Schutzgebühr: 45,- €

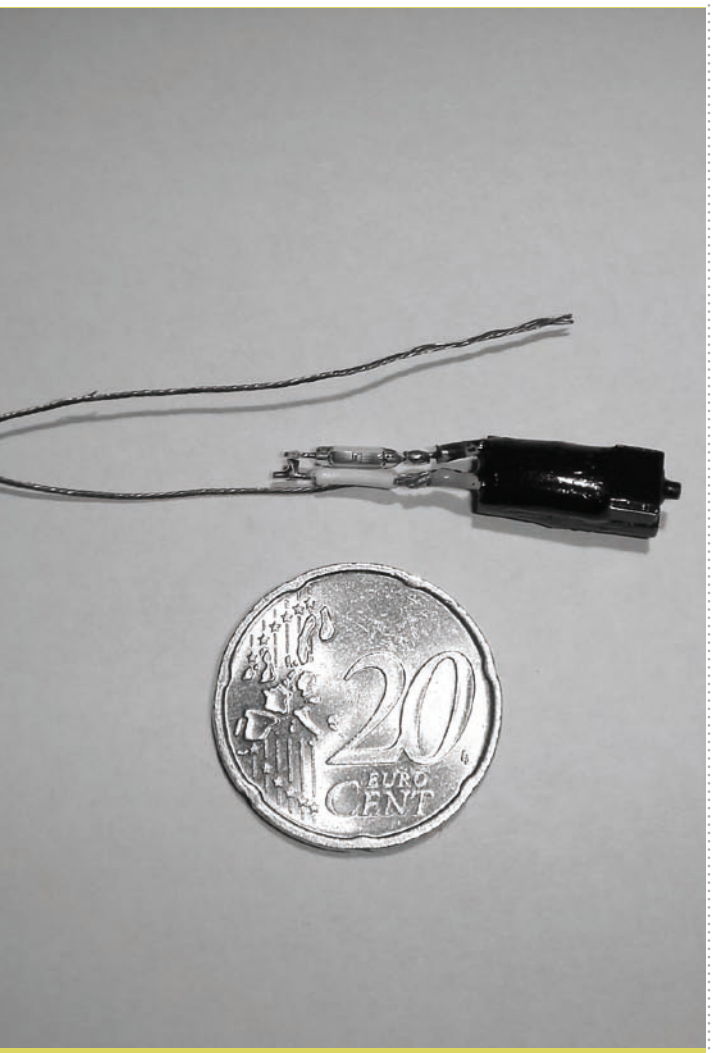
RECHTLICHER LEITFADEN
LAUSCHABWEHR UND INFORMATIONSSCHUTZ

HERAUSGEBER:
RA ROBERT NIEDERMEIER,
ANSGAR ALFRED HUTH

INHALTSVERZEICHNIS

I.

BEDEUTUNG DER LAUSCHABWEHR / INFORMATIONS-SCHUTZ UND IT-SICHERHEIT



ABHÖRWANZE

Die Lauschabwehr und der Informationsschutz stellen einen wichtigen Teilbereich der IT-Sicherheit dar. Unternehmen verstehen heute die IT-Sicherheit immer noch weitgehend als Thema der Bereiche Technik und Organisation. Nur wenige Profis unter den IT-Verantwortlichen haben erkannt, dass das Spielfeld der IT-Sicherheit neben dem Bereich Technik und Organisation auch aus dem Bereich Recht besteht. ***Die Rechtslage verlangt von einem professionellen Verantwortlichen in der IT-Sicherheit die Kenntnis der wesentlichen rechtlichen Zusammenhänge für sein Aufgabengebiet, ebenso wie ein Autofahrer die Straßenverkehrsordnung kennen muss. Ohne diese Kenntnisse werden IT-Sicherheitsverantwortliche ihre Aufgabe nicht korrekt erledigen können und zwangsläufig privathaftende Amateure der IT-Sicherheit bleiben.***

Informationen (Know how) stellen in der heutigen Zeit nach wie vor das größte und fundamentalste Wirtschaftsgut eines Unternehmens dar. Das gesprochene oder geschriebene Wort ist hierbei das Ziel von Lauschangriffen, da der Gegenstand der Kommunikation wie Vertragsentwürfe, Angebote, Konditionen, Kalkulationen, Bewerbungen, Personalien und personenbezogene Daten hierbei übertragen werden. Dieser Informationsaustausch erfolgt sowohl intern als auch extern.

1. Rechtliche Vorgaben zur Wahrung der IT-Sicherheit / zur Abwehr von Lauschangriffen

IT-Sicherheit gehört mittlerweile zur unabdingbaren Voraussetzungen der Tätigkeit eines jeden Unternehmens. Die Verpflichtung des Unternehmens, die Sicherheit seiner Daten und IT-Systeme zu gewährleisten ist in Regelwerken auf nationale, europäische und internationale Ebene vorgesehen. Auf nationaler Ebene sehen unter anderem gewerbeordnungsrechtliche Grundsätze, das Telekommunikationsgesetz und das Datenschutzgesetz Verpflichtungen für die Unternehmen, angemessene technische Vorkehrungen oder sonstige Maßnahmen zur Gewährleistung der IT-Sicherheit zu treffen, vor. Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich sieht eine Pflicht zur Schaffung eines unternehmensinternen Risikofrüherkennungssystems für Aktiengesellschaften vor; zu Risiken der Gesellschaft gehört unter anderem eine fehlende IT-Sicherheit.

