

Sicher ins Internet

Dieter Altmann
DH1GAE

1. Wer sind unsere Gegner?

2. IP-Adressen und Ports

3. Demo

4. Was ist jetzt zu tun?

a: grundsätzlich

b: von Zeit zu Zeit (verregnetes Wochenende)

d: bei einer Neuinstallation

c: wenn man einen Virus eingefangen hat

Unsere Gegner

Die Personen

↑
kriminelle
Energie

Know How →

↑
kriminelle
Energie

Industriespione
Geheimdienste
Ermittlungsdienste

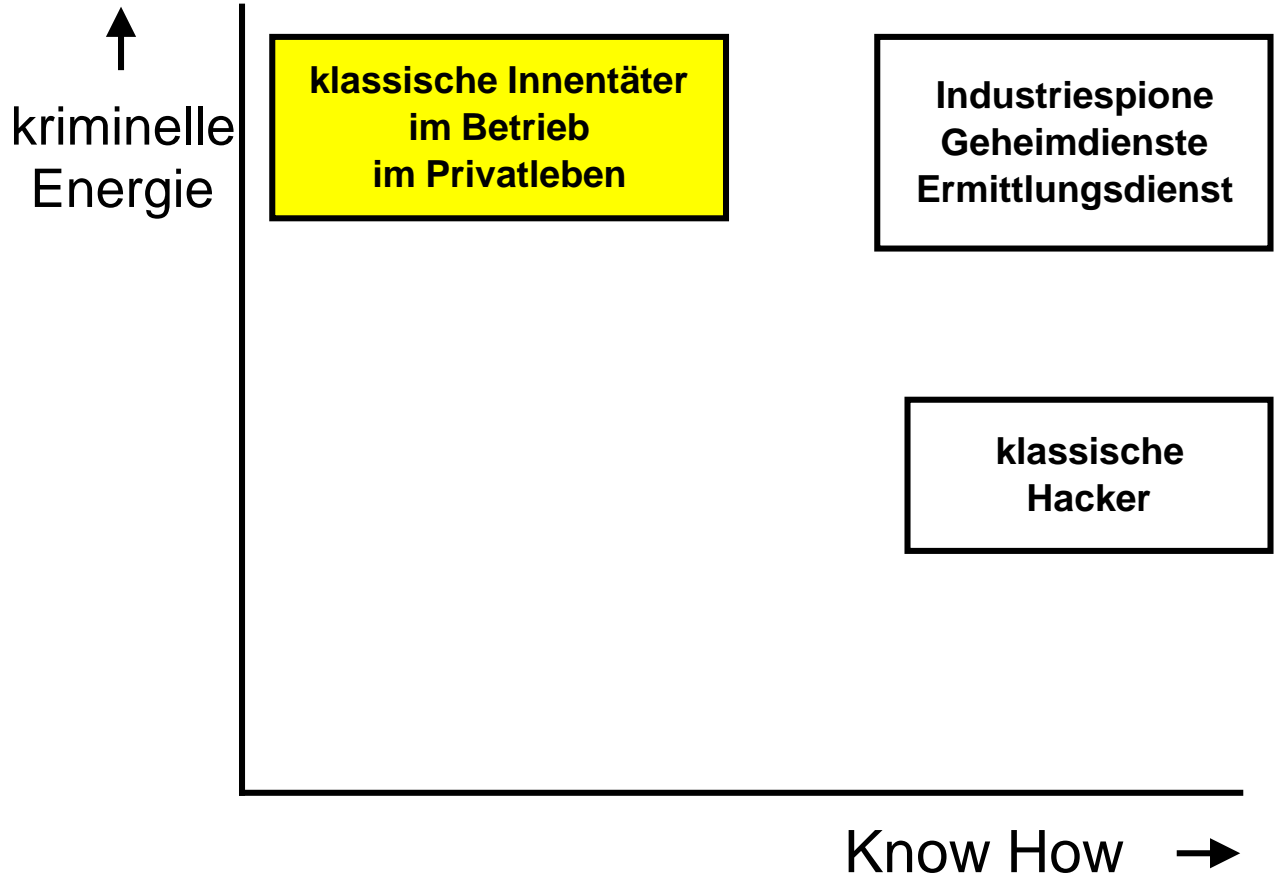
Know How →

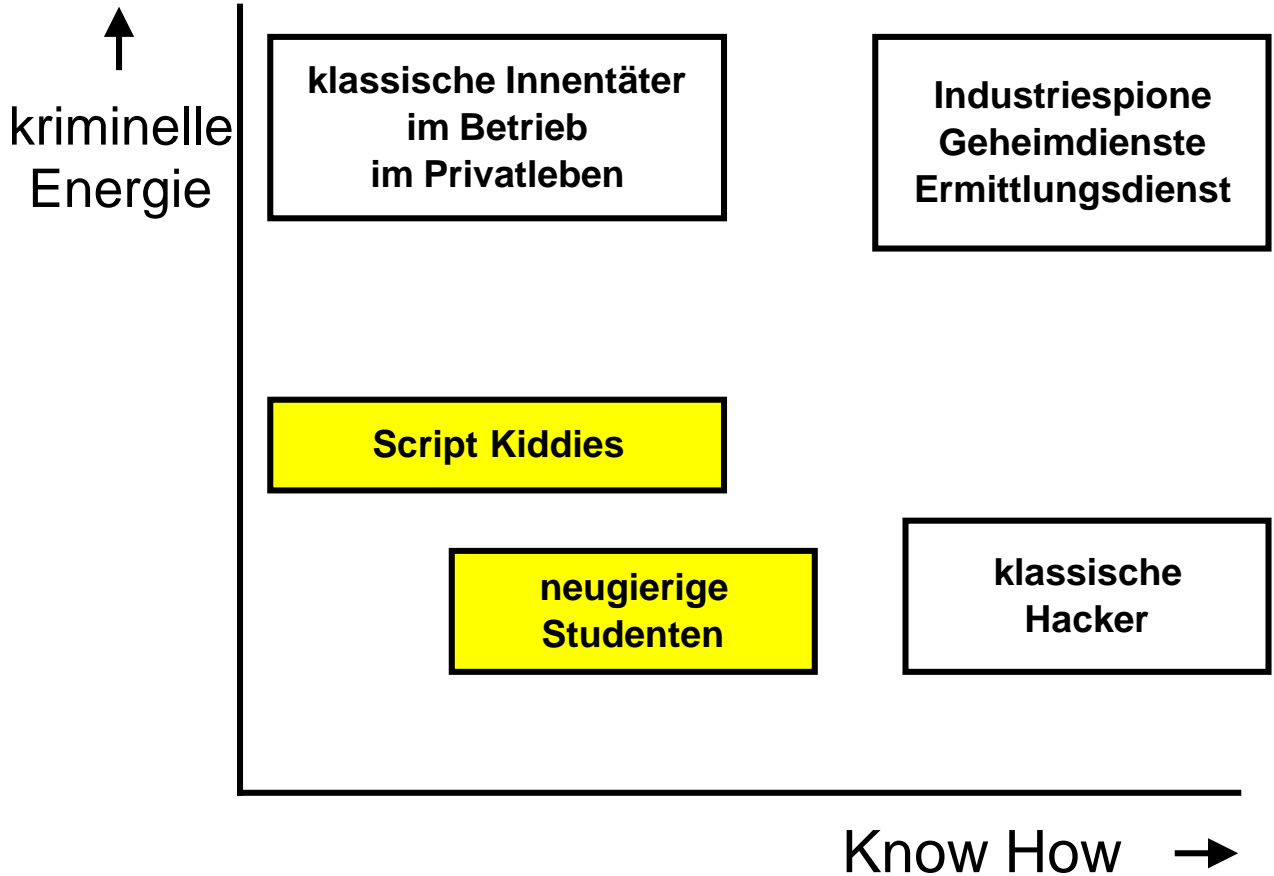
↑
kriminelle
Energie

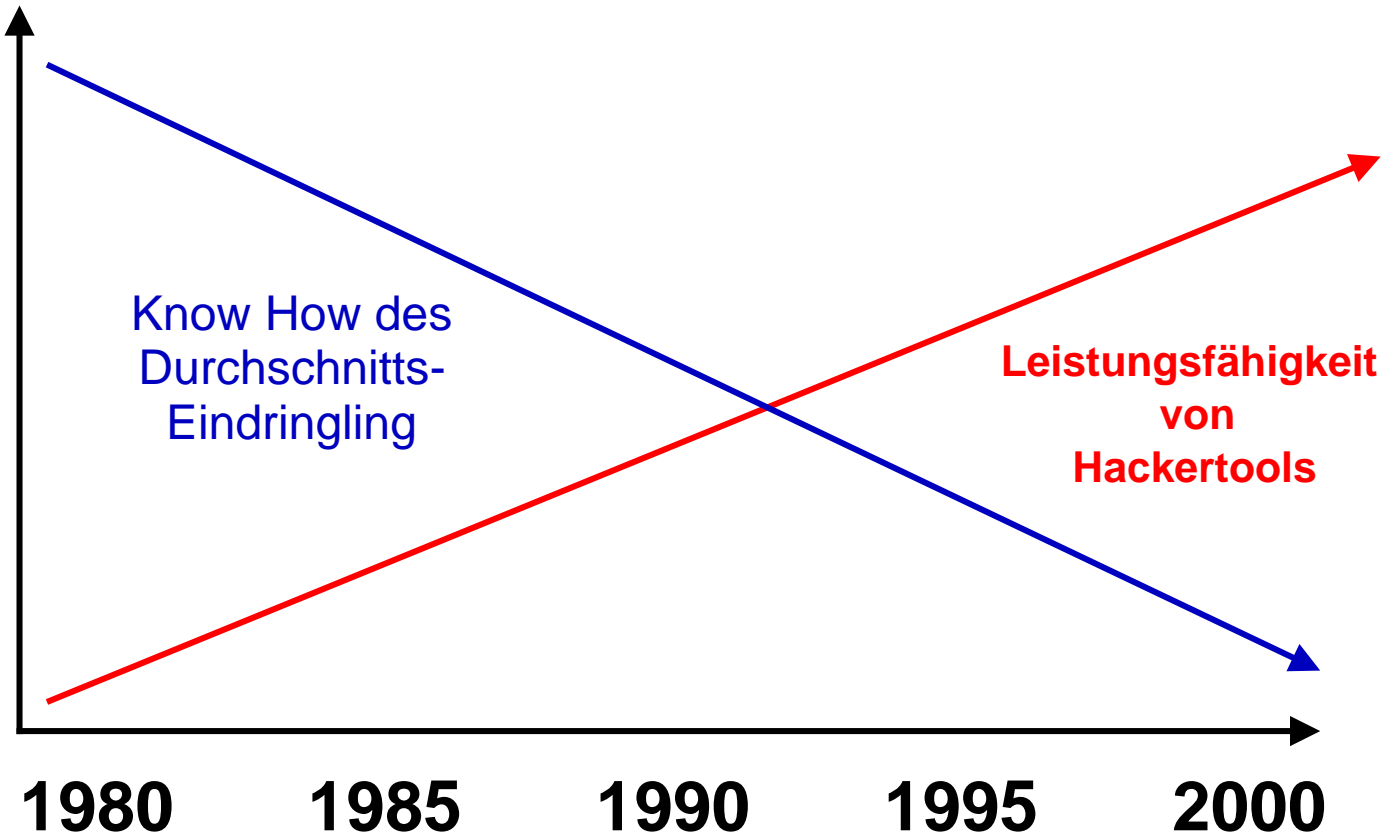
Industriespione
Geheimdienste
Ermittlungsdienst

klassische
Hacker

Know How →







Know How des
Durchschnitts-
Eindringling

Leistungsfähigkeit
von
Hackertools

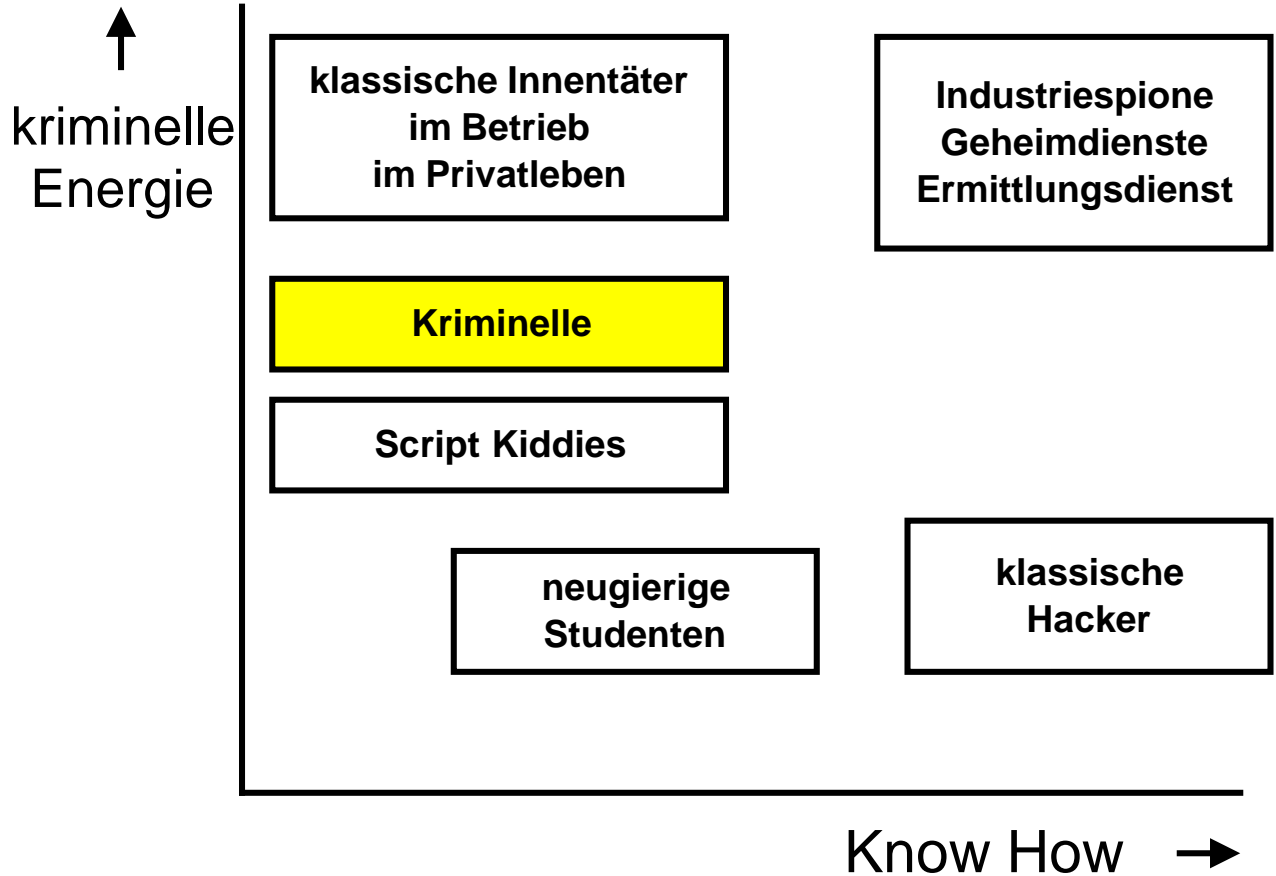
1980

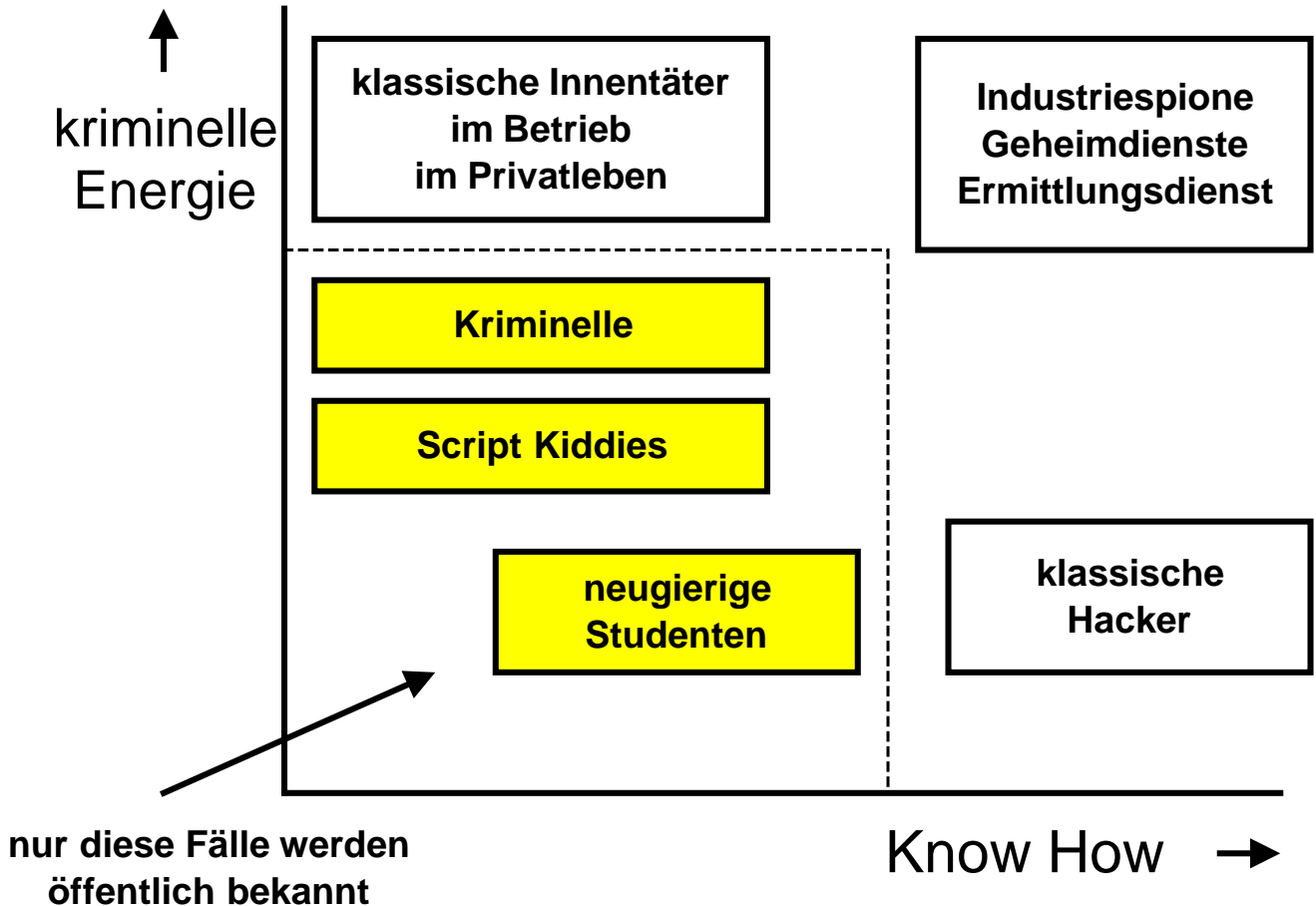
1985

1990

1995

2000





Unsere Gegner

Die Waffen

Phishing Mails

From: <Usersupport> usp@aol.com

To: <Dieter Altmann> armer-dieter@aol.com

Subject: Mailserver Problem

Sehr geehrter Benutzer,

aufgrund eines Plattencrashes sind Ihre Daten auf dem Mailserver beschädigt worden. Da wir jede Nacht Backups erstellen, können Sie davon ausgehen, dass kein Datenverlust vorliegt.

Bitte teilen Sie uns Ihr Passwort per Email mit, sodass wir die Backups mit Ihren Daten einspielen können.

Entschuldigen Sie die Unannehmlichkeiten.

Mit freundlichen Grüßen, Florian Maier, AOL.

Phishing Mails

Viren

Phishing Mails

Viren

Würmer

Phishing Mails

Viren

Würmer

Tojanische Pferde

Phishing Mails

Viren

Würmer

Tojanische Pferde

Backdoors

Phishing Mails

Viren

Würmer

Tojanische Pferde

Backdoors

Zombi-Tools

Phishing Mails

Viren

Würmer

Tojanische Pferde

Backdoors

Zombi-Tools

Rootkits

Phishing Mails

Viren

Würmer

Tojanische Pferde

Backdoors

Zombi-Tools

Rootkits

Browser-Hijacker

Phishing Mails

Viren

Würmer

Tojanische Pferde

Backdoors

Zombi-Tools

Rootkits

Browser-Hijacker

Spyware-Tools

Phishing Mails

Viren

Würmer

Tojanische Pferde

Backdoors

Zombi-Tools

Rootkits

Browser-Hijacker

Spyware-Tools

Dialer

Phishing Mails

Viren

Würmer

Tojanische Pferde

Backdoors

Zombi-Tools

Rootkits

Browser-Hijacker

Spyware-Tools

Dialer

Hoaxes

Phishing Mails

Viren

Würmer

Tojanische Pferde

Backdoors

Zombi-Tools

Rootkits

Browser-Hijacker

Spyware-Tools

Dialer

Hoaxes

USW... USW...

Unsere Gegner

Die Wege

Via E-Mail

Via Internet

Via Software

Via Tauschbörsen

Via "Freunde"

IP-Adressen und Ports

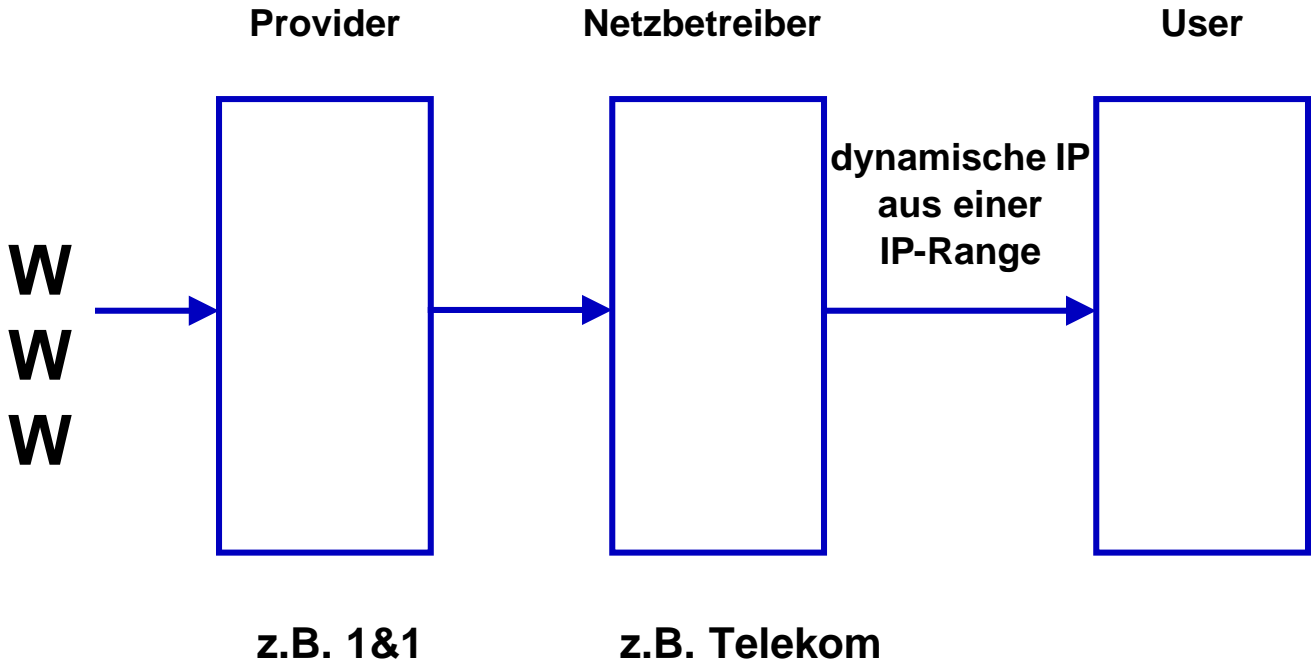
Kurze Einführung

sehr kurz :-)

80.127.34.223

80.127.34.223:80

192.168.1.1



Demo

extrem kurz :-)))

Was ist zu tun?

Grundsätzlich!

1. Lesen was da steht !!!!!

Nicht automatisch "OK" klicken

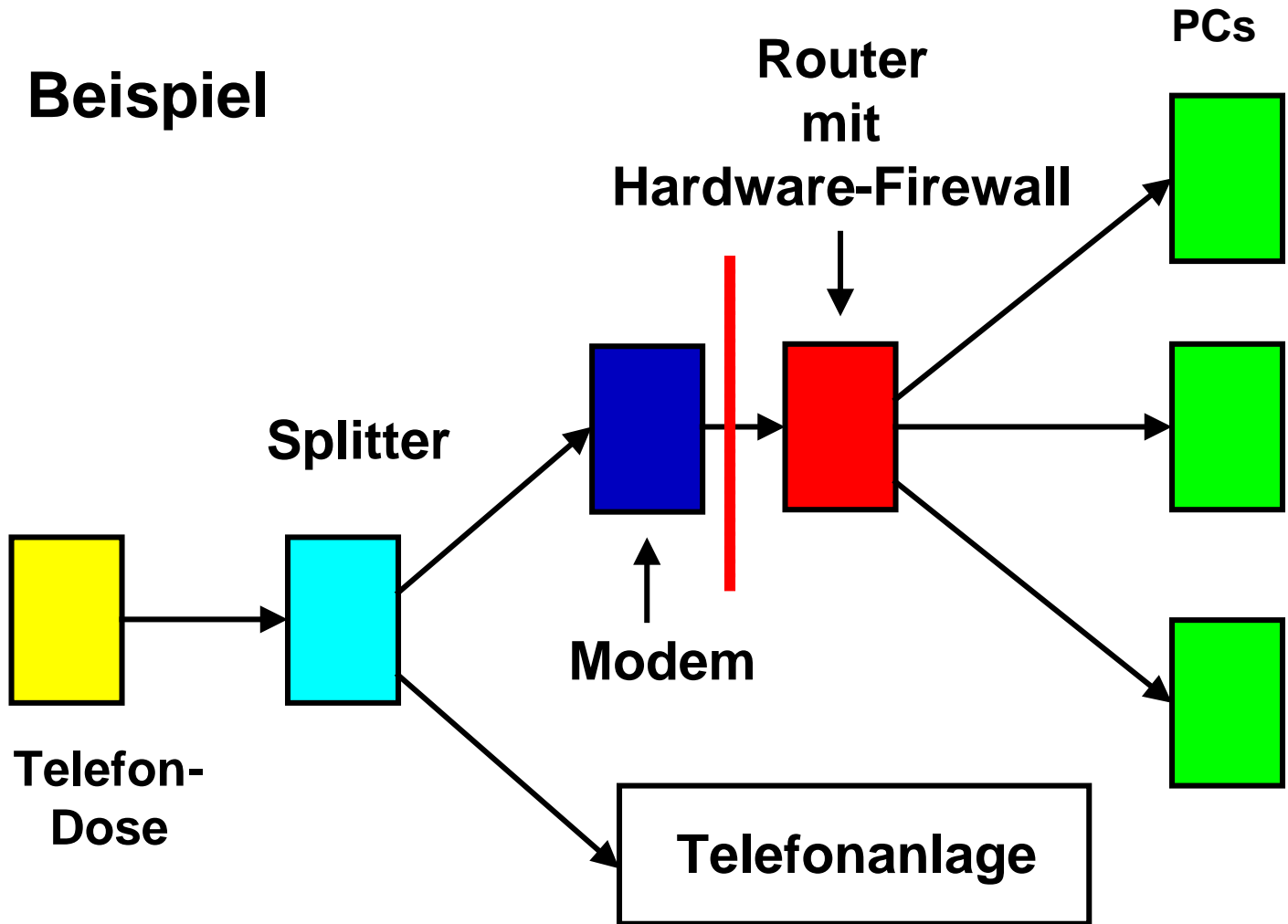
2. Virens Scanner einsetzen

Tagesaktuell !

3. Eine Firewall betreiben

Am besten extern
und zusätzlich
eine Personal-Firewall

Beispiel



4. E-Mails mit Umsicht behandeln

Besonders die Anhänge

5. Regelmäßig Daten extern sichern

Besonders die, die man selbst erstellt hat

6. Nicht als Administrator surfen

Extra User anlegen

7. Updates durchführen

Am besten automatisch

8. Dialer-Warner einsetzen

Nur bei Modem- oder ISDN-
Betrieb nötig

9. Phishing-sensibel reagieren

Niemals auf den in der E-Mail angegebenen Link gehen, sondern direkt auf die Seite der Bank

10. Auf Verschlüsselung achten

Schloss in der Symbolleiste

und (extra Thema "W-LAN")

Was ist zu tun?

Von Zeit zu Zeit

An einem verregneten
Wochenende

1. DSL-Speed-Manager einsetzen
2. Virens Scanner komplett durchlaufen lassen
3. Eicar-Testvirus einsetzen
4. Mit diversen Tools "spielen"
5. Log-Dateien anschauen
6. Task-Manager anschauen
7. Dienste anschauen
8. Computer-Zeitschriften lesen
9. Homepage "www.p18.org" besuchen
10. Sich selbst angreifen.

Was ist zu tun?

Bei einer Neuinstallation

1. Offline bleiben
2. Grundeinstellungendurchführen
3. Offline Virens Scanner installieren
4. Bei XP offline SP2 installieren
5. Online gehen
6. Virens Scanner aktualisieren
7. Betriebssystem aktualisieren
8. (Einträge im Task-Manager notieren)
9. Restliche Software aufspielen
10. Eventuell "Image" brennen

Was ist zu tun?

Wenn man einen "Schädling"
erwischt hat

1. Ruhe bewahren :-)
2. Nicht überreagieren
3. Virens Scanner von extern einsetzen
4. Infos bei Virens Scanner-Firmen einholen
5. Nach dem Problem "googeln"
6. Gegen-Tools einsetzen
7. Die verschiedenen Auto-Start-Stellen prüfen.
8. Registry überprüfen
9. Bei XP Wiederherstellung durchführen
10. Backup aufspielen

Ende

Noch Fragen ?