KARG UND PETERSEN
Kommunikation für Weiterdenker

Whitepaper

Kommunikationsstrategien für effektiven Know-how-Schutz

Neue Trends im Know-how-Schutz

So schafft Unternehmenskommunikation zukunftsfähige Sicherheitskulturen

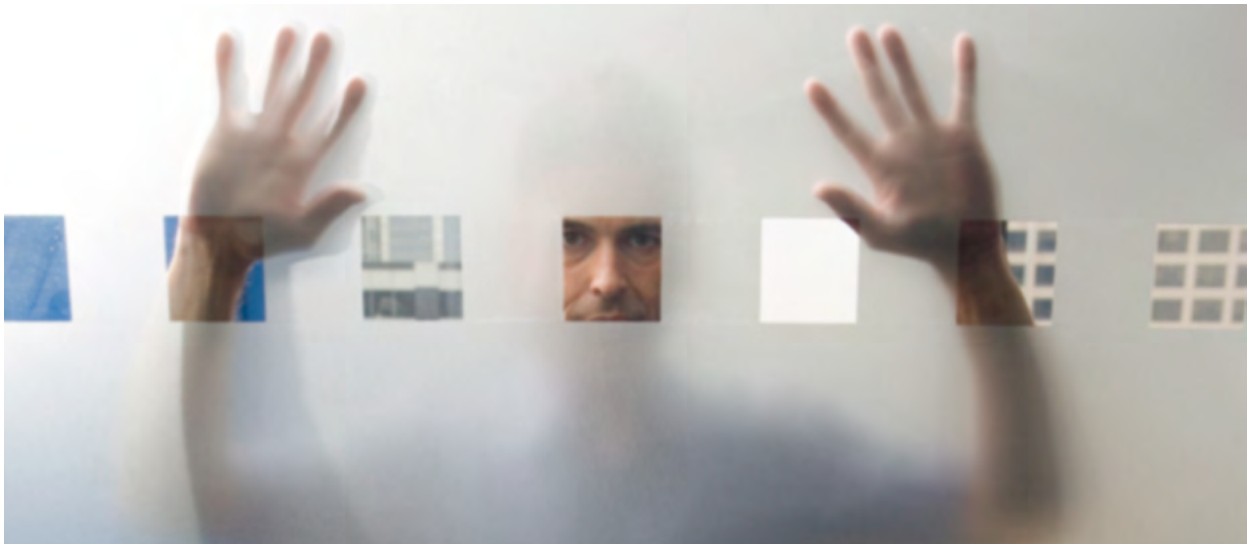
Dr. Tim Karg, Dipl. Pol. Steffen Baumhauer

Das vorliegende Whitepaper basiert auf einem 2013 erschienen Beitrag
im Sicherheits-Magazin SECURITY insight (Seite 38f., Ausgabe 2/2013)

Kurzfassung

Know-how-Schutz und Informationssicherheit sind entscheidend für den Unternehmenserfolg – insbesondere auch im Mittelstand und bei kleineren Unternehmen. Während viele Firmen bereits mit neuer IT aufrüsten, wird eine Gefahrenquelle noch viel zu oft unterschätzt: die Menschen selbst, die im Unternehmen und seinem Umfeld arbeiten. Neue Wege binden daher die Unternehmens-kommunikation gezielt in den Know-how-Schutz ein, um Mitarbeiter und Geschäftspartner zu sensibilisieren und zu Mitstreitern für mehr Sicherheit zu machen. Ziel ist es, Know-how umfassend und präventiv zu schützen – und eine vertrauensvolle, selbstbewusste und wehrhafte Sicherheitskultur zu schaffen.

November 2013



Die entscheidende Gefahr bei Know-how-Diebstahl sind die Menschen selbst – sowohl im Unternehmen selbst als auch im direkten Umfeld.

