

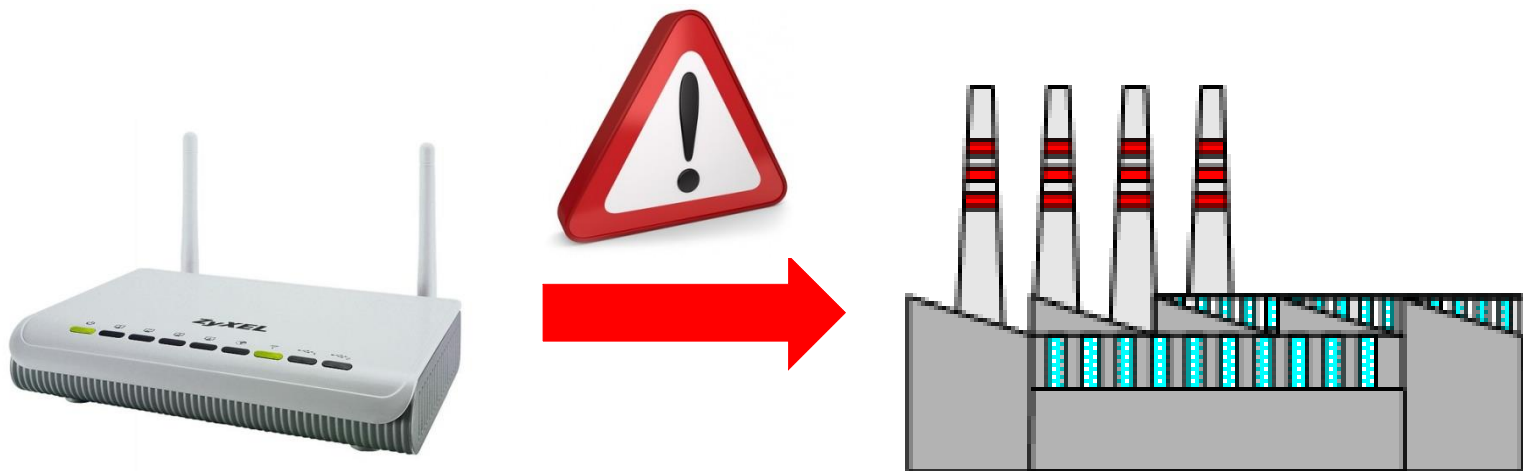
Home-Router als Einfallstor ins Firmennetzwerk?

walter.sprenger@csnc.ch
BeerTalk, 9. November 2015





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

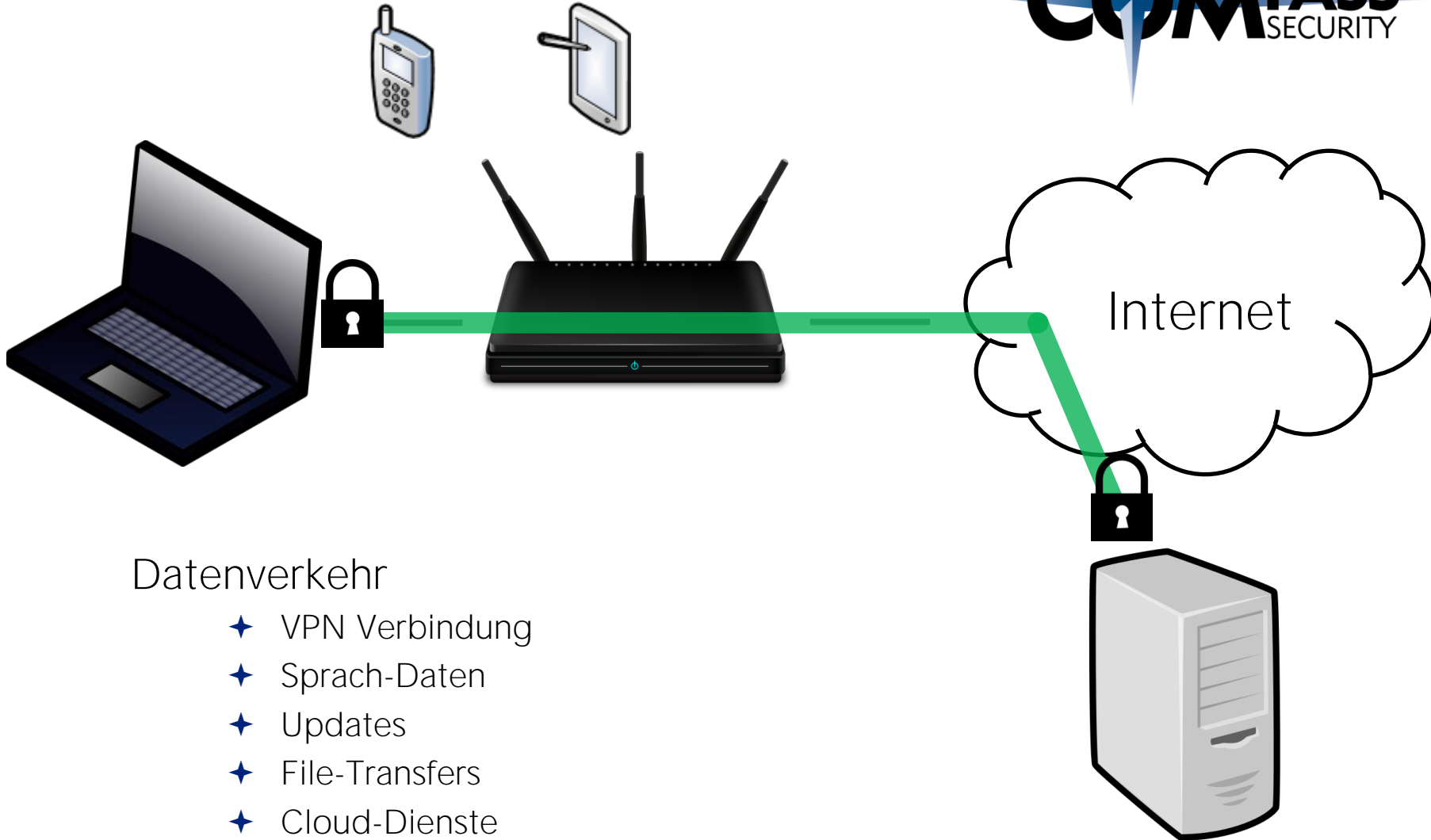
Welche Funktionen übernimmt der Home-Router?

- ✦ 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



Geräte am Home-Router?





