzwerkpartnern bieten wir unseren Kunden Lösungen für die „Einfache Produktauthentifizierung". Einfache Produktauthentifizierung beschreibt eine einfach zu handhabende, wirtschaftliche, flexible und sichere Methode, ein Originalprodukt schnell von einer Fälschung zu unterscheiden.

Flexibel heißt, dass man die, für das menschliche Auge unsichtbare Markierung auf vielfältige Weise fest in das Produkt, in die Verpackung oder in eine bestehende Kennzeichnung (Etiketten, Aufdrucke, Logos, ...) quasi als Add-on einbringen kann. Wirtschaftlich, weil die Einbringung des Markers keine großen Investitionen zur Anpassung der Produktionsprozesse erfordert. Die Einführung der Authentifizierungslösung kann also schnell umgesetzt werden. Zusätzlich sind selbst kleinste Konzentrationen der Marker nachweisbar, welches die variablen Kosten reduziert!
Unsere Lösungen basieren auf Technologien, die sich schon länger im Hochsicherheitsbereich bewährt haben. Unsere Sicherheitspigmente sind sehr robuste und langlebige Materialien, die selbst durch Temperaturen von mehreren hundert Grad Celsius nicht beeinträchtigt werden. Je nach Anforderung stehen verschiedene Sicherheitsstufen zur Verfügung.

Die Authentifizierung kann mit Hilfe unserer leicht zu bedienenden, kompakten Handdetektoren einfach und schnell durchgeführt werden. Natürlich unterstützen wir unsere Kunden in der Planung, Entwicklung und Implementierung ihrer spezifischen einfachen Authentifizierungslösung.

Together with our network partners we provide solutions for "Simple Product Authentication" to our customers. Simple Product Authentication comprises a simple to handle, flexible, cost-effective, and secure method to distinguish an original product from the counterfeit quickly.

Flexible means that the marker which is invisible for the human eye can be integrated in versatile fashions into the product or an existing labelling (bar code on 2D-labels, imprints, logos ...). The marker functions can be introduced as a simple add-on. Cost-effective, because the introduction of the authentication marker does not require big investments in adapting production processes. This also means the introduction of the Simple Authentication can be managed within a short time frame. Additionally even very small concentrations of the marker can be detected, which saves variable cost. Our solutions utilize technologies, which have been applied and proven for many years in high security applications, e.g. banknote printing. The applied security pigments are very robust and offer high stability as well as a long-life cycle. Temperatures of several hundred degrees Celsius do not impact their effectiveness. Depending on customer requirements different security levels are available.

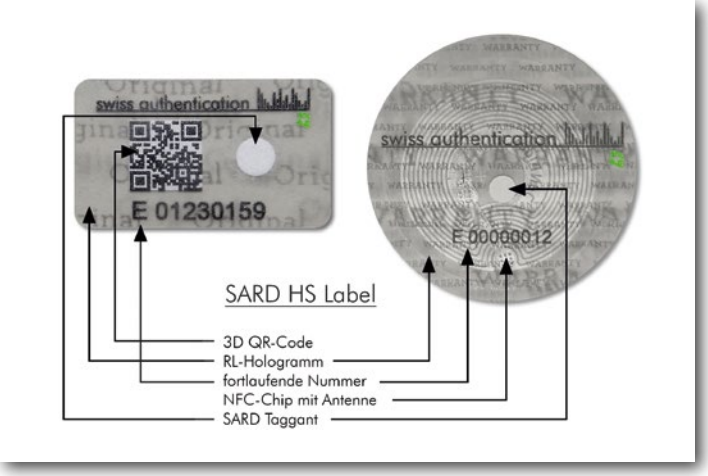
The verification of the Simple Authentication feature can be managed at any place with easy-to-operate handheld detectors. In order to support our customers in their effort to plan, develop and implement their specific Simple Authentication solution.

Sensor Instruments Entwicklungs- und Vertriebs GmbH • Schlinding 11
94169 Thurmansbang • Germany
Phone +49 8544 9719-0 • E-Mail info@sensorinstruments.de
Internet www.sensorinstruments.de

Ihr Spezialist für Produkt- und Dokumentenschutz
your specialist in brand and document protection

Die SARD mit Hauptsitz in der Schweiz ist eine weltweit tätige Unternehmung, die sich auf den Produkt- und Dokumentenschutz spezialisiert hat. Mit kundenspezifischen Sicherheitskonzepten bietet sie massgeschneiderte, zuverlässige Sicherheitslösungen auf hohem Niveau und stellt den Kundennutzen in den Vordergrund.

Based in Switzerland, Swiss Authentication is a global company specializing in brand and document protection. Using customized security concepts, Swiss Authentication offers tailor-made, reliable premium security solutions and puts clientbenefits first.



Die SARD Substanz

Die weltweit einzigartige und patentierte SARD Substanz (Nanosubstanz in Pulverform) ist hitzebeständig bis 1'500 Grad Celsius, resistent gegen Säuren, hat eine faktisch unendliche Haltbarkeit und ist toxikologisch unbedenklich. Unter Verwendung eines von SARD hergestellten Detektors ist die forensisch zuverlässige Authentifizierung möglich. Der Code in Pulverform wird als Markierung auf einem Produkt aufgetragen. Die in der Substanz programmierten Informationen lassen sich in Form von Text, Zahlen oder Bildern mit einem lasergestützten Detektor identifizieren.

Die SARD bietet 3 unterschiedliche Preis- und Sicherheitskategorien an; der Kunde ist hier in der Lage, die Fälschungssicherheit wirtschaftlich in den Verkaufspreis einzukalkulieren.

Elektronische Authentifizierung

Die chipbasierte Sicherheitstechnologie bietet eine individualisierte Sicherheit pro Kunde und Produkt. Durch den Einsatz von unserem ASIC (application specific integrated circuit) und der implementierten, chiffrierten Software kann der Hersteller sicherstellen, dass beispielsweise ein komplexes medizinisches System nur dann läuft, wenn alle Komponenten Originale sind. Eine Implementierung in bestehende Systeme ist mit wenig Aufwand möglich. Eine Eindrahtverbindung als Schnittstelle zur Host-CPU wird durch einen chiffrierten, öffentlichen und privaten Schlüssel gesichert. Die Verschlüsselung ist analog zu heutigen Zahlungssystemen. Über die Host-Software wird entschieden, was beim Einsatz von nicht-originalen Komponenten geschehen soll (Warnung, Abschalten, Melden an Hersteller etc.).