1. Herausforderung Informationssicherheit

Der Schaden, der in der deutschen Wirtschaft durch Know-how-Diebstahl und Informationsabfluss entsteht, ist schwer zu messen und verdeutlicht doch eindrucksvoll, wie relevant das Thema für eigentlich jedes Unternehmen ist. Eine aktuelle Studie geht beispielsweise für das Jahr 2012 von etwas über 4 Milliarden Euro Schadenssumme durch Industriespionage aus, 50 Prozent mehr als noch 2007. Dagegen schätzt das Bundesamt für Verfassungsschutz, dass deutschen Unternehmen jedes Jahr sogar rund 30 bis 60 Milliarden Euro Schaden durch Know-how-Diebstahl und Produktpiraterie entstehen.[1] In einer Umfrage unter mittelständischen Betrieben aus Baden-Württemberg gaben rund zwei von drei Unternehmen an, bereits Opfer ungewollten Know-how-Abflusses gewesen zu sein.[2]

Für die Unternehmen kann das schmerzhafte Folgen haben: Neben signifikanten finanziellen Verlusten zählen zu den möglichen Konsequenzen auch langfristige Nachteile gegenüber Wettbewerbern oder etwa Imageschäden für das eigene Unternehmen. Teilweise werden die Auswirkungen erst Jahre später sichtbar, etwa durch sinkende Margen oder den Verlust von Marktanteilen.[3]

Generell können Unternehmen verschiedenster Größe und unterschiedlichster Branchen von Know-how-Abfluss betroffen sein. Die Gefahr beschränkt sich dabei nicht, wie oft vermutet wird, auf international tätige Konzerne oder große Forschungsabteilungen. Im Gegenteil: Gerade kleinere, innovative Unternehmen in Deutschland sind sogar überproportional stark gefährdet. Und rund acht von zehn Spionagefällen ereignen sich nicht etwa im Ausland, sondern im Inland.[4] Diese Gefahr wird in vielen innovativen Unternehmen aus dem heimischen Mittelstand oftmals noch deutlich unterschätzt.

Defizite und Risiken im Know-how-Schutz werden oft bereits im Arbeitsalltag vieler Unternehmen deutlich: Flipchart-Notizen, die nach einem Meeting achtlos hängen gelassen werden; der Vertriebsmitarbeiter, der mutmaßlichen Neukunden wunschgemäß ein Angebot mit ungewöhnlich ausführlichen technischen Spezifikationen vorstellt; oder

etwa das Passwort, das zu einfach ist und für den IT-Spion kein Hindernis darstellt – trotz vieler Warnungen sind Kombinationen wie „123456“ oder „iloveyou“ unter den häufigsten Passwörtern.[5]

Was manchem als Sicherheits-Alptraum erscheinen mag, kommt in der Praxis immer wieder vor – egal ob interne Details an eine Facebook-Bekanntschaft weitergegeben oder hochgeheime Konstruktionspläne für jeden zugänglich in einem Müllcontainer im Hinterhof entsorgt werden. Der Verfassungsschutz kennt daneben Fälle, in denen Mitarbeiter absichtlich großen Schaden verursachten, wie der Austauschstudent, der ungehindert Daten auf eine externe Festplatter kopiert, oder den Entwicklungsingenieur, der den Quellcode einer Steuerungssoftware an die Konkurrenz weiterleitet.[6]

Klassischerweise reagieren Unternehmen mit technischen Schutzsystemen wie IT-Firewalls und Verschlüsslungssoftware. Oder mit organisatorischen Maßnahmen wie Zutrittskontrollen am Werkstor. Allerdings reichen solche Schritte allein meist nicht aus. Auch die oben erwähnten Beispiele hätten durch keine noch so technisch perfekte Firewall verhindert werden können.

2. Neues Potenzial durch Kommunikation

Ohne die aktive Unterstützung durch die eigenen Mitarbeiter kann firmeninterner Know-how-Schutz nicht funktionieren. Das zeigen auch aktuelle Forschungsergebnisse, in denen immer wieder deutlich wird: Wenn Know-how verloren geht, sind in den allermeisten Fällen Mitarbeiter oder Geschäftspartner direkt beteiligt![7] Dabei können sie entweder als „Innentäter“ absichtlich Informationen stehlen, oder ganz unbeabsichtigt Know-how nach außen dringen lassen. So oder so sind die Menschen das größte Risiko – und daher sind sie auch zentral für den Erfolg entsprechender Schutzmaßnahmen.

