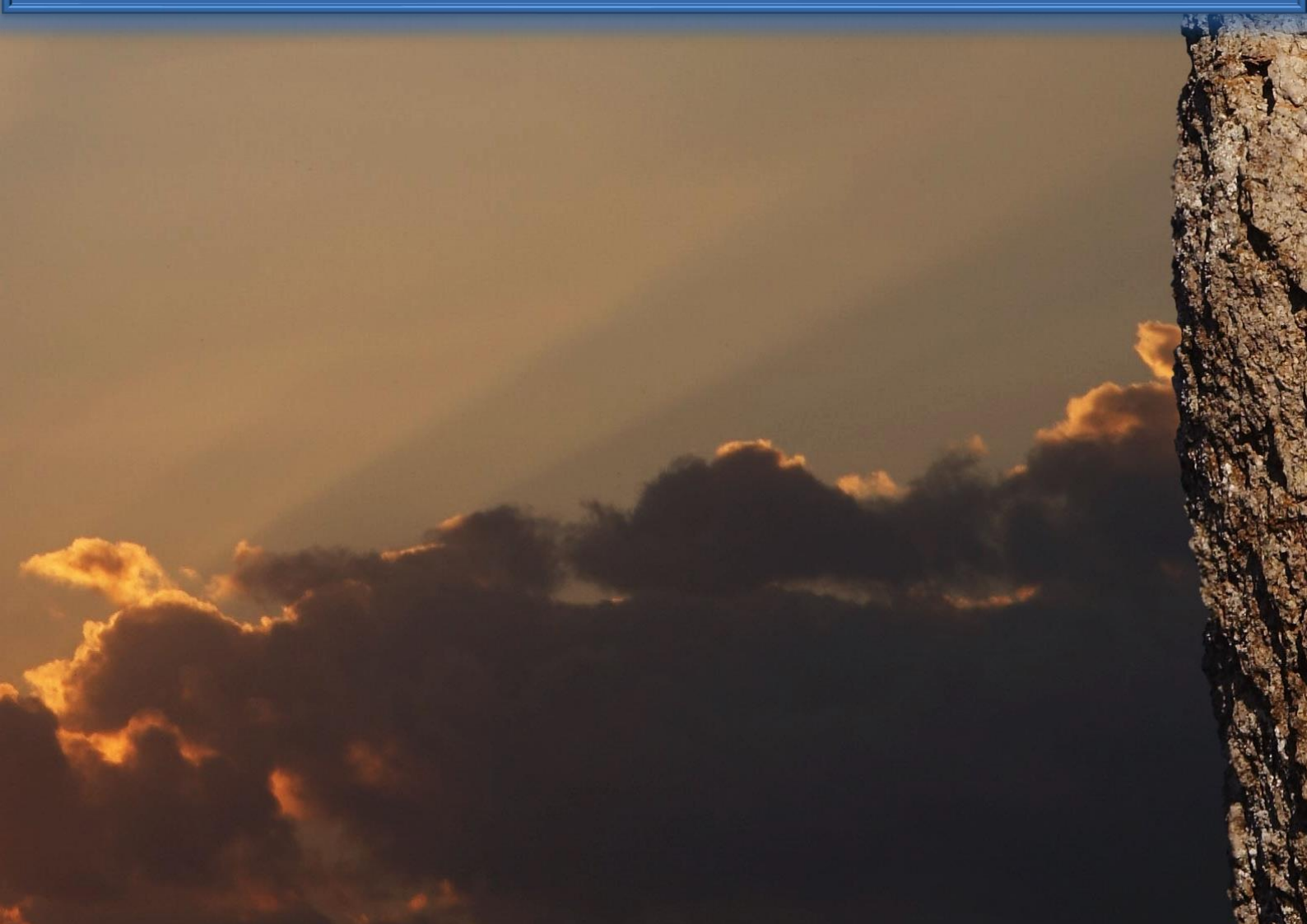


# Focus Control



## SPECIFICATIONS



# SPECIFICATIONS

---

## Service description "effective eavesdropping protection in 3 phases"

Below you will find an overview with detailed service descriptions, how our team works and which methods we use to effectively locate and neutralize all types of active and passive listening devices. The degree of security based on our equipment used is 98% (as of April 2019) that we will find what we are looking for. The ECM Ground Check is carried out according to tested methods and standards with at least 5 redundant (overlapping) inspection and test procedures in the field of "electronic & metrological examinations". These are supplemented by 13 further inspection and test procedures in the field of "visual & physical detection". We examine according to military standards and basically assume extremely prof. perpetrators, whose focus is industrial espionage with the help of state agencies, who have access to intelligence technologies and who have unlimited means at their disposal.

## Basic organizational process

After placing the order:

We will send you a complete information package (basic recording, process organization, to-do checklist, etc.) to a neutral, secure address. Alternatively, we arrange an appointment outside the company or at your site in a non-endangered area of the company for the basic recording and the discussion of the further process organization. Among other things, concrete deployment dates are discussed, questions answered, rooms to be examined and your desired focal points determined. Furthermore, you will receive a to-do checklist to ensure a smooth process on both sides.

On site at your premises:

On the basis of the process organization, we will enter your company discreetly and neutrally in the presence of one of your employees. We are then shown all rooms to be examined, and access to the PBX, server room and neighboring rooms must also be accessible. We will then proceed according to the schedule and bring our equipment (about 15 suitcases) into the rooms to be examined and set up our measuring stations.

Final meeting:

We arrange an appointment for the final discussion and handover of expert opinions outside the company or in a non-endangered area of the company.