All-in-Label Authentifizierung

Das All-in-Label ist eine Kombination zwischen einer völlig neuen Hologrammtechnik, verbunden mit einem NFC Chip, einer auf das Hologramm aufgedruckten fortlaufenden Seriennummer und der SARD Markierung. Hiermit werden 5 Anforderungen gleichzeitig erfüllt: visuelle Erkennung, Nachverfolgbarkeit, individueller Informationseinbau, Seriennummer und absolut sichere Authentifizierung.

The SARD substance

The patented SARD taggant is unique (specially formulated nano-substances) and heat resistant to 1'500 °C, resistant to acid chemicals, has an infinite shelf life and is non toxic. The encrypted information is easily decoded by using our SARD detector. The taggant is added onto a product. The taggant solution can be encoded with whatever identification is desirable (serial numbers, text or pictures) and is decoded by using an infrared laser.

SARD offers three levels of price and security; the client may calculate the price based upon the security level chosen.

electronic authentication

The chip-based technology offers individualized security for every client and every product. Using our ASIC (application specific integrated circuit) and encrypted software, producers can ensure that a complex medical system will work only if all components are original, for instance. This form of authentication is particularly attractive because it can be easily implemented into existing systems. A single-wire interface to the host CPU is secured by an encrypted, public and private key similar to that used on current payment systems. The host software decides what happens if non-original components are used (warning, switch-off, report to the producer etc.).

all-in-label authentication

The all-in-label is a combination of a completely new hologram technology and a NFC chip, a consecutive serial number and the SARD taggant. 5 requirements are met at once: visual recognition, traceability, insertion of individual information, serial number and secure authentication.

swiss authentication
research and development AG

Swiss authentication research and development AG
Konstanzerstr. 17-19 • 8274 Tägerwilen • Switzerland
Phone +41 71 666 6161 • E-Mail info@swiss-authentication.ch
Internet www.swiss-authentication.ch

Mehrwert aus Ihren Patenten
Adding Value to IP

PATEV prüft, bewertet & gestaltet IP-Portfolien, recherchiert und analysiert Technologie- & IP-Daten und liefert die Basis für Handlungslinien von großen, mittelständischen Unternehmen.

PATEV audits, evaluates and strategizes patent portfolios, by transforming IP management data into valuable lines of action for the CEO / CFO of large and mid-sized enterprises.

PATEV ermöglicht effektive Management-Entscheidungen und stärkt den Beitrag des IP-Managements für den Geschäftserfolg. PATEV arbeitet mit der Patent-Abteilung, berichtet dem C-Level-Management und schafft Best Practice-Lösungen:

- IP-Portfolio und Technologie Benchmark, Monetäre Bewertung von Patentportfolien
- Wertorientiertes Patentmanagement
- IP Strategie Benchmark Best in Class
- IP Prozessqualität, Patent-Handbuch
- Patenteinfluss auf den Geschäftserfolg
- Ein- und Auslizenzierung, Open Innovation

PATEV ist europäischer Marktführer mit Vorhaben in Asien, USA/Kanada. Kunden von PATEV sind multinationale Konzerne und mittelgroße Technologie-Unternehmen. PATEV ist Gründungsmitglied von PATEV-ICM, dem globalen Netzwerk, für IP-Dienstleistungen von nationalen Partnern.

PATEV enables effective management decisions and strengthens the contribution of IP management. PATEV collaborates with the IP department, reports to the C-level management and provides Best Practice solutions:

- *IP Portfolio and Technology Benchmark, Portfolio Monetary Valuation*
- *Value Based IP Strategy, Upgrade IP Portfolio*
- *IP Strategy Benchmark Best in Class*
- *Process Quality in IP Management, IP Handbook*
- *Business Impact of Intellectual Property rights*
- *Licensing In / Out, Open Innovation*

PATEV is a European leader with projects in Asia, USA/Canada. PATEV's customers are multinational listed companies and medium-sized technology companies. PATEV is founding member of PATEV-ICM, the network for global IP professional services provided by national partners.

ADDING VALUE TO IP
PATEV

PATEV Associates GmbH • Albert-Einstein-Str. 62a • 76228 Karlsruhe • Germany
Phone +49 721 945406-0 • E-Mail info@patev.de
Internet www.patev.de

Produktschutz: verdeckt und maschinenlesbar!
Product protection: concealed and machine-readable!

Das System Tailor-Safe® bietet höchste Sicherheit gegen Plagiate und ungerechtfertigte Reklamationsansprüche. Durch die Maschinenlesbarkeit der verdeckten Kennzeichnung erfolgt gleichzeitig eine sichere Rückverfolgbarkeit der Produkte.

Einzigartige Markierung

Individualisierte, nicht imitierbare und dabei höchst belastbare Sicherheitspigmente werden wahlweise in das Produkt eingearbeitet oder aufgebracht. Die Markierung ist toxikologisch unbedenklich, chemisch inert und physikalisch stabil bis 1700°C.

Einfache Identifizierung

Mobile Handmessgeräte weisen jederzeit und überall in Sekundenbruchteilen nach, ob es ein Originalprodukt oder eine Fälschung ist. Die industrielle Anwendung mittels Inline-Sensoren erfolgt mit bis zu 10.000 Messungen pro Sekunde. Bereits äußerst geringe Mengen der Pigmente reichen für einen zuverlässigen Kopierschutz aus und sorgen so für einen kostengünstigen Produktschutz.

Tailor-Safe®:
einzigartig, maschinenlesbar und gerichtsfest!

The Tailor-Safe® system offers uncompromising security against plagiarism and fraudulent warranty claims. The concealed, but machine-readable markers also allow the full traceability of the marked products.

Unique Markers

Custom, forge-proof, and highly durable security pigments are added to or built into the product itself. The markers are toxicologically safe, chemically inert, and physically stable at up to 1700°C.

Simple Identification

Mobile scanners can be used to tell original from fake in the fraction of a second, anytime and anywhere. Applied on an industrial scale, inline sensors achieve up to 10,000 checks per second. Even tiny amounts of the pigments are enough to identify fakes for cost-efficient product protection.

Tailor-Safe®:
unique, machine-readable, forensic proof!

