“Sicherheit im World Wide Web”
Funknetze, Digitaler Lauschangriff, E-Mails

Christian Czeczil, Pannonia IT

Nickelsdorf, 21. Mai 2015

Übersicht - Themen

- Einführung
  - Vorstellung
  - Ziele
  - Anforderungen an Sicherheitssysteme
  - Werkzeuge
  - Szenario
- Themen
  - Funknetze
  - Digitaler Lauschangriff
  - E-Mails

Vorstellung

- Ausbildung (2000 – 2009)
  - HTL Spengergasse Wien 1050 (EDV– und Organisation)
  - Fachhochschule Hagenberg (Computer- und Mediensicherheit)
- Vorträge/Security/Datenschutz
- BERGMANN engineering & consulting GmbH
  - Firewalls
  - Spam Filter
  - Serversysteme
  - VPN Lösungen
- Pannonia IT
- Systembetreuer

BERGMANN
engineering & consulting gmbh

Pannonia IT
Nur wer Fragen sucht kann Antworten finden
Entdecken wir beides gemeinsam
office@pannoniait.at

LSR
LANDESSCHULRAT FÜR BURGENLAND

Ziele des Vortrags

- **Ziele ☺**
  - **Bewusstsein schaffen**
  - **Freie Technologien kennen lernen**
  - **Gefahren im Internet kennen lernen**

Anforderungen an Sicherheitssysteme

- **Grundlegende Anforderungen**
  - **Integrität**

    Wurden meine Daten verändert?
  - **Authentizität**

    Wurde mit dem “richtigen” Partner kommuniziert?
  - **Vertraulichkeit**

    Wurden meine Daten vor Dritten geschützt?
  - **Verfügbarkeit**

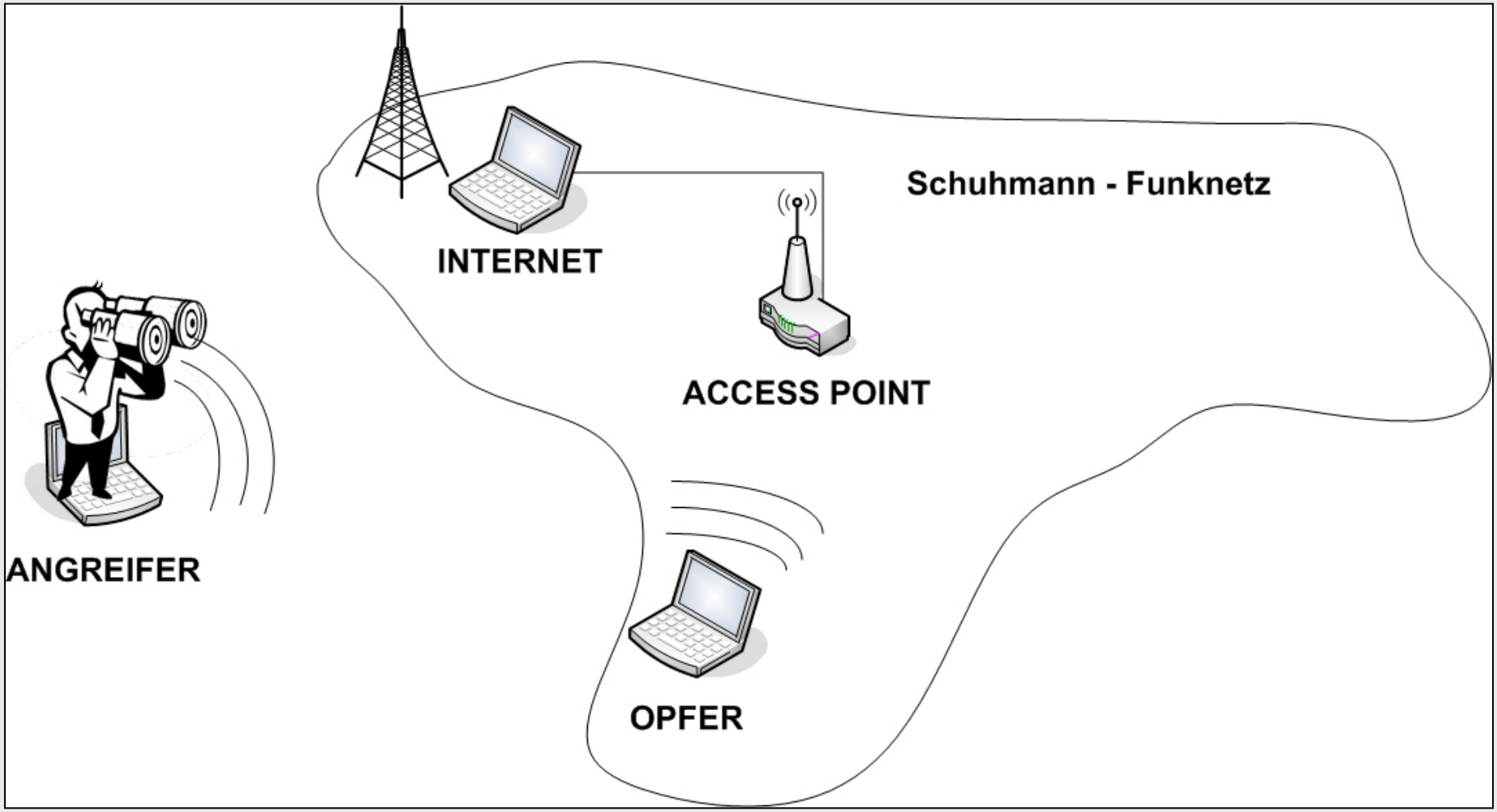
    Kann ich auf meine Daten zugreifen?
- **Verantwortungsbewusstsein**
  - **“Jede Kette ist so stark wie ihr schwächstes Glied”**

- **Die Werkzeugkiste – Linux Betriebssystem: Kali**

Quelle: http://www.kali.org

  - **Funknetze**
    - Aircrack-ng Suite
    - Pyrit
    - Kismet
  - **Netzwerkanalyse**
    - Wireshark
    - Dsniff
    - Nmap
    - sslstrip
  - **Installation auf USB Stick möglich ☺**

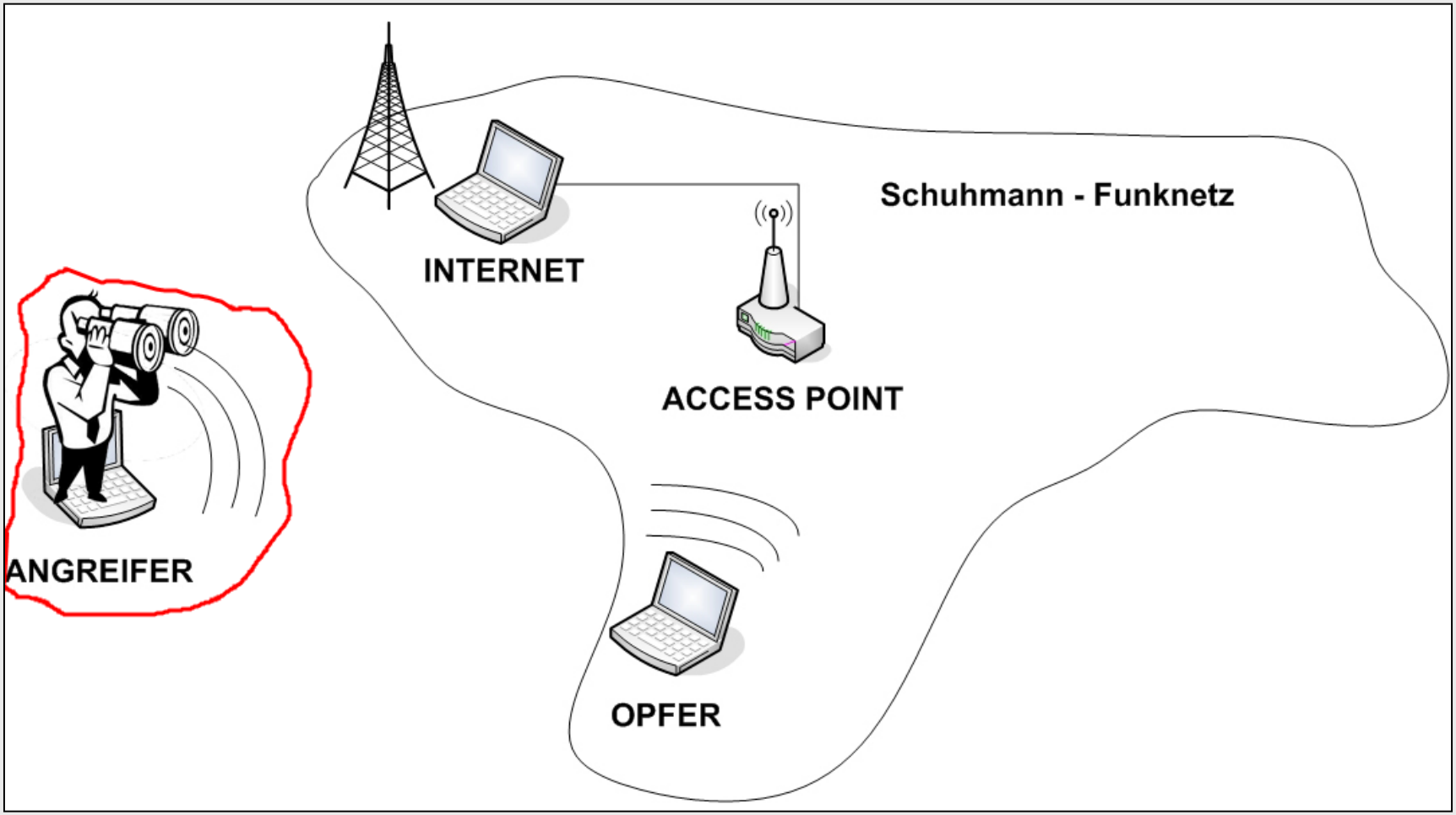
- **Netzwerk der Familie Schuhmann:**



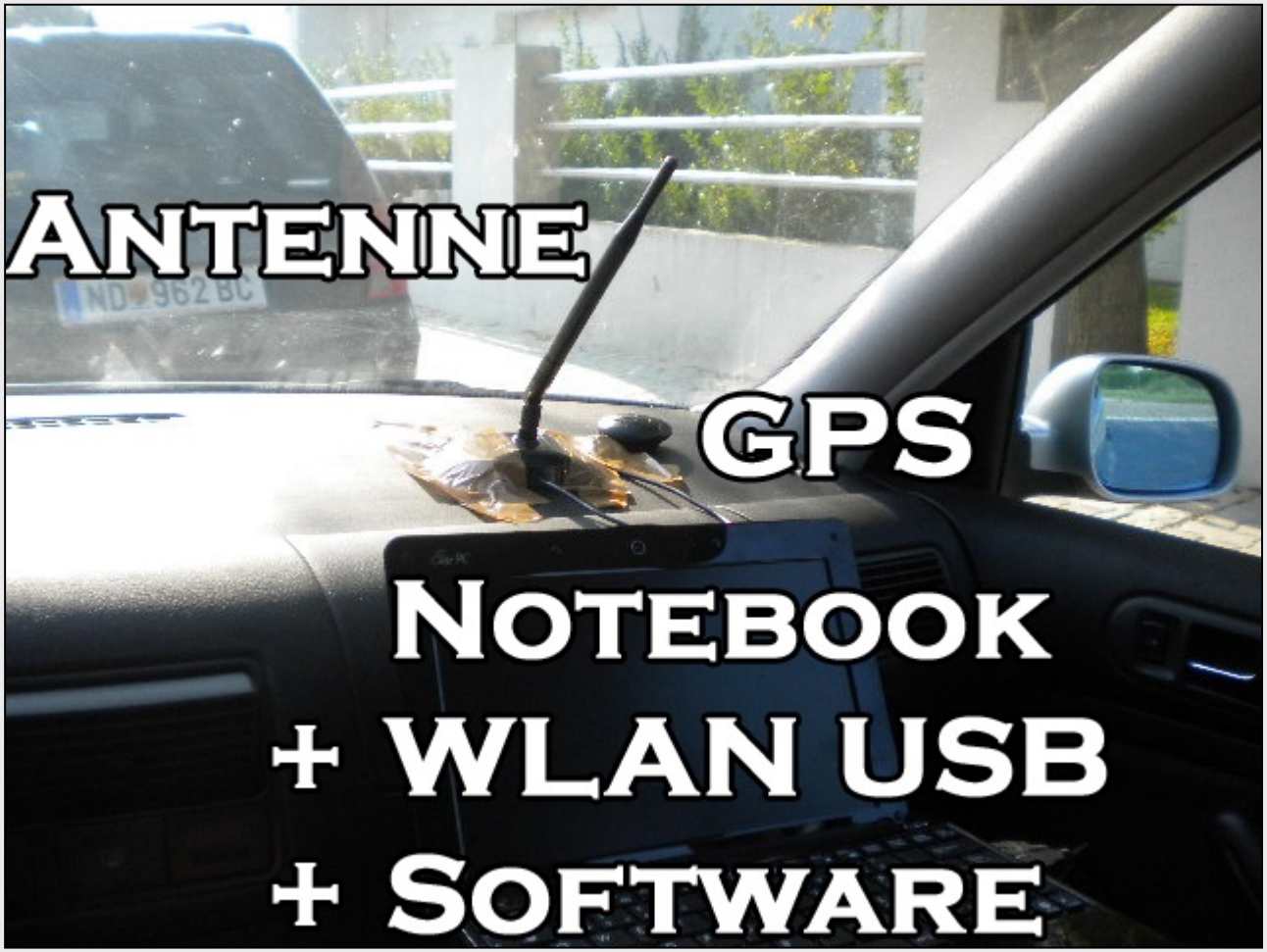
Übersicht - Themen

- Einführung
  - Vorstellung
  - Ziele
  - Anforderungen an Sicherheitssysteme
  - Werkzeuge
  - Szenario
- Themen
  - **Funknetze**
  - Digitaler Einbruch
  - E-Mails

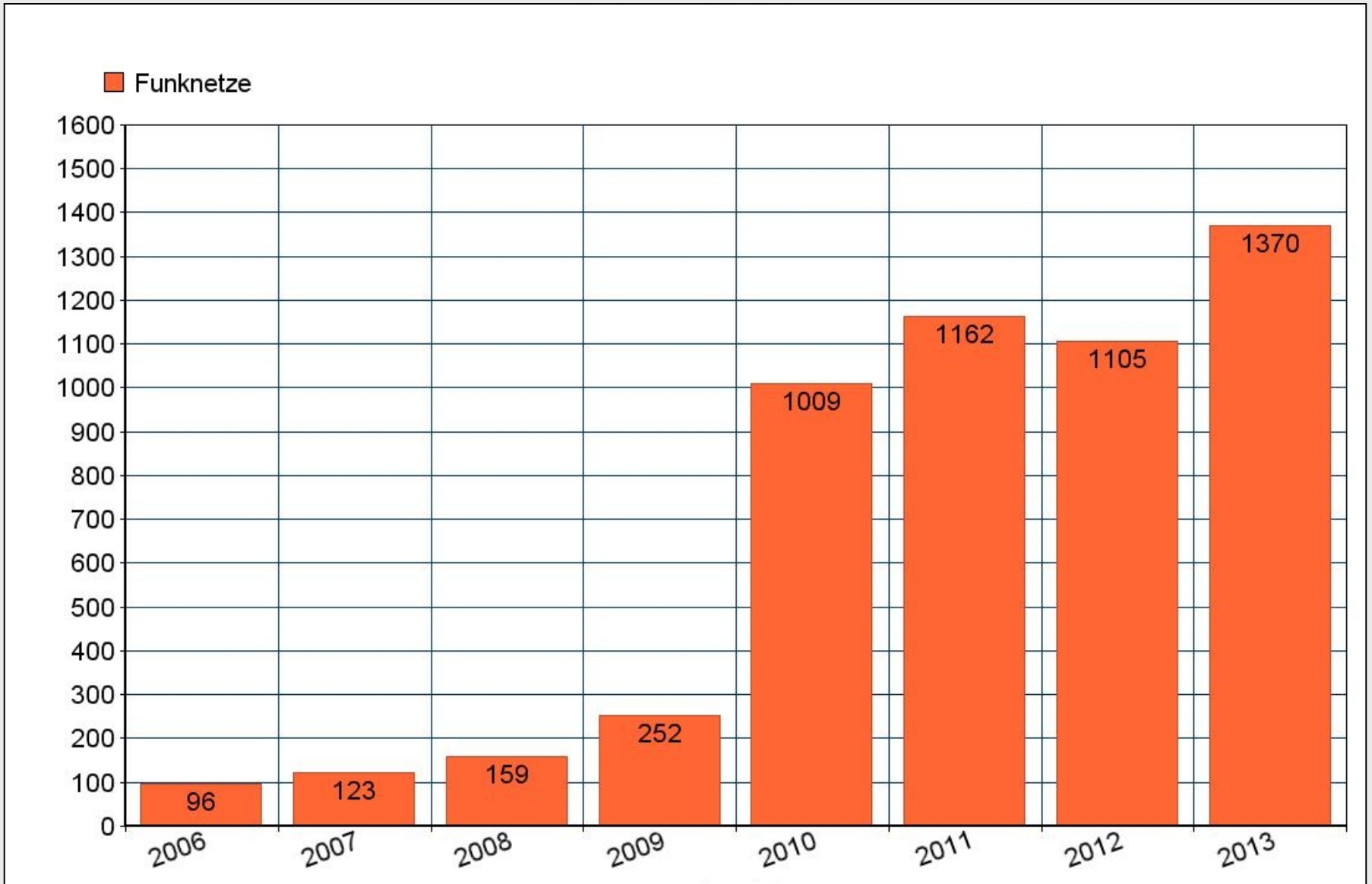
Funknetze: Versuchsaufbau



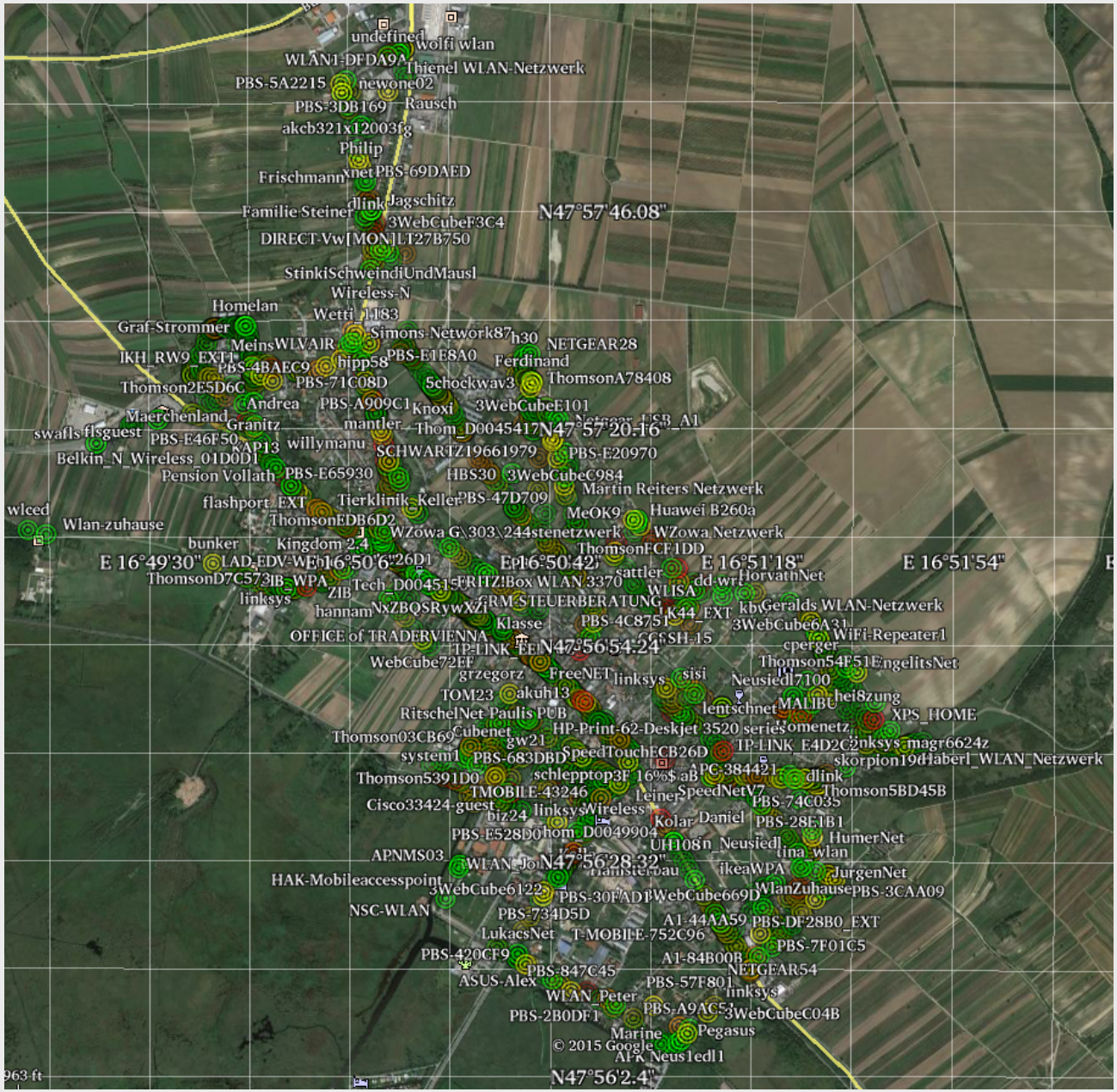
- **Wardriving**



Funknetze: Verfügbarkeit in Neusiedl am See



Funknetze: Neusiedl am See - Verfügbarkeit



WLAN: Schutzmaßnahmen

- **Reduktion der Sendeleistung**
- **WPA/WPA2 Passphrase selber wählen**
- **Keine Standardeinstellungen auf WLAN-Router**
- **WPS deaktivieren**

HINWEIS

Sicherheitslücke in Telekom-Modems erlaubt Zugriff auf WLAN

11. März 2011 10:02

WPA-Schlüssel kann mit Web-Tool geknackt werden – Betroffene WLAN-Modems ausgeliefert

Die von der Telekom Austri
WLAN-Modems der Herste
schwere Sicherheitslücken
einfach Zugriff auf das Net
Leck kann laut einem Beric
WPA-Verschlüsselung ausg
Standardeinstellungen nich
Problem betrifft nicht nur T
welche die betroffenen WL

Kostenloses Tool errechn

SICHERHEITSLÜCKE

UPC: "Keine Sicherheitslücke in unserem WLAN-Router"

ANDREAS PROSCHOFSKY, 26. Juli 2011 10:17

cht: Über geheimes
iert werden

22.11.2012 09:00 « Vorige | Nächste »

Voreingestelltes WPA2-Passwort bei Belkin-Routern leicht zu berechnen

vorlesen / MP3-Download

Das voreingestellte WPA2-Passwort einiger Belkin-Router kann man offenbar leicht errechnen, wie Jörg Schneider und Jakob Lell von der TU Berlin herausgefunden haben. Demnach wird d Standard-Passwort mit Hilfe einer Substitutionstabelle von der MAC-Adresse der WAN-Schnittstelle abgeleitet.

Das Problem hierbei: Die MAC-Adresse der WAN-Schnittstelle weicht nur minimal von der über Funk ausgesandten MAC-Adresse des WLAN-Moduls ab. Somit kann jeder, der sich in Reichweite des Routers befindet, das WPA2-Passwort errechnen und sich in das Netz einbuchen.

Programm erschnüffelt WLAN-Passwort durch WPS-Lücke

31. Dezember 2011, 14:15

foto: flickr/roland

Open-Source-Software Reaver ermittelt Passwort innerhalb von 4 bis 10 Stunden

Mit Reaver hat Tactical Network Solutions (TNS) eine Open-Source-Software entwickelt, die Passwörter von verschlüsselten WLAN-Routern ermitteln kann. Möglich ist das durch eine von Stefan Viehböck entdeckte Sicherheitslücke. Das US-Unternehmen nutzt die Software schon seit einem Jahr. Bisher hielt man sie aber geheim.

Kein Grund zur Geheimhaltung

Nachdem Viehböck die Sicherheitslücke veröffentlicht hat, sieht TNS keinen Grund mehr zur Geheimhaltung. Darum bietet das Unternehmen Reaver über Google Code zum Download an. Je nach Access Point soll Reaver innerhalb von vier bis zehn Stunden ein WPA/WPA2 Passwort im Klartext anzeigen können.

Funknetze: Empfehlung

- **Keinem offenen “Hotspot/Funknetz” vertrauen**

- **Firmware der Router upgraden**

Geheime Hintertür in zahlreichen privaten Routern aufgespürt

3. Jänner 2014, 09:40

Geräte von Linksys und Netgear lassen sich zum Teil aus dem Netz fernsteuern - Liefert Passwörter im Klartext

Was ein echter Bug und was eine gezielte Hintertür ist, lässt sich angesichts der Enthüllungen der letzten Wochen und Monate kaum mehr mit Sicherheit beantworten. Entsprechend darf nun ein neuer Vorfall rund um eine Reihe von Routern der Firmen Linksys und Netgear für Spekulationen sorgen.

foto: linksys

Der Ausgangspunkt der Recherche aber bei weitem nicht der einzige betroffene Router: der WAG200G von Linksys.

Verblüffende Erkenntnis

Hat doch der auf Reverse Engineering spezialisierte Entwickler Eloi Vanderbecken herausgefunden, dass zahlreiche Router auf dem Port 32764 auf Befehle warten. Wie sich nach einer gezielten Firmware-Analyse zeigt, dürfte es sich hierbei um eine Konfigurationsschnittstelle handeln, deren Vorhandensein allerdings nirgendwo dokumentiert ist.

Offen

Dies darf auch nicht verwundern, lässt sich auf diesem Weg doch jegliche Passwortsperre umgehen. Ohne Autorisierung kann über den betreffenden Port nicht nur der Router in den Werkzustand versetzt werden, das Gerät liefert auf Anfrage auch brav alle WLAN-Passwörter im Klartext.

Außenstelle

Besonders besorgniserregend: Bei einigen der betroffenen Geräte ist diese Schnittstelle sogar aus dem Internet erreichbar - also nicht nur aus dem lokalen Netz. Wie heise security aufgespürt hat, lassen sich denn auch tatsächlich über die Spezialsuchmaschine Shodan mehrere tausende IP-Adressen finden, bei denen der betreffende Port von außen zu erreichen ist.

Hintertür in D-Link-Routern ermöglicht Web-Angriff

15. Oktober 2013, 09:59

Passwortabfrage kann beim Web-Interface umgangen werden

In Routern von D-Link ist wieder eine Sicherheitslücke entdeckt worden. Durch Ändern des User Agents kann im Browser die Passwortabfrage beim Web-Interface umgangen werden, berichtet heise. Entdeckt wurde die Hintertür von der Hacker-Gruppe /dev/ttyS0.

foto: d-link

In D-Link-Routern ist eine Hintertür entdeckt worden, die Angreifen ausnutzen können.

Angriff über das Internet möglich

Angreifer können die Einstellungen der Router ändern oder bei WAN-Konfiguration einen Angriff über das Web durchführen. Betroffen sind demnach Modelle der Serien DIR-100, DI-524, DI-524UP, DI-604S, DI-604UP, DI-604+ und TM-G5240. Daneben sollen auch die Planex-Router BRL-04UR und BRL-04CW gefährdet sein, da diese mit D-Link-Firmware laufen.

WAN-Konfiguration deaktivieren

Hersteller D-Link arbeitet bereits an der Behebung der Sicherheitslücke. Ob sie mittels Software-Update geschlossen werden kann, ist noch nicht klar. Wenn es einen Patch gibt, wird er über die Seite von D-Link veröffentlicht. Vorerst wird Nutzern dringend empfohlen, die WAN-Konfiguration abzuschalten. (red, derStandard.at, 15.10.2013)

Demonstration

Sicherheitseinstellungen WLAN Router

THOMSON TG585 v7

de en

- Startseite
- Thomson Gateway
- Breitbandverbindung
- Weitere Funktionen
- Heimnetzwerk
  - Geräte
  - Schnittstellen
- Hilfe

Startseite > Heimnetzwerk > Schnittstellen > WLAN: Thomson03[illegible]E05 Übersicht | Details | Konfigurieren

Ihre DSL-Verbindung ist unterbrochen. Überprüfen Sie, ob [illegible] Ihr Thomson Gateway ordnungsgemäß mit der Telefonleitung verbunden ist. Falls das Problem weiterhin besteht, lesen Sie die Dokumentation.

WLAN-Zugangspunkt - Thomson036E05

- **Konfiguration**

Schnittstelle aktiviert:	☑
Physische Adresse:	00:24:17:1B:B5:2D
Netzwerkname (SSID):	Thomson036E05
Schnittstellentyp:	802.11g
Tatsächliche Geschwindigkeit:	54 Mbps
Band:	2.4G Hz
Kanalwahl:	Automatisch
Region:	Europe
Kanal:	1
Multicast von Breitbandnetzwerk zulassen:	☑

- **Sicherheit**

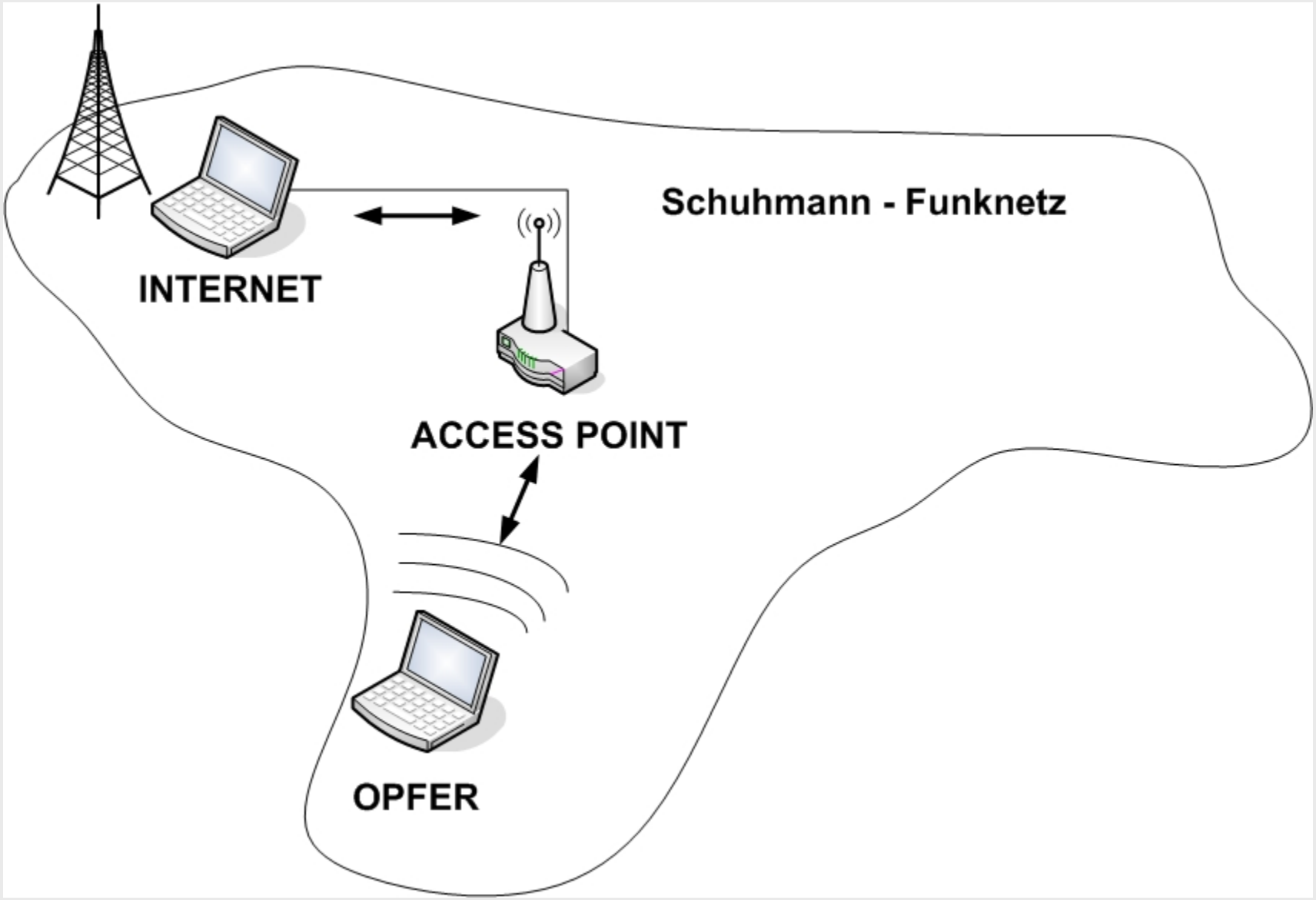
Netzwerkname (SSID) anzeigen:	☑
Neue Geräte zulassen:	Neue Stationen sind zugelassen (autc
Encryption:	● Deaktiviert ● WEP-Verschlüsselung verwenden ● WPA-PSK-Verschlüsselung verwenden
WPA-PSK-Schlüssel:	5DC0F3062C
WPA-PSK-Version:	WPA

Übernehmen Abbrechen

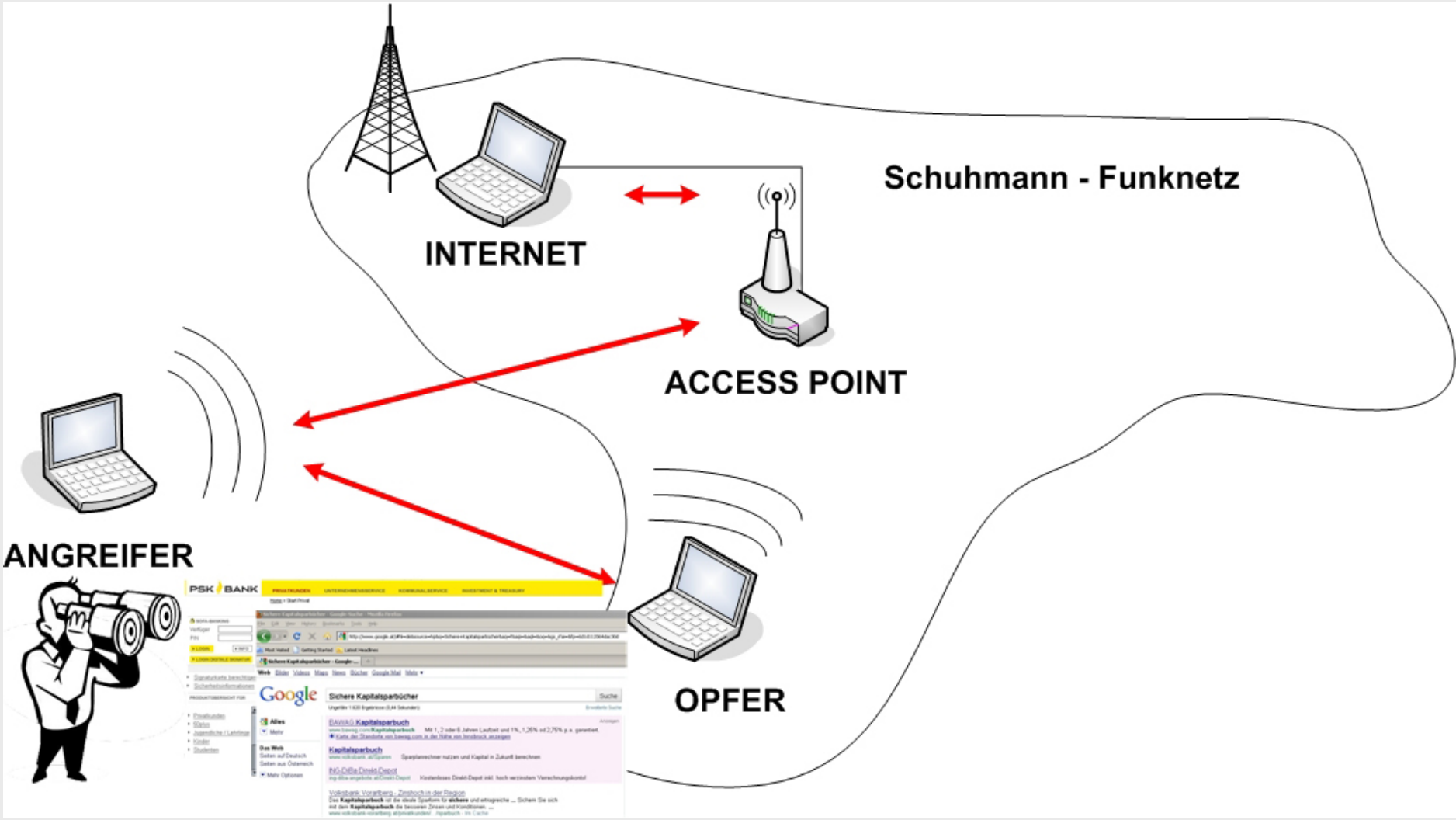
Übersicht - Themen

- Einführung
  - Vorstellung
  - Ziele
  - Anforderungen an Sicherheitssysteme
  - Werkzeuge
  - Szenario
- Themen
  - Funknetze
  - **Digitaler Lauschangriff**
  - E-Mails

Digitaler Lauschangriff: Versuchsaufbau



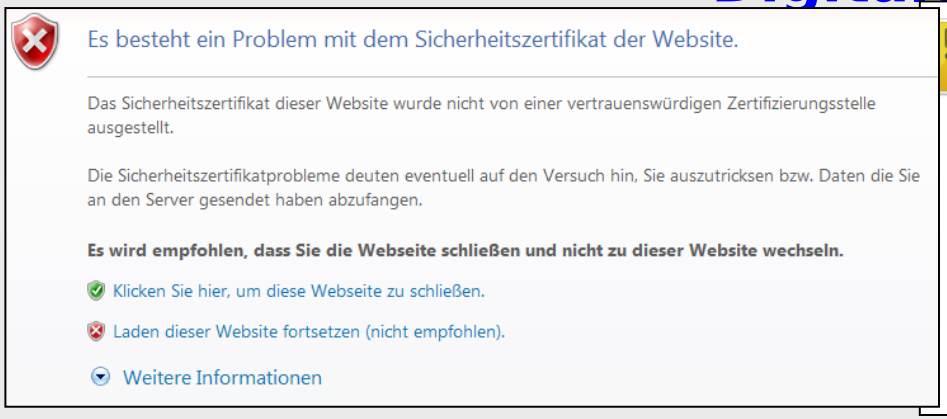
Digitaler Lauschangriff: Versuchsaufbau

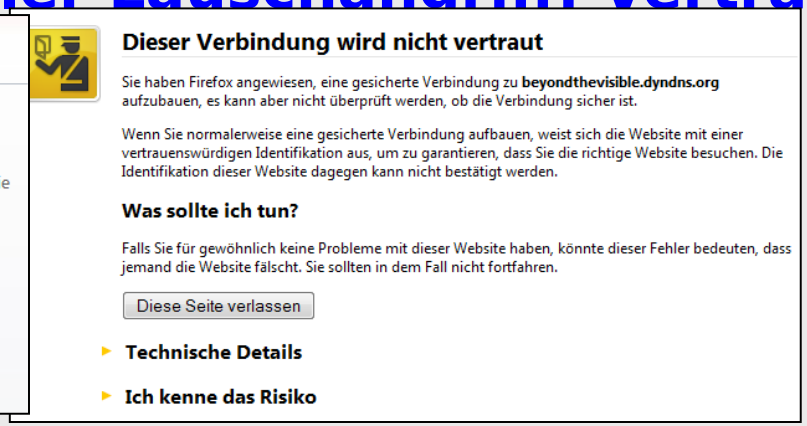


Demonstration

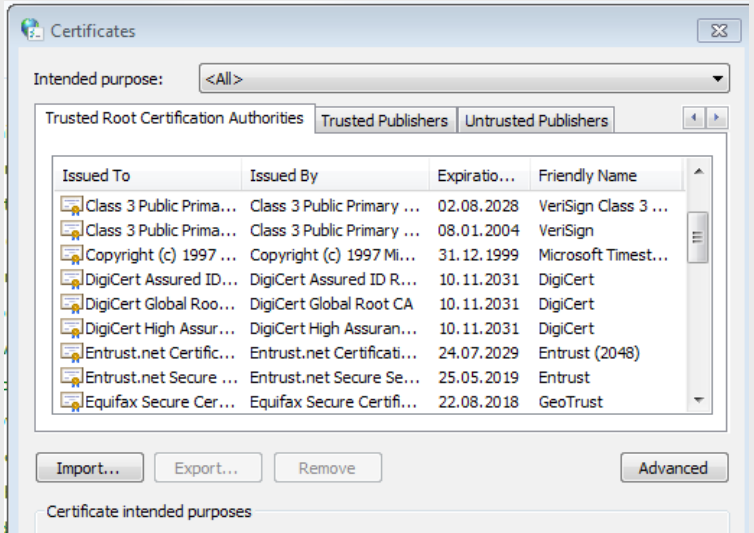
Digitaler Lauschangriff

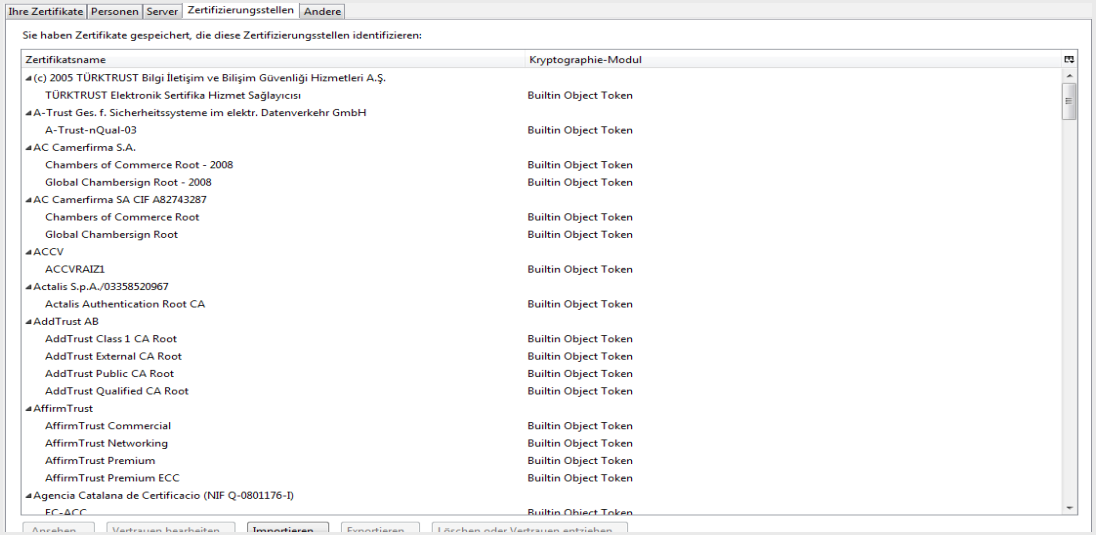
Digitaler Lauschangriff: Vertrauen?





- **Wie entsteht dieses Vertrauen ?**
  - **Certificate Authority (CA) ⇔Digitaler Notar** unterschreibt das Zertifikat des Servers
  - **Betriebssysteme und Programme werden mit CA Liste ausgeliefert**

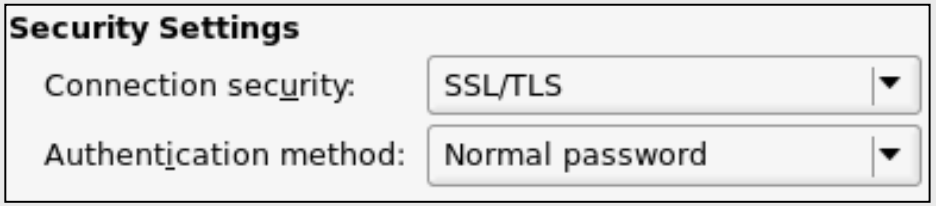




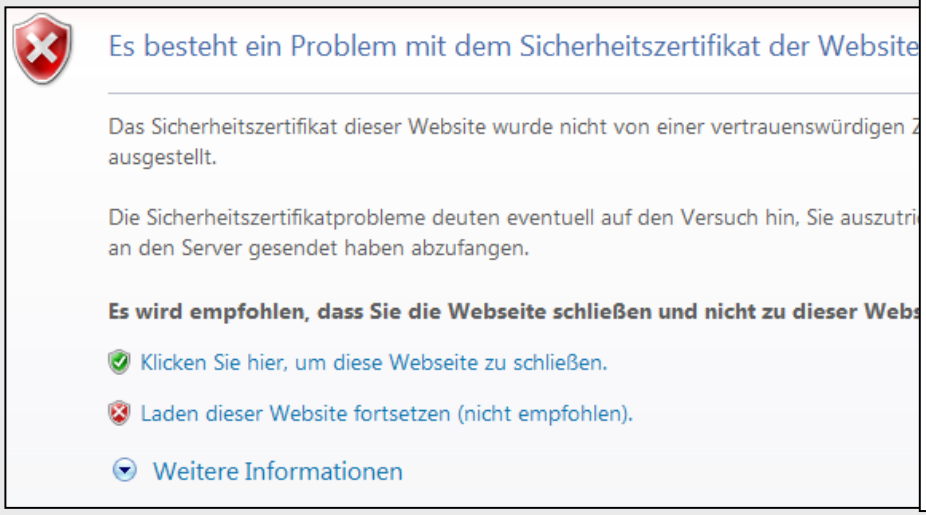
Digitaler Lauschangriff: Sicherheitsmaßnahmen

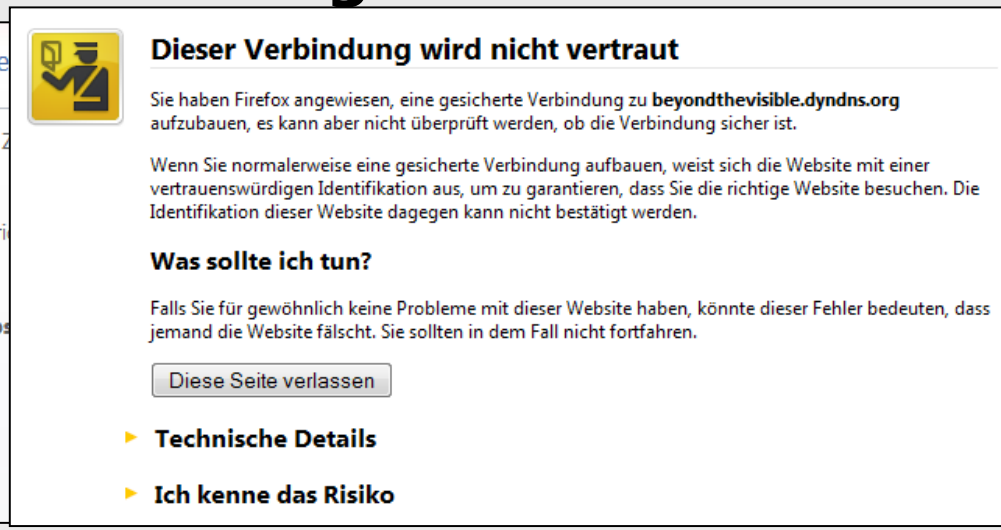
- **Sicherheitsmaßnahmen:**
  - **Verschlüsselte Seiten benutzen**

  - **Verschlüsselt E-Mails abrufen/versenden**



  - **Zertifikatswarnungen nicht ignorieren**



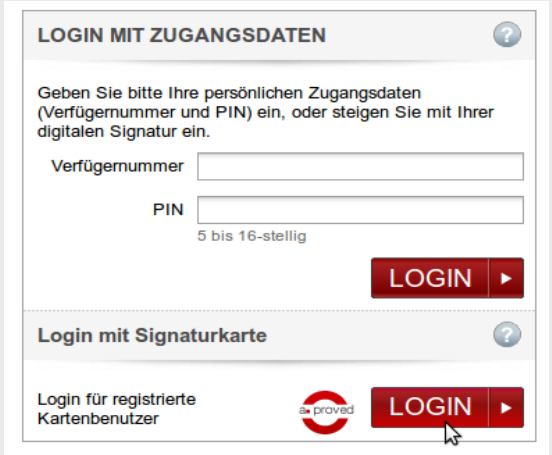


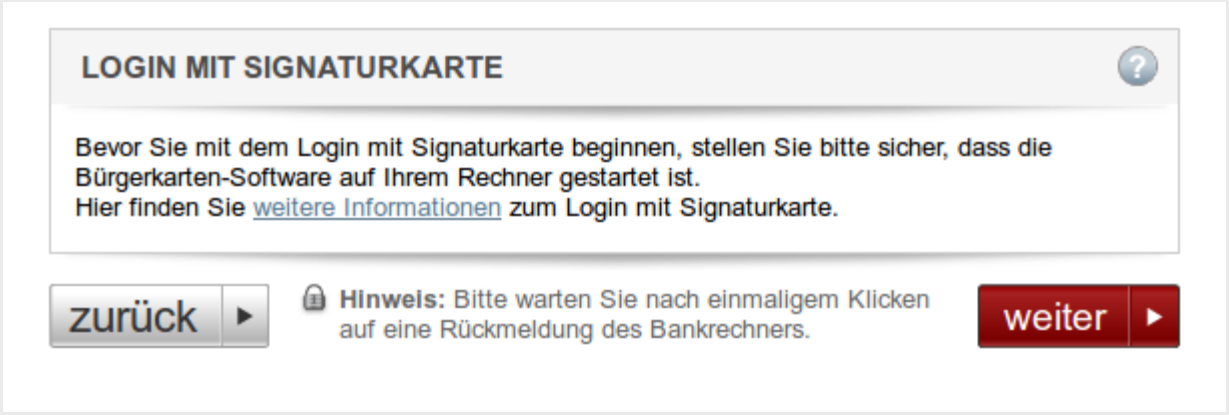
Digitaler Lauschangriff: Sicherheitsmaßnahmen

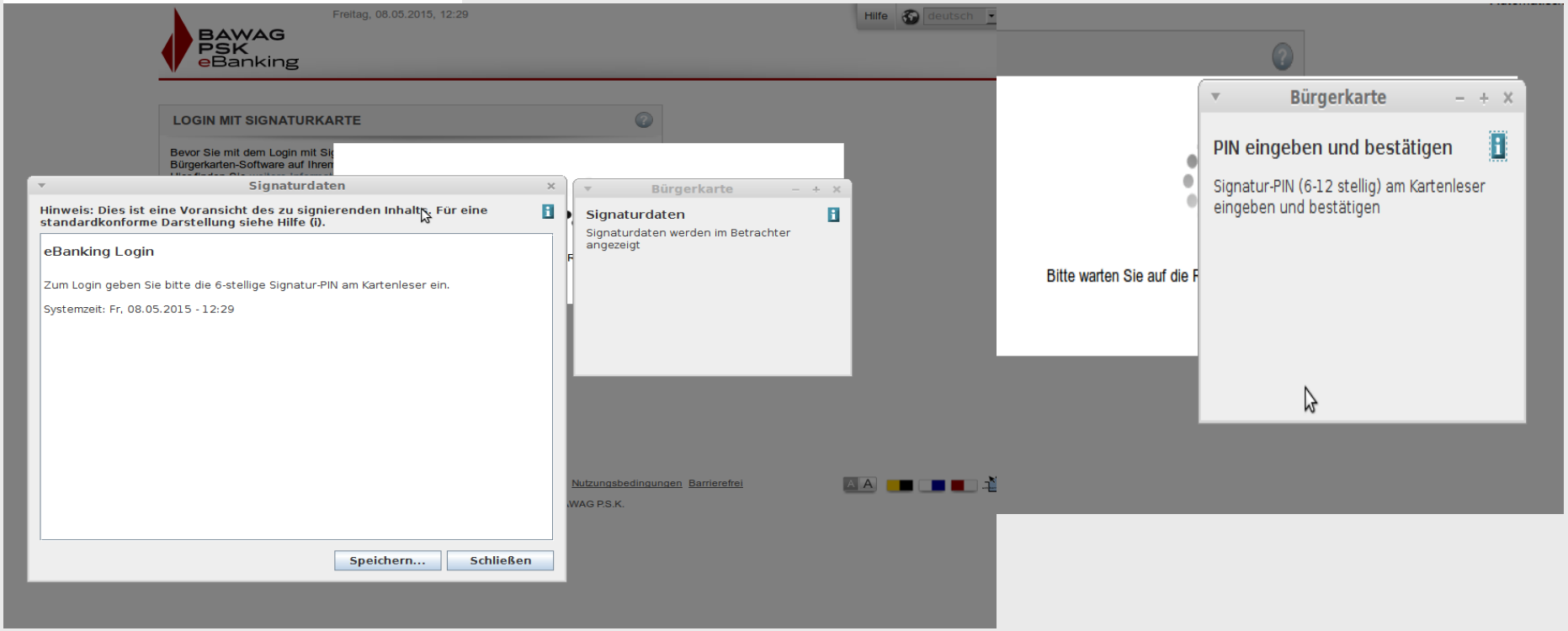
- **Bürgerkarte für Online Banking**
  - **Gratis Aktivierung**
  - **E-Card “Bankomatkarte”**
  - **Kartenlesegerät**

Digitaler Lauschangriff: Sicherheitsmaßnahmen

- **Bürgerkarte**

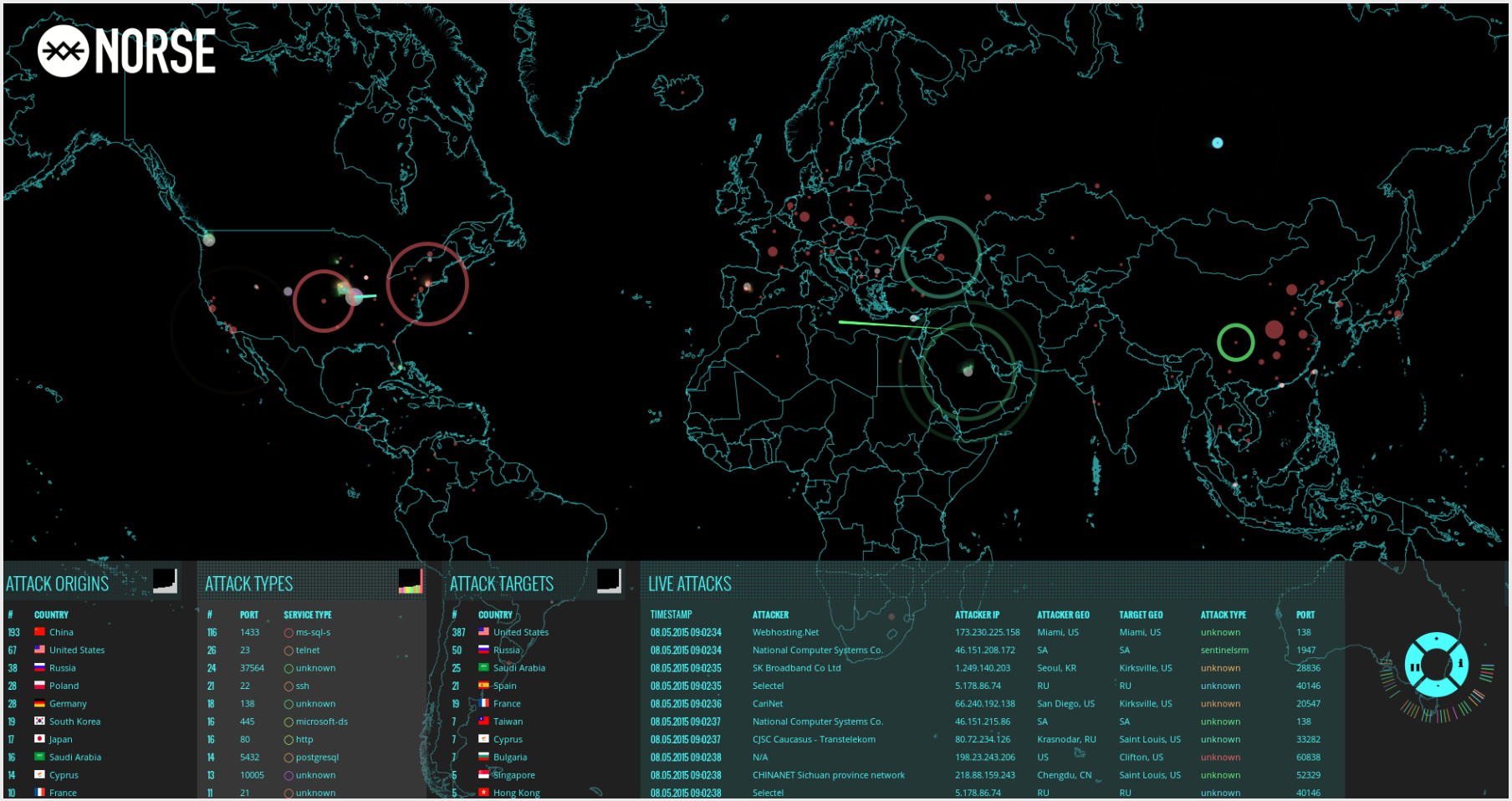






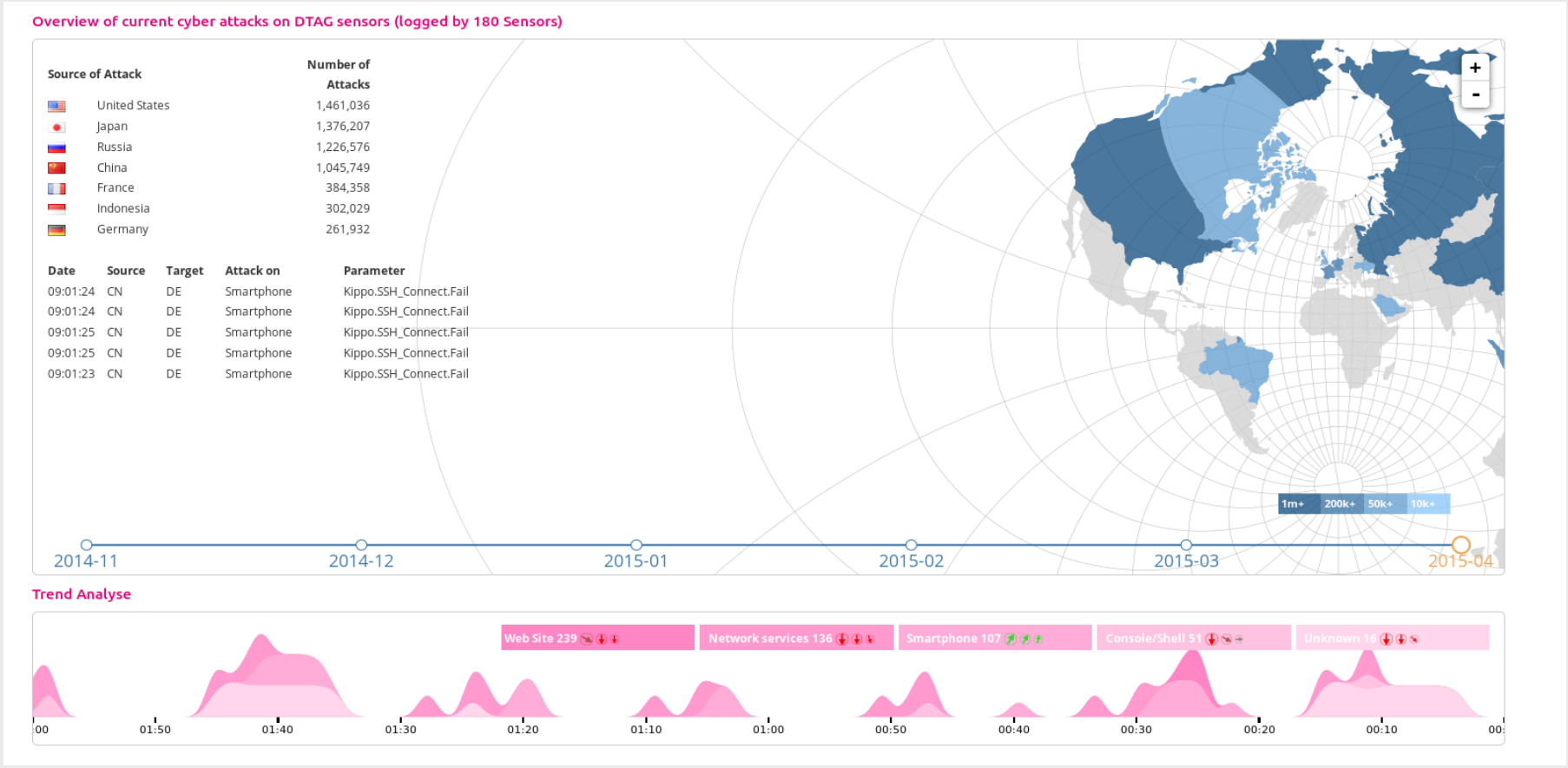
Digitaler Lauschangriff: “Cyber War”

- zB: http://map.norsecorp.com/



Digitaler Lauschangriff: “Cyber War”

- **zB: http://www.sicherheitstacho.eu**



Übersicht - Themen

- Einführung
  - Vorstellung
  - Ziele
  - Anforderungen an Sicherheitssysteme
  - Werkzeuge
  - Szenario
- Themen
  - Funknetze
  - Digitaler Einbruch
  - **E-Mails**

Demonstration

E-Mail

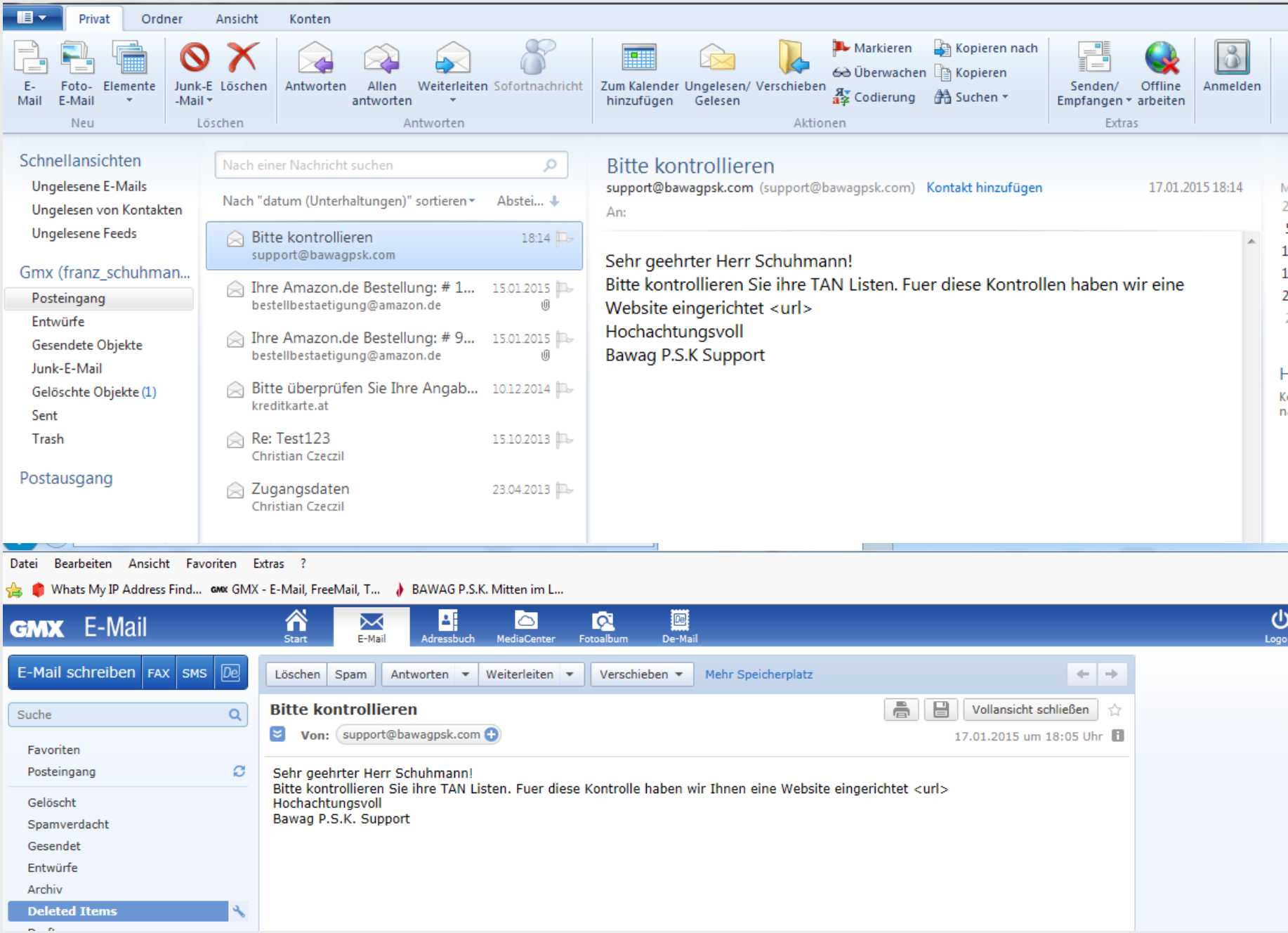
E-Mail: Der digitale Brief

```
Connected to localhost.
Escape character is '^]'.
220 island.pannoniait.at ESMTP Postfix
EHLO fun
250-island.pannoniait.at
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
mail from:<fraud@island.pannoniait.at>
250 2.1.0 Ok
rcpt to:<franz_schuhmann_76@gmx.at>
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
From:<support@bawagpsk.com>
Subject: Bitte kontrollieren
Sehr geehrter Herr Schuhmann!
Bitte kontrollieren Sie ihre TAN Listen. Fuer diese Kontrollen haben wir eine We
bsite eingerichtet <url>
Hochachtungsvoll
Bawag P.S.K Support
.
250 2.0.0 Ok: queued as CCC731804DB5
```

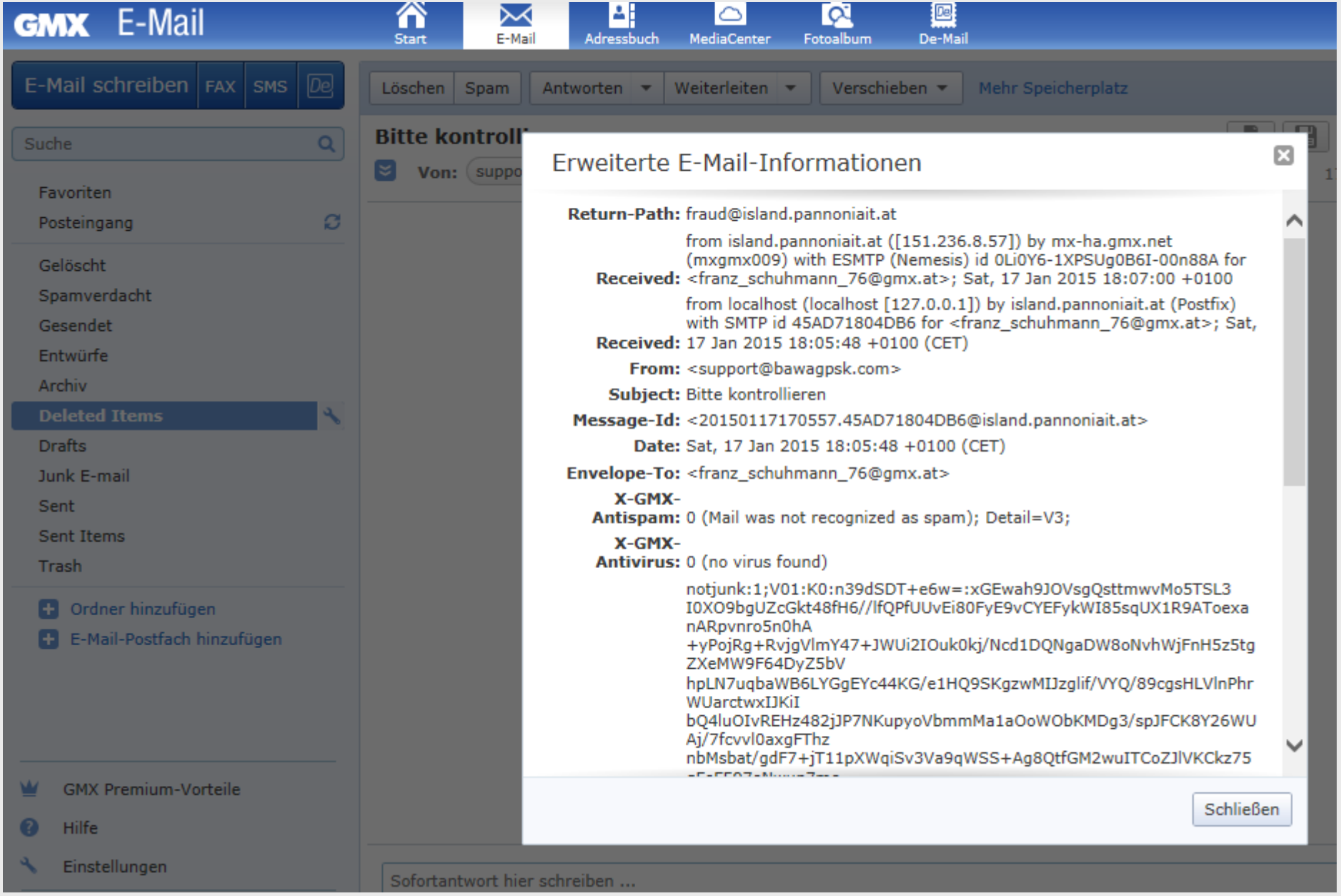
Briefumschlag

Inhalt des Briefes

E-Mail: Sicht des Empfängers



E-Mail: Header



E-Mail: Sicherheitsmaßnahmen

- **Sicherheitsmaßnahmen:**
  - **Keinem Absender vertrauen**
  - **E-Mail Header überprüfen**
  - **Inhalte hinterfragen**

Demonstration
Schutzmaßnahmen
Backup

Fragen ?

Kontaktmöglichkeiten - Resümee

Pannonia IT

Nur wer Fragen sucht kann Antworten finden
Entdecken wir beides gemeinsam

office@pannoniait.at

Vielen Dank für eure Aufmerksamkeit ☺