Illustrationen: Carla Schnettler

Sicherheit in der Wirtschaft

Spione, Fälscher, Diebe – Firma in Gefahr

Sie kommen via Internet, sitzen bereits im Unternehmen oder agieren aus dem Ausland – die Täter, die es auf Unternehmen abgesehen haben, sind so unterschiedlich wie ihre Methoden.

Es war am Aschermittwoch 2016, als die Computer in der Radiologie des Lukaskrankenhauses in Neuss nur noch schleppend liefen. Die Mitarbeiter informierten sofort die IT-Abteilung. In der Zwischenzeit ging auch in der Notaufnahme technisch nicht mehr viel. Den Computerprofis der Klinik war schnell klar: Hier ist etwas Größeres im Gange. Das System war von einer Schad-Software befallen – ein besonders aggressiver Virus. Die Geschäftsführung berief umgehend den Krisenstab ein. Alle Systeme wurden heruntergefahren, um die Patientendaten zu schützen und zu verhindern, dass sich der Virus immer weiter durch das System frisst. Einziger Hinweis auf die Täter war eine Erpressermeldung in schlechtem Englisch. Wenn das Lukaskrankenhaus seine Daten zurückhaben wolle, solle man sich an eine bestimmte E-Mail-Adresse wenden.

Das Krankenhaus sah sich plötzlich in die Vergangenheit versetzt. Alle Abläufe mussten ohne Computer über die Bühne gebracht werden – und das tagelang. Was das für ein Krankenhaus bedeutet, wird einem erst klar, wenn Sprecherin Ulla Dahmen von damals berichtet: „Nur um ein paar Beispiele zu nennen: Eigentlich liefert unser Labor rund 700 Befunde pro Tag, die elektronisch auf die einzelnen Stationen verteilt werden. Plötzlich konnten nur noch 150 erstellt und manuell verteilt werden. Die Patientenaufnahme funktionierte nur noch mit Papier und Bleistift, die Abrechnung mit den Kassen war unmöglich, ebenso die Medikamentenbestellung." Während die Mitarbeiter versuchten, irgendwie den Betrieb am Laufen zu halten, waren neben anderen auch die Spezialisten des LKA Kompetenzzentrums Cybercrime mit der Lösung beschäftigt. Schließlich kamen sie der Schad-Software auf die Spur, und ein passendes Antivirenprogramm konnte geschrieben werden. Das Krankenhaus nutzte das Abschalten der Systeme als Chance und strukturierte vor dem priorisierten Hochfahren der Systeme die gesamte Netzwerk- und Sicherheitstechnologie neu.

Cyber-Angriffe auf Unternehmen sind mittlerweile an der Tagesordnung. Die Hacker richten dabei einen enormen Schaden an. Der Digitalverband Bitkom spricht laut einer Studie von rund 55 Mrd. Euro pro Jahr. Die TÜV Informationstechnik (TÜViT) hält zudem nur drei Prozent der Unternehmen für ausreichend geschützt. Die Fahndung nach den Tätern ist schwierig. Die Hacker, die das Lukaskrankenhaus lahmgelegt haben, wurden bis heute nicht gefasst, die Suche läuft noch. Für 2016 hat das LKA etwa 80.000 Delikte rund um das Thema Internet erfasst, 22.708 waren Hacker-Angriffe.

Ransomware derzeit besonders beliebt

Beliebte Maschen sind momentan der CEO-Fraud und die Infizierung des Systems mit Ransomware. Bei der Ransomware handelt es sich um eine klassische Erpressung, wie sie auch das Lukaskrankenhaus getroffen hat. Der Virus erreicht das System per Mail. Klickt der Nutzer den Anhang an, wird das System konterminiert, und alle Daten werden verschlüsselt. Wer seine Daten zurückhaben will, muss zahlen. Die Hacker sprechen hier die breite Masse an und schicken den Virus an zahlreiche Empfänger. Beim CEO-Fraud hingegen gehen die Täter gezielt vor. Hier werden E-Mail und Absender gefälscht. Nur beim genauen Hinsehen erkennt man die kleinen Änderungen. So schaffen es die Hacker, sich beispielsweise als Geschäftsführer des Unternehmens auszugeben und eine Zahlungsaufforderung an die Buchhaltung zu senden. Auf diesem Weg hat der Automobilzulieferer Leoni rund 40 Mio. Euro verloren.