Tailorlux
intelligent materials

Tailorlux GmbH • Fraunhoferstr. 1 • 48161 Münster • Germany
Phone +49 2534 644-440 • E-Mail info@tailorlux.com
Internet www.tailorlux.com

Globale Produkt- und Markenschutzlösungen aus einer Hand
Global product and brand protection from one source

U-NICA ist auf die Entwicklung und Produktion von Sicherheitslösungen für den Produkt- und Markenschutz spezialisiert und zählt weltweit zu den führenden Anbietern. Wir bieten sichere und erprobte Prozesse für die Integration von Authentifizierungs-, Identifizierungs- und Verifizierungsmerkmalen.

U-NICA is specialized in the development and production of solutions for product and brand protection, and counts as a world leader in this field. U-NICA provides proven solutions in the integration of authentication, identification and verification features.

scryptoTRACE® – digitale END-TO-END Lösung
Sicherheitscodes werden unsichtbar in das bestehende Design der Produktverpackung integriert und können mit der scryptoTRACE Smartphone App ganz einfach geprüft werden. Verifikationsresultate mit zusätzlichen Daten (u. a. Geocodierung) werden in einer Datenbank gesammelt und dem Brand Owner unmittelbar in einem benutzerfreundlichen Webportal zur Verfügung gestellt. Das System bildet eine einfache und intelligente Markenschutzlösung für einen geschlossenen Benutzerkreis.

scryptoTRACE® – digital end-to-end solution
Invisible security codes are introduced onto product packaging, within existing design, by standard printing processes. The scryptoTRACE lets products be simply checked with a smartphone. Verification results, together with other critical data (such as Geocode) are gathered in a secure databank and are available to the brand owner via a web portal. The system is a simple and intelligent brand protection solution, appropriate for a closed user group.

spectroTAG® – Sicherheitsfarben und -taggants
Eine Sicherheitsmarkierung auf dem Produkt ist oft die einzige Möglichkeit um das Original eindeutig von der Fälschung zu unterscheiden. Die spectroTAG Produktreihe ermöglicht schnelle Authentifizierung mit einfach zu bedienenden, tragbaren Lesegeräten. spectroTAG Sicherheitsmarkierungen sind unsichtbarer und bleiben selbst unter einer UV Lichtquelle dem Fälscher verborgen.

spectroTAG® – security inks and taggants
Secure marking of the product itself is often the only certain way to distinguish a fake from an original product. The spectroTAG product range enables fast authentication with simple, portable readers. Markings are invisible, easily integrated into a range of substrates and remain invisible to the counterfeiter.

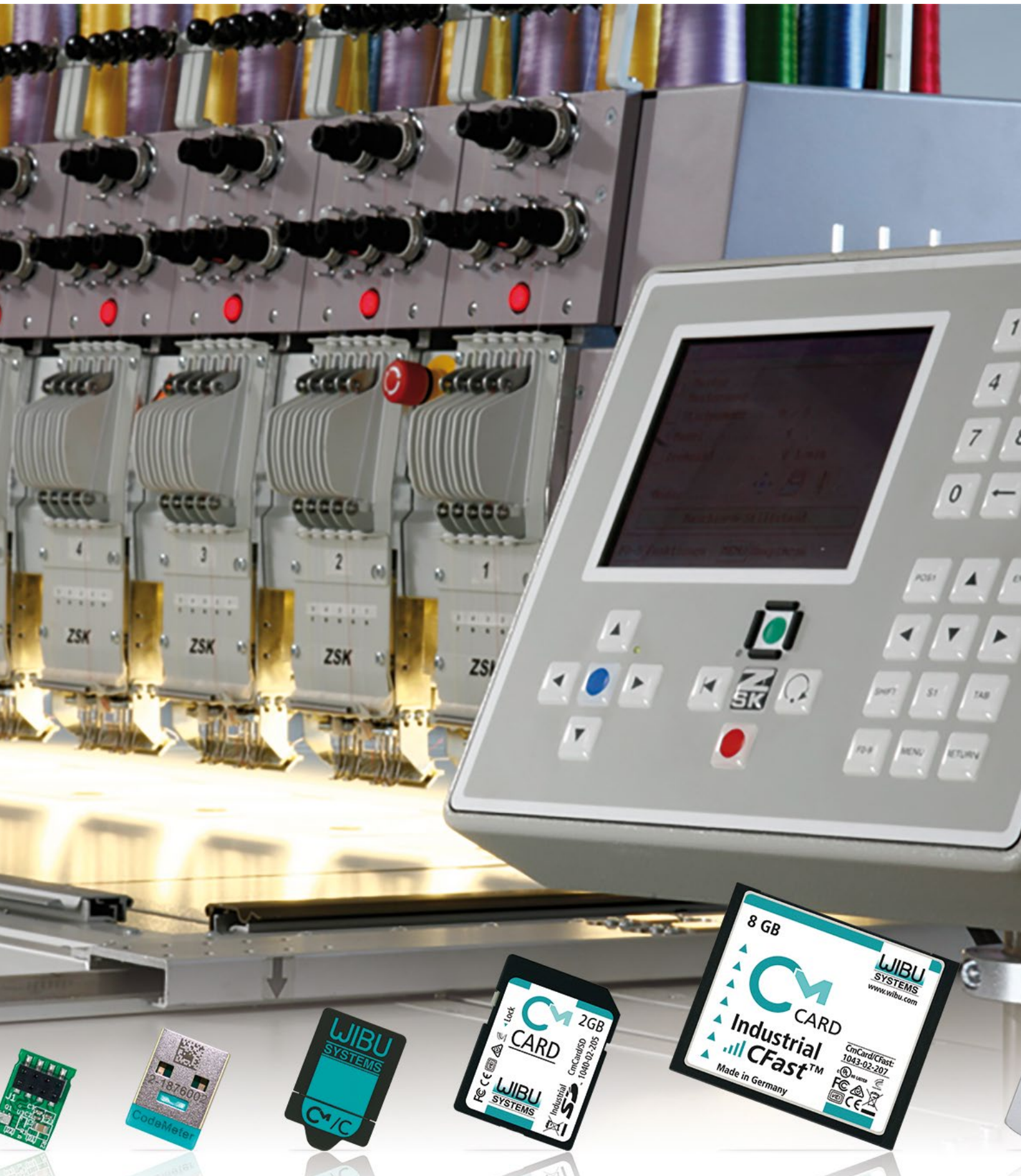
intraGRAM® – holografischer Schutz im Kunststoff
Holographische Sicherheitselemente sind als Identifikationsmerkmale im Produktschutz bekannt für den charakteristische Regenbogeneffekt der von Auge verifiziert werden kann. Das intraGRAM Sicherheitselement wird im Spritzgusswerkzeug integriert und auf das Kunststoffteil direkt und dauerhaft übertragen. Der holografische Effekt kann mit zusätzlichen Funktionen wie Mikrotexten, versteckten Symbolen sowie dynamischen Strukturen erweitert werden.

intraGRAM® – holographic protection in plastic
Holographic security elements are well known in product protection, as the characteristic rainbow effect is verified by the naked eye. The intraGRAM security feature is introduced – permanently – to plastic products during the injection molding process. The holographic effect can be further secured and enhanced with microtext, hidden symbols, or dynamic structures.

Quelle: U-NICA
Source: U-NICA

U-NICA Solutions AG • Industriestr. 4 • 7208 Malans • Switzerland
Phone +41 41 9 19 9900 • E-Mail solutions@u-nica.com
Internet www.u-nica.com

Endpoint-Security schützt industrielle Lösungen und Know-how
Endpoint Security to Safeguard Industrial Products and Know-How



CodeMeter kombiniert den sicheren Speicher von Schlüsseln und Lizenzen mit Schutz und Integration in Vertriebsprozesse.
CodeMeter combines secure key and license storage, protection and integration in sales processes.

SECURITY LICENSING PERFECTION IN PROTECTION

WIBU-SYSTEMS AG, 1989 von Oliver Winzenried und Marcellus Buchheit gegründet und eigentümergeführt, wurde 2014 mit dem Deutschen IT-Sicherheitspreis ausgezeichnet und zählt als innovativer Technologieführer zu Sicherheit für umfassende Softwarelizenzverwaltung.

Das Wibu-Systems-Motto „Perfection in Protection, Licensing and Security“ verdeutlicht das Bestreben, Sabotage, Spionage und Cyber-Attacken in intelligenten Fabriken wirkungsvoll zu bekämpfen.

Mit dem Flagschiffprodukt CodeMeter®, der sicheren Komplettlösung, schützt Wibu-Systems geistiges Eigentum und Produkt-Know-how, das in Maschinen und PCs, in industriellen PC, Embedded-Systemen, mobilen Geräten, Tablets, speicherprogrammierbare Steuerungen (SPSen) und Mikrocontrollern steckt, vor Softwarepiraterie, Produktpiraterie, Reverse-Engineering und Manipulationen. Industrietaugliche Hardware oder softwarebasierte Lösungen vereinen sicheres Booten und zertifikatsbasierte Vertrauensanker und zeichnen diese robusten und innovativen Technologien aus. Sie unterstützen die Hersteller intelligenter Geräte, ihre in Software realisierten Funktionen und Anwendungen sicher zu verteilen, selbst in der Cloud und in virtuellen Umgebungen. Zusätzlich erlaubt CodeMeter flexible Lizenzierung, sodass Softwareanbieter und Hersteller neue Geschäftsmodelle aufbauen, die Logistik vereinfachen und den Umsatz steigern können.

Mit Sitz in Karlsruhe unterhält Wibu-Systems Niederlassungen in den USA und China, Verkaufsbüros in Europa sowie ein engmaschiges, weltweites Netzwerk an Distributoren.

Die verschiedenen Bauformen des CmDongles wurden speziell für industrielle Anforderungen entwickelt.
A range of CmDongle form factors designed specifically for industrial applications.

Wibu-Systems, a privately held company founded by Oliver Winzenried and Marcellus Buchheit in 1989, who was conferred the German IT Security Award in 2014, is an innovative security technology leader in the global software license lifecycle management.

Through its motto “Perfection in Protection, Licensing and Security”, Wibu-Systems reinforces its dedication to eradicate sabotage, espionage and cyber-attacks in smart factories. With its flagship CodeMeter® all-in-one security platform, Wibu-Systems safeguards digital assets and product know-how that are available in machines and on personal computers, industrial PCs, embedded systems, mobile devices, tablets, programmable logic controllers and microcontrollers from software counterfeiting, product piracy, reverse-engineering and machine code tampering.

Industrial grade hardware secure elements or software-based solutions associated with secure boot and certificate-based anchor of trust are the characteristic traits of this robust and cutting edge technology that helps intelligent device manufacturers safely distribute their applications even in cloud and virtualized models.

Additionally, CodeMeter provides flexible license management to support software vendors and manufacturers in generating alternative business models, simplifying logistics and increasing profit revenues.

Headquartered in Karlsruhe, Germany, Wibu-Systems holds subsidiaries in the USA and China, sales offices throughout Europe, and a capillary world distribution network.

WIBU SYSTEMS

WIBU-SYSTEMS AG • Rüppurrer Str. 52-54 • 76137 Karlsruhe • Germany
Phone +49 721 93172-0 • E-Mail info@wibu.com
Internet www.wibu.com

Informationssicherheit, Industrial Security, Produktpiraterie und Know-how-Schutz - Aktuelle Aktivitäten im Überblick

Information security, industrial security, product piracy and know-how protection: summary of current activities

Die **VDMA Arbeitsgemeinschaft Produkt- und Know-how-Schutz (AG Protect-ing)** bündelt die Aktivitäten der Anbieter von Technologien und Dienstleistungen zu Produkt- und Know-how-Schutz. Schutzmaßnahmen rund um Produktpiraterie, Wirtschaftsspionage, Security in Produkten und Prozessen sowie Technologie-Diebstahl stehen dabei im Fokus.

Zu organisatorischen Maßnahmen rund um Security unterstützt die **Abteilung Informatik** die Mitglieder des VDMA und ist erster Ansprechpartner für Mitglieder, Behörden und Politik.

