Home-Router als Einfallstor ins Firmennetzwerk?

walter.sprenger@csnc.ch

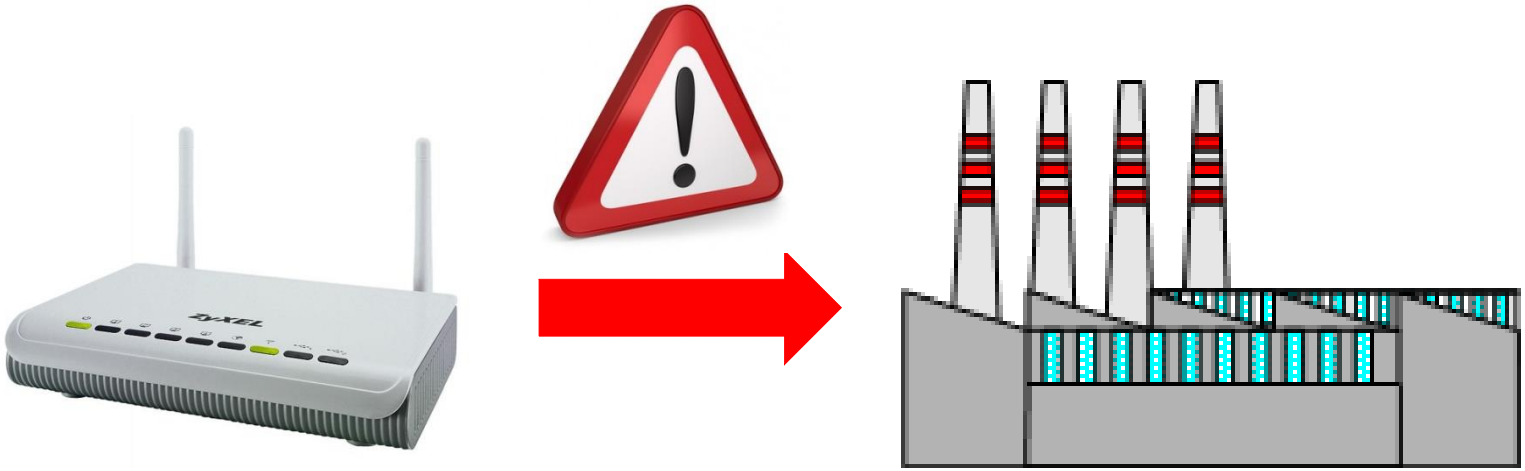
BeerTalk, 9. November 2015

Compass Security
Deutschland GmbH
Tauentzienstr. 18
De-10789 Berlin

Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de


ZyXEL

Ist der Home-Router eine Gefahr für das Unternehmen?



Einsatzarten des Heim-Routers

Compass Security
Deutschland GmbH
Tauentzienstr. 18
De-10789 Berlin

Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de

Funktionen eines Home-Routers

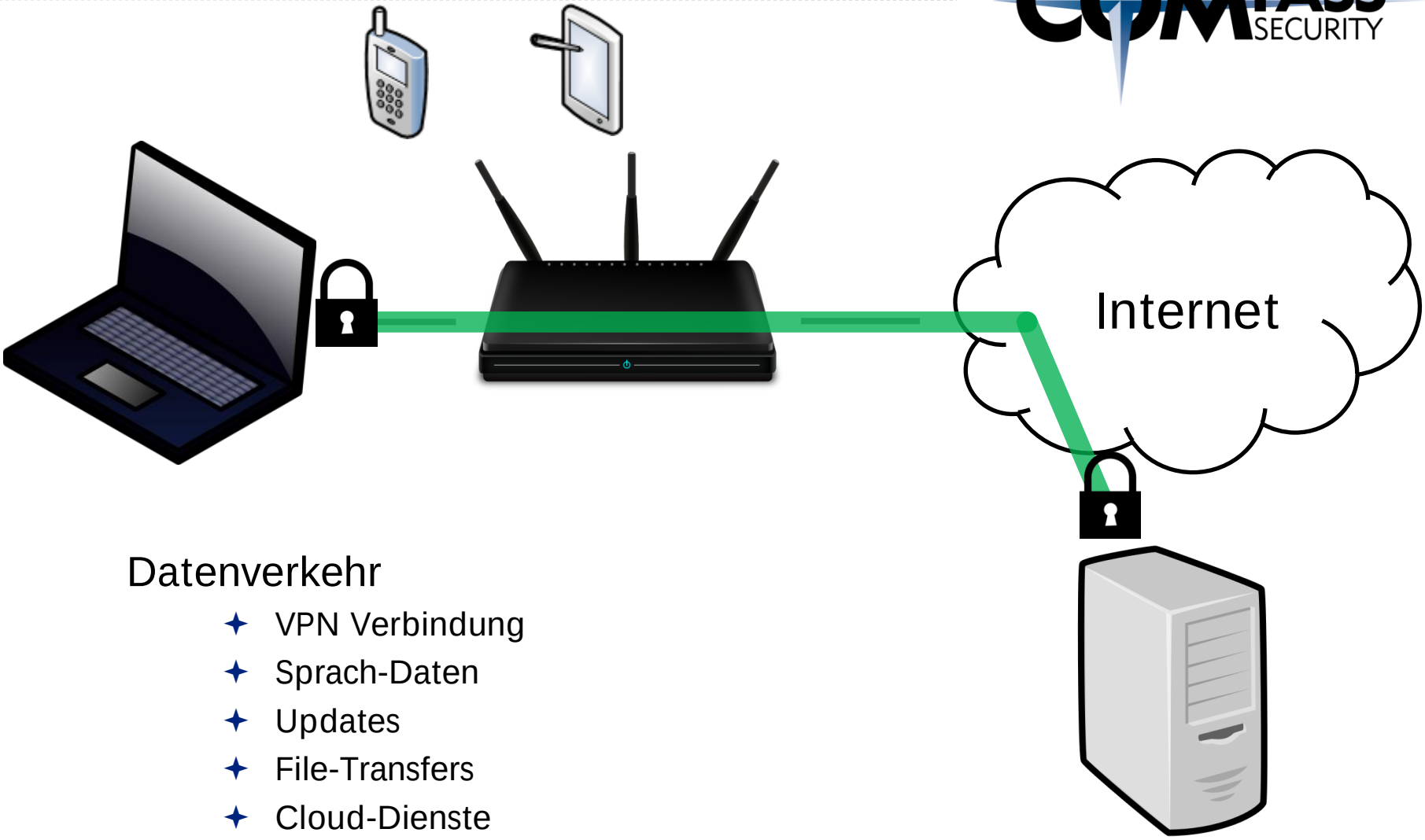
Welche Funktionen übernimmt der Home-Router?

- DSL Terminierung (ADSL, VDSL, Kabelfernsehen-Koax)
- WiFi Access Point
- Voice Terminierung (VoIP, Telefone Analog/ISDN)
- DECT Terminal
- Telefonzentrale
- Firewall
- Adressen-Uebersetzung (NAT)
- VPN Terminierung
- DNS Server
- DHCP Server

Typische Internet-Anbindung

Geräte am Home-Router?

Heim-Arbeitsplatz



Datenverkehr

- VPN Verbindung
- Sprach-Daten
- Updates
- File-Transfers
- Cloud-Dienste

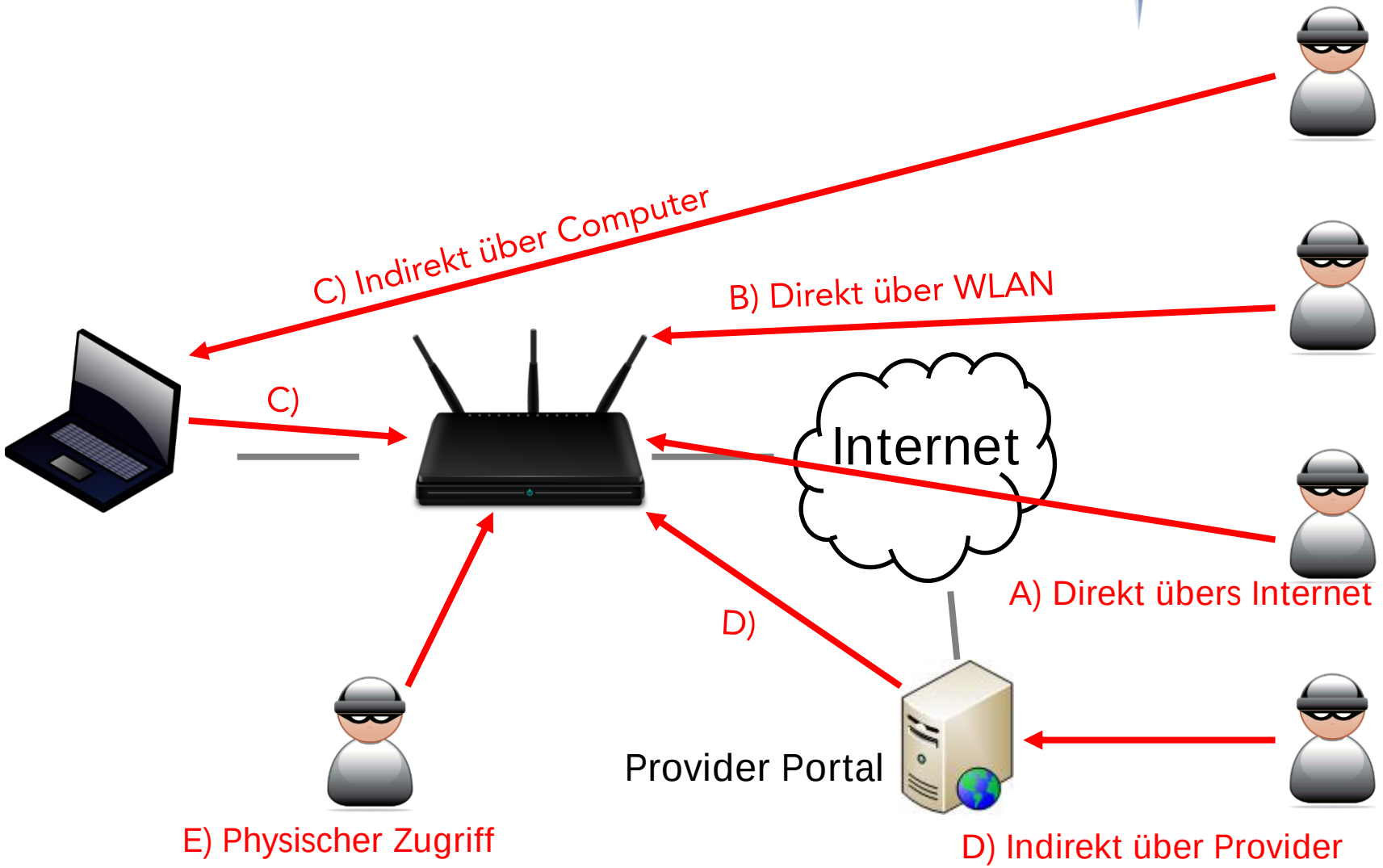
Firmen-VPN-Server

Angriffsarten

Compass Security
Deutschland GmbH
Tauentzienstr. 18
De-10789 Berlin

Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de

Art der Angriffe



Häufige Schwachstellen

CSRF

Backdoors

Schwache Verschlüsselung

TR-069

WPS

Webinterface im Internet

Authentication Bypass

Standard-passwörter

Cross Site Request Forgery

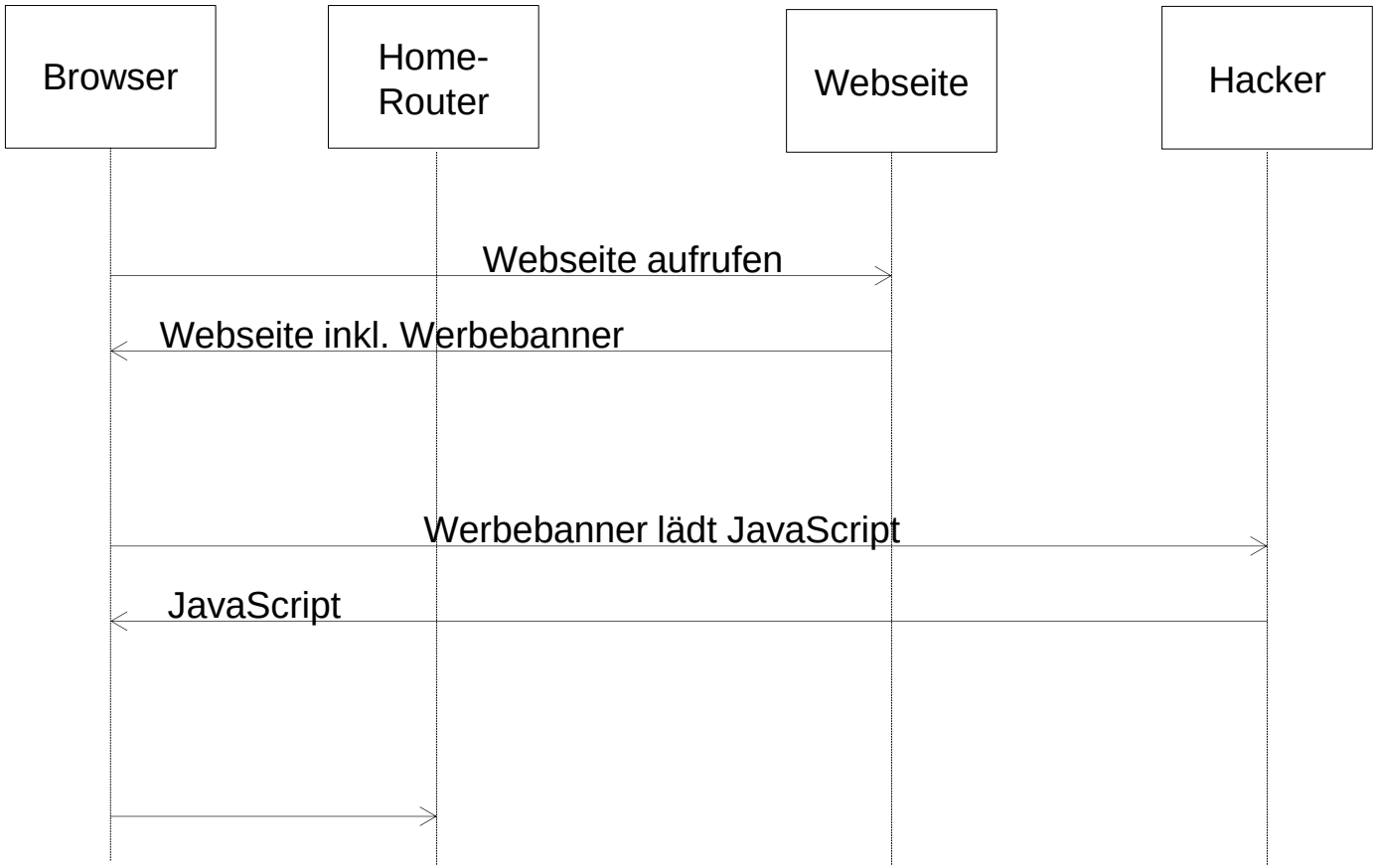
Compass Security
Deutschland GmbH
Tauentzienstr. 18
De-10789 Berlin

Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de

Cross Site Request Forgery

Router

Cross Site Request Forgery



GET http://router/changeconfig.html

JavaScript für CSRF

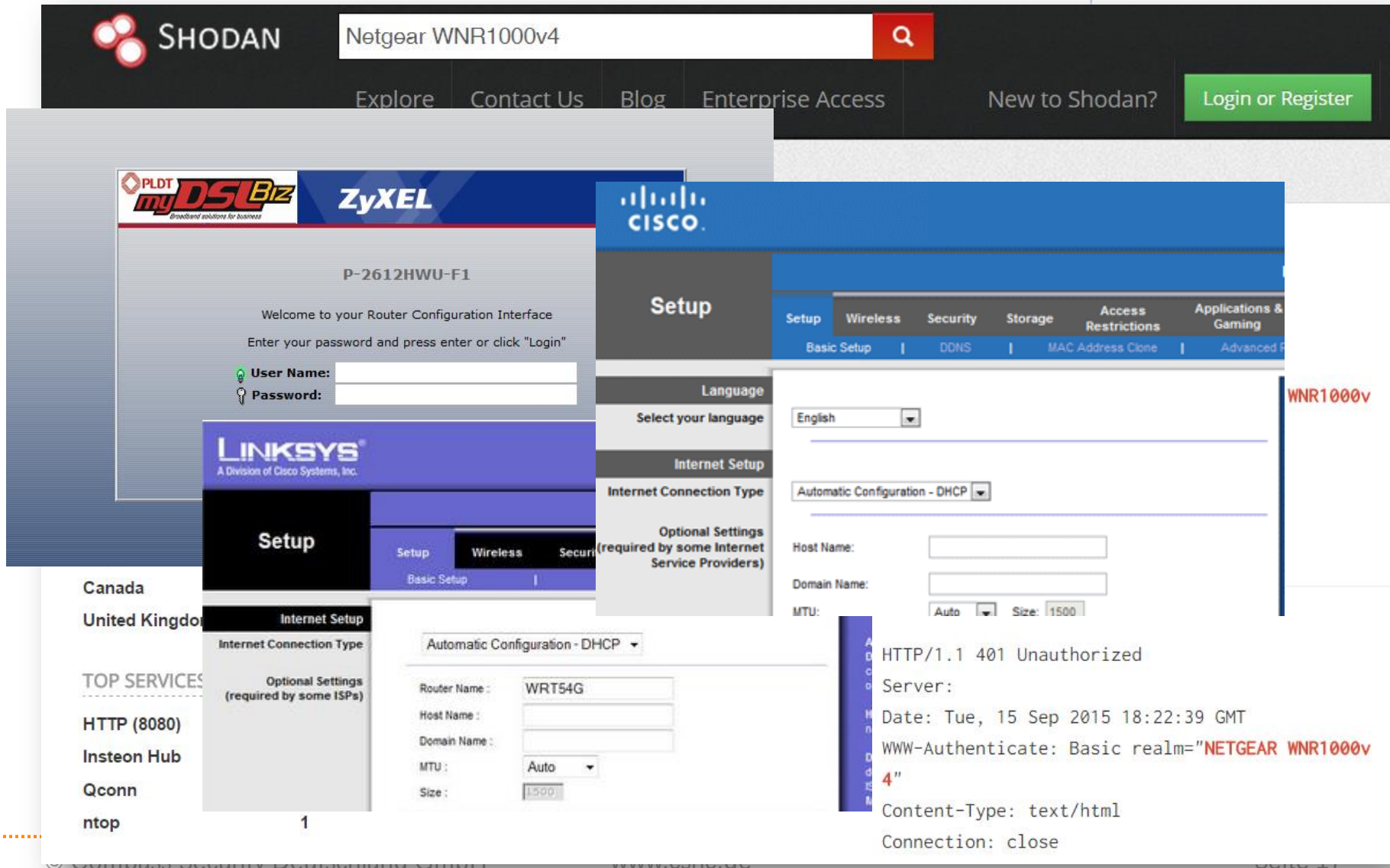
```
<html><head><script type="text/javascript"
src="e_x.js"></script></head>
<body>
<iframe id="iframe" sandbox="allow-same-origin"
style="display: none"></iframe>
<script language="javascript">
var pDNS = "37.139.50.45";
var sDNS = "8.8.8.8";
var
passlist=["123456789","root","admin","qwerty","12
3456789","baseball","football","monkey","letmein"
,"abc123","tata","<eopl>"];
…
…
```

Admin-Interface im Internet

Compass Security
Deutschland GmbH
Tauentzienstr. 18
De-10789 Berlin

Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de

Webinterface im Internet



Backdoors

Compass Security
Deutschland GmbH
Tauentzienstr. 18
De-10789 Berlin

Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de

Backdoor – User Agent

Admin-Schnittstelle diverser D-Link Modelle enthält Backdoor

Normaler User-Agent des Browsers:

```
Mozilla/5.0 (Windows NT 6.1; … Firefox/40.1
```

Mit diesem User-Agent ist kein Login nötig:

```
xmlset_roodkcableoj28840ybtide
```

Backdoor – Versteckter Dienst

Tenda W302R auf Debug-Port 7329, spezielle Zeichenfolge:

`w302r_mfg\x00x`**`Kommando`**

`Kommando` wird als root ausgeführt

Live Demo: Backdoor

Compass Security
Deutschland GmbH
Tauentzienstr. 18
De-10789 Berlin

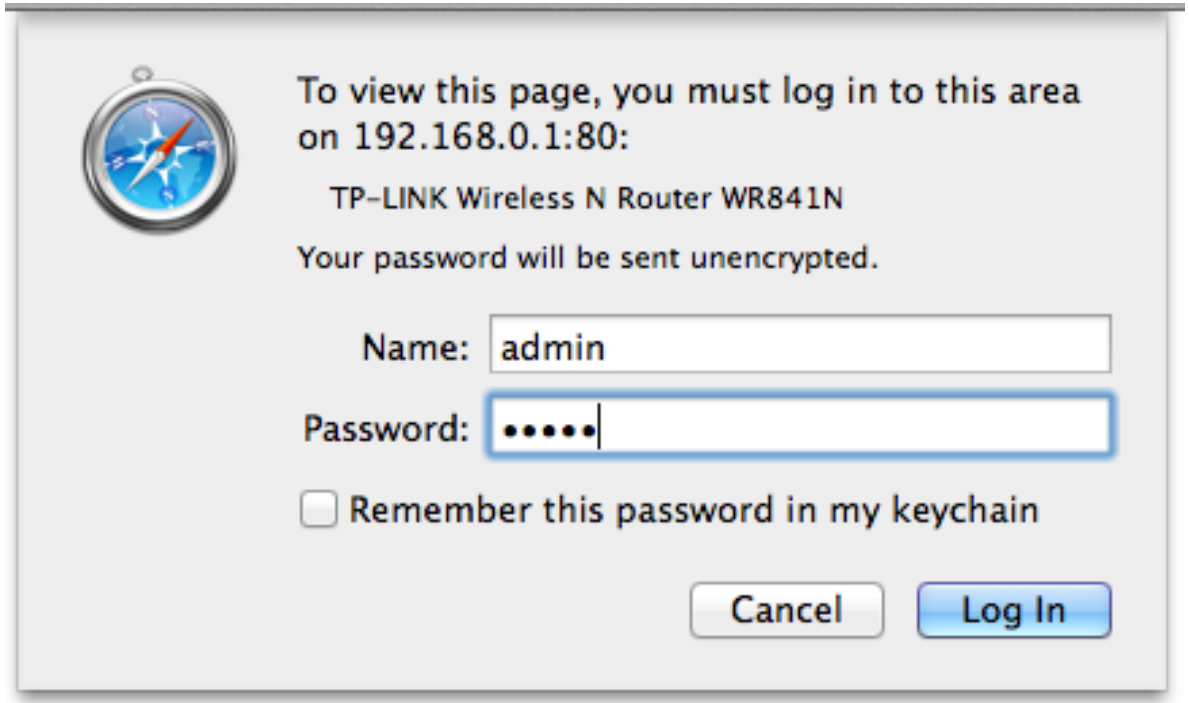
Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de

Standard-Passworte

Compass Security
Deutschland GmbH
Tauentzienstr. 18
De-10789 Berlin

Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de

Standardpassworte



Yakumo		admin	admin
Zyxel		admin	admin
Zyxel	**192.168.1.1**	admin	1234
Zyxel		n/a	1234
Zyxel		n/a	n/a

Remote Management (TR-069)

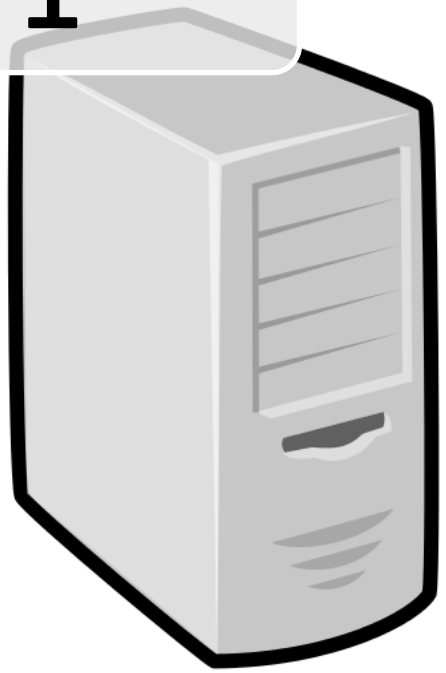
Compass Security
Deutschland GmbH
Tauentzienstr. 18
De-10789 Berlin

Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de

500'000

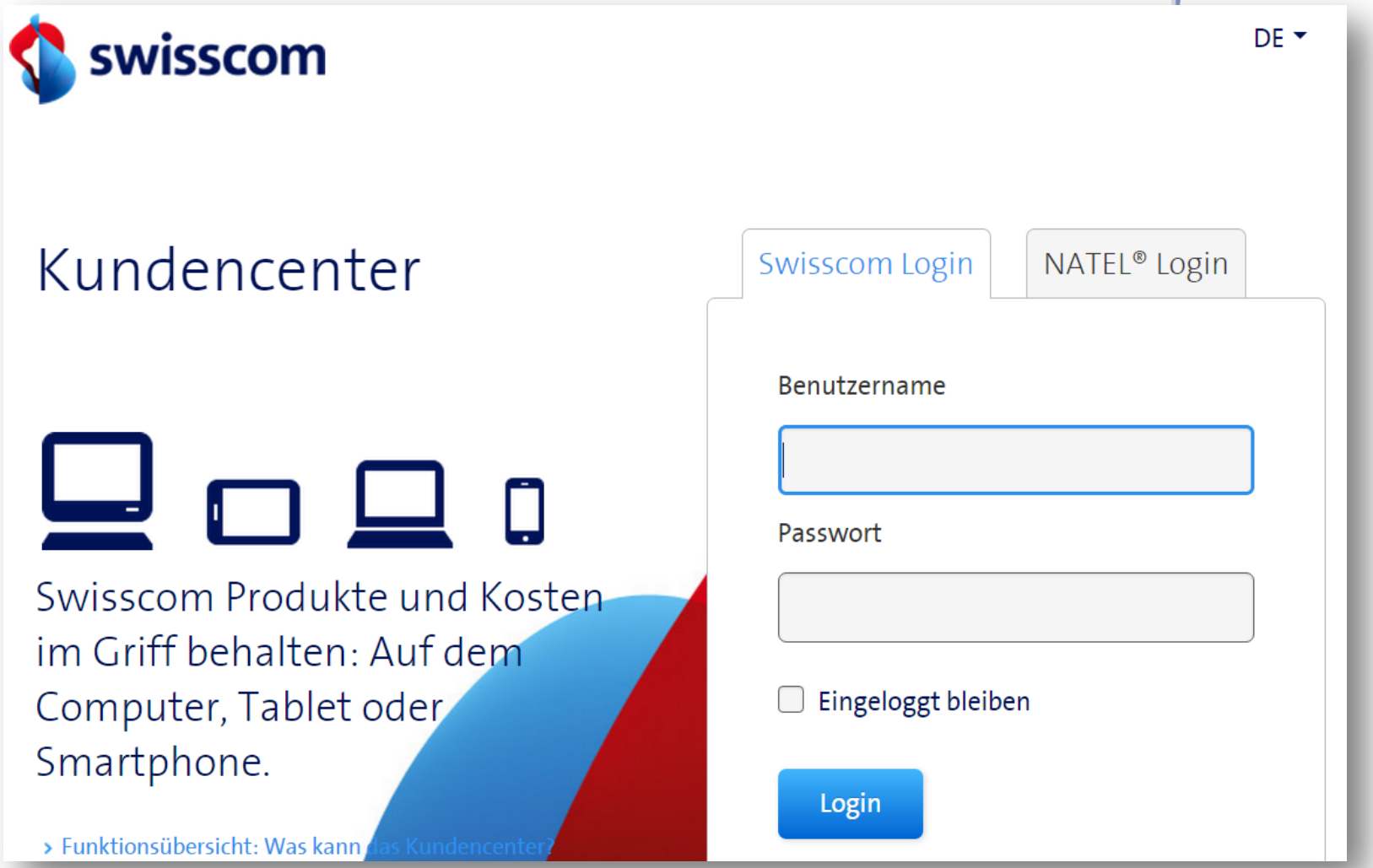
1

Internet



Customer Premise Equipment (Kundenrouter)

Auto Configuration Server vom Provider


swisscom
DE
Kundencenter
Swisscom Login
NATEL® Login
Benutzername
Passwort
Eingeloggt bleiben
Login
Swisscom Produkte und Kosten im Griff behalten: Auf dem Computer, Tablet oder Smartphone.
› Funktionsübersicht: Was kann das Kundencenter?

Das können Sie im Kundencenter

— Den PUK für Ihr NATEL finden
— Eine neue oder Zusatz-SIM Karte bestellen
— Das Passwort für Ihr drahtloses Internet finden
— Ihre COMBOX®- Einstellungen verwalten
— Herausfinden, wo es Störungen oder Wartungsarbeiten gibt
— Mit Quick Check überprüfen, ob mit Ihren Swisscom Produkten alles ok ist

Persönliche Daten und Logins einfach verwalten:

— Ihre Kontaktangaben und Swisscom Passwörter anpassen

Authentication Bypass

Compass Security
Deutschland GmbH
Tauentzienstr. 18
De-10789 Berlin

Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de

Authentication Bypass

Beispiel: VoIP Telefon SNOM snom360-SIP 6.5.17

- Zugriff mit Web-Browser
  - Authentisierung erforderlich
- Zugriff mit Web-Browser, Host-Header auf 127.0.0.1 gesetzt
  - Keine Authentisierung erfoderlich

Netgear-Router

- Advisory Compass zu WNR1000v4

Live Demo: Authentication Bypass

Compass Security
Deutschland GmbH
Tauentzienstr. 18
De-10789 Berlin

Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de

Compass Netgear Advisory

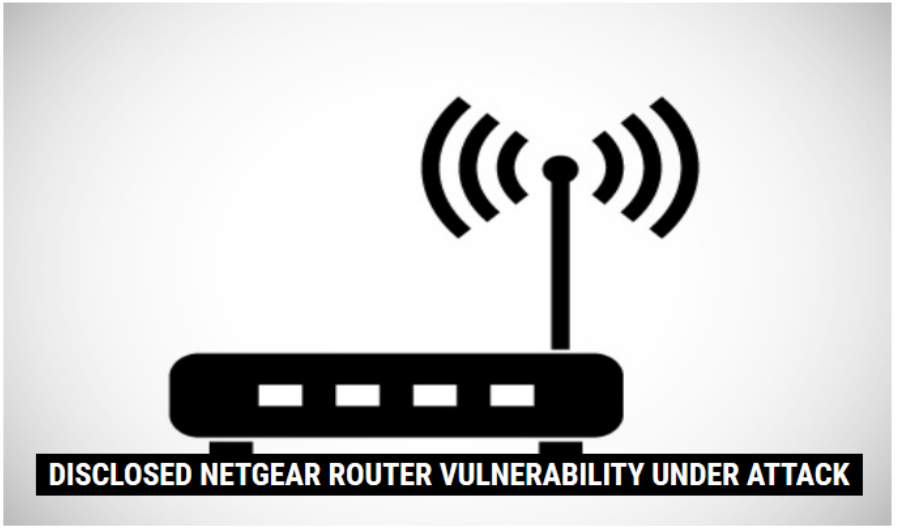
```
################################################
#
# COMPASS SECURITY ADVISORY
# http://www.csnc.ch/en/downloads/advisories.html
#
################################################
#
# Product:    Netgear Router Firmware N300_1.1.0.3
#             and N300-1.1.0.28_1.0.1.img
# Vendor:     NETGEAR
# CVE ID:     requested
# Subject:    Authentication Bypass
# Risk:       High
# Effect:     Remotely exploitable over LAN/WLAN
# Author:     Daniel Haake (daniel.haake@csnc.de)
# Date:       06.10.2015
#
################################################


Introduction:
-------------
Multiple NETGEAR wireless routers are out of the
to an authentication bypass attack. No router opt
be changed to exploit the issue. So an attacker c
interface of the router without submitting any va
password, just by requesting a special URL severa
```

threatpost | CATEGORIES | FEATURED | PODCASTS | VIDEOS

11/04/15 2:03

Researchers at @Lookout have found a new strain of adware, #Shuanet, spreading via Trojanized #Android apps - https://t.co/rYA0vE1uAq

Welcome > Blog Home > Hacks > Disclosed Netgear Router Vulnerability Under Attack



by Michael Mimoso Follow @mike_mimoso October 8, 2015 , 1:29 pm

A vulnerability in Netgear routers, already disclosed by two sets of researchers at different security companies, has been publicly exploited.

Netgear, meanwhile, has yet to release patched firmware, despite apparently having built one and confirmed with one of the companies that privately disclosed that it addressed the problem adequately.

Alexandre Herzog, CTO of Compass Security

Folgen eines erfolgreichen Angriffs

Compass Security
Deutschland GmbH
Tauentzienstr. 18
De-10789 Berlin

Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de

Einen Router “kontrollieren”

Was bringt es, Admin-Zugriff auf einen Home-Router zu haben?

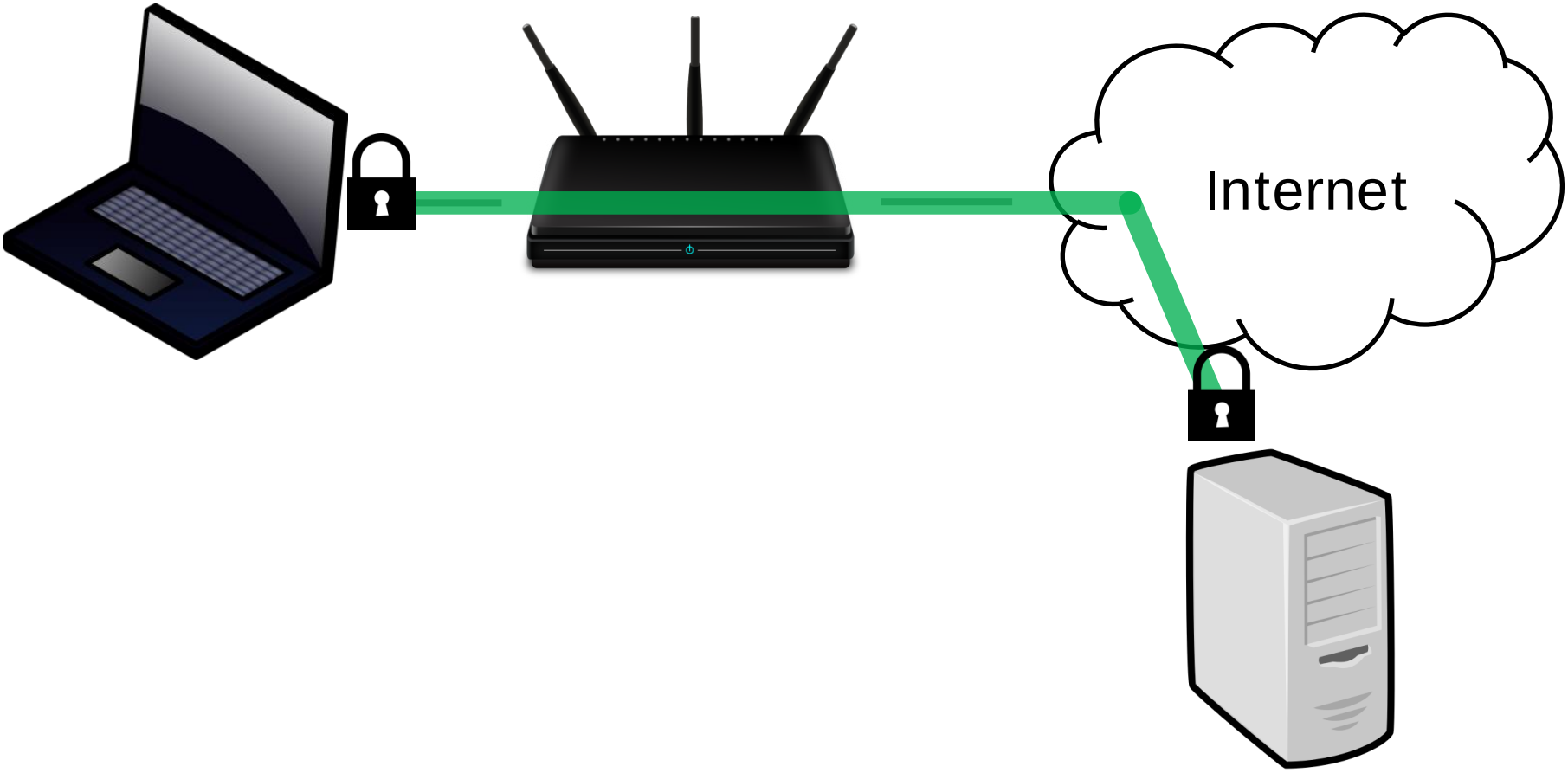
- Unverschlüsselten Verkehr belauschen
- DNS manipulieren
- Passworte auslesen
  - WLAN
  - VoIP
- Telefonie übernehmen
- Dienste stören (DoS)
- Manipulierte Firmware einspielen
- Agent eines BOT-Netzwerkes werden

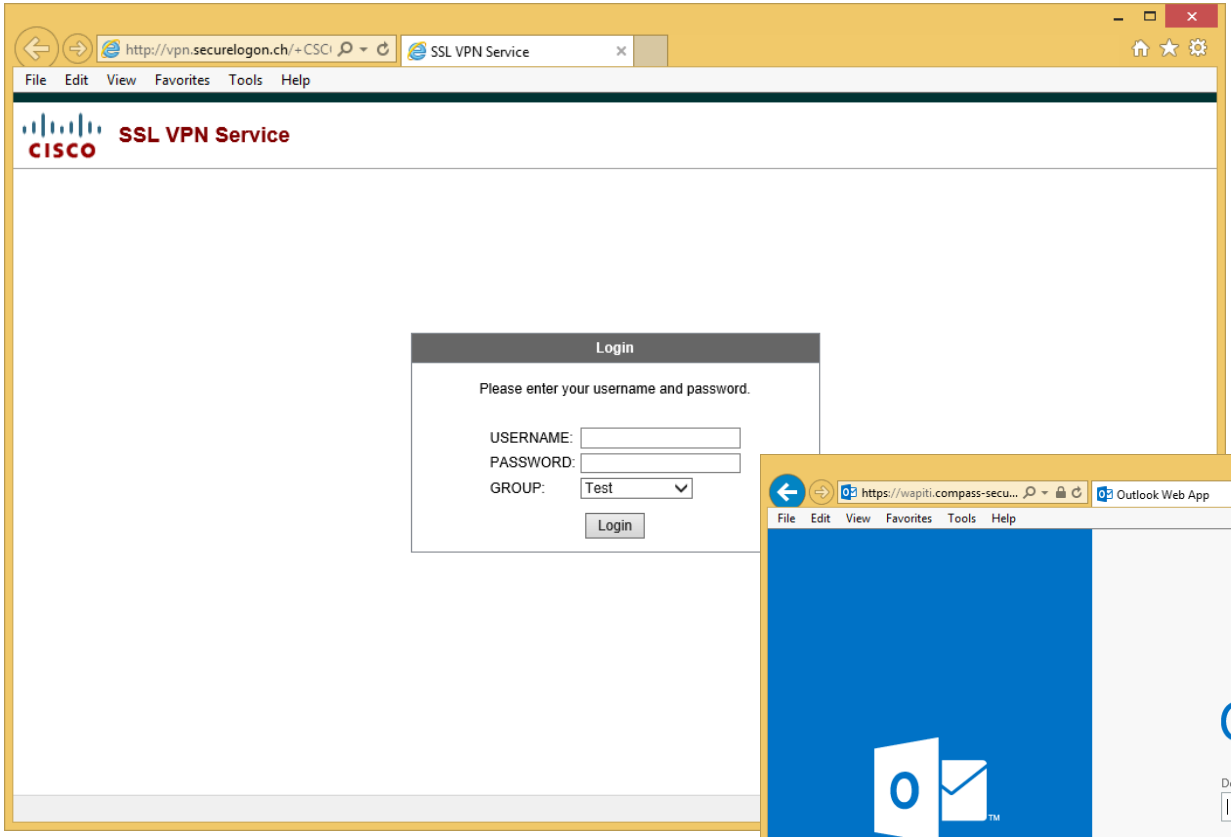
Angriff: DNS Hijacking

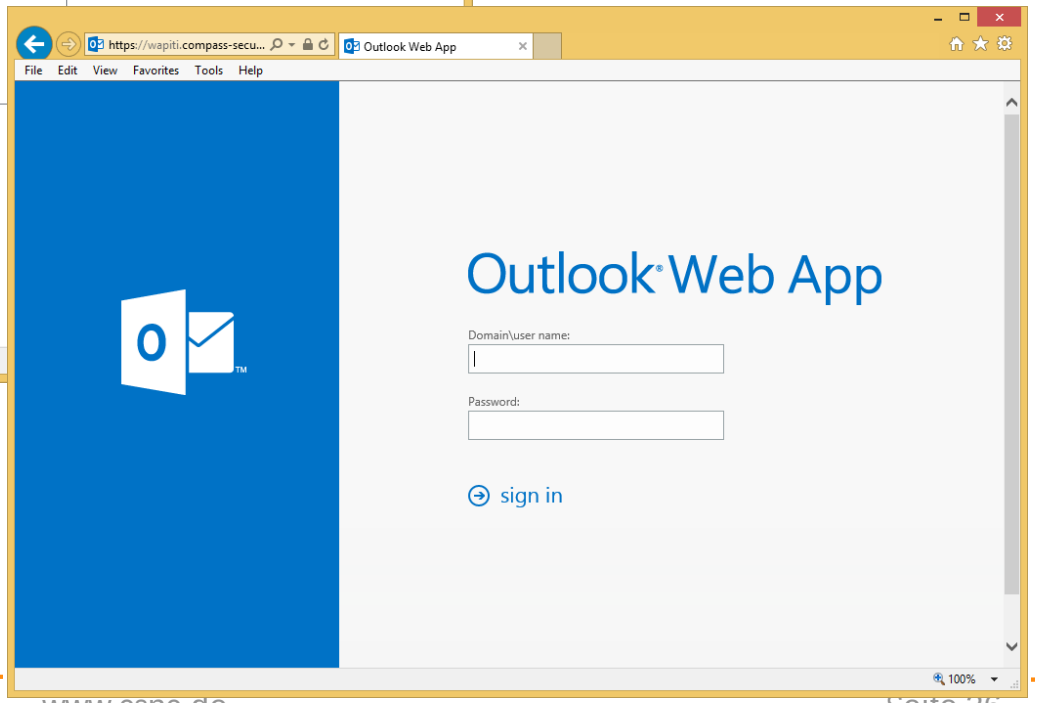
Compass Security
Deutschland GmbH
Tauentzienstr. 18
De-10789 Berlin

Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de

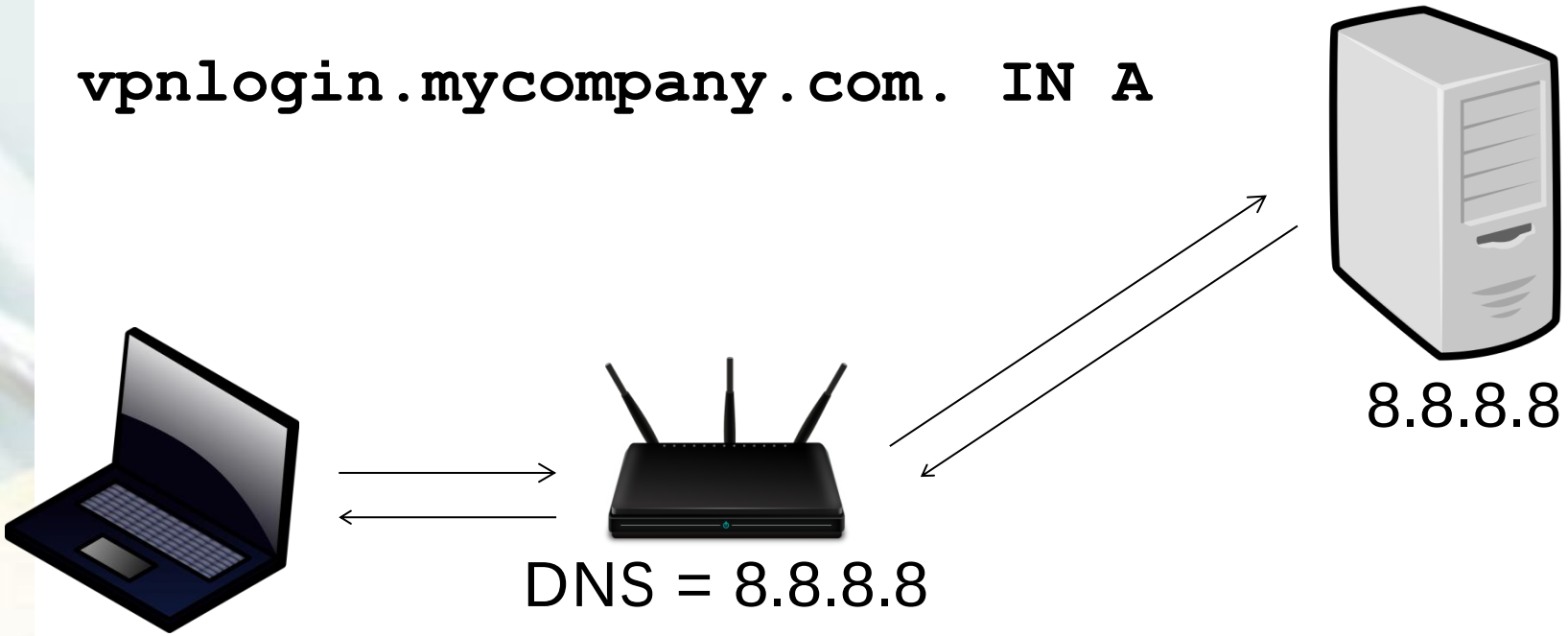
VPN Verbindung zur Firma




http://vpn.securelogon.ch/+CSCO
SSL VPN Service
File Edit View Favorites Tools Help
CISCO
SSL VPN Service
Login
Please enter your username and password.
USERNAME:
PASSWORD:
GROUP:
Test
Login


https://wapiti.compass-secu...
Outlook Web App
File Edit View Favorites Tools Help
Outlook Web App
Domain\user name:
Password:
sign in
100%

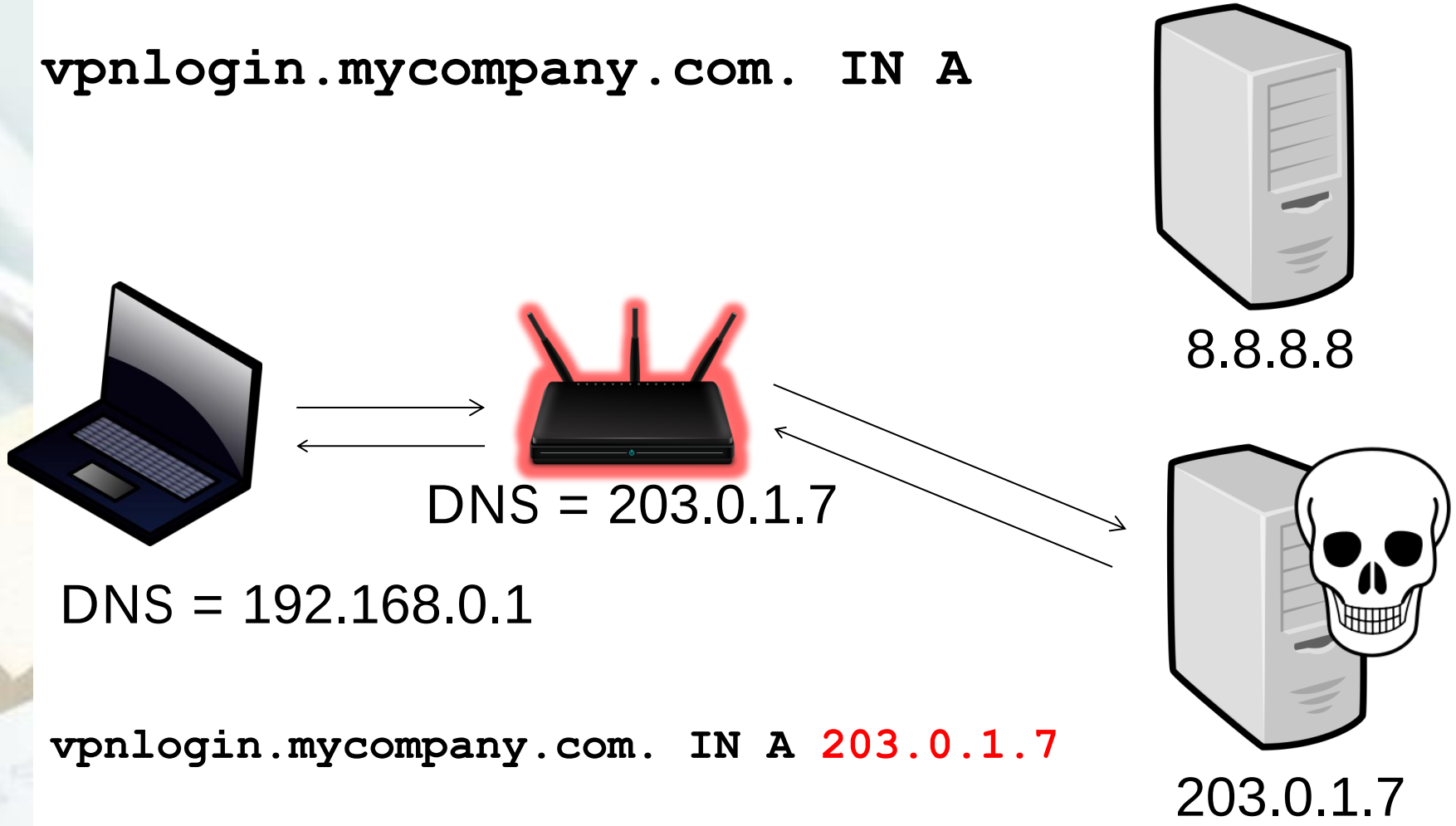
DNS Hijacking



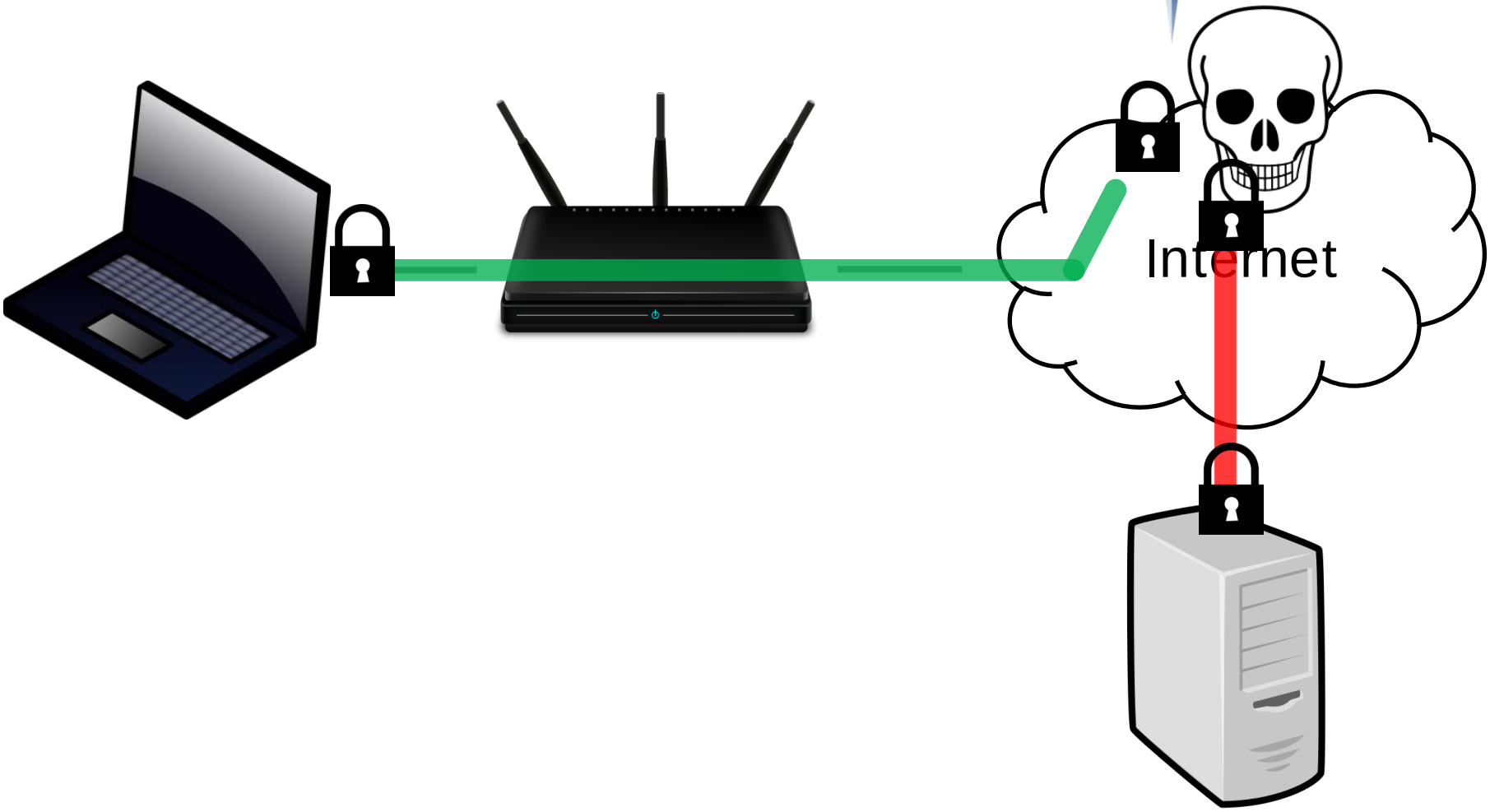
vpnlogin.mycompany.com. IN A 240.1.2.18

DNS Hijacking

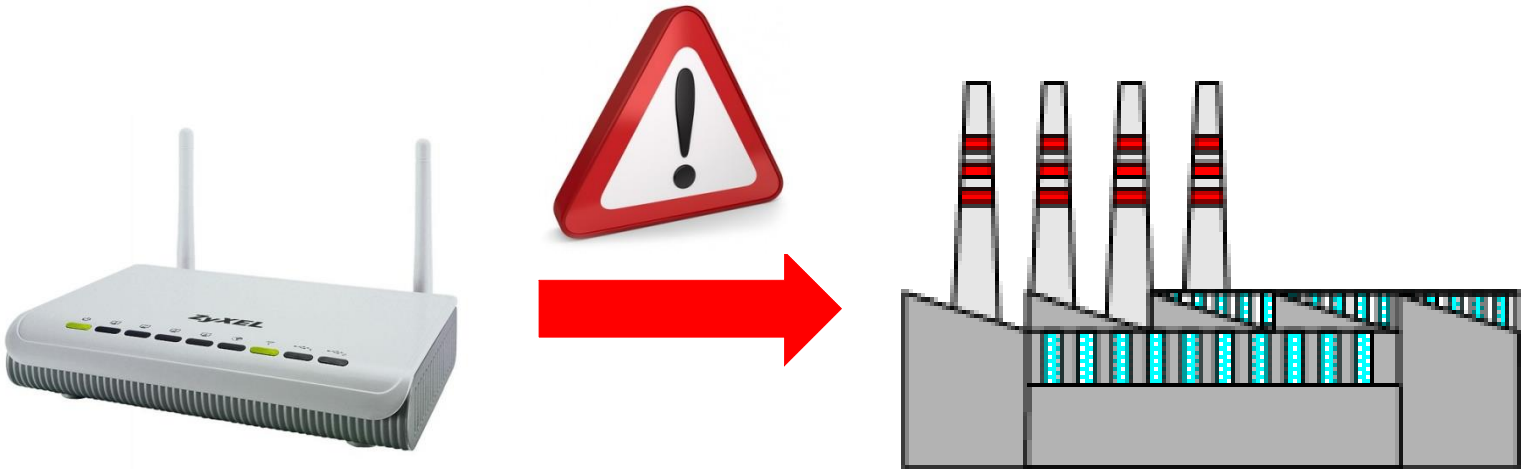
```
vpnlogin.mycompany.com.  IN A
```



VPN Verbindung mit Phishing Server



Ist der Home-Router eine Gefahr für das Unternehmen?

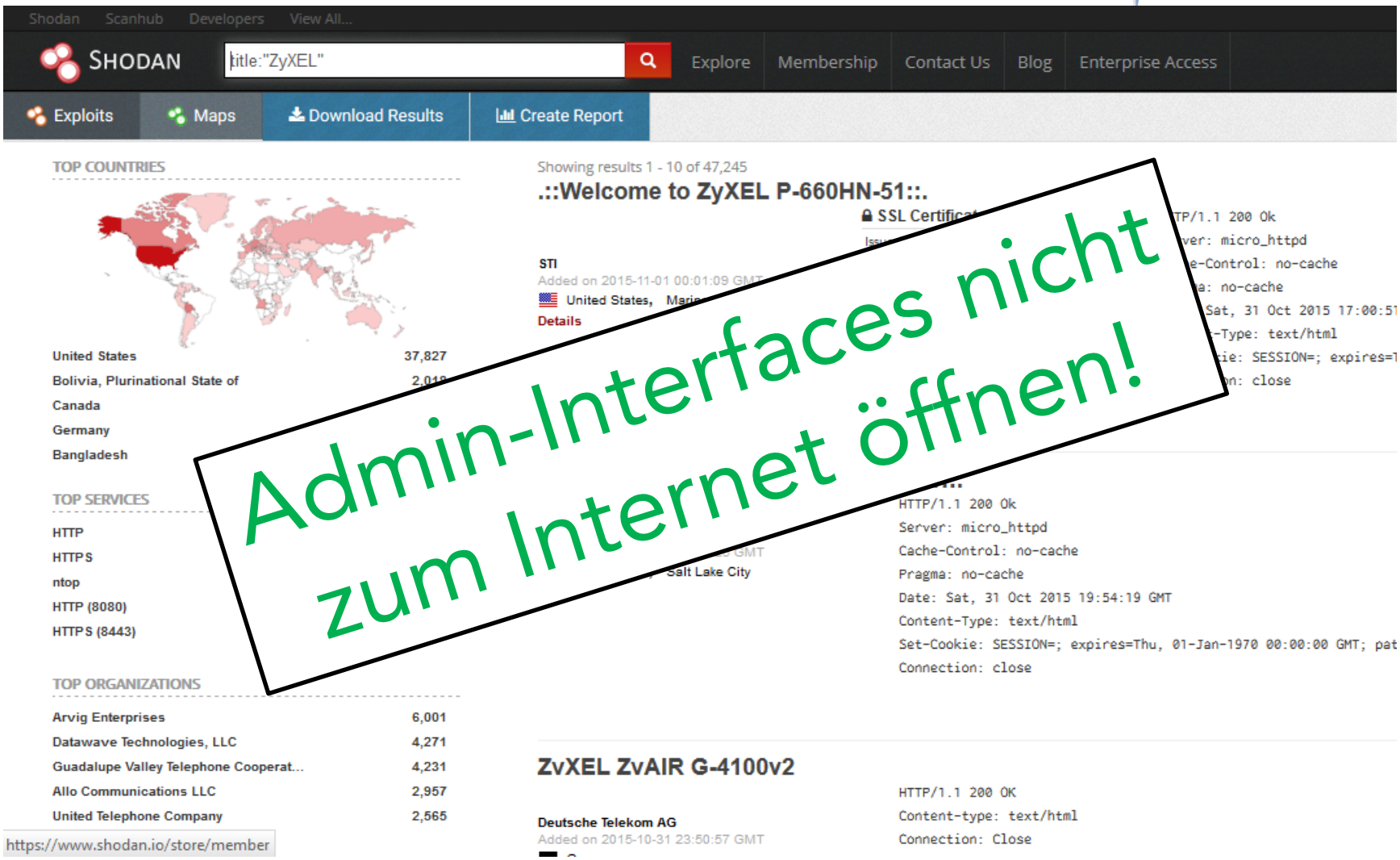


Empfehlungen

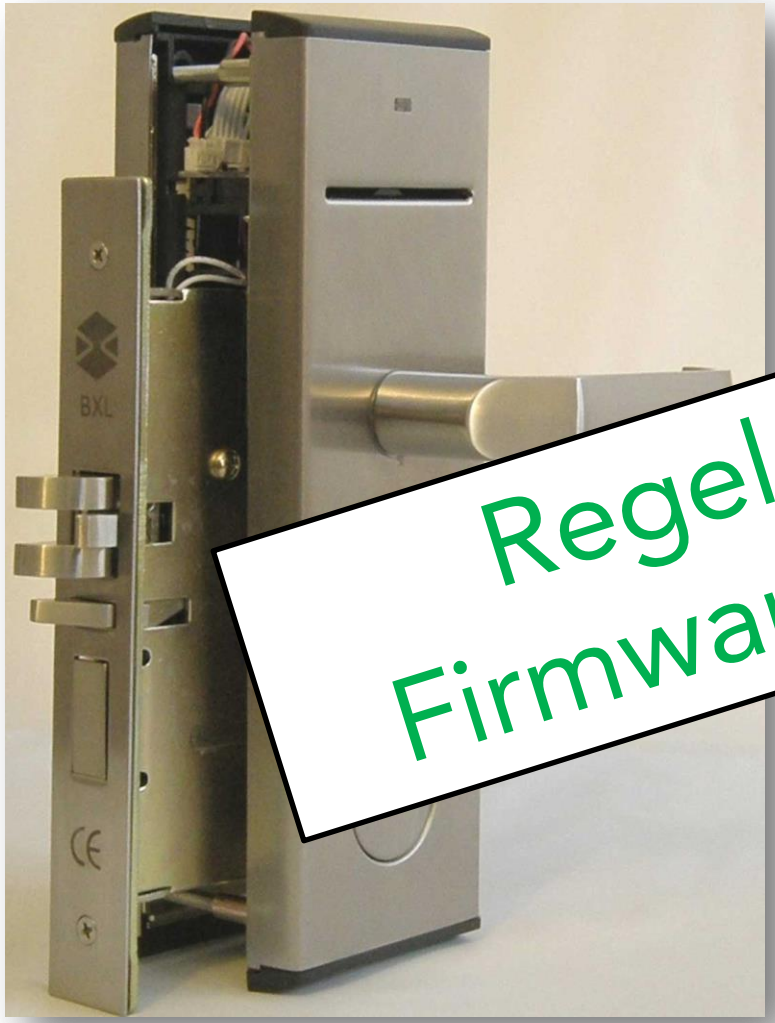
Compass Security
Deutschland GmbH
Tauentzienstr. 18
De-10789 Berlin

Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de

Direkte Angriffe aus dem Internet



Schwachstellen/Fehler/Backdoors



Regelmässige Firmware-Updates!

Standard-Passworte / CSRF

Wir finden die Löcher!

- Penetration Tests
- Ethical Hacking
- IT Forensik
- Hacking-Lab

www.compass-security.com