Auf europäischer Ebene ist die Datenschutzrichtlinie für elektronische Kommunikation (Richtlinie 2002/58/EG) von Bedeutung. Sie bestimmt, dass der Betreiber eines öffentlich zugänglichen Kommunikationsdienstes geeignete technische und organisatorische Maßnahmen ergreifen muss, um die Sicherheit seiner Dienste zu gewährleisten.

Auf internationaler Ebene sind vor allem die verschärften Anforderungen durch Basel II und Sarbanes-Oxley-Gesetz für US börsennotierte Unternehmen und deren ausländische Tochtergesellschaften zu beachten. Basel II zwingen zum Ergreifen von Maßnahmen, denn die IT-Sicherheit wird zukünftig auch bei der Kreditvergabe und –rückzahlung von Relevanz sein. SOX verlangt von den betroffenen Unternehmen die Integrität ihrer Daten sicherzustellen. Unzureichende IT-Sicherheit führt zu den Schadensersatzansprüchen gegenüber dem Unternehmen sowie zur persönlichen Haftung der Geschäftsführung.

ABHÖRWANZE IM KUGELSCHREIBER

II.

WELCHE RISIKEN BESTEHEN

ABHÖRWANZE IM EINWEGFEUERZEUG

In der heutigen Zeit besteht das größte Risiko in der ungewollten und unbemerkten Weitergabe von Geschäftsgeheimnissen an Dritte.
Jedes Unternehmen muss sich daher über IT-Sicherheitsrelevante Fragen Gedanken machen, um letztendlich Schäden (Geld- und Imageverlust) zu vermeiden. Die finanziellen Auswirkungen eines Lauschangriffs können leicht die Existenz des Unternehmens bedrohen.

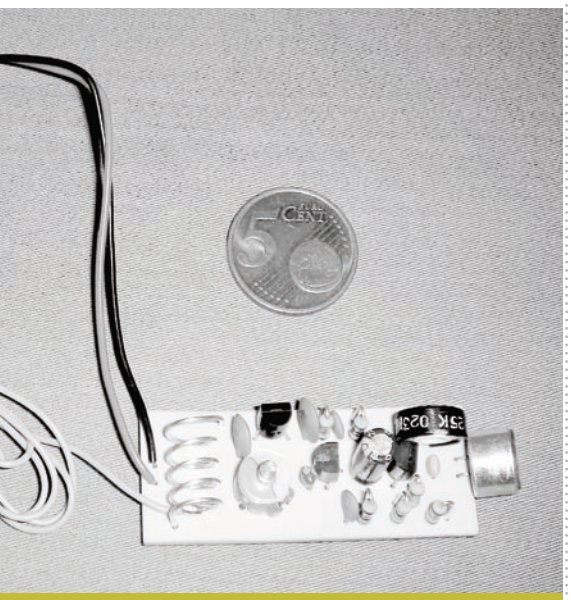
Jeder Lauschangriff, der aufgrund mangelnder oder unzureichend umgesetzter IT-Sicherheitsmaßnahmen in einem Unternehmen eintritt, hat signifikante finanzielle Auswirkungen auf das Unternehmen und zwar meist verbunden mit wesentlich höheren Kosten, als denen für ein passendes IT-Sicherheitskonzept bzw. erforderliche Lauschabwehreinsätze. Wer Vorsorge trifft, kann damit zukünftige Ausgaben verhindern oder zumindest wesendlich vermindern. Eine vollständige IT-Sicherheitspolitik berücksichtigt immer, über die technischen Lösungen hinaus, die organisatorischen Maßnahmen und insbesondere die rechtlichen Aspekte im Bereich IT-Sicherheit.

II.

1. Technische Möglichkeiten des Lauschangriffs

Die Lauschangriffe werden z.B. mittels versteckt angebrachter „Wanzen“, die von Mitarbeitern, Fremdpersonal oder Dritten in die Geschäftsräume verbracht werden realisiert, aber auch unbewusst mitunter vom Abgehörten persönlich ermöglicht. Dies ist dann der Fall, wenn die Wanze in einem Werbegeschenk wie einem Kugelschreiber, Aschenbecher oder Gemälde versteckt ist und von der Zielperson eigenhändig in den zu überwachenden Raum eingebracht und platziert wird.

Folgende Abhöreinrichtungen kommen bei Lauschangriffen insbesondere zur Anwendung:



ABHÖRWANZE FÜR 5 EURO

„Wanzen“ Minisender

Funktion:

Versteckte, getarnte Raummikrofone übertragen Gespräche über Funk. Reichweite: 20 m bis 5 km. In Verbindung mit einer Scanner-Handy-Einheit: Reichweite weltweit. Energieversorgung meist über Batterie, aber auch über Netzstrom- und Telefonnetz oder Solarzellen. Passive Wanzen benötigen keine angebaute Energieversorgung. Die benötigte Energie wird einfach von außen eingestrahlt.

Versteck:

Die winzigen elektronischen Bauteile können in jedem Hohlraum stecken, in abgehängten Decken, Böden, Möbeln, Elektrogeräten, Zimmerpflanzen. Hier zählt Phantasie, Einfallsreichtum und Erfahrung.

II.

