PRÄVENTION GEGEN
PRODUKTPIRATERIE

Das Technologie-Netzwerk:
Intelligente Technische Systeme OstWestfalenLippe

it's owl

Produkt- und Know-how-Schutz

Mit Hintergrundinformationen
vom Verfassungsschutz

Projektvorstellung

Projektteam v.l.n.r.: Daniel Kliewe (Fraunhofer), Stefan Peter (HNI), Ulrich Jahnke (DMRC), Katharina Altemeier (UNITY AG), Daniel Eckelt (HNI)

Das Forschungsverbundprojekt „Prävention gegen Produktpiraterie – Innovationen schützen“ (3P) des Spitzenclusters it’s OWL „Intelligente Technische Systeme OstWestfalenLippe“ wird gemeinsam von vier Partnern aus Forschung und Wirtschaft durchgeführt. Das Projekt trägt dazu bei, die Forschungs- und Entwicklungsinvestitionen der Clusterunternehmen nachhaltig gegen Produktpiraterie zu sichern.

Ein Augenmerk des Projekts ist, durch Aufklärung und Sensibilisierung ein Bewusstsein für die vielfältigen Bedrohungen durch Produktpiraterie zu schaffen. Darüber hinaus soll die Industrie zur Anwendung präventiver Schutzmaßnahmen wie dem „Social Engineering“ geführt werden, da juristische Maßnahmen lediglich eine Teilmenge eines ausgewogenen Schutzportfolios darstellen können.

Insbesondere intelligente technische Systeme (ITS), die das Potential für einen branchenübergreifenden Innovationssprung bieten, gilt es frühzeitig und ganzheitlich zu schützen. Einerseits stellen ITS völlig neue Anforderungen an den Produktschutz, andererseits bieten sie inhärente Lösungsmöglichkeiten. Nur durch die Berücksichtigung dieser Aspekte können der Wettbewerbsvorsprung erhalten und Arbeitsplätze langfristig gesichert werden.

Weitere Informationen finden Sie unter „Projekte\Nachhaltigkeitsmaßnahmen“ auf: **www.its-owl.de**

Indikatoren für eine drohende Gefahr

Das vorliegende Informationsblatt soll Sie auf das Thema „Bedrohung Ihres Unternehmens durch Wirtschaftsspionage[1] und Konkurrenzausspähung[2]“ aufmerksam machen. Im Fokus des Berichts stehen Aktivitäten der Nachrichtendienste, die derzeitig einen großen Anteil an der weltweiten Bedrohung durch Spionage ausmachen. Hierzu zählen unter anderem China, Russland, Israel, USA etc. Besonders gefährdet sind deutsche Unternehmen des Maschinen- und Anlagenbaus sowie verwandter Branchen.

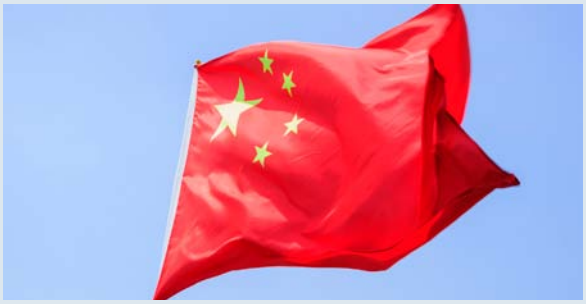
Ziel ist es, Sie mit fundierten Hintergrundinformationen, bereitgestellt durch das Bundesamt für Verfassungsschutz, zu sensibilisieren. Neben der Darstellung potentieller Gefahren der Wirtschaftsspionage und Konkurrenzausspähung durch die Nachrichtendienste werden wir Sie auch auf präventive Aspekte zur Spionageabwehr hinweisen.

