
JENDATA
Computersysteme GmbH

KR BUSINESS EDITION

V1.2

Dokumentation

Vielen Dank für den Erwerb eines KR Business Edition
aus dem Hause JENDATA, wir bedanken uns für das
uns entgegengebrachte Vertrauen.

Bei Rückfragen wie z.B. technischen Fragen, weiteren
Entwicklungen oder Hinweisen wenden Sie sich bitte an
folgende Adresse:

JENDATA Computersysteme GmbH
Konrad-Zuse-Straße 5/7
07745 Jena

Tel: (0 36 41) 62 46-0 Fax: (0 36 41) 62 46-20

E-Mail: kr@jendata.de
http: www.jendata.de

Inhaltsverzeichnis:

1. Hinweise	3
2. Der KR Business Edition.....	4
2.1 Funktionalität	4
2.2 Lieferumfang	4
3. Hardware	5
3.1 System	5
3.2 Stromversorgung	5
3.3 Anschlüsse	6
4. Verwendete Software	7
4.1 Betriebssystemsoftware	7
4.2 Systemprogramme	7
5. Wissenswertes	10
5.1 Editor	10
5.2 Bootprozess/ Startskripte.....	11
6. Konfiguration.....	13
6.2 ISDN	13
6.3 E-Mail	15
6.4 Proxyserver	17
6.5 Firewall	18
6.5.1 Allgemein	18
6.5.2 ipfwadm	19
6.5.3 ipchains	22
6.6 Virenschaner	24
6.7 SSH	25
7. Technische Daten	26
8. Weiterführende Unterlagen	27

1. Hinweise

Das vorliegende Handbuch soll Ihnen als Ratgeber dienen und Ihnen den KR BUSINESS EDITION näher vorstellen.

Der KR BUSINESS EDITION ist ein Komplettgerät zum Anschluss Ihres Firmennetzes an das Internet.

Das Gerät bedarf keiner Bedienung vor Ort, es kann nur ferngewartet werden. Aus diesem Grund existieren keine Bedienelemente.

Bitte beachten Sie die folgenden Hinweise:



Das Abdecken der seitlichen Lüftungsschlitze und/oder des Lüfterauslasses führt zur Beschädigung des Gerätes.

Der Betrieb hat nur in waagrechtem Zustand zu erfolgen.

Der Service darf nur von Fachpersonal ausgeführt werden.

2. Der KR Business Edition

2.1 Funktionalität

Der KR BUSINESS EDITION verfügt je nach Konfiguration über folgende Funktionen:

- eingebaute Online-USV
- E-Mail in Intranet und Internet *
- WEB-Zugang *
- Proxyserver für hohe Sicherheit & Performance*
- Online-Virenschanner *
- Firmenweites DNS *
- Hausinterner Webserver (Intranetserver)*
- Fernwartfähig

*Je nach Ausstattung

2.2 Lieferumfang

Im Lieferumfang des KR BUSINESS EDITION befinden sich:

- Grundgerät
- Stromversorgungskabel
- Dokumentation.



Frontansicht

3. Hardware

3.1 System

Der KR besteht aus einem stabilen Metallgehäuse, das die Abmessungen von (Höhe) 44 mm (1 HE) x (Tiefe) 255 mm x (Breite) 442 mm hat. Es ist zur Verwendung in 19“-Schränken geeignet.

Als Kernstück ist ein 80x86-kompatibles Industrieprozessorsystem eingesetzt. Es verfügt über einen Watchdog. Dieser startet ein festgefahrener System automatisch neu.

Die Verbindung zwischen dem Firmennetzwerk und dem Provider stellt ein Netzwerkinterface her. Komplettiert wird die Recheneinheit durch eine Festplatte mit einer Kapazität von mindestens 20 GB.

3.2 Stromversorgung

Die Stromversorgung erfolgt über ein primärgetaktetes zweistufiges Netzteilsystem. Die integrierte prozessorgesteuerte USV arbeitet im Online-Betrieb. Sobald der KR BUSINESS EDITION von der Versorgungsspannung getrennt ist, beendet die USV alle gestarteten Prozesse und fährt die Recheneinheit kontrolliert herunter. Das System wird so vor Datenverlust geschützt.