1. Technische Möglichkeiten des Lauschangriffs

Mini-Diktiergeräte

Funktion:

Die Winzlinge zeichnen Sprache auf. Ein Diktiergerät in Scheckkartengröße nimmt viele Stunden Gespräche auf, selbst das allerkleinste Gerät in einem Kugelschreiber schafft mehrere Stunden Gesprächsaufnahme. Moderne Handys besitzen ebenfalls eine Gesprächsaufnahmefunktion die etliche Stunden getarnte Gesprächsdokumentation realisieren.

Versteck:

Fast immer bringen Besucher die Aufnahmegeräte mit. Die Geräte werden entweder am Körper getragen, in Aktenkoffer bzw. anderen Konferenzutensilien eingebaut, oder vor dem Gesprächstermin in einem Einrichtungsgegenstand des relevanten Raumes versteckt.

KUGELSCHREIBER MIT 8 STD. GESPRACHSAUFNAHME

II.

1. Technische Möglichkeiten des Lauschangriffs

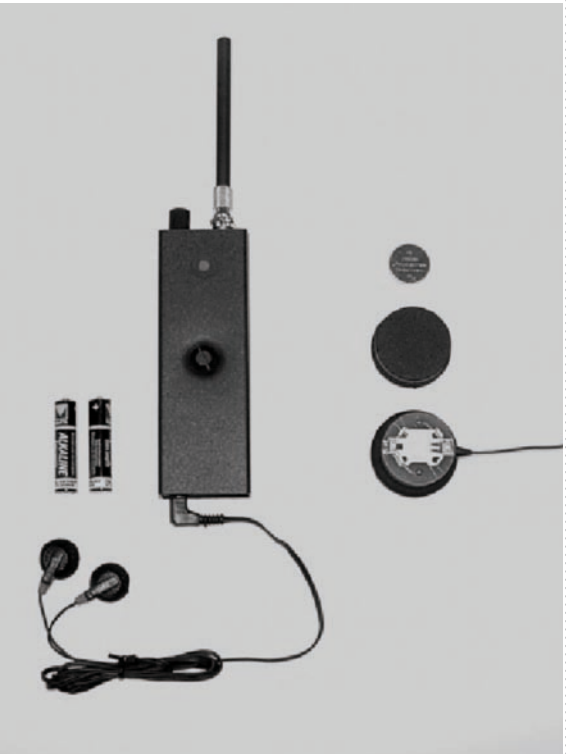
Manipulierte GSM-UMTS- Handys

Funktion:

Durch Manipulationen der Hardware und oder der Software eines Handys können diese Kommunikationsmittel zur getarnten Gesprächsüberwachung und Aufzeichnung missbraucht werden. Der Leistungsumfang jedes Handys lässt sich per Fernsteuerung jederzeit abändern. Handys die während eines sensiblen Gespräches eigenmächtig und vom Besitzer nicht erkennbar eine Telefonverbindung zu einer anderen Rufnummer in Übersee aufbauen, sind seit Jahren Realität.

Versteck:

Der Informationspunkt „Versteck“ entfällt bei dieser Abhörtaktik, da der Abgehörte permanent dafür sorgt, daß die Abhörtechnik (das eigene Handy) sich in seiner Nähe befindet und auch jederzeit betriebbereit bzw. erreichbar ist.



KÖRPERSCHALLWANZE
MIT EMPFÄNGER

Körperschallmikrofon

Funktion:

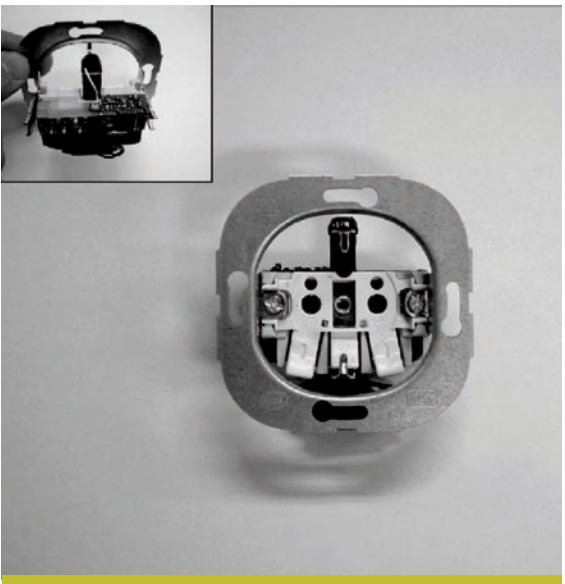
Der Lauscher nutzt z. B. einen Heizkörper oder die ganze Wand wie ein Mikrofon. Schallwellen versetzen Körper in Schwingungen, die das Gerät auffängt, verstärkt, filtert und hörbar macht.

Versteck:

Der Lauscher sitzt unbehelligt im angrenzenden Raum oder sendet weltweit per Funkwanze die Gespräche weiter. Beliebte Lauschstellen sind auch Versorgungsschächte, die vertikal oder horizontal durch alle Etagen führen.

II.

1. Technische Möglichkeiten des Lauschangriffs



UNTERPUTZSTECKDOSEN MIT ABHÖRWANZE

Drahtfunk

Funktion:

Funktioniert innerhalb des Gebäudes. Der Langwellensender nutzt die 220-Volt-Stromleitung als Antenne und bezieht den Strom aus dem Netz. Diese Netzstromwanzen benötigen somit keine Batterie. Sie eignen sich hervorragend für eine dauerhafte „Datenverbindung".

Versteck:

In 220V-Elektrogeräte eingebaut. Oft tauschen die Lauscher vorhandene gegen präparierte Geräte aus oder implantieren das kleine Senderchen während einer Reparatur oder günstigen Aufrüstung. Besonders beliebt: Einbau in handelsübliche Mehrfachsteckdosen, Verlängerungskabel oder Unterputzsteckdosen.

Festverdrahtete Raummikrofone

Funktion:

Die klassische Stasi-Wanze wird oft schon bei der Errichtung eines Gebäudes fest installiert. Gespräche werden von einer festen Abhörstation im Haus belauscht, ausgewertet oder weitergeleitet.

Versteck:

Raummikrofone finden sich vor allem in Deckenverkleidungen und Mauerhohlräumen. Diese Abhörvariante wird z.B. in Hotels, Konferenzzentren und Passagierflugzeugen eingesetzt.

II.

1. Technische Möglichkeiten des Lauschangriffs

Richtmikrofone

Funktion:

Der Schall wird durch ein Parabol-Richtmikrofon oder Standard-Richtmikrofon eingefangen. Die Schallwellen werden wie bei einer Körperschall-Auswertung mehrfach verstärkt, gefiltert und ausgewertet.

Versteck:

Der Lauscher lauert z. B. im Freien auf einer Parkbank und richtet die Spitze seines Regenschirmes unbemerkt auf eine Person oder ein geöffnetes Bürofenster. Diese Regenschirmspitze, die während des Spazierens durch eine kleine Hülse geschützt ist, stellt das Richtmikrofon dar.

RICHTMIKROFON

Telefonwanzen

Funktion:

Die Täter klemmen sie z. B. direkt an die Telefonleitung, die dann auch den Strom liefert. Der Sender wird aktiviert, wenn der Hörer abgenommen wird, überwacht permanent den Raum in Sachen Schallwellen oder wird von außen aktiviert.

Versteck:

Telefon, Telefonanschlussdose, Telefonleitung, innerhalb oder außerhalb des Gebäudes (Verteilerkasten)

II.

1. Technische Möglichkeiten des Lauschangriffs

FAXMONITORING ZUM AUFZEICHNEN VON FAXEN

Fax-Monitoring-System

Funktion:

Das System protokolliert alle ein- und ausgehenden Faxnachrichten auf Papier oder Datenträger. Die Teilnehmer merken davon nichts.

Versteck:

Das Gerät wird direkt an die Telefonleitung innerhalb oder außerhalb des Gebäudes angeschlossen.

LUFTERFRISCHER MIT EINGEBAUTER KAMERA

Kamerawanzen

Funktion:

Versteckte, getarnte Kamerawanzen übertragen Bild und Ton per Funkverbindung. Reichweite: 20 m - 5 km. In Verbindung mit einer Empfänger-Handy-Einheit Reichweite: weltweit. Energieversorgung meist über Batterie, aber auch über Netzstrom.

Versteck:

Die Zuckerwürfel großen Kameras können in jedem Hohlraum stecken, z.B. in abgehängten Decken, Bilder, Spiegel, Möbeln, Elektrogeräten.

III.

WER IST FÜR DIE IT-SICHERHEIT / LAUSCHABWEHR IM UNTERNEHMEN VERANTWORTLICH

FUNKEMPFÄNGER MIT GESPRÄCHS-AUFZEICHNUNG

Für IT-Sicherheit rechtlich verantwortlich ist die Unternehmensleitung, etwa die Geschäftsführung oder der Vorstand.
Die Pflicht der Geschäftsführung oder Vorstände zur Wahrung der IT-Sicherheit ergibt sich mittlerweile aus zahlreichen gesetzlichen Vorschriften. So wurde z.B. das KonTraG § 91 Abs. 2 AktG eingeführt, wonach Vorstände einer Aktiengesellschaften ein Risikofrüherkennungs- und Überwachungssystem im Unternehmen implementieren müssen. Zu den Risiken einer Gesellschaft gehört unter anderem eine fehlende oder mangelhafte IT-Sicherheit bzw. Informationsschutzmaßnahmen.
Das gilt nicht nur für Aktiengesellschaften, sondern auch für alle anderen Gesellschaftsformen.

Die Unternehmensleitung kann Entscheidungsbefugnisse an Mitarbeiter des Unternehmens delegieren, insbesondere an leitende Angestellte, etwa den Prokuristen oder den Leiter der IT-Abteilung. Diese können ihrerseits innerhalb ihres Verantwortungsbereichs Verantwortung delegieren, etwa an die Administratoren oder andre Mitarbeiter der IT-Abteilung. In jedem Fall sind die betreffenden Personen sorgfältig auszuwählen und zu überwachen, und es ist – etwa durch Schulungen und die Zurverfügungstellung der erforderlichen Sachmittel – sicherzustellen, dass sie ihre Aufgaben erfüllen.

Delegierung der Pflichten zur Wahrung der IT-Sicherheit befreit die Geschäftsführung von der Haftung für fehlende IT-Sicherheit nach AktG oder GmbHG nicht. Auch bei der Delegierung entsprechender Pflichten muss die Geschäftsführung die sachgerechte Erfüllung dieser Pflichten überwachen.

Die Unternehmensleitung erhält Unterstützung durch besondere Beauftrage, die die IT-Sicherheit überwachen, der Unternehmensleitung darüber berichten und Vorschläge unterbreiten sollen, ohne aber selbst über Entscheidungs- oder Weisungsbefugnisse zu verfügen.

Dies gilt zum einen für den betrieblichen oder behördlichen Datenschutzbeauftragten, der unter den Voraussetzungen des Datenschutzrechts zwingend zu bestellen ist, und zum anderen für den IT-Sicherheitsbeauftragten, dessen Bestellung zwar nur ausnahmsweise- etwa im Telekommunikationsrecht oder für bestimmte Behörden – rechtlich geregelt ist, aber faktisch zur Gewährleistung der IT-Sicherheit erforderlich ist.

III.

UKW-SELSTBAUSATZ-
ABHÖRWANZE

1. Stehe ich als IT-Sicherheitsverantwortlicher mit einem Bein im Gefängnis?

Wird eine IT-spezifische Straftat im Aufgabenbereich eines IT-Verantwortlichen entdeckt, so kann sich dieser entweder persönlich oder als Repräsentant des Unternehmens stellvertretend für die Tat strafbar gemacht haben.

Die unbefugte Offenbarung geheimer Informationen über das Unternehmen (Betriebs- und Geschäftsgeheimnisse) oder über Mitarbeiter (personenbezogene Daten) stellt ein enormes Risiko für das Unternehmen dar. Die Unternehmensleitung unterliegt hierbei strengen Anforderungen.

Strafbar macht sich dabei auch, wer es (etwa aus Kostengründen) pflichtwidrig unterlässt, die erforderlichen Sicherheitsmaßnahmen zu implementieren, und dabei billigend in Kauf nimmt, dass beispielsweise, geheime Informationen Dritten zugänglich gemacht werden.

Zu diesen Sicherheitsmaßnahmen gehört neben der E-Mailfilterung auch der Schutz vor Lauschangriffen bzw. Schutz des Firmeninternen Netzwerkes sowie der datenkritischen Räumlichkeiten im Unternehmen.

Diese Sicherungsmaßnahmen müssen auch von den Verantwortlichen auf Funktionalität und Effektivität permanent überprüft und revidiert werden. Für den Bereich

III.

Lauschabwehr bedeutet dies, daß die Lauschabwehrüberprüfungen in verantwortbaren Intervallen in den sensiblen Räumlichkeiten ausgeführt werden. Je kleiner die Zeitabstände zwischen den Lauschabwehrüberprüfungen sind, desto überschaubarer und klarer ist bei einem detektierten Lauschangriff der entstandene Schaden bzw. betroffene Geschäftsbereich einzugrenzen. Ein detektierter Lauschangriff, der einen Informationsabfluss über mehreren Wochen oder gar Monaten für das Unternehmen darstellt, ist in seiner Tiefen- und Auswirkung in Sachen Unternehmensplanung und KnowHow-Verlust kaum noch einzugrenzen bzw. abzuschätzen.

2. Hafte ich als Verantwortlicher mit meinem Privatvermögen

Sind im Unternehmen die notwendigen IT-Sicherheitsstrukturen nicht oder unzureichend implementiert worden, und kommt es daraufhin zu einer unbefugten Informationsweitergabe an Dritte, so riskiert der IT-Sicherheitsverantwortliche die Haftung des Unternehmens und seiner eigenen Person. D.h. er muss gegebenenfalls mit seinem Privatvermögen für entstandene Schäden aufkommen. Anders als im Strafrecht, haftet der IT-Sicherheitsverantwortliche im Zivilrecht auch für Fahrlässigkeit. Wurde von der Geschäftsleitung kein Mitarbeiter (rechtlich nachweisbar) zum IT-Sicherheitsverantwortlichen ernannt, haften natürlich in erster Linie die Geschäftsführer bzw. Vorstände des belauschten Unternehmens mit Ihrem privaten Vermögen für den entstandenen Know-how-Verlust.

GPS-FAHRZEUGWANZE

Hierbei handelt fahrlässig, wer die im Geschäftsverkehr einem ordentlichen Geschäftsmann obliegende Sorgfaltpflicht verletzt. Wer grob fahrlässig Sicherheitsmaßnahmen unterlässt, muss damit rechnen, dass ihm entstandene Schäden nicht oder nicht vollständig ersetzt werden. So kann der Schädiger den Einwand des Mitverschuldens anführen, weil der Schaden nur in geringem Umfang entstanden wäre. Die Versicherung kann die Leistung verweigern, wenn die IT-Sicherheit betreffende Obliegenheiten in den Versicherungsbedingungen verletzt wurden. ***Auch von der Geschäftsleitung ignorierte***

Berichte, Gutachten oder Schutzmaßnahmen-Empfehlungen des IT-Sicherheitsverantwortlichen oder externen Sachverständigen, führen zur Haftung des gesamten Führungsstabes eines Unternehmens.

III.

3. Welche sonstigen Sanktionen drohen

Eine Haftung mit dem Privatvermögen kommt bei Vermögensschäden in Betracht. Darüber hinaus drohen IT-Sicherheitsverantwortlichen in der Unternehmensleitung die Abberufung und Kündigung der Anstellungsverträge.

FERNGESTEUERTE ZIGARETTE MIT EINGEBAUTER ABHÖRWANZE UND AKKUPACK

IV.

RECHTLICHE PFLICHT ZUR LAUSCHABWEHR / INFORMATIONSSCHUTZ

Die rechtliche Verpflichtung ergibt sich zum einen aus einer vertraglichen Vereinbarung und zum anderen aber auch aus dem Bundesdatenschutzgesetz sowie der Verschwiegenheitspflicht bei Berufsgeheimnisträgern.