*The **VDMA Working Group on Product and Know-how Protection (AG Protect-ing)** pools the activities by providers of technologies and services for product and know-how protection. Here the focus is on protective measures covering product piracy, industrial espionage, security in products and processes together with technology theft.*

*The **Informatics Department** supports the VDMA members with organisational measures covering all aspects of security and acts as the initial contact for members, authorities and the political sector.*

www.protect-ing.de

pks.vdma.org

VDMA Arbeitskreis „Industrial Security“

Aufgaben:	Erarbeitet Leitlinien und Praxishilfen für die Industrial Security
Teilnehmer:	Maschinen- und Anlagenbauer, Betreiber, Automatisierer, Dienstleister, Security-Spezialisten, Bundesamt für Sicherheit in der IT (BSI)
Vorsitzender:	Wolfgang Bokämper, Kolbus GmbH & Co. KG

VDMA Arbeitskreis „Informationssicherheit“

Aufgaben:	Erarbeitet Leitlinien und Praxishilfen der IT- und Informationssicherheit.
Teilnehmer:	CISOs und IT-Sicherheitsbeauftragte der Maschinen- und Anlagenbauer
Vorsitzender:	Rolf Strehle, Voith GmbH

VDMA Arbeitskreis „Track & Trace“

Aufgaben:	Erarbeitet Praxishilfe für den Einsatz von T&T-Technologien
Teilnehmer:	Maschinen- und Anlagenbauer, Automotive-Zulieferer, Anbieter aus Intralogistik, Produktschutz, Fälschungsschutz
Vorsitzender:	Horst Lang, Festo AG & Co. KG, Esslingen

VDMA Task Force on Industrial Security

Tasks:	*Produces guidelines and practical aids for industrial security*
Participants:	*Machine and plant manufacturers, operators, automation specialists, service providers, security specialists, Federal Office for Information Security (BSI)*
Chair:	*Wolfgang Bokämper, Kolbus GmbH & Co. KG*

VDMA Task Force on Information Security

Tasks:	*Produces guidelines and practical aids for IT and information security.*
Participants:	*CISOs and IT security officers of machine and plant manufacturers*
Chair:	*Rolf Strehle, Voith GmbH*

VDMA Task Force on Track & Trace

Tasks:	*Produces practical aids for using T&T technologies*
Participants:	*Machine and plant manufacturers, automotive suppliers, providers of intralogistics, product protection, counterfeiting protection*
Chair:	*Horst Lang, Festo AG & Co. KG, Esslingen*

Positionen des VDMA
VDMA briefs

Industrie 4.0: Wandel gestalten, Potenziale nutzen
Industry 4.0: Shaping change, using potential

VDMA 2014

Die Digitalisierung durch das Internet verändert die Lebens- und Arbeitswelt nachhaltig. Auch die Produktion wird digitalisiert – genannt Industrie 4.0.

Diese Entwicklung bietet dem deutschen Maschinen- und Anlagenbau alle Chancen, seine führende Position auszubauen. Ob die Industrienation Deutschland Industrie 4.0 zum Geschäftsmodell machen kann, hängt nicht nur von den Unternehmen ab.

Wichtige Rahmenbedingungen müssen mit Politik und Gesellschaft vereinbart werden.

Digitisation through the internet is having a sustainable effect in changing the living and working world. Production is also being digitised; this is known as Industry 4.0.

It is a development that offers the German engineering sector every chance to expand its leading position. Whether Germany as an industrial country can adopt Industry 4.0 as its business model depends not just on the companies.

Important framework conditions have to be agreed with the political sector and society at large.

Potenzial von Industrie 4.0 für Europa nutzen
Using the potential of Industry 4.0 for Europe

VDMA 2015

Sprache
Deutsch/Englisch

Der Maschinen- und Anlagenbau entwickelt neue Lösungen für die Industrie 4.0.

Damit kann der Industriestandort Europa wachsen. Die Politik muss sich dafür aber stärker auf die industriepolitischen Aspekte der Digitalisierung konzentrieren. Nur wenn die Unternehmen auf dem europäischen Markt gute Rahmenbedingungen finden, können sie den Weg zu Industrie 4.0 gehen und neben Wohlstand und Beschäftigung auch die europäische Idee voran bringen.

Language
German/English

The engineering sector is developing new solutions for Industry 4.0.

The aim is to let Europe grow as a place for industry. But the political sector must concentrate more on industrial policy aspects of digitisation. The companies on the European market need to be offered good framework conditions for them to take up Industry 4.0, thus boosting the European idea as well as enhancing prosperity and employment.

Industrial Security: Sichere Maschinen und Anlagen
Industrial Security: Secury Machinery

VDMA 2015

Sprache
Deutsch/Englisch

Steht die Produktion, geht bares Geld verloren. Fallen kritische IT-Infrastrukturen wie in Krankhäusern oder bei Energieversorgern aus, stehen Menschenleben auf dem Spiel.

Informationstechnik in Produktionssystemen sowie Maschinen und Anlagen vor Sabotage, Spionage oder Manipulation zu schützen, ist Aufgabe der „Industrial Security".

Language
German/English

Money is lost when production stands still. And when critical IT infrastructures fail in hospitals or power utilities, lives can be at stake.

Protecting information technology in production systems and machinery from sabotage, espionage or manipulation is the task of industrial security.

Produktpiraterie vorbeugen und ahnden
Preventing and punishing product piracy

VDMA 2015

Sprache
Deutsch/Englisch

Innovationskraft und Wettbewerbsfähigkeit des deutschen Maschinen- und Anlagenbaus werden durch Plagiate enorm bedroht.

Investitionen in Forschung und Entwicklung lohnen sich nur dann für Unternehmen, wenn Produktpiraterie verhindert wird. Die Bundes-regierung und die Europäische Union müssen die Unternehmen stärker als bisher im Kampf gegen Plagiate unterstützen.

Language
German/English

Counterfeit products present a huge threat to the innovation powers and competitiveness of the German engineering sector.

Investment in research and development will only be worthwhile for companies if product piracy can be prevented. The Federal Government and the European Union must give companies far greater support than hitherto in their fight against counterfeit products.IFRS für die Investitionsgüter-Industrie

IT-Sicherheit
IT Security

Leitfaden zur Informationssicherheit Teil 1: Sensibilisierung
VDMA Guideline „Information Security, Part 1: Staff Awareness"

VDMA 2009

Preis
44,00 €

VDMA-Mitglieder
22,00 €

Link
http://www.vdmashop.de/advanced_search_result.php?keywords=informationssicherheit

Price
44,00 €

VDMA members
22,00 €

Link
http://www.vdmashop.de/advanced_search_result.php?keywords=informationssicherheit

Leitfaden zur Informationssicherheit Teil 2: Informationssicherheits-Management-System (ISMS)
VDMA Guideline „Information Security, Part 2: ISMS, Documents and Templates

VDMA 2013

Preis
50,00 €

VDMA-Mitglieder
kostenfrei

Link
http://www.vdmashop.de/advanced_search_result.php?keywords=informationssicherheit

Price
50,00 €

VDMA members
free of charge

Link
http://www.vdmashop.de/advanced_search_result.php?keywords=informationssicherheit

---

Leitfaden zur Informationssicherheit Teil 3: Datenaustausch
VDMA Guideline „Information Security Part 3: Data Exchange

VDMA 2016‘
(angekündigt)

Preis
50,00 €

VDMA-Mitglieder
kostenfrei

Link
http://www.vdmashop.de/advanced_search_result.php?keywords=informationssicherheit

VDMA 2016
(announced)

Price
50,00 €

VDMA members
free of charge

Link
http://www.vdmashop.de/advanced_search_result.php?keywords=informationssicherheit

VDMA Stellungnahme BYOD
VDMA Statement BYOD

VDMA 2012

Nur für VDMA-Mitglieder!
kostenfrei

Eine Stellungnahme des AK Informationssicherheit zu Bring Your Own Device.

