TechNote

XCAPI und Firewalls

Stand: 14. Juni 2011







www.te-systems.de





Seite 2

Zusammenfassung

Alle aktuellen Windows-Versionen schützen die Netzwerkschnittstellen mit einer Firewall, die einerseits den Computer vor unberechtigten Zugriffen von außen schützen soll, und andererseits dem Benutzer eine gewisse Kontrolle darüber geben kann, welche Programme ihrerseits auf das Netzwerk zugreifen dürfen. Die VoIP-Controller der XCAPI sind davon nicht ausgenommen und sind daher ebenso eingeschränkt, vor allem, was den eingehenden Datenverkehr von der PBX angeht.

Die meisten XCAPI-Installationen sind in ein lokales Netzwerk integriert, welches über einen Router mit dem Internet verbunden ist. Diese Router übernehmen oftmals ebenso eine Firewall-Funktion und blockieren eingehende Nachrichten von den VoIP-Providern.

XCAPI und Firewalls

Damit die XCAPI problemlos mit der PBX oder dem VoIP-Provider kommunizieren kann, muss die Firewall überwunden werden. Die einfachste Methode besteht darin, die Firewall zu deaktivieren. Was im lokalen Netzwerk noch vertretbar ist, ist jedoch auf dem Router zum Internet unbedingt zu vermeiden. Daher gibt es in der XCAPI eine Möglichkeit, die Kommunikation auf eine bestimmte Gruppe von Ports festzulegen, die wiederum fest in der Firewall konfiguriert werden können.

Im Folgenden wird eine einfache und in der Praxis häufig verwendete Lösung beschrieben:

Firewall-Konfiguration: XCAPI - PBX







Die XCAPI ist auf einem Rechner im LAN installiert und muss lediglich mit einer PBX kommunizieren, die im gleichen Subnetz erreichbar ist. Wenn aus Sicht der Sicherheit nichts dagegen spricht, kann im Betriebssystem, auf dem die XCAPI läuft, die Firewall deaktiviert werden. Dadurch können alle TCP- und UDP-Pakete ungehindert zwischen der XCAPI und der PBX (und zu allen anderen Netzwerkgeräten) übertragen werden. In der Windows-Systemsteuerung können unter Windows-Firewall alle relevanten Einstellungen vorgenommen werden.

Möglichkeit 1: Firewall deaktivieren Häufig wird bei Problemen mit der Firewall nur die Einstellung Aktiv auf Inaktiv gesetzt.



Es sind jedoch auch die Einstellungen im Reiter Erweitert zu beachten, da diese im Regelfall noch immer die Kommunikation behindern. Aus diesem Grund muss in den Netzwerkverbindungseinstellungen des Erweitert-Reiters ebenso die Netzwerkschnittstelle (z. B. LAN-Verbindung 1, etc.) deaktiviert werden, die die XCAPI nutzen soll.

gemein Ausnahmen	Erweitert	
Netzwerkverbindungs	einstellungen	
Der Windows-Firewall Wählen Sie eine Verb Ausnahmen für eine ir	ist für die unten aufgelisteten Ve indung aus und klicken Sie auf ' ndividuelle Verbindung hinzuzufü	rbindungen aktiviert. 'Einstellungen'', um gen:
LAN-Verbindung		Einstellungen
J Sicherheitsprotokollier Zum Zweck der Probl Protokolldatei ersteller	ung embehandlung können Sie eine 1.	Einstellungen
ICMP		
Mit dem Internet Cont können Computer im 1 Statusinformationen g	ol Message-Protokoll (ICMP) Netzwerk Fehler- und emeinsam verwenden.	Einstellungen
Standardeinstellunger		
Klicken Sie auf "Wied Standardzustand für a festzulegen.	lerherstellen'', um den Ille Windows-Firewalleinstellung	en <u>W</u> iederherstellen



Erweiterte Firewall-Einstellungen beachten

Diese Einstellungen reichen nur auf Systemen bis Windows Server 2003, welcher nach einer Standard-Installation ausnahmsweise immer mit deaktivierter Firewall läuft und daher in den meisten Fällen keine Probleme bereitet.

Auch in Windows-Versionen ab Server 2008 gibt es die einfache Ansicht, in der die Firewall deaktiviert werden kann:

Windows-Firewall ein- oder	Windows-Firewall				
Programm durch die Windows-Firewall	Die Windows-Firewall kann dazu beitragen, Hacker oder böswillige Software daran zu hindern, Zugriff auf den Computer über das Internet bzw. ein Netzwerk zu erlangen.				
kommunizieren lassen	Wie kann eine Firewall zum Schutz des Computer beitragen				
	😵 Der Computer ist ungeschützt. Aktivieren Sie die Wi	ndows-Firewall.			
	Windows-Firewall ist aus.	Einstellungen ändern			
	Netzwerkstandort:	Öffentliches Netzwerk			
	Was sind Netzwerkstandorte?				
	Windows-Firewall verwendet nicht die empfohlenen Einstellungen zum Schutz dieses Computers. <u>Was</u> sind die empfohlenen Einstellungen?	<u>Einstellungen jetzt</u> <u>aktualisieren</u>			
	·				



Windows-Systeme ab Vista haben noch eine weitere Firewall-Konfiguration, die ebenfalls zu beachten ist:

In der Windows-Systemsteuerung befindet sich unter Verwaltung das Konfigurationsprogramm für die Windows-Firewall mit erweiterter Sicherheit.

Win	dows-Firewall mit erweiterter Sicherheit	
itei	Aktion Ansicht ?	
indo	ws-Firewall mit erweiterter Sicherheit - Lokaler Computer	
1	Die Windows-Firewall mit erweiterter Sicherheit bietet Netzwerksicherheit für Computer unter Windows.	
Übe	rsicht	•
Do	omänenprofil ist aktiv	
8	Die Windows-Firewall ist ausgeschaltet.	
Pri	ivates Profil	
8	Die Windows-Firewall ist ausgeschaltet.	
Öf	fentliches Profil ist aktiv	
8	Die Windows-Firewall ist ausgeschaltet.	
	Windows-Firewalleigenschaften	
-	Varhigel og en selskarde silvere sels	
	Verbindungssicherheitsregein	
Fir	ewallregeln anzeigen und erstellen	
Erst kön auto Verl zug duro	ellt Frewallregeln, um Verbindungen mit bestimmten Programmen oder Pots zuzulassen oder zu blockieren. Es nen außerdem Verbindungen nur dan zugelassen werden, wenn diese authentifizient sind oder von einem xisierten Benutzer, einer autorisierten Gruppe oder einem autorisierten Computer ausgehen. Engehende andungen werden standardmäßig nur dann nicht blockiert, wenn sie einer Regel entsprechen, durch die sie elassen werden. Augehende Verbindungen werden nur dann nicht zugelassen, wenn sie einer Regel entsprechen, ch die sie blockiert werden.	
Ð	Eingehende Regeln	
Ð	Ausgehende Regeln	
Ak	tuelle Firewallrichtlinie und IPsec-Richtlinie sowie Aktivität anzeigen	
Zeid		
füra	gt Informationen zu derzeit angewendeten Firewall- und Verbindungssicherheitsregeln sowie Sicherheitszuordnungen sktive Netzwerkverbindungen an.	
für a	gt Irformationen zu derzeit angewendeten Firewall- und Verbindungssicherheitsregeln sowie Sicherheitszuordnungen aktive Netzwerkverbindungen an. Deerwachung	



Hier wird über Profile geregelt, ob eine Verbindung genutzt werden darf, oder nicht abhängig davon, welches Netzwerkprofil für die Netzwerkkarte ausgewählt wurde, die die XCAPI nutzen soll. Hier können gezielt einzelne oder auch alle Profile deaktiviert werden, um eine einwandfreie Kommunikation zuzulassen.

- Status -	Erewallstatus:
-	Eingehende Verbindungen: Blockieren (Standard)
	Ausgehende Verbindungen: Zulassen (Standard)
	Geschützte Netzwerkverbindungen: Anpassen
Einstellu	Ingen
%	Geben Sie die Einstellungen an, die das Verhalten der Windows-Firewall steuern.
Protoko	lierung
	Geben Sie die Protokollierungs- einstellungen für die Problembehandlung

Firewall-Konfiguration: XCAPI - Router - VoIP-Provider

Die sichere, dafür mit etwas Konfigurationsaufwand verbundene Variante, kann sowohl im Intranet als auch für externe Verbindungen zu VoIP-Providern genutzt werden. Die Firewall des XCAPI-Rechners und/oder des Routers wird nur auf bestimmten Ports geöffnet, die die XCAPI für die Signalisierung und die RTP-Daten benötigt. Die für die VoIP-Kommunikation wichtigen Pakete können somit ungehindert zwischen XCAPI und Gegenstelle ausgetauscht werden, während die Firewall weiterhin das lokale Netzwerk und die restlichen Funktionen des Betriebssystems schützt.





Möglichkeit 2: Port-Bereich definieren

Während die VoIP-Signalisierung in den meisten Fällen über standardisierte Ports läuft (z.B. 5060 für SIP und 1720 für H.323), werden erst während des Rufaufbaus zwischen der XCAPI und dem Teilnehmer festgelegt, welche Ports für die RTP-Daten genutzt werden. Das stellt den Firewall-Administrator vor das nächste Problem, da unter diesen Voraussetzungen eigentlich alle Ports freigeschaltet werden müssten. Es ist sehr wahrscheinlich, dass die RTP-Daten bei jedem Ruf über einen anderen Port geleitet werden. Um dieser Problematik zu entgehen, kann in der XCAPI-Konfiguration ein Port-Bereich festgesetzt werden, den die XCAPI ausschließlich nutzt. Dementsprechend muss der Administrator lediglich diesen Port-Bereich in der Firewall freigeben, was das Sicherheitsrisiko einschränkt.

Um die XCAPI auf einen bestimmten Port-Bereich festzulegen, müssen Sie in der Experten-Ansicht den Konfigurationseintrag des VoIP-Controllers erweitern und unter Netzwerk das Menü Port-Reservierung öffnen.

🜠 XCAPI Konfiguration	
Datei Ansicht Hilfe	
0	
Datei Anscht Hilfe	TCP UDP Port-Bereich Ist hier ein Port-Bereich konfiguriert, so wird jeder Port für diesen Dienst jenem enthommen. Dadurch ist es möglich, eine Firewall so zu konfigurieren, dass alle Pakete für diesen Bereich durchgelassen werden. ✓ Port-Bereich für diesen Dienst aktivieren ✓ Port-Bereich in Windows XP Firewall eintragen Erster Port 38000 Anzahl 130



Hier können Sie für TCP und UDP zunächst den Port-Bereich für das entsprechende Protokoll aktivieren. Mit Hilfe der Schaltfläche Empfehlung wird automatisch ein Port-Bereich vorgeschlagen. Falls der Bereich nicht in Ihre Planung passt, können Sie auch anhand der Vorgaben einen eigenen Bereich festlegen. Hierbei ist zu beachten, dass der Bereich die gleiche Anzahl an Ports umfasst, wie der Vorschlag der XCAPI.

🕅 XCAPI Konfiguration	
Datei Ansicht Hilfe	
9 2 3	
Konfiguration	TCP UDP Port-Bereich Ist hier ein Port-Bereich konfiguriert, so wird jeder Port für diesen Dienst jenem entnommen. Dadurch ist es möglich, eine Firewall so zu konfigurieren, dass alle Pakete für diesen Bereich durchgelassen werden. Image: Port-Bereich für diesen Dienst aktivieren Image: Port-Bereich in Windows XP Firewall eintragen Erster Port 38000 Empfehlung Anzahl 240 Empfehlung
J	

Anpassung der Ports bei Erweiterung der XCAPI-Lizenzen

Die Anzahl der Ports wird aus verschiedenen Parametern der Controller-Konfiguration - wie etwa die Anzahl der zur Verfügung stehenden Kanäle - berechnet. Je mehr parallele Rufe der Controller bearbeiten kann, desto größer ist die Anzahl der benötigten RTP-Ports. Das sollten Sie auch beachten, wenn Sie nachträglich die Anzahl der Kanäle erhöhen. In diesem Fall muss die Anzahl der Ports in der Port-Reservierung ebenso erhöht werden.

Nachdem die XCAPI auf eine bestimmte Reihe von Ports festgelegt wurde, müssen diese Ports noch in der Firewall freigegeben werden. Wird die XCAPI auf Windows XP genutzt, kann das automatisch durch das Konfigurationsprogramm geschehen. Bei neueren Systemen kann es sein, dass Sie diese Ports manuell in die Firewall-Konfiguration eingeben müssen.



Definierten Port-Bereich in lokaler Firewall eintragen

Hier finden Sie eine Beispielkonfiguration einer SIP-Anbindung:

Wir haben einen SIP-Controller konfiguriert, der sich an einem SIP-Provider registrieren soll und 30 Kanäle parallel nutzen kann.

Z	
XCAPI Konfiguration	
Datei Ansicht Hilfe	
■ ⁻ ■ ●	
Konfiguration Information Information	Controller Features Bezeichnung Jedem Controller kann eine Bezeichnung zugewiesen werden, damit dieser später leichter erkannt werden kann. Dieses Feld dient lediglich der Identifikation im Konfigurationsprogramm und kann auch leer gelassen werden. Bezeichnung SIP-Provider Kanäle Dieser Controller stellt CAPI Anwendungen die hier eingestellte Zahl von Kanälen zur Verfügung. Die effektive Kanalanzahl wird durch die verfügbaren Lizenzen beeinflusst. Kanäle 30
	1

XCAPI Konfiguration	
Datei Ansicht Hilfe	
8 5 8 0	
Konfiguration Information Image: State of the sta	SIP Optionen Proxies Protokoll Timer Overlap Failover und überlauf Information Diese Informationen sind zum Herstellen einer Verbindung erforderlich und werden u.a. für die Autorisierung en einen Registrar und Proxy verwendet. Das "contact"-Engabefeld kann dazu benutzt werden, den Standardwert des "contact header" zu ersetzen. Benutzername Hans Mustermann Kennwort •••••• Angezeigter Name Organisation Contact •••••• SIP-Domäne und Registrar Die "Standard SIP-Domäne" wird an jede SIP-Adresse angehängt werden, bei der keine Domäne angeben ti.b. To-kolas SIP-Domäne" angehängt werden. Standard SIP-Domäne sp.myvoipaccount.net Lokale SIP-Domäne sp.myvoipaccount.net VID-Registrar verwenden sp.myvoipaccount.net



Der SIP-Provider erfordert den Einsatz eines STUN-Servers, da wir uns in einem lokalen Netzwerk befinden.

🛠 XCAPI Konfiguration	
Datei Ansicht Hilfe	
Konfiguration Konfiguration Charling CAPI 2.0 Optionen Fax Controller Fax Controller Fax Controller Fax Controller Fax Deprovider Fax Deprovider Fax Deprovider Fax Deprovider Fax Controller Fax Controller Fax Deprovider Fax Controller Fax Controller Fax Fax Fax Fax Fax Fax Fax Fa	Methode Statische IP-Adresse STUN NAT Traversal Ist diese Option aktiviert, so ist es möglich das System hinter einem NAT Router bzw. Gateway zu betreiben. Legen Sie fest, mit welcher Methode das NAT Traversal vorgenommen werden soll. IST UN

🜠 XCAPI Konfiguration		×
Datei Ansicht Hilfe		
9 2 8 0		
Konfiguration Configuration CAPI 2.0 Optionen Fax CAPI 2.0 Optionen CAPI 2.0 Optionen CAPI 2.0 Optionen CAPI 2.0 Optionen CAPI 2.0 Optionen CAPI 2.0 Optionen CAPI 2.0 CAPI 2.0	Methode Statische IP-Adresse STUN STUN Server Geben Sie die IP-Adresse oder den Hostnamen des STUN-Servers ein, der verwendet werden soll. Netzwerk-Adresse stun fwdnet.net Standard	
Port Reservierung Port Reservierung Port Reservierung Romannenfiter		



Die Empfehlung für die Port-Reservierung beginnt mit dem Wert 10000 als erster Port und einer Anzahl von 100 Ports für TCP und 180 Ports für UDP.

Zunächst sollte geprüft werden, ob TCP überhaupt benötigt wird, da SIP oftmals nur über UDP genutzt wird und RTP-Daten generell nur per UDP übertragen werden. In unserem Beispiel unterstützt unser SIP-Provider lediglich UDP, daher können wir darauf verzichten, die Ports für TCP freizuschalten.

Unter diesen Voraussetzungen ergeben sich folgende benötigte Ports:

- 5060/UDP für die SIP-Signalisierung.
- 3478/UDP für den STUN-Server.
- 10000-10179/UDP (insgesamt 180 Ports) für die Port-Reservierung.

Diese Ports müssen zunächst in der lokalen Firewall des XCAPI-Rechners freigeschaltet werden, damit die Pakete überhaupt bis zur XCAPI vordringen können. Weiterhin muss im Router, der das lokale Netzwerk mit dem Internet verbindet, eine Port-Weiterleitung für die einzelnen Ports auf die entsprechenden Zielports zur IP-Adresse der XCAPI eingerichtet werden.

🕷 Windows-Firewall mit erweiterter Siche	erheit							
Datei Aktion Ansicht ?								
Fingebende Regeln								1
Ausgehende Regeln	Name A	Profil	Aktiviert	Aktion	Programm	Lokale Adresse	Protokoll	Lokaler Port 🔺
Verbindungssicherheitsregeln	XCAPI-Controller 1, UDP Port 3478 (STUN-Server)	Alle	Ja	Zulassen	Beliebig	Beliebig	UDP	3478
🗉 🌉 Überwachung	XCAPI-Controller 1, UDP Port 5060 (SIP)	Alle	Ja	Zulassen	Beliebig	Beliebig	UDP	5060
	XCAPI-Controller 1, UDP Port 10000	Alle	Ja	Zulassen	Beliebig	Beliebig	UDP	10000
	XCAPI-Controller 1, UDP Port 10001	Alle	Ja	Zulassen	Beliebig	Beliebig	UDP	10001
	XCAPI-Controller 1, UDP Port 10002	Alle	Ja	Zulassen	Beliebig	Beliebig	UDP	10002
	XCAPI-Controller 1, UDP Port 10002	Alle	Ja	Zulassen	Beliebig	Beliebig	UDP	10002
	XCAPI-Controller 1, UDP Port 10003	Alle	Ja	Zulassen	Beliebig	Beliebig	UDP	10003
	XCAPI-Controller 1, UDP Port 10004	Alle	Ja	Zulassen	Beliebig	Beliebig	UDP	10004
	XCAPI-Controller 1, UDP Port 10005	Alle	Ja	Zulassen	Beliebig	Beliebig	UDP	10005
	XCAPI-Controller 1, UDP Port 10006	Alle	Ja	Zulassen	Beliebig	Beliebig	UDP	10006
	XCAPI-Controller 1, UDP Port 10007	Alle	Ja	Zulassen	Beliebig	Beliebig	UDP	10007
	XCAPI-Controller 1, UDP Port 10008	Alle	Ja	Zulassen	Beliebig	Beliebig	UDP	10008
	XCAPI-Controller 1, UDP Port 10009	Alle	Ja	Zulassen	Beliebig	Beliebig	UDP	10009
	XCAPI-Controller 1, UDP Port 10010	Alle	Ja	Zulassen	Beliebig	Beliebig	UDP	10010
	XCAPI-Controller 1, UDP Port 10011	Alle	Ja	Zulassen	Beliebig	Beliebig	UDP	10011
	XCAPI-Controller 1, UDP Port 10012	Alle	Ja	Zulassen	Beliebig	Beliebig	UDP	10012
	XCAPI-Controller 1, UDP Port 10013	Alle	Ja	Zulassen	Beliebig	Beliebig	UDP	10013
	XCAPI-Controller 1, UDP Port 10014	Alle	Ja	Zulassen	Beliebig	Beliebig	UDP	10014
	XCAPI-Controller 1, UDP Port 10015	Alle	Ja	Zulassen	Beliebig	Beliebig	UDP	10015
	XCAPI-Controller 1, UDP Port 10016	Alle	Ja	Zulassen	Beliebig	Beliebig	UDP	10016
	XCAPI-Controller 1, UDP Port 10017	Alle	Ja	Zulassen	Beliebig	Beliebig	UDP	10017
	XCAPI-Controller 1, UDP Port 10018	Alle	Ja	Zulassen	Beliebig	Beliebig	UDP	10018
	XCAPI-Controller 1, UDP Port 10019	Alle	Ja	Zulassen	Beliebig	Beliebig	UDP	10019
	XCAPI-Controller 1, UDP Port 10020	Alle	Ja	Zulassen	Beliebig	Beliebig	UDP	10020
	XCAPI-Controller 1, UDP Port 10021	Alle	Ja	Zulassen	Beliebig	Beliebig	UDP	10021
	XCAPI-Controller 1, UDP Port 10022	Alle	Ja	Zulassen	Beliebig	Beliebig	UDP	10022
	XCAPI-Controller 1, UDP Port 10023	Alle	Ja	Zulassen	Beliebig	Beliebig	UDP	10023
	XCAPI-Controller 1, UDP Port 10024	Alle	Ja	Zulassen	Beliebig	Beliebig	UDP	10024
	XCAPI-Controller 1, UDP Port 10025	Alle	Ja	Zulassen	Beliebig	Beliebig	UDP	10025
	XCAPI-Controller 1, UDP Port 10026	Alle	Ja	Zulassen	Beliebig	Beliebig	UDP	10026
	XCAPI-Controller 1, UDP Port 10027	Alle	Ja	Zulassen	Beliebig	Beliebig	UDP	10027
	XCAPI-Controller 1, UDP Port 10028	Alle	Ja	Zulassen	Beliebig	Beliebig	UDP	10028
	XCAPI-Controller 1, UDP Port 10029	Alle	Ja	Zulassen	Beliebia	Beliebia	UDP	10029
	XCAPI-Controller 1, UDP Port 10030	Alle	Ja	Zulassen	Beliebia	Beliebia	UDP	10030
	XCAPI-Controller 1, UDP Port 10031	Alle	Ja	Zulassen	Beliebia	Beliebia	UDP	10031
	XCAPI-Controller 1, UDP Port 10032	Alle	Ja	Zulassen	Beliebia	Beliebia	UDP	10032
	XCAPI-Controller 1, UDP Port 10033	Alle	Ja	Zulassen	Beliebia	Beliebia	UDP	10033
	XCAPI-Controller 1, UDP Port 10034	Alle	Ja	Zulassen	Beliebia	Beliebia	UDP	10034
	XCAPI-Controller 1, UDP Port 10035	Alle	Ja	Zulassen	Beliebia	Beliebia	UDP	10035
	XCAPI-Controller 1, UDP Port 10036	Alle	Ja	Zulassen	Beliebia	Beliebia	UDP	10036
I	1					,		Þ



Definierten Port-Bereich in globaler Firewall eintragen

Die XCAPI teilt dem SIP-Provider jetzt während des Rufaufbaus mit, dass die RTP-Daten an einen der 180 Ports zwischen 10000 und 10179 geschickt werden können. Der Router wird die RTP-Pakete entgegennehmen und an die XCAPI im lokalen Netzwerk weiterleiten.

Mit diesem Wissen können Firewall-bedingte Probleme auch wesentlich leichter diagnostiziert werden:

Wenn nur Port 5060 freigegeben wurde und somit die Signalisierung zwischen XCAPI und Provider funktioniert, kann es sein, dass bei einem ausgehenden Ruf von der XCAPI die Audiodaten nur einseitig hörbar sind. Die Daten von der XCAPI werden eventuell von der lokalen Firewall und von der im Router in Richtung Provider durchgelassen, aber die Richtung vom Provider zur XCAPI wird durch den Router geblockt. Wenn dieses Phänomen beobachtet wird, sollten Sie noch einmal die Konfiguration aller beteiligter Firewalls prüfen.





Seite 13

Haftungsausschluss

Copyright © 2011 TE-SYSTEMS GmbH

Alle Rechte vorbehalten

Kein Teil dieses Dokuments oder das Dokument als Ganzes dürfen ohne vorherige schriftliche Genehmigung von TE-SYSTEMS GmbH in irgendeiner Form reproduziert werden.

Die in diesem Dokument gemachten Angaben entsprechen dem Kenntnisstand zum Zeitpunkt der Erstellung. Die TE-SYSTEMS GmbH behält sich das Recht vor, Veränderungen ohne vorherige Ankündigung vorzunehmen.

Bei der Zusammenstellung von Texten und Abbildungen sowie bei der Erstellung der Software wurde mit größter Sorgfalt vorgegangen. Dennoch kann für die Richtigkeit, Aktualität und Vollständigkeit des Inhalts, eine Wirtschaftlichkeit oder die fehlerfreie Funktion von Software für einen bestimmten Zweck keinerlei Gewähr übernommen werden. Die TE-SYSTEMS GmbH schließt daher jegliche Haftung für Schäden aus, die direkt oder indirekt aus der Verwendung dieses Dokuments entstehen.

Marken

Alle verwendeten Namen von Produkten und Dienstleistungen sind Marken oder eingetragene Marken (auch ohne gesonderte Kennzeichnung) der jeweiligen privaten oder juristischen Personen und unterliegen als solche den gesetzlichen Bestimmungen.

Drittrechte

Third Party Disclaimer and Limitations

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

This product includes source code derived from the RSA Data Security, Inc. MD2, MD4 and MD5 Message Digest Algorithms.

This product includes source code derived from the RFC 4634 Secure Hash Algorithm software.

TE-SYSTEMS GmbH

Geschäftsführer Andreas Geiger Oliver Körber

> Anschrift Max-von-Laue-Weg 19 38448 Wolfsburg

Telefon 05363 8195-0 Fax 05363 8195-999 freecall 0800 8379783

E-Mail info@te-systems.de Internet www.te-systems.de www.xcapi.de