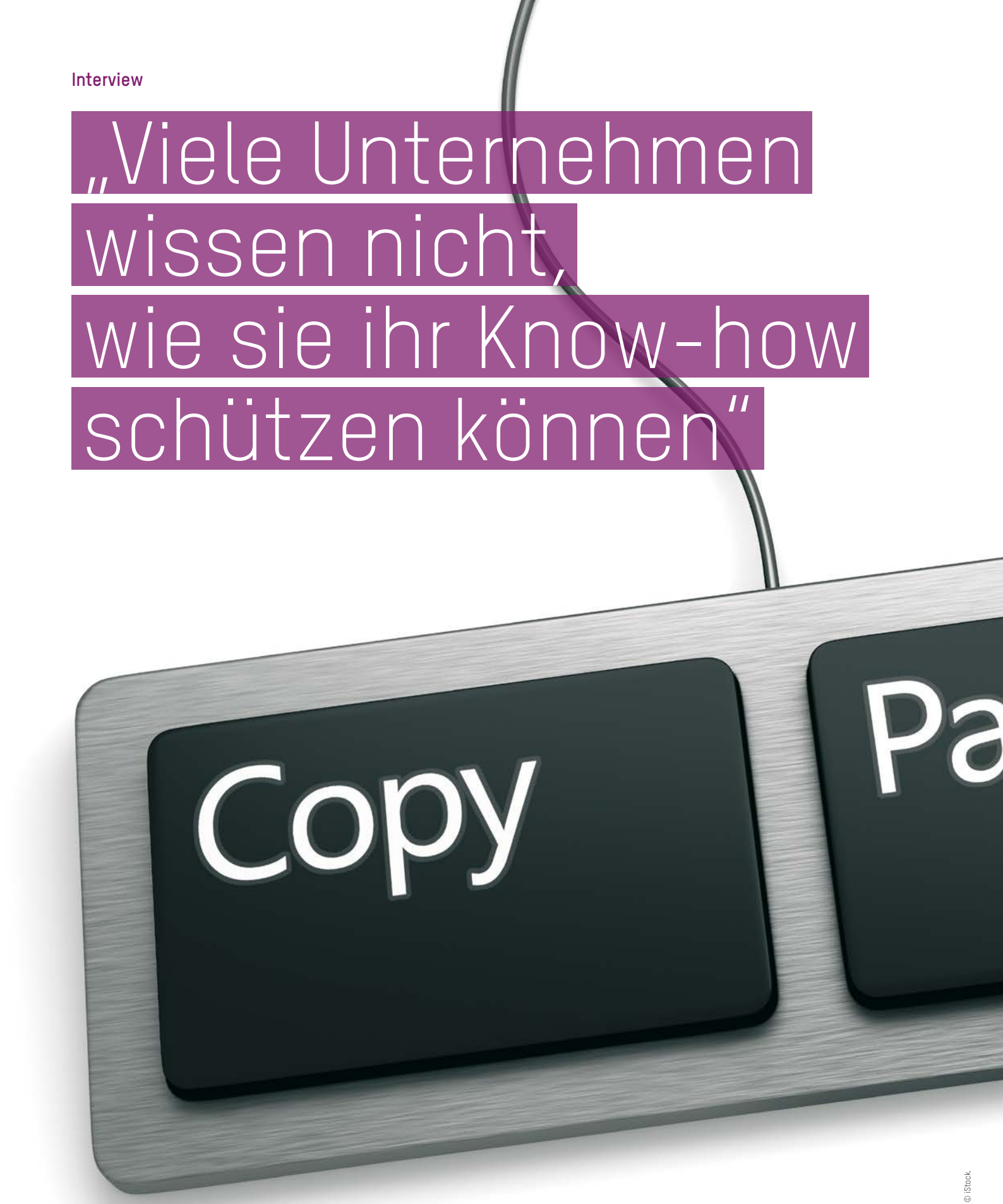
# „Viele Unternehmen wissen nicht, wie sie ihr Know-how schützen können“




Bildquelle © iStock.

Jedes Jahr entsteht der Industrie ein Schaden in Milliardenhöhe, weil Produkte im In- und Ausland illegal hergestellt werden. Maschinen- und Anlagenbauer wie auch die Betreiber von Produtionsanlagen sollten darauf achten, ihr geistiges Eigentum und ihre Produkte zu schützen. Wie so ein Schutz aussehen könnte, erklärt Oliver Winzenried von der Arbeitsgemeinschaft Produkt- und Know-how-Schutz im VDMA.


