

# LEISTUNGSBESCHREIBUNG

## Leistungsbeschreibung „wirkungsvoller Abhörschutz in 3 Phasen“

Nachfolgend erhalten Sie eine Übersicht mit detaillierten Leistungsbeschreibungen, wie unser Team vorgeht und welche Methoden wir einsetzen, um wirkungsvoll alle Arten von aktiven, und passiven Abhöranlagen zu lokalisieren und zu neutralisieren. Der Sicherheitsgrad ausgehend von unserem eingesetzten Equipment liegt bei 98 % (Stand Juni 2011) dass wir fündig werden. Der ECM-Groundcheck wird nach geprüften Methoden und Standards mit mindestens 5 redundanten (überlappenden) Prüf- und Testverfahren im Bereich der „elektronischen & messtechnischen Untersuchungen“ durchgeführt. Diese werden durch 13 weitere Prüf- und Testverfahren im Bereich der „visuellen & physischen Detektion“ ergänzt. Wir prüfen nach militärischem Standard und gehen grundsätzlich von äußerst prof. Tätern aus, deren Schwerpunkt Wirtschaftsspionage unter Mithilfe staatlicher Stellen ist, die Zugang zu nachrichtendienstlichen Technologien haben und denen uneingeschränkte Mittel zur Verfügung stehen.

## Grundsätzlicher organisatorischer Ablauf

### Nach Auftragserteilung:

Wir senden Ihnen an eine neutrale, gesicherte Adresse ein komplettes Informationspaket (Basisaufnahme, Ablauforganisation, To-Do-Checkliste etc.) zu. Alternativ vereinbaren wir außerhalb des Betriebes oder bei Ihnen vor Ort in einem nicht gefährdeten Unternehmensbereich einen Termin für die Basisaufnahme und die Besprechung der weiteren Ablauforganisation. Hierbei werden u.a. konkrete Einsatztermine besprochen, Fragen beantwortet, zu untersuchende Räume und Ihre gewünschten Schwerpunkte festgelegt. Weiterhin bekommen Sie eine To-Do-Checkliste ausgehändigt, um einen beidseitigen reibungslosen Ablauf sicherzustellen.

### Vor Ort bei Ihnen:

Auf Basis der Ablauforganisation werden wir diskret und neutral im Beisein eines Mitarbeiters von Ihnen, Ihre Firma betreten. Uns werden dann alle zu untersuchenden Räume gezeigt, auch Zugänge zu TK-Anlage, Serverraum und Nachbarräume müssen zugänglich sein. Wir werden dann lt. Ablaufplan vorgehen und unser Equipment (ca. 10 Koffer) in die zu untersuchenden Räume einbringen und unsere Messstationen aufbauen.

### Abschlussbesprechung:

Wir vereinbaren außerhalb des Betriebes oder in einem nicht gefährdeten Unternehmensbereich einen Termin für die Abschlussbesprechung und Gutachtenübergabe.



- **Fachkundig**
- **Zuverlässig**
- **Diskret**

# LEISTUNGSBESCHREIBUNG

## Phase 1 „Wir planen & analysieren“

### Identifizierung der Risiken / Sicherheitsanalyse nach Kaizen / Status Quo-Feststellung durch Einsatz diverser Checklisten u. a.:

1. Durchführung einer tiefgehenden Schwachstellenanalyse der in den zu untersuchenden Räumlichkeiten in Frage kommenden Angriffstechniken und möglichen Angriffsziele. Check der internen Sicherheitstandards.
2. Checkliste Detailaufnahme der Räume inkl. Versorgungseinrichtungen, technische Einrichtungen, TK- und EDV-Einrichtungen, komplette Ausstattungs- und Einrichtungsgegenstände sowie aller Schnittstellen nach außen hin.
3. Prüfung der technischen & organisatorischen Maßnahmen, vorhandener Schwachstellen mit Risikoidentifizierung, aller Angriffsmöglichkeiten, Zugangs-, Zutritt- und Zugriffsmöglichkeiten u.a. nach § 9 BDSG. Überprüfung der Ablaufschnittstellen auf Sicherheitsrisiken.

