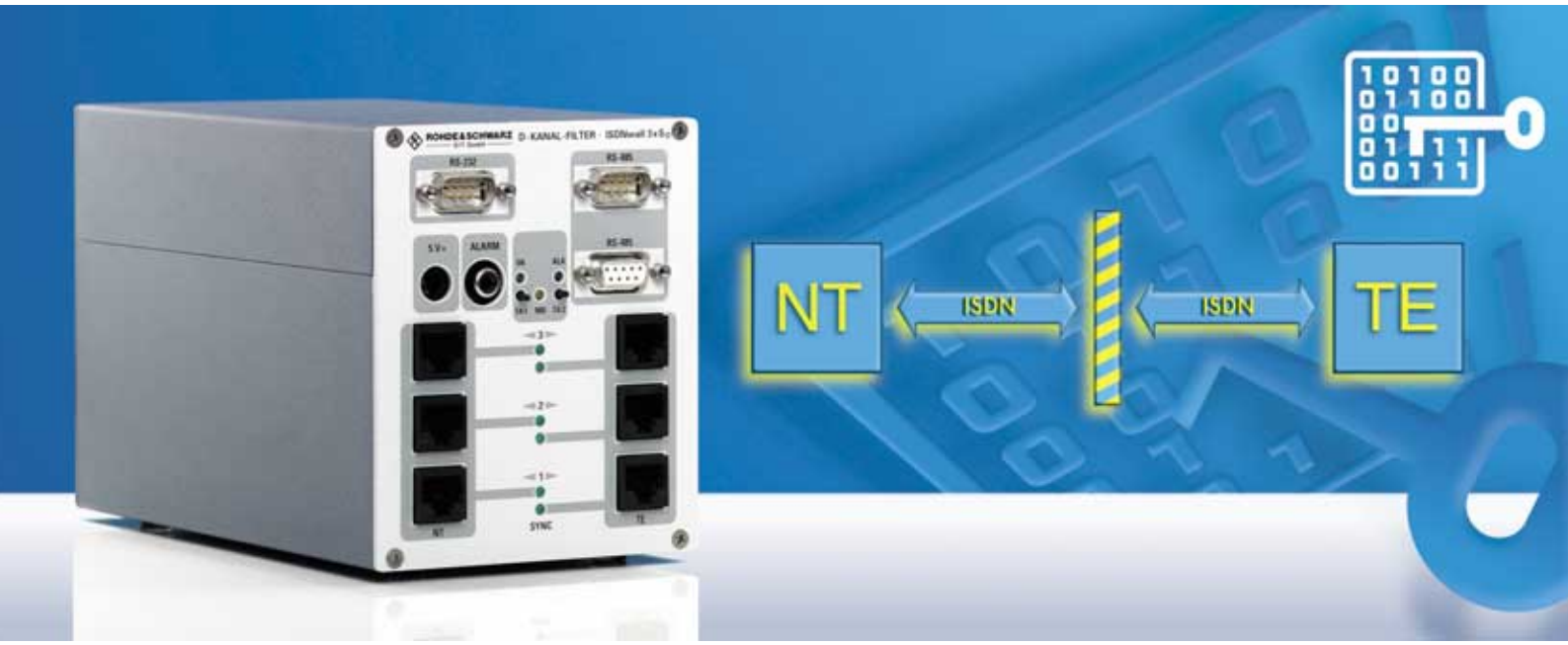


D-Kanal-Filter ISDNwall

Zur Absicherung digitaler TK-Anlagen gegen Manipulationen aus dem öffentlichen Netz

- Firewall zum ISDN-Netz
- Intrusion detection
- Für Anschluss S_0, $3xS_0$ und S_{2M}
- Alarmierung und Protokollierung bei Sicherheitsverstößen
- Hohe Sicherheitsstandards bei Administration und Revision
- Anpassbar an veränderte Bedrohungslagen

BSI Bundesamt für Sicherheit in der Informationstechnik

ROHDE&SCHWARZ

Problem

Die analoge Technik im Bereich privater Telekommunikationsanlagen (TK-Anlagen) ist rasant durch digitale Technik abgelöst worden. Besonders in Unternehmen und Behörden ist das Integrated Services Digital Network (ISDN) nicht mehr wegzudenken; zunehmend wird die gesamte Unternehmenskommunikation nach außen mit ISDN abgewickelt. Weitgehend unbemerkt drohen bei dieser Umstellung neue Gefahren für die TK-Anlagen der Unternehmen und Behörden. Während bei der Analogtechnik in erster Linie die physikalischen Komponenten des Systems (z.B. das Leitungsnetz) Ziele von Angriffen waren, rückt bei digitalen Systemen die logische Verwundbarkeit wie die Manipulation der TK-Anlage über deren eigene Programme oder Datenbanken in den Vordergrund.

Moderne digitale TK-Anlagen enthalten oft mehrere hundert Funktionen, von denen viele missbräuchlich verwendet werden können. So wird einerseits dem Benutzer derartiger Anlagen eine große Vielfalt nützlicher und sinnvoller Funktionen zur Verfügung gestellt, andererseits aber werden einem potentiellen Angreifer/Täter Missbrauchs- und Manipulationsmöglichkeiten geboten. Dabei werden die Benutzer solche Angriffe/Missbräuche in der Regel nicht feststellen können.