***Welcher Schaden entsteht Maschinen- und Anlagenbauern durch Produktpiraterie und Know-how-Klau?***
Den Mitgliedern im VDMA entsteht jährlich ein geschätzter Schaden von 7,9 Milliarden Euro, was 4 Prozent des Umsatzes entspricht. So lautet das aktuelle Ergebnis einer Umfrage, die der VDMA alle 2 Jahre zum Thema Produktpiraterie durchführt. Betroffen sind 9 von 10 Unternehmen mit mehr als 1.000 Mitarbeitern. Über 50 Prozent der Unternehmen berichten, dass komplette Maschinen oder Produkte nachgebaut wurden.

***Sind sich die Unternehmen des Bedrohungspotenzials bewusst?***
Durchaus. Andere werden sich dessen bewusst, wenn sie Plagiate sehen oder wenn sie Gewährleistung für ein gefälschtes Produkt geben sollen. Erst beim genaueren Hinsehen kommt auf, dass es kein eigenes Produkt ist, sondern ein Plagiat.

***Gibt es Branchen, die besonders betroffen sind?***
Ja, die gibt es. Am stärksten betroffen sind Holzbearbeitungsmaschinen, Textilmaschinen und die Landtechnik.

***Woher kommen die Plagiate typischerweise?***
Nummer eins beim Nachbau und bei Plagiaten von Maschinen und Produkten ist China. Der Anteil ist mit 72 Prozent immer noch

„Anlagenbauer und -betreiber sollten ihr Know-how und ihre Produkte schützen", sagt Oliver Winzenried, Vorsitzendes des Vorstands der Arbeitsgemeinschaft Produkt- und Know-how-Schutz.

hoch, er ist jedoch im Vergleich zur Vorgängerumfrage leicht gesunken. An 2. Stelle kommt, für viele überraschend, Deutschland.

***Wie gehen die Piraten in der Regel vor?***
Die häufigste Methode ist mit 72 Prozent Reverse-Engineering. Maschinen und Produkte werden auseinander genommen und analysiert. Die mechanischen Teile werden nachgebaut, die Software wird dekompiliert. Anschließend geht es darum, die Verfahren in der Maschine zu verstehen. Dann können sie in die eigenen Maschinen integriert werden, ohne große Aufwände in die Entwicklung investieren oder jahrelange Erfahrung in der Praxis sammeln zu müssen. Genau genommen handelt es sich noch nicht einmal um Plagiat, weil die Verfahren verstanden und selbst angewandt werden. Allerdings können vorhandene Patente verletzt werden.

***Woran scheitert die Integration von Schutzmaßnahmen?***
Viele Unternehmen wissen gar nicht, welche technischen Maßnahmen es überhaupt gibt und welche zu ihren Maschinen und Produkten passen.

***Lassen sich gängige Schutzmechanismen, die in der IT bewährt sind, übertragen?***
Schutzmaßnahmen, die aus der Büro-IT bekannt sind, lassen sich nur zum Teil auf den Maschinenbau übertragen. Läuft zum Beispiel eine Maschine in der Prozessindustrie, kann der Anwender nicht zwischendurch rebooten oder einen Virenscan laufen lassen, der minutenlang das System ausbremst. Hier unterscheiden sich die Anforderungen sehr.

***Welche Maßnahmen können Maschinen- und Anlagenbauer oder auch Anlagenbetreiber ergreifen?***
Ein Maschinenbauer, der Komponenten in seine Maschine integriert, kann die Security nicht selbst entwickeln und dann um die einzelne Komponente herumstülpen. Vielmehr müssen die Komponentenhersteller dies vorbereitet haben. Die Herausforderung für den Maschinenbauer und den Betreiber einer Anlage ist immer noch groß genug, dann ein sicheres Gesamtsystem zu schaffen, das alle Security-Funktionen integriert und richtig verwendet.

***Gibt es auch seitens der Anlagenbetreiber Schutzbedürfnisse?***
Ein Hersteller von Markenkleidung zum Beispiel möchte sicher gehen, dass auf seinen Produktionsanlagen in Asien nur die angeforderte Menge an T-Shirts produziert und ausschließlich an ihn abgegeben wird. Er will verhindern, dass außerhalb der vereinbarten Produktionszeiten weitere Stück ge-

Bildquelle © VDMA, BSR

fertigt werden, die die Produzenten auf dem Graumarkt auf eigene Rechnung verkaufen. Ein entsprechender Schutz kann verhindern, dass unbemerkt mehr produziert wird. Die Mechanismen können in allen Industrien Anwendung finden, stehen jedoch noch am Anfang. Im Zuge von Industrie 4.0, wenn immer mehr Daten in die Produktion wandern, wird der Schutz zunehmend wichtiger.

***Gibt es einen Standard in Bezug auf Schutzmechanismen, auf den sich Hersteller beziehen können?***
Standards, die für die Safety genormt sind und nationale oder internationale Gültigkeit besitzen, gibt es derzeit für die Security nicht. Es entstehen derzeit Normen wie die IEC 62443 oder ISA99 in den USA, die versuchen Security Assurance Level (SAL) zu definieren. Rücksicht finden dabei sowohl Produkt- und Know-how-Schutz wie auch Schutz vor Manipulation und Veränderung.

***Welche Kriterien sollte ein Hersteller bei der Wahl seines Lieferanten bereits heute berücksichtigen?***
Hersteller und Betreiber sollten darauf achten, dass sie ihr Know-how schützen können. Darüber hinaus sollten die Lieferanten bei der Kommunikation auf offene Standards setzen, damit eine Interoperabilität gegeben ist. So können Maschinen- oder Anlagenbauer auch unterschiedliche Komponenten zu einer Gesamtanlage integrieren.

Wenn diese offenen Standards die Sicherheit unterstützen, bedeutet das für die Anwender ein großes Plus. Beispiele sind OPC UA oder IEC 62541, die eine sichere Kommunikation von Komponenten ermöglichen. Intelligente Schutzmechanismen eröffnen Maschinen- und Anlagenbauern neue Geschäftsmodelle, nämlich dann, wenn Funktionen, die in Software realisiert sind, damit konfiguriert werden können. ←

## Know-how schützen mit Technology Guarding

Mit Technology Guarding schützen B&R-Kunden ihre Produkte und ihr Know-how zuverlässig. Den dafür nötigen USB-Dongle bringt B&R auf Wunsch bereits bei der Assemblierung an.

**Mit Technology Guarding von B&R können Maschinen- und Anlagenbauer ihr Know-how und ihre Prozessdaten schützen. Sie haben die Möglichkeit, Lizenzen einfach zu verwalten und Betriebsstunden manipulationssicher zu zählen.**

Für die Verwaltung von einzelnen Maschinenoptionen auf unterschiedlichen Maschinen können B&R-Kunden Technology Guarding nützen. Auf der einen Seite sind Anlagenbetreiber in der Regel nicht bereit, Funktionen zu bezahlen, die sie nicht für ihre Anwendung nützen. Auf der anderen Seite wollen Maschinen- und Anlagenbauer zusätzliche Funktionen nicht einfach kostenfrei zur Verfügung stellen. Sie müssen daher die Maschinenoptionen pro Kunde verwalten. B&R bietet ihnen dafür ein Lizenzmanagement an. Die jeweiligen Lizenzen pro Kunde werden zentral über einen Lizenzserver verwaltet und an der Maschine über einen USB-Dongle sichergestellt.

**USB-Dongle ist Teil der Hardware-Assemblierung**
Technology Guarding wird in der Software Automation Studio programmiert und mittels eines USB-Sticks an der Hardware umgesetzt. Bereits während der Assemblierung der Hardwareprodukte kann B&R den USB-Dongle anbringen, sodass der Kunde die Komponenten zum Beispiel direkt an den Schaltschrankbauer liefern lassen kann. Sollte es nötig sein, die Hardware im Feld zu tauschen, stellt dies kein Problem dar. Der USB-Stick wird einfach in die neue Komponente eingesetzt und übernimmt dort automatisch seine Funktion.

**Betriebsstunden manipulationssicher zählen**
Mit Technology Guarding schützen Maschinen- und Anlagenbetreiber nicht nur ihre eigenen Produkte, sie können auch ihren Kunden wertvollen Schutz bieten. So lassen sich zum Beispiel an der Maschine die Betriebsstunden manipulationssicher mitzählen. Produkte können nicht unbemerkt hergestellt werden und dann etwa illegal den Weg auf den Markt finden. Hersteller, die ihre Maschinen verleasen, können mit dieser Funktion sicherstellen, dass die Abrechnung der Betriebsstunden auf den Maschinen korrekt ist. Technology Guarding bildet für Hersteller die technische Basis für ihre Leasing-Geschäftsmodelle.

**Die Vorteile**
- Produkt-Know-how und Prozessdaten schützen
- Betriebsstunden manipulationssicher zählen
- Maschinenoptionen effizient verwalten