Auf Anforderung per E-Mail bei **biljana.gabric@vdma.org** erhältlich.

VDMA members only!
free of charge

Statement by the Task Force on Information Security on „bringing your own device“.

*Available on request by e-mail from **biljana.gabric@vdma.org**.*

Industrial Security
Industrial Security

Industrial Security – die unangreifbare Maschine
Industrial Security – the Unassailable Machine

VDMA 2014

Sprache
Deutsch

Preis
kostenfrei

Aktuelle Beiträge von VDMA-Mitgliedern sowie Behörden zur Industrial Security, u.a. Fernwartung, Anlagen-Security, Security by Design, Apps im Maschinenbau, kostenfreie Tools.

Auf Anforderung per E-Mail bei **biljana.gabric@vdma.org** erhältlich.

Language
German

Price
free of charge

Current contributions from VDMA members and authorities on industrial security, including remote maintenance, plant security, security by design, apps in engineering, free tools.

*Available on request by e-mail from **biljana.gabric@vdma.org**.*

Fragenkatalog Industrial Security – Einfach anfangen.
Questionnaire on Industrial Security – Easy Start

VDMA 2014

Sprache
Deutsch

Preis
kostenfrei

Einstiegshilfe in die Auswahl und Bewertung von Security- Maßnahmen für Produktionsumgebungen.

Ersteinschätzung mit Hilfe von 33 Fragen.

Link
http://pks.vdma.org/article/-/articleview/6262936

Language
German

Price
free of charge

Starters‘ aid for selecting and assessing security measures for production environments.

Initial appraisal based on 33 questions.

Link
http://pks.vdma.org/article/-/articleview/6262936

INS-Studie „Security in Automation“
INS Study „Security in Automation“

DIN/NAM/VDMA 2014

Preis
kostenfrei

Vergleich und Bewertung von nationalen und internationalen Normen und Standards für Automations- und Produktionssicherheit.

Link
http://pks.vdma.org/article/-/articleview/6264245

Price
free of charge

Comparison and assessment of national and international standards and specifications for automation and production security.

Link
http://pks.vdma.org/article/-/articleview/6264245

Studie „Status Quo der Security in Produktion und Automation“
Study „Status Quo of Security in Production and Automation“

VDMA 2013

Preis
kostenfrei

Einschätzung von VDMA-Mitgliedern zur industriellen Security, mit praxisnahen Handlungsempfehlungen.

Link
http://pks.vdma.org/article/-/articleview/2717338

Price
free of charge

Appraisal by VDMA members of industrial security, with practical recommendations.

Link
http://pks.vdma.org/article/-/articleview/2717338

Produktpiraterie
Product piracy

Studie „Produktpiraterie 2014“
Study „Product Piracy 2014“

VDMA 2014

Sprache
Deutsch/Englisch

Preis
kostenfrei

Einschätzung von VDMA-Mitgliedern zu Produktpiraterie. Aktuelle Statistiken und Rückblick auf die Entwicklung seit 2003.

Link
http://pks.vdma.org/article/-/articleview/3616439

Language
German/English

Price
free of charge

Appraisal by VDMA members of product piracy. Current statistics and review of developments since 2003.

Link
http://pks.vdma.org/article/-/articleview/3616439

Studie „Produktpiraterie 2016“
Study „Product Piracy 2016“

VDMA 2016
(angekündigt)

Sprache
Deutsch/Englisch

Preis
kostenfrei

Einschätzung von VDMA-Mitgliedern zu Produktpiraterie. Aktuelle Statistiken und Rückblick auf die Entwicklung seit 2003.

Link
http://pks.vdma.org

VDMA 2016
(announced)

Language
German/English

Price
free of charge

Appraisal of product piracy by VDMA members. Current statistics and review of developments since 2003.

Link
http://pks.vdma.org

Branchenführer „Produkt- und Know-how-Schutz“
Branch Guide „Product and Know-how Protection“

VDMA 2016

Sprache
Deutsch/Englisch

Preis
kostenfrei

Übersicht und Matrix der Technologiebereiche und Mitglieder in der VDMA Arbeitsgemeinschaft „Produkt- und Know-how-Schutz“.

Link
http://pks.vdma.org/article/-/articleview/3703079

Language
German/English

Price
free of charge

Overview and matrix of the technology areas and members in the VDMA working group Product and Know-how Protection.

Link
http://pks.vdma.org/article/-/articleview/3703079

Leitfaden „Produkt- und Know-how-Schutz“
Guideline „Product and Know-how Protection“

VDMA 2013

Sprache
Deutsch/Englisch

Preis
kostenfrei

Anleitung zum erfolgreichen Einsatz von Schutzmaßnahmen inkl. praxisnaher Beispiele.

Link
http://pks.vdma.org/article/-/articleview/1351236

Language
German/English

Price
free of charge

Instructions for successful use of protection measures including practical examples.

Link
http://pks.vdma.org/article/-/articleview/1351236

INS-Studie „Schutzkonzepte gegen Produktpiraterie“
INS Study „Protection Concepts Against Product Piracy“

DIN/NAM/VDMA 2012

Preis
kostenfrei

Vergleich und Kombination verschiedener publizierter Schutzkonzepte zu Produktpiraterie, Erstellung einer strukturierten Vorgehensweise.

Link
http://pks.vdma.org/article/-/articleview/582627

Price
free of charge

Comparison and combination of various published protection concepts on product piracy, taking a structured approach.

Link
http://pks.vdma.org/article/-/articleview/582627

Know-how-Schutz
Know-how protection

Branchenführer „Produkt- und Know-how-Schutz“
Branch Guide „Product and Know-how Protection“

VDMA 2016

Sprache
Deutsch/Englisch

Preis
kostenfrei

Übersicht und Matrix der Technologiebereiche und Mitglieder in der VDMA Arbeitsgemeinschaft „Produkt- und Know-how-Schutz“.

