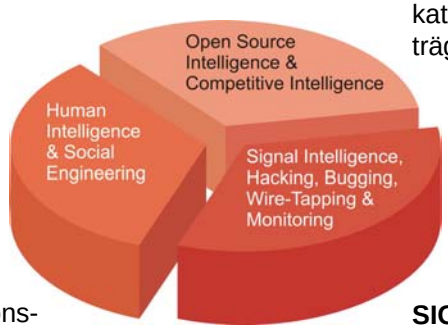
Gästeüberwachung in Hotels

Referent: Manfred Fink, Coburg,
öffentlich bestellter und vereidigter
Sachverständiger für Abhörsicherheit

Methoden der Informations-beschaffung

OSINT
Informationsgewinnung, z.B. von Publikationen, www, Vorträge, Reportagen

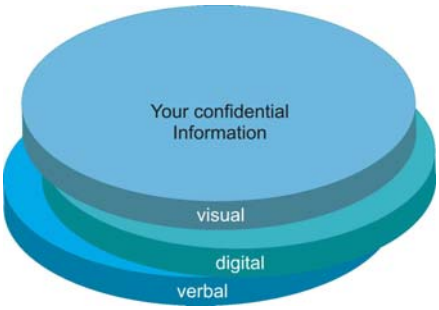


HUMINT
Informationsgewinnung von menschlichen Quellen

SIGINT
Informationsgewinnung durch elektronische Maßnahmen

Ausspähungsziele allgemein

VISUELL
- Meetings
- Videokon-ferenzen
- Pläne
- Prototypen
- Dokumente



DIGITAL
- ISDN
- VoIP
- LAN
- WLAN & VoWLAN
- eMail

VERBAL
- persönliche Gespräche
- Telefongespräche (Festnetz, Mobilfunk)

3

Informationsquellen in Hotels

- **Gäste werden u.U. überwacht mittels:**
  - **Zugriff auf Buchungssystem und Meldedaten**
  - **Observation in öffentlichen Bereichen**
  - **Abhören der Kommunikationswege (TK, WLAN)**
  - **Abhören von Hotelzimmern und Konferenzräumen**
  - **Videoüberwachung von Hotelzimmern**
  - **Heimliche Zimmerdurchsuchungen („Plastikschlüssel“)**
  - **Gesprächsabschöpfung (z.B. in der Hotelbar!)**

4

Zimmerüberwachung

- **Betroffen sind insbesondere**
  - **Luxuszimmer und Suiten sind weltweit als Risiko einzustufen (vgl. Fall Marriott-Hotel, Wien) - dies gilt auch für Deutschland!**
  - **In totalitären Regimen ist von einer nahezu vollständigen Überwachung der Besucher auszugehen (vgl. Fälle Palast-Hotel, Berlin (heute SAS) oder Neptun-Hotel, Warnemünde)**

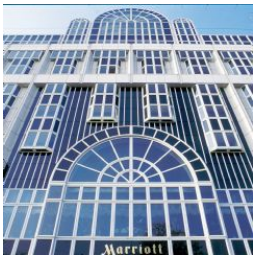
5

Zimmerüberwachung

- **Fallbeispiel: Marriott-Hotel, Wien**
  - **Angriffsform:** **Professionelle ferngesteuerte Raumwanzen für Langwellen**
  - **Methode:** **Versteckt in Gipskartonwänden**
  - **Zweck:** **Abhören von OPEC-Mitgliedern?**
  - **Zeitraum:** **1991? bis 1997**
  - **Tatort:** **3 Luxussuiten des US-Hotels**
  - **Lauscher:** **Unbekannte, professionelle Täter**
  - **Opfer:** **Viele VIP‘s, nicht rekonstruierbar**

6

Zimmer-über-wachung



Berliner Zeitung

ONLINE

> AKTUELLE AUSGABE

> SPEZIAL

SUCHE/ARCHIV

Stichwort

Finden

> JOURNAL

> ANZEIGENMARKT

> SERVICE

> INFORMATIONEN

Lauschangriff auf ein Hotel in Wien

Nobelsuiten vom US-Geheimdienst abgehört

24.04.1997 *Andreas Förster, Wien*

Ein Elektriker brachte den Stein ins Rollen: Als er im vergangenen Februar einen Stecker im Wiener Hotel "Marriott" erneuern wollte, hielt er plötzlich ein etwa zehn Zentimeter langes Kabel in der Hand, an dessen Spitze ein Miniaturmikrofon baumelte. Der Fund des Elektrikers sorgt seither für Aufsehen in Wien: Die teure Suite im vornehmen Haus am Parkring war verwanzt.

Und nicht nur die Suite. Noch in zwei weiteren Zimmern wurden die eiligst bestellten Wanzenjäger fündig. Mikrofone fanden sich hinter Tapeten und in den Zimmertelefonen. Den Wert der gefundenen Technik beziffern Experten auf rund 150 000 Mark.

Eindeutige Klarheit besteht bei den Wiener Fahndern offenbar in der Frage, wer die Lauscher an der Hotelwand waren: Der US-Geheimdienst National Security Agency (NSA), die größte Lauschbehörde der Welt, soll die Mikros installiert haben. Wie das Wiener Nachrichtenmagazin "profil" meldet, habe der Deutsche Bundesnachrichtendienst die Wiener Kollegen

7

Zimmerüberwachung

Marriott VIENNA

8

Zimmerüberwachung

- **Fallbeispiel: Neptun-Hotel, Warnemünde**
  - **Angriffsform:** Audiovisuelle Überwachung (und Human Intelligence in der Bar)
  - **Methode:** Z.B. getarnt in Wänden
  - **Zweck:** Informationsabschöpfung, vorwiegend bei westlichen Gästen
  - **Zeitraum:** 19?? bis 1990 (?)
  - **Tatort:** Zahlreiche (alle?) Zimmer des Hotels
  - **Lauscher:** MfS der ehemaligen DDR
  - **Opfer:** Viele Staatsgäste, wie Politiker und westliche Unternehmer (Uwe Barschel feierte dort seinen 40. Geburtstag!)

9

Zimmerüberwachung

ARD DIGITAL — Mehr Information.

Home | Programmvorschau | Über ARD Digital | EinsPlus | EinsExtra | EinsFestival

Suchen bei ARD Digit

- EinsExtra
- Tagesprogramm
- Highlights
- Reihen & Ereignisse
- Livestream
- Was ist EinsExtra
- Programmwochen

Hotel der Spione - Das "Neptun" am Ostseestrand

Ein Film von Wolfram Bortfeldt und Friederike Pohlmann

Das Hotel Neptun in Warnemünde hat die Wende erstaunlich gut überstanden: Aus dem DDR-Devisenhotel und der sozialistischen Bettenburg ist ein 5-Sterne-Wellness-Hotel geworden. Die Geschichte des Hotels ist eng verknüpft mit dem Chef Klaus Wenzel, der das Haus seit 35 Jahren führt - eine einmalige Karriere. Von Anfang an rankten sich Gerüchte um das "Neptun", für viele ist es heute noch das "Stasi-Hotel". Die Autoren Wolfram Bortfeldt und Friederike Pohlmann sahen sich im Hotel um, sprachen mit Mitarbeitern und recherchierten in Archiven. Sie fanden unter anderem weit über 100 Akten von Inoffiziellen Mitarbeitern des Ministeriums für Staatssicherheit (MfS) im Hotel. Überraschendes Ergebnis: Einige dieser IM haben sich bis heute gehalten. Sie hatten der Staatssicherheit ermöglicht, die Gäste - darunter viele Prominente aus dem Westen - rund um das "Neptun" zu bespitzeln. Der Film schildert die Geschichte des "Neptun" und zeigt, wie das MfS ein DDR-Hotel voll unter Kontrolle hatte - eine "Stasi-Bastion" am schönen Ostseestrand.

10

Zimmerüberwachung

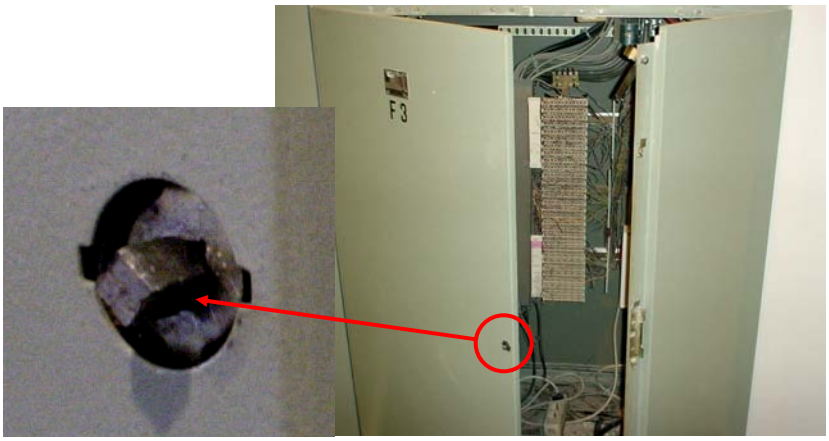
11

Zimmerüberwachung

- **Methoden**
  - **Mobilfunk-Störsender zwingen zur Nutzung überteuerter, abgehörter Festnetzanschlüsse (z.B. in Verteilern, Anschlussdosen, Endgeräten)**
  - **Versteckte Wanzen oder fest installierte Mikrofone hören die Gespräche im Hotelzimmer ab**
  - **Visuelle Überwachung, z.B. mittels heimlich ausgetauschter, präparierter Geräte (z.B. Fernseher, Rauchmelder)**

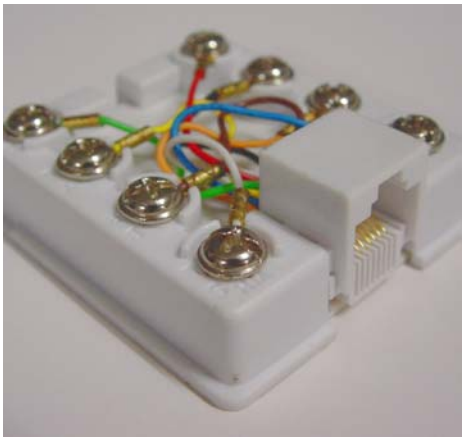
12

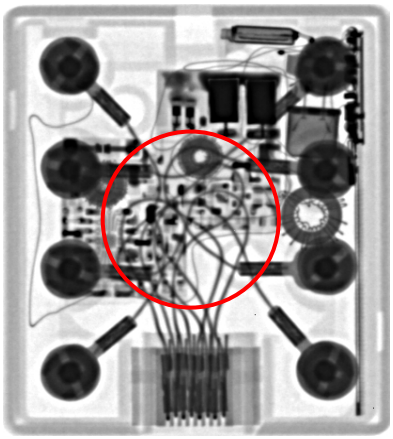
Zimmerüberwachung



13

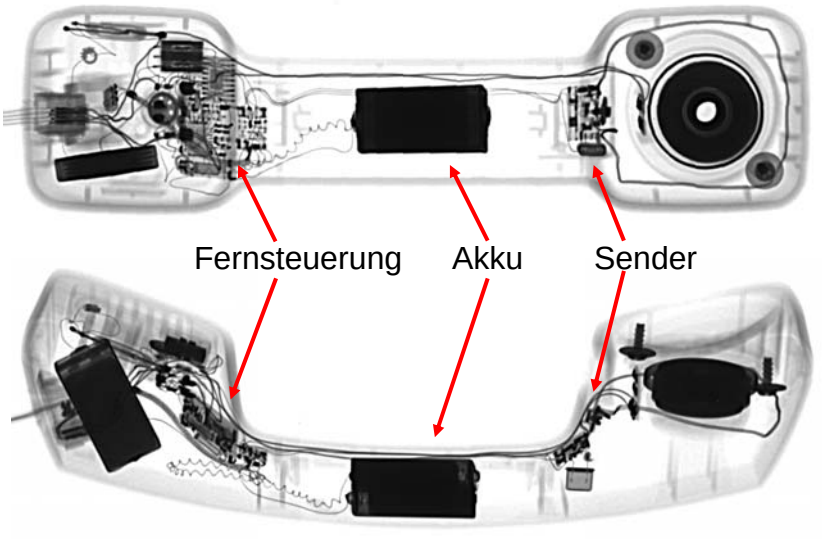
Zimmerüberwachung





14

Zimmerüberwachung



Zimmerüberwachung

16

Zimmer-
über-
wachung

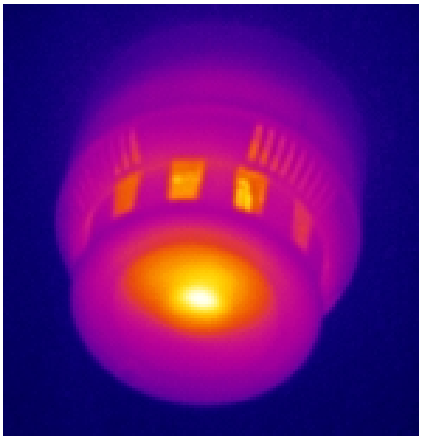
TacTronix™

Tactical Electronics for Critical Missions

Covert Wireless Video Surveillance System: 13" Television[1] (71086)

- High Resolution Low Lux Color or Black/White Camera
- Wide Angle Pinhole or Micro Lens
- Integrated Omni Directional Antenna
- Built-in High Power Video Transmitter[2] in Various Available Frequencies[3]
- Sensitive Multi-Channel Receiver
- Ultra Sensitive Microphone
- Optional Pan/Tilt or Pan/Tilt/Zoom with Wireless Remote Control

Zimmerüberwachung



18

Vorbeugung

- **Organisatorische Zimmerabsicherung**
  - **Die Zimmerreservierung sollte nicht unter dem Firmennamen oder auf dem Namen prominenter Personen erfolgen**
  - **Bei häufigen Aufenthalten an einem Ort sollte das Hotel öfters gewechselt werden**
  - **In unscheinbaren Gasthöfen, kleinen Hotels oder Pensionen sind die Sicherheitsrisiken u.U. kalkulierbarer, als bei internationalen Hotelketten**

19

Vorbeugung

- **Technische Zimmerabsicherung**
  - **Überprüfung (Sweep) auf Wanzen, Mikrofone und verdeckte Kameras**
  - **Entfernen kritischer Geräte (Telefone, TV-Geräte, Radiowecker usw.)**
  - **Einsatz von Rauschgeneratoren und/oder HF-Schirmung bei hohen Sicherheitsanforderungen**

20

Vorbeugung

21

Vorbeugung

22

Vor-
beu-
gung

23

Vorbeugung

Quelle:
em-screen

24

Vorbeugung

- **Telekommunikation in Hotels**
  - **Fremde Telekommunikationseinrichtungen sind als unprüfbar und daher als hohes Sicherheitsrisiko einzustufen**
  - **Bei allen Kommunikationsarten (Sprache, Fax, Daten) kann nur vertrauenswürdige Verschlüsselungstechnik angemessen schützen**
  - **Notfalls einen zufällig ausgewählten, öffentlichen Fernsprecher benutzen (nicht jedoch im Hotel!)**

25

Vorbeugung

26

Vorbeugung

- **Telekommunikation in Hotels**
  - **Falls kein Chiffriergerät zur Verfügung steht, Informationen auf verschiedene Wege aufsplitten (z.B. Lückentexte per eMail oder Fax und Textpassagen per GSM oder Festnetz)**
  - **Am Telefon keine Schlüsselbegriffe verwenden und Namen oder Sachverhalte nicht im Klartext besprechen, sondern umschreiben und interne Abkürzungen verwenden**

27

Vorbeugung

- **Telekommunikation in Hotels**
  - **Unverschlüsselt übermittelte Faxe können dann nicht automatisch ausgewertet werden, wenn der Text handschriftlich diagonal verfaßt wurde**
  - **Bei eMails keinesfalls auf hochwertige Verschlüsselung verzichten, bzw. Steganografie einsetzen (auch als möglicher Ersatz bei staatlichem Verbot von Chiffriertechnik)**
  - **Keine öffentlichen WLAN-Hotspots verwenden**

28

Vorbeugung

- **Steganographie**

Quelle: BSI

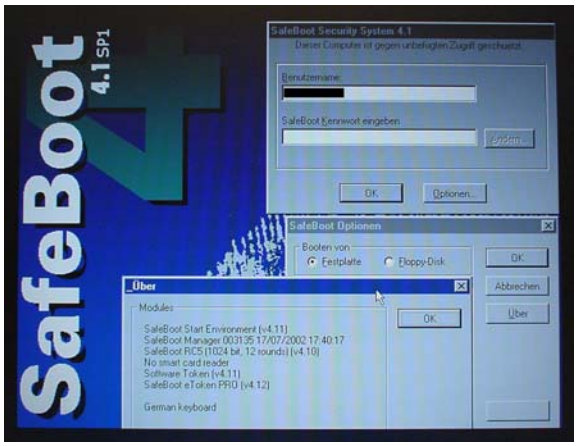
29

Vorbeugung

- **Schutz von Datenträgern**
  - **Datenträger und Laptops nicht in Hotelzimmern (auch nicht im Tresor!), Büros oder Autos lassen**
  - **Auf Laptops, USB-Stick, DVDs, usw. vertrauliche Daten stets nur verschlüsselt speichern**
  - **Boot-Passwortschutz, Fingerprint, Token nutzen**
  - **Evtl. vorbereitete „Spieldaten“ deponieren, um Gegner zu „beschäftigen“**

30

Vorbeugung



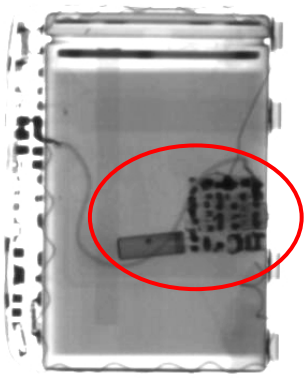
31

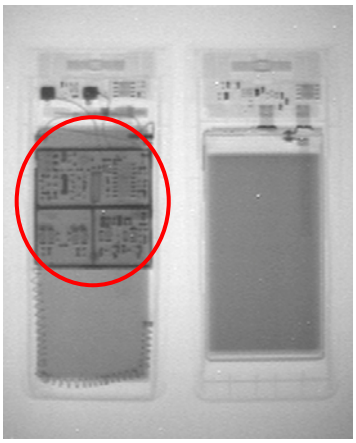
Vorbeugung

- **Absicherung in öffentlichen Bereichen**
  - **Keine Lokale regelmäßig aufsuchen, sondern ohne erkennbares Schema öfters wechseln**
  - **Keine Tischreservierungen auf Firmennamen oder tatsächlichen Familiennamen bekannter Personen vornehmen**
  - **Persönliche Dinge (Kleidungsstücke, Koffer, Mobiltelefone usw.) auch für kurze Zeit nicht unbeaufsichtigt lassen**

32

Vorbeugung





33

Vorbeugung

- **Absicherung in öffentlichen Bereichen**
  - **Keine vertraulichen Gespräche in öffentlichen Lokalen führen (der „zufällige“ Tischnachbar könnte auf Sie angesetzt sein)**
  - **Unvermeidbare persönliche Unterredungen nicht im Klartext, sondern „verklausuliert“ führen, da die Nennung von Namen und konkreten Fakten bei bekannten Sachverhalten unnötig ist**

34

Zusammenfassung

- **Grundsätze**
  - **Professionelle Informationsbeschaffer über-lassen nichts dem Zufall**
  - **Der Schutz von Privatsphäre und Daten ist in fremder Umgebung erheblich erschwert**
  - **Hotelzimmer zählen ohne zusätzliche Sicherheits-vorkehrungen zu den unsichersten Orten**

35