

SLAC

„Relax & Recover“

Secure Linux Disaster Recovery

Schlomo Schapiro
Senior Consultant
2007-12-06

Agenda

- I Problemstellung**
- I Disaster Recovery Verfahren**
- I Linux & Disaster Recovery**
- I Lösungen - Relax & Recover**
- I Enterprise Secure Disaster Recovery**
- I Live Demo & Feedback**

prinzipielle Problemstellung

- **Verfügbarkeit = Fehlererkennungszeit + Wiederherstellungszeit**
- **Auch eine Erhöhung der Redundanz, z.B. durch RAID, Spiegelung oder Cluster, schützt nicht vor Installations-, Konfigurations-, Bedienungs- und Softwarefehlern**
- **Oftmals fehlen durchdachte Havariekonzepte mit konkreten Handlungsanweisungen !**
- **Wiederinbetriebnahme in einem „Ausfallrechenzentrum“ ?**

Backup ist nicht Restore !

HEY, STUFF THIS!



STEINFELD



Backup ≠ Havarielösung

- ! Backupsoftware sichert Dateien
- ! komplettes System ist mehr als Dateien
- ! Backupsysteme benötigen ein korrekt installiertes und konfiguriertes System zur Dateiwiederherstellung
- ! D.h. manuelle Wiederherstellung der Systemumgebung (Wie war sie ? Fehler !)

Sehr zeitaufwändig und fehleranfällig !

Agenda

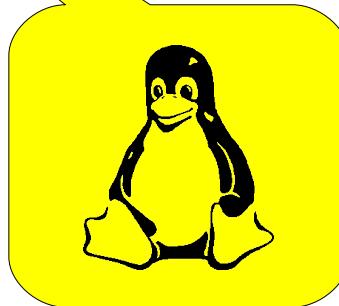
- I Problemstellung
- I **Desaster Recovery Verfahren**
- I Linux & Desaster Recovery
- I Lösungen - Relax & Recover
- I Enterprise Secure Desaster Recovery
- I Live Demo & Feedback

HW oder SW Disaster ?



SAN

FC / iSCSI



Lokale Festplatten:

- System
- Daten



SAN Festplatten:

- System (Boot von SAN)
- Daten

Desaster Recovery – HW / SW Strategien

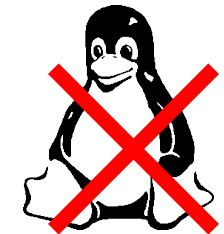
Hardware Desaster:

- Ersatzhardware (ggf. Festplatten umstecken)
- Ersatz-VM (insbesondere mit SAN Boot)



Software Desaster:

- wenige Dateien -> Restore aus Backup
- System -> Restore aus Image oder Backup
- Daten -> Restore von System & Restore der Daten aus Backup



Im Folgenden: Desaster Recovery = Systemwiederherstellung !

Was bedeutet Disaster Recovery ?

- **Sicherung des Betriebssystems und der Anwendungen ohne Datenbestände, aber mit der gesamten Systemkonfiguration**
- **Sicherung im laufenden Betrieb**
- **Automatisierter Prozess**
- **Sicherung auf einen externen Datenspeicher, z.B. Tape, CD/DVD, NFS ...**

Was bedeutet Disaster Recovery ?

- Wiederherstellung auf „nackter Hardware“ ohne weitere Hilfsmittel möglich
- Andere Hardware (mit gleichen Treibern)
- Keine Nachkonfiguration nötig – System ist sofort voll einsatzbereit und fertig konfiguriert

Start

– Kaffee trinken –

Fertig !



Desaster Recovery - Strategien

I Disk Imaging

- + Bei offline-Backup kein Problem mit offenen Files
- Sehr problematisch im laufenden Betrieb
- Keine perfekte Open Source Software für Linux

I Dateien kopieren & HD Layout sichern

- + Im laufenden Betrieb möglich
- + Backup unabhängig von HD Layout
- Höherer Aufwand bei Wiederherstellung (scriptbar)
- Evtl. Konsistenzprobleme (sollten aber für Backup gelöst sein)

Agenda

- | Problemstellung
- | Disaster Recovery Verfahren
- | **Linux & Disaster Recovery**
- | Lösungen - Relax & Recover
- | Enterprise Secure Disaster Recovery
- | Live Demo & Feedback

Vorteile eines Linux Systems

- **Alle Informationen sind in Dateien gespeichert, gesperrte Dateien selten**
- **Betriebssystem und Anwendungen sind schlank - in 600 MB ist ein kompletter Server mit Standardanwendungen möglich**
- **Offene Systeme - Offene Verfahren**
- **Alle Schritte der Installation sind skriptbar: Partitionierung, Dateisysteme, Boot Manager, ...**

Desaster Recovery – Medien

- Wichtig: Externe Speicherung
- Bootfähiges Medium: CD/DVD, USB Stick, LAN, Tape
- Medium meist eine Kombination aus Bootmedium und Backupmedium, z.B bootfähige
 - CD/DVD mit Backupdaten
 - USB Stick (ggf. mit Backupdaten)
 - Netzwerkkarten (PXE) & Daten per NFS/CIFS/...
 - Tapes – HP OBDR (CD Emulation)
- Trennung Booten & Backupdaten:
 - Booten von CD/DVD, USB Stick, LAN
 - Restore mit Backupsoftware, rsync, tar usw.



Desaster Recovery – Funktionsweise

- **Sicherung des Festplattenlayouts:**
 - Partitionen und RAID/LVM Konfiguration
 - Dateisysteme und Dateisystemlabel
 - Boot Loader (GRUB, LILO, ELILO)
- **Sicherung der Dateien (tgz, rsync, extern, ...)**
- **Erstellen eines Bootmediums mit der Systemkonfiguration (und dem Dateibackup)**
- **Aus dem laufenden System heraus, Vorteil: 100% kompatibel zur Hardware**

Desaster Recovery – Rescue Linux

- Erstellung eines „Rescue Linux“ aus dem laufenden System
- Optimal angepasster „Werkzeugkasten“
- Clonen der Betriebsumgebung:
 - Kernel
 - Treibereinstellungen
 - Netzwerkkonfiguration usw.
 - Basisprogramme
 - Systemtools
- Betrieb in einer RAM Disk



Desaster Recovery – Wiederherstellung

- Boot vom Desaster Recovery Medium
- Wiederherstellung Festplattenlayout:
 - Partitionierung / RAID & LVM einrichten
 - Formatieren (mkfs, mkswap, ...)
 - Labels
- Wiederherstellung der gesicherten Dateien
- Wiederherstellung des Boot Loaders
- Reboot
- Fertig !

Agenda

- | Problemstellung
- | Disaster Recovery Verfahren
- | Linux & Disaster Recovery
- | **Lösungen - Relax & Recover**
- | Enterprise Secure Disaster Recovery
- | Live Demo & Feedback

Kommerzielle Lösungen

- i.d.R. als Teil eines Backupsystems
- Fast immer kostenpflichtig und sehr teuer bis ~1000 EUR / Client !
- Manchmal auch kostenlos, taugt es ?
- Nicht immer mit dem Backup integriert
- DR Modul nicht für jede Backupsoftware verfügbar
- Decken nur einfache Installationen ab
- meist fertige „feste“ DR Bootmedien - unflexibel bei Hardware- und Treiberproblemen
- Keine Zertifizierungen für Server Hardware

Open Source Disaster Recovery

Es gibt eine Auswahl an Systemen mit unterschiedlichen Funktionsansätzen:

- Relax & Recover
- mkCDrec
- Mondo Rescue
- CRU
- BACULA
- Selber Skripte schreiben
- <das System, von dem ich noch nicht gehört habe>

Relax & Recover – ReaR

- rear.sourceforge.net
- GPL Software – Entwickler in Berlin & Belgien
- 100% Shell Skript – keine GUI
- Nutzt Host Kernel, Module & Binaries (ab Kernel 2.6)
- Unterstützt SW/HW RAID, LVM
- Backup auf NFS & CIFS
- Boot von CD/DVD, USB Medien und PXE

- Nachfolger von mkCDrec (mkcdrec.sourceforge.net)

Relax & Recover – Flexibilität

- **Konzentration auf Disaster Recovery, nicht Backup**
- **Integration von Backupsoftware - Auslagerung der Dateisicherung in die Backupsoftware**
- **Einfaches Full Backup möglich**
- **Komplementärprodukt zu klassischer Backupsoftware:**
 - **Backup-Software: Dateisicherung**
 - **ReaR: Systemsicherung (Festplatten-Layout ...)**
 - **ReaR benutzt Backup-SW bei der Systemwiederherstellung um die Dateien zu restaurieren**

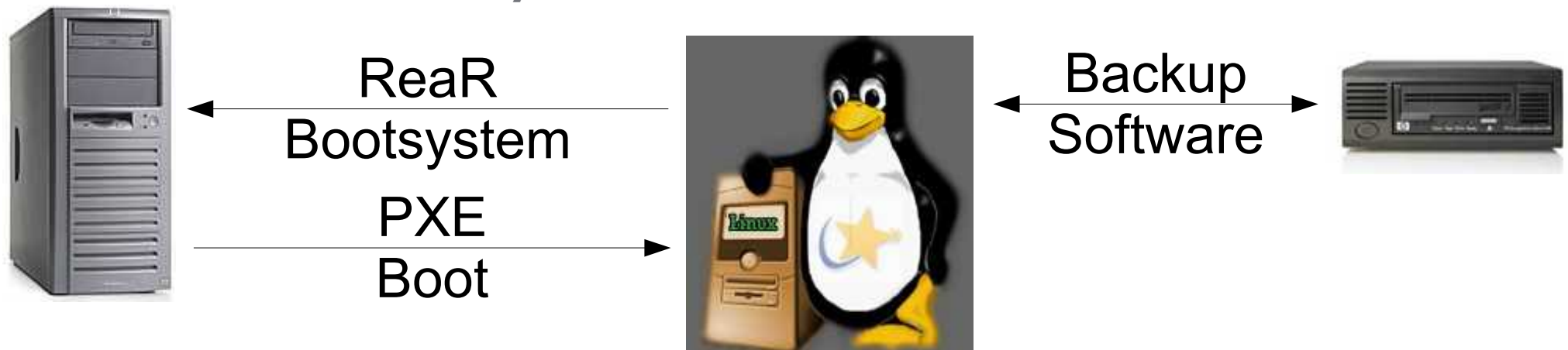
Relax & Recover – Backup-Software

- **Bereits unterstützte Backup-Software**
 - **Qnetix Galaxy**
 - **IBM Tivoli Storage Manager**
 - **Rsync**
 - **TAR Archive auf NFS/CIFS Freigabe**
- **Transparente Integration**
- **Niedriger Umsetzungsaufwand (ca. 2-3 Tage)**
- **Problemlos auch für weitere Backup-Software möglich**

Relax & Recover – Netzwerkintegration

Netzwerk Disaster Recovery Lösung

- Backup-Software – Dateisicherung
- ReaR – Systemumgebung
- Boot von ReaR per PXE aus dem Netz:
Keine Medien bei der Wiederherstellung nötig
- Automatische Installation eines Ausweichrechenzentrums von einem Recoveryserver



Relax & Recover – Neu in Version 1.6

- Bugfixes (bonding, localboot, nfs, Paketabhängigkeiten ...)
- Erste Gehversuche auf Ubuntu 7.10 und Debian 4
- Erste Denkversuche auf ia64 (RHEL)
- Verbesserte TSM Unterstützung
- Verbesserte tar Backups
- Verbesserungen im DR Modul (extra devices ...)
- mkdeb erstellt DEB Pakete
- Mehr Fehler werden bemerkt und gemeldet
- Neue Versionierung:
 - Gerade Zahlen – stable: 1.6, 1.8, 1.10 usw., 2.0
 - Ungerade Zahlen – unstable: 1.5, 1.7, 1.9 usw., 2.1

Relax & Recover – Entwicklung

Open Source Entwicklungsmodell

- Patche einschicken
- Sponsoring

Modulares Design

- ReaR ist ein Framework, um mit vielen kleinen Shellskripte einen großen Effekt zu erreichen
- Maximale Wiederverwendbarkeit von Code (Symlinks)
- Einfache Entwicklung und Debugging
- Wenig Interferenzen durch „Sonderlösungen“

Dokumentation auf Homepage

- Hierarchische Struktur
- Verweise in den Quellcode

Relax & Recover – Konfiguration

- Parametrisierung nach Betriebssystem, Architektur usw.
- Einbindung von Konfigurationsdateien (in /etc/rear):

System definition:

```
ARCH = Linux-i386
OS = GNU/Linux
OS_VENDOR = Ubuntu
OS_VENDOR_ARCH = Ubuntu/i386
OS_VENDOR_VERSION = Ubuntu/7.10
```

Configuration tree:

```
Linux-i386.conf : OK
GNU/Linux.conf : OK
Ubuntu.conf : missing/empty
Ubuntu/i386.conf : missing/empty
Ubuntu/7.10.conf : OK
site.conf : OK
local.conf : OK
```

Relax & Recover – Aufruf

```
rear [Options] <command> [command options ...]
```

```
Relax & Recover Version 1.6 / 2007-12-05
```

```
Build: ca11921a633b566ef54031e33d755bf5
```

```
Copyright (C) 2006-2007
```

```
    Schlomo Schapiro, probusiness Berlin AG
```

```
    Gratien D'haese, IT3 Consultants
```

```
Relax & Recover comes with ABSOLUTELY NO WARRANTY; for details
```

```
see the GNU General Public License at http://www.gnu.org/licenses/gpl.html
```

Available Options:

```
-V          version information
-d          debug mode
-D          debugscript mode
-S          Step-by-step mode
-s          Simulation mode (shows the scripts included)
```

List of commands:

```
dump        Dump configuration and system information
help        print out usage
mkbackup    Create rescue media and backup system.
mkdist      Create distribution tar archive with this rear version
mkrescue    Create rescue media only
recover     Recover the system
```

Relax & Recover – Beispiel

```
# cat /etc/rear/local.conf
OUTPUT=ISO
BACKUP=NETFS
NETFS_URL=nfs://lucky/media/scratch/backup
MODULES_LOAD=( vmxnet )

# rear mkbakup
Relax & Recover Version 1.6 / 2007-12-05
The preparation phase OK
Physical devices that will be recovered:
    /dev/hdd /dev/sda /dev/sdb /dev/sdc /dev/sdd /dev/sde
Creating root FS layout OK
Copy files and directories OK
Copy program files & libraries OK
Copy kernel modules OK
Create initramfs OK
Creating archive 'nfs://lucky/media/scratch/backup/rear/backup.tar.gz'
Transferred 264 MB in 140 seconds [1935 KB/sec]
Making ISO image OK
Wrote ISO Image /tmp/ReaR.iso (12M)
Copying resulting files to network location OK
The cleanup phase OK
Finished in 143 seconds.
```

Beispiel – Festplattenkonfiguration

```
# df -h
Filesystem                Size      Used Avail Use% Mounted on
/dev/sda2                  895M      773M   122M   87% /
udev                      126M      180K   126M    1% /dev
/dev/mapper/vg1-lv1       194M      4.1M   180M    3% /media/vg1-lv1
/dev/mapper/vg2-lv1       194M      4.1M   180M    3% /media/vg2-lv1
/dev/mapper/vg3-lv1       194M      4.1M   180M    3% /media/vg3-lv1
/dev/hdd2                  144M      133M    12M   92% /media/hdd2
/dev/sdb4                  251M      8.1M   230M    4% /media/sdb3
/dev/sdc4                  251M      8.1M   230M    4% /media/sdc3
/dev/hdd5                  187M      148K   187M    1% /media/xfsl
/dev/hdd6                   95M      148K    95M    1% /media/jfsl
/dev/mapper/vg4-lv1       194M      4.1M   180M    3% /media/vg4-lv1
/dev/sde                   199M      4.1M   185M    3% /media/sde
/dev/md1                   274M      8.1M   252M    4% /media/md1
```

```
# pvs
PV          VG      Fmt  Attr  PSize   PFree
/dev/hdd1   vg2     lvm2 a-    476.00M 276.00M
/dev/md0    vg1     lvm2 a-    564.00M 364.00M
/dev/sdb3   vg3     lvm2 a-    192.00M 184.00M
/dev/sdc3   vg3     lvm2 a-    192.00M    0
/dev/sdd    vg4     lvm2 a-    204.00M  4.00M
```

Beispiel – ReaR Wiederherstellung

```
# rear recover
Relax & Recover Version 1.6 / 2007-12-05
Backup archive size is 180M
Initializing physical devices OK
Creating the LVM2 devices OK
Creating file systems OK
Recreated this filesystem layout:
Filesystem          Size  Used Avail Use% Mounted on
/dev/mapper/rear--ubuntu-root
                    3.5G   72M  3.3G   3% /mnt/local
/dev/sda1            236M   6.1M  218M   3% /mnt/local/boot
Restoring from 'nfs://lucky/media/scratch/backup/rear-ubuntu/backup.tar.gz' OK
Installing boot loader (I hope you used grub and it works ...)
Creating swap files and partitions OK
Finished recovering your system
```

You can explore it under /mnt/local

Thank you for using Relax & Recover Version 1.6

Finished in 200 seconds.

Agenda

- | Problemstellung
- | Disaster Recovery Verfahren
- | Linux & Disaster Recovery
- | Lösungen - Relax & Recover
- | **Enterprise Secure Disaster Recovery**
- | Live Demo & Feedback

Enterprise DR – Anforderungen

- **Standardisierung**
- **Skalierung**
- **Automatisierung**
- **Integration in vorhandene Systemumgebung**
- **Sicherheit**
- **Abdeckung aller benutzten Systeme**
- **Wartung und Support und Schulungen**
- **Generallizenz (site license)**

Enterprise DR – Relax & Recover

- **Standardisierung von zentralen Konfigurationsteilen:**
 - `site.conf`
- **Skalierung & Automatisierung**
 - „rear mkrescue“ nicht interaktiv, auch als cron job
 - Automatische Weiterverarbeitung der Bootumgebung einfach
 - Sicherung der Bootumgebung durch Backupsoftware
 - Netzwerkboot – extreme Skalierung möglich
- **Integration in Systemumgebung**
 - Unterstützung interner und externer Backupmethoden
 - Email

Enterprise DR – Relax & Recover

■ Sicherheit

- Keine geheimen Daten in Bootumgebung
- Sicherer Export der Bootumgebung per Email möglich
- Remotezugriff auf Rescuesystem nur per SSH Schlüssel

■ Abdeckung von Systemen

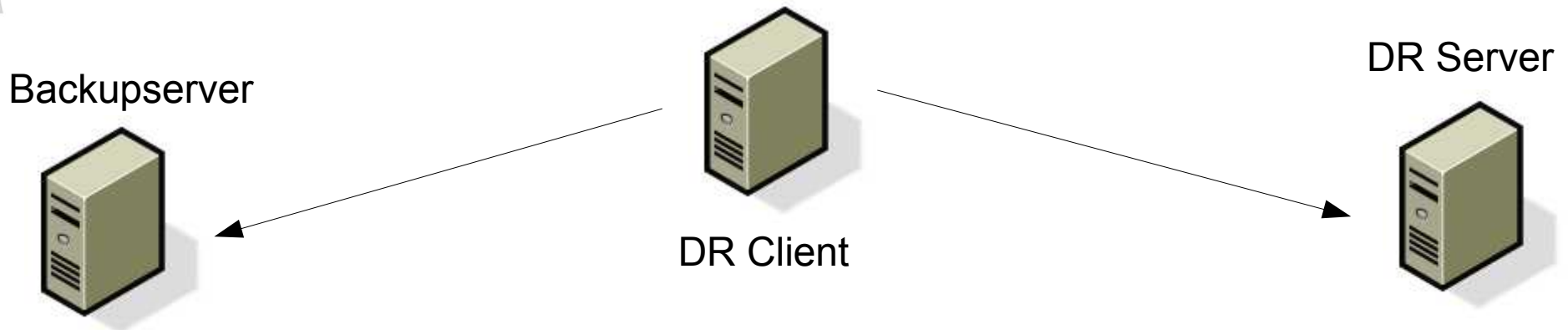
- i386 & x86_64 stabil
- Enterprise Linux stabil (Red Hat, Novell, Ubuntu)
- Gentoo, Debian, andere Linux Distros „funktionieren auch“

■ Wartung und Support und Schulungen

- ... bieten wir gerne an

■ Generallizenz verschenken wir großzügig :-)

Sicherheitsaspekte beim DR



Transfer der Backupdaten

- Backup-SW sicher ?
- Unsicher:
 - NFS
- Sicher
 - CIFS
 - SSH
 - RSYNC (über SSH)

Transfer der Bootumgebung

- Unsicher:
 - NFS
 - CIFS
 - SSH
 - RCP
- Manipulationssicher:
 - SMTP

Enterprise Linux Disaster Recovery

- **Linux – Einfaches Disaster Recovery**
- **Integration DR – Backupsoftware**
- **Automatisches Erstellen der DR Information**
- **Netzwerkboot in das DR System**
- **DR ist integraler Teil der Infrastruktur**
- **Skaliert problemlos auch für große Strukturen**
- **DR auch für Clients interessant**

Open Source & Business

- **Lizenzfreie Software**
- **Investition in Open Source ist wirtschaftlicher als Lizenzen kaufen und „abnutzen“ !**
- **Support & Entwicklung durch probusiness**
- **Open Source Sponsoring:**
 - **OpenVPN Gateway Builder**
 - **Relax & Recover (Initiatoren & Hauptentwickler)**
 - **mkcdrec 0.8.6ff (TSM, Networker, Debian)**
 - **nagiosadmin (GUI für Nagios)**
- **Schnelle Reaktion durch persönlichen Kontakt**
- **What You Get Is What You Wanted**
- **Bisher ausschliesslich positive Erfahrungen**

Agenda

- ! Problemstellung
- ! Disaster Recovery Verfahren
- ! Linux & Disaster Recovery
- ! Lösungen - Relax & Recover
- ! Enterprise Secure Disaster Recovery
- ! **Live Demo & Feedback**

Linux Disaster Recovery – Live Demo

Fragen & Antworten ...

Demo (~ 10 min):

- SLES 9
- ReaR Backup & Boot-CD erstellen
- DAU löscht System
- Booten von ReaR-CD
- Wiederherstellung
- Alles wird gut :-)



Starting

Press F2 to enter SETUP, F12 for Network Boot, ESC for Boot Menu

Ein durchdachtes Linux Disaster Recovery Konzept lässt den Admin sicher und beruhigt zu Hause schlafen ...



Thanks You ! Questions & Answers



Schlomo Schapiro
pro|business Berlin AG
Potsdamer Platz 11
10785 Berlin
Telefon 030 / 25 93 78-23
Telefax 030 / 25 93 78-22

pro|business
Berlin AG

www.probusiness.de

sschapiro@probusiness.de



redhat.
CERTIFIED
ENGINEER

Kontakt

pro | business
Berlin AG

Potsdamer Platz 11
D-10785 **Berlin**
Tel.: 0 30/25 93 78-0
Fax: 0 30/25 93 78-44

pro | business
Berlin AG

Freibergerstr. 39
D-01067 **Dresden**
Tel.: 03 51/6 46 30-13
Fax: 03 51/6 46 30-11

pro | business
AG

Expo Plaza 1
D-30539 **Hannover**
Tel.: 05 11/6 00 66-0
Fax: 05 11/6 00 66-155

pro | business
Hamburg AG

Elbberg 6b
D-22767 **Hamburg**
Tel.: 0 40/18 88 28-0
Fax: 0 40/18 88 28-28

pro | business
SI AG

Otto-Volger-Straße 19
D-65843 **Sulzbach**
Tel.: 0 61 96/5 61 42-10
Fax: 0 61 96/5 61 42-11

pro | business
SI AG

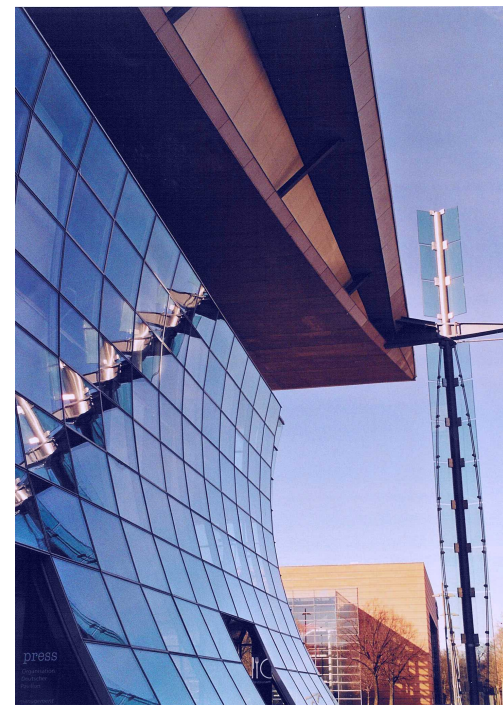
Max-Eyth-Straße 35
D-71088 **Holzgerlingen**
Tel.: 0 70 31/4 63 83-65
Fax: 0 70 31/4 63 83-66

pro | business
IT AG

Stadttor 1
D-40219 **Düsseldorf**
Tel.: 02 11/38 54 66-0
Fax: 02 11/38 54 66-99

pro | business
München AG

Graf-zu-Castell-Straße 1
D-81829 **München**
Tel.: 0 89/99 22 95-0
Fax: 0 89/99 22 95-11



info@probusiness.de
www.probusiness.de