# SPECIFICATIONS

## Phase 1 "We plan and analyze"

### **Identification of risks / safety analysis according to Kaizen / status quo determination by using various checklists, among others:**

1. Carrying out an in-depth vulnerability analysis of the attack techniques and possible targets in the premises to be examined. Check of internal security standards.
2. Checklist Detailed examination of the rooms including utilities, technical facilities, telecommunications and IT facilities, complete equipment and furnishing items as well as all interfaces to the outside.
3. Examination of technical & organizational measures, existing vulnerabilities with risk identification, all attack possibilities, access, access and access options, etc. according to § 9 BDSG. Checking the flow interfaces for security risks.

## Phase 2 "We measure, test and find"

### **Active eavesdropping / Localization & deactivation of eavesdropping systems / Metrological investigations**

The ECM-Ground-Check is carried out according to tested methods and standards with at least 5 redundant (overlapping) inspection and test procedures in the field of "electronic & metrological examinations". These are supplemented by 13 further inspection and test procedures in the field of "visual & physical detection". All scans and tests are carried out by an expert for eavesdropping protection and a technical employee with a time delay (test-retest method) to check the reliability of the measurement results (consistency test).

#### A: Inspection and test procedures "electronic & metrological examinations"

1. High-frequency measurements: inspection of sensitive rooms and individual components
2. Long-wave measurements & line verification on 220-volt lines and consumers, electricity, network, PBX etc. with high-end measuring system TALAN
3. Optical eavesdropping: infrared measurements in the visible window area
4. Comprehensive analysis of telephones, telephone lines, telephone system
5. Investigations with GSM detector
6. Examinations with video camera wireless scanner
7. Examination in 3 steps of the building fabric, the furnishings and utensils and the electrical components with a prof. semiconductor detector (NLJD)
8. Control by means of active & passive IR thermography of floor, walls, objects