3.3 Anschlüsse

Der KR BUSINESS EDITION verfügt über drei Anschlüsse. Der Anschluss an die Netzspannung erfolgt über den mitgelieferten Kaltgerätestecker auf der Rückseite des Gerätes. Die Frontanschlüsse d1 und d2 werden je nach Konfiguration (lt. gerätespezifischem Beiblatt) wie folgt belegt.

Ethernet

Ist der Anschluss als Ethernet bezeichnet, handelt es sich um 10BaseT an RJ45. Der Anschluss kann direkt mit einem Hub/Switch verbunden werden. Standardmäßig ist d2 mit dem internen Ethernet verbunden.

ISDN

Ist ein ISDN-Anschluss konfiguriert, ist dieser ein DSS1 (Euro-ISDN) auf RJ45. Er wird direkt mit dem S0 eines Mehrgeräteanschlusses bzw. einer Telefonanlage verbunden. Der Standardanschluss ist d1.

FAX

Wird der KR BUSINESS EDITION mit der Option Fax ausgeliefert, erfolgt der Anschluss von Ethernet und Faxline über ein mitgeliefertres Spezialkabel an d1.

4. Verwendete Software

Im Auslieferungszustand ist die Systemsoftware vollständig installiert und konfiguriert. Auf grundlegende Softwarebestandteile soll im Folgenden kurz aufmerksam gemacht werden. Möglichkeiten zur Anpassung an Ihre eigenen Bedürfnisse finden Sie in Abschnitt 5 (Konfiguration).

4.1 Betriebssystemsoftware

Als Betriebssystem dient ein UNIFIX LINUX V2 (SYS V init) in der Kernelversion 2.0.35 bzw. 2.2.19 (je nach Ausstattung).

Das File-System ist je nach Anwendung ext2 bzw. ext3. Kernelversion 2.0.35 verfügt optional über ein Filecache.

4.2 Systemprogramme

E-Mail

Das E-Mail-Programm Sendmail gewährleistet ein sicheres und stabiles Arbeiten.

Es ist standardmäßig auf folgende Ports eingestellt.

Provider- IN & OUT:	uucp
User-IN:	smtp
User-OUT:	pop3

Die Verwendung von imap ist möglich.

ISDN

Das ISDN-System basiert auf dem klassischen ISDN für LINUX (i4l), es werden die HiSax-Treiber eingesetzt. Die Einwahl beim Provider kann nach einem der folgenden Verfahren erfolgen:

- rawIP (Transparent HDLC)
Identifizierung nach der Telefonnummer
- ppp (Point to Point Protocol)
Identifizierung mit Login und Passwort

Der KR BUSINESS EDITION ist standardmäßig auf rawIP eingestellt.

Proxy

Als Proxyserver ist SQUID für LINUX konfiguriert. Es gestattet in der Standardeinstellung interne Zugriffe auf die Ports 3128 und 8080. Der externe Zugriff ist gesperrt. Standardmäßig haben alle Nutzer Zugriff auf den Proxyserver.

SSH

Die Secure Shell (sichere Shell) gehört zur Grundausstattung. Sie ermöglicht die Fernwartung über einen verschlüsselten und damit nicht mitzulesenden Kanal.

Optional wird mit der SSH ein geschützter Kanal zwischen zwei KR BUSINESS EDITION geschaltet, um Standorte miteinander zu verbinden.

Firewall

Hier handelt es sich um eine Kernelfirewall, die neben der Sicherheit einen hohen Datendurchsatz gestattet.

Alle drei Wege (INPUT, FORWARD und OUTPUT) sind konfiguriert.

Soweit keine speziellen Konfigurationen angegeben sind, werden folgende Ports offen gehalten:

Extern: 21, 22 und 23 für die Fernwartung

Intern: 21, 22, 23, 25, 37, 42, 110, 3128 und 8080

Dynamische Ports sind in der Standardinstallation nicht geschaltet. Dasselbe gilt für Masquerading.

Virenschaner (*)

Als Virenschaner wird die F-Prot Engine in der neusten Version verwendet. Um ständig über die neusten Virendefinitionen zu verfügen, wird in bestimmten Zeitintervallen ein automatisches Update durchgeführt.

Watchdog

Die zur Steuerung des Hardwareseitig implementierten Watchdog eingesetzte Software ist Watchdog für LINUX in der Version 0.0.2.

Sie ist an die Konfigurationsadressen 0x443 und 0x843 des Industrieprozessorsystems angepasst.