Den besten Schutz vor Know-how-Verlust stellen präventive Maßnahmen dar. Durch die kontinuierliche Beobachtung und Analyse folgender Indikatoren können Sie präventive Schutzmaßnahmen[3] frühzeitig einleiten und einen effektiven Schutz Ihrer sensiblen Daten gewährleisten. [BfV07]

- Einbußen beim Know-how-Vorsprung
- Verlust oder Diebstahl von Datenträgern
- Dubiose Geschäfts- und Gesprächspartner
- Auffälliges Verhalten eines Mitarbeiters
- Unerklärlicher Rückgang von Aufträgen, Kundenverlust
- Einbindung eines chinesischen Firmenangehörigen oder herausragenden Wissenschaftlers in ein bundesweites Akademikernetz – wie z.B. „Vereinigung Chinesischer Akademischer und Studentischer Gesellschaften in Deutschland“ (CASD)
- Plagiate durch Konkurrenzfirmen

Die chinesischen Nachrichten- und Sicherheitsdienste

Aufgrund der von Deng Xiaoping Ende der 1970er Jahre eingeleiteten und in den Folgejahren konsequent fortgeführten Reform- und Öffnungspolitik konnte die chinesische Wirtschaft enorm wachsen. Das derzeitige Entwicklungsprogramm sieht vor allem eine weitere Steigerung der Innovationsfähigkeit u.a. durch die Aneignung von westlichem Know-how für alle Bereiche der chinesischen Wirtschaft vor. Die Volksrepublik China unternimmt daher auch weiterhin enorme Anstrengungen, um zügig die Technologielücke zu den hochentwickelten Industriestaaten zu schließen. Die chinesischen Nachrichten- und Sicherheitsdienste haben mit ihren speziellen Instrumenten alle Möglichkeiten, dieses strategische Vorhaben umfassend zu unterstützen.



Die deutschen Nachrichtendienste wissen schon seit längerer Zeit, dass die Volksrepublik China sich hierbei stark auf die Arbeit ihrer Nachrichtendienste stützt. Dabei erfolgt die Beschaffung von Know-how und westlicher Hightech-Produkte auf breiter Front über sämtliche staatlichen und privaten Ebenen mit allen zur Verfügung stehenden Mitteln und Wegen, auch unter Verletzung des geistigen Eigentums u.a. durch Missachtung von Patentrechten. [BfV07]

1 Unter Wirtschaftsspionage ist die staatlich gelenkte oder gestützte, von fremden Nachrichtendiensten ausgehende Ausforschung von Wirtschaftsunternehmen und Betrieben zu verstehen.
2 Bei der Konkurrenzausspähung handelt es sich um die Ausforschung, die konkurrierende Unternehmen gegeneinander betreiben.
3 Über Schutzmaßnahmen, die für Ihr Unternehmen geeignet sind, geben wir Ihnen gerne einen Überblick.

Reale Gefährdungssituation

Angriffsziele

Grundsätzlich kann man davon ausgehen, dass es wenig gibt, das für die Nachrichtendienste und Produktfälscher uninteressant ist. Sobald mit einem Produkt oder einer Entwicklung finanzieller Erfolg, sprich Gewinn, zu erwarten ist, besteht die reale Gefahr der Spionage. Dennoch lassen sich einige Angriffsziele herausstellen [BfV07]:

- Forschungsergebnisse, Produktideen und Designstudien
- Konstruktionsunterlagen, Herstellungsverfahren, Qualitätsprüfungsmaßnahmen
- Spezialwerkzeuge und Steuerungssysteme
- Lieferanten, Versorgungskonzeptionen, Lagerbestände
- Strategische/ taktische Entscheidungen der Unternehmensleitung
- Verkaufsstrategien, Marketingstudien, Absatz-/ Vertriebswege, Lizenzverträge
- Umsätze und Kundenadressen
- Kalkulationsunterlagen, Budgetplanungen und Investitionsvorhaben

Schwachstellen im Unternehmen

Sicherheitsbezogene Schwachstellen im Unternehmen (z.B. unzufriedene Mitarbeiter) werden von den Nachrichtendiensten oder konkurrierenden Unternehmen gezielt genutzt. Bei folgenden Themen sollten Sie mit größter Achtsamkeit agieren [BfV07].

- Joint Ventures
- Personalaustausch im Unternehmen
- Offenlegungspflichten wie Zertifizierungsverfahren (CCC) oder Verpflichtungen zur Nutzung chinesischer Architektur- und Designinstitute
- Mangelnder Schutz von Patenten, Gebrauchs- und Geschmacksmustern
- Überwachung ausländischer Geschäftsleute und Wissenschaftler durch chinesische Sicherheitsbehörden

Abb. 1: Herausforderung Produktpiraterie – eine Bedrohung für deutsche Unternehmen [VDMA12]

Reale Gefährdungssituation

Beschaffungsmethoden der Nachrichtendienste

Der Informationsbeschaffung liegt eine massive kriminelle Energie zugrunde. Folgende Methoden sollten Sie kennen [BfV07]:

- Überwachung der Telekommunikation
- Eindringen in Informationssysteme
- Abhör- und Lauschangriffe
- Zweckentfremdung von Gebrauchsgegenständen (USB-Sticks)
- Diebstahl von Entwicklungsunterlagen, Software, Proben, Mustern, Zeichnungen, digitalen Datenträgern
- Zugriff auf Kommunikationstechnik (wie beispielsweise kurzfristiges Entziehen von Laptops zum Kopieren der Festplatte)
- Schaffung von Kompromatsituationen zur Anwerbung/ Erpressung

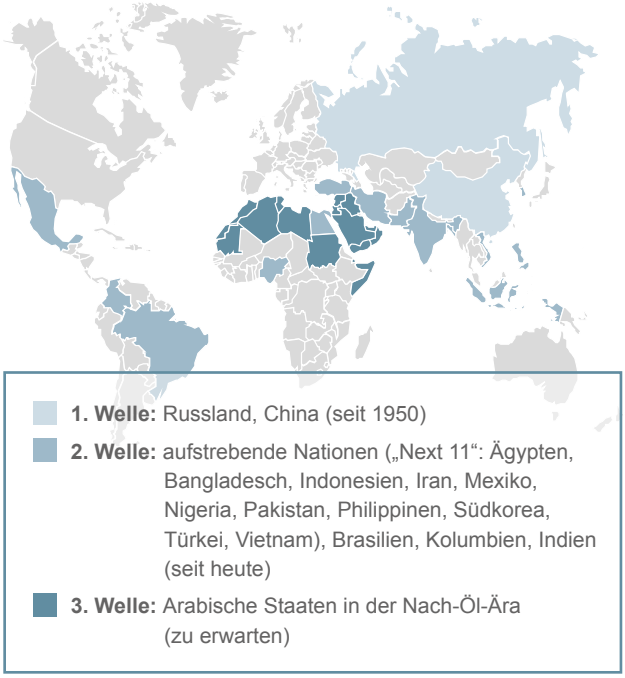
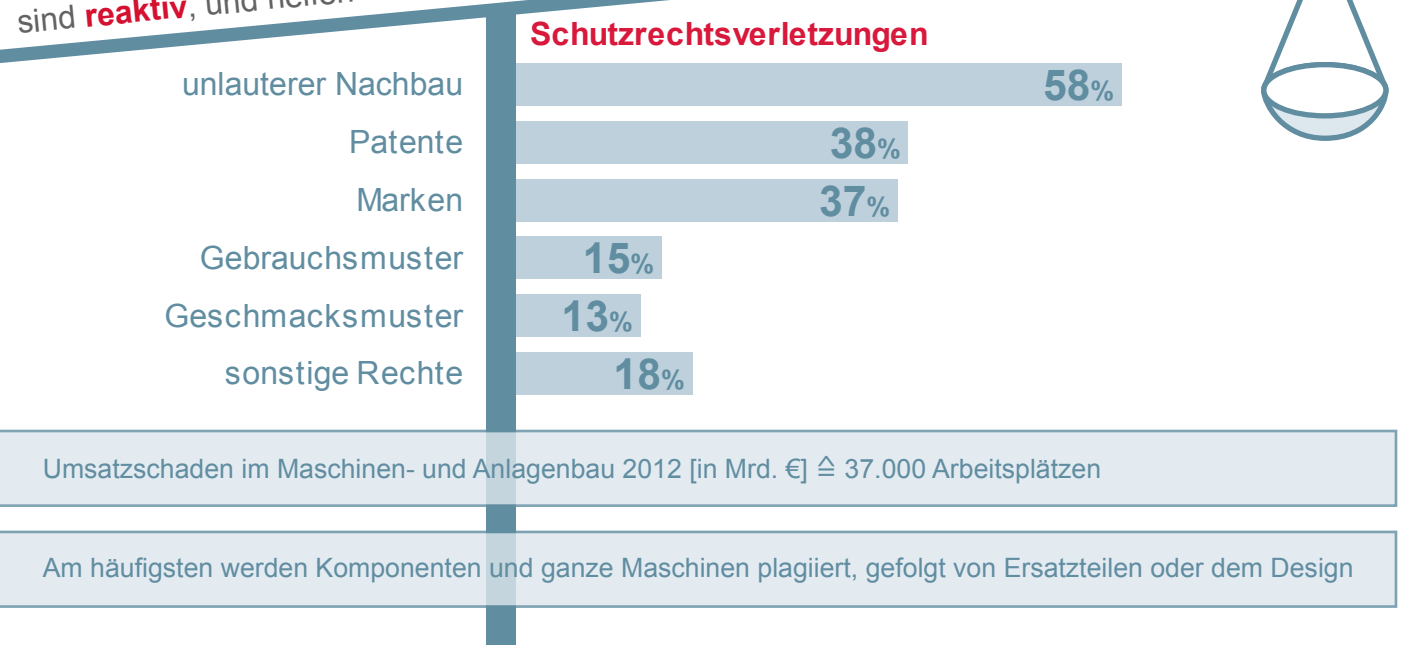