Auf diese Erkenntnis folgen bei vielen Firmen Vertraulichkeitserklärungen für die eigenen Mitarbeiter und Geschäftspartner. Inwiefern diese Maßnahmen den gewünschten Sicherheitseffekt erzielen können, bleibt allerdings fraglich. So zeigt eine Studie aus den USA,[8] dass in den allermeisten Fällen, in denen Know-how absichtlich von internen Tätern verraten wurde, eine solche Verschwiegenheitsvereinbarung vorlag. Bei unbeabsichtigten Know-how-Verstößen greifen die Vereinbarungen sogar noch weniger, ist sich der Täter doch gar nicht bewusst, dass er etwas Falsches tut. Rechtliche Vereinbarung ohne aktive Information und Sensibilisierung sind also nicht effektiv.

Unternehmen müssen die Personen, die Zugang zu Ihrem Know-how haben, aktiv in den Know-how-Schutz einbinden. Das direkte Firmenumfeld rückt somit in den Fokus: Allen voran sind natürlich die eigenen Mitarbeiter wichtig, aber auch Geschäftspartner, Vertriebsfirmen oder Joint-Venture-Partner können beim Know-how-Schutz relevant werden. Darüber hinaus kann es sinnvoll sein, auch Dienstleister in die Schutzmaßnahmen mit einzubeziehen, wie beispielsweise IT Service Provider, Zeitarbeitsfirmen oder externe Pförtner und Reinigungspersonal.

Hier setzen spezielle Kommunikationsmaßnahmen an. Es geht darum, Aufmerksamkeit und Risikobewusstsein zu schaffen, vor allem aber auch Menschen aufzuklären, zu informieren und mitzunehmen, um aktiv Know-how-Verlust vorzubeugen und Geheimnisse zu schützen.

Nicht nur der unabsichtliche Know-how-Abfluss kann verhindert werden, wenn ein Bewusstsein für Informationssicherheit geschaffen wird („Awareness"). Sondern auch gezielte Versuche der Industriespionage können so abgewehrt werden. Denn für Hacker-Angriffe und Password Phishing sind unachtsame Mitarbeiter ein willkommenes Einfallstor, ähnlich auch für das oft als Social Engineering bezeichnete gezielte Ausfragen und Manipulieren von Gesprächspartnern.

Nur wenn die Mitarbeiter wissen, wie wichtig Informationssicherheit ist und dass auch sie selbst beim Know-how-Schutz gefragt sind, können sie aktiv zum Schutz vor Industriespionage und Konkurrenzausspähung beitragen. Kommunikation verstärkt gezielt die Wirksamkeit bestehender Maßnahmen: IT-Schutz, Zutrittskontrollen, etc. werden den Mitarbeitern erklärt und zugleich wird deren Partizipation und Mithilfe eingefordert. Im Einzelfall ist es außerdem sinnvoll, auch die Konsequenzen eines möglichen Fehlverhaltens mit dem notwendigen Fingerspitzengefühl offen und transparent anzusprechen.

Kommunikation bietet so entscheidendes, neues Potenzial für einen effektiveren Know-how-Schutz. Sie kann die Loyalität zum Unternehmen steigern, Aufmerksamkeit sowohl gegen unbeabsichtigte Know-how-Abflüsse als auch gezielte Angriffe schaffen, Handlungsanweisungen geben und sogar helfen, mögliche Lecks frühzeitig zu entdecken. Kurz zusammengefasst: Die eigenen Mitarbeiter werden zu Mitstreitern, die sowohl im Alltag als auch bei speziellen Situationen wie etwa Werksführungen oder Messen auf Informationssicherheit achten.

Fallbeispiele: Informations-Abfluss – und wie Kommunikation ihn verhindert

Unabsichtliches Leck

Zufrieden lehnt sich Karin R. zurück. Ihr neuer Fachartikel im einschlägigen Branchenmagazin wird Eindruck machen, da ist sie sich sicher. Schließlich ist ihr Produkt der Konkurrenz um Jahre voraus – und wenn nun erst einmal die technischen Details ihrer neuesten Errungenschaft bekannt werden, dürften die Kundenaufträge von selbst hereinflattern.

