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

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 Eternet

Unternehmensgruppe

JM DATA

JM DATA IT-SOLUTIONS & TELECOM

aicall

HCN Cable Connected

JA NETZ GMBH

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 Benutzen
  - 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 Verschlüsslung nur mit viel Rechenleistung möglich

- **Verschlüsselung ändert sich regelmäßig**

Entwicklung

BPI (Docsis 1.0)

- Verschlüsselung bis zu 56-bit DES
- Key refresch(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 6/0/1
Router(config-if)# cable privacy eae-policy total-enforcement
```

BPI minimal Config

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

BPI+ Overhead

useable bandwidth for Ethernet frames =	No BPI	45.614.467	Mbs
Ethernet packets per s =		89.091	pps
if BPI turned on adds overhead of 5 bytes per frame			
useable bandwidth for Ethernet frames BPI on =	With BPI	42.573.503	Mbs
Ethernet packets per s BPI on =		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 DCHP Server um MAC – IP Relation zu legitimieren
- Ausnahmen am CMTS konfigurierbar

CABLE TFT-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:

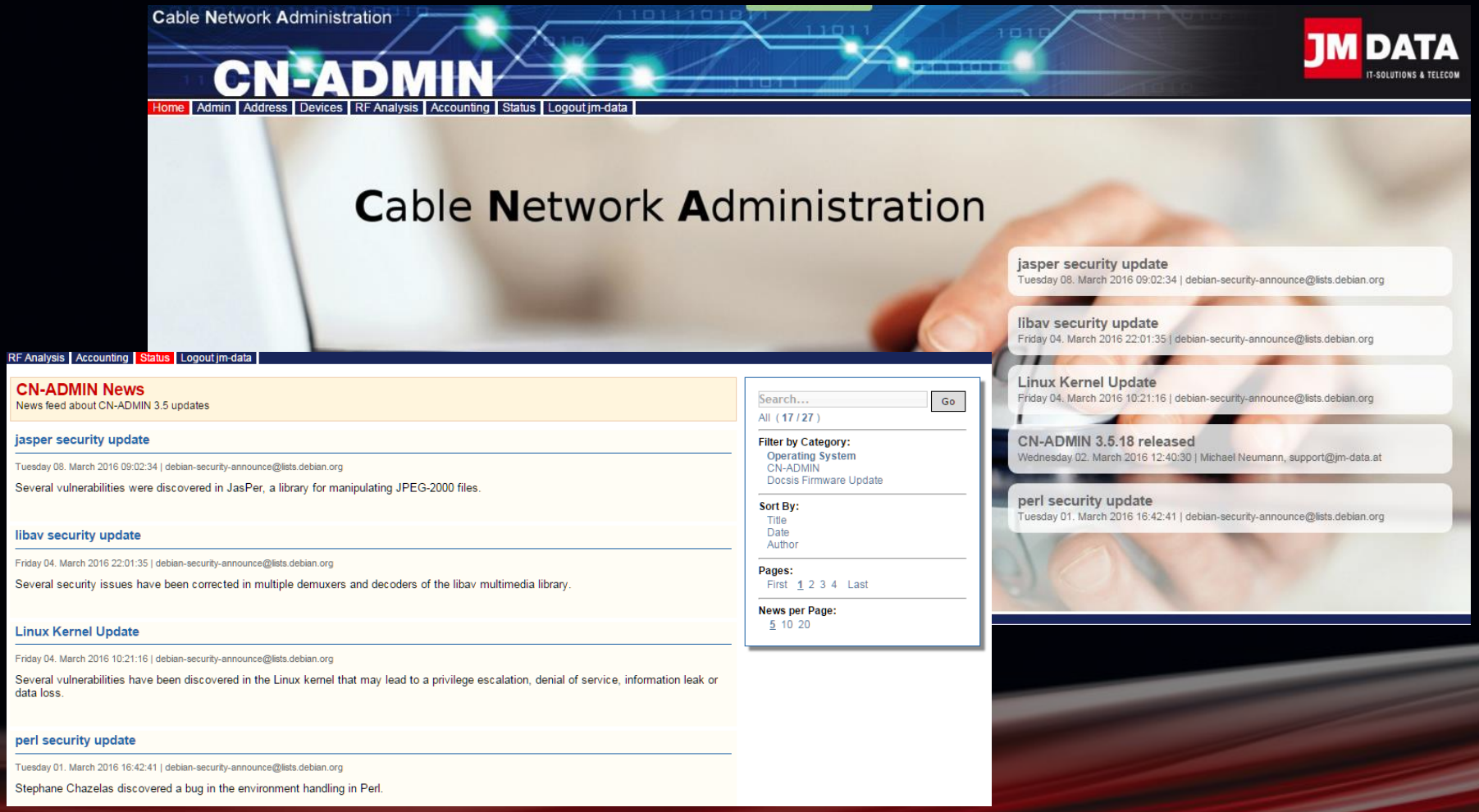
cable tftp-enforce (Im Interface Config Mode)

Software und Firmware

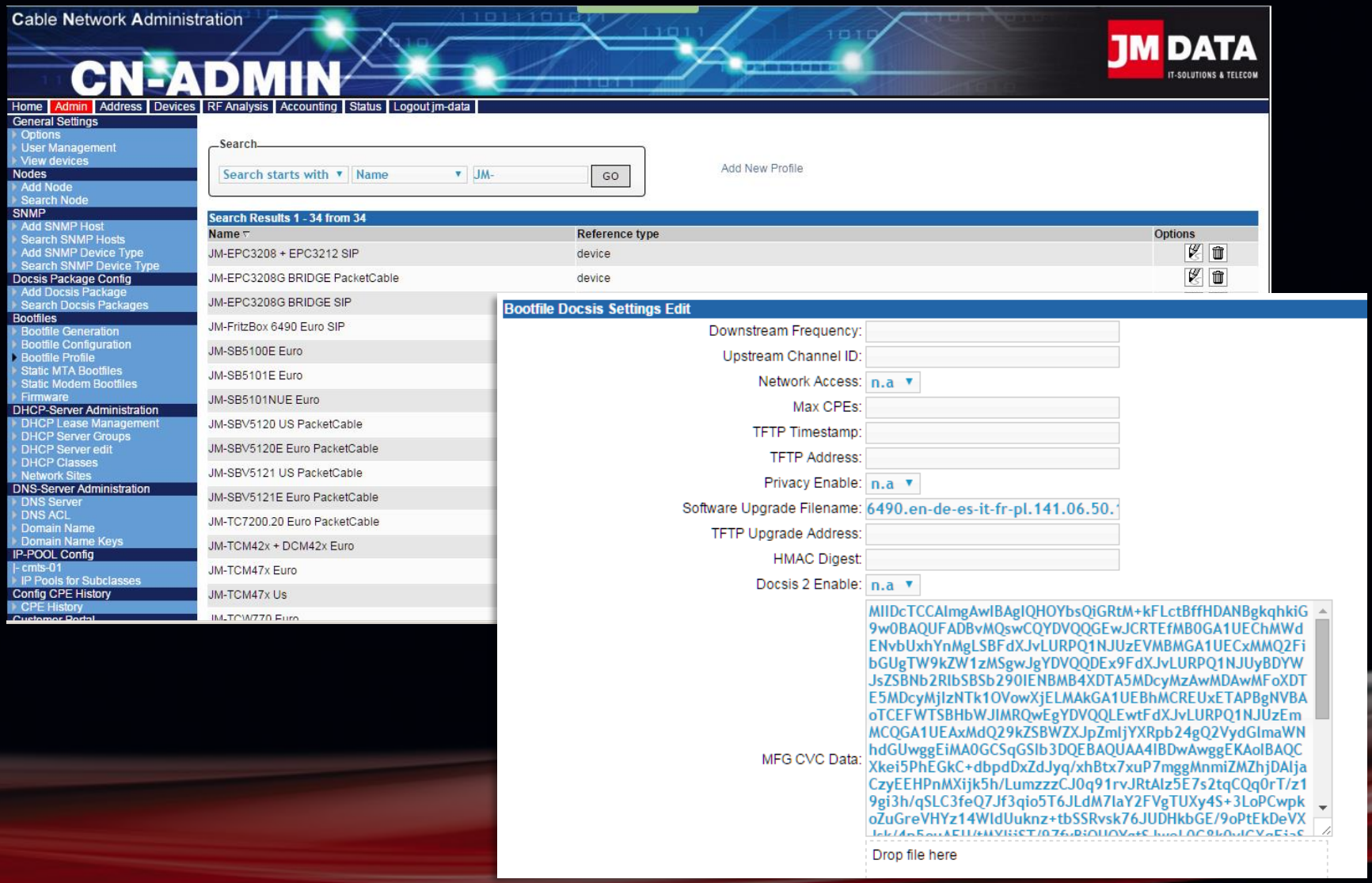
Software muss auf Servern und Cable Modems aktuell gehalten werden.

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

CN-ADMIN 3.5


Cable Network Administration
CN-ADMIN
JM DATA
IT-SOLUTIONS & TELECOM
Home
Admin
Address
Devices
RF Analysis
Accounting
Status
Logout jm-data
Cable Network Administration
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
RF Analysis
Accounting
Status
Logout jm-data
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.
Search...
Go
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

Cable Modem Firmware Update



Danke für Ihre Aufmerksamkeit

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

JM-DATA
IT-Solutions for CATV