Abb. 2: Die drei Wellen der Wirtschaftsspionage [VDMA13]

sind **reaktiv**, und helfen erst, wenn bereits Schaden entstanden ist. **Sie reichen nicht aus!**



Umsatzschaden im Maschinen- und Anlagenbau 2012 [in Mrd. €] ≙ 37.000 Arbeitsplätzen

Am häufigsten werden Komponenten und ganze Maschinen plagiiert, gefolgt von Ersatzteilen oder dem Design

Wahre Geschichten

Wenn die Liebe zum Verhängnis wird, ...
… steht es schlecht um die Mitarbeiterloyalität. Einem deutschen Unternehmen ist Folgendes widerfahren: Nachdem sich der Angestellte „Hals über Kopf“ in die chinesische Praktikantin verliebte, verschwanden kurz darauf wichtige Daten in Richtung China. Ein chinesischer Wettbewerber konnte binnen kurzer Zeit einen Entwicklungssprung von 15 Jahren vorweisen. Die genaue Sachlage konnte nie geklärt werden, aber die Indizien sind eindeutig.
Konsequenz für das Unternehmen:
Massive Umsatzausfälle

Wenn Ihre Mitarbeiter auf XING aktiv sind, ...
… sollten Sie das Folgende wissen: Ausländische Nachrichtendienste, die Komplizen in deutschen Unternehmen suchen, finden alle Informationen im Internet. Besonders beliebt ist die Recherche auf dem Sozialen Netzwerk XING. Die Nachrichtendienste finden hier alle Informationen, um den nächsten Informanten zu identifizieren.
Risiko: Informationsverlust

Wenn der Besuch vor der Tür steht, ...
... sollten Sie besonders aufmerksam sein. Chinesische Delegationen reisen in der Regel in großen Gruppen an und sind nur schwer zu kontrollieren. Einer will rauchen, der nächste muss auf die Toilette und ein weiterer fühlt sich plötzlich unwohl. Da die Vertreter des heimischen Unternehmens in der Regel in deutlicher Unterzahl sind, fällt es ihnen schwer, alle Besucher zu beaufsichtigen. In zahlreichen Fällen wurden Bild- oder Filmaufnahmen erstellt oder sogar Daten von ungeschützten Informationssystemen auf mobile Datenträger gespeichert.
Risiko: Verlust sensibler Informationen

Wenn das Geld lacht, …
... gelten plötzlich andere Gesetze. Einem österreichischen Unternehmen wurde diese Geschichte zum Verhängnis: Ein als Schwachstelle des Unternehmens identifizierter Angestellter wurde von chinesischen Spionen angesprochen und für die Übermittlung sensibler Daten bezahlt. Der Fall klärte sich zwar vor Gericht bis ins Detail auf, das Unternehmenswissen aber war verloren.
Konsequenz für das Unternehmen:
Drohende Insolvenz