Bleibt die Frage, wie sich Unternehmen am besten schützen können. Betrachtet man die technische Seite, besteht noch bei zahlreichen Unternehmen Handlungsbedarf, sagt nicht nur der TÜV. Auch Tim Berghoff von der G Data Software AG spricht aus Erfahrung. Das Unternehmen unterstützt Firmen bei der Sicherung ihres Netzwerks. „Prävention und Planung sind bei der Netzwerksicherheit einfach alles. Die ist jedoch in den meisten Firmen nichts, mit dem sich Geld verdienen lässt - somit läuft die Netzwerksicherheit Gefahr, zu einem reinen Kostenfaktor zu verkommen", sagt der Profi. „Sicherheitsexperten sind hier oft von vornherein in der Defensive, da sich potenzielle Schäden nur schwer beziffern und somit auch nur schwer als Argument anbringen lassen." Neben einem spezifisch angepassten Schutz vor schädlicher Software und einer Netzwerküberwachung muss auch eine Web-Inhaltskontrolle erfolgen.

Dennoch: „Die rein technische Komponente kann keinen 100-prozentigen Schutz bieten", sagt Peter Vahrenhorst vom LKA. Die menschliche Komponente spielt eine immense Rolle. Neben der Software sollten die Unternehmen in die Mitarbeitersensibilisierung investieren und diese immer wieder auffrischen. Wichtige Passwörter unter die Schreibtischunterlage kleben und nie ändern oder mal eben mit dem Firmenhandy im WLAN an der nächsten Ecke surfen – über die Gefahren machen sich Mitarbeiter oft keine Gedanken. „Die Unternehmen sollten ihre Mitarbeiter nicht kontrollieren, aber sensibilisieren", rät Tanja Neumann von der IHK. Und das LKA empfiehlt, im ersten Schritt alle ankommenden E-Mails auf die richtige Schreibweise der Adressen zu prüfen. Die Rechner sollten immer auf dem aktuellsten Systemstand sein. Anhänge dürfen niemals einfach geöffnet werden. Und: Im Zweifel lieber einmal mehr die IT-Abteilung fragen. „Mit wenigen Schritten decke ich so viele Eventualitäten ab, wenn auch nicht alle", sagt Vahrenhorst.

Das LKA beobachtet aber, dass es mittlerweile zum gesellschaftlichen Phänomen geworden

PARTNER DER UNTERNEHMEN: DIE IHK HILFT

Fülle von Informationen
Die IHK Mittlerer Niederrhein bietet Beratungen und eine Fülle von Informationen zum Thema IT-Sicherheit an. Auf der IHK-Internetseite ist eine umfangreiche Übersicht über Anlaufstellen, Verlinkungen zu Leitfäden, Broschüren sowie zu Online-Analysen und Website-Checks zu finden.

Tanja Neumann
Tel. 02151 635-310
E-Mail: neumann@krefeld.ihk.de
www.mittlerer-niederrhein.ihk.de/12336