Am nächsten Tag lernt Karin beim e-Learning-Modul zur Informationssicherheit, dass öffentliche Quellen wie Fachartikel oder auch ganz einfach fingierte Kundenanfragen eine der wichtigsten Informationsquellen in der Wirtschaftsspionage sind. Vorsichtig geworden denkt sie noch einmal nach, überarbeitet ihren Artikel und beschränkt die technischen Details auf ein vertretbares Minimum.

Frustrierter Mitarbeiter

Klaus M. plant, eine Mail an einen Freund bei einer Konkurrenzfirma zu schicken. Er ist seit längerem mit seiner Arbeit in der Kundenbetreuung unzufrieden und überlegt, den Job zu wechseln. Zusammen mit seiner Frage, wie die Stellensituation bei der Konkurrenz aussieht, möchte er auch einige Projektexzerpte versenden – schließlich soll sein Freund ja auch sehen, was er die letzten Jahre alles geleistet hat.

In einem Newsletter zum Thema Know-how-Schutz erfährt Klaus kurze Zeit später mehr zur Informationssicherheit in seiner Firma. Er wird unter anderem daran erinnert, dass er als „restricted" gekennzeichnete Projektbeispiele nicht weitergegeben darf. Und es wird ihm bewusst, dass er entdeckt werden könnte – und dass bei Missachtung möglicherweise ernste Strafen auf ihn warten. Das Risiko möchte Klaus nicht eingehen.

Hacker-Angriff

„Schon wieder die von der IT", denkt sich Lukas P. zu der E-Mail, die ihn auffordert, Benutzernamen und Passwort neu zu vergeben. Und das gerade jetzt, wo er ein wichtige Projektpräsentation fertig machen muss. Lukas überlegt nicht lange, sondern antwortet gleich. Schließlich möchte er schnell mit der „eigentlichen" Arbeit weitermachen. So bemerkt er auch nicht die eigentlich auffällig vielen Rechtschreibfehler in der Mail.

Kurz danach holt Lukas Ausdrucke für seine Projektpräsentation und bemerkt das neue Sicherheits-Plakat direkt über dem Drucker. Sofort denkt er an die Mail, die er vor kurzem erhalten hatte und die er nun in einem ganz anderen Licht sieht. Misstrauisch geworden leitet er die verdächtige Nachricht sofort an den IT-Schutz weiter, so dass die Kollegen dort schnell auf die mögliche Bedrohung reagieren können.

3. Breite Maßnahmen-Palette und individuelle Lösungen

Spezielle Kommunikation für Know-how-Schutz und Informationssicherheit bietet zahlreiche verschiedene Maßnahmen. Sicherheitsverantwortliche müssen sich also zunächst fragen, was genau sie erreichen wollen.

Wenn zuerst einmal grundlegende Aufmerksamkeit für das Thema Informationssicherheit geschaffen werden soll, kann man etwa auf klassische Kampagnen-Medien wie unternehmensinterne Plakate setzen, die aufmerksamkeitsstark in der Kantine oder neben der Zeitschaltuhr positioniert werden. Eine weitere Möglichkeit sind Dialog-Medien, etwa gezielte E-Mail-Aussendungen, die sich kostengünstig und schnell im Betrieb umsetzen lassen. Damit klar wird: Know-how-Schutz ist die Aufgabe jedes Einzelnen, nicht nur der Sicherheitsabteilung.

Soll Know-how-Schutz nachhaltig verankert werden, eignet sich beispielsweise ein firmeninterner Newsletter, der regelmäßig aktuelle Informationen und Tipps liefert. Ergänzen kann man diese Maßnahmen außerdem durch den gezielten Einsatz von Borschüren: Informationen zur IT-Sicherheit, die zusammen mit einem neuen Laptop ausgegeben werden, oder beispielsweise Hinweise zu Auslandsreisen und zum richtigen Umgang mit Besuchern, die man per E-Mail zugestellt bekommt, sobald man seine Reise gebucht bzw. seinen Besuch angemeldet hat.