Wenn Sie einen USB-Stick auf Ihrem Unternehmensparkplatz finden, ...
… hat diesen nicht immer jemand verloren. Eine einfache aber effektive Masche zum Eindringen in Informationssysteme ist das Platzieren von USB-Sticks an auffälligen Orten. Findet Ihr Mitarbeiter den Datenträger, geht er wohlmöglich von einem Verlust aus und hat noch gute Absichten, wenn er diesen zur Bestimmung des Eigentümers mit seinem Computer verbindet. Was er nicht weiß: der Datenträger ist mit einem Trojaner gespickt.
Risiko: Ungesichertes Unternehmensnetzwerk

Schutzmaßnahmen gegen Wirtschaftsspionage

Checkliste

Zur Prävention eines möglichen Informationsabflusses sind Sicherheitskonzepte unumgänglich. Nachfolgend sind beispielhaft einige der möglichen Schutzmaßnahmen dazu aufgeführt [BfV07]:

- Erstellung und Umsetzung eines IT-Sicherheitskonzepts
- Aufmerksame Besucherbetreuung
- Schutz der Kerninformationen des Unternehmens
- Verhinderung von Know-how-Abfluss durch registrierbare Schutzrechte
- Möglichst Einsatz von eigenen Dolmetschern
- „Need-to-know“-Prinzip bei firmeneigenem Know-how
- Wegschließen von vertrauliche Unterlagen beim Verlassen des Arbeitsplatzes
- Gesundes Misstrauen gegenüber firmenfremdem Personal
- Prüfung von Bewerbungen (Referenzpersonen, Lücken in Lebensläufen, Unter- oder Überqualifizierung, Initiativbewerbungen und sonstige Auffälligkeiten)
- Striktes Einhalten von Zugangsberechtigungen
- Fachkundiges Personal am Empfang
- Anmeldung und Registrierung aller Besucher (Name, Grund, Zeitpunkt Betreten und Verlassen)
- Erfassung und Registrierung von Besucherfahrzeugen
- Begleitung von Besuchern
- Sichtbares Tragen eines Besucherausweises
- Schriftliche Anerkennung der Sicherheitsvorschriften (z.B. Film- und Fotografierverbot, Umgang mit mobilen Datenträgern)
- Keinen oder eingeschränkten Zugriff auf das Firmennetzwerk gewähren
- Konsequentes Vorgehen bei Missachtung

