

Sicherheit im Docsis Netzwerk

CableTech 2016

Michael Neumann


mn@jm-data.at



Sicherheit im Docsis Netzwerk

- IP Planung
- ACL und Firewalls
- BPI – BPI+ – SEC
- IP SOURCE VERIFY
- TFTP-ENFORCE
- Software und Firmware

Über JM-DATA

- 1998 von Jürgen Meixner gegründet
 - Seit 2000 im Provider und Kabel TV Sektor tätig
 - Seit 2004 Erfahrung im VoIP Bereich
 - Seit 2007 Betreiber eigener Kabelnetze
- 
- A decorative graphic at the bottom of the slide consisting of several horizontal, wavy lines in shades of red and dark red, creating a sense of motion or a stylized wave.

Tätigkeitsbereiche

- Consulting
- ISP
- Provisioning und Monitoring
- Refurbished und Neuware
(Router, Switches, CMTS, OLT, ONU, ...)
- Voice (MGCP, SIP)

CN-ADMIN Produkt

Provisioning und Monitoring

- DHCP
- TFTP
- Radius
- TR-069
- SNMP

Technologien

- Docsis
- Radius
- PON / GePon
- Active Ethernet

Unternehmensgruppe



IP-Planung

Subnet per Verwendungsgruppe (IPv4 und IPv6)

- Core / Provisioning
- CM MNGT
- MTA
- CPE
- CPE CGN
- CPE Blocked
- Service Access (Office, Technik, ect)

IP-Planung

Die Subnetze der Geräte Gruppen groß genug planen

MTA 10.250.0.0/255.255.0.0

- Netzsegment A 10.250.0.0/255.255.240.0
- Netzsegment B 10.250.16.0/255.255.240.0
- Reserve

CM MNGT 10.10.0.0/255.255.0.0

- Netzsegment A 10.10.0.0/255.255.240.0
- Netzsegment B 10.10.16.0/255.255.240.0
- Reserve

CPE Blocked 10.60.0.0/255.255.0.0

- Netzsegment A 10.60.0.0/255.255.240.0
- Netzsegment B 10.60.16.0/255.255.240.0
- Reserve

ACL und Firewalls

Provisioning

- Server Firewalls

CMTS

- IN und OUT ACL
- SNMP ACL
- CLI Access

Cable Modem

- Tarifspezifische Service Sperren

Provisioning Firewalls

TFTP

- CM erlauben
- MTA erlauben

ToD

- CM erlauben
- MTA erlauben

IPv6 nicht vergessen

CMTS ACL

Cable Modem MNGT

Nur für Provisioning und Monitoring erlauben

MTA

Nur Provisioning und Voice Services erlauben

Zumindest SNMP, TELNET nur für Provisioning und Monitoring erlauben

SNMP

SNMP nur für definierte community und ACL erlauben

Warum ACL Wichtig ist

z.B. WLAN Daten auslesen

```
snmpwalk -c public -v2c 10.11.1.230 .1.3.6.1.4.1.4413.2.2.2.1.18.1.2
```

...

```
iso.3.6.1.4.1.4413.2.2.2.1.18.1.2.1.1.3.32 = STRING: "MYSSID"
```

...

```
iso.3.6.1.4.1.4413.2.2.2.1.18.1.2.3.4.1.2.32 = STRING: "CHANGEME"
```

...

Warum ACL Wichtig ist

z.B. MTA Daten auslesen

```
snmpwalk -c public -v2c 10.14.4.55 .1.3.6.1.4.1.2863.78.3.4.1.1
```

...

```
.1.3.6.1.4.1.2863.78.3.4.1.1.1.1    sip.sip.at  
.1.3.6.1.4.1.2863.78.3.4.1.1.3.1    435033333  
.1.3.6.1.4.1.2863.78.3.4.1.1.4.1    passwordline1  
.1.3.6.1.4.1.2863.78.3.4.1.1.5.1    435033333  
.1.3.6.1.4.1.2863.78.3.4.1.1.6.1    sip.sip.at
```

...

Cable Modem Firewall

Folgende Ports per Default sperren

- SMTP Port 25 TCP IN
- DNS Port 53 TCP/UDP IN
- DHCP Port 68 UDP IN
- NETBIOS Port 135-139 TCP/UDP IN + OUT
- SNMP Port 161 - 162 TCP/UDP IN + OUT
- SMB Port 445 TCP IN + OUT

Nur für Business Kunden oder nach Bedarf öffnen

BPI – BPI+ – SEC

Baseline Privacy Interface

- Privatsphäre der Daten von Cable Modem Benutzern
 - Verschlüsselung der Daten zwischen CMTS und Modem
- Schutz vor unerlaubten Service Nutzung

Warum BPI Notwendig ist

Shared Downstream

Mithören mit wenig Aufwand möglich

- USB Stick um ca. € 30,--
- Linux System

Mit hören am gesamten Downstream möglich für Daten und Telefonie

Mit BPI je nach Verschlüsselung nur mit viel Rechenleistung möglich

- Verschlüsselung ändert sich regelmäßig

Entwicklung

BPI (Docsis 1.0)