Datenverkehr

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

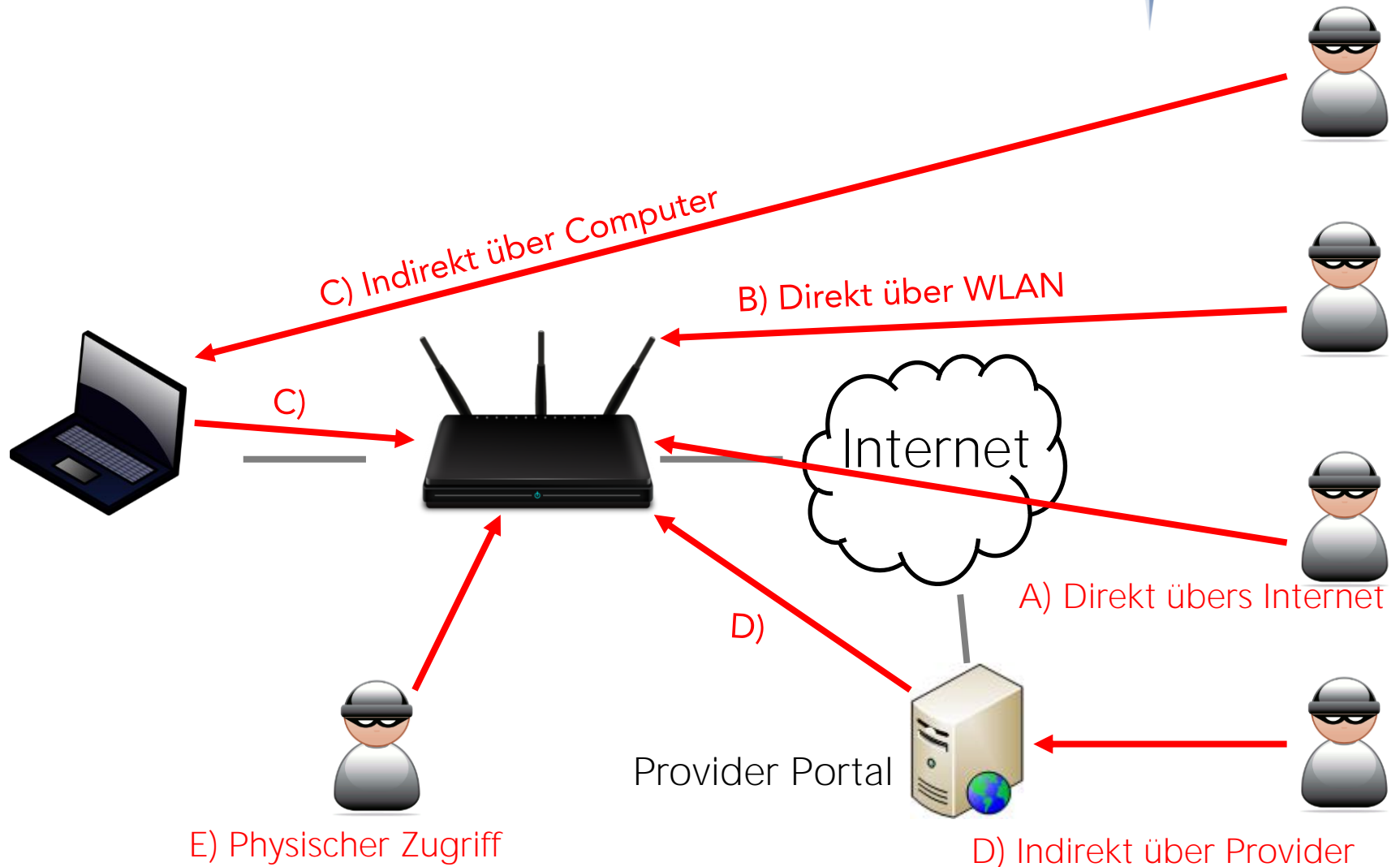
Firmen-VPN-Server



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



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



Login Abonnieren Immo · Auto · Job · Marktplatz · Trauer · SonntagsZeitung · Das Magazin Suche


Letztes Update: 14:20 Uhr

Tagesanzeiger

12°/10°


Front Zürich Schweiz International Wirtschaft Börse Sport Kultur Leben Wissen Auto Blogs Panorama Mehr ▾

Wahlbörse Schweiz – Gewinner: FDP +2.0, SP +1.6, SVP +0.6 – Verlierer: CVP -0.8, Grüne -0.8, BDP -0.3 – Jetzt mitmachen / Zum Wahlspezial



Jetzt mit Mi-Fonds ordentlich zulegen.

Companys ist pleite und schliesst zwölf Läden



Meistgelesen Newsticker

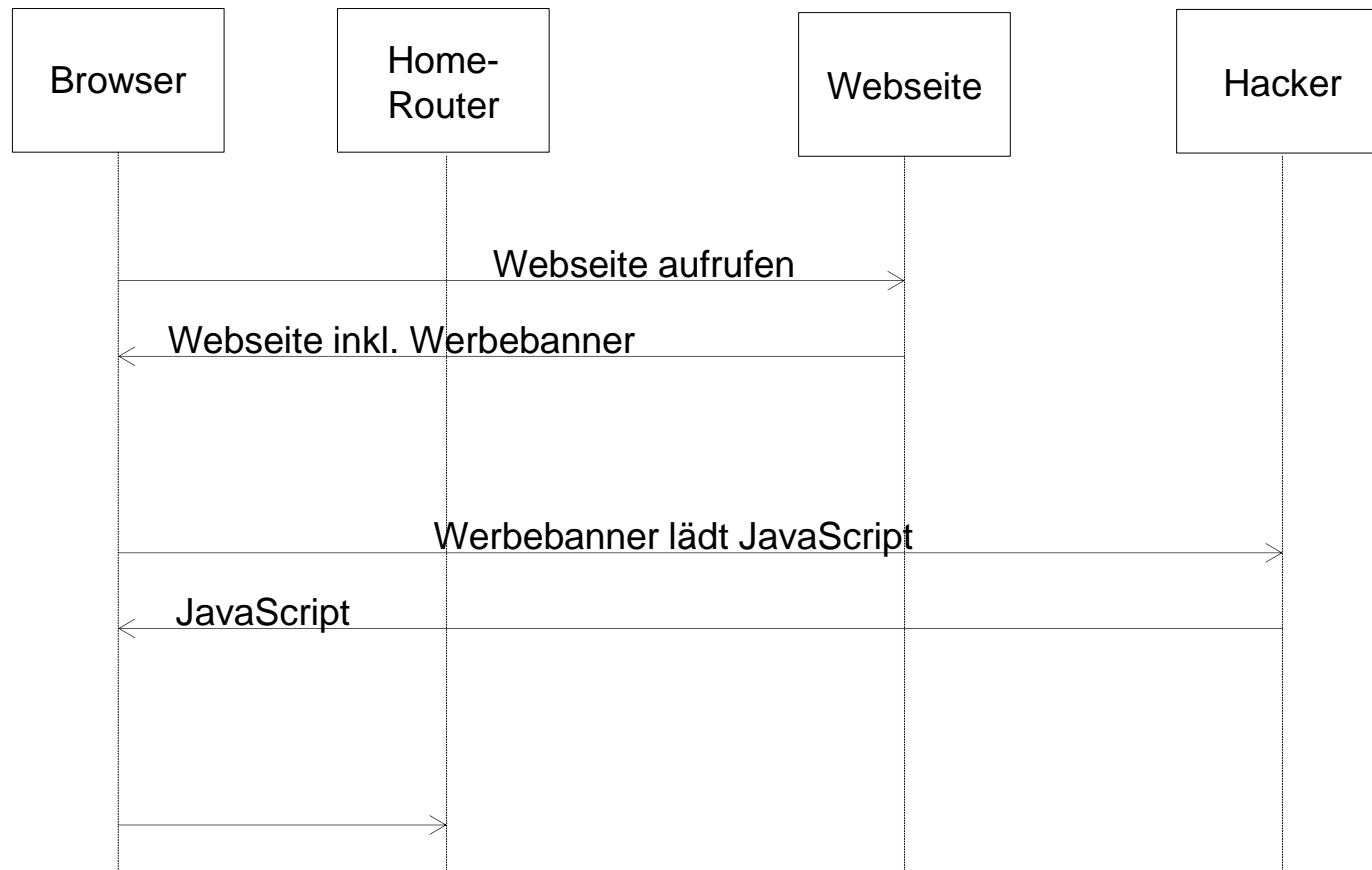
- «Wir wissen nicht, wer Sie sind, und wir wissen nicht, wohin Sie gehen»
- Das 55-Meter-Zaubertor von Rom
- Beschwerde gegen «Kassensturz» wegen Wahlwerbung
- 750 Euro machen niederländischen Premier zum Syrer
- Idee der Flüchtlingsinsel: Sawiris' Bruder macht Ernst

@tagesanzeiger folgen Gefällt mir



Router

Cross Site Request Forgery



GET http://router/changeconfig.html

```
<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



SHODAN

Explore | Contact Us | Blog | Enterprise Access | New to Shodan?

PLDT myDSL Biz ZyXEL

P-2612HWU-F1

Welcome to your Router Configuration Interface

Enter your password and press enter or click "Login"

User Name:

Password:

CISCO

Setup

Setup | Wireless | Security | Storage | Access Restrictions | Applications & Gaming

Basic Setup | DDNS | MAC Address Clone | Advanced F

Language

Select your language: English

Internet Setup

Internet Connection Type: Automatic Configuration - DHCP

Optional Settings (required by some Internet Service Providers)

Host Name:

Domain Name:

MTU: Auto Size: 1500

LINKSYS A Division of Cisco Systems, Inc.

Setup

Setup | Wireless | Security

Basic Setup

Internet Setup

Internet Connection Type: Automatic Configuration - DHCP

Optional Settings (required by some ISPs)

Router Name: WRT54G

Host Name:

Domain Name:

MTU: Auto

Size: 1500

- Canada
- United Kingdom
- TOP SERVICES
- HTTP (8080)
- Insteon Hub
- Qconn
- ntop

```
WNR1000v
HTTP/1.1 401 Unauthorized
Server:
Date: Tue, 15 Sep 2015 18:22:39 GMT
WWW-Authenticate: Basic realm="NETGEAR WNR1000v
4"
Content-Type: text/html
Connection: close
```



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

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
```

Tenda W302R auf Debug-Port 7329, spezielle Zeichenfolge:

```
w302r_mfg\x00xKommando
```

Kommando wird als root ausgeführt



Live Demo: Backdoor

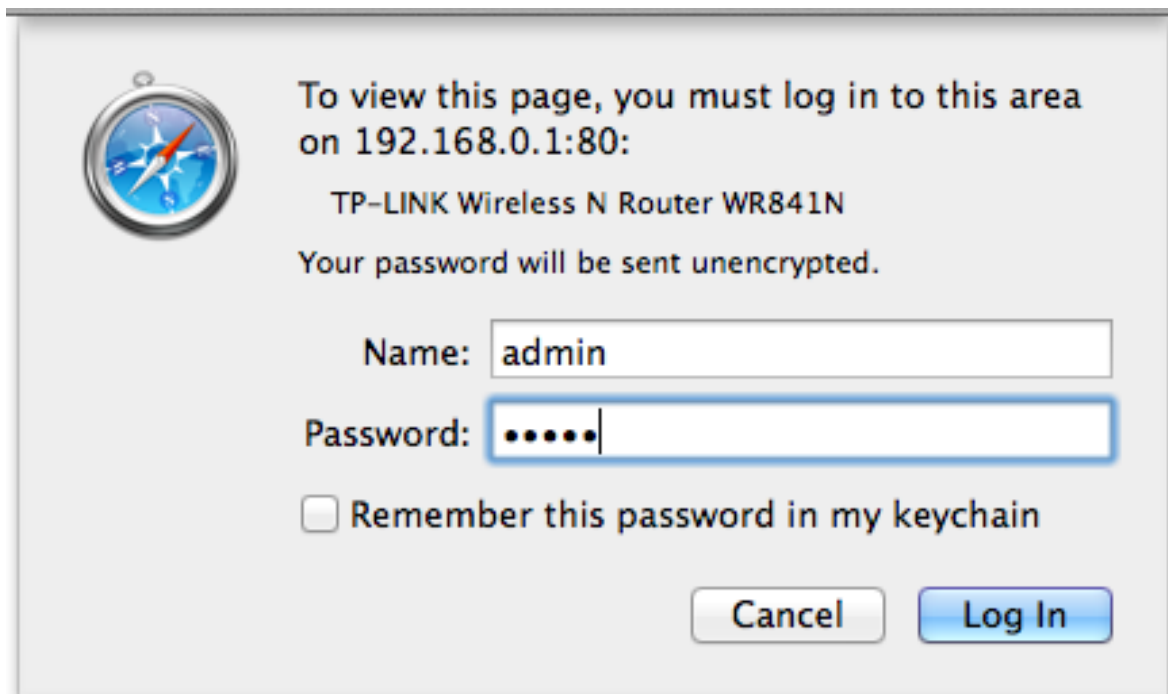
Compass Security
Deutschland GmbH
Tauentzienstr. 18
De-10789 Berlin

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



To view this page, you must log in to this area on 192.168.0.1:80:

TP-LINK Wireless N Router WR841N

Your password will be sent unencrypted.

Name:

Password:

Remember this password in my keychain

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

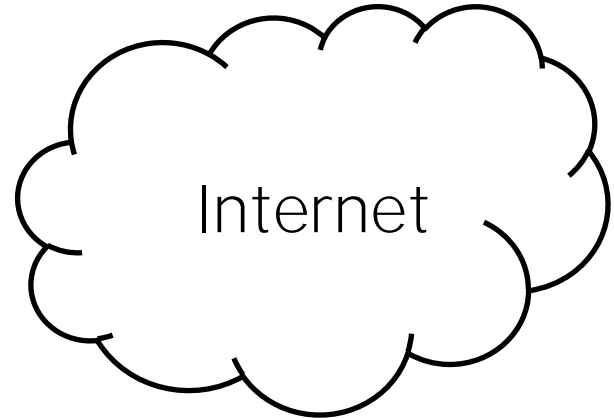
Remote Management (TR-069)