Weitere Daten finden Sie unter:

<http://www.jendata.de/download/>

(*) je nach Ausstattung

5. Wissenswertes

5.1 Editor

Unter Unix/Linux werden grundsätzlich alle Konfigurationen als Textdatei abgespeichert. Der versierte Administrator nutzt zum Bearbeiten dieser Dateien deshalb die mitgelieferten Editoren (**emacs**, **vi**, **joe** oder **edit**).

Der **emacs** ist der universellste Editor, er benötigt jedoch etwas Einarbeitungszeit. Besonders für größere Programmierprojekte ist dieser Editor sehr gut geeignet. Eine Befehlsdokumentation finden Sie in */usr/doc/emacs-refcard.dvi.gz*.

Der erfahrene Unix-Nutzer wird natürlich dem **vi** den Vorzug geben. Dieser Editor ist Bestandteil fast aller Unixdistributionen und deshalb sehr verbreitet. Ohne grafische Benutzeroberfläche und Maussteuerung kann er selbst über eine schmale Modemleitung problemlos genutzt werden.

Der **joe** ist sehr einfach zu handhaben. Gestartet wird der Editor durch die Eingabe von *joe Dateiname*. Alle Befehle werden durch die Tastenkombination **CTRL+K**-ausgeführt. Mit den Tasten **CTRL+K-H** rufen Sie die Hilfe auf.

Falls Sie keinerlei Erfahrung im Umgang mit Unix/Linux besitzen sollten sie **edit** nutzen.

5.2 Bootprozess/ Startskripte

Nachdem der Kernel alle Gerätetreiber geladen hat ruft er das Programm `/etc/init` auf. Dessen Programmablauf wird vorrangig durch die Datei `/etc/inittab` bestimmt. Als erstes wird das Runlevel definiert, welches beim Booten standardmäßig gestartet wird.

Danach wird die Datei `sysinit` abgearbeitet, hier werden grundlegende Systemkonfiguration gestartet. So wird zum Beispiel die Aufteilung der Swap-Partition durchgeführt oder die Systemzeit mit der internen Rechneruhr synchronisiert.

Den nächste Schritt leistet der Aufruf von `rc`. Je nach Runlevel werden jetzt verschieden Skripte abgearbeitet. Dies kann das Starten des E-Maildienstes, der Firewall, des Proxyserver und unzähliger weiterer Dienste sein.

Da jedes Runlevel teils gleiche, teils unterschiedliche Skripte verwendet, wäre es unsinnig für jedes Runlevel eigene Skripte zu nutzen. Alle Skripte der verschiedenen Diensten sind deshalb im Verzeichnis `/etc/init.d` enthalten. Jedes Runlevel greift jetzt mit sogenannten symbolischen Links auf diese Skripte zu.

Sie können also bei Bedarf einen Dienst durch Eingabe des Befehles `/etc/init.d/Dienst start/stop` manuell starten oder herunterfahren. Sie müssen sich aber über die möglichen Folgen im Klaren sein. Sollte zum Beispiel der Firewalldienstes manuell heruntergefahren werden, so ist ihr System für mögliche Angreifer leicht zu überwinden.

Der nächste Eintrag in der *rc.inittab* beantwortet die oft gestellte Frage, warum fährt Unix/Linux mit der Tastenkombination *Strg+Alt+Entf* geordnet herunter und startet neu? Der durch die Tastenkombination ausgelöste Interrupt wird vom Betriebssystem abgefangen und in der *inittab* kontrolliert verarbeitet.

Im letzten Abschnitt der Datei *inittab* wird die Anmeldung des Benutzers an den verschiedenen Konsolen von Unix/Linux geregelt.

6. Konfiguration

Alle hier dokumentierten Konfigurationsschritte sollten nur von fachkundigem Personal mit Root-Rechten vorgenommen werden. Falsche Einstellungen können Systemabstürze und Schäden hervorrufen.

6.2 ISDN

Gestartet wird der ISDN-Dienst mit dem Befehle */etc/init.d/isdn restart*. Bei Bedarf kann der Dienst mit */etc/init.d/isdn stop* vollständig heruntergefahren werden.

Das ISDN-Startscript, */etc/init.d/isdn*, ist bereits vollständig konfiguriert, es lässt sich mit einem Editor nach Ihren Wünschen anpassen.

In diesem Script ist der vollständige Startvorgang des ISDN-Dienstes festgelegt. Des weiteren wird überprüft, ob ein ISDN-Kanal zur Datenübertragung ausreicht oder ob eine Kanalbündelung nötig ist. Im Folgenden sollen die wichtigsten Befehle im Startscript (*/etc/init.d/isdn*) kurz erklärt werden.

addiff	ISDN-Gerät wird hinzugefügt
encap	Encapsulations-Protokoll
l2_prot	Netzwerkprotokoll für die 2. Schicht (Datensicherungsschicht, lt. OSI-Referenzmodell)
l3_prot	Netzwerkprotokoll für die 3. Schicht (Netzwerkschicht, lt. OSI-Referenzmodell)
eaz	(Endgeräteauswahlziffer) Telefonnummer des ISDN-Gerätes

huptimeout	Zeit in Sekunden, nachdem bei nichtgenutzter Leitung die Verbindung getrennt wird
chargeup	vor dem nächsten Gebührenintervall wird bei ungenutzter Leitung aufgelegt (on/off)
secure	eingehende Rufnummern werden überprüft, Sicherheitsmodus (on/off)
callback	Rückrufmodus (in/out/off)
addphone	Nummern die gewählt werden dürfen (in/out)
dialmode	Verbindungsaufbaumodus (auto/manual/off)
addslave	zweite ISDN-Leitung wird hinzugefügt
sdelay	Anzahl der max. Zeichenübertragung pro Sekunde, liegt der Datendurchsatz darüber wird die zweite ISDN-Leitung zugeschaltet

Beachten Sie bitte:

Wenn Sie sich über ISDN am KR BUSINESS EDITION angemeldet haben, sollten Sie den Befehl `/etc/init.d/isdn stop` tunlichst vermeiden.

6.3 E-Mail

Der Befehl `sendmail -bd -q30m` startet das E-Mail-Programm. Der Parameter `-db` veranlasst, dass das Programm im Daemonmodus startet, es wartet also im Hintergrund auf ankommende Mails.

Alle abgehenden E-Mails werden im Verzeichnis `/var/spool/mqueue` gesammelt und versandt.

Fehlgeschlagene Sendeversuche werden entsprechend dem Parameter `-q30m` alle 30 Minuten wiederholt.

Alle ankommenden Mails durchlaufen einen Prüfmechanismus, wenn sie von Sendmail entgegengenommen werden. Diese Mails werden mit mehreren Datenbanken verglichen, damit sie einen bestimmten Nutzer erreichen. Alle nicht zuordenbaren Mails werden auf diesem Wege abgewiesen.

In der editierbaren `/etc/aliases` wird zum Beispiel die Verteilung der E-Mails an lokale Benutzer festgelegt. Mit dem Befehl `newaliases` wird aus dieser Datei eine zugriffssichere Datenbankdatei für diesen Prüfmechanismus erzeugt.

Jeder Nutzer besitzt eine eigene Datei in `/var/spool/mail/` auf dem Server, in dem alle ankommenden E-Mails gespeichert werden. Mit einem Mail User Agent (z.B. Netscape Messenger, MS Outlook) kann jeder Nutzer seine E-Mails aus seinem eigenen Verzeichnis vom Server abholen.

In der Datei `/etc/sendmail.cf` sind die wichtigsten Konfigurationen von Sendmail gespeichert. Diese Datei wird bei der Installation generiert und ist in einer

eigenen Syntax verfasst. Sie sollte nur von erfahrenen Administratoren editiert werden. Es sei jedoch auf einige wichtige Befehlszeilen verwiesen.

DS smtp: mail.beispiel-domain.de heißt die Befehlszeile, die den Node Name des E-Mail-Servers enthält. Der Server nimmt E-Mails im SMTP-Modus entgegen.

Mit *DS uucp: uucp.beispiel-domain.de* werden die E-Mails im UUCP-Modus entgegengenommen.

Bei Marke *DM beispiel-domain.de* können Sie einen Domainnamen eintragen. Alle ausgehenden E-Mails werden mit dieser Domain als Absender gesendet.

Ab Marke *S98* besteht die Möglichkeit eigene benutzerspezifische Rules einzutragen.

6.4 Proxyserver

Squid für Linux wird über die Konfigurationsdatei *\$Path/etc/squid.conf* eingestellt. Wobei gilt *\$Path=/usr/local/squid* bzw. *\$Path=/usr/local/squid-2.4*. Die Verzeichnisse variieren, je nachdem welche Versionsnummer zum Einsatz kommt. Alle nötigen Parameter werden bereits bei der Installation von uns konfiguriert. Die *squid.conf* ist ausführlich kommentiert, sollte aber dennoch nur von erfahrenen System-Administratoren editiert werden. Falls Einträge geändert werden, muss die Datei mit dem Befehl *\$Path/bin/squid -k reconfigure* neu eingelesen werden. Sie können Squid mit *\$Path/bin/squid -k shutdown* kontrolliert herunterfahren und mit *\$Path/bin/squid* wieder neu starten.

Über den Eintrag *http_port* wird eine Portadresse eingestellt. Über diesen Port kann der Client eine Verbindung mit dem Proxyserver aufbauen. Standardmäßig ist die Portadresse 3128 und 8080 definiert. Prinzipiell ist jede Portadresse einstellbar. Sie sollten sich aber bewusst sein, dass diese Adresse nur von Squid genutzt wird und damit nicht mehr für andere Programme zur Verfügung steht.

Jeder Proxyserver, so auch Squid, sollte über einen ausreichend großen Cachearbeitspeicher verfügen. Die Größe dieses Speichers kann in der Zeile *cache_mem* verändert werden, sie wird vom Arbeitsspeicher des Rechners abgezweigt.

6.5 Firewall

Um eine Firewall wirklich sicher zu konfigurieren, benötigt man jahrelange Erfahrung im Bereich der Netzwerksicherheit. Sie müssen ständig auf dem neusten Stand sein, um neu entdeckte Sicherheitslücken zu schließen. Wir können im Folgenden nur Ratschläge und Hinweise zur richtigen Einstellung einer Firewall geben. Eine umfassende Administration von einem Fachmann kann diese Dokumentation nicht ersetzen.

6.5.1 Allgemein

IPFW ist eine Kernelfirewall die als Paketfilter fungiert. Konfiguriert wird diese Firewall entweder mit **ipfwadm** oder mit **ipchains**. Beide Administrationswerkzeuge sind gut dokumentiert, die entsprechenden Manualseiten können als umfassendes Nachschlagewerk dienen. Die Firewall sollte schon beim Booten des Systems gestartet werden. Üblicherweise werden in einem Startskript wie */etc/rc.d/init.d/firewall* die nötigen Parameter für die Firewall definiert.

Mit der verwendeten Firewall wird der gesamte Paketverkehr des Netzwerkes gefiltert und somit überwacht. Mögliche Angriffe werden protokolliert und können so zurückverfolgt werden. Auch bietet sich die Möglichkeit zu überwachen wieviel Verkehr zwischen einzelnen Rechnern und dem KR Business Edition besteht. Dieses Verfahren wird IP-Accounting genannt.

Alle Pakete müssen einen Filtermechanismus auf Paketebene durchlaufen. Die drei nichtlöschbaren Regellisten (Input, Forward, Output) werden bereits bei der Installation definiert.

Ein ankommendes Datenpaket durchläuft als erstes einen Prüfsummentest. Es findet ein Test statt, der die vollständige und fehlerfreie Übertragung des Paketes überprüft. Ist die Übertragungssicherheit nicht gewährleistet wird das Paket abgewiesen.

Danach muss sich das Datenpaket den Regeln des Input unterziehen. Ist dies geschehen wird entschieden wie mit dem Paket weiter zu verfahren ist. Falls das Paket an andere Rechner weitergeleitet werden soll, müssen die Regeln des Forward getestet werden. Bevor ein Paket den KR Business Edition verlässt wird das Regelwerk der Output überprüft. Sollte keine der Prüfregel zutreffen, dann wird das Paket nach einem definierten Standardverfahren (default policy) verarbeitet.

6.5.2 ipfwadm

IPFWADM bietet die Möglichkeit sowohl eingehende als auch ausgehende TCP-, UDP- und ICMP-Pakete zu filtern.

Alle Einstellungen werden nach einer einheitlichen Syntax im Startskript angegeben.

ipfwadm –Grundoption –Befehl –Parameter [Option]

Fünf **Grundoptionen** können definiert werden.

ipfwadm -A	spezifiziert die IP-Accounting-Regeln
ipfwadm -I	Input-Regeln
ipfwadm -O	Output-Regeln
ipfwadm -F	Forward-Regeln
ipfwadm -M	Masquerading-Administration

Die wichtigsten **Befehle** lauten.

-a	eine oder mehrere Regeln werden an das Ende der Regelliste angefügt
-d	eine oder mehrere Regeln werden gelöscht
-f	entfernt alle Regeln der Regelliste (Vorsicht bei der Fernwartung, alle Zugriffe werden abgewiesen)
-h	Hilfeaufruf
-i	eine oder mehrere Regeln werden an den Anfang der Regelliste eingefügt
-l	Regelliste wird angezeigt
-p	Änderung der Standardeinstellung der Paketbehandlung, falls keine Regel zutrifft

Wichtige **Parameter** für die Firewallkonfiguration.

-D	Destination, Zieladressendefinition
-P	Verweist auf das Protokoll bei der Regeldefinition (all/tcp/udp/icmp)
-S	Source, Ursprungsadressendefinition
-W	Interfacename mit dem ein Paket versendet oder empfangen wird (isdn/eth)

Wenn eine Regel hinzugefügt wird, muss definiert werden was mit dem Paket geschehen soll. Es bestehen die folgenden Möglichkeiten.

a	accept, das Paket wird akzeptiert
d	deny, das Paket wird abgewiesen, der Absender erhält keine ICMP-Nachricht
r	reject, das Paket wird abgewiesen, der Absender erhält eine ICMP-Nachricht

Abschließend sollen einige Beispielzeilen die vorhergehenden Befehle nochmals erläutern.

Alle Pakete der Rechner 132.31.25.XXX werden abgelehnt.

```
ipfwadm -I -a d -S 132.31.25.0/255.255.255.0
```

Deny wird als Standardeinstellung für die Input-Regeln festgelegt.

```
ipfwadm -I -p d
```

Überwachung des Send- und Empfangsverkehrs der KR BUSINESS EDITION.

```
ipfwadm -A -a -S MyIP -D 0/0
```

```
ipfwadm -A -a -S 0/0 -D MyIP
```

6.5.3 ipchains

Der Befehlsaufbau von ipchains und ipfwadm ist ähnlich. Bis auf wenige Ausnahmen kann gesagt werden, alle Befehle, Parameter und Optionen die bei ipfwadm klein geschrieben sind werden bei ipchains groß geschrieben und umgekehrt. Mit ipchains ist es jetzt möglich Sprungmarken für Regeln zu definieren. Die Einstellungen, die bei der Installation der KR Business Edition definiert sind, sollten nicht verändert werden. Falls Sie dennoch Einstellungen ändern wollen, empfiehlt es sich alle alten Regeln zu löschen und danach die Firewall neu einzurichten. Dabei sollten die allgemeinsten Regeln am Anfang definiert werden und die speziellen am Ende des Firewallskriptes. Alle Standardeinstellungen (default-policy) müssen immer separat editiert werden und sollten am Anfang eines jeden Firewallstartskriptes stehen.

Im Folgenden wird eine kleine Befehlsübersicht angegeben. Alle nicht enthaltenen Befehle können im Manual nachgelesen werden.

Ipchains -N	Neue Sprungmarke wird definiert
Ipchains -F	Regeln werden gelöscht, wenn nichts angegeben wird werden alle gelöscht
Ipchains -L	Zeigt eine Regelliste an
Ipchains -P Regelliste deny/accept/reject	Standardregeln werden definiert
Ipchains -A	Hängt eine Regel an das Ende einer vorhandenen Regel

Ipchain -s	Zieladresse
Ipchain -d	Quelladresse
Ipchain -p	Protokollangaben
Ipchain -I	Netzwerkinterface
Ipchains -y	Nur SYN-Bit von TCP ist gesetzt, alle TCP-Pakete die einen Verbindungsaufbau versuchen werden betrachtet
Ipchain -j	Sprungzielangabe, falls die Regel zutrifft

Analog zu den Beispielen aus Kapitel 5.5.2 werden hier einige Befehlszeilen dokumentiert.

Alle Pakete der Rechner 132.31.25.XXX werden abgelehnt.

```
ipchains -A input deny -s 132.31.25.0/255.255.255.0
```

Deny wird als Standardeinstellung für die Input-Regeln festgelegt.

```
ipfwadm -A input -P deny
```

Der kommende und gehende Verkehr des KR BUSINESS EDITION wird überwacht.

```
ipchains -A output -s MyIP -d 0/0
```

```
ipchains -A -input -s 0/0 -d MyIP
```

6.6 Virens Scanner

Als Virens Scanner leistet die F-Prot Engine ihre Arbeit. Es existieren 3 Skripte die den Scanprozess steuern.

Das erste regelt das Verhalten von virmail. Es werden alle Mails vor ihrer lokale Ablage auf Viren überprüft. Vor der Übergabe der Mails an Procmail müssen auch diese Mails nach Viren untersucht werden. Dieses steuert das Skript für virprocmail. Mit dem letzten wird das gesamte System nach Viren durchsucht. Mit virscan -h erhalten Sie zu diesem Thema Hilfe.

Alle zeitgesteuerten Prozesse werden in der Unix/Linux-Umgebung mit crontab geregelt. So zum Beispiel der automatische Update der Virendefinitionen. Mit crontab -l erhalten Sie eine Auflistung aller eingestellten Zeitprozesse.

6.7 SSH

Um zwei Rechner mit einander über SSH (secure shell) zu verbinden, muss auf einem Rechner ein Programm gestartet sein, das auf eine Anfrage zum Verbindungsaufbau wartet. Dieses sogenannte Daemonprogramm heißt *sshd* und wartet am Port 22 auf eine Anfrage von einem Client. Es sollte automatisch beim Bootvorgang über einen Eintrag in einem Startskript (z.B. */etc/rc.d/rc.local*) oder manuell mit der Befehlszeile */etc/init.d/sshd start* gestartet werden. Die serverseitige Konfiguration wird in der Datei */etc/sshd_config* vorgenommen. Hier einige wichtige Einstellungen.

PasswordAuthentication yes	Passwort erforderlich
PermitEmptyPassword no	Leerer Passwortstring nicht erlaubt
KeyRegenerationIntervall (default 3600 Sekunden)	Verschlüsselung wird in bestimmten Intervallen neu generiert
KeepAlive yes	Verbindungsstörungen werden erkannt, Server verschwendet keine Ressourcen
PermitRootLogin no	Root darf sich aus Sicherheitsgründen nicht über ssh einloggen
Port 22	Port auf dem der Daemon auf Anfragen wartet

Eine ausführliche Anleitung finden Sie im SSH-Manual.

7. Technische Daten

System	80X86 kompatibler Industrierechner
Anschlüsse	
ISDN	Mehrgeräteanschluss (DSS1 bzw. 1TR6, RJ45)
Ethernet	(Fast) Ethernet, RJ45 (Cat 5)
Fax	Fax G3 (TAE-N)
Betriebsspannung	Kaltgerätestecker
Anschlusswerte	
Betriebsspannung	84 - 250 V, 50 - 60 Hz
Leistungsaufnahme	70 VA max., 30 VA typ.
Betriebsumgebung	
Temperatur	5 – 55 °C
rel. Luftfeuchte	10 – 90 % (nicht kondensierend)
geogr. Höhe	minus 250 – 3000 m
Lagerbedingungen	
Temperatur	minus 40 – 65 °C
rel. Luftfeuchte	5 – 95 % (nicht kondensierend)
geogr. Höhe	minus 250 – 8000 m
Abmessungen	443*44*251 mm
Lautstärke	60 dB max.

8. Weiterführende Unterlagen

Als angemeldeter User erhalten Sie mit dem Befehl „documentation“ eine Dokumentation der verwendeten Programme.

Die komplette CD von UNIFIX LINUX befindet sich als Image auf der Partition /dev/hda2. Auf Wunsch erhalten Sie diese als CD inkl. Startdiskette zugesandt.

Als weiterführende Literatur empfehlen wir Fachbücher zu den einzelnen Themengebieten.

- Sendmail – Bryan Costales u.a. - ISBN: 1565922220
- SSH Secure Shell – Daneil J. Barret u.a. - ISBN: 3897212870
- Linux in a Nutshell – Ellen Siever - ISBN: 3897211955

Notizen:

Notizen:

JENDATA

Computersysteme GmbH

Konrad-Zuse-Straße 5/7
07745 Jena

Telefon: (0 36 41) 62 46-0
Fax: (0 36 41) 62 46-20

<http://www.jendata.de>
service@jendata.de