In diesen Medien findet auch die Aufklärung und Information („Education“) der Mitarbeiter und Geschäftspartner statt. Wichtig dabei sind klare und praxisnahe Handlungsanweisungen, die zentrale Themen leicht verständlich machen: Was muss ich beachten, wenn ich auf Geschäftsreise gehe? Wie können sensible Dokumente entsorgt werden und wie werden sie gekennzeichnet? Wie funktionieren Zutrittskontrolle und Besucheranmeldung?

Gerade für Firmen, die über mehrere Niederlassungen verteilt sind, können vertiefende Informationen zudem über e-Learning-Angebote vermittelt werden. Mitarbeiter in jedem Standort können so erreicht werden, ohne dass Reisekosten anfallen. Lokale „Informationssicherheits-Botschafter“ unter den Mitarbeitern vor Ort können diesen Effekt sogar ohne großen Aufwand unterstützen mit Hilfe von Kommunikationsmaterialien, die sie aus der Zentrale erhalten. So wird auch sichergestellt, dass in allen Unternehmensstandorten die richtigen Botschaften kommuniziert werden, ohne dabei relevante regionale Besonderheiten außer Acht zu lassen. Daneben können hier aber auch moderne Kommunikationswege wie etwa ein moderiertes Online-Forum oder unternehmensinterne Social Media sehr sinnvoll eingesetzt werden. Wichtig ist zudem ein Intranet-Portal, um auf Gefahrensituationen hinzuweisen und ausführlichere Handlungshilfen zu geben.

Bei all diesen Kommunikationsmaßnahmen ist vor allem eines entscheidend: der richtige Ton. Ein zu starker Fokus auf Risiken und der „erhobene Zeigefinger“ können sogar kontraproduktiv sein.[9] Stattdessen sollte man vor allem auf die Motivation der Mitarbeiter abzielen und überzeugend darstellen, wie wichtig Informationssicherheit für das Unternehmen insgesamt und damit auch für jeden einzelnen Arbeitsplatz ist. Und es kommt entscheidend darauf an, dass die Inhalte passen: Beispielsweise muss das Reinigungspersonal anders angesprochen werden als die Forschungs- und Entwicklungsabteilung.

Gute Know-how-Schutz-Kommunikation setzt dabei auf Spezialmaßnahmen, die exakt auf jedes einzelne Unternehmen, seine Mitarbeiter und die individuelle Bedrohungslage abgestimmt sind. Ein Beispiel dafür sind sogenannte Whistle-Blowing-Systeme, die helfen können, Informations-Lecks frühzeitig zu entdecken, eventuell bereits entstandenen Schaden zu begrenzen oder im günstigsten Falle präventiv vorgehen zu können. Oft empfiehlt sich hierfür ein Ombudsmann, mit dem Mitarbeiter vertrauensvoll reden können. Ein großer Vorteil ist aber auch ein abschreckender Effekt: Durch die Kommunikation des Whistle-Blowing-Systems werden sich Mitarbeiter zugleich bewusst, dass grob fahrlässige oder absichtliche Verstöße sanktioniert werden können – und dass die Möglichkeit besteht, entdeckt zu werden.

Auf keinen Fall darf dabei aber eine Kultur des gegenseitigen Misstrauens und des Denunziantentums im Unternehmen entstehen. Die Informationen und der Ton, in dem die Mitarbeiter zum Whistle-Blowing informiert werden, muss hier eine schwierige Gradwanderung bewältigen. Nur dann werden die Mitarbeiter das Angebot verstehen, ihm vertrauen und es annehmen.

4. Kein erfolgreicher Feldzug ohne Strategie

Die Umsetzung eines kommunikativen Feldzugs ist häufig schwieriger als zunächst gedacht. Und: Lösungen „von der Stange“ können sogar mehr schaden als nutzen. Für einen erfolgreichen und effizienten Know-how-Schutz müssen also einzelne Maßnahmen genau ausgesucht und auf die jeweilige Situation des einzelnen Unternehmens abgestimmt werden. Das Ergebnis sind im besten Sinne vernetzte Maßnahmen, die unter anderem auch vorhandene technische Lösungen einbinden und verfügbare Ressourcen berücksichtigen.

