XnetSolutions

SX-GATE

Software Update
Release Note

Version: 7.0-2-6

Inhaltsverzeichnis

Teil I Wichtige Informationen ... 4

1 Technische Unterstützung ... 4

2 Vorbereitung ... 4

3 Installation ... 4

Teil II Änderungen in dieser Software-Version ... 7

1 Sicherheitskritisch ... 8

Aktualisierung des Linux-Kernels und der Systembibliothek glibc ... 8

RAR-Entpacker ... 8

2 Bugfix ... 8

OpenVPN ... 8

E-Mail Dateianhangsfilter ... 8

SPAM-Ordner E-Mail-Report ... 8

3 Neu ... 8

Reverse-Proxy-Option für Quarantänebereich des Dateianhangsfilters ... 8

Monitoring für SSH-TCP-Forwarding ... 8

Teil III Änderungen in vorherigen Versionen ... 9

1 Version 7.0-2-5 ... 9

Sicherheitskritisch ... 9

Windows-Freigaben ... 9

Bugfix ... 9

NTLM-Authentifzierung und Mitgliedschaft in der Windows-Domäne ... 9

2 Version 7.0-2-4 ... 10

Sicherheitskritisch ... 10

IPSec-Server ... 10

Intrusion-Prevention und F-Secure Antivirus ... 10

Update ... 10

Aktualisierung des Linux-Kernel ... 10

3 Version 7.0-2-3 ... 11

Sicherheitskritisch ... 11

Intrusion-Detection / -Prevention ... 11

IPsec CRL ... 11

Bugfix ... 11

Autostart des Dienstes "weitere Server" ... 11

Webmail über Reverse-Proxy ... 11

Firewall-Regeln mit vielen Adressen ... 11

4 Version 7.0-2-2 ... 12

Sicherheitskritisch ... 12

Web-Proxy ... 12

Filterung von eingehenden E-Mails mit Absenderadresse aus der eigenen Domain ... 12

Windows-Dienste ... 12

Neue Funktionen ... 13

Protokollierung auf Syslog-Server ... 13

Eingabe von IP-Bereichen ... 13

Bugfix ... 14

Cluster mit Fallback ... 14
Anzeige von Dateianhängen in der E-Mail Quarantäne ... 14
Anzeige der Schnittstellen-Tabelle ... 14
5 Version 7.0-2-1 ... 15
Neue Funktionen ... **15**
Abweisen von E-Mails mit unerwünschten Dateianhängen ... 15
Bugfix ... **16**
Import-Funktion für Konfigurationstabellen ... 16
DSL-Einwahl nach Neustart ... 16
Backup auf NetAPP Windows-Freigabe ... 16
Speicherleck im Reverse-Proxy ... 16

1 Wichtige Informationen

Die in dieser Release Note enthaltenen Informationen beruhen auf sorgfältiger Recherche. Dennoch läßt es sich nicht ausschließen, dass eine Information im Einzelfall unzutreffend ist. Wir bitten daher um Ihr Verständnis, wenn wir keine Gewähr für die Richtigkeit der Informationen übernehmen und jede Haftung ausschließen. Sollten Sie feststellen, dass eine Information unzutreffend ist, bitten wir um Ihre Rückmeldung.

Richten Sie Ihre Rückmeldung bitte an die folgende E-Mail Adresse: support@xnetsolutions.de

1.1 Technische Unterstützung

Um technische Unterstützung bei der Durchführung des Software-Updates zu erhalten, können Sie unseren technischen Support via Telefon oder E-Mail erreichen. Wenn Sie den technischen Support kontaktieren, halten Sie bitte folgende Informationen bereit:

- momentan installierte SX-GATE Software-Version
- Geräte-ID
- SX-GATE Support-IP-Adresse

Diese Informationen können Sie über die Startseite auslesen.

So erreichen Sie den technischen Support:

Rufnummer:	+49 (0) 7032-95596-21
E-Mail:	support@xnetsolutions.de

1.2 Vorbereitung

Das Update der Systemsoftware erfolgt mit einer Update-Datei, um alle notwendigen Komponenten und Subsysteme intelligent zu aktualisieren. Die aktuelle Update-Datei enthält dabei alle vorherigen Updates seit dem letzten Update auf eine Hauptversion. Die Updates sind immer in der Reihenfolge der Versionsnummerierung zu installieren.