## Phase 2 „Wir messen, prüfen & finden“

### Aktive Lauschabwehr / Lokalisieren & deaktivieren von Abhöranlagen / Messtechnische Untersuchungen

Der ECM-Groundcheck wird nach geprüften Methoden und Standards mit mindestens 5 redundanten (überlappenden) Prüf- und Testverfahren im Bereich der „elektronischen & messtechnischen Untersuchungen“ durchgeführt. Diese werden durch 13 weitere Prüf- und Testverfahren im Bereich der „visuellen & physischen Detektion“ ergänzt. Alle Scans und Prüfungen werden von einem Sachverständigen für Abhörschutz und einem technischen Mitarbeiter zeitversetzt durchgeführt (Test-Retest-Methode), um die Zuverlässigkeit der Messergebnisse zu prüfen (Konsistenztest).

### A: Prüf- und Testverfahren „elektronische & messtechnische Untersuchungen

1. Hochfrequenzmessungen: Überprüfung der sensiblen Räume und Einzelkomponenten
2. Langwellenmessungen & Leitungsüberprüfung an 220-Volt-Leitungen und Verbrauchern, Strom, Netzwerk, TK-Anlage u.a. mit High-End-Messsystem TALAN
3. Optischer Lauschangriff: Infrarotmessungen im einsehbaren Fensterbereich
4. Umfassende Analyse der Telefone, Telefonleitungen, der Telefonanlage
5. Untersuchungen mit GSM-Detektor
6. Untersuchungen mit Videokamera-Funkscanner
7. Untersuchung in 3 Schritten der Bausubstanz, der Einrichtungs- und Gebrauchsgegenstände und der Elektrokomponenten mit einem prof. Halbleiterdetektor (NLJD)
8. Kontrolle mittels aktiver & passiver IR-Thermografie von Boden, Wände, Gegenständen

**STORM - SECURE.de**

- **Fachkundig**
- **Zuverlässig**
- **Diskret**

# LEISTUNGSBESCHREIBUNG

## Phase 2 „Wir messen, prüfen & finden“

### B: Prüf- und Testverfahren „visuelle & physische Detektion“

1. Visuelle Überprüfung des gesamten Mobilars (Schränke, Schubladen, Gebrauchs- und Einrichtungsgegenstände inkl. Wände, Decken).
2. Visuelle Überprüfung der PC-Tastaturen und deren Anschlüsse am PC auf suspekten Mitschnittadapter, MIC an Soundkarte, Onlinezugang.
3. Falls Telefon/TAE im Raum, dann werden Telefon, Hörer und Telefonleitung bis zur Telefondose auf Manipulationen, Tapes etc. hin untersucht.
4. Mit Videoskop, Endoskop, Spiegel, Rest-Überprüfung aller schwer zugänglichen Bereiche (Schrankrückseite, abgehängte Decken, Kabel- und Versorgungskanäle, Hohlräume, Heizung, Belüftungs- bzw. Klimaanlage etc.).
5. Mit Kameradetektor den gesamten Raum und die Einrichtungsgegenstände scannen nach verdeckten Kameras & Objektiven aller Art.
6. Einzelüberprüfung mit Metalldetektor aller normalerweise nicht metallischen Gebrauchs- und Einrichtungsgegenstände und Teile der Bausubstanz.
7. Öffnung bzw. intensive Prüfung von Steckdosenleisten, Verteilern, 12-V-/220-Volt Verbrauchern, im Raum befindlichen Steckdosen etc.
8. Detektion von optischen Abhörversuchen: Fensterdurchsichtkontrolle auf das Nachbargebäude & Gelände mittels Nachtsichtgerät, Digitalkamera & Fernglas nach Auffälligkeiten, IR-Sender, Laserabhöranlagen.
9. Visuelle Außenüberprüfung, Außenbereichskontrolle (Geländegang) und mit Metalldetektor insb. der nach außen angrenzenden Raumwände, Fenster auf Stethoskope, Tape, MIC etc
10. Ausbreitungstest von Schallwellen in der Bausubstanz. Wird mit einem Stethoskop überprüft (Boden, Wände, Decken, Klimaanlage, Lüftung, Haustechnik).
- 11. Konkurrenzloser Praxistest „GET-IN-EXTERN“:**  
Öffnungs-Spezialist testet, überwindet und umgeht bestehende Zugangssicherungen, Sicherheitsanlagen & Schutzmaßnahmen mittels prof. Aufsperr- und Manipulationswerkzeugen im Rahmen der Schwachstellenanalyse.
12. Test der TK-Telefonanlage nach verdächtigen ISDN-Leistungsmerkmalen. Test vorh. AB`s und Voice-Mail-Systeme nach Grundkonfiguration, Fernabfragemöglichkeit, Passwort & PIN-Einstellung.
13. Funktionskontrolle bei vorh. Zugangskontrollsystemen, EMA, Türsprechanlagen, Kameras, PIR etc.
14. Dokumentation mittels Digitalkamera von a) Schwachstellen, b) Auffälligem, c) der Raumansicht d) der Aussicht nach draußen durch die Fenster