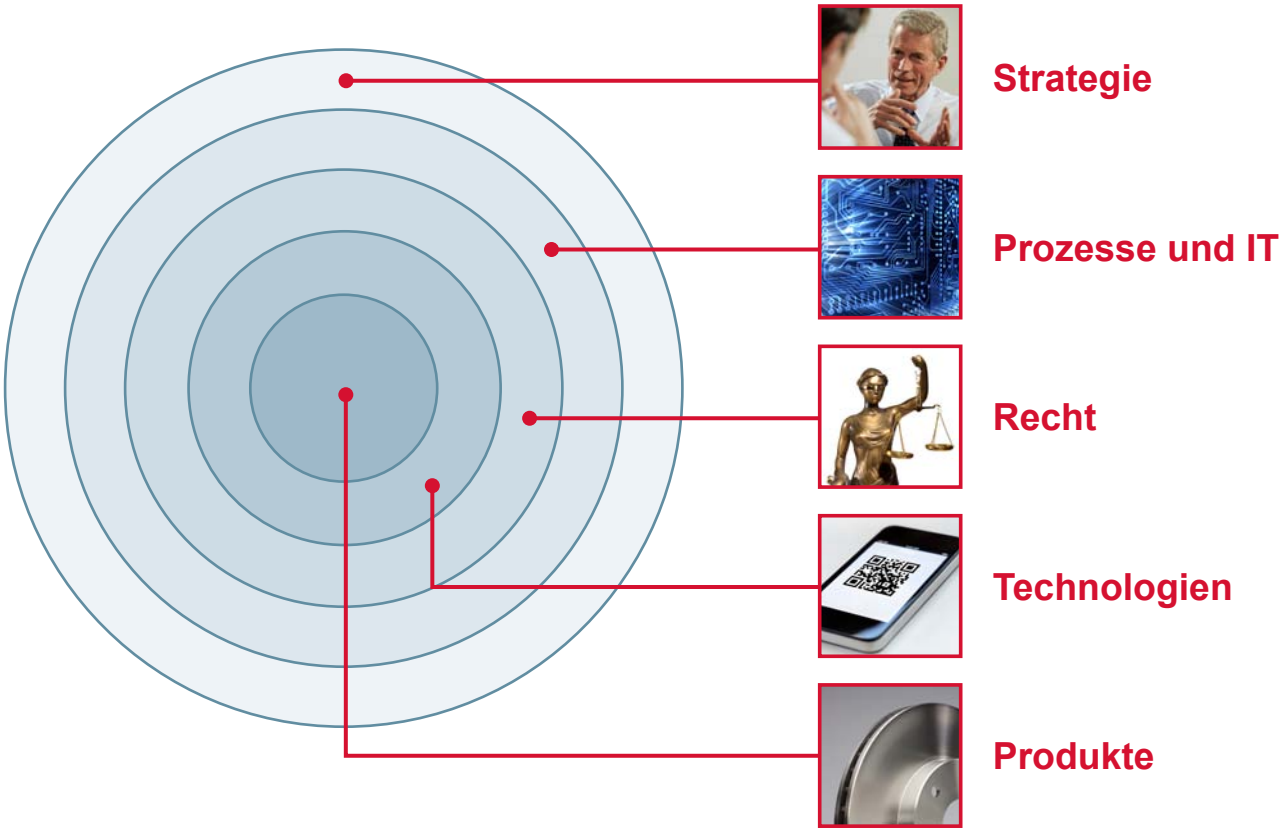


Abb. 3: Ganzheitlicher Produktschutz erfolgt auf 5 Ebenen [UNITY AG]

Kontakt

Für Fragen und Erläuterungen stehen wir Ihnen selbstverständlich gern zur Verfügung.

UNITY
CONSULTING & INNOVATION

Christoph Plass
Mitglied des Vorstands
UNITY AG
Lindberghring 1
33142 Büren

Telefon +49 2955 743-434
Fax +49 2955 743-299
E-Mail christoph.plass@unity.de
www.unity.de

HEINZ NIXDORF INSTITUT
Universität Paderborn
Produktentstehung
Prof. Dr.-Ing. Jürgen Gausemeier

Prof. Dr.-Ing. Jürgen Gausemeier
Seniorprofessor
Heinz Nixdorf Institut
Universität Paderborn
Fürstenallee 11
33102 Paderborn

Telefon +49 5251 606267
Fax +49 5251 606268
E-Mail juergen.gausemeier@hni.upb.de
www.hni.uni-paderborn.de/pe

Quellenangaben:

[BfV07] **Bundesamt für Verfassungsschutz (BfV):**
Spionageabwehr – Bedrohung der deutschen Wirtschaft durch chinesische Wirtschaftsspionage: Information und Prävention, 2007
Unter: http://www.germanexpats.com/papers/bfv_chi.pdf, 14. März 2014

[VDMA13] **Verband Deutscher Maschinen- und Anlagenbau e.V. (VDMA):**
Status quo des Know-how Schutzes im Maschinen- und Anlagenbau, 2013
Unter: http://pks.vdma.org/article/-/articleview/1351004, 14. März 2014

[VDMA12] **Verband Deutscher Maschinen- und Anlagenbau e.V. (VDMA):**
VDMA Studie Produktpiraterie, 2012.
Unter: http://pks.vdma.org/article/-/articleview/783674, 14. März 2014

Dieses Forschungs- und Entwicklungsprojekt wird / wurde mit Mitteln des Bundesministeriums für Bildung und Forschung (BMBF) im Rahmen des Spitzenclusters „Intelligente Technische Systeme OstWestfalenLippe (it´s OWL)“ gefördert und vom Projektträger Karlsruhe (PTKA) betreut. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autor.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

BETREUT VOM
PTKA Projektträger Karlsruhe
Karlsruher Institut für Technologie

INVENTED IN GERMANY