- Verschlüsselung bis zu 56-bit DES
- Key refresh(KEK)

BPI+ (Docsis 1.1 / 2.0)

- Modem Authentication (PKI)

SEC (Docsis 3.0)

- Verschlüsselung 128-bit AES
- Early Authentication and Encryption (EAE)

Privacy Config Example

```
Router> enable
```

```
Router# configure terminal
```

```
Router(config)# cable privacy bpi-plus-enforce
```

```
Router(config)# cable shared-secret xxx
```

```
Router(config)# service password-encryption
```

```
Router(config)# cable logging layer2events
```

```
Router(config)# cable privacy encrypt-alg-priority aes128-des56-des40
```

```
Router(config)# interface cable 6/o/1
```

```
Router(config-if)# cable privacy eae-policy total-enforcement
```

BPI minimal Config

Immer Nutzbar ab Docsis 1.0 – > Zumindest eine Grundverschlüsselung der gesendeten Daten

Cable Network Administration

CN-ADMIN

Home Admin Adressen Vertrag Devices PON HF-Analyse Accounting Radius Status Ticket-Lite Logout jm-data

- General Settings
 - Optionen
 - User Management
 - View devices
- Nodes
 - Add Node
 - Search Node
- SNMP
 - Add SNMP Host
 - Search SNMP Hosts
 - Add SNMP Device Type
 - Search SNMP Device Type
- Docsis Package Config
 - Add Docsis Package
 - Search Docsis Packages
- Bootfiles
 - Bootfile Generation
 - Bootfile Configuration
 - Bootfile Profile
 - Static MTA Bootfiles
 - Static Modem Bootfiles
 - Firmware
- DHCP-Server Administration
 - DHCP Lease Management
 - DHCP Server Groups
 - DHCP Server edit
 - DHCP Classes
 - Network Sites
- DNS-Server Administration
 - DNS Server
 - DNS ACL
 - Domain Name
 - Domain Name Keys
- IP-POOL Config
- GPON PRN LABOR-1

Bootfile Docsis Settings Edit

Downstream Frequency:

Upstream Channel ID:

Network Access: No ▾

Max CPEs: 3

TFTP Timestamp:

TFTP Address:

Privacy Enable: Yes ▾

Software Upgrade Filename:

TFTP Upgrade Address:

HMAC Digest:

Docsis 2 Enable: n.a ▾

MFG CVC Data:

BPI+ Overhead

useable bandwidth for Ethernet frames =
Ethernet packets per s =

No BPI

45.614.467 Mbs
89.091 pps

if BPI turned on adds overhead of 5 bytes per frame
useable bandwidth for Ethernet frames BPI on =
Ethernet packets per s BPI on =

With BPI

42.573.503 Mbs
83.151 pps

Shared Secret

Authentication shared-secret encryption key

Schlüssel der im CMTS und Bootfile übereinstimmen muss.

Zusätzlicher Mechanismus in der BPI+ Konfiguration der verhindern soll dass Modems ungewünschte Bootfiles laden können.

Source Verify

Kontrolle der erlauben IP Adressen über den Upstream

- MAC Adressen werden nur über definierte DHCP Pakete erlaubt
- Kontrolle welche Geräte in welche IP Bereiche dürfen
- Lease Query – CMTS fragt DHCP Server um MAC – IP Relation zu legitimieren
- Ausnahmen am CMTS konfigurierbar

CABLE TFTP-ENFORCE

Konfiguration am CMTS

Zusätzliche Kontrolle das nur Modems online kommen die ein TFTP Config File über das CMTS vom Provisioning Server beziehen.

Ein zusätzlicher Mechanismus der das Manipulieren von Cable Modems verhindern hilft.

CMTS Config:



cable tftp-enforce (Im Interface Config Mode)

Software und Firmware

Software muss auf Servern und Cable Modems aktuell gehalten werden.

- Schließen von Sicherheitslücken
- Verbesserungen der bestehenden Funktionen
- Neue Funktionalitäten

CN-ADMIN 3.5

Cable Network Administration



[Home](#) | [Admin](#) | [Address](#) | [Devices](#) | [RF Analysis](#) | [Accounting](#) | [Status](#) | [Logout jm-data](#)

Cable Network Administration

CN-ADMIN News
News feed about CN-ADMIN 3.5 updates

jasper security update
Tuesday 08. March 2016 09:02:34 | debian-security-announce@lists.debian.org

Several vulnerabilities were discovered in Jasper, a library for manipulating JPEG-2000 files.

libav security update
Friday 04. March 2016 22:01:35 | debian-security-announce@lists.debian.org

Several security issues have been corrected in multiple demuxers and decoders of the libav multimedia library.

Linux Kernel Update
Friday 04. March 2016 10:21:16 | debian-security-announce@lists.debian.org

Several vulnerabilities have been discovered in the Linux kernel that may lead to a privilege escalation, denial of service, information leak or data loss.

perl security update
Tuesday 01. March 2016 16:42:41 | debian-security-announce@lists.debian.org

Stephane Chazelas discovered a bug in the environment handling in Perl.