**STORM - SECURE.de**

- **Fachkundig**
- **Zuverlässig**
- **Diskret**

# LEISTUNGSBESCHREIBUNG

## Phase 3 „Wir schützen & sichern ab“

### Sachverständigen-Gutachten / Konkrete Maßnahmenempfehlungen / Nachhaltige Umsetzung

- 1. Austausch risikoreicher Gegenstände im Einzelfall gegen versiegelte Neuware**
- 2. Versiegelungen aller geprüften Einrichtungsgegenstände & Inventarisierung**

Alle gefährdeten, geöffneten bzw. risikoreichen Gebrauchs- und Einrichtungsgegenstände bzw. Komponenten, technische Einrichtungen bzw. Hohlräume und Kabelkanäle werden nach der „elektronischen & messtechnischen“ und der „visuellen & physischen“ Untersuchung mit einem manipulationssicheren Sicherheitslabel verplombt. Eine nicht sichtbare, unzerstörbare Entfernung dieser Sicherheits-Labels und somit ein mögliches nachträgliches Einbringen von Abhöranlagen ist nicht mehr möglich. Bei Wiederholungsprüfungen wird der Aufwand eines „Abhörschutzeinsatzes“ reduziert. Neu eingebrachte Komponenten werden dadurch erkannt, wenn man regelmäßig die pro Raum von uns erstellte Inventarliste für Vergleichskontrollen mit dem tatsächlichen IST-Bestand gelabelter bzw. ungelabelter Komponenten quercheckt. Die Sicherheits-Labels und die Raum-Inventarliste dienen uns oder dem Kunden als nachhaltige schnelle Kontrollmöglichkeit.
- 3. Bei Fund von Abhöranlagen bekommen Sie eine detaillierte Beschreibung der Funktionsweise und des möglichen Täterkreises**
- 4. Inkl. schriftlichem Sachverständigen-Gutachten durch den Sachverständigen für Abhörschutz & Sicherheitstechnik (BDSF) Jürgen Steimer. Es beinhaltet:**
  - Alle Messprotokolle mit Daten, Bildern, Ergebnissen und verwendeten Messgeräten
  - Erläuterung aller durchgeführten Maßnahmen und verwendeten Checklisten
  - Auflistung organisatorischer und technischer Maßnahmenempfehlungen zur Beseitigung bzw. Verringerung von uns festgestellter Schwachstellen und Risiken
  - Weitere grundsätzliche & nachhaltig erforderlichen Maßnahmen und Empfehlungen zum Schutz gegen Know-how-Abfluss & Missbrauch Ihrer Internas
  - Inventarliste pro Raum mit Übersicht der von uns versiegelten Komponenten



- **Fachkundig**
- **Zuverlässig**
- **Diskret**

# LEISTUNGSBESCHREIBUNG

## Optionale Dienstleistungen, Untersuchungen & Schulungen

- Überprüfung weiterer sicherheitsrelevanter Objekte u.a. **Vorstands-Wohnungen** etc.
- „**Car-Screening**“, prof. Abhörschutz und nachhaltige Absicherungen von Kfz
- „**Handy-Check**“, Soft- und Hardwaretests auf Spy- und Tracking Tools, Versiegelung
- Fachgerechte Außerbetriebnahme von Freisprechmikrofonen bei Telefonen
- **Röntgeninspektion mittels Durchlauf- bzw. Freistrahli-Röntgengerät von:**
  - Telekommunikationsanschlussdosen, Telefonhörern
  - Bausubstanz
  - Dekorations-, Gebrauchs- und Einrichtungsgegenständen
  - Elektro-Kleingeräte (insb. Tastaturen, Taschenrechnern, PC-Mäusen, Radio, Handy
- „**Revision von Videokonferenzanlagen**“: bzgl. widerrechtlicher Zugriffsmöglichkeiten von Innnetägern auf die Konfiguration, Zugriffsmöglichkeiten aus dem Netzwerk, Überprüfung sicherheitskritischer Funktionalitäten bzw. Konfiguration, externe unberechtigte Einwahl etc.
- **Schulung & Sensibilisierung Ihrer Mitarbeiter, Präsentationen, Workshops**
- **Einrichtung sicherer Sprach- und Datenverbindungen (Approved Circuits)**



- **Fachkundig**
- **Zuverlässig**
- **Diskret**