Insbesondere das Bundesdatenschutzgesetz sieht in § 9 BDSG die Pflicht vor, dass jede verantwortliche Stelle die geeigneten technischen und organisatorischen Maßnahmen einführen muss, um die Anforderungen des Bundesdatenschutzgesetzes zu gewährleisten.

Hierunter fallen beispielsweise eine gestufte Zugangskontrolle zu personenbezogenen Daten, die nur je nach Verwendungszweck dem jeweiligen Sachbearbeiter zugänglich sind. Es ist folglich zu gewährleisten, dass kein Dritter an die firmenintern vorhandenen Daten und Informationen herankommt.
Folge des unzureichenden Informationsschutzes ist die Haftung des Unternehmens gegenüber den betroffenen Dritten. ***Werden Kunden- oder Geschäftspartnerdaten durch unzureichenden Schutz der Öffentlichkeit bekannt gegeben, so ist das Unternehmen den Schadensersatzansprüchen dieser Personen ausgesetzt.***

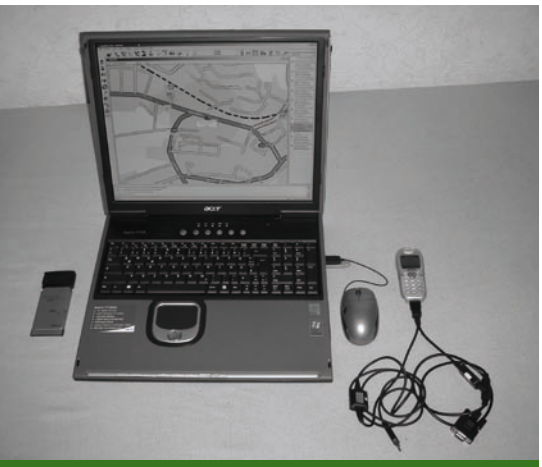
Unternehmen die viele Ressourcen für IT-Sicherheit ausgeben aber keine korrespondierenden Maßnahmen im Bereich Informationsschutz treffen, offenbaren einen expliziten Strukturbruch, weil der Bereich des Schutzes eigener Geschäftsgeheimnisse sowie des Schutz der Geschäftsgeheimnisse von Vertragspartner nur gesamtheitlich möglich ist.

RAUCHMELDER-KAMERA

IV.

Bereits diese Diskrepanz stellt die Erfüllung von Compliance Vorgaben in Frage und führt zur Exponierung der verantwortlichen Führungskräfte. Diese Exponierung kann sich massive negativ auswirken, weil der dargestellte Strukturbruch regelmäßig zu Verlust oder Einbussen beim Versicherungsschutz des Unternehmens und/oder der Führungskräfte (D&O Versicherung) führt. Versicherungen sehen in ihren Vertragsbedingungen regelmäßig vor, dass nur Unternehmen die korrekt gesetzeskonform strukturiert sind Versicherungsdeckung genießen.

In der letzten Zeit wurden Führungskräfte von ihren Unternehmen wiederholt gerichtlich in Anspruch genommen und – privat – zur Kasse gebeten. Diese Urteile werden regelmäßig nicht veröffentlicht, weil sich die Streitparteien zur Vertraulichkeit verpflichten. Hinweise, wie etwa im VW-Korruptionsfall, dass die zuständige D&O Versicherung den entstandenen Schaden trägt sind die absolute Ausnahme.



GPS-FAHRZEUGWANZEN-ÜBERWACHUNGSZENTRALE

AUSRÜSTUNG ZUM ÜBERWACHEN DES GSM-HANDYNETZES

V.

WAS KANN ICH ALS VERANTWORTLICHER TUN

Jeder Schadensfall, der aufgrund mangelnder oder unzureichender Sicherheitsmaßnahmen eintritt, hat eine signifikante finanzielle Auswirkung auf Ihr Unternehmen, und zwar mit meist wesentlich höheren Kosten verbunden, als jene für ein passendes Sicherheitskonzept.
Wer Vorsorge trifft, kann damit zukünftige Schäden und Verluste verhindern oder zumindest vermindern. Eine vollständige Sicherheitspolitik berücksichtigt immer, über die technischen Lösungen hinaus, die organisatorischen Maßnahmen und insbesondere rechtliche Aspekte im Bereich der Sicherheit des Unternehmens gegenüber dem Lauschangriff.

1. Welche technischen Möglichkeiten gibt es?

VIDEORECORDER MIT EINGEBAUTER SPIONAGEKAMERA

Das Unternehmen muss im Bezug auf die E-Mail und Internetnutzung Software zur E-Mailfilterung, Intrusiondetection, Firewall etc. einsetzen.
Das gesprochene Wort in sensiblen Räumen (Büros der Entscheider, deren Vorzimmer, Konferenzzimmer, Räume in denen sensible Gespräche stattfinden können) muß durch regelmäßige Lauschabwehreinsätze eines Sachverständigen gegen Lauschangriffe bzw. Spionagetechnik geschützt werden.

Im Bezug auf das gesprochene Wort übertragen per Telekommunikation (ISDN, GSM, UMTS, VoIP, etc.) hat eine regelmäßige Überprüfung der Telefonleitungen, der Telefonanlage bzw. der TK-Geräte stattzufinden. Besonders sensible Informationen und Gespräche dürfen nur kryptologisch verschlüsselt per Telekommunikation übersendet werden.
Es kann hierbei auch in Erwägung gezogen werden, einen abhörgeschützen Besprechungsraum einzurichten.
Gestufte Zugangskontrollen im gesamten Unternehmensbereich besonders zu sensiblen Räumlichkeiten mittels Codekarten oder biometrischer Authentifizierung, in Verbindung mit einer ausgereiften Videoüberwachung, stellen die Basis des Informationsschutzes dar.