Neues Seminar: „Mitarbeiter sensibilisieren für die digitale Sicherheit"
Nur, wenn alle Mitarbeiter für relevante Gefährdungen sensibilisiert sind, können Unternehmensdaten geschützt werden. Ein neues IHK-Seminar vermittelt Kenntnisse und Kompetenzen für sicherheitsbewusstes Verhalten. Auf dem Programm: „Grundlagen der IT-Sicherheit", „Sensibilisierung für Risiken und Bedrohungen", „Wie Sie das Ausspähen von Informationen vermeiden", „Sicherer Umgang mit E-Mails", „Passwort-Regeln", „Sicherheit für mobile Geräte" und „Sicher im Internet". Der erste Kurs beginnt am 30. November (jeweils donnerstags, 9 bis 16.30 Uhr, IHK in Krefeld). Der zweite Kurs startet am 11. April 2018 (jeweils mittwochs, 9 bis 16.30 Uhr, IHK in Neuss). Das Entgelt für acht Unterrichtseinheiten beträgt 240 Euro.

Tel. 02151 635-455
E-Mail: bildung@krefeld.ihk.de
www.wb-ihk.de/F041-SK117
www.wb-ihk.de/F041-SN118

IT-Sicherheitstag NRW am 5. Dezember
Mit Impulsvorträgen, Experten- und Basic-Foren, Seminaren und einer Fachausstellung bietet der IT-Sicherheitstag am 5. Dezember im Colosseum Theater in Essen für Unternehmen wertvolle Informationen zu den Themen Daten-, Informations- und IT-Sicherheit sowie konkrete Hilfestellung beim Aufbau eines Netzwerks. Der Fachkongress wird von den Industrie- und Handelskammern in Nordrhein-Westfalen (IHK NRW) organisiert. Er richtet sich speziell an kleine und mittelständische Unternehmen.

Tanja Neumann
Tel. 02151 635-310
E-Mail: neumann@krefeld.ihk.de
www.it-sicherheitstag-nrw.de

Beratung durch Patentanwälte: Schutz vor Ideenklau und Plagiaten
Gewerbliche Schutzrechte können vor Ideenklau und Plagiaten schützen. Um Unternehmern eine erste Hilfestellung bei Fragen zu gewerblichen Schutzrechten (zum Beispiel zu Patenten, Gebrauchsmustern und Marken) zu ermöglichen, bietet die Industrie- und Handelskammer Mittlerer Niederrhein monatlich eine kostenfreie Erstberatung durch Patentanwälte aus der Region an. Die kommenden Termine: 12. Oktober, 16. November und 14. Dezember (jeweils 16 bis 18 Uhr).

Kathrin Kloppenburg
Tel. 02131 9268-572
E-Mail: kloppenburg@neuss.ihk.de
www.mittlerer-niederrhein.ihk.de/6557

ist, dass wir Techniken nutzen, ohne uns Gedanken über die möglichen Folgen zu machen. Kleines Beispiel des Kriminalbeamten: Im Konferenzraum eines mittelständischen Unternehmens aus Krefeld hängt ein Internet-TV aus Südkorea. Das Gerät wird nicht über eine Fernbedienung, sondern per Sprachbefehle gesteuert. Leider liest niemand in der Firma die AGB bis zur Seite 352 durch, auf der steht: „Bitte nicht so viel Sprechen beim TV gucken." Alle Aufnahmen werden nämlich nach Südkorea gesendet, um zu entschlüsseln, ob es sich um einen Befehl für das Gerät handelt. „In dem Moment habe ich im Wohnzimmer oder eben im Konferenzraum ein 24-Stunden-Überwachungsgerät stehen", sagt Vahrenhorst. Gleiches gilt für viele weitere Geräte mit Sprachsteuerung.

Mittlerweile beschäftigt sich auch die Hochschule Niederrhein mit dem Thema. Dort wurde im Juni das Kompetenzzentrum für Informationssicherheit Clavis eröffnet. Das strategische Ziel von Clavis, um insbesondere die Partner in der Region zu unterstützen, lautet: Anwendungsorientierte Forschung zur Sicherstellung und Erhöhung der Informationssicherheit von Organisationen in der Region Mittlerer Niederrhein. Das Kompetenzzentrum versteht sich dabei als ein regionales Bindeglied zwischen der Industrie, weiteren Forschern und der Lehre. Der lateinische Begriff „Clavis" bedeutet „Schlüssel" und beinhaltet damit einerseits das Thema der Sicherheit von Informationen durch Verschlüsselung und symbolisiert andererseits den Zugang der regionalen Industrie zur Hochschule Niederrhein. „Die Digitalisierung der Gesellschaft kann nur funktionieren, wenn wir dabei auch an die Informationssicherheit denken", sagt Dr.-Ing. René Treibert, Professor für Wirtschaftsinformatik und Leiter des neuen Kompetenzzentrums.

