Interview

mit Dipl.-Ing. Günter Holzhauser, Experte für Wirtschaftsschutz und Spionageabwehr

Wie überrascht man doch war, als uns die Aktionen der NSA durch die Veröffentlichungen von Edward Snowden bekannt wurden. Dabei handelt es sich hier nur um eine Sparte der „Spionage" und noch nicht einmal um die wichtigste. Günter Holzhauser beschäftigt sich seit über 20 Jahren mit der Materie. Im Gespräch mit Chefredakteur Rudolf K. Schiwon erklärt er die gesamte „Branche", so dass man aus dem Staunen nicht mehr herauskommt und am Ende die Frage bleibt: Wie kann man sich gegen diesen „Lindwurm" schützen?

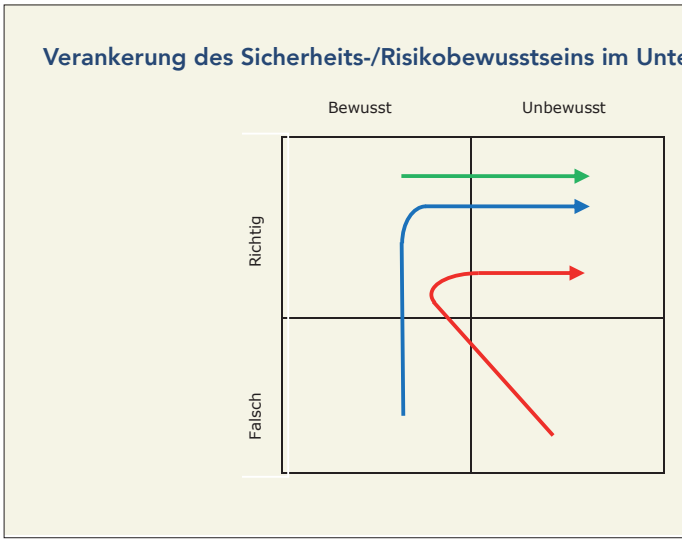
cpm: Herr Holzhauser, Sie gelten als ausgewiesener Fachmann für eine Materie, die einem eigentlich sehr geläufig sein sollte, die es dann aber letztlich nicht ist: Wirtschaftsschutz. Was verbirgt sich hinter der Begrifflichkeit?
Holzhauser: Die Bundesinitiative „Wirtschaftsschutz" wurde offiziell am 28. August 2014 gestartet. Das Bundesministerium des Innern, die Bundesvereinigung der Deutschen Industrie (BDI) und der Deutsche Industrie- und Handelskammertag (DIHK) haben gemeinsam die Absicht bekundet, zukünftig den Schutz unserer Wirtschaft in der Fläche zu konzipieren. Für die Ausgestaltung dieses Vorhabens wurde die „Die Nationale Wirtschaftsschutzstrategie" auf den Weg gebracht. Sie wird gerade unter Beteiligung der deutschen Wirtschaft in verschiedenen Arbeitsgruppen ausgestaltet. Was verstehen wir darunter? Ich zitiere das BDI-Positionspapier: „Wirtschaftsschutz ist die Summe aller Maßnahmen von Politik, Behörden und Wirtschaft zur Minimierung von Risiken bei der Unternehmenssicherheit".

cpm: Was wird unter dem Begriff Risiken subsummiert?
Holzhauser: Welche Bedrohungen und Risiken sich im Einzelnen in der Ausgestaltung zeigen, muss erst einmal abgewartet werden. In Rahmen meiner operativen Arbeit habe ich mit einer Sicherheitsbehörde Ende des vergangenen Jahres mögliche Kategorien gebildet, die auf höherer Abstraktionsebene zu dem Wirtschaftsschutz gezählt werden könnten. Die Bedrohungslandschaft ist sehr komplex und heterogen, je nach Auge des Betrachters kann sie unterschiedlich kategorisiert werden. Wir hatten im Dezember des vergangenen Jahres Wirtschaftsspionage (durch fremde Geheimdienste), Industrie- und Wettbewerbsspionage, Sabotage, Organisierte Kriminalität, kriminelle Einzeltäter, Linksextremismus, Terrorismus und Unglücke/Katastrophen dem Wirtschaftsschutz zugeordnet.