Link
http://pks.vdma.org/article/-/articleview/3703079

Language
German/English

Price
free of charge

Overview and matrix of the technology areas and members in the VDMA working group Product and Know-how Protection.

Link
http://pks.vdma.org/article/-/articleview/3703079

Leitfaden „Produkt- und Know-how-Schutz“
Guideline „Product and Know-how Protection“

VDMA 2013

Sprache
Deutsch/Englisch

Preis
kostenfrei

Anleitung zum erfolgreichen Einsatz von Schutzmaßnahmen inkl. praxisnaher Beispiele.

Link
http://pks.vdma.org/article/-/articleview/1351236

Language
German/English

Price
free of charge

Instructions for successful use of protection measures including practical examples.

Link
http://pks.vdma.org/article/-/articleview/1351236

INS-Studie „Status Quo des Know-how-Schutzes im Maschinen- und Anlagenbau“
INS Study „Status Quo of Know-how Protection in the Engineering Sector“

DIN/NAM/VDMA 2013

Preis
kostenfrei

Übersicht der Know-how-Schutz-Aktivitäten von VDMA-Mitgliedern.

Link
http://pks.vdma.org/article/-/article-view/1351004

Price
free of charge

Overview of know-how protection activities by VDMA members.

Link
http://pks.vdma.org/article/-/articleview/1351004

INS-Studie „Kennzeichnung und Identifizierung von Maschinenbauprodukten“
INS Study „Marking and Identifying Engineering Products“

DIN/NAM/VDMA 2011

Preis
kostenfrei

Auflistung und Klassifizierung von Kennzeichnungs- und Identifizierungstechnologien in Bezug auf Condition Monitoring, Logistik und Produktpiraterie.

Link
http://pks.vdma.org/article/-/articleview/6138567

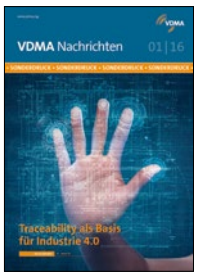
Price
free of charge

List and classification of marking and identification technologies with regard to condition monitoring, logistics and product piracy.

Link
http://pks.vdma.org/article/-/articleview/6138567

Track & Trace
Track & Trace

Traceability als Basis für Industrie 4.0
Traceability as Basis for Industry 4.0



VDMA 2016

Sprache
Deutsch

Preis
kostenfrei

Aktuelle Beiträge von VDMA-Mitgliedern sowie Forschungsinstituten zur Traceability, u.a. Traceability-Modell, Direkt-markierung, Fälschungsschutz, Identitäten und Technologien.

Auf Anforderung per E-Mail bei **biljana.gabric@vdma.org** erhältlich.

Language
German

Price
free of charge

Current contributions from VDMA members and research institutes on traceability, including traceability model, direct marking, counterfeiting protection, identities and technologies.

*Available on request by e-mail from **biljana.gabric@vdma.org**.*

Ihre Ansprechpartner im VDMA
Your Contact at VDMA

Steffen Zimmermann
Referent Informationssicherheit &
Industrial Security
Geschäftsführer AG Protect-ing

Telefon: +49 69 6603-1978
Mobil: +49 170 3385440
E-Mail: steffen.zimmermann@vdma.org

Steffen Zimmermann
Spokesman Information Security &
Industrial Security Managing
Managing Director WG Protect-ing

Phone: +49 69 6603-1978
Mobil: +49 170 3385440
E-Mail: steffen.zimmermann@vdma.org

Biljana Gabric
Assistentin der Geschäftsführung

Telefon +49 69 6603-1360
E-Mail: biljana.gabric@vdma.org

Biljana Gabric
Assistant to the Management

Phone +49 69 6603-1360
E-Mail: biljana.gabric@vdma.org

Aktuelle Termine 2016/17
Save the dates 2016/17

07.06.2016
VDMA Anwendertag „Produktpiraterie“
VDMA, Frankfurt

08.12.2016
VDMA Infotag „Informationssicherheit
und Know-how- Schutz“
VDMA, Frankfurt

14.02.2017
VDMA Infotag „Industrial Security“
VDMA, Frankfurt

Sie möchten informiert werden?
Schreiben Sie uns eine E-Mail, wenn Sie über
aktuelle Themen und Termine informiert werden möchten.

07/06/2016
VDMA User Day „Product Piracy“
VDMA, Frankfurt

08/12/2016
VDMA Information Day „Information Security
and Know-how Protection“
VDMA, Frankfurt

14/02/2017
VDMA Information Day “Industrial Security”
VDMA, Frankfurt

Would you like to be kept informed?
Send us an e-mail if you would like to be informed about
current topics and events.

Mitglieder der Arbeitsgemeinschaft Produkt- und Know-how-Schutz
Working group members Product and Know-how Protection

3S Simons Security Systems GmbH
Lise-Meitner-Str. 6
48301 Nottuln
Germany
Phone: +49 2502 2333-0
info@secutag.com
www.secutag.com

@-yet GmbH
Schloß Eicherhof
42799 Leichlingen
Germany
Phone: +49 2175 1655-0
info@add-yet.de
http://www.add-yet.de

B

Balluff GmbH
Schurwaldstr. 9
73765 Neuhausen
Germany
Phone: +49 7158 173-315
info@balluff.de
www.balluff.de

Borries Markier-Systeme GmbH
Siemensstr. 3
72124 Pliezhausen
Germany
Phone: +49 7127 9797-0
info@borries.com
www.borries.com

Brainloop AG
Franziskanerstr. 14
81669 München
Germany
Phone: +49 2304 759-0
info@brainloop.com
www.brainloop.com

D

Diagramm Halbach GmbH & Co. KG
Am Winkelstück 14
58239 Schwerte
Germany
Phone: +49 2304 759-0
info@halbach.com
www.halbach.com
www.sicherheitsdruck.de

F

Fraunhofer IPT Projektgruppe Entwurfstechnik Mechatronik
Zukunftsmeile 1
33102 Paderborn
Germany
Phone: +49 5251 5465-101
info@ipt.fraunhofer.de
www.ipt.fraunhofer.de

Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC
Parkring 4
85748 Garching
Germany
Phone: +49 89 3229986-292
info@aisec.fraunhofer.de
www.aisec.fraunhofer.de