Informationssicherheit für kritische Infrastrukturen

Forschungsschwerpunkt des Kompetenzzentrums, das mit Experten aus drei Fachbereichen besetzt ist, ist die Informationssicherheit für die sogenannten kritischen Infrastrukturen. Dies sind Bereiche des öffentlichen Lebens, die für die Gesellschaft von elementarer Bedeutung sind. Dazu gehören etwa Gesundheit, Energie, Transport und Verkehr.

Laut des IT-Sicherheitsgesetzes von 2015 müssen Unternehmen aus diesen Bereichen ein Managementsystem für Informationssicherheit vorweisen. Mit dem Gesetz will die Bundesregierung erreichen, dass die IT-Systeme und digitalen Infrastrukturen Deutschlands zu den sichersten weltweit werden. Auch klein- und mittelständische Unternehmen sind betroffen, sagt Tanja Neumann von der IHK, die sich von dem Gesetz langfristig einiges für die Sicherheit verspricht: „Die gesamte Wertschöpfungskette muss für die sogenannten kritischen Infrastrukturen sicher sein. Damit sind auch die Zulieferer davon betroffen." Clavis versteht sich auf diesem Gebiet als praxisorientierter Forschungspartner der regionalen Industrie und bietet Organisationen entsprechende Konzepte und Kurse im Weiterbildungsprogramm an.

Nicht immer kommen die Angreifer aus dem Netz

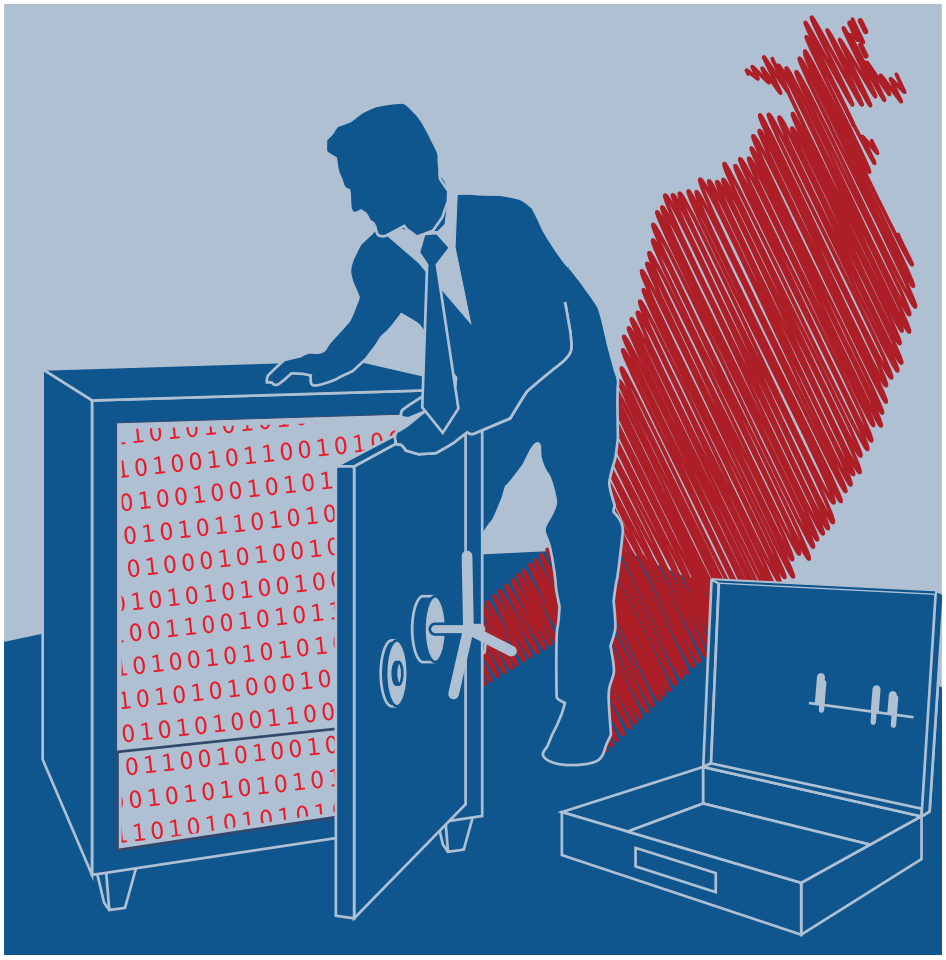
Gefahren gehen nach wie vor auch von klassischen Vergehen wie Einbruch aus. Seit rund 20 Jahren beschäftigt man sich bei Protection One in Meerbusch mit diesem Thema. Mit einer komplett neuen Sicherheitsphilosophie ist das Unternehmen damals als Vorreiter auf den Markt gegangen und bis heute erfolgreich. „Herkömmlich sichern Unternehmen und teilweise auch Privatleute ihre Räumlichkeiten mit Alarmanlagen, teilweise auch verbunden mit einer Wach- und Schließgesellschaft. Wenn Ein-