cpm: Sie nannten eben Wirtschaftsspionage durch fremde Geheimdienste. Wie haben wir uns das vorzustellen?
Holzhauser: Deutschlands Wirtschaft und Wissenschaft steht an der Spitze der Aufklärungsziele durch fremde Nachrichtendienste. Wirtschaftsspionage ist die nationalstaatlich gelenkte Spionage durch fremde Geheimdienste. Sie beschaffen sich mit illegalen Mitteln Informationen und Know-how, das sie zum Aufbau eigener Industrien brauchen oder ihren eigenen Unternehmen im immer stärker werdenden Wettbewerb zur Verfügung stellen. Je nach Land gibt es unterschiedliche Motive und Interessen im Kontext der Wirtschaftsspionage. Das, was im eigenen Land an Know-how nicht vorhanden ist, nicht entwickelt oder gekauft werden kann, wird oft mit den Mitteln der Spionage beschafft. Die Methoden, mit denen fremde Nachrichtendienste Organisationen und Unternehmen angreifen, sind vielfältig. In Zeiten von Snowden hören und lesen wir sehr viel von SIGINT – Signals Intelligence – also der Aufklärung von Kommunikation und IT. Im Kontext der professionellen Spionage ist aber der Mensch das größte Thema. Cyber und IT ist eine Facette, es ist aber nicht *die* Facette. Ich möchte betonen, dass ich hier von professioneller Spionage und nicht von der Kriminalität rede. Das ist zu trennen. Die deutsche Wirtschaft unterschätzt diesen Sachverhalt massiv. Spionage sucht sich den Weg des geringsten Widerstandes, der geringste Widerstand ist nicht die IT!

„Deutschlands Wirtschaft und Wissenschaft steht an der Spitze der Aufklärungsziele durch fremde Nachrichtendienste."

Foto: cpm



cpm: Der ebenfalls genannte Bereich Industrie- und Wettbewerbsspionage klingt sehr professionell. Wie haben wir uns das vorzustellen?

Holzhauser: Im Grundsatz verstehen wir hier die Spionage durch Unternehmen, die im Wettbewerb stehen. Hier arbeiten ausländische Unternehmen auch oft mit ihren Geheimdiensten zusammen. Unternehmen heuern sich oft Ex-Nachrichtendienstler an, die die dreckige Arbeit machen. Solche „Dienstleister" finden sie in Anzeigen von Zeitungen oder auch im Internet. Die Methoden der Industrie- und Wettbewerbsspionage sind denen der Wirtschaftsspionage ähnlich, sie sind in der Regel auch professionell. Industrie- und Wettbewerbsspionage muss nicht zwangsläufig von einem konkurrierenden Unternehmen ausgehen, oft ist es ausreichend, einfach nur erfolgreich als Unternehmen zu sein. Dieser Fakt alleine kann den Impuls auslösen, das Wirtschaftsmodell eines Unternehmens kopieren zu wollen und Spionageaktivitäten zu starten. Sie sehen, das Thema Industrie- und Wettbewerbsspionage hat auch viele Facetten.

„Cyber und IT ist eine Facette, es ist aber nicht *die* Facette".

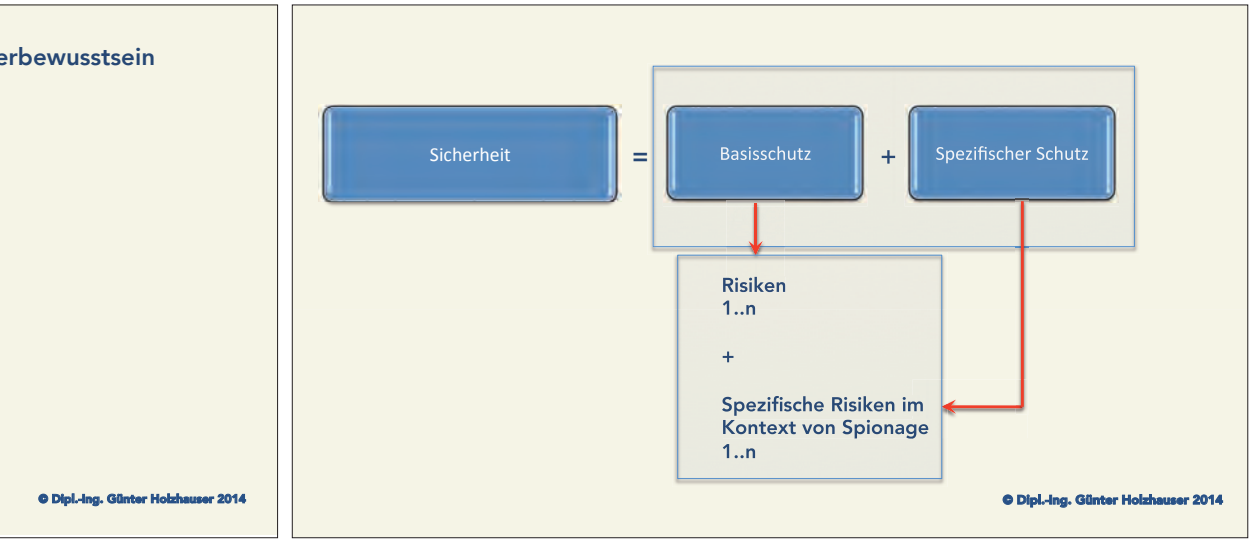
cpm: Linksextremismus zählen Sie zum Wirtschaftsschutz. Die Wirtschaft muss sich vor dem Linksextremismus schützen? Warum das?

