Die Wanze in der Kaffeekanne
IHK-Arbeitskreis „Sicherheit in der Wirtschaft“ trifft sich zum Thema Lauschabwehr

Die Methoden sind nicht aus einem James Bond-Film entliehen, sondern tagtägliches Handwerkszeug der Wirtschaftsspionage: Die Abhörwanze, die über das Cateringunternehmen in der Kaffeekanne eingeschleust wird, die Kamera im Miniaturformat in der Kreuzschlitzschraube in der Wandvertäfelung oder auch das Abhören von Meetings über hochmodernste Lasertechnologie an der Glasscheibe des Besprechungsraumes. Viele Lauschangriffe ausländischer Geheimdienste sind sehr einfach, aber trotzdem effektiv und vom Kostenaufwand gering. Kein Wunder, dass bei einer geschätzten Schadenssumme von jährlich ca. 50 Milliarden Euro durch das Abhören durch ausländische Geheimdienste der deutschen Wirtschaft nicht nur ein Renommee-Schaden entsteht.

Beim vergangenen Treffen des IHK-Arbeitskreises „Sicherheit in der Wirtschaft“ ging es genau zu diesem Thema der Schäden durch Wirtschafts- und Industriespionage. Andreas Nees von der Deutschen Telekom AG/Lauschabwehr berichtete im ersten Teil des Zusammentreffens über die technischen Angriffsmöglichkeiten und die Konsequenzen solch eines Informationszugriffs. Nach seinen Ausführungen kommen gut drei Viertel der Täter intern aus dem Haus und werden von Dritten für ihre Tätigkeit direkt angeworben. Auch Kleinunternehmen sind von Interesse; längst sind nicht nur die Großindustrieentwicklungen im Fokus der Geheimdienste. Dabei können Nebeninformationen dann spannend werden, wenn sie im größeren Gesamtzusammenhang bei der Spionage durch weitere Firmen- und Zuliefererdetails zusammengesetzt werden und ein großes Gesamtbild ergeben.
Die Angriffsmöglichkeiten sind dabei groß: Der Heizkörper als Schallverstärker, der Deckenlautsprecher mit Rückkoppelung als Mikrofon und selbst das LAN-Kabel mit eingebauten Mikrofon dienen als Abhörmöglichkeit: Die Kombination von aktiven und passiven Geräten ermöglichen mittlerweile Geheimdiensten, sich für geringes Geld relativ einfach ein komplettes Informationsbild zu verschaffen.

Nees stellte die Möglichkeiten dar, welche Tricks die Ausspähspezialisten mittlerweile aus dem Koffer von James Bond-Filmen auf Lager haben und zeigte zugleich, welche technischen Aufspürmöglichkeiten durch das Team der Lauschabwehr der Telekom eingesetzt werden. Das können das aktive Aufspüren von Sendern mit Hochfrequenzscans sein, ein Leitungs- und Gerätecheck für Anzapfungen und Manipulationen in der Kommunikationsinfrastruktur mit kleinsten Messabweichungen, die aber auch inaktive Wanzen finden. Komplettiert wird das Suchbild durch ein mobiles Röntgensystem, was ermöglicht, technische Geräte zu durchleuchten auf die Einbringung von Komponenten, die, verglichen mit original Röntgenbildern, aufdecken, was nachträglich in das Gerät eingebaut wurde. Die Gesamtbetrachtung der eingesetzten Maßnahmen münden in ein Schutzkonzept, was auch nachträglich und dauerhaft sicherstellten soll, dass der einmal auf potenzielle Lauschangriffe durchgeleuchtete Raum bzw. Gegenstände auch sicher bleiben. Absolute, hundertprozentige Sicherheit, so Nees, sei zwar technisch nahezu zu realisieren, Schwachstelle bleibe jedoch immer noch der Mensch, der auf persönliche Angriffe immer noch sensibilisiert werden müsse und eine ungleich größere und andere Angriffsfläche für Spionage biete, als die Technik.