Hinweis:

Die Folge eines unterbrochenen Update-Vorgangs könnte sein, dass Ihr SX-GATE nicht mehrt bootet. Schalten Sie das SX-GATE deshalb nicht aus oder führen einen manuellen Neustart durch, während das Update durchgeführt wird. Sollte ein Neustart notwendig sein, wird dies durch das Update automatisch durchgeführt.

1.3 Installation

Bitte beachten Sie, dass Ihr SX-GATE die erforderlichen Voraussetzungen erfüllen muss, bevor Sie dieses Software-Update Installieren.

- **Arbeitsspeicher mindestens 2048 MB (2 GB) - optimal mindestens 4096 MB (4 GB)**

Sie können die aktuelle Speicherbestückung in der Konfigurationsoberfläche **auf der Startseite** einsehen. Für alle Fragen bzgl. des Software-Updates wenden Sie sich bitte an den technischen Support.

Gehen Sie folgendermaßen vor, um ein Software-Update durchzuführen:

Hinweis:

Erstellen Sie bitte vor dem durchführen des Software-Updates ein System-Backup, ein Benutzer-Backup und ein E-Mail-Backup.

Für das Durchführen eines Software-Updates haben Sie die folgenden Möglichkeiten:

- **Automatisches Software-Update über die SX-GATE Konfigurationsoberfläche**

Führen Sie über das Menü **»System → Update«** ein interaktives Software-Update durch. Wählen Sie dazu die Option **»interaktiv (empfohlen)«** und folgen Sie den Anweisungen auf dem Bildschirm. Wählen Sie im folgenden die Schaltfläche **»Weiter«**, um das Update automatisch zu installieren. Über das Fortschreiten des Software-Updates und einen bei Bedarf erforderlichen Reboot des SX-GATE werden Sie im interaktiven Update-Log informiert.