brecher aber irgendwo rein wollen, kommen sie auch rein", erklärt Geschäftsführer Martell Schilling. Protection One bietet eine 24-Stunden-Fernüberwachung mit Live-Täteransprache. Ist der Einbrecher im Gebäude, geht in Meerbusch der Alarm los. Per Hör-, Sprech- und Sehverbindung schalten sich die Mitarbeiter der Notruf-Serviceleitstelle in die Räume ihres Kunden und sprechen den Einbrecher aktiv an. Gleichzeitig geht eine individuell mit dem Kunden vereinbarte Interventionskette los. „Die Einbrecher werden lautstark aufgefordert, das Gebäude sofort zu verlassen. Das Ergebnis ist durchschlagend. Der Überraschungseffekt ist so groß, dass die Täter in der Regel sofort die Flucht ergreifen. So wird weiterer Schaden abgewendet", sagt Schilling. Durch die detaillierte Beschreibung, die Protection One der Polizei übermitteln kann, kommt es nicht selten vor, dass die Einbrecher der Polizei auf ihrer Flucht regelrecht in die Arme laufen. Das alles passiert in einer durchschnittlichen Interventionszeit von 30 Sekunden. Das Unternehmen hat eine unabhängig auditierte Schadensvermeidungsquote von 96 Prozent.

„Es geht weniger darum, materielle Dinge zu stehlen. Auch ein Unternehmen hat einen emotionalen, ideellen Wert", berichtet Schilling. „Der psychische Schaden nach einem Einbruch ist groß. Die Mitarbeiter sind verunsichert, es wird viel geredet, viel spekuliert. Das kann den Firmenablauf massiv stören und so einen großen finanziellen Schaden anrichten." Laut Kriminalstatistik 2016 gab es rund zwei Mio. Fälle von Diebstahlkriminalität in Deutschland. Die Aufklärungsquote liegt nur bei 20 Prozent.

Jährlicher Schaden: Rund 100 Mrd. Euro

36 Prozent – sprich mehr als jedes Dritte - aller deutschen Unternehmen haben laut einer Studie des Wirtschaftsprüfers KPMG mit wirtschaftskriminellen Handlungen zu tun gehabt. Die Studie ist aus dem Jahr 2016 und bezieht sich auf einen Befragungszeitraum der vorangegangenen zwei Jahre. Die Prüfer gehen von einem jährlichen Schaden von rund 100 Mrd. Euro aus. 45 Prozent der Delikte sind Betrug und Untreue. „Dabei zeigt sich – wie auch in den Studien der vorherigen Jahre – weiterhin ein verblüffendes Detail in der Risikoeinschätzung der Unternehmen. So sehen 80 Prozent aller Befragten ein hohes beziehungsweise sehr hohes Risiko für deutsche Unternehmen, Opfer von Wirtschaftskriminalität zu werden.



Das Risiko für das eigene Unternehmen hingegen sehen lediglich 32 Prozent der Befragten", heißt es in der Studie. Doch was ist, wenn der Feind schon in den eigenen Reihen unterwegs ist? Jörn Weber ist Privatermittler, spezialisiert auf jegliche Form von Wirtschaftskriminalität – sei es im Internet oder in der realen Welt (s. auch Interview, S. 18). Der ehemalige Polizist und sein Team der corma GmbH aus Brüggen werden von Unternehmen beauftragt, sowohl vorab als Sicherheitsberater als auch nach einem Vorfall, um die Täter zu ermitteln.

Auch er weiß: „Aktuelle oder ehemalige Mitarbeiter nutzen besonders häufig das Vertrauen des Arbeitgebers aus." Ein Beispiel aus seinem Berufsalltag: Mitarbeiter eines Technikunternehmens haben auf Ebay Ersatzteile entdeckt, die einwandfrei als Firmeneigentum identifiziert werden konnten. Verkäufer war ein Kollege. Diebstahl kommt in deutschen Unternehmen häufig vor. Die Geschäftsführung sollte aber einen kühlen Kopf bewahren. In diesem Fall wurde der Mitarbeiter in einem Impuls direkt zur Rede gestellt. Der erste Fehler. Im Anschluss durfte er zurück an seinen Arbeitsplatz. Der zweite Fehler. „Man sollte erst sauber ermitteln und dann Konsequenzen ziehen", so der Ermittler. Hier war der Diebstahl eindeutig. Das ist nicht immer der Fall. Was passiert beispielsweise mit Dingen, die das Unternehmen nicht mehr braucht und entsorgt? „Das muss die Geschäftsführung individuell festlegen. Wichtig ist in allen Fällen, klare Regeln aufzustellen und diese auch zu kommunizieren", so Weber.

Der Ermittler rät auch, gerade bei Neubesetzungen die Kandidaten genau unter die Lupe

>> Die Digitalisierung der Gesellschaft kann nur funktionieren, wenn wir dabei auch an die Informationssicherheit denken. <<
Dr.-Ing. René Treibert, Leiter des Kompetenzzentrums Clavis, Hochschule Niederrhein

zu nehmen – je höher der Posten, desto gründlicher sollte geschaut werden. Denn, so banal es klingt, es gibt ihn, den Bewerber aus einem asiatischen Land, der eingeschleust wird, um die neusten Entwicklungen im Pharmaunternehmen ins Ausland zu transferieren. Oder den Abteilungsleiter, der durch hervorragende Zeugnisse an seine Stelle gekommen ist, nun aber ganz und gar nicht die erwartete Leistung bringt, weil seine Unterlagen alle gefälscht waren.

Bei corma hat man täglich mit solchen Betrügereien zu tun. Schon nach kleinen Recherchen ist Weber und seinem Team meist schnell klar, dass im Lebenslauf etwas nicht stimmt. „Zum Beispiel hat einmal ein Mitarbeiter im Lebenslauf angegeben, er hätte bei der Telekom gearbeitet. Zum fraglichen Zeitpunkt hieß das Unternehmen aber noch Post. So sind wir ihm dann auf die Schliche gekommen", erklärt er.

Weber nimmt auch ganze Unternehmen unter die Lupe. Zum Beispiel, wenn größere Investitionen oder Übernahmen anstehen. So können vorab größere Schäden abgewendet werden, wie einst in Sachen Nürburgring. „Hätte man uns vorher mit einem Hintergrundcheck beauftragt, hätten wir dieses Desaster vermeiden können", sagt Weber. 2009 sollte das Gelände um einen Freizeitpark erweitert werden. Um die 300 Mio. Euro für das Projekt zusammenzubekommen, sollten private Investoren gefunden werden. Der angebliche Finanzvermittler stellte sich jedoch als Betrüger heraus, der nach Abkassieren der Vermittlungssumme weg war. Peinlich für alle Beteiligten.

Alles, was erfolgreich ist, wird gerne gefälscht

Wenn Marcus Hardelauf auf Fachmessen für Textilmaschinen unterwegs ist, kommt es nicht selten vor, dass er Geräte sieht, die zwar aussehen wie die seines Arbeitgebers Textechno, es aber nicht sind. Die Plagiate sind in der Regel mit minderwertiger Qualität produziert und stammen meistens aus China. Das Unternehmen mit Sitz in Mönchengladbach ist seit vielen Jahren weltweit einer der führenden Hersteller von Präzisionsprüfgeräten für die Textil- und Chemiefaserindustrie. „Viele unserer Geräte sind Standards in der Qualitätssicherung der Textilindustrie. Der Einsatz von Plagiaten kann hier zu deutlichen Qualitätsmängeln im Endprodukt führen", sagt der Verkaufsleiter. „Seit mehr als 20 Jahren ist Produktpiraterie für uns ein großes Thema."

Allein der Schaden, der durch gefälschte Produkte entsteht, die ins Land geschmuggelt werden, ist enorm. Im vergangenen Jahr hat der Zoll 41 Mio. gefälschte Produkte an den Außengrenzen sichergestellt. Sie hatten einen Wert von fast 673 Mio. Euro. Zehn Prozent der Deutschen haben laut einer Studie Fälschungen zu Hause, ohne es zu wissen.

„Die Plagiate werden immer perfekter und professioneller hergestellt", heißt es vom Aktionskreis gegen Produkt- und Markenpiraterie (APM). Die betroffenen Unternehmen müssen mit Umsatzverlusten rechnen und für die mögliche Rechtsverfolgung zahlen. Das geht bis hin zum Arbeitsplatzverlust. Der APM geht davon aus, dass allein im Bekleidungssektor durch Produkt- und Markenpiraterie 3.500 Stellen abgebaut wurden.

„Für die Fälscher ist grundsätzlich jedes Produkt interessant, das erfolgreich ist", sagt Peter Gretenkord vom Verband. Richtig schützen kann sich dabei niemand. Allerdings kann man es den Fälschern so schwer wie möglich machen. Sind Fälschungen auf dem Markt, muss das Unternehmen versuchen, die Einfuhr zu stoppen, indem eine Anfrage beim Zoll gestellt wird. Privatermittler Jörn Weber ermittelte erst neulich in einem Fall, in dem die Täter versucht hatten, 45 Paletten gefälschte Adapter auf den deutschen Markt zu bringen. Hier konnte er jedoch noch eingreifen und den enormen wirtschaftlichen Schaden für seinen Mandanten verhindern.

Hat er dann die Fälschung in der Hand, verfolgt er zurück, wo die Ware produziert wird. Dabei geht es ihm nicht um den kleinen Zwischenhändler hier in Deutschland. Er will an den Hauptproduzenten, denn nur so kann die Produktion langfristig gestoppt werden. Wer sich nicht sicher ist, was er gegen Patentfälscher machen kann, für den hat Elke Hohmann von der IHK einen Tipp: „Wir bieten monatlich eine Erfinder- und Patentberatung durch Patentanwälte an, die beim Schutz von geistigen Eigentum hilft." *Nina Mützelburg*