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

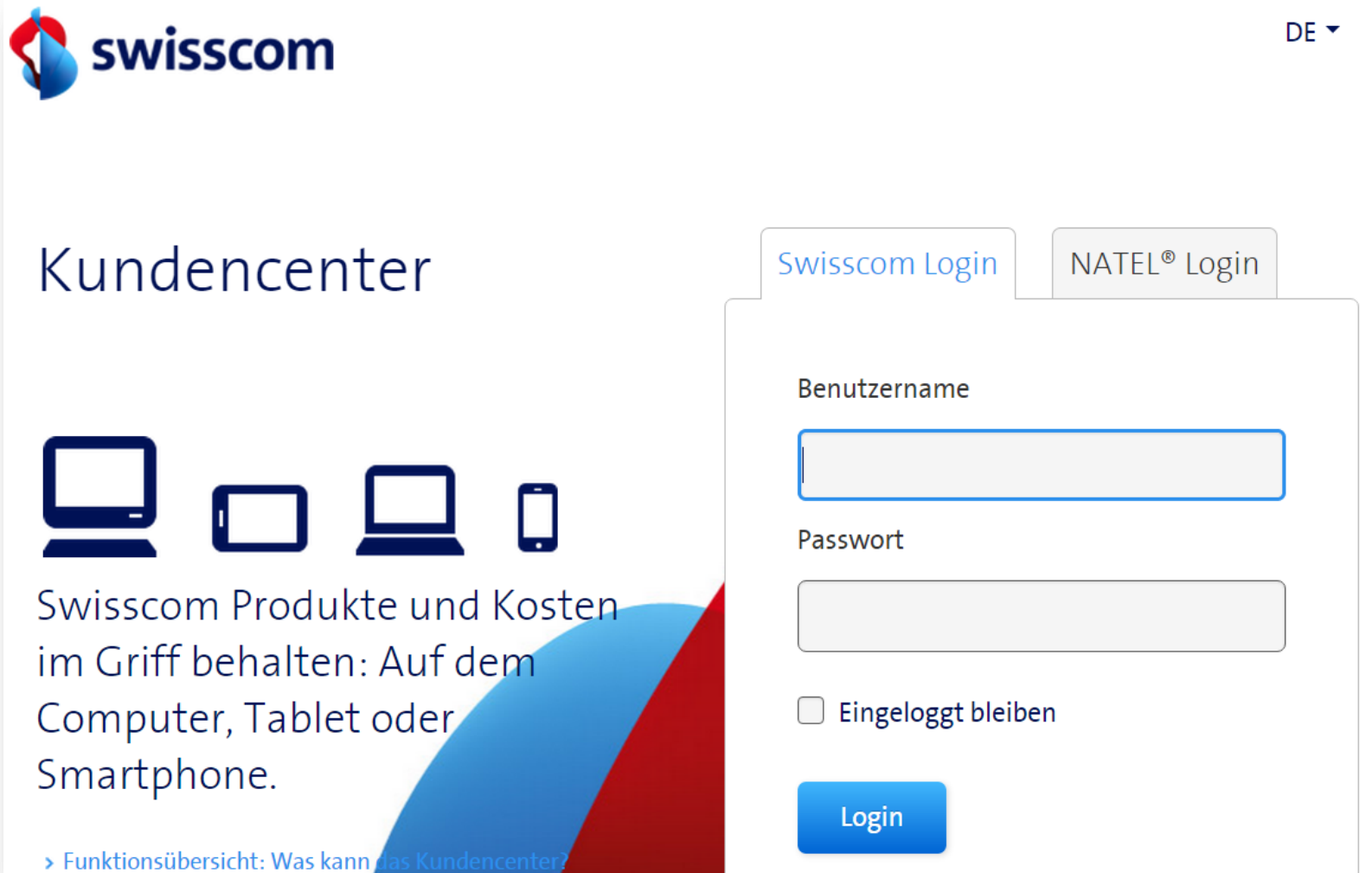
500'000


1







Customer
Premise
Equipment
(Kundenrouter)

Auto
Configuration
Server
vom Provider

A screenshot of the Swisscom Kundencenter login page. The page features the Swisscom logo in the top left and a language selector "DE" in the top right. The main heading is "Kundencenter". Below it, there are icons for a desktop monitor, a tablet, a laptop, and a smartphone. The text reads: "Swisscom Produkte und Kosten im Griff behalten: Auf dem Computer, Tablet oder Smartphone." At the bottom left, there is a link: "> Funktionsübersicht: Was kann das Kundencenter?". On the right side, there is a login form with two tabs: "Swisscom Login" (active) and "NATEL® Login". The form contains fields for "Benutzername" and "Passwort", a checkbox for "Eingeloggt bleiben", and a blue "Login" button.

 swisscom DE ▾

Kundencenter

Swisscom Produkte und Kosten im Griff behalten: Auf dem Computer, Tablet oder Smartphone.

[> Funktionsübersicht: Was kann das Kundencenter?](#)

Swisscom Login NATEL® Login

Benutzername

Passwort

Eingeloggt bleiben

Login

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

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 erforderlich

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 box vulnerable to an authentication bypass attack. No router option can be changed to exploit the issue. So an attacker can access the web interface of the router without submitting any valid password, just by requesting a special URL several



CATEGORIES

FEATURED

PODCASTS

VIDEOS

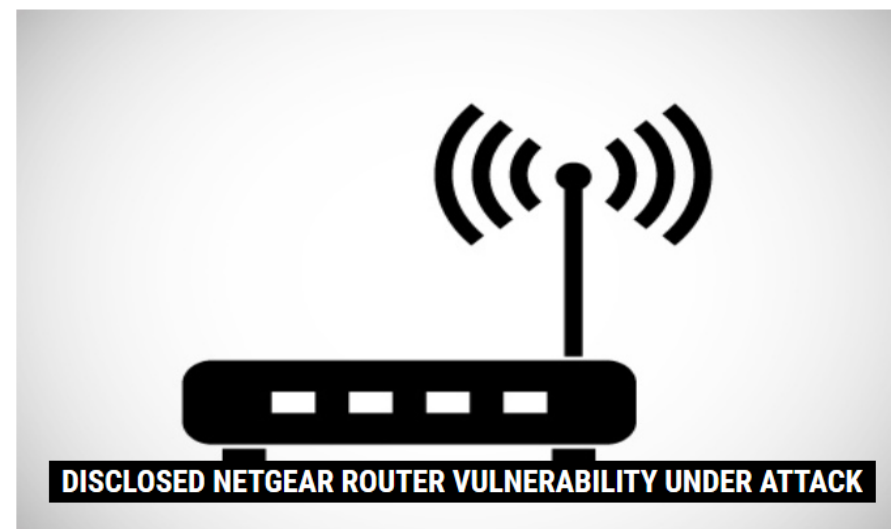


11/04/15 2:03



Researchers at @Lookout have found a new strain of malware, #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