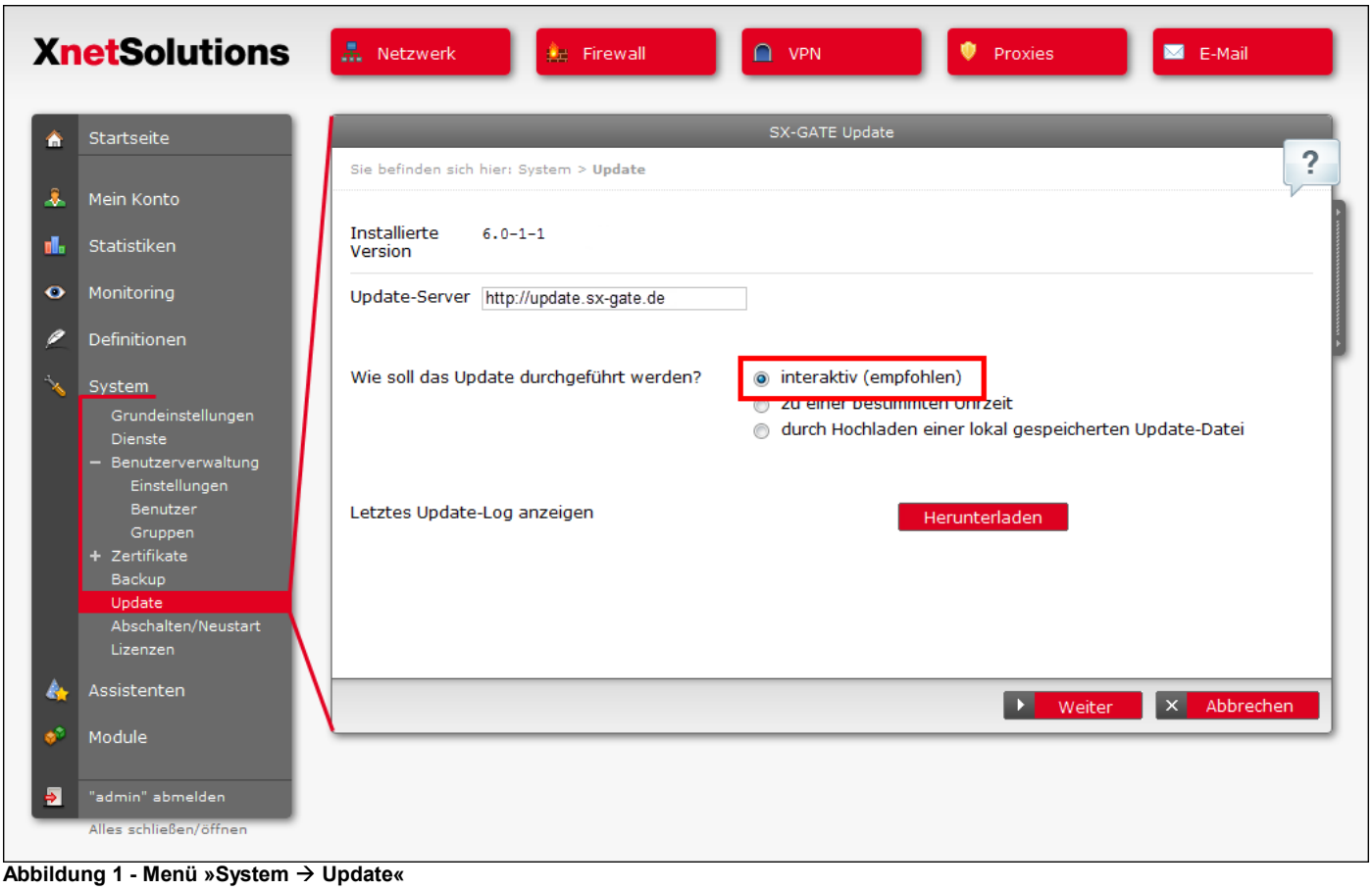

Abbildung 1 - Menü »System → Update«

- **Manuelles Software-Update**

Bevor Sie das Software-Update durchführen können ist es erforderlich, dass Sie das benötigte Software-Update Version 7.0-2-6 von der SX-GATE Update-Webseite herunterladen.

Die Update-Webseite erreichen Sie unter http://www.xnetsolutions.de → Menü **»Support -> Software Updates«**.

Führen Sie über das Menü **»System → Update«** ein manuelles Software- Update durch. Wählen Sie dazu die Option »durch Hochladen einer lokal gespeicherten Update-Datei« und folgenden Sie den Anweisungen auf dem Bildschirm.

