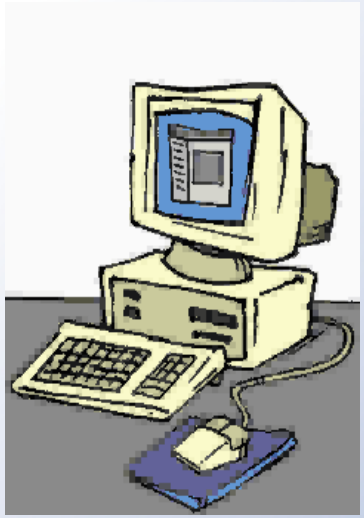
Live Hacking: So brechen Hacker in Ihre Netze ein



Sebastian Schreiber
<Schreiber@SySS.de>

SySS GmbH
Friedrich-Dannenmannstr. 2
72070 Tübingen

Agenda

1. Einleitung
2. Angriffe auf Webshops
3. Netbios-Angriffe mit LANGuard
4. Angriffe auf Domino-Server
5. Simulation eines komplexen Angriffs auf HTTPS
   a) (Überlisten eines Switchs)
   b) Erlangen einer Man-in-the-Middle-Position durch DNS-Spoofing
   c) Einsatz eines Krypto-Relays zum Knacken einer HTTPS-Session
   d) Ausspionieren und Abfangen einer PIN/TAN-Kombination
6. War-Driving – Hacking „en passant"
7. Session-Hijacking bei TCP/IP
8. Durchtunneln von Firewalls (falls noch Zeit)

Drei Thesen zur Internetsicherheit

(1) Hackertools liegen zum Download bereit: Heute kann selbst ein Laie in IT-Netze eindringen.

(2) Nur die Attacken von Kindern und Vandalen werden überhaupt entdeckt.

(3) Die Risiken des Internets werden völlig unterschätzt; die Netze sind weitgehend ungeschützt. Dies wird sich in Zukunft nicht ändern!

Agenda

- Angriffe auf Lotus Notes Server
- Offene Netbios-Shares: Languard
- Allg.: Abhören Verbindungen
- Angriffe auf SSL-Verbindungen
- Angriffe auf Webshops (falls Zeit)


astro-shop - Ihr Warenkorb - Microsoft Internet Explorer
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Suchen Favoriten Verlauf
Adresse http://10.103.30.7:8080/Warenkorb.html?PHPSESSID=c6931f99859bb3
Wechseln zu
Links Heise Newsticker SecurityFocus Digitalkmera Google Alldas.org
astro-shop
Startseite | Katalog | Extra | Warenkorb | Mein Konto | AGB | Support | Maili
Suche
Geben Sie hier einen Begriff zur Suche in unserem Katalog ein.
Mehrere Begriffe können Sie mit einem Leerzeichen Trennen, z. B. "UHC Astronomik"
Suche
Artikelgruppen
Allgemeines
Astronomik Filter
Astrophotographie
Beobachtung Praxis
Ihr Warenkorb
Anzahl Artikel Preis Summe
1 Ändern Löschen Glorious Eclipses II 34.90 34.90
1 Ändern Löschen Das Kosmos Buch vom Weltraum -3.90 -3.90
Gesamtsumme 31.00
Die Versandkosten betragen innerhalb Deutschlands Euro 2.95, in die benachbarten EG-Länder Euro 7.95, in andere Europäische Länder Euro 14.95 und Weltweit ab Euro 19.95.
Bestellung fertigstellen
Internet

Problem beim Angriff auf SSL-geschützte Webserver:

Klassische Sicherheitsscanner wie Nessus, Whisker oder der Stealth HTTP Security Scanner versagen bei HTTPS. Um über normales HTTP auf die Applikation zugreifen zu können, wurde der Stunnel (http://www.stunnel.org) im Client-Mode eingesetzt (`stunnel -c -d 80 -r ziel.com:443`). Dieser Trick ermöglicht den Einsatz der oben genannten Scanner. Um schnell an die verschickten URLs zu kommen, wurde eine Kombination aus Dnsspoof und Webmitm eingesetzt. Als Resultat erhält man (erwartungsgemäß) ein falsches Zertifikat, da der Name der Site nicht übereinstimmt.

```
./sslproxy -L localhost -l 80 -R https-server -r 443
```

http://www.obdev.at/products/ssl-proxy

Wird das Internet in Zukunft sicherer?

„Ja!“	„Nein!“
Sicherungssoftware wird immer besser;	... aber die Hackertools auch.
Budget für Security in Firmen steigt	... langsamer als die Anzahl und Komplexität der Systeme.
IT-Security findet Beachtung	... insbesondere bei jugendlichen Hackern.
Neue Sicherheitsstandards	... setzen sich nicht durch.

... aus dem Polizeibericht

- http://www.bka.de/pks/pks2001/index2.html
- Probleme: riesige Dunkelziffer, da Angst vor Publizität.
- FBI/CSI-Studie 2002:
  - *Bezifferbarer* Schaden in den USA: 455Mio$.

… Folgerung aus der Polizeistatistik …

Frage: Wie hoch ist die Dunkelziffer?

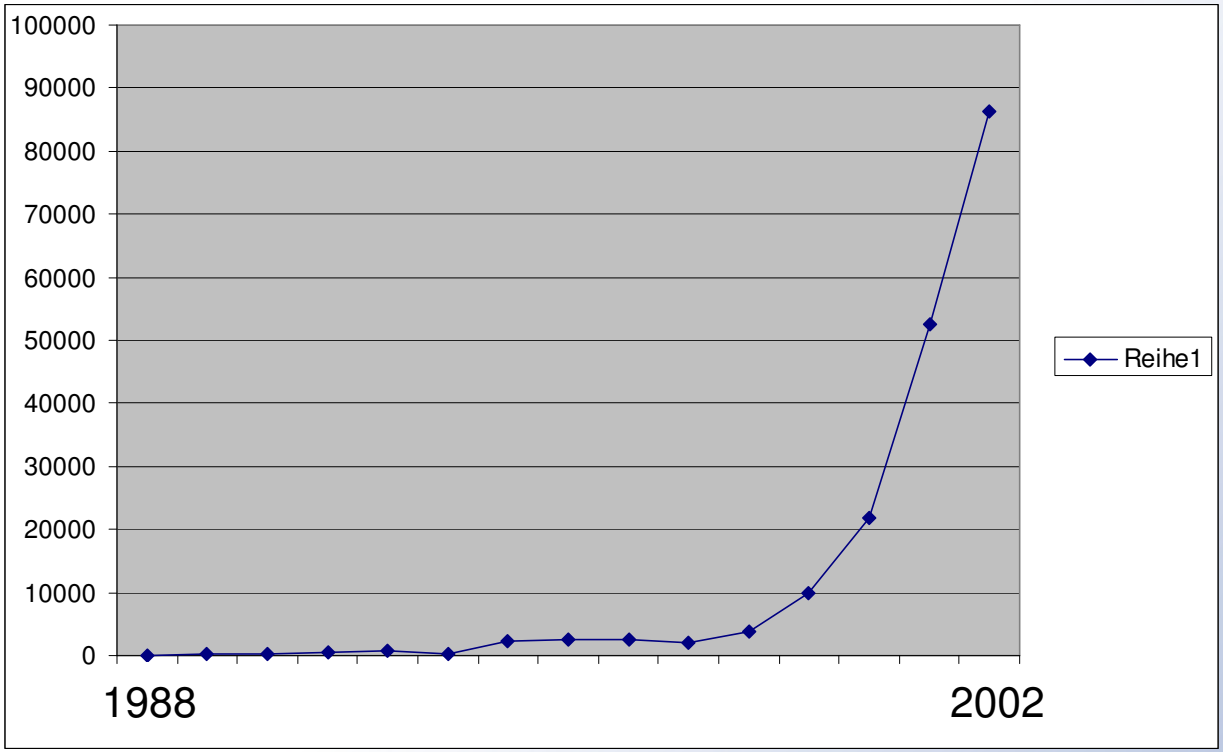
- In der Regel zeigen Unternehmen Straftaten nicht an.

- In der Regel entdecken Unternehmen gar nicht, dass sie Opfer von Hackerattacken werden.

Kriminalstatistik	2000	2001	Steigerungsrate 2000/2001
Sabotage	268	920	343%
Ausspähung	538	1463	272%
Computerbetrug	17310	59670	345%
Prozentsatz der Ausspähungen, die vom Opfer entdeckt werden	3,00%	4,00%	
Prozentsatz der entdeckten Fälle, die zur Anzeige gebracht werden.	10,00%	8,00%	
Hochrechung: Reale Fälle pro Jahr	**179333**	**457188**	

Incident Statistik von Cert.org

Jahr	Incidents
1988	6
1989	132
1990	252
1991	406
1992	773
1993	134
1994	2340
1995	2412
1996	2573
1997	2134
1998	3734
1999	9859
2000	21756
2001	52658
2002	86272



Neue Sicherheitsschwächen

Vulnerabilities reported

1995-1999

Year	1995	1996	1997	1998	1999
Vulnerabilities	171	345	311	262	417

1.2000-2002

Year	2000	2001	Q1-
Vulnerabilities	1,090	2,437	2,148

Total vulnerabilities reported (1995-Q2,2002): **7,181**

Pro Tag sind das 11,8 neue Sicherheitsschwächen!!

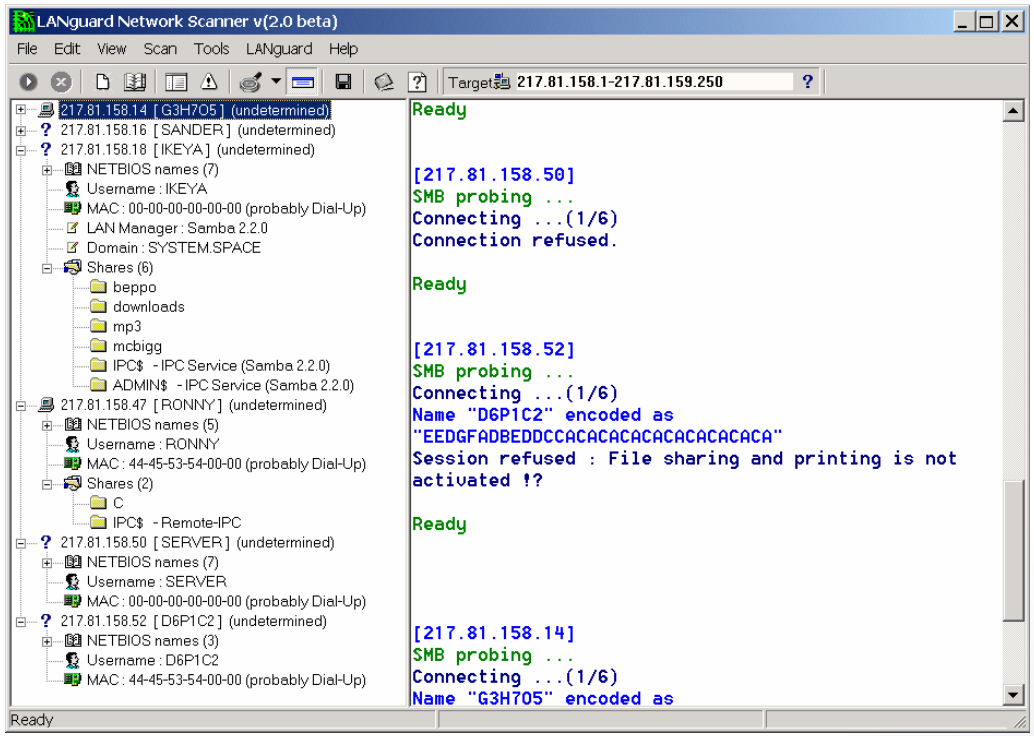
Tendenz steigend!

Bsp. Feb 2001: Anna-Kournikova-Virus

Zitat aus dem Heise-Ticker:

"OnTheFly" erklärt auch, er habe das Virus nicht einfach aus Spaß an der Freude in Umlauf gebracht. Vielmehr wollte er beweisen, dass Anwender nicht viel aus früheren E-Mail-Würmern wie ILOVEYOU gelernt hätten. ***Nach seinen Aussagen hat "OnTheFly" ein Virus Construction Set benutzt, um seinen Wurm zu programmieren, da er sich nicht mit Programmiersprachen auskenne.*** Weil er ein großer Fan des Tennis-Stars sei, habe er den Wurm "AnnaKournikova" getauft: "Sie verdient ein wenig Beachtung, nicht wahr?"

Motivation: Scanning einer IP-Range mit Languard



Viele PCs haben unerwünschte Freigaben – im Unternehmen und zuhause.

Rechtliche Hintergründe

- §202A StGB (Ausspähung von Daten)

  "...die gegen unberechtigten Zugang besonders gesichert sind,..."

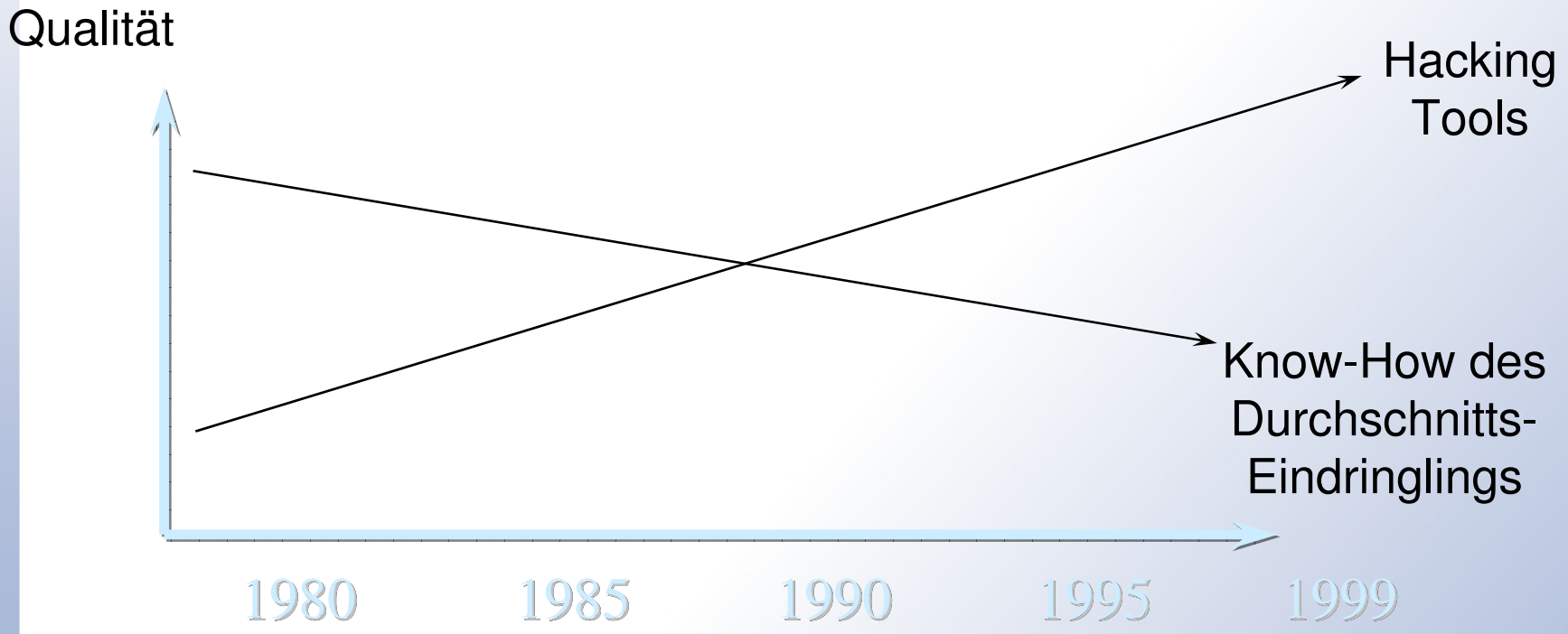
- Schlussfolgerung:
  - Lediglich Datendiebstahl/Sabotage ist verboten - reine Einbrüche nicht.
  - Ausspähung von *ungesicherten* Daten ist nicht strafbar.
- Konkrete Gesetzeslücken:
  - Netbios-Ausspähungen
  - Lotus-Domino-Angriffe
  - WLAN-Angriffe („War-Driving")

Hacker in den Medien

- T-Online-Hack
- Melissa-Virus
- D.o.S. gegen Lycos, CNN, durchgeführt von „Mafiaboy“
- ILOVEYOU: bisher 10 Milliarden DM Schaden

→ Keine raffinierten Techniken;
Die Angreifer sind meist Kinder!

Entwicklungstendenzen

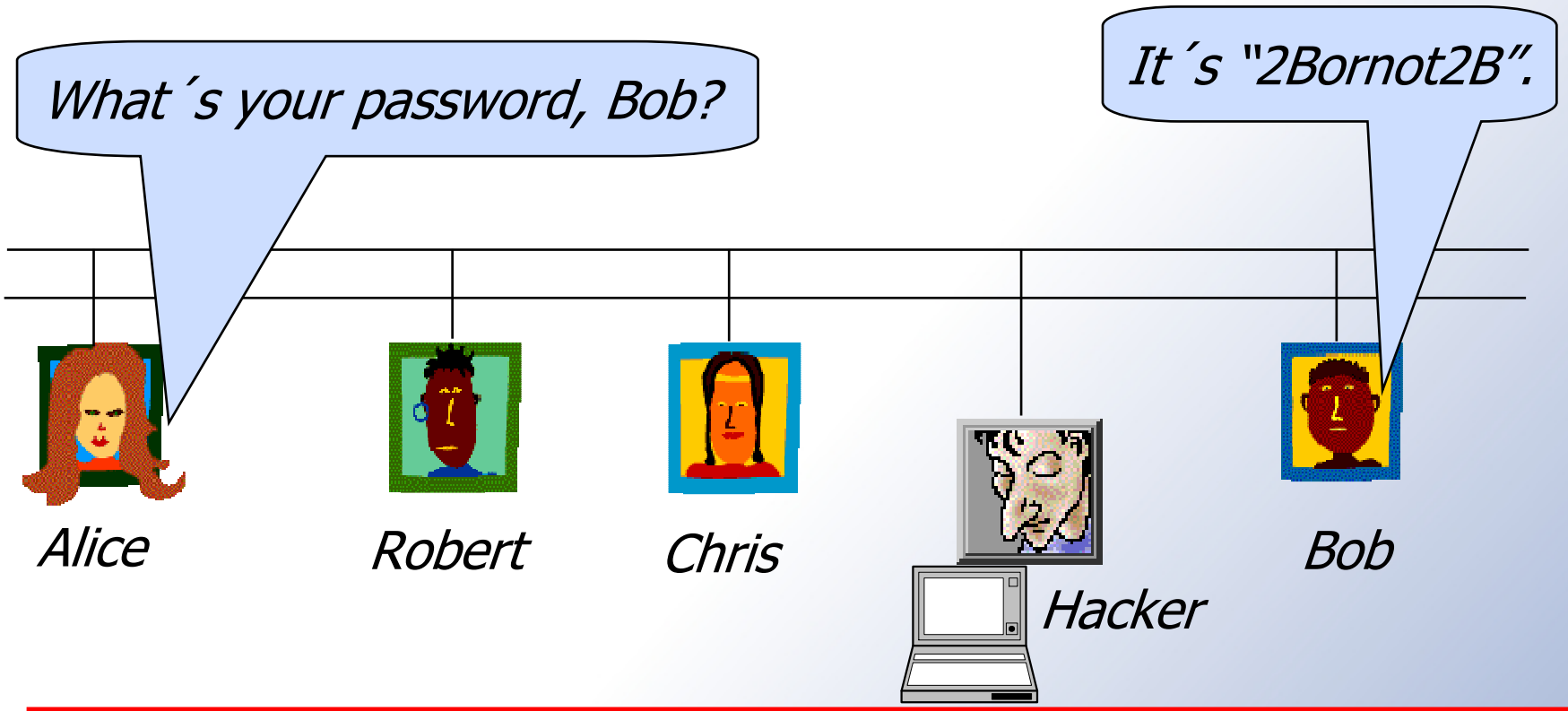


Simulation einer komplexen Attacke – live!

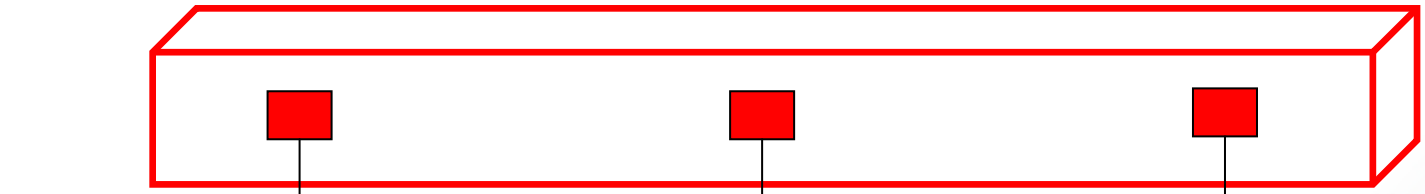
1. Überlisten eines Switchs
2. Erlangen einer Man-in-the-Middle-Position durch DNS-Spoofing
3. Einsatz eines Krypto-Relays zum Knacken einer HTTPS-Session
4. Ausspionieren und Abfangen einer PIN/TAN-Kombination

Eavesdropping

- Ethernet basiert auf CSMA/CD



Sniffen am Switch mittels ARP-Spoofing



MAC	Port
MAC_S	2
MAC_S	3 ??

Client C

Server S

Hacker H

IP	MAC
IP_S	~~MAC_S~~ MAC_H

IP	MAC
IP_C	~~MAC_C~~ MAC_H

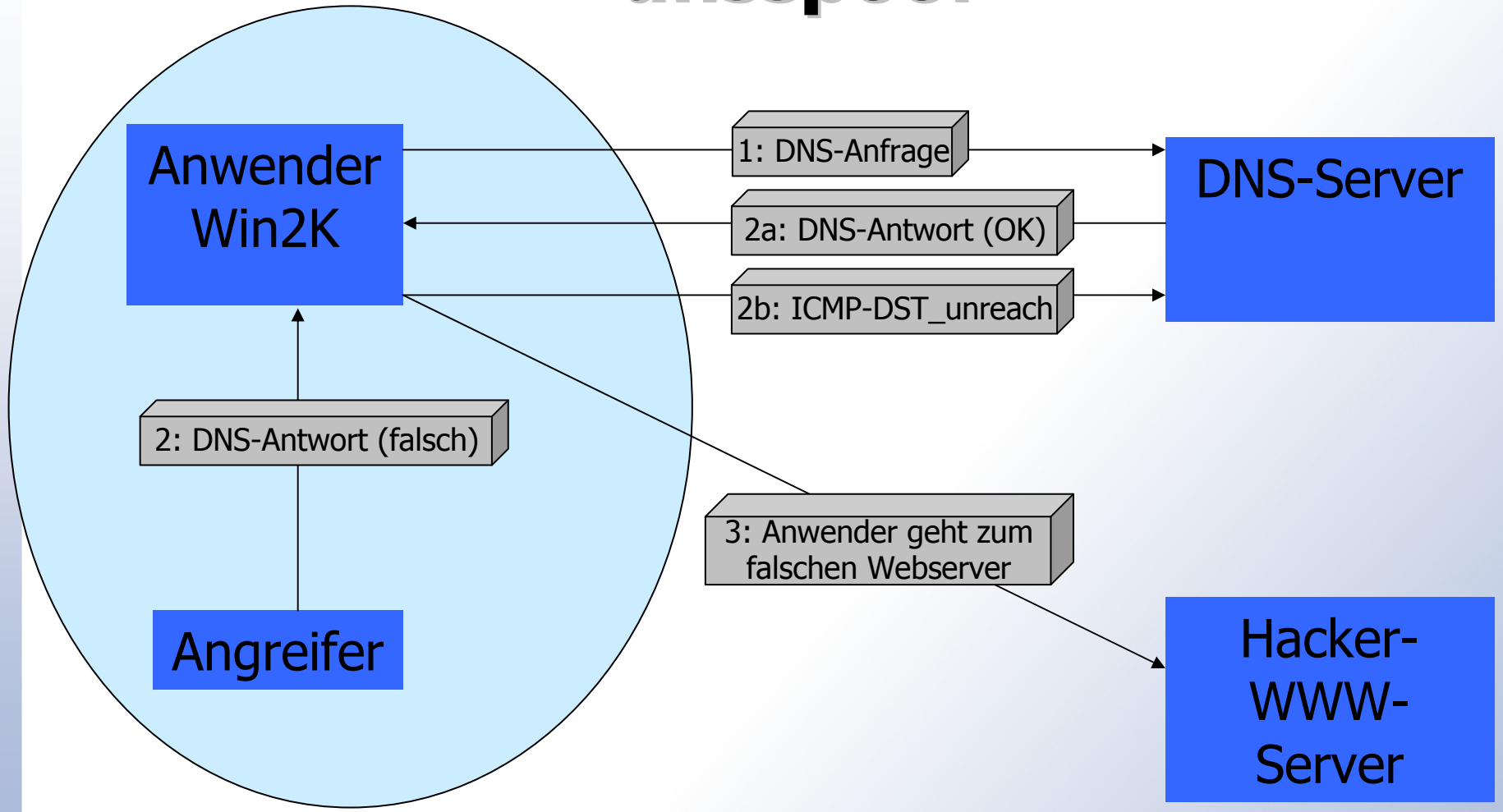
Pakete weiterleiten

Arp Relaying!

Schutz vor ARP-Spoofing

1. Feste ARP-Tabellen in Endgeräten (arp –s)
2. Feste ARP-Tabellen in Switches (???).
3. Arpwrap (Unix) – detektiert Attacken
4. Einsatz von IEEE 802.1x (Authentifikation am Switch, basiert auf EAP)
   ->Besonders interessant bei Wireless LANs

DNS-Spoofing mit dnsspoof



Public-Key Verfahren

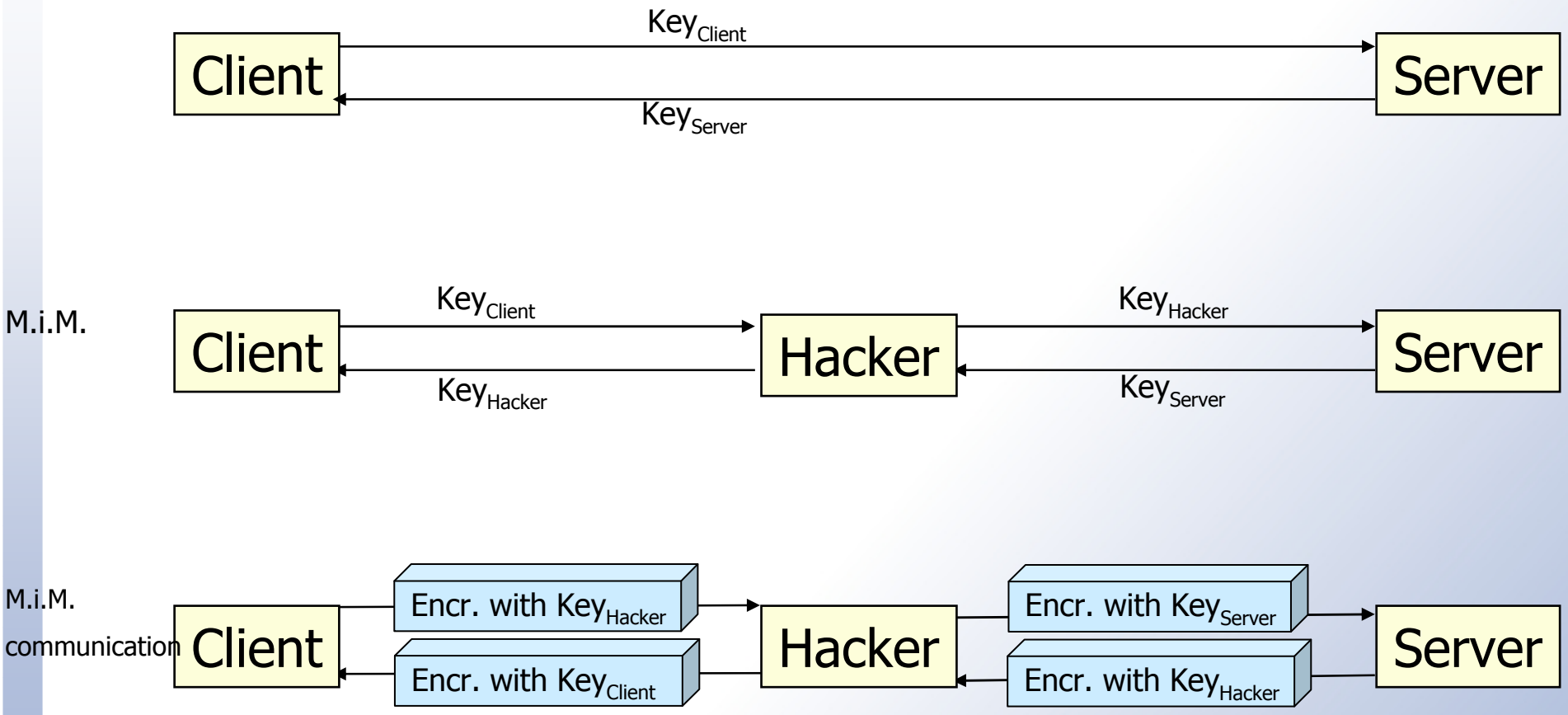
Vorteile:

- Effizient (dank Hybridverfahren)
- Komfortabel
  - Kein „Shared Secret“ und kein geheimer Schlüsseltausch nötig.
  - Niedrige Schlüsselzahl
  - Zertifikate
- Sehr sicher

Offene Fragen:

- Wie werden die Public Keys ausgetauscht?
  - Über einen sicheren Kanal?
  - Mit Zertifikaten

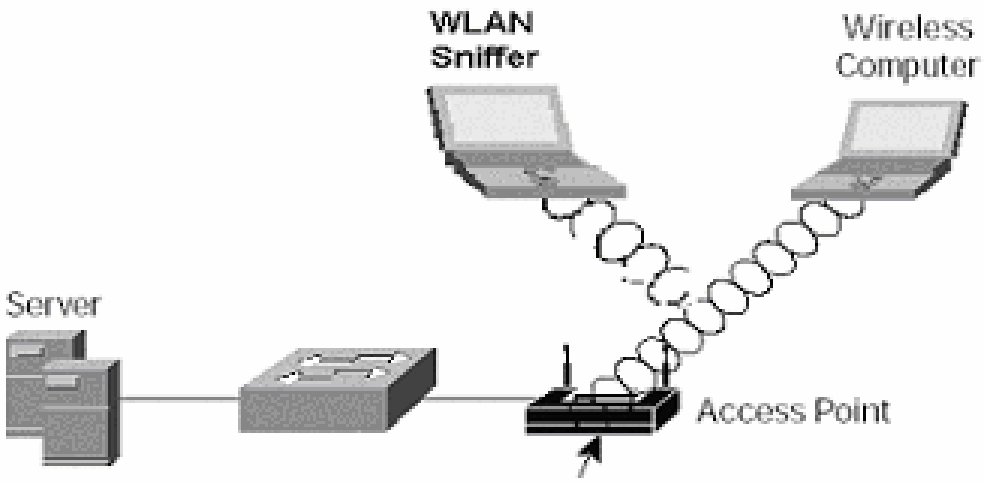
Man-in-the-Middle - Attacke



WLAN

- WLAN basiert auf IEEE 802.11 (wie Ethernet)
- Ethernetattacken auf WLAN übertragbar (Sniffing, Spoofing, Hijacking, MiM ....)
- Wachsendes Gefahrenpotential
- Unterliegen kaum physikalischen Grenzen
- Reichweitenvergrößerung durch Zusatzantennen

WLAN - Probleme



- WLAN - Sniffer nicht detektierbar → hohe Anonymität
- SSID f. Auth. unbrauchbar
- statische WEP Verschlüsselung zu schwach

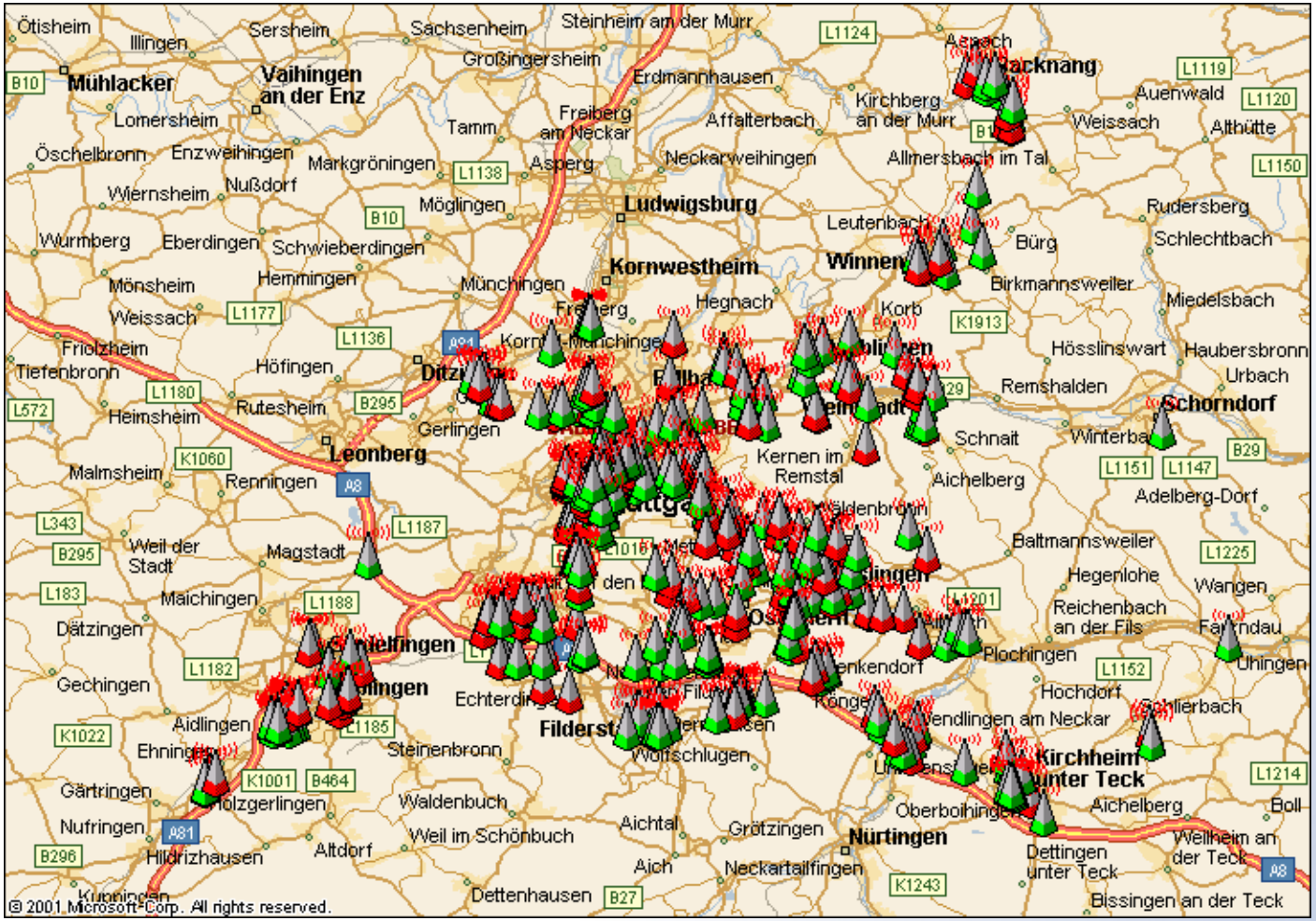
Lösung: *Mutual Authentication* zwischen Client, AP (+ Radius) u. dynamische WEP Keys

WLAN – Hacking

- AP leicht installierbar (Problem Putzfrau)
- Wardriving mit „Netstumbler“
- WEP Keys entschlüsseln mit „Airsnort“
- DoS – Attacken gegen Client+AP + Systeme im LAN !!!
- ARP-Spoofing – Attacken z.Bsp. mit „Hunt“
- Sniffing z.Bsp. mit Dsniff
- MiM – Attacken auf SSH, SSL....

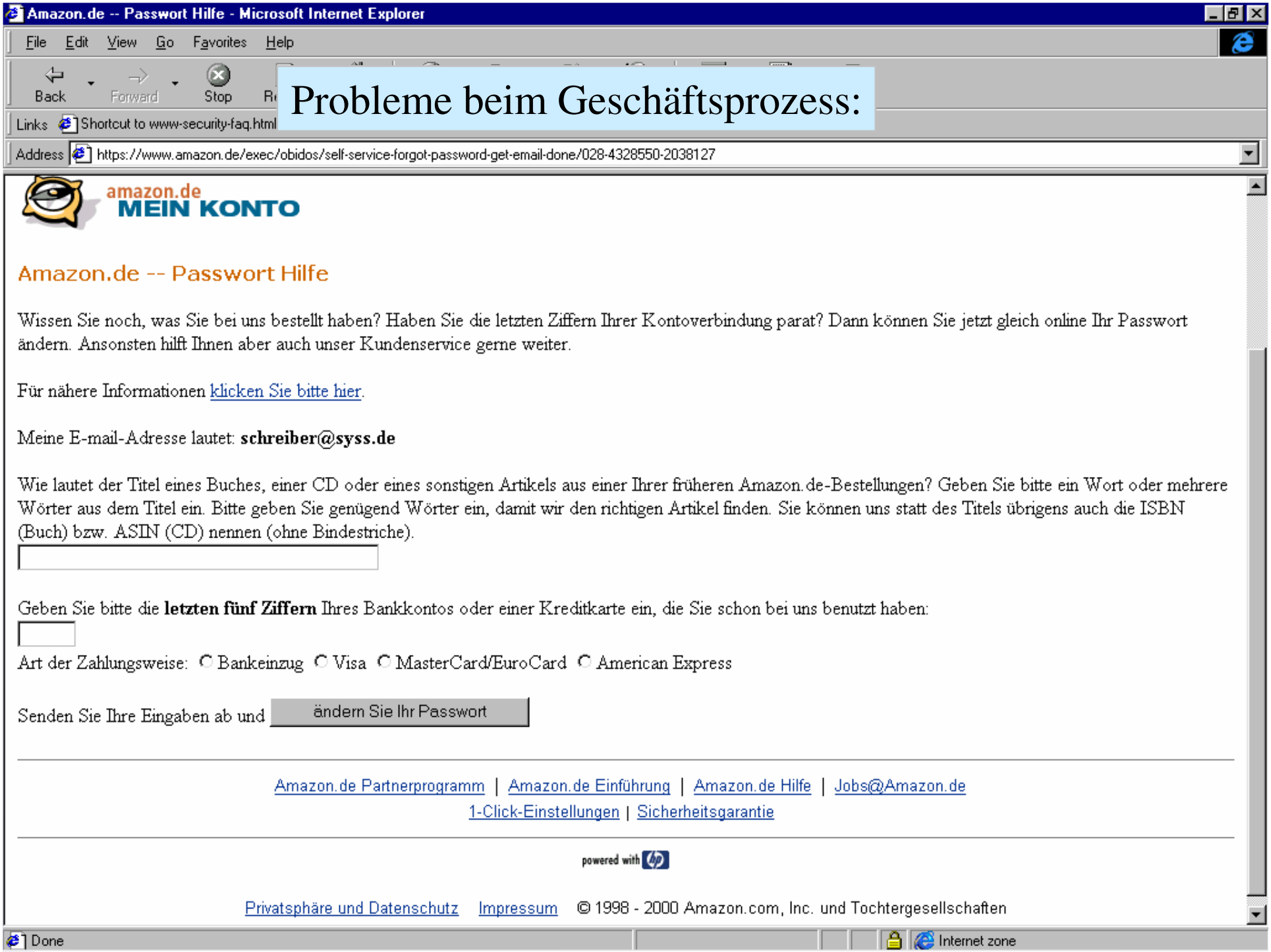
War-Driving 1/2

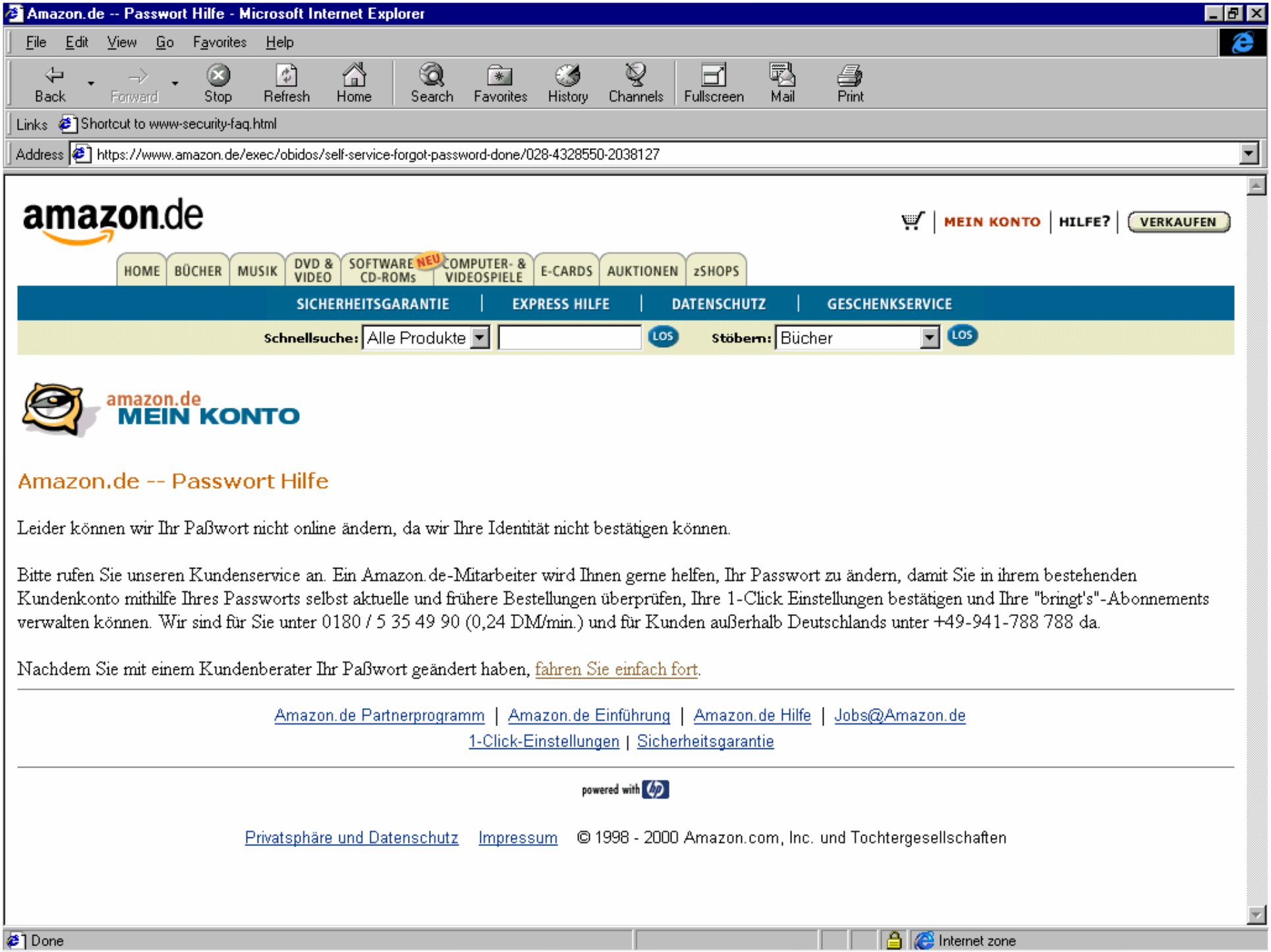
War-Driving 2/2



Ich freue mich auf Ihre Fragen!

(weitere abgedruckte Folien sind nicht Bestandteil des Vortrags und werden nur diskutiert, wenn noch Zeit ist – oder wenn spezielle Nachfragen kommen.)


Amazon.de -- Passwort Hilfe - Microsoft Internet Explorer
File Edit View Go Favorites Help
Back Forward Stop
Probleme beim Geschäftsprozess:
Links Shortcut to www-security-faq.html
Address https://www.amazon.de/exec/obidos/self-service-forgot-password-get-email-done/028-4328550-2038127
amazon.de
MEIN KONTO
Amazon.de -- Passwort Hilfe
Wissen Sie noch, was Sie bei uns bestellt haben? Haben Sie die letzten Ziffern Ihrer Kontoverbindung parat? Dann können Sie jetzt gleich online Ihr Passwort ändern. Ansonsten hilft Ihnen aber auch unser Kundenservice gerne weiter.
Für nähere Informationen klicken Sie bitte hier.
Meine E-mail-Adresse lautet: schreiber@syss.de
Wie lautet der Titel eines Buches, einer CD oder eines sonstigen Artikels aus einer Ihrer früheren Amazon.de-Bestellungen? Geben Sie bitte ein Wort oder mehrere Wörter aus dem Titel ein. Bitte geben Sie genügend Wörter ein, damit wir den richtigen Artikel finden. Sie können uns statt des Titels übrigens auch die ISBN (Buch) bzw. ASIN (CD) nennen (ohne Bindestriche).
Geben Sie bitte die letzten fünf Ziffern Ihres Bankkontos oder einer Kreditkarte ein, die Sie schon bei uns benutzt haben:
Art der Zahlungsweise: Bankeinzug Visa MasterCard/EuroCard American Express
Senden Sie Ihre Eingaben ab und ändern Sie Ihr Passwort
Amazon.de Partnerprogramm | Amazon.de Einführung | Amazon.de Hilfe | Jobs@Amazon.de
1-Click-Einstellungen | Sicherheitsgarantie
powered with
Privatsphäre und Datenschutz Impressum © 1998 - 2000 Amazon.com, Inc. und Tochtergesellschaften
Done
Internet zone


Amazon.de -- Passwort Hilfe - Microsoft Internet Explorer
File Edit View Go Favorites Help
Back Forward Stop Refresh Home Search Favorites History Channels Fullscreen Mail Print
Links Shortcut to www-security-faq.html
Address https://www.amazon.de/exec/obidos/self-service-forgot-password-done/028-4328550-2038127
amazon.de
MEIN KONTO | HILFE? | VERKAUFEN
HOME BÜCHER MUSIK DVD & VIDEO SOFTWARE NEU CD-ROMs COMPUTER- & VIDEOSPIELE E-CARDS AUKTIONEN zSHOPS
SICHERHEITSGARANTIE | EXPRESS HILFE | DATENSCHUTZ | GESCHENKSERVICE
Schnellsuche: Alle Produkte LOS Stöbern: Bücher LOS
amazon.de MEIN KONTO
Amazon.de -- Passwort Hilfe
Leider können wir Ihr Paßwort nicht online ändern, da wir Ihre Identität nicht bestätigen können.
Bitte rufen Sie unseren Kundenservice an. Ein Amazon.de-Mitarbeiter wird Ihnen gerne helfen, Ihr Passwort zu ändern, damit Sie in ihrem bestehenden Kundenkonto mithilfe Ihres Passworts selbst aktuelle und frühere Bestellungen überprüfen, Ihre 1-Click Einstellungen bestätigen und Ihre "bringt's"-Abonnements verwalten können. Wir sind für Sie unter 0180 / 5 35 49 90 (0,24 DM/min.) und für Kunden außerhalb Deutschlands unter +49-941-788 788 da.
Nachdem Sie mit einem Kundenberater Ihr Paßwort geändert haben, fahren Sie einfach fort.
Amazon.de Partnerprogramm | Amazon.de Einführung | Amazon.de Hilfe | Jobs@Amazon.de
1-Click-Einstellungen | Sicherheitsgarantie
powered with
Privatsphäre und Datenschutz Impressum © 1998 - 2000 Amazon.com, Inc. und Tochtergesellschaften
Done
Internet zone

WLAN – Hacking

- Anonyme Internetnutzung (Haftung?,Kosten?)
- Sniffing (Industriespionage)
- Datendiebstahl
- Datenmanipulation
- Rogue AP (der Stärkere gewinnt!)

➔ Erhöhtes Gefahrenpotential für Nutzer+Daten

➔ Momentan zu schwacher Industriestandard

Ausbruch aus Firewall (Theorie)

- Worauf basiert TCP/IP? -- Auf der Sicherungsschicht, die den Austausch von Bit-Streams ermöglicht.
- Idee: Einsatz von Layer-7-Protokollen zur „Simulation“ von Layer-2.

7	Application Layer	HTTP, HTTPS, SMTP, FTP, DNS, ICMP
6	Presentation Layer	
5	Session Layer	
4	Transport Layer	
3	Network Layer	
2	Data Link Layer	
1	Physical Layer	

PPP

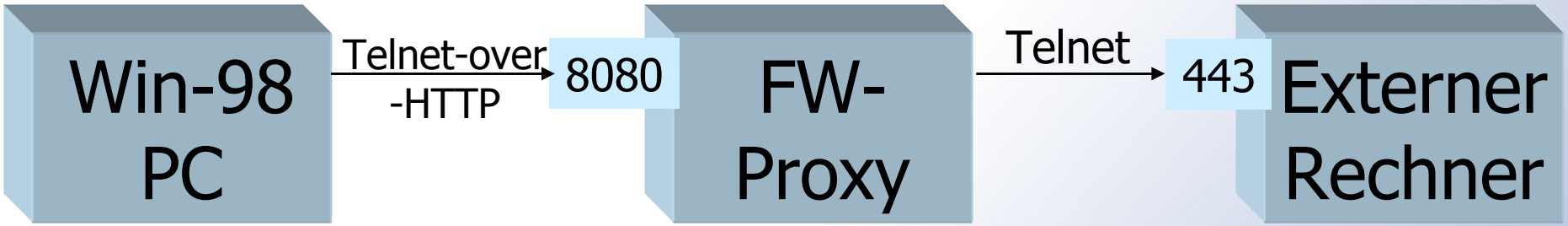
7	Application Layer
6	Presentation Layer
5	Session Layer
4	Transport Layer
3	Network Layer
2	Data Link Layer
1	Physical Layer

Ausbruch aus Firewall (Praxis 1/3)

- Bsp: Nur HTTP-Zugriff wird auf externe Rechner gestattet.
- ---> Mitarbeiter installiert auf externem Rechner ein telnetd, der auf Port 80 lauscht.

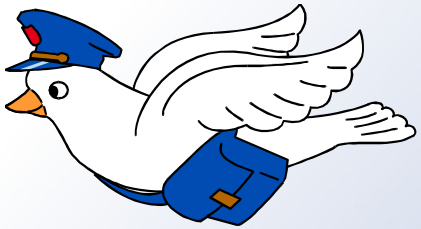
Ausbruch aus Firewall (Praxis 2/3)

- Als Reaktion führt das Unternehmen Proxy-Zwang ein.
- ---> Mitarbeiter benutzt das CONNECT-Feature



CONNECT host.de:443 HTTP/1.0

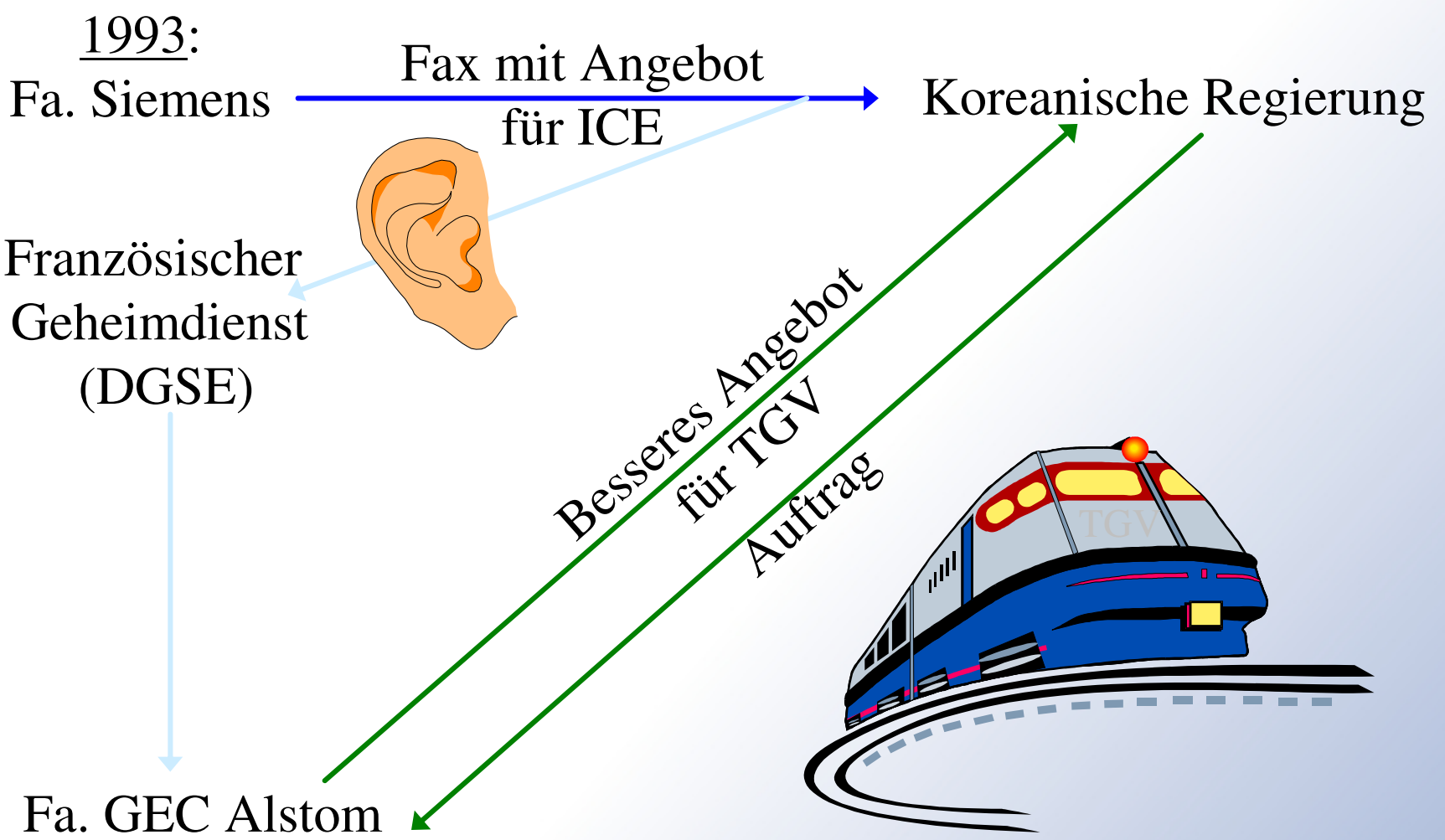
Ausbruch aus Firewall (Praxis 3/3)



- Resultat: *IP-over-Everything* möglich.
- Man kann IP auf jeder möglichen Kommunikation aufsetzen lassen; TCP-Pakete lassen sich auch über E-Mail transportieren.

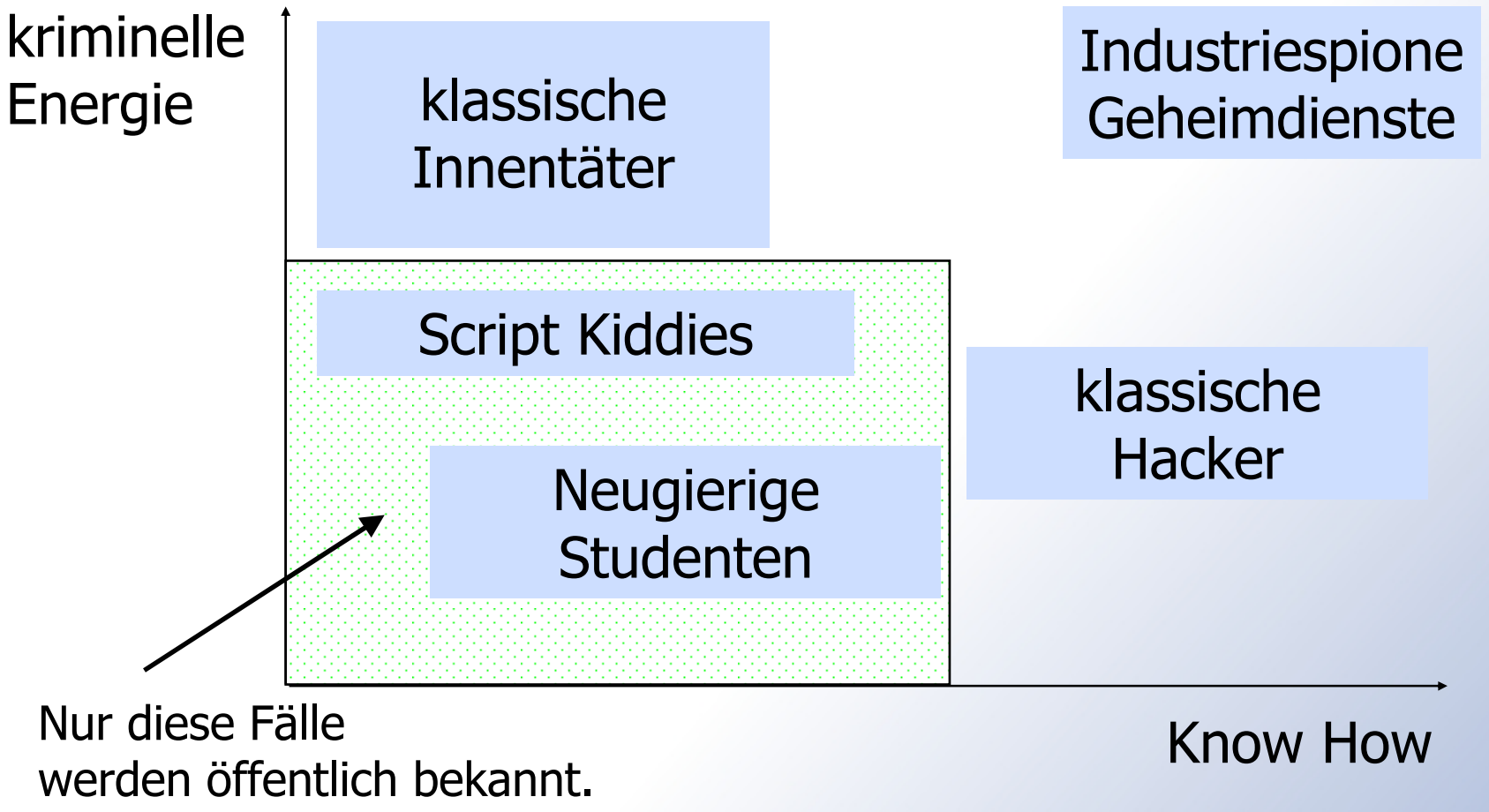
Resultat: sofern irgendeine Kommunikation mit dem Internet möglich ist, lassen sich sämtliche Zugangsrestriktionen einer FW außer Kraft setzen.

Fallbeispiel: Computerspionage



Abhörsystem ECHELON
Geheimdienste online?

Täterprofile



Wie erobert man einen Zugang eines E-Commerce-Servers?

z.B. so:

- Angriffe auf die Verbindungen (Sniffing, Spoofing, Hijacking).
- D.o.S.-Angriffe (Z.B. von Mafiaboy)
- Angriffe über HTTP
  - Buffer-Overruns
  - CGI-Attacken
  - Path-Climbing-Vulnerabilities
  - Meta-Character-Attacks
  - Direkter Zugriff möglich (z.B. bei Lotus Domino)
- Andere Dienste: FTP, TELNET, MS-SQL,...
- Schlecht konfigurierte Rechner