G

GS1 Germany GmbH
Maarweg 133
50825 Köln
Germany
Phone: +49 221 94714-442
duennebacke@gs1- germany.de
www.gs1-germany.de

H

Hans Turck GmbH & Co. KG
Witzlebenstr. 7
45472 Mülheim an der Ruhr
Germany
Phone: +49 208 4952-0
more@turck.com
www.turck.com

HiSolutions AG
Bouchéstr. 12
12435 Berlin
Germany
Phone: +49 30 533289-0
info@hisolutions.com
www.hisolutions.com

Hoffmann Engineering GmbH
Lessingstr. 29c
76344 Eggenstein-Leopoldshafen
Germany
Phone: +49 721 9614129-0
info@hoffmann-en.com
www.hoffmann-en.com

Hologram Company Rako GmbH
Möllner Landstr. 15
22969 Witzhave
Germany
Phone: +49 4104 693-250
info@hologram-company.com
hologram-company.com

I

Innovation IP
Wilhelm-Hertz-Str. 8
80805 München
Germany
mp@innovation-ip.de
www.innovation-ip.de

INNOVENT e.V. Technologieentwicklung Jena
Prüssingstr. 27 B
07745 Jena
Germany
Phone: +49 3641 2825-10
innovent@innovent-jena.de
www.innovent-jena.de

L

LEONHARD KURZ Stiftung & Co. KG
Schwabacher Str. 482
90763 Fürth
Germany
Phone: +49 911 7141-834
sales@kurz.de
www.kurz.de

O

OCS Checkweighers GmbH
Adam-Hoffmann-Str. 26
67657 Kaiserslautern
Germany
Phone +49 631 34146-0
info.ww@ocs-cw.com
www.ocs-cw.com

OpSec Security GmbH
Inselkammerstr. 1
82008 Unterhaching
Germany
Phone: +49 89 790783-00
info@opsecsecurity.com
www.opsecsecurity.com

P

PATEV Associates GmbH
Albert-Einstein-Str. 62a
76228 Karlsruhe
Germany
Phone: +49 721 945406-0
info@patev.de
www.patev.de

PROSTEP AG
Dolivostr. 11
64293 Darmstadt
Germany
Phone: +49 6151 9287-0
info@prostep.com
www.prostep.com

S

Schreiner Group GmbH & Co. KG
Bruckmannring 22
85764 Oberschleißheim
Germany
Phone: +49 89 31584-5634
info@schreiner-group.com
www.schreiner- group.com

Securikett Ulrich & Horn GmbH
Straße 10, Objekt 48
2355 Wiener Neudorf
Austria
Phone: +43 2236 677925
office@securikett.com
www.securikett.com

SEEBURGER AG
Edisonstr. 1
75015 Bretten
Germany
Phone: +49 7252 96-0
info@seeburger.de
www.seeburger.de

Sensor Instruments Entwicklungs- und Vertriebs GmbH
Schlinding 11
94169 Thurmansbang
Germany
Phone: +49 8544 9719-0
info@sensorinstruments.de
www.sensorinstruments.de

SICK AG
Erwin-Sick-Str. 1
79183 Waldkirch
Germany
Phone: +49 7681 202-0
info@sick.de
www.sick.de

Siemens AG Corporate Technology
Otto-Hahn-Ring 6
81739 München
Germany
Phone: +49 89 636-0
info@siemens.com
www.siemens.com

Steinbeis University Berlin Institute "Global Consulting and Government"
Landsbergser Allee 18
10249 Berlin
Germany
Phone: +49 30 293309-0
shb@stw.de
www.steinbeis- network.de

swiss authentication research and development AG
Konstanzerstr. 17
8274 Tägerwilen
Switzerland
Phone: +41 71 6666161
info@swiss-authentication.ch
www.swiss- authentication.ch

T

Tailorlux GmbH
Fraunhoferstr. 1
48161 Münster
Germany
Phone: +49 2534 64444-0
info@tailorlux.com
www.tailorlux.com

tesa scribos GmbH
Sickingenstr. 65
69126 Heidelberg
Germany
Phone: +49 6221 33507-10
info@tesa-scribos.com
www.tesa-scribos.de

Trend Micro Deutschland GmbH
Zeppelinstraße 1
85399 Hallbergmoos
Germany
Phone: +49 811 88990-700
sales_info@trendmicro.de
www.trendmicro.de

TRUMPF Laser Marking Systems AG
Tumpfstr. 8
7214 Grüsch
Switzerland
Phone: +41 81 3076-161
info@ch.trumpf.com
www.trumpf.com/de/produkte/lasertechnik.html

U

U-NICA Solutions AG
Industriestr. 4
7208 Malans
Switzerland
Phone: +41 419199900
solutions@u-nica.com
www.u-nica.com

UNITY AG
Lindberghring 1
33142 Büren
Germany
Phone: +49 2955743-0
matthias.schwarzenberg@unity.de
www.unity.de

V

VICCON GmbH
Ottostr. 1
76275 Ettlingen
Germany
Phone: +49 7243 719734
info@viccon.de
www.viccon.de

W

WIBU-SYSTEMS AG
Rüppurrer Str. 52 – 54
76137 Karlsruhe
Germany
Phone: +49 721 93172-0
info@wibu.com
www.wibu.com

Impressum *Imprint*

Herausgeber / *Editor*
Arbeitsgemeinschaft Produkt- und Know-how-Schutz im Verband Deutscher Maschinen- und Anlagenbau e.V. (VDMA)
Lyoner Str. 18
60528 Frankfurt am Main
P.O. Box 71 08 64
Germany
Phone +49 69 6603-1360
Fax +49 69 6603-2360
E-Mail protect-ing@vdma.org
Internet www.protect-ing.de

Verlag / *Publisher*
VDMA Verlag GmbH
Lyoner Str. 18
60528 Frankfurt am Main
P.O. Box 71 08 64
Germany
Phone +49 69 6603-1580
Fax +49 69 6603-2580
E-Mail verlag@vdma.org
Internet www.vdma-verlag.com

Druck / *Printing*
h. reuffurth gmbh, Mülheim am Main

Layout und Design / *Layout & Design*
VDMA Verlag GmbH
Frankfurt am Main, Germany

Product and Know-how Protection
A working group within VDMA

Lyoner Str. 18
60528 Frankfurt am Main
Germany

Phone +49 69 6603-1978
Fax +49 69 6603-2978
E-Mail protect-ing@vdma.org
Internet pks.vdma.org

pks.vdma.org

vf920816