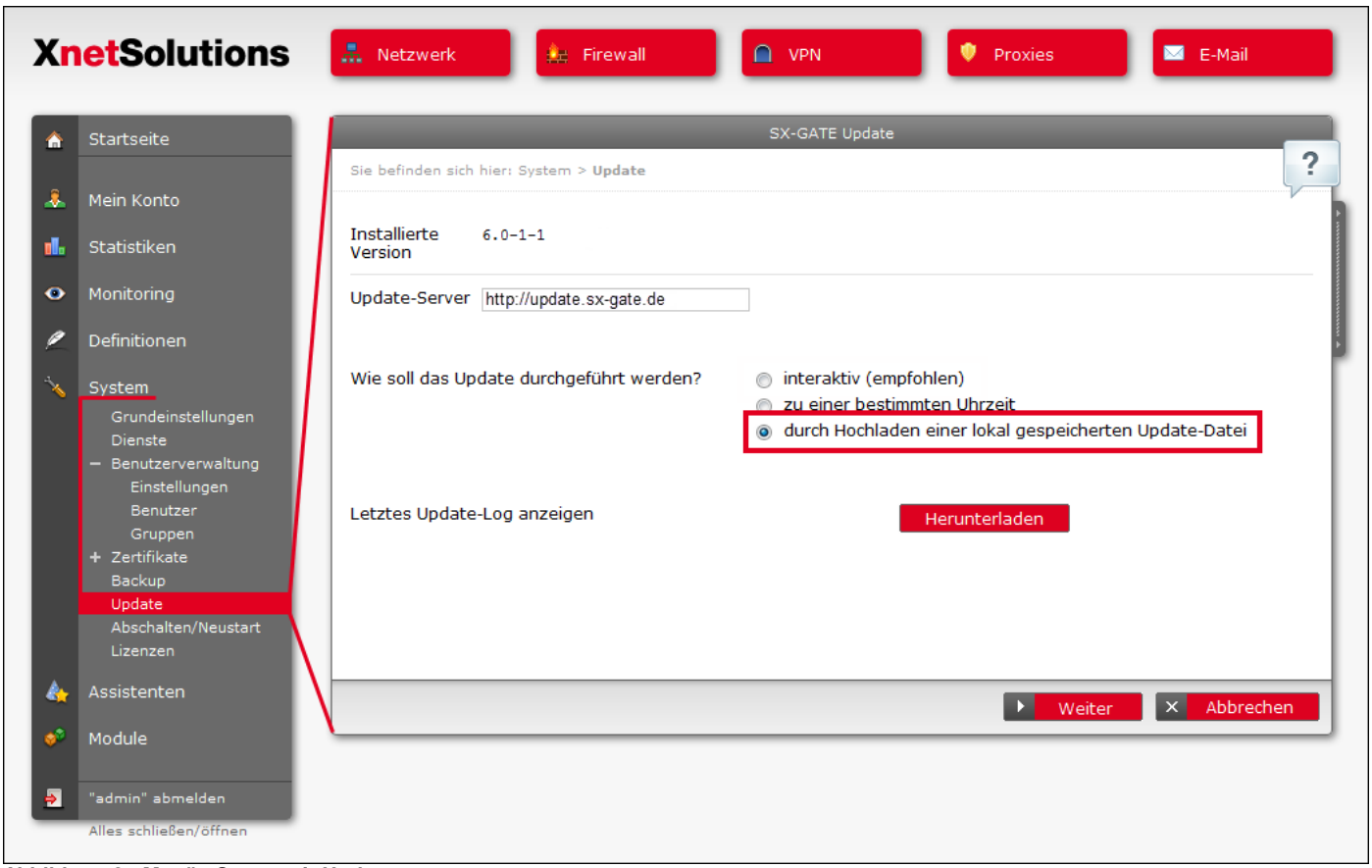

Abbildung 2 - Menü »System → Update«

Wichtig:

Der Update-Vorgang kann, je nach Größe des Updates und Leistungsfähigkeit des SX-GATE, einige Zeit in Anspruch nehmen.

2 Änderungen in dieser Software-Version

Neustart erforderlich

Nach dem Update führt das System automatisch einen oder mehrere Neustarts durch. Bitte führen Sie keinen manuellen Reboot durch! Das System kann dadurch funktionsunfähig werden.

2.1 Sicherheitskritisch

2.1.1 Aktualisierung des Linux-Kernels und der Systembibliothek glibc

Der Schutzmechanismus, mit dem die verschiedenen Speicherbereiche eines Programmes voneinander getrennt werden, lässt sich umgehen. Dies ermöglicht das Ausführen von eigenem Code oder das Ausweiten der Berechtigungen. Mit dem Update werden entsprechende Angriffe erschwert.

2.1.2 RAR-Entpacker

Mit Hilfe eines manipulierten RAR-Archives konnte ein Angreifer den im E-Mail-Virenscan eingesetzten RAR-Entpacker dazu bringen, im Rahmen der Berechtigungen eigenen Code auszuführen.

2.2 Bugfix

2.2.1 OpenVPN

Mit Hilfe von speziellen Datenpaketen konnte ein Angreifer den OpenVPN-Server zum Absturz bringen.

2.2.2 E-Mail Dateianhangsfilter

In der Administrationsoberfläche wurden Dateinamen mit ausländischen Zeichensätzen nicht korrekt angezeigt. In den Benachrichtigungsmails betraf dies neben dem Dateinamen auch den Betreff.

Um den Text der Benachrichtigungsmails zu vereinfachen, sind die Kopfzeilen der Original-Mail nicht mehr Bestandteil des Textes sondern werden als Anhang zugeordnet.

2.2.3 SPAM-Ordner E-Mail-Report

Im täglichen E-Mail-Report, der neue E-Mails im SPAM-Ordner auflistet, wurden Absendernamen und Betreff möglicherweise abgeschnitten. Bei Verwendung von ausländischen Zeichensätzen war die Anzeige nicht korrekt.

2.3 Neu

2.3.1 Reverse-Proxy-Option für Quarantänebereich des Dateianhangsfilters

Seit 7.0-2.0 kann der Administrator den Empfängern ermöglichen, unter bestimmten Voraussetzungen selbst auf gefilterte E-Mails oder Anhänge zugreifen zu können. Über einen neuen Schalter können diese Zugriffe nun auch im Reverse-Proxy freigegeben werden, falls von außen ein Zugriff auf die Quarantäne notwendig ist.

2.3.2 Monitoring für SSH-TCP-Forwarding

Auf einem neuen Reiter im Menü "Monitoring > Netzwerk > Status" werden jetzt Verbindungen mit dem SSH-TCP-Forwarder angezeigt.

