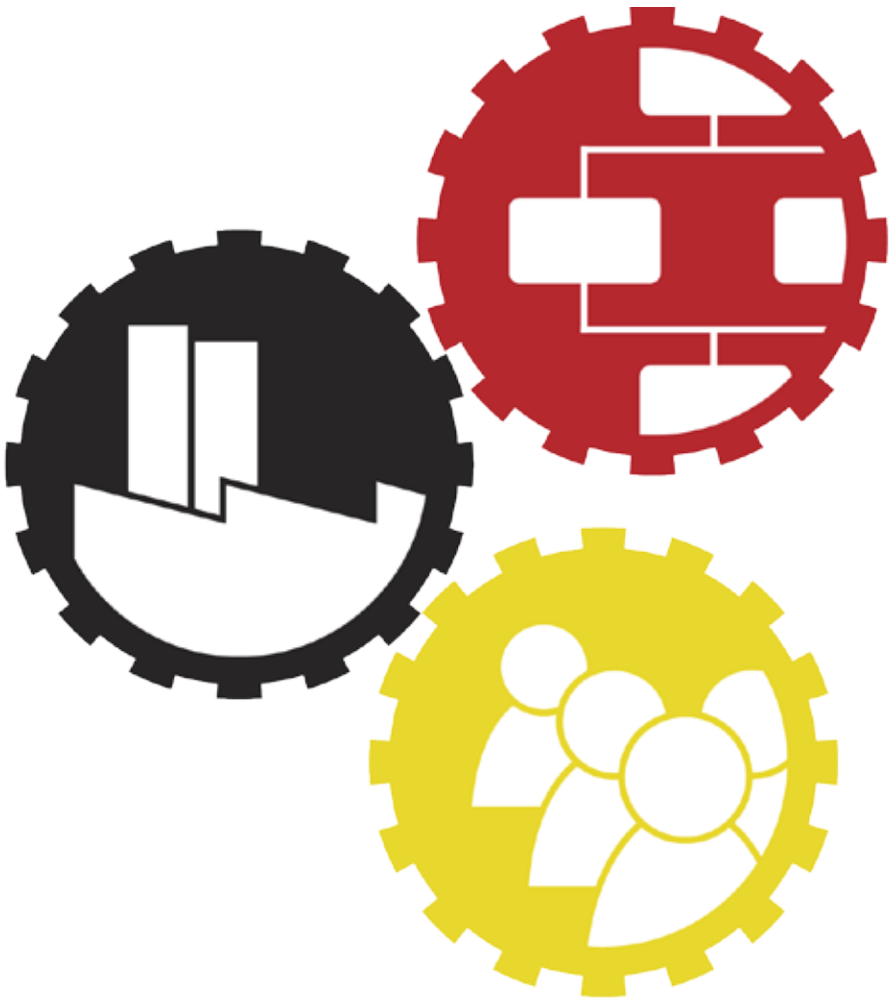
ASW
Bundesverband

Wirtschaftsgrundschutz

Baustein IS2 Lauschabwehr



Disclaimer

Der Baustein „IS2 Lauschabwehr“ ist in der alleinigen Autorenschaft des ASW Bundesverbandes entstanden und erscheint ohne die Beteiligung der beiden Bundesbehörden BSI und BfV. Vorgaben zum Schutz von staatlich geheim zu haltenden Verschlusssachen unterliegen gesonderten Vorschriften des Bundes und der Länder. Die hier dargelegten Anforderungen können davon abweichen und sind nicht mit den Vorgaben im staatlichen Geheimschutz gleichzusetzen.

1 Relevanzentscheidung für diesen Baustein

- **Fordern Kunden oder Partner Lauschabwehrüberprüfungen durchzuführen?**
- **Bestehen vertragliche Verpflichtungen zum sicheren Umgang mit Informationen?**
- **Beschäftigt sich die Institution mit Hochtechnologie (z. B. im Bereich Rüstung, Luft- und Raumfahrt, Mikroelektronik, Nanotechnologie, Chemie, Pharma)?**
- **Ist die Institution als „kritische Infrastruktur" einzustufen?**
- **Gehört die Institution zu den Marktführern der Branche?**
- **Stützt sich das Geschäftsmodell der Institution auf exklusives Know-how oder exklusive Technologien?**
- **Bewegt sich die Institution in einem Markt mit nur wenigen Anbietern?**
- **Spielt die Institution eine bedeutsame Rolle in der internationalen Finanzwirtschaft?**
- **Betreibt die Institution eine aggressive Expansionspolitik?**
- **Gab es in der Institution Fälle unerklärlicher Informationsabflüsse oder Lauschangriffe?**

Der Kampf um den Rohstoff Wissen ist in vollem Gange. Im Fokus steht grundsätzlich jedes Unternehmen mit nennenswertem Budget und aktiver Konkurrenz.

globaler Konkurrenzkampf

Abhören ist die neue Waffe im globalen Konkurrenzkampf. Die aktuellen Enthüllungen über Abhörpraktiken und Lauschangriffe lassen aufhorchen und machen heute mehr denn je bewusst, dass

grundsätzlich jedes Unternehmen davon betroffen sein kann. Für jede innovative Institution zählt es zu den höchsten Bedrohungen, wenn ihr Know-how an die Wettbewerber abfließt. Für betroffene Organisationen sinken der Wettbewerbsvorteil und die Konkurrenzfähigkeit.

Ebenso folgenschwer ist die Ausspähung von Angebotsunterlagen und Preisen bei Aufträgen. Betroffenen ist die Intensität der wirtschaftlichen Bedrohung mitunter nicht bewusst.

Das Abhören und Anzapfen von Besprechungen und Telefonaten ist für kriminell agierende Wettbewerber schon immer ein attraktiver Weg um an Informationen zu gelangen. Die kontinuierliche Weiterentwicklung miniaturisierter Überwachungselektronik macht Lauschangriffe immer einfacher und führt zu einer Erhöhung der Abhörrisiken. Die Technik wird immer günstiger und kann mittlerweile auch von Laien bedient werden. Das Einbringen von Abhöreinrichtungen ist oft schnell und ohne größeren Aufwand möglich. Die Menge und Varianten der erhältlichen Abhöreinrichtungen nehmen mittlerweile besorgniserregende Ausmaße an.

unterschätzte Bedrohung

Die Gefährdung durch klassische Lauschangriffe wird von vielen Institutionen häufig unterschätzt und nicht als echte Bedrohung wahrgenommen. Viele Präventionsstrategien sind unterentwickelt oder nur auf Teilaspekte wie die IT-Infrastruktur ausgerichtet. Das Szenario Lauschangriff wird mitunter kaum in die Betrachtung einbezogen. Nach wie vor werden jedoch die geheimsten Informationen mündlich ausgetauscht, und die Angreifer wissen genau, wo es sich zu lauschen lohnt.

Oftmals sind Lauschangriffe nicht direkt wahrnehmbar, sondern nur deren Auswirkungen. Oft mit ruinösen Folgen für die betroffene Institution.

Die Bedrohung ist viel konkreter, als der Öffentlichkeit bisweilen bekannt ist. Lauschangriffe haben sich in den letzten Jahren zu einem globalen Geschäftsmodell entwickelt. Als Auftraggeber für Konkurrenzausspähung und Know-how-Beschaffung gelten Konkurrenten aus dem In- und Ausland, aber auch eigene Kunden, potentielle Partner, Newcomer oder Einsteiger aus anderen Branchen.

Die Verwendungszwecke der erbeuteten Informationen sind vielfältig. Sie reichen von der Einsparung der eigenen Entwicklungskosten über die Vorteilsbeschaffung bei Aufträgen oder Ausschreibungen, die private und geschäftliche Erpressbarkeit, Know-how- und Erfindungsdiebstahl sowie Patentbetrug bis zu Sabotage und Behinderung.

Vorbereitung und Sensibilisierung

Lauschabwehr bedarf deshalb einiger grundsätzlicher Regelungen und Vorbereitungen durch die Institution sowie in hohem Maße durch die Geheimnisträger selbst. Umso wichtiger ist daher, dass es neben Regelungen auch Sensibilisierungsmaßnahmen für Geheimnisträger in einer Institution gibt, um besonders kritische Daten, etwa die der Vorstandsebene oder der Bereiche Finance, Strategie, Forschung und Entwicklung vor Lausch- und Spähangriffen zu schützen.

Dieser Baustein liefert Verantwortlichen einer Institution eine Hilfestellung für eine strukturierte Vorgehensweise zur Erreichung einer angemessenen Lauschabwehr und zeigt die wesentlichen Grundsätze für dessen Etablierung.

2 Beschreibung

Unter Lauschabwehr wird die Gesamtheit aller Maßnahmen verstanden, um das Abhören (Mithören) von Gesprächen zu verhindern. Diese erstrecken sich auf den Schutz persönlich im Raum und mittels Telekommunikationstechnik geführter Gespräche sowie auf die Sicherheit übermittelter Daten.

Um Lauschangriffen entgegenzuwirken, sind sensible Gespräche und Informationen mit angemessenen Schutzmaßnahmen zu versehen. Die Etablierung eines Managements für Abhörsicherheit bietet in diesem Zusammenhang einen systematischen Ansatz, um geeignete Vorsorgemaßnahmen zum Schutz von vertraulichen Informationen zu identifizieren und umzusetzen.

Zielsetzung der Lauschabwehr

Zielsetzung ist es, den für eine Abhöraktion (von sensiblen Informationen) erforderlichen Aufwand derart zu erhöhen, dass die Ergebnisse in keinem inhaltlich oder zeitlich vertretbaren Verhältnis dazu stehen.

Lauschabwehr reicht von der Planung und dem Bau von abhörsicheren Räumlichkeiten und Kommunikationsleitungen und dem gezielten Suchen von Abhörgeräten (aktive Lauschabwehr oder auch „Sweep“ genannt) über sichere Kommunikation mithilfe von Kryptographiegeräten bis zur Schulung und Sensibilisierung der Geheimnisträger.

3 Gefährdungslage

Die Methoden von Lauschangriffen sind äußerst vielfältig und reichen vom Lauschen an der Tür über manipulierte Telefone und Funkwanzen bis hin zum Einsatz von Laserabhörgeräten.

wachsende Angriffsmöglichkeiten

Die Entwicklung der Abhörtechnik schreitet bei den weltweit mehreren hundert Anbietern schnell voran. „Wanzen“ in der Größe eines Streichholzkopfes sind keine Seltenheit mehr. Wegen der hohen Verfügbarkeit und einfachen Beschaffungsmöglichkeit illegaler Lauschmittel über das Internet muss bereits bei semiprofessionellen Tätern mit raffinierten Angriffen gerechnet werden. Im Bereich der drahtlosen Abhörtechnik ist eine vermehrte Zweckentfremdung hochwertiger Standard-Funkübertragungsverfahren (wie z. B. Mobilfunk, WLAN, Bluetooth) zu beobachten. Durch die zunehmend IP-basierten und drahtlosen IT- und TK-Systeme wachsen die Angriffsmöglichkeiten auf Netze und Endgeräte.

Viele Präventionsstrategien sind unterentwickelt oder nur auf Teilaspekte wie die IT-Infrastruktur ausgerichtet. Angreifer nutzen alle ihnen zur Verfügung stehenden Mittel zur Informationsgewinnung, seien sie noch so trivial. Es gilt der Grundsatz, je einfacher, umso effektiver.

Die Angriffswege lassen sich in die folgenden wesentlichen Bereiche gliedern:

- Angriffe auf visuelle Informationen
- Angriffe auf Gespräche im Raum

- Angriffe auf Telekommunikationseinrichtungen und -leitungsnetze im Haus
- Angriffe auf öffentliche Netze
- Angriffe auf die Mobilkommunikation

Folgende Gefährdungen sind im Rahmen von Lauschangriffen von besonderer Relevanz:

G 1 Einblicknahme in Gebäude von außen (z. B. Fernrohr oder Teleobjektiv)
G 2 Einbau verdeckter Videokameras in Räumen
G 3 Einsatz von Flugdrohnen mit Videokamera
G 4 Angriffe auf Videokonferenzanlagen und PC-Kameras
G 5 Audiorekorder ohne Übertragung nach außen
G 6 Anzapfen von Lautsprechern und Durchsageanlagen
G 7 Zweckentfremdung regulärer Medientechnik (Mikrofone)
G 8 Einbau verborgener Mikrofone mit leitungsgebundener Übertragung
G 9 Platzierung von Miniatursendern aller Art (Funkwanzen)
G 10 Geräte zur optischen Übertragung nach außen (z. B. mit IR-Licht)
G 11 Einsatz optischer Abhöranlagen von außen (z. B. Laser)
G 12 Körperschallmikrofone (Körperschall/Schalldämmung an der Fassade oder Wandrückseite)
G 13 Angriffe auf Freisprecheinrichtungen, Videokonferenzanlagen und PC-Mikrofone (z. B. in Headsets) und Funkmikrofone
G 14 Anschluss kleiner Computer mit Abhörsoftware am LAN
G 15 Anschluss von WLAN-Accesspoints am LAN
G 16 Anzapfen von Telefonleitungen und Fax
G 17 Anschluss von Miniatursendern an bzw. in TK-Einrichtungen
G 18 Manipulation der Konfiguration von Kommunikationsservern
G 19 Überwachung von Satellitenverbindungen
G 20 Anzapfen von Überseekabeln
G 21 Abhören terrestrischer Richtfunkverbindungen
G 22 Abhören über offizielle Schnittstellen der Provider
G 23 Überwachung der Satellitenverbindung bei THURAYA, INMARSAT, IRIDIUM etc.
G 24 Überwachung der (Funk-)GSM-/UMTS-/LTE-Luftschnittstellen (z. B. mittels „IMSI-Catcher“)

G 25 Angriffe über Bluetooth- und WLAN-Schnittstellen

G 26 Übermittlung oder Download von Schadsoftware

G 27 Lokale Installation von Schadsoftware („Spyware“, z. B. Trojaner)

G 28 Hardwaremanipulation (z. B. Akku mit separatem Minisender)

4 Maßnahmen

Lauschabwehrmaßnahmen und Sensibilisierung

Lauschabwehrmaßnahmen und Sensibilisierung sind ein wesentlicher Erfolgsfaktor für die Erreichung und Aufrechterhaltung eines angestrebten Sicherheitsniveaus.

Die Institution legt ein Prozessmodell fest, das eine angemessene Lauschabwehr zum Ziel hat. Mit dem Prozessmodell sind die grundlegenden Aufgaben zur Entwicklung eines Lauschabwehrkonzepts beschrieben. Dies umfasst die Festlegung von Verantwortlichkeiten und Rollen ebenso wie die Dokumentation und eine längerfristige Planung. Letztere stellt sicher, dass die Maßnahmen aufeinander aufbauen und zielgerichtet durchgeführt werden."

Der Betriebsprozess für die Lauschabwehr ist als klassischer Regelkreis ausgelegt. Die Maßnahmen folgen hierbei dem Plan-Do-Check-Act-Regelkreis und unterteilen sich in die folgenden drei wesentlichen Prozessblöcke:

- **Führungsprozess**
- **Betriebsprozess (Planung, Umsetzung, Überprüfung, Verbesserung)**
- **Berichts-/Kontrollwesen**

Abbildung 1 stellt dies grafisch dar.

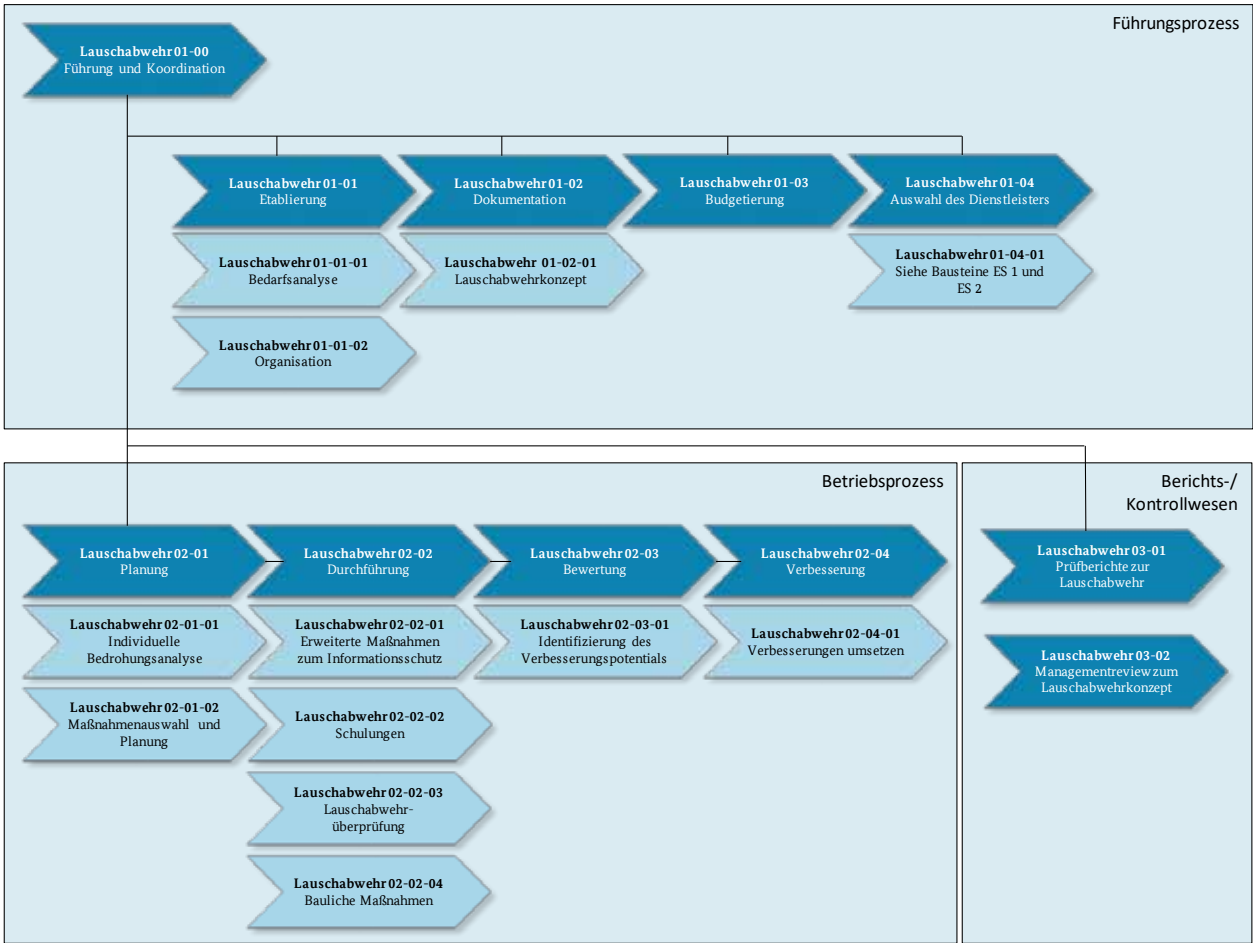


Abbildung 1: Prozessdiagramm Lauschabwehr

Die **Maßnahmen** dieses Bausteins sind **in drei Kategorien eingeteilt**. Sie richten sich nach dem **erforderlichen Detailgrad** bzw. der **gewünschten Ausprägung** (siehe Relevanzentscheidung) auf Basis der Anwendungsentscheidung gemäß Standard 200-1:

A-Kategorie – Basismaßnahmen: unabdingbarer Wirtschaftsgrundschutz
B-Kategorie – Standardmaßnahmen: vollständiger Wirtschaftsgrundschutz
C-Kategorie – erweiterte Maßnahmen: erweiterter Schutz bei hohem Risikopotential

M 1 Verantwortung der Institution (A)

Die Sicherstellung eines angemessenen Schutzes vor Lauschangriffen obliegt der Leitung der Institution. Diese delegiert die damit zusammenhängenden Aufgaben an einen Verantwortlichen zur Umsetzung.

Verantwortung der Leitung

Laut der Richtlinie über Netz- und Informationssicherheit („NIS-Richtlinie“) sowie der Richtlinie 2013/40/EU über Angriffe auf Informationssysteme müssen ab 2018 alle Unternehmen in der Europäischen Union präventive Maßnahmen zur Bekämpfung der Industriespionage intern selbst umsetzen.

M 2 Identifizieren des Schutzbedarfs (A)

Die Institution identifiziert relevante Personen, Geschäftsbereiche und Räumlichkeiten, die einem erhöhten Schutzbedarf unterliegen und den Aufwand für Lauschabwehrmaßnahmen rechtfertigen.

Bei der Schutzbedarfsanalyse werden folgende Aspekte berücksichtigt:

Schutzbedarf

- **Ermittlung der Bedrohungslage durch entsprechende Analysen**
  - Wie groß ist mein Schaden bei Informationsverlust?
  - Wer sind die potentiellen Angreifer (Konkurrenz, Geheimdienste, Erpresser…)?
- **Welche Informationen sind besonders zu schützen?**
  - eindeutige Identifizierung und Klassifizierung des Unternehmens-Know-hows
- **Welche Personengruppen und Bereiche sind besonders zu schützen?**
  - z. B. Vorstandsebene oder die Bereiche Finance, Strategie, Forschung und Entwicklung, Aufsichtsrat, Betriebsrat
- **Gibt es anlassbezogenen Schutzbedarf (Projekte, Patentverfahren, Angebotsphase)?**
  - z. B. Patentanmeldung, Mergers & Acquisitions, Marketingkonzepte, Angebotsverfahren

M 3 Definieren eines Lauschabwehrkonzepts (A)

Die Institution definiert ein Lauschabwehr- und Sensibilisierungskonzept. Sie legt hierin Rahmenbedingungen, bspw. Ziele, Verantwortlichkeiten und Vorgehensweisen, fest.

Lauschabwehrkonzept

Bei der Entwicklung des Konzepts werden folgende Aspekte berücksichtigt:

- **Welche Schutzmaßnahmen sind für welchen Anwendungsfall vorgesehen und angemessen?**
  - z. B. Schulung für Geheimnisträger, Vorstände, Entwicklungsabteilung
  - Ist die Einführung von Kryptotechnik für bestimmte Bereiche (Kryptophone, E-Mail-Verschlüsselung, High-Secure-Notebooks etc.) notwendig?
  - ggf. Festlegen von Schutzbereichen und Zonen, bauliche Maßnahmen (z. B. abhörgeschützte oder abhörsichere Räume) und erweiterte Zutrittsregelungen (z. B. auch für Service- und Reinigungskräfte)
  - regelmäßige Lauschabwehrüberprüfungen für bestimmte Personen oder Bereiche
- **Festlegung klarer Anweisungen für Lauschabwehr**
- **In welchen Abständen werden welche zusätzlichen Schutzmaßnahmen wo durchgeführt?**

Bei der Planung sollte berücksichtigt werden, dass es in den meisten Fällen nicht sinnvoll ist, ganze Bürogebäude auf Abhöreinrichtungen zu untersuchen. Stattdessen sollten die besonders gefährdeten Bereiche und Personen festgelegt und betrachtet werden.

Das Konzept muss die Personen und Bereiche dauerhaft schützen. Ein durchgeführter „Sweep“ beispielsweise stellt immer nur eine Momentaufnahme dar und somit nur eine Beurteilung der Lage zum Zeitpunkt der Überprüfung. Daher kann es sinnvoll sein, diesen in regelmäßigen (bzw. auch unregelmäßigen) Zeitabständen oder bei Bedarf (z. B. vor und während wichtiger Besprechungen) zu wiederholen. Auch das Errichten eines sogenannten „Warrooms“, der für sensible Besprechungen herangezogen werden kann und unter besonderer

Aufsicht steht, erleichtert den dauerhaften Schutz und reduziert somit langfristig Aufwand und Kosten.

M 4 Umsetzen erweiterter Maßnahmen im Bereich der Informations- und Kommunikationstechnik (A)

erweiterte Maßnahmen

Die Institution nutzt für die Umsetzung von Maßnahmen in der Informations- und Kommunikationstechnik die Hinweise und Empfehlungen des IT-Grundschutzes. Neben den dort geführten allgemeinen Empfehlungen zur IT-Sicherheit empfiehlt es sich, im Hinblick auf die Lauschabwehr weitergehende Maßnahmen umzusetzen, wie beispielsweise:

1. generelle Pflicht zum **offenen Tragen der Betriebsausweise**
2. **Clear-Desk-Policy**
3. Durchführung gesetzeskonformer **Taschen- und Einlasskontrollen**
4. Festlegung **restriktiver Zugangsberechtigungen** für Personal, Besucher und Fremdfirmen
5. **eindeutige Festlegung des Umgangs mit Besuchern** (Abholung am Empfang, Erfassung, Ausweisprüfung, Besucherscheine, Empfangsregelungen bzw. -verbote für Büroräume usw.)
6. genereller **Verzicht auf Outsourcing in sicherheitsrelevanten Bereichen**
7. Durchführung von **Servicearbeiten und Reinigungsarbeiten in gefährdeten Bereichen nur unter Aufsicht**
8. Einsatz **hochwertiger, lokal platzierter Aktenvernichter** (mind. Sicherheitsstufe 4)
9. **Verzicht auf Aktenvernichtung außer Haus** durch externe Dienstleister
10. **Entsorgungskonzept durch sicheren Abtransport und Vernichtung jederart Datenträger**
11. **Verzicht auf zentral aufgestellte Etagendrucker und -kopierer**
12. Festlegung **eindeutiger Regelungen für die Handhabung defekter Festplatten** von Computern und Großkopierern
13. **Verbot, mobile Endgeräte aus den Händen zu geben**
14. **Verzicht auf drahtlose Technologien** (WLAN, Wireless-USB, Bluetooth, ZigBee, Wibree usw.)

15. **generelles Verbot mobiler TK-Endgeräte** (GSM, UMTS, LTE, DECT) beim Führen vertraulicher Gespräche
16. **Verbot von Funktastaturen in sensiblen Bereichen**
17. **Verzicht auf drahtlose Medientechnik** (z. B. Funkmikrofone, IR-Headsets)
18. besondere **Vorsicht bei der Nutzung fremder Infrastruktur** (LAN-Verkabelung, Switches, Router, WLAN-Netze usw.)
19. **konsequentes Verbot der Nutzung fremder Datenträger** (USB-Sticks, ext. HDD, CD/DVD)

Die Institution identifiziert die für sie sinnvollen weitergehenden Maßnahmen zum Schutz der verwendeten Informations- und Kommunikationstechnik. Sie überführt die identifizierten Maßnahmen in die bestehenden Sicherheitskonzepte.

M 5 Durchführen von Schulungen und Sensibilisierungsmaßnahmen (A)

Die Sensibilisierung der Mitarbeiter hinsichtlich des Szenarios Lauschangriff stellt einen wichtigen Teil des Informationsschutzes dar und berücksichtigt auch übergreifende Bereiche (wie z. B. Social Engineering, Informationsschutz auf Reisen und die Erschwerung der Informationsbeschaffung aus öffentlichen Quellen), da Schutzmaßnahmen im Hinblick auf das gesprochene Wort nur einen Teil der Gesamtrisiken für Informationsabflüsse abdecken.

Die **Schulungen umfassen im Wesentlichen**:

- **Verhalten als Geheimnisträger** und mögliche Angriffspunkte
- **Sensibilisierung** für Informationsabflussrisiken
- **Information über potentielle Lauschangriffe** und Methoden
- Hinweise bezüglich **vorbeugender Lauschabwehrmaßnahmen**
- **Verhalten auf Reisen**

M 6 Budgetierung Lauschabwehr (B)

Maßnahmen zur Lauschabwehr sind zu budgetieren. Der Zeitaufwand und somit auch die Kosten für einen zu untersuchenden Raum richten sich immer nach dessen Beschaffenheit hinsichtlich Fläche, Ausstattung (je mehr Möbel, Zwischendecken, Kabelkanäle etc. vorhanden sind, desto mehr Aufwand), angrenzende neben/unter/über dem Gefahrenbereich liegende Bereiche.

M 7 Auswahl eines geeigneten Dienstleisters für Lauschabwehrüberprüfungen (B)

geeignete Dienstleister

Umfassende Maßnahmen zur Auswahl von geeigneten Dienstleistern können den Wirtschaftsgrundschutzbausteinen ES1 – Integritätsprüfung externer Parteien sowie ES2 – Auswahl und Steuerung von Sicherheitsdienstleistungen entnommen und im Rahmen der Auswahl von Dienstleistern für Lauschabwehrüberprüfungen angewendet werden. Zusätzlich sollten folgende Aspekte beachtet werden:

- Setzt der Dienstleister entsprechende **Ausrüstung und Prüfverfahren gemäß M8** ein?
- Gibt es eine **ausführliche und transparente Leistungsbeschreibung**?
- **Enthält** das **Leistungsangebot** die **Mindestanforderungen für eine Lauschabwehrüberprüfung** (Anforderungen: siehe M8: Lauschabwehrüberprüfung)?
- Sind die **veranschlagten Zeitaufwendungen realistisch** (wenige m² pro Mannstunde bei hohen Sicherheitsanforderungen)?
- Besteht eine **angemessene Relation von Preis und Leistung**?

Neben qualifizierten Dienstleistern befinden sich auf dem Markt für Lauschabwehrprüfungen auch zahlreiche unseriöse Anbieter. Die Gefährdungen G7 und G11 des Bausteins ES1 sowie die Maßnahme M15 des Bausteins ES2 haben dabei eine besonders hohe praktische Relevanz. Referenzen über in Betracht kommende Anbieter können z. B. bei Sicherheitsfachverbänden eingeholt werden.

M 8 Durchführen von Lauschabwehrüberprüfungen (B)

In besonders sensiblen Bereichen wird empfohlen, regelmäßig Lauschabwehrüberprüfungen durchzuführen. Dabei ist auf die Auswahl eines entsprechenden qualifizierten Dienstleisters zu achten (Anforderungen: siehe M7: Auswahl eines geeigneten Dienstleisters).

Lauschabwehrüberprüfungen sollten folgende Maßnahmen umfassen:

- **Organisation von Lauschabwehrüberprüfungen:** Beratung und Risikoanalyse zusammen mit der Institution. Festlegung von Überprüfungsflächen, Zeitpunkt, Teilnehmern, Überprüfungs- und Folgemaßnahmen. Nach der Überprüfung werden die Prüfergebnisse mit der Institution besprochen und Empfehlungen ausgesprochen.
- **visuelle Überprüfung des Raums:** visuelle Überprüfungen der Räume und angrenzenden Bereiche, einschließlich Decken, Fenstern, Türen, Wänden, Böden, Bodentanks, Möbeln und Inventar, Schächten, Kanälen, elektrischen Geräte, Außenbereichen etc., unter Zuhilfenahme optischer Hilfsmittel (z. B. Video-Endoskop, Inspektionsspiegel etc.). Auf Wunsch Versiegelung der überprüften Geräte und Einrichtungen. Die Siegel dürfen nicht zerstörungsfrei entfernt werden können und müssen eindeutig zu identifizieren sein.
- **Halbleiterdetektion zur Lokalisierung elektronischer Bauteile:** Detektion aktiver und nicht aktiver elektronischer Baugruppen zur Lokalisierung inaktiver Abhöreinrichtungen durch Einsatz eines non-linear Junction Detectors
- **Überprüfung des Hochfrequenzspektrums (HF-Messung):** Überprüfung des Funkspektrums bis in einen hohen GHz-Bereich mittels Differenzspektrumanalyse inkl. Mobilfunk, WLAN und Bluetooth, Überprüfung der DECT-Infrastruktur und der Trägerfrequenzen auf dem Stromnetz (Babyphone). Zum Einsatz kommen Spektrumanalyzer, Messempfänger, Peileinrichtungen sowie Nahfeld- und Magnetfeldsonden.
- **Infrarotanalyse:** Überprüfung des Raums auf Übertragungseinrichtungen im Infrarotbereich mittels Infrarotkamera
- **Anwendung von Thermographie:** aktive und passive Thermografie zur Erkennung von Inhomogenitäten in der

Bausubstanz und zur Detektion eingeschalteter elektronischer Baugruppen

- **Leitungsüberprüfung von Inhouse-Netzen:** messtechnische Überprüfung von Inhouse-Netzen, Kommunikationsleitungen und Verteilern auf Fremdsignale, Manipulationen und Abhöreinrichtungen (z. B. mit Time-Domain-Reflectometer, LAN-Analyzer, Multimeter, Oszilloskop, Langwellenempfänger, Audio-Verstärker). Visuelle Überprüfungen der Inhouseleitungen im lokalen Netz, einschließlich aller relevanten Verteiler und Abschlusseinrichtungen und Verifizierung des vorhandenen Leitungsnetzes.
- **zerstörungsfreie Überprüfung mittels Röntgentechnik:** beschädigungsfreie Überprüfung nicht zu öffnender Gegenstände und technischer Geräte mittels hochauflösender digitaler Röntgentechnik. Hierbei sollte je nach Erfordernissen des Anwendungsbereichs (z. B. bei komplexen elektronischen Geräten) geprüft werden, welche Röntgentechnologie einzusetzen ist.
- **Konfigurationsanalyse von TK-Anlagen:** Hierunter sind alle Überprüfungen zusammengefasst, die sich auf eine Manipulation der Telefonanlage und ihrer Endgeräte beziehen. Softwaremanipulationen, illegale Features, manipulierte Leistungsmerkmale, Backdoors der Hersteller, Missbrauch der Fernwartungszugänge und illegale Zugriffsmöglichkeiten aus dem LAN. Zugang zu den Bedienterminals, Sicherungsdateien und Zugang zu den Daten und Räumlichkeiten.
- **umfassende Dokumentation und Berichterstattung**.

M 9 Umsetzen baulicher und technischer Maßnahmen (B)

Im Rahmen der Lauschabwehr prüft die Institution, ob spezielle bauliche oder elektronische Maßnahmen zur Erhöhung der Abhörsicherheit getroffen werden müssen.

- **Freigeländesicherung (Perimeterschutz)**
- **Objektaußenhautsicherung**
- **Schleusen mit Personenvereinzelung**
- **Verlagerung wichtiger Räume in innenliegende (Kern-) Bereiche oder Untergeschosse**

- **Videoüberwachung**
- **Gefahrenmeldeanlagen**
- **Errichten von abhörgeschützten Bereichen**
- **Einsatz vertrauenswürdiger Verschlüsselung bei Festnetztelefonen und mobilen Endgeräten**
- **Rauschgeneratoren**
- **Schallisolation von Räumen nach erhöhten Anforderungen der DIN 4109**
- **Einbau von Außenjalousien**
- **Detektionssysteme**

M 10 Einrichtung von abhörgeschützten oder abhörsicheren Räumen oder Bereichen (C)

abhörsichere Räume

Um den höchsten Anforderungen der Lauschabwehr gerecht zu werden, kann es notwendig sein, einen abhörgeschützten oder abhörsicheren Raum einzurichten.

Wesentliche Maßnahmen sind hierbei die Schaffung eines Faradayschen Käfigs und die Filterung bzw. Entkoppelung metallischer Leitungen und Rohre. Hierbei wird hinsichtlich der zu erwartenden Schutzwirkung zwischen abhörgeschützten und abhörsicheren Räumen unterschieden:

1. In einem abhörsicheren Raum ist das Abhören des gesprochenen Worts nach menschlichem Ermessen durch Lauschangriffe Dritter nahezu ausgeschlossen. Ein solcher Raum verfügt über keinerlei Fenster, ist im Gebäudekern oder unterirdisch gelegen, besitzt u. a. eine metallische HF-Schirmung (>100 dB Dämpfung) und wird mit weitgehend autarken Systemen nach dem sogenannten „Raum-im-Raum-Prinzip“ errichtet. Ein Abhören ist grundsätzlich nur durch Innentäter, z. B. mittels Sprachaufzeichnung, möglich. Typische Anwender sind Botschaften und VS-Bereiche von Regierungen.

2. Beim abhörgeschützten Raum wird das Abhören des gesprochenen Worts durch Lauschangriffe Dritter zwar stark erschwert, ist jedoch mit entsprechend großem Aufwand prinzipiell möglich. Ein Raum dieser Art kann auch mit Fenstern ausgestattet sein, besitzt üblicher-

weise eine HF-Schirmung und darf neben einer 230-V-Netzversorgung über einfache Systeme der Nachrichten- bzw. Gebäudetechnik (z. B. Telefon mit Verschlüsselung, Rauchmelder, Sprinkler, Warmwasserheizung usw.) verfügen. Den aufgrund der deutlich geringeren Kosten akzeptierten Restrisiken ist insbesondere durch geeignete organisatorische Maßnahmen zu begegnen. Typische Anwender sind weniger sensible Bereiche in Botschaften und bei Regierungen sowie das Topmanagement in Institutionen der freien Wirtschaft.

5 Weiterführende Informationen

Weiterführende Informationen zur Lauschabwehr können den nachfolgenden Veröffentlichungen entnommen werden.

- *Bundesministerium für Wirtschaft und Energie 2004: Geheimschutzhandbuch – Handbuch für den Geheimschutz in der Wirtschaft, Stand: 08.09.2014*
- *SecuPedia Wiki-Plattform (www.secupedia.info): Stichworte "Abhörsicherheit", „Abhörgeschützte und abhörsichere Räume"*
- *Lauschziel Wirtschaft: Abhörgefahren und -techniken, Vorbeugung und Abwehr, Boorberg-Verlag, Stuttgart 1996*

6 Anlage

Das Wichtigste auf einen Blick (Themenübersicht)

Etablierung	Organisation	Umsetzung
Verantwortung der Organisation	Planen von Schutzmaßnahmen	erweiterte Maßnahmen zum Informationsschutz
Identifizierung des Schutzbedarfs	Festlegen des Budgets	Schulungen
	Auswahl geeigneter Dienstleister	Lauschabwehrprüfungen
		bauliche Maßnahmen

Dokumentation
Erstellen eines Lauschabwehrkonzepts

Maßnahmenübersicht und -kategorien

A - Basismaßnahmen	B - Standardmaßnahmen	C - erweiterte Maßnahmen
M 1 Verantwortung der Institution M 2 Identifizieren des Schutzbedarfs M 3 Definieren eines Lauschabwehrkonzepts M 4 Umsetzen erweiterter Maßnahmen im Bereich der Informations- und Kommunikationstechnik M 5 Durchführen von Schulungen und Sensibilisierungsmaßnahmen	A + M 6 Budgetierung Lauschabwehr M 7 Auswählen eines geeigneten Dienstleisters für Lauschabwehrüberprüfungen M 8 Durchführen von Lauschabwehrüberprüfungen M 9 Umsetzen baulicher und technischer Maßnahmen	A und B + M 10 Einrichtung von abhörgeschützten oder abhörsicheren Räumen oder Bereichen

Danksagung

Wir bedanken uns bei den vielen Experten, die ihr Fachwissen bei der Erstellung dieses Bausteins einfließen ließen und durch ihr Engagement die Entstehung erst ermöglicht haben. Insbesondere gilt unser Dank folgenden Autoren und Mitwirkenden: Herrn Carsten Baeck (Deutsche Risikoberatung GmbH), Herrn Jens Bolte (Telekom Lauschabwehr) und Herrn Manfred Fink (öffentlich bestellter und vereidigter Sachverständiger für Abhörsicherheit).

Impressum

Herausgeber
ASW Bundesverband
Allianz für Sicherheit in der Wirtschaft e.V.
Neue Schönhauser Str. 20, 10178 Berlin
asw-bundesverband.de

Redaktion/Bezugsquelle/Ansprechpartner
Prof. Timo Kob (Gesamtprojektleitung)

Gestaltung, Produktion
HiSolutions AG

Stand
September 2018

Auflage
1. Auflage

Diese Broschüre ist Teil der Öffentlichkeitsarbeit der Bundesregierung. Sie wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt.