Internet of Things:
Müssen wir das Internet davor schützen?

Prof. Dr. Rainer W. Gerling
IT-Sicherheitsbeauftragter
Max-Planck-Gesellschaft

Zitate

- „The Internet of Things Is Wildly Insecure—And Often Unpatchable“
  Bruce Schneier, 6. Januar 2014

- „build security into devices at the outset, rather than as an afterthought in the design process“
  Federal Trade Commission, 27. Januar 2015

- „Das Internet of Things gefährdet das freie Netz“
  golem.de, 26. September 2016

- „The market can't fix this because neither the buyer nor the seller cares.“
  Bruce Schneier, 15. Oktober 2016

The Insecurity of Things
(https://www.mpg.de/jv2016)

IoT:
The Insecurity of Things

Adi Shamir
Computer Science Dept
Weizmann Institute
Israel

Max Planck Society Plenary Session
June 16-th 2016

67. JAHRESVERSAMMLUNG
DER MAX-PLANCK-GESELLSCHAFT

WiFi Steckerset

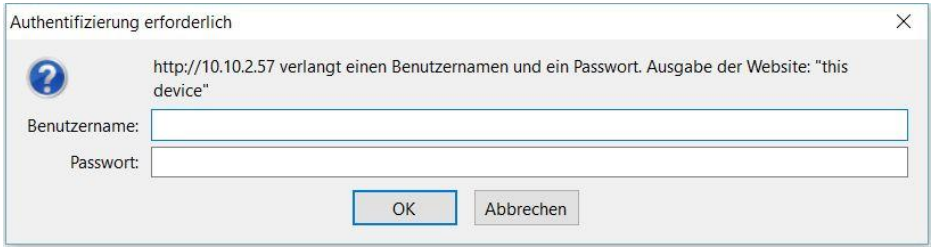
- Die Mastersteckdose ist ein WLAN/433Mhz-Gateway
  - Kommunikation über die Cloud
- Portscan findet Port 80 geöffnet

Abb: Aldi-Süd

WiFi Steckerset

- Die Mastersteckdose ist ein WLAN/433Mhz-Gateway
  - Kommunikation über die Cloud
- Portscan findet Port 80 geöffnet

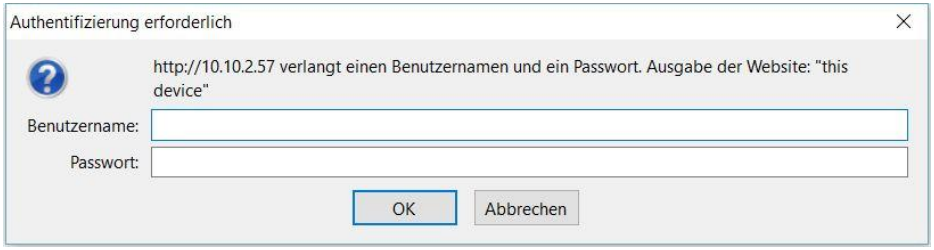
Abb: Aldi-Süd



WiFi Steckerset

- Die Mastersteckdose ist ein WLAN/433Mhz-Gateway
  - Kommunikation über die Cloud
- Portscan findet Port 80 geöffnet

Abb: Aldi-Süd



- Anmeldung: admin/admin

WiFi Steckerset

- Die Mastersteckdose ist ein WLAN/433Mhz-Gateway
  - Kommunikation über die Cloud
- Portscan findet Port 80 geöffnet

Abb: Aldi-Süd

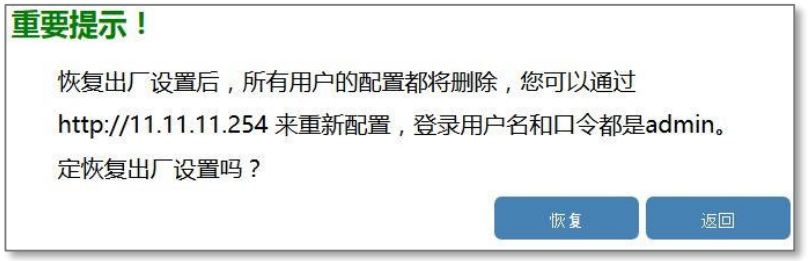
- Anmeldung: admin/admin

WiFi Steckerset

- Die Mastersteckdose ist ein WLAN/433Mhz-Gateway
  - Kommunikation über die Cloud
- Portscan findet Port 80 geöffnet

Abb: Aldi-Süd

- Anmeldung: admin/admin

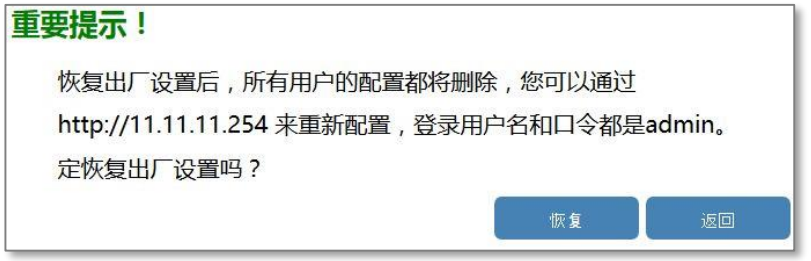


WiFi Steckerset

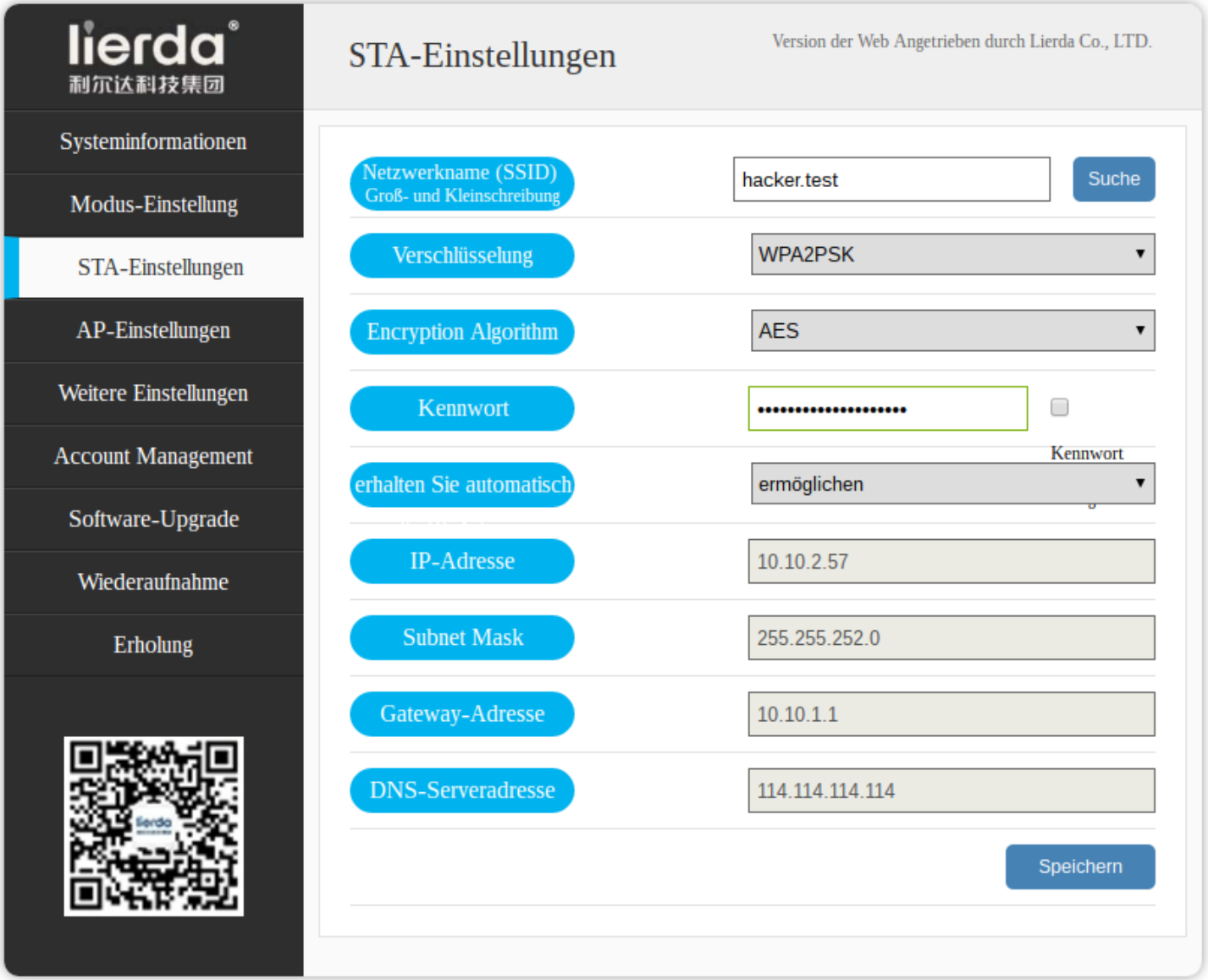
- Die Mastersteckdose ist ein WLAN/433Mhz-Gateway
  - Kommunikation über die Cloud
- Portscan findet Port 80 geöffnet

Abb: Aldi-Süd

- Anmeldung: admin/admin
- Mit Chrome lesbar! ☺



Manchmal hilft Google ☺: Chrome



DHCP aktiv

DNS aus China

Belkin WeMo

- Geräte werden über die Cloud gesteuert
- Wemo Link ist ein WLAN/ZigBee Gateway
- Darauf läuft OpenWrt (ältere Version)
- Auf allen WeMo-Geräten mit WLAN läuft ein DNS-Server als OpenRelay (dnsmasq)

SSHowDowN

- Angriff gegen
  - Überwachungskameras, Netzwerkvideorekorder , Videorekorder (Videoüberwachung)
  - Satellitenempfänger
  - Netzwerkgeräte (z.B. Router, Hotspots, WiMax, Kabel- und DSL-Modems)
  - Mit dem Internet verbundene NAS-Geräte (Network Attached Storage)
- CVE-2004-1653 vom 31.8.2004
  - TCP-Weiterleitung (SSH-Tunnel) per Default aktiviert
- „Internet of unpatchable Things“ *(Akamai)*

IoT Botnetze

- Mirai
  - Maximum 380.000 Geräte
    - Binaries für arm, arm5n, arm7, m68k, mips, mpsl, ppc, sh4, spc, x86
  - Zahl ist rückläufig
  - Quellcode im Oktober 2016 veröffentlicht!
  - Wurde für den DDoS Angriff auf KrebsonSecurity benutzt
- Bashlight
  - Rund 1.000.000 Geräte
- Geräte werden über telnet-Zugänge mit Default-Passworten gehackt
  - SSH bietet keinen Schutz gegen Default-Passworte ☹

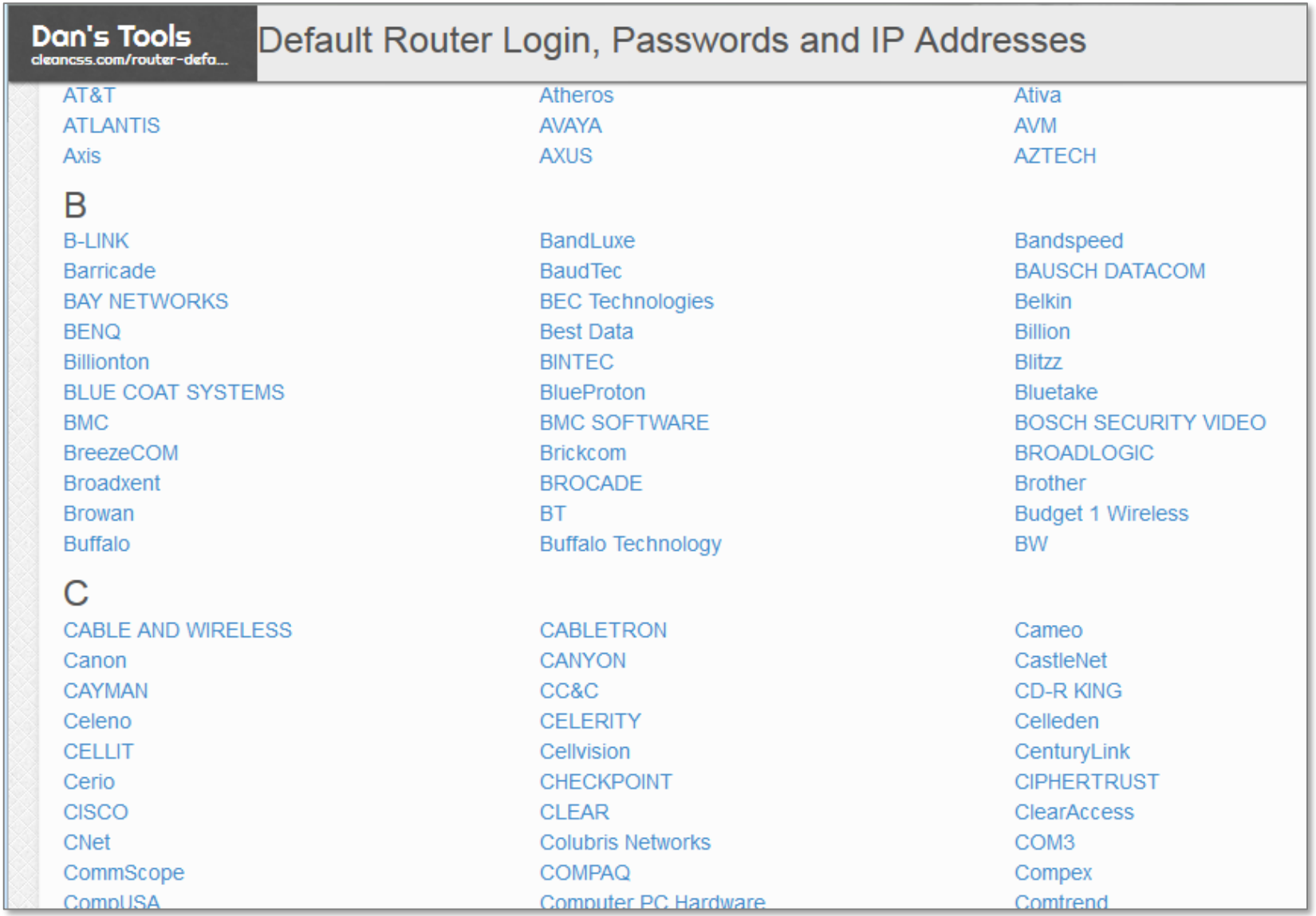
IoTPOT
(http://christian-rossow.de/publications/iotpot-woot2015.pdf)

- HoneyPot für IoT
  - Telnet HoneyPot; simuliert verschiedene IoT Geräte
  - Innerhalb 39 Tagen auf 165 verschiedenen IP-Adressen
  - 70.230 Verbindungsversuche
  - 49.121 erfolgreiche Login
  - 16.934 Versuche Malware von extern herunter zu laden
- 43 heruntergeladene unterschiedliche Schadsoftwaren-Proben
  - 39 waren Virustotal unbekannt
- Viele der Verbindungsversuche kamen von (bereits infizierten) IoT Geräten

Default Passwords from Mirai Source Code

- root/xc3511
- root/vizxv
- root/admin
- admin/admin
- root/888888
- root/xmhdipc
- root/default
- root/juantech
- root/123456
- root/54321
- support/support
- root/(none)
- admin/password
- root/root
- root/12345
- user/user
- admin/(none)
- root/pass
- admin/admin1234
- root/1111
- admin/smcadmin
- admin/1111
- root/666666
- root/password
- root/1234
- root/klv123
- Administrator/admin
- service/service
- Supervisor/supervisor
- guest/guest
- guest/12345
- guest/12345
- admin1/password
- Administrator/1234
- 666666/666666
- 888888/888888
- ubnt/ubnt
- root/klv1234
- root/Zte521
- root/hi3518
- root/jvbzd
- root/anko
- root/zlxx.
- root/7ujMko0vizxv
- root/7ujMko0admin
- root/system
- root/ikwb
- root/dreambox
- root/user
- root/realtek
- root/00000000
- admin/1111111
- admin/1234
- admin/12345
- admin/54321
- admin/123456
- admin/7ujMko0admin
- admin/1234
- admin/pass
- admin/meinsm
- tech/tech
- mother/fucker

Default Passworte finden



Dan's Tools
cleancss.com/router-defa...

Default Router Login, Passwords and IP Addresses

AT&T
ATLANTIS
Axis
Atheros
AVAYA
AXUS
Ativa
AVM
AZTECH

B

B-LINK
Barricade
BAY NETWORKS
BENQ
Billionton
BLUE COAT SYSTEMS
BMC
BreezeCOM
Broadxent
Browan
Buffalo
BandLuxe
BaudTec
BEC Technologies
Best Data
BINTEC
BlueProton
BMC SOFTWARE
Brickcom
BROCADE
BT
Buffalo Technology
Bandspeed
BAUSCH DATACOM
Belkin
Billion
Blitzz
Bluetake
BOSCH SECURITY VIDEO
BROADLOGIC
Brother
Budget 1 Wireless
BW

C

CABLE AND WIRELESS
Canon
CAYMAN
Celeno
CELLIT
Cerio
CISCO
CNet
CommScope
CompUSA
CABLETRON
CANYON
CC&C
CELERITY
Cellvision
CHECKPOINT
CLEAR
Colubris Networks
COMPAQ
Computer PC Hardware
Cameo
CastleNet
CD-R KING
Celleden
CenturyLink
CIPHERTRUST
ClearAccess
COM3
Compex
Comtrend

House of Keys

https://github.com/sec-consult/houseofkeys

- Woher hat mein IoT-Gerät eigentlich seine Schlüssel?
  - Die sind fest in die Firmware eingebrannt ☹
- Analyse der Firmware erlaubt Extraktion der privaten Schlüssel!!!
  - X.509 Zertifikate für das Web-Management (https)
  - SSH-Server Schlüssel
  - Es konnten >580 private (!) Schlüssel extrahiert werden
    - 9% aller HTTPS Server (~150 Server Zertifikate bei 3.2 Millionen Servern)
    - 6% aller SSH Server (~80 SSH Server Schlüssel bei 900.000 Servern)
  - Teilweise stammen die Schlüssel aus den SDK der Chip/Hardware-Hersteller
- Von November 2015 bis September 2016 nahm die Zahl der Webseiten mit bekannten privaten Schlüsseln um 40% zu!

Internet of Things:

Müssen wir das Internet davor schützen?

Ja!!!!

Internet of Things:

Müssen wir das Internet davor schützen?

Vielen Dank für Ihre Aufmerksamkeit !

https://www.mpg.de/7854031/datensicherheit_wissenschaft