3 Änderungen in vorherigen Versionen

3.1 Version 7.0-2-5

3.1.1 Sicherheitskritisch

3.1.1.1 Windows-Freigaben

Bei aktivierten Windows-Freigaben konnte ein Client eine Bibliothek hochladen und zur Ausführung bringen. Wenn der Dienst "Windows-Freigaben" nicht läuft, was der Grundeinstellung entspricht, ist das System nicht angreifbar.

3.1.2 Bugfix

3.1.2.1 NTLM-Authentifzierung und Mitgliedschaft in der Windows-Domäne

Bei NTLM basierter Proxy-Authentifizierung gab es mit der in Version 7.0-2.2 installierten neuen Samba-Version Probleme. Teils wurden nur viele Log-Meldungen erzeugt, auf anderen Sytemen musste hingegen der Dienst "Mitgliedschaft in Windows Domäne" regelmäßig neu gestartet werden.

Bitte erstellen Sie auf betroffenen Sytemen nach Abschluss des Updates im Menü "Module > Web-Proxy > Einstellungen" auf dem Reiter "NTLM-Anmeldung" das Domänen-Konto neu. Sollte bei "IP-Adresse des ActiveDirectory-Servers" anstatt einer IP der Name der Windows-Domäne konfiguriert sein, ändern Sie diesen bitte in die IP-Adresse eines Ihrer Domain-Controller ab.

3.2 Version 7.0-2-4

3.2.1 Sicherheitskritisch

3.2.1.1 IPSec-Server

Mit manipulierten Zertifikaten ließ sich der IPsec-Server zum Absturz bringen oder sogar Programmcode ausführen.

3.2.1.2 Intrusion-Prevention und F-Secure Antivirus

Seit 27.04.2017 wurden teilweise die Updates des F-Secure Virenscanners durch die Intrusion-Prevention blockiert. Systeme mit Pflegevertrag und automatischem Update der IDS/IPS-Signaturen haben am 28.04.2017 Signaturen erhalten, in denen das Problem behoben wurde. Für alle anderen Systeme werden die Signaturen mit diesem Update aktualisiert.

3.2.2 Update

3.2.2.1 Aktualisierung des Linux-Kernel

3.3 Version 7.0-2-3

3.3.1 Sicherheitskritisch

3.3.1.1 Intrusion-Detection / -Prevention

Mit manipulierten, fragmentierten Paketen konnten das IDS/IPS dazu gebracht werden, falsche Pakete bei der Reassemblierung des Datenstroms zu benutzen.

3.3.1.2 IPsec CRL

Zertifikatssperrlisten wurden vom IPsec-Server nicht geladen.

3.3.2 Bugfix

3.3.2.1 Autostart des Dienstes "weitere Server"

Auf dem Cluster Master und nach dem Einspielen eines System-Backups wurde das automatische Starten nach Reboots für "weitere Server" nicht aktiviert.

3.3.2.2 Webmail über Reverse-Proxy

Das Versenden von E-Mails im Webmailer schlug fehl, wenn der Zugriff über den Reverse-Proxy erfolgte.

3.3.2.3 Firewall-Regeln mit vielen Adressen

In Version 7.0-2.2 kam es beim Laden von Firewall-Regeln mit sehr vielen IP-Adressen zu einem Fehler. Die Regeln wurden daraufhin in einem zeitaufwändigen Verfahren schrittweise geladen, was zu temporären Zugriffsproblemen führen konnte.

3.4 Version 7.0-2-2

3.4.1 Sicherheitskritisch

3.4.1.1 Web-Proxy

Ein Fehler bei der Verarbeitung bedingter Anfragen ermöglichte es internen Angreifern, Zugriff auf die Sitzungen anderer Nutzer und damit potentiell auf vertrauliche Daten zu erlangen.

3.4.1.2 Filterung von eingehenden E-Mails mit Absenderadresse aus der eigenen Domain

Das Update behebt mehrere Möglichkeiten, diese in 7.0-1.1 neu eingeführten Filter zu umgehen. So wurden z.B. bislang nur die E-Mail-Adresse, nicht jedoch der Text-Teil des From-Headers untersucht und nur der erste From-Header geprüft.

Der Sender-Header wird ab sofort ebenfalls geprüft.