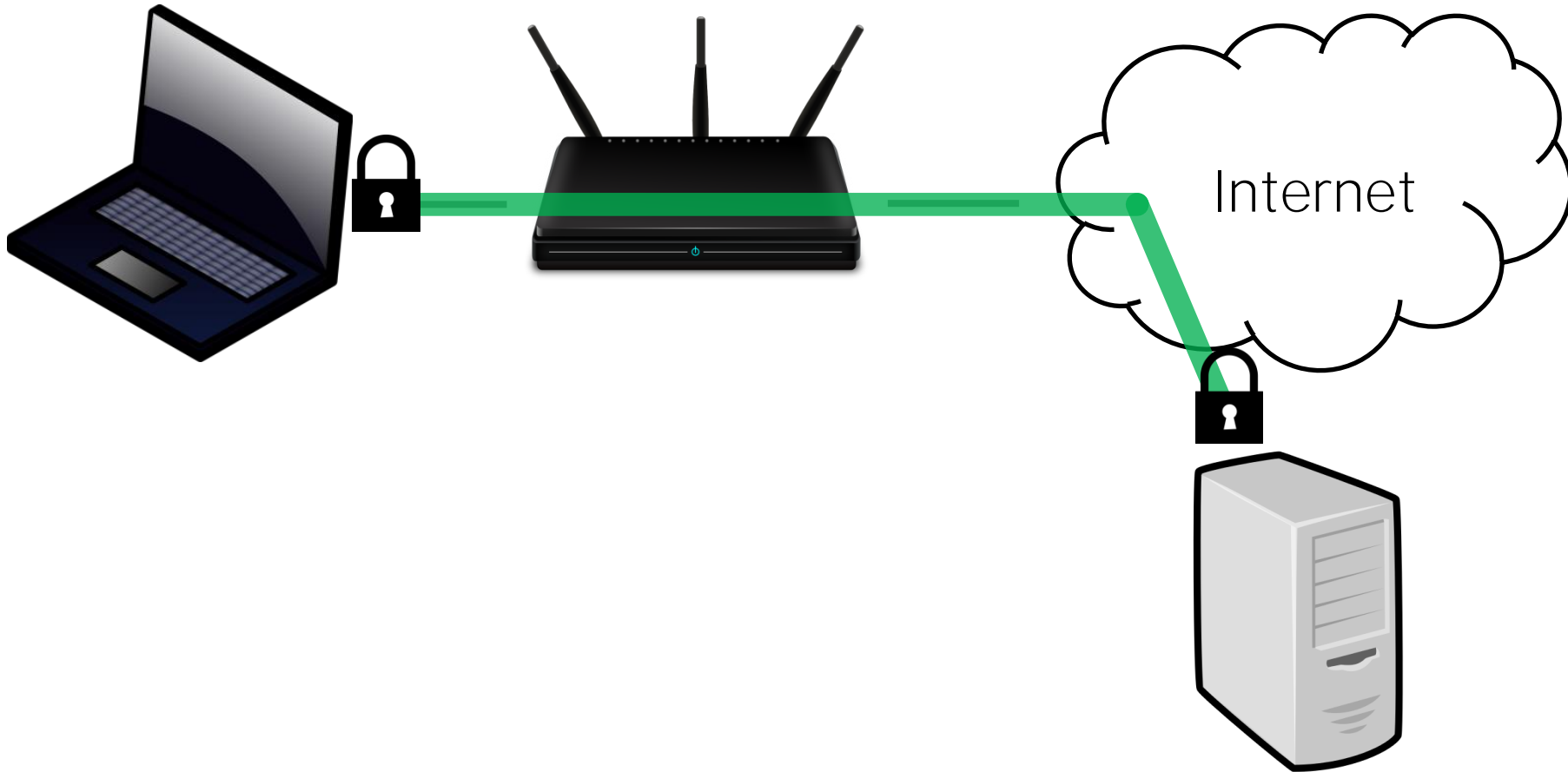
Tel. +49 30 21 00 253-0
Fax +49 30 21 00 253-69
team@csnc.de
www.csnc.de

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

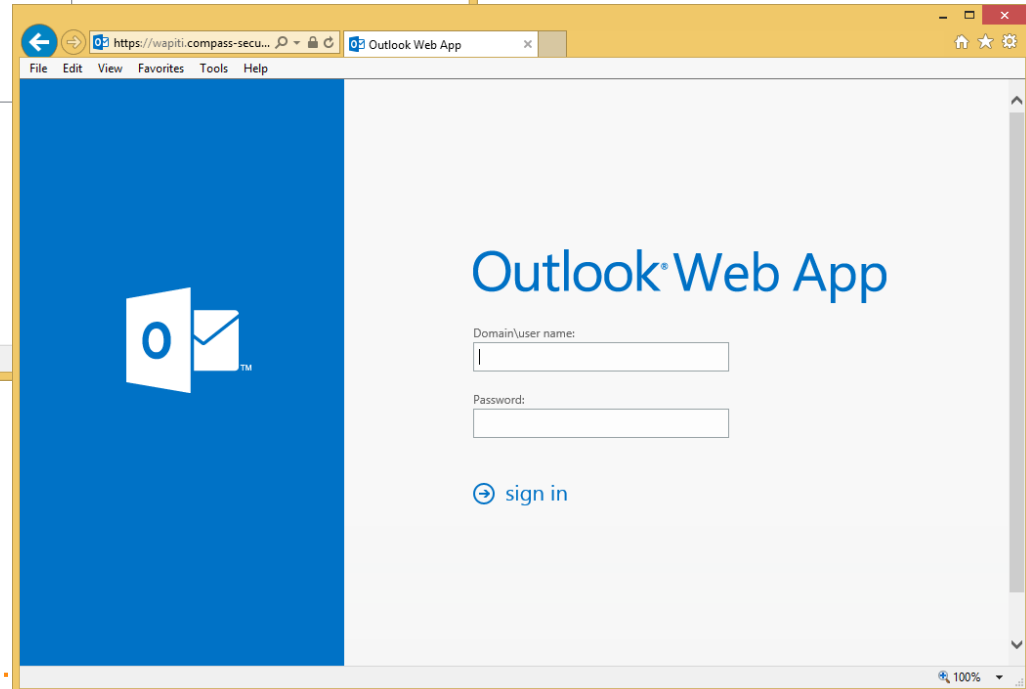
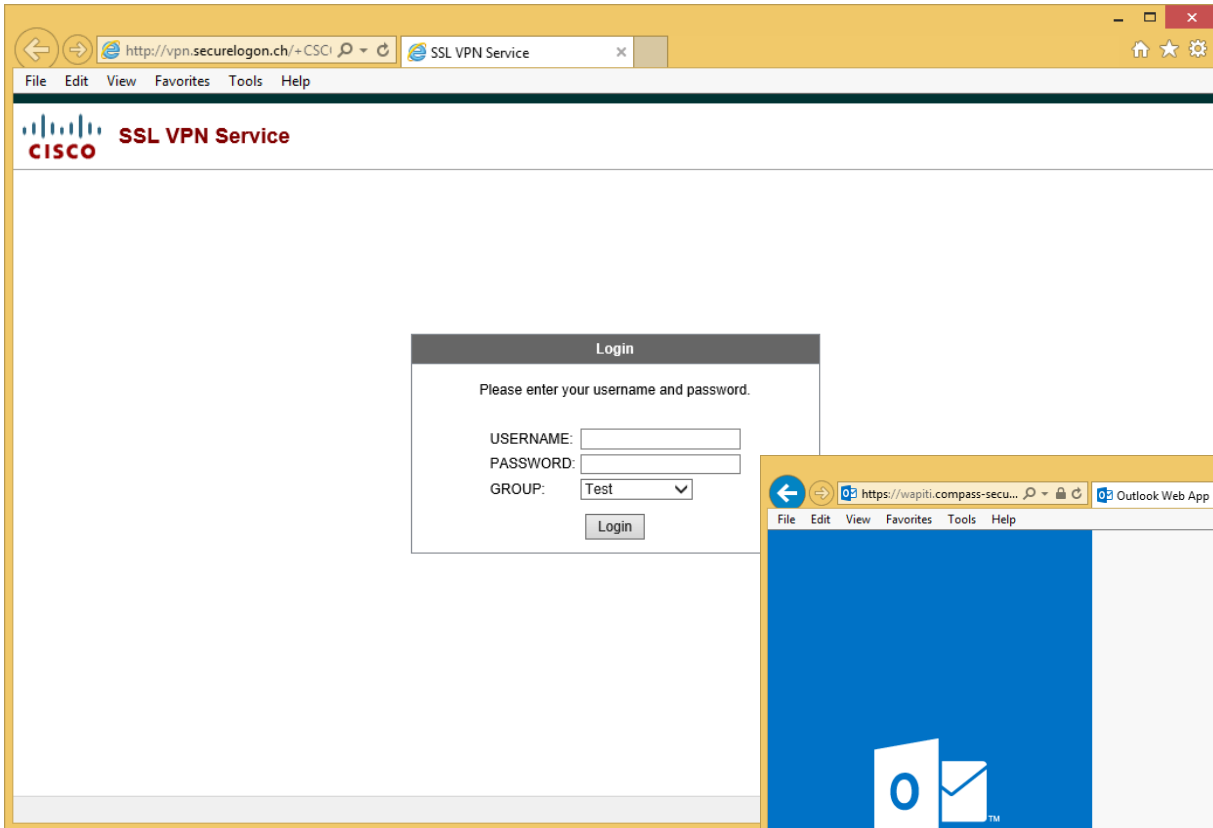
- ✦ Unverschlüsselten Verkehr belauschen
- ✦ DNS manipulieren
- ✦ Passworte auslesen
 - ✦ WLAN
 - ✦ VoIP
- ✦ Telefonie übernehmen
- ✦ Dienste stören (DoS)
- ✦ Manipulierte Firmware einspielen
- ✦ Agent eines BOT-Netzwerkes werden