All (17 / 27)

Filter by Category:

- Operating System
- CN-ADMIN
- Docsis Firmware Update

Sort By:

- Title
- Date
- Author

Pages:

First [1](#) [2](#) [3](#) [4](#) Last

News per Page:

[5](#) [10](#) [20](#)

jasper security update
Tuesday 08. March 2016 09:02:34 | debian-security-announce@lists.debian.org

libav security update
Friday 04. March 2016 22:01:35 | debian-security-announce@lists.debian.org

Linux Kernel Update
Friday 04. March 2016 10:21:16 | debian-security-announce@lists.debian.org

CN-ADMIN 3.5.18 released
Wednesday 02. March 2016 12:40:30 | Michael Neumann, support@jm-data.at

perl security update
Tuesday 01. March 2016 16:42:41 | debian-security-announce@lists.debian.org

Cable Modem Firmware Update

Cable Network Administration

CN-ADMIN

Home | **Admin** | Address | Devices | RF Analysis | Accounting | Status | Logout jm-data

General Settings

- Options
- User Management
- View devices

Nodes

- Add Node
- Search Node

SNMP

- Add SNMP Host
- Search SNMP Hosts
- Add SNMP Device Type
- Search SNMP Device Type

Docsis Package Config

- Add Docsis Package
- Search Docsis Packages

Bootfiles

- Bootfile Generation
- Bootfile Configuration
- Bootfile Profile
- Static MTA Bootfiles
- Static Modem Bootfiles
- Firmware

DHCP-Server Administration

- DHCP Lease Management
- DHCP Server Groups
- DHCP Server edit
- DHCP Classes
- Network Sites

DNS-Server Administration

- DNS Server
- DNS ACL
- Domain Name
- Domain Name Keys

IP-POOL Config

- cmis-01
- IP Pools for Subclasses

Config CPE History

- CPE History

Customer Portal

Search

Search starts with Name JM- GO Add New Profile

Search Results 1 - 34 from 34		
Name	Reference type	Options
JM-EPC3208 + EPC3212 SIP	device	
JM-EPC3208G BRIDGE PacketCable	device	
JM-EPC3208G BRIDGE SIP		
JM-FritzBox 6490 Euro SIP		
JM-SB5100E Euro		
JM-SB5101E Euro		
JM-SB5101NUE Euro		
JM-SBV5120 US PacketCable		
JM-SBV5120E Euro PacketCable		
JM-SBV5121 US PacketCable		
JM-SBV5121E Euro PacketCable		
JM-TC7200.20 Euro PacketCable		
JM-TCM42x + DCM42x Euro		
JM-TCM47x Euro		
JM-TCM47x Us		
JM-TW770 Euro		

Bootfile Docsis Settings Edit

Downstream Frequency:

Upstream Channel ID:

Network Access: n.a

Max CPEs:

TFTP Timestamp:

TFTP Address:

Privacy Enable: n.a

Software Upgrade Filename: 6490.en-de-es-it-fr-pl.141.06.50.

TFTP Upgrade Address:

HMAC Digest:

Docsis 2 Enable: n.a

MFG CVC Data:

MIIDcTCCAImgAwIBAgIQHOYbsQiGRtM+kFLctBffHDANBgkqhkiG
9w0BAQUFADBvMQswCQYDVQQGEwJCRTEfMBOGA1UEChMwWD
ENvbUxhYnMgLSBFdXJvLURPQ1NlUzEVMBMGA1UECxMMQO2Fi
bGUgTW9kZW1zMScwJgYDVQQDEx9FdXJvLURPQ1NlUzEVMBMGA1
JzZSBnb2RibSBsb290IENBMB4XDTA5MDcyMzAwMDAwMFAxODT
E5MDcyMjIzNTk1OVowXjELMAkGA1UEBhMCREUxETAPBgNVBA
oTCEFWTSBHbWJIMRQwEgYDVQQLEwtfdXJvLURPQ1NlUzEVM
mCQGA1UEAxMzMjZkZSBWZXJpZmlyYXRpb24gQ2VydGimaWN
hdGUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC
Xkei5PhEGkC+dbpdDxZdJyq/xhBtx7xuP7mGgMnmiZMZhDALja
CzyEEHPnMXijk5h/LumzzzCJOq91rvJRTAlz5E7s2tqCQq0rT/z1
9gi3h/qSLC3feQ7Jf3qio5T6JLdM7laY2FVgTUXy4S+3LoPCwPk
oZuGreVHYz14WldUuknz+tbSSRvsk76JUDHkbGE/9oPtEKDeVX
JkL4p5wAEU/MYiSST/076-RiOUQY+GtLyeLQC8k0udCkXcEiS

Drop file here

**Danke für Ihre
Aufmerksamkeit**

**Michael Neumann
mn@jm-data.at
www.jm-data.at**

JM-DATA
IT-Solutions for CATV