Holzhauser: Wenn wir über den Schutz der Wirtschaft reden, dann müssen wir wirklich auch den Linksextremismus dazu zählen. Einer der Schwerpunkte des Linksextremismus ist der zunehmend gewaltbereite Schwerpunkt des „Antimilitarismus". Die Bundeswehr, die Verteidigungswirtschaft aber auch rein zivile Lieferanten der Bundeswehr sind Ziel von Anschlägen mit teilweise erheblichen Sachschäden. „Kriegstreiberei" und „Profit mit dem Krieg" sind dann die Erklärungen der Täter. Der „Antimilitarismus" formiert richtige Kampagnen zur Durchsetzung seiner Ziele mit Gewalt. 2011 gab es die Kampagne „Krieg beginnt hier" mit der Losung „Kriegstreiberei und Militarisierung markieren, blockieren, sabotieren!" In dem Kontext kam es zu Anschlägen gegen verschiedene Bundeswehreinrichtungen und Unternehmen der Verteidigungswirtschaft. Um den Bogen jetzt zu Ihrer Frage zu spannen, sobald ein Unternehmen als Lieferant der Bundeswehr in Erscheinung tritt, kann es Zielobjekt linksextremistischer Gewalt werden. Vereine der Verteidigungsindustrie und ein Fachverlag – also Ihre Kollegen – waren in der Vergangenheit auch schon Opfer von Anschlägen.

cpm: Wenn Sie den gesamten aufgeführten Komplex betrachten: Wie bewerten Sie die derzeitige Lage und welche Trends zeichnen sich für die Zukunft ab?

Holzhauser: Im Kontext von professioneller Wirtschaftsspionage wird für mich das Thema Cyber und IT zu sehr in den

Dipl.-Ing. Günter Holzhauser,
Jahrgang 1965, arbeitet branchenunabhängig im Bereich Wirtschaftsschutz und Spionageabwehr. Er verfügt über Hochschulausbildungen im Bereich Maschinenbau, Security Management und Wirtschaftsschutz (Spionageabwehr). Aktuell Promotion an der Universität der Bundeswehr. H. hat 24 Jahre Branchenerfahrung national und international für Wirtschaft, Regierungsorganisationen, Spezialkräfte und Dienste. Seine Dienstleistungen für Wirtschaft und Organisationen liegen unter anderem im Kontext der Spionageabwehr in den Bereichen Bedrohungs- und Risikoanalysen, Umfeldanalysen und Lagebilder für die relevanten Einzelbedrohungen. Schwerpunkt ist der Informationsschutz. Weitere Felder: Spionageabwehr, Sicherheitsstrategien, -konzepte und -maßnahmen, Schulungen und Security im Organisationsprozess.



Grafiken: Holzhauser

Vordergrund gestellt. Die Sicht für die klassischen und analogen Bedrohungen fehlt oft oder möchte nicht gesehen werden. Mit IT und Dienstleistungen für die IT lässt sich sehr viel Geld verdienen, weltweit reden wir hier über Mega-Märkte der Zukunft. Eine Schweizer Studie hat herausgefunden, dass ca. 90% der Investitionen in einem Unternehmen in die IT gesteckt werden. Im breiten Spektrum der Bedrohungen und dem wichtigen Thema Informationsschutz im Unternehmen oder Organisationen hilft dieses Investment wohl kaum. In meinem operativen Tagesgeschäft mache ich sehr oft die Erfahrung, dass die Unternehmen fälschlicherweise Datensicherheit mit Informationssicherheit gleichsetzen. Gesamtheitliche Informationssicherheit bezieht sich immer auf das gesamte Unternehmen und das Business. Hier gilt es immer, das Unternehmen auch außerhalb der territorialen Grenzen und im Umfeld seines Wirkens zu betrachten. Dort finden die meisten Angriffe auf das Know-how von Unternehmen statt.