Wirtschaftsspionage sichert Marktführerschaft
Beim zweiten Teil des Treffens berichtete Ulrich Mayer vom Landesamt für Verfassungsschutz Baden-Württemberg über die derzeitige Bedrohung durch Wirtschaftsspionage durch die USA, Russland und China, die gegenüber weiteren ausspähenden Nationen den größten Aufwand zur Ausspähung von Wirtschaftsinformationen betreiben. Der Verfassungsschutz schätzt dabei die Geheimdienstmitarbeiterzahl in China auf 1 Million. Russland mit 375.000 sowie die USA mit 130.000 direkten und indirekten Mitarbeitenden in der Wirtschaftsspionage und beim Geheimdienst bestechen darüber hinaus mit schierer Größe. Schwierigkeit dabei ist, dass im Schnitt ein dreiviertel Jahr vergeht, bis ein Angriff überhaupt bemerkt wird – im besten Falle.

Dabei wird ein Großteil der Angriffsfälle nicht an die jeweiligen Verfassungsschutzbehörden gemeldet, da aus Angst vor Imageverlust und Kundensensibilität oftmals versucht wird, den Angriff als „belanglos“ abzutun. Möglicherweise sind auch direkten Schäden im ersten Blick nicht so groß: Oftmals erfolgt dann der tatsächliche Angriff aber erst zu einem späteren Zeitpunkt, wenn ein Gesamtbild über weitere Teilmosaiksteinchen aus weiteren Angriffen, auch bei anderen Firmen, zusammengesetzt ist. Dabei, so Mayer, sei das Angriffsszenario vielfältig: Beim Bundesnetz z.B. geht man täglich von 2.000 bis 3.000 Angriffen aus; dabei zwei bis drei ernsthafte Bedrohungen, die auch weiterführende Konsequenzen haben könnten. Angreifer seien Cyber-Kriminellen oder Nachrichtendienste bis hin zu Häckerfreaks – jeder in einer anderen Absicht und entweder finanziellen oder immateriellen Zielen. Dabei ist die Spionage nicht unbedingt das Ziel: Auch die Sabotage, insbesondere im hochsensiblen Energiesektor bei der Stromversorgung, kann Ziel eines Angriffs von ausländischen Nachrichtendiensten sein. Derzeit nehmen Angriffe auf gesamte Branchen stark zu. Auch das besondere Phänomen der Erpressungstrojaner (Ransomware), bei dem ganze Computernetzwerke mittels einer Verschlüsselungssoftware lahmgelegt werden und nur gegen vermeintliche Schutzgelderpressung in Internetwährungen versprochen wird preiszugeben, haben 2016 überproportional zugenommen. Spezialist Mayer vom Verfassungsschutz stellt dar, wie der „Digitale Krieg“ mit dem black-out der Stromversorgung als Terrorziel mittlerweile eine ernsthafte Bedrohung wird.

Hierbei kommt dann der Verfassungsschutz Baden-Württemberg ins Spiel: Mit dem Erstkontakt beim vertraulichen Telefon bis hin zur umfassenden, selbstverständlich kostenlosen und nach außen für die Mitarbeiter nicht sichtbaren Begleitungen und Beratungen durch die Spezialisten des Verfassungsschutzes zeigte Mayer auf, wie der Schutz der Wirtschaft in Baden-Württemberg gelingt: Im Fokus stehen dabei die insbesondere sensiblen menschlichen Angriffsfaktoren über das sogenannte „Social Engineering“, d.h. das Ausspähen von Informationen über vertrauliche, persönliche Kontakte, gefolgt von der Prävention als Managementaufgabe, der Schaffung von Bewusstsein für die Bedrohung, insbesondere auch bei Kleinbetrieben, bis hin zu den ganzheitlichen Schutzkonzepten, die auf personeller, auf organisatorischer und auf materieller Ebene den Schutz der baden-württembergischen Wirtschaft und dem hier vorhanden know-how sicherstellen sollen. Und dies, so die Zusage Mayers, kostenlos für alle Unternehmen mit größtmöglicher Sorgfalt und auch absoluter Diskretion.

Text: Alex Wolf, IHK Rhein-Neckar