V.

2. Welche organisatorischen Möglichkeiten gibt es?

Technische Maßnahmen müssen von einer Reihe organisatorischer Maßnahmen flankiert werden.
Am wichtigsten ist es, die IT-Sicherheitspolitik im Hinblick auf Lauschabwehr / Informationsschutz zu koordinieren und etwa auf der Grundlage einer IT-Sicherheitsrichtlinie ein IT-Sicherheitskonzept zu entwickeln und zu implementieren.
Ein solches Vorhaben hilft zudem die Schwachstellen innerhalb der IT-Sicherheitsinfrastruktur zu identifizieren.
Codekarten oder biometrischer Authentifizierung, in Verbindung mit einer ausgereiften Videoüberwachung, stellen die Basis des Informationsschutzes dar.

Ein schriftliches IT-Sicherheitskonzept dokumentiert die Organisation der IT-Infrastruktur und deren Überwachung. Nur auf diesem Wege ist es zuverlässig möglich, im Streitfall den (Entlastungs-) beweis zu führen, die gesetzlichen Anforderungen an die IT-Sicherheit erfüllt zu haben.
Ein im Vorfeld erstelltes Gutachten eines unabhängigen Lauschabwehr-Sachverständigen belegt nach einem stattgefundenen Informationsdiebstahl, daß sich die Geschäftsleitung mit dem Thema Lauschabwehr ernsthaft befasst hat. Regelmäßig stattgefundene Lauschabwehrüberprüfungen belegen die Pflichterfüllung der Geschäftsleitung bzw. der Verantwortlichen in Sachen Informationssicherheit und KnowHow-Schutzmaßnahmen.

PAPIERTUCHSPENDER MIT EINGEBAUTER KAMERA

Ein wesentlicher Teil organisatorischer Maßnahmen liegt im psychologischen Bereich. Bei der Implementierung des IT-Sicherheitskonzepts für Lauschabwehr / Informationsschutz sind das Bewusstsein der Mitarbeiter für IT-Sicherheit und die Akzeptanz der erforderlichen Maßnahmen die entscheidenden Faktoren.
Sofern eine Mitarbeitervertretung besteht, sollte diese frühzeitig mit einbezogen werden.

V.

Als organisatorische Maßnahmen im Rahmen des IT-Sicherheitskonzept für Lauschabwehr / Informationssicherheit kommen namentlich in Betracht:

- reservierte, normalerweise verschlossene und besonders ausgestattete Besprechungsräume
- Handyverbot (zeitlich und räumlich klar definiert)
- Überprüfung der Einhaltung des Handyverbotes mittels Detektoren.
- Disziplin im Gesprächsverhalten, auch während der Pausen eines Meetings
- Regelmäßige Untersuchung der sensiblen Räume durch einen Lauschabwehrexperten
- Überprüfung von Werbegeschenken auf mögliche Wanzen
- Disziplin bei der Nutzung von Telekommunikationseinrichtungen
- Informationsschutz im Empfangsbereich und in öffentlich einsehbaren Bereichen (Empfangstre sen – Besucherbuch geschlossen halten und Dokumente mit der Schriftseite nach unten ablegen, Überwachungsmonitore nicht einsehbar, etc.)
- berichten bzw. diskutieren über Firmeninternas nicht im Privatleben.
- Mitarbeiterschulungen zum Thema Informationsschutz am Arbeitsplatz.
- Sensibilisieren der KnowHow-Träger des Unternehmens zum Thema Industriespionage.
- Konsequenter Einsatz von Gesprächs- und Datenverschlüsselung
- Regelmäßige Überprüfung der Netz-, Telefon- und Datenleitungen auf Manipulationen durch einen Lauschabwehr-Sachverständigen
- Fernwartungen von IT-Systeme und TK-Anlagen nicht zulassen.

V.

3. Welche rechtlichen Möglichkeiten gibt es?

Die technischen und organisatorischen Maßnahmen müssen sich innerhalb des rechtlich zulässigen Rahmens halten. Daher ist es dringend zu empfehlen, das Implementieren von Lauschabwehr / Informationsschutzkonzepten rechtlich begleiten zu lassen.

Eine rechtliche Begleitung stellt sicher, dass die gesetzlich vorgeschriebenen Strukturen für Informationsschutz im nötigen Umfang und in der nötigen Tiefe im Unternehmen implementiert werden und das Unternehmen über diese Strukturen eine beweisrelevante Dokumentation führt.

Grundvoraussetzung für die Überwachung des Internet- / Emailverkehrs, sowie des Kommunikationsverhaltens bzgl. des Telefonierens ist es, dass diese Medien ausschließlich zu Unternehmenszwecken eingesetzt werden. Die private Nutzung muss deshalb gänzlich ausgeschlossen werden. Anderenfalls wird das Unternehmen zum Telekommunikationsdiensteanbieter der dem Fernmeldegeheimnis unterliegt. Speicherung sowie die Inhaltskontrolle der Korrespondenz des Arbeitnehmers, sei sie auch geschäftlicher Natur, wird dadurch problematisch.

Entscheidet sich die Geschäftsleitung zum Zwecke der Sicherheit im Unternehmen die Videoüberwachung einzuführen, so ist auf die Vorgaben des Bundesdatenschutzrechts Rücksicht zu nehmen.
Bei der Überwachung am Arbeitsplatz, ist zu beachten, dass diese nicht von § 6b BDSG mitumfasst ist. Allgemeine Vorschriften zum Schutz personenbezogener Daten sind daher anwendbar. Die Einführung einer Videoüberwachung der Arbeitnehmer bedarf der Zustimmung des Betriebsrates gemäß § 87 I Nr. 6 BetrVG. Aber auch nach Einholung der Zustimmung des Betriebsrates ist die pauschale lückenlose Videoüberwachung des Arbeitnehmers unzulässig.

Bei der Verwendung von Videoüberwachungsanlagen zum Zwecke der Zutrittskontrolle ist § 31 BDSG heranzuziehen. Es bedarf daher der Wahrnehmung berechtigter Interessen für konkrete Zwecke. Dies ist dann der Fall, wenn es nach vernünftigen Erwägungen durch die Sachlage gerechtfertigt ist. Der konkrete Zweck der Videoüberwachung muss vor Inbetriebnahme der Überwachung festgelegt, d.h. dokumentiert sein.

VI. ZUSAMMENFASSUNG

Um ein größtmögliches Maß an Lauschabwehr / Informationssicherheit zu gewährleisten, empfiehlt es sich, in Zusammenarbeit mit einem unabhängigen Sachverständigen ein gesondertes IT-Sicherheitskonzept für Lauschabwehr / Informationssicherheit zu erstellen. Nur hierdurch kann effektiv vermieden, zumindest aber auf ein Mindestmaß reduziert werden, dass durch Lauschangriffe sensible Unternehmensdaten in die Hände von Dritten gelangen.

Gerade in der heutigen Zeit, in der das Know How das wichtigste Unternehmensgut darstellt, müssen für die Mitarbeiter sowie die Geschäftsleitung eindeutige Regelungen im Bezug auf Geschäftsgeheimnisse gelten.
Anderenfalls drohen dem Unternehmen auch Kürzungen, etwa im Bereich der Betriebshaftpflichtversicherung oder ein entsprechender Reputationsverlust im jeweiligen Branchensegment.

Mit ansteigender Frequenz blühen und vergehen Unternehmen immer schneller in unserer heutigen Zeit. Wer hier als Geschäftsführer sein leichtverderbliches Wissensgut „Informationen“ nicht im Griff hat, der sollte das Wort Zukunftsplanung aus seinem Sprachjargon streichen. Überleben werden nur noch die Unternehmen, die ihr Informationswissen geschickt ausbauen und effektiv schützen werden. So lautet nun einmal das Gesetz unserer Leistungsgesellschaft und es wird sich in Zukunft weiterhin verschärfen!

Die Geschäftsführer und/oder die Verantwortlichen eines Unternehmens machen sich auf alle Fälle privathaftend strafbar, wenn sie es (etwa aus Kostengründen) pflichtwidrig unterlassen, die erforderlichen Sicherungsmaßnahmen (z.B. Lauschabwehrüberprüfungen) zu implementieren und dabei billigend in Kauf nehmen, dass betriebsinterne nicht öffentliche Informationen Dritten unkontrolliert zugänglich gemacht werden.

Abhanden gekommene Unternehmensinternas sind weder ersetzbar noch wiederzubeschaffen.

Im Bereich der IT-Sicherheit und der Lauschabwehr gilt daher vorbeugen statt beseitigen.

HERAUSGEBER:
RA ROBERT NIEDERMEIER,

Robert Niedermeier ist Mitglied der Information Communikation Technology (ICT) Arbeitsgruppe bei der Heussen Rechtsanwaltsgesellschaft und überwiegend mit Fragen der Bereiche Recht, Technik und Organisation bei Datenschutz und IT-Security befaßt. Mit seinem internationalen Team projektiert er für Banken, Versicherungen und internationale Unternehmen den weltweiten Roll-out homogener Datenschutz- und IT Sicherheitsstrukturen im Konzern und entwickelt neue Modelle für Compliance im Bereich IT-Security. In seiner Eigenschaft als Vorstand des European Institute for Computer Anti-Virus Research (EICAR) diskutiert er mit der IT-Security Branche über die rechtliche Zulässigkeit des sogenannten „Strike-Back".

ANSGAR ALFRED HUTH

Ansgar Alfred Huth ist international anerkannter Datenschutz- und Lauschabwehr-Sachverständiger, der in den Bereichen Abhörsicherheit und Informationsschutz für die Industrie- und Bankenwelt seit vielen Jahren tätig ist.
Ebenso bildet er in seinen zum Teil öffentlichen Seminaren, europäische Spezialeinheiten sowie Behördenvertreter und Sicherheitsverantwortliche in Sachen Spionageabwehr und Informationsgewinnung aus.
Auch VIP´s setzen im Bereich „Schutz der Familie und Privatsphäre" auf das Know-how diese Lauschabwehr-Spezialisten. Sein unsichtbares Wirken im Hintergrund vieler auch börsennotierter Konzerne, sichert den Entscheidern und Verantwortlichen dieser Unternehmen, den lebenswichtigen Faktor „Informationsschutz" professionell und auf Dauer ab.

RA ROBERT NIEDERMEIER

ANSGAR ALFRED HUTH

www.spionage.info