Jede Firma muss sich genau die Informationssicherheits-Kommunikation schaffen, die sie braucht. Bei der Planung ihrer individuellen Kommunikationsmaßnahmen sollten Unternehmen idealerweise auf Fachwissen aus beiden Bereichen, Kommunikation und Informationssicherheit, zurückgreifen. Das hilft, Awareness und Aufmerksamkeit genau dort zu erzeugen, wo Informationssicherheit gelebt werden muss. Und das hilft auch, Information genau zu steuern, eventuell negative Folgen zu vermeiden und im Endeffekt die Wettbewerbsfähigkeit und die wirtschaftliche Zukunft des Unternehmens langfristig zu sichern. Durch eine vertrauensvolle, selbstbewusste und wehrhafte Sicherheitskultur.

Weitere Informationen:

Eine Auflistung konkreter Kommunikationsmöglichkeiten bietet die kostenfreie Broschüre „Wer vergreift sich an Ihrem Know-how?“:

http://www.karg-und-petersen.de/know-how-schutz

[1] Bundesamt für Verfassungsschutz, zitiert nach: Mangelnder Know-How Schutz verursacht hohe Schäden. Verband Deutscher Maschinen- und Anlagenbau (VDMA), 2013; Studie Industriespionage. Aktuelle Risiken für die deutsche Wirtschaft durch Cyberwar. Corporate Trust, 2012.

[2] Mit Sicherheit Erfolgreich. Erfolgsfaktor Know-how-Schutz. Hrsg. vom Sicherheitsforum Baden-Württemberg, 2005.

[3] Status quo des Know-how-Schutzes im Maschinen- und Anlagenbau. DIN e.V., 2013.

[4] Datenklau: neue Herausforderungen für deutsche Unternehmen. Ernst & Young, 2011.

[5] Consumer Password Worst Practices. The Imperva Application Defense Center, Imperva White Paper, 2010.

[6] “Innentäter”, ein unterschätztes Risiko für Unternehmen. In: Wirtschaftsschutz. Prävention durch Information, Ausgabe 1/2012. Hrsg. vom Bundesamt für Verfassungsschutz, 2012.

[7] So beispielsweise: SiFo-Studie 2009/10: Know-how-Schutz in Baden-Württemberg. Hrsg. vom Sicherheitsforum Baden-Württemberg, 2010. Studie Industriespionage. Aktuelle Risiken für die deutsche Wirtschaft durch Cyberwar. Corporate Trust, 2012.

[8] Behavioral Risk Indicators of Malicious Insider Theft of Intellectual Property: Misreading the Writing on the Wall. Shaw, Eric/Stock, Harley, Symantec White Paper, 2011.

[9] Maximising the Effectiveness of Information Security Awareness. Stewart, Geordie/Austen, John, Royal Holloway Series/ Royal Holloway University of London, 2009.

Über Karg und Petersen

Die Karg und Petersen Agentur für Kommunikation GmbH in Tübingen hat sich mit einem eigenen Fachteam unter anderem auf Kommunikation für Unternehmenssicherheit spezialisiert. Karg und Petersen berät Firmen verschiedenster Branchen zu Sicherheitsthemen und unterstützt nationale und internationale Kunden seit vielen Jahren mit Kommunikationsdienstleistungen gegen Wirtschaftskriminalität. Die inhabergeführte Agentur wurde in einer unabhängigen Qualitätsstudie der Universität München als eine der Top-Ten-Agenturen Deutschlands eingestuft.
Mehr Informationen sind verfügbar unter *www.karg-und-petersen.de*.

Karg und Petersen Agentur für Kommunikation GmbH
Dorfackerstraße 26 | 72074 Tübingen | Deutschland

Telefon: +49 7071 98988-0 | Fax: +49 7071 98988-10
Know-how-schutz@karg-und-petersen.de | www.karg-und-petersen.de/know-how-schutz