3.4.1.3 Windows-Dienste

Im Samba-Server wurden diverse Sicherheitsprobleme behoben, die nach unserer Auffassung jedoch nicht relevant sein dürften. Vorsichtshalber stellen wir dennoch ein Update zur Verfügung.

3.4.2 Neue Funktionen

3.4.2.1 Protokollierung auf Syslog-Server

Kostenpflichtige Funktion und nur auf Systemen mit Software-Updatevertrag verfügbar.

Der Inhalt der meisten Log-Dateien kann jetzt in Kopie auf einen Syslog-Server gesendet werden.

3.4.2.2 Eingabe von IP-Bereichen

In der Administrations-Oberfläche lassen sich nun an vielen Stellen neben einzelnen IP-Adressen und Netzwerken auch IP-Bereich wie z.B. "192.168.0.100-192.168.0.120" eingeben.

3.4.3 Bugfix

3.4.3.1 Cluster mit Fallback

Das Verhalten von Cluster-Master-Knoten, die zugleich über ein Fallback auf eine zweite Internet-Leitung verfügen, wurde überarbeitet. Wenn der Netzwerk-Link auf der primären Internet-Leitung verloren geht, erfolgt kein Wechsel auf den Backup-Knoten mehr. Stattdessen erfolgt ein Fallback auf die zweite Internet-Leitung.

3.4.3.2 Anzeige von Dateianhängen in der E-Mail Quarantäne

Vereinzelt wurden Anhänge nicht angezeigt, wenn deren Dateinamen auf bestimmte Weise kodiert waren.

3.4.3.3 Anzeige der Schnittstellen-Tabelle

Auf Hyper-V Systemen und manchen VDSL-Systemen wurde die Schnittstellen-Tabelle im Monitoring nicht angezeigt.

3.5 Version 7.0-2-1

3.5.1 Neue Funktionen

3.5.1.1 Abweisen von E-Mails mit unerwünschten Dateianhängen

Bei der Filterung von Dateianhängen steht nun eine zusätzliche Option zur Verfügung, bei der E-Mails mit unerwünschten Anhängen nicht unter Quarantäne gestellt, sondern gar nicht erst angenommen werden.
Diese Option ist nicht geeignet für Systeme, die eingehende E-Mails von einem POP- oder IMAP-Server abholen.

3.5.2 Bugfix

3.5.2.1 Import-Funktion für Konfigurationstabellen

Mit der neuen Import-Funktion aus 7.0-2.0 gab es noch ein paar Schwierigkeiten. Der Import funktioniert nun auch mit Chrome und der doppelte Import bei Verwendung des Internet-Explorers wurde behoben. Teilweise wurde die letzte Zeile des Imports fälschlicherweise als fehlerhaft beanstandet. Schließlich ist der Importvorgang jetzt toleranter bezüglich des Dateiformats, so dass sich die Import-Dateien nun mit den meisten Editoren bearbeiten lassen sollten.

3.5.2.2 DSL-Einwahl nach Neustart

An manchen DSL-Anschlüssen ging nach einem Neustart des Systems die DSL-Verbindung nicht online, wenn die DSL-Schnittstelle auch für IPsec-VPN genutzt wurde.

3.5.2.3 Backup auf NetAPP Windows-Freigabe

Das Backup schlug fehl, sofern in der NetAPP NTLMv2-Signed aktiviert ist.

3.5.2.4 Speicherleck im Reverse-Proxy

Testmöglichkeit

Überzeugen Sie sich zwei Wochen lang von unseren Produkten und Leistungen – ganz ohne Verpflichtung und völlig kostenfrei.

Kompetente Beratung

Oft ist die gewünschte Lösung einfacher und effizienter zu realisieren als erwartet.
Sprechen Sie mit uns über Ihre Anforderungen.
Gemeinsam finden wir den richtigen Weg.

Erreichbarkeit

Ihren persönlichen Ansprechpartner erreichen Sie ohne Umwege über seine direkte Durchwahl.

Vorabaustausch

Im Falle einer Störung senden wir Ihnen umgehend vorab ein vorinstalliertes und voll funktionstüchtiges Gerät zu.

Hotline

Bei allen technischen Fragen können Sie sich auf ein erfahrenes Support-Team verlassen.

XnetSolutions

Benzstraße 32, 71083 Herrenberg/Germany
Telefon +49 (0) 7032 955 96-0
Telefax +49 (0) 7032 955 96-25
info@xnetsolutions.de
www.xnetsolutions.de