Sweeping - Detektion versteckter Audio- und Video-Devices

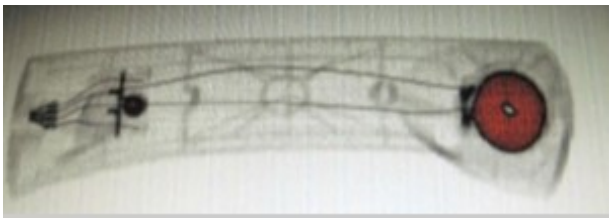
Der Verlust von vertraulichen oder geheimen Informationen kann unabsehbare Folgen für ein Unternehmen haben. Neben dem eigentlichen Reputationsverlust, dem Geschäftsrisiko und einem finanziellen Schaden können sich Betroffene mit straf-, wirtschafts-, privat- und aufsichtsrechtlichen Vorwürfen konfrontiert sehen.

Um an Informationen, Daten, Patente, Akten, Technologien und Personenangaben usw. zu gelangen, verwendet die Gegenseite (z.B. in- und ausländische Konkurrenz) unerlaubte Hilfsmittel und Methoden – auch in der Schweiz. Der Einsatz der immer kleineren, effizienteren sowie preisgünstigeren Technik und Elektronik ermöglicht versteckte Ton- und Bildaufnahmen, wodurch geheime oder vertrauliche Daten und Informationen gezielt zu Unberechtigten gelangen können.

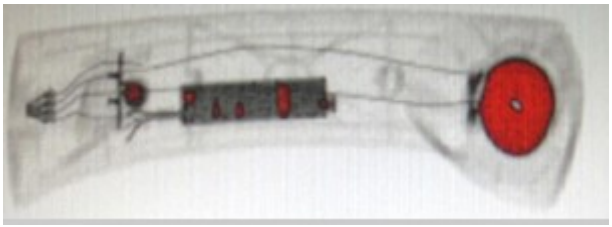
Sweeping

Um diesen Bedrohungen präventiv sowie reaktiv entgegenzuwirken, wird seit geraumer Zeit das forensische Mittel «Sweeping» eingesetzt. Die Untersuchung der Infrastruktur und Technik von Entscheidungsträgern bzw. deren Gesprächspartnern ist ein geeignetes und zielgerichtetes Gegen- und Abwehrmittel. Geschäftsgebäude - vom Rohbau bis zum fertigen Zustand -, Sitzungsräume, Vortragssäle, Büros, private Wohnobjekte sowie Fahr- und Flugzeuge werden systematisch untersucht, verdächtige Gegenstände identifiziert und entfernt. Folgendes Vorgehen findet Anwendung:

- Detaillierte **physische Durchsuchung** der Gebäudeinfrastruktur und des Mobiliars. Dies beinhaltet auch die De- und Montage von Einbauten und elektrischen Komponenten zwecks **visueller Kontrolle** von Hohlräumen und Installationskanälen.
- Erstellen **thermischer Aufnahmen** zwecks Identifikation von elektrischen Devices anhand der Wärmeentwicklung.
- Durchführen von **Frequenzmessungen** unter Verwendung hoch sensibler Instrumente, wodurch aktive Sender ausfindig gemacht werden können.
- **Schallmessungen** an Fensterfronten zur Erkennung von externen Lauschangriffen.
- **Röntgen** von portablen Gegenständen und Gerätschaften, um fest oder temporär verbaute Abhörgeräte oder Kameras sichtbar zu machen
- Dokumentation und Beratung von geeigneten **Sofort- und Gegenmassnahmen** zur künftigen Abwehr von Lauschangriffen sowie generell zugunsten der **Informationssicherheit**



Telefonhörer ohne Wanze (Röntgenbild)



Telefonhörer mit Wanze (Röntgenbild)

Untersuchungshandlungen

In der Schweiz haben Unternehmen, Private und Institutionen grundsätzlich keinen Anspruch auf behördliche Unterstützung in Form von solchen Untersuchungshandlungen. Sehr wenige spezialisierte Firmen führen gezielte «Sweeping»-Einsätze durch. Die Untersuchungshandlungen vor Ort sind je nach Anzahl und Grösse der Objekte personal- sowie zeitintensiv. Die Auftragsausführung findet meist ausserhalb der Bürozeiten und unter hoher Vertraulichkeit statt. Ausgewiesene, eingespielte und auftragsbezogen zusammengesetzte Teams mit Elektronikern, Informatikern, Technikern und Kriminalisten erledigen in Absprache mit dem Auftraggeber die konzentrierte Arbeit vor Ort. Allfällig gefundene «Bugs» oder «Wanzen» bzw. Überreste davon (z.B. Stromgeber) werden dokumentiert, entfernt und isoliert. Zugleich werden auf Wunsch offensichtliche Schwachstellen der Informationssicherheit dokumentiert.

Fazit

Der heutige Wirtschaftsschutz (Unternehmensschutz) muss sich mit allen Disziplinen der Integralen Sicherheit befassen. Die Risiken für Unternehmen in der Schweiz werden immer vielfältiger und komplexer. Cyberattacken, Wirtschaftskriminalität, Industriespionage, Sabotage und Social Engineering Angriffe finden mit einer deutlich höheren Kadenz und kaum durchschaubarer Verflechtung statt. Diese Herausforderungen gebieten so gezielte Untersuchungshandlungen wie «Sweeping». Dadurch werden rechtzeitig massgeschneiderte, präventive und reaktive Abwehrmassnahmen bereitgestellt, um personelle und materielle Schäden, Betriebsstillstände sowie Reputationsverluste zu verhindern.

Chris Eckert