Ich persönlich glaube, dass die Bedrohungen und Risiken in der Zukunft zunehmen werden. Gerade im Kontext der zunehmenden digitalen Sozialisation unserer Gesellschaft. Als Beispiel seien hier die Trends Social Business, Industrie 4.0, das vernetzte Auto und das Internet der Dinge genannt. Hier werden wir in Zukunft mit neuen Bedrohungen und Risiken konfrontiert werden. Angriffe auf Zielpersonen werden zum Beispiel im vernetzten Auto oder im vernetzten Eigenheim einfacher durchzuführen sein. Die Bedrohung durch Sabotage wird aus meiner Sicht zunehmen.

cpm: Sie haben insgesamt eine sehr bedrohliche Situation geschildert, die offensichtlich von den Betroffenen so nicht wahrgenommen wird. Was meinen Sie muss geschehen, damit man Sicherheit erfolgreich betreiben kann?

Holzhauser: Das ist eine sehr gute Frage. Vieles hat mit dem Grundproblem „Wahrnehmung“ zu tun. Die Bedrohung beginnt bei uns selbst. Jeder Mensch konstruiert sich seine Wahrnehmung für Sicherheit im Rückspiegel aus der eigenen Sozialisation. Das Gehirn arbeitet nach dem Muster der Wiedererkennung. Wenn sie 20 Menschen fragen, was sie unter Sicherheit verstehen, sagen ihnen 20 Menschen unterschiedliche Dinge. Je nach Sozialisation eines Menschen entsteht aus diesem Konstrukt heraus das subjektive Bild für Sicherheit. Der eine hat eine hohe Sensibilität, der andere eine geringe, wiederum andere keine Sensibilität. In meinem Tagesgeschäft und in Gesprächen mit Organisationen und Unternehmen begegnen

„Die subjektive Einschätzung der eigenen Bedrohung liegt weit weg von der real existierenden Bedrohung für die Organisation.“

mir in der Regel Menschen mit geringer oder fehlender Sensibilität. Leider sind diese Menschen meist in der Führungsebene von Unternehmen oder Organisationen zu finden. Bedrohungen und Risiken werden meist bagatellisiert und weg geredet. Die subjektive Einschätzung der eigenen Bedrohung liegt weit weg von der real existierenden Bedrohung für die Organisation.

Ich hatte vor kurzem ein längeres Gespräch mit der Sicherheitsabteilung eines Großkonzerns, in dem wir einhellig der Meinung waren, dass eine Sensibilisierung und Aufklärung über Bedrohungen und Risiken schon im Grundstudium an Universitäten beginnen müsste. D.h., dass zum Beispiel in den Fachrichtungen Maschinenbau, Elektrotechnik, Betriebswirtschaft, Volkswirtschaftslehre, Politik, usw. Vorlesungen zur Sensibilisierung eingeführt werden müssten. Die Führungskräfte der Zukunft sollten frühzeitig mit diesen Themen konfrontiert werden. Es gibt aktuell viele Studien, die sich mit dem Thema der massiv unterschätzten Wirtschaftsspionage in Unternehmen beschäftigen. Meine persönliche These ist die, dass das Niveau eines Sicherheitskonzeptes im Unternehmen direkt vom Sicherheitsbewusstsein der Unternehmensleitung abhängt. In mittelständischen Betrieben ist die Sicherheit meist von einzelnen Personen abhängig. Bei Geschäftsführern mit geringem Sicherheitsbewusstsein haben Sie in der Regel fragmentierte oder fehlende Sicherheitsstrukturen im Unternehmen, aber auch margen- und liquiditätsschwache Unternehmen vernachlässigen die Sicherheitsstrukturen. Der Straftatbestand der Fahrlässigkeit oder des Vorsatzes durch Unterlassung ist dann schnell erfüllt.

Sicherheit hat für mich in erster Linie mit dem Etablieren eines Sicherheitsbewusstseins zu tun. Das ist für mich die größte Hürde, die es im Kontext von Sicherheit zu nehmen gilt.

cpm: Herr Holzhauser ,
ich danke Ihnen für das Gespräch. ■