Angriff: DNS Hijacking

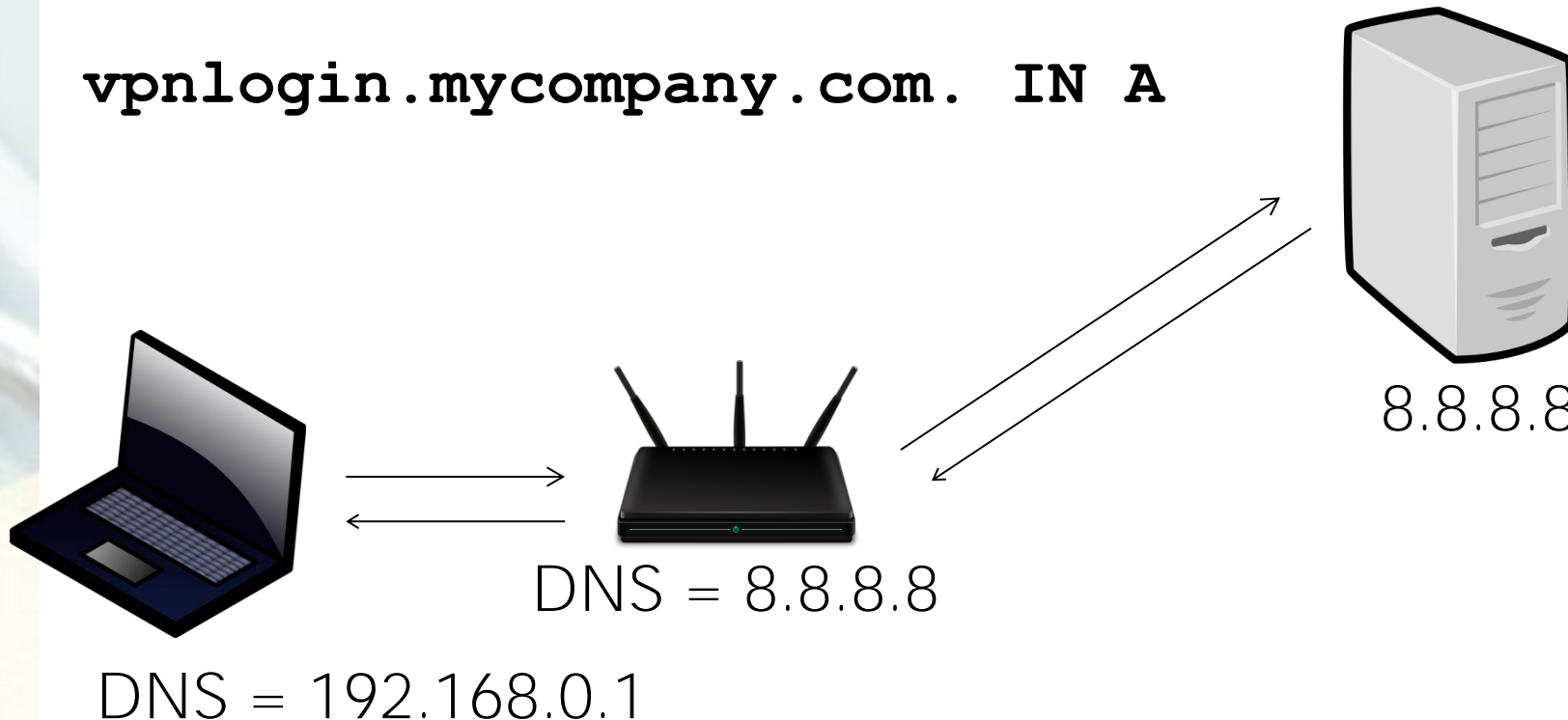
VPN Verbindung zur Firma



vpn.securelogon.ch



vpnlogin.mycompany.com. IN A

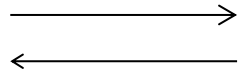


vpnlogin.mycompany.com. IN A 240.1.2.18

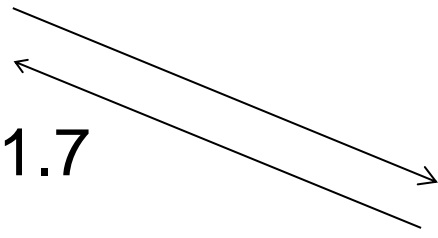
DNS Hijacking



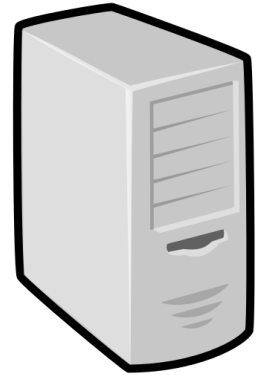
vpnlogin.mycompany.com. IN A