# SPECIFICATIONS

---

## Phase 2 "We measure, test and find"

### B: Inspection and test procedure "visual & physical detection"

1. Visual inspection of all furniture (cupboards, drawers, utensils and furnishings including walls, ceilings).
2. Visual inspection of PC keyboards and their connections on the PC for suspicious recording adapters, MIC to sound card, online access.
3. If telephone/TAE in the room, then telephone, receiver and telephone line up to the telephone socket are examined for manipulations, tapes, etc.
4. With videoscope, endoscope, mirror, residual inspection of all hard-to-reach areas (cabinet back, suspended ceilings, cable and supply ducts, cavities, heating, ventilation or air conditioning, etc.).
5. With camera detector, scan the entire room and furnishings for hidden cameras & lenses of all kinds.
6. Individual inspection with metal detector of all normally non-metallic utensils and furnishings and parts of the building fabric.
7. Opening or intensive testing of socket strips, distributors, 12 V/220 volt consumers, sockets in the room, etc.
8. Detection of optical eavesdropping attempts: Window inspection of the neighboring building & grounds by means of night vision device, digital camera & binoculars for abnormalities, IR transmitters, laser eavesdropping systems.
9. Visual exterior inspection, outdoor control (off-road) and with metal detector esp. of the adjoining room walls, windows on stethoscopes, tape, MIC, etc.
10. Propagation test of sound waves in the building fabric. Checked with a stethoscope (floor, walls, ceilings, air conditioning, ventilation, home automation).
11. Unrivalled practical test "GET-IN-EXTERN":  
Opening specialist tests, overcomes and circumvents existing access guards, security systems & protective measures using prof. unlocking and manipulation tools as part of the vulnerability analysis.
12. Test of the PBX for suspicious ISDN features. Test vorh. AB's and voice-mail systems according to basic configuration, remote query option, password & PIN setting.
13. Functional control at vorh. Access control systems, EMA, door intercoms, cameras, PIR etc.
14. Documentation by means of a digital camera of a) weak points, b) conspicuous, c) the room view d) the view outside through the windows.

# SPECIFICATIONS

Phase 3 "We protect and secure"

**Expert reports / Concrete recommendations for measures / Sustainable implementation**

**1. Exchange of risky items in individual cases for sealed new goods**

**2. Sealing of all tested furnishings & inventory**

All endangered, opened or high-risk utensils and furnishings or components, technical equipment or cavities and cable ducts are sealed with a tamper-proof security label after the "electronic & metrological" and the "visual & physical" examination. An invisible, indestructible removal of these security labels and thus a possible subsequent introduction of eavesdropping systems is no longer possible. In the case of repeat tests, the effort of a "eavesdropping protection operation" is reduced. Newly introduced components are recognized by regularly cross-checking the inventory list created by us for comparison checks per room with the actual stock of labeled or unlabeled components. The security labels and the room inventory list serve us or the customer as a sustainable quick control option.

**3. If eavesdropping devices are found, you will receive a detailed description of the functionality and the possible circle of perpetrators**

**4. Incl. written expert opinion by the expert for eavesdropping protection and security technology (BDSF). It includes:**

- All measurement protocols with data, images, results and measuring instruments used
- Explanation of all measures carried out and checklists used
- List of organizational and technical recommendations for measures to eliminate or reduce weaknesses and risks identified by us
- Further basic & sustainably necessary measures and recommendations to protect against know-how leakage & misuse of your internal information
- Inventory list per room with overview of the components sealed by us

# SPECIFICATIONS

## Optional Services, Examinations & Training

- Review of other security-relevant properties, including board apartments, etc.
- "Car-Screening", prof. eavesdropping protection and sustainable protection of motor vehicles
- "Handy-Check", software and hardware tests on spy and tracking tools, sealing
- Professional decommissioning of hands-free microphones on telephones
- X-ray inspection by means of continuous or free-jet X-ray equipment from:
  - Telecommunications sockets, telephone receivers
  - Building
  - Decoration, utensils and furnishings
  - Small electrical appliances (esp. Keyboards, calculators, PC mice, radio, mobile phone)
- **"Revision of video conferencing systems": with regard to unlawful access possibilities of internal offenders to the configuration, access options from the network, checking security-critical functionalities or configuration, external unauthorized dial-up, etc.**
- **Training & sensitization of your employees, presentations, workshops**
- **Establishment of secure voice and data connections (Approved Circuits)**