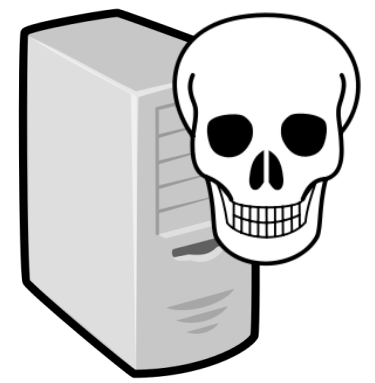
DNS = 203.0.1.7



DNS = 192.168.0.1



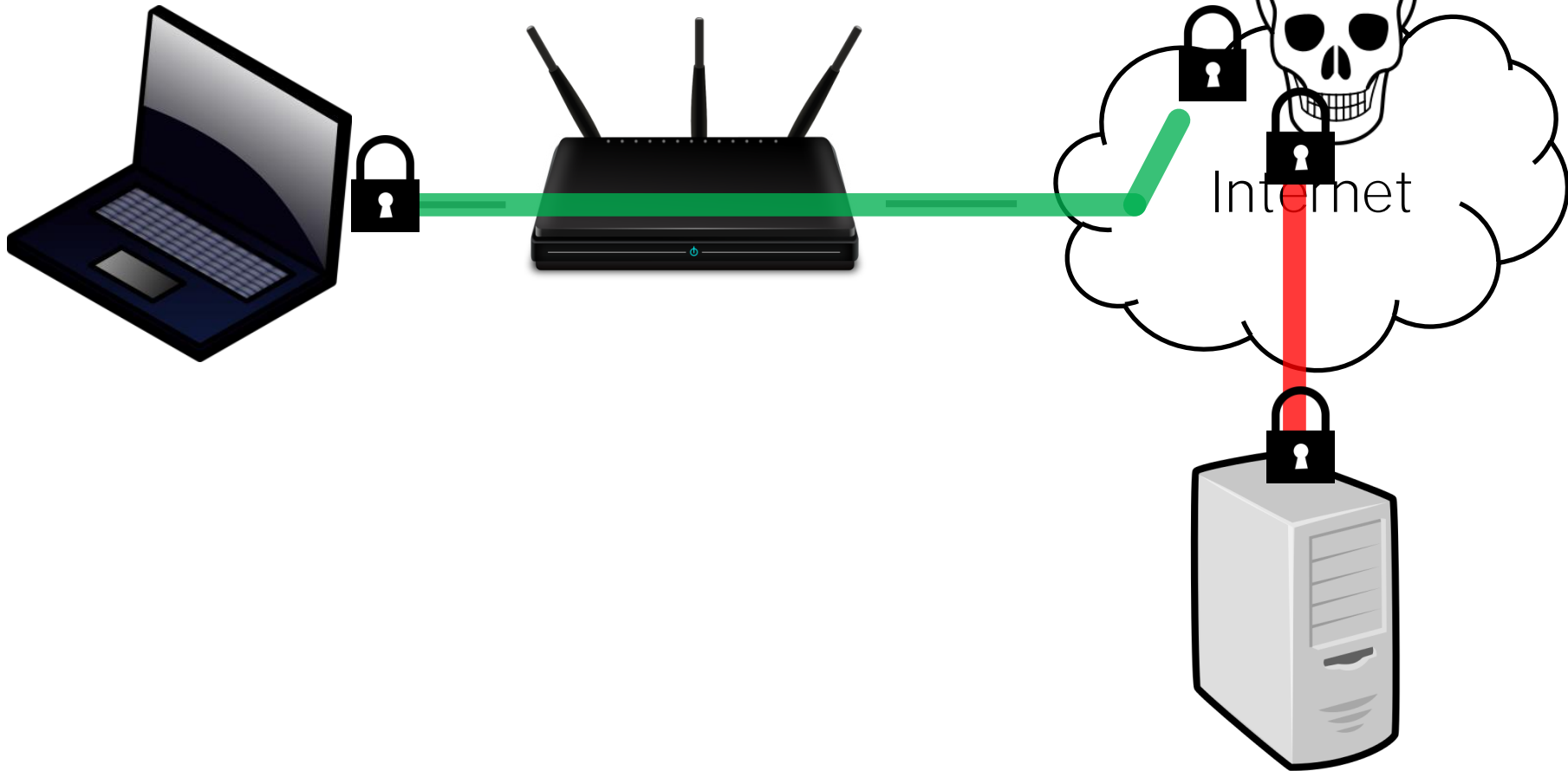
8.8.8.8



203.0.1.7

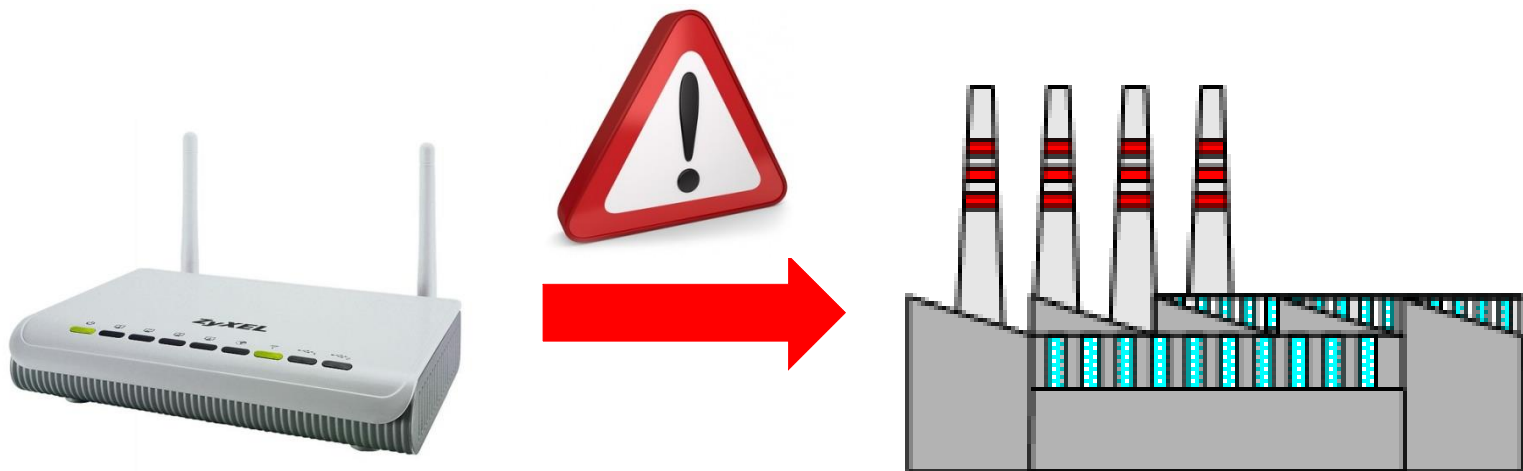
vpnlogin.mycompany.com. IN A **203.0.1.7**

VPN Verbindung mit Phishing Server



vpn.securelogon.ch

Ist der Home-Router eine Gefahr für das Unternehmen?





Empfehlungen

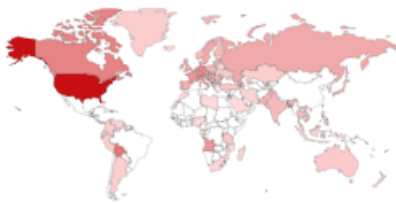
Compass Security
Deutschland GmbH
Tauentzienstr. 18
De-10789 Berlin

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



Showing results 1 - 10 of 47,245

TOP COUNTRIES



Country	Count
United States	37,827
Bolivia, Plurinational State of	2,018
Canada	
Germany	
Bangladesh	

TOP SERVICES

HTTP	
HTTPS	
ntop	
HTTP (8080)	
HTTPS (8443)	

TOP ORGANIZATIONS

Arvig Enterprises	6,001
Datawave Technologies, LLC	4,271
Guadalupe Valley Telephone Cooperat...	4,231
Allo Communications LLC	2,957
United Telephone Company	2,565

<https://www.shodan.io/store/member>

ZyXEL ZvAIR G-4100v2

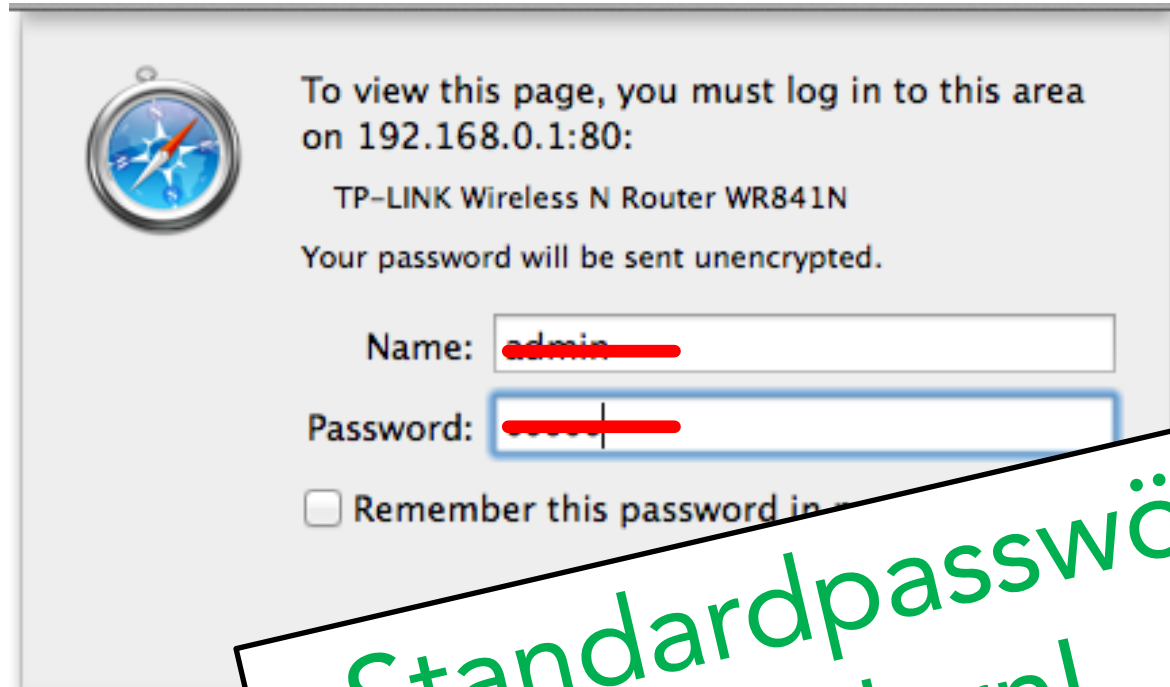
Deutsche Telekom AG
Added on 2015-10-31 23:50:57 GMT

```
HTTP/1.1 200 OK
Server: micro_httpd
Cache-Control: no-cache
Pragma: no-cache
Date: Sat, 31 Oct 2015 19:54:19 GMT
Content-Type: text/html
Set-Cookie: SESSION=; expires=Thu, 01-Jan-1970 00:00:00 GMT; path=/
Connection: close
```



Regelmässige
Firmware-Updates!



A screenshot of a web browser's login page for a TP-LINK Wireless N Router WR841N. The page has a light gray background and a small compass icon in the top left corner. The text reads: "To view this page, you must log in to this area on 192.168.0.1:80: TP-LINK Wireless N Router WR841N Your password will be sent unencrypted." Below this, there are two input fields: "Name:" with the value "admin" and "Password:" with a redacted password. A checkbox labeled "Remember this password in" is also visible.

To view this page, you must log in to this area on 192.168.0.1:80:

TP-LINK Wireless N Router WR841N

Your password will be sent unencrypted.

Name:

Password:

Remember this password in

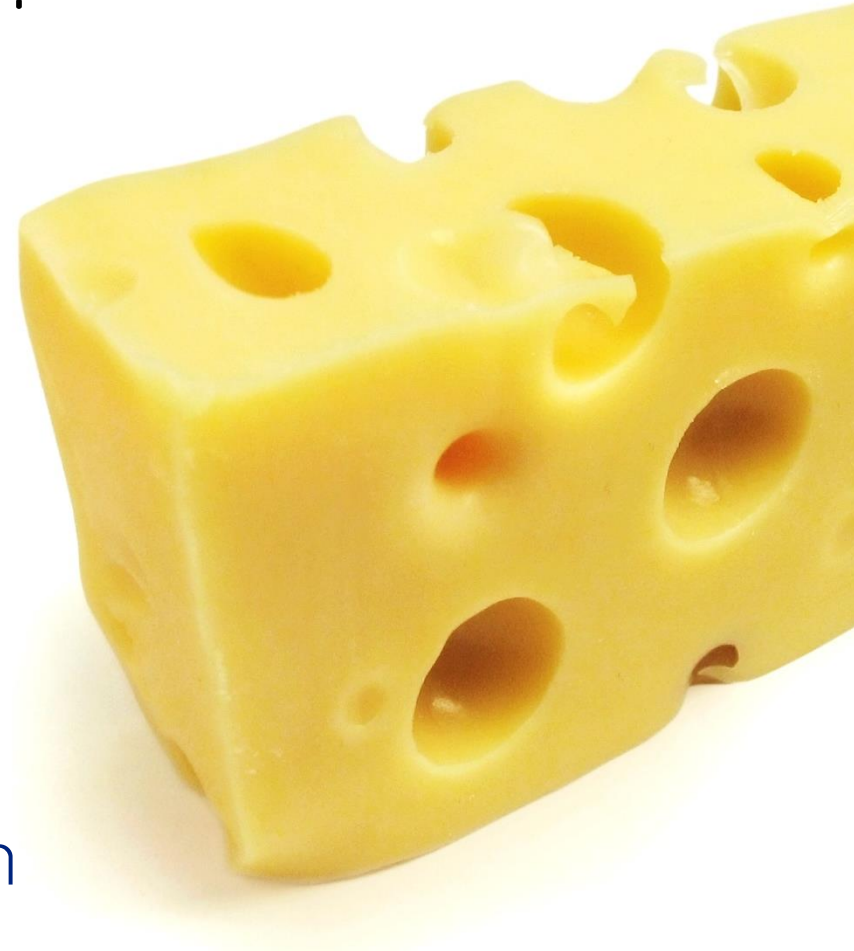
Standardpasswörter ändern!

Vielen Dank für Ihre Aufmerksamkeit



Wir finden die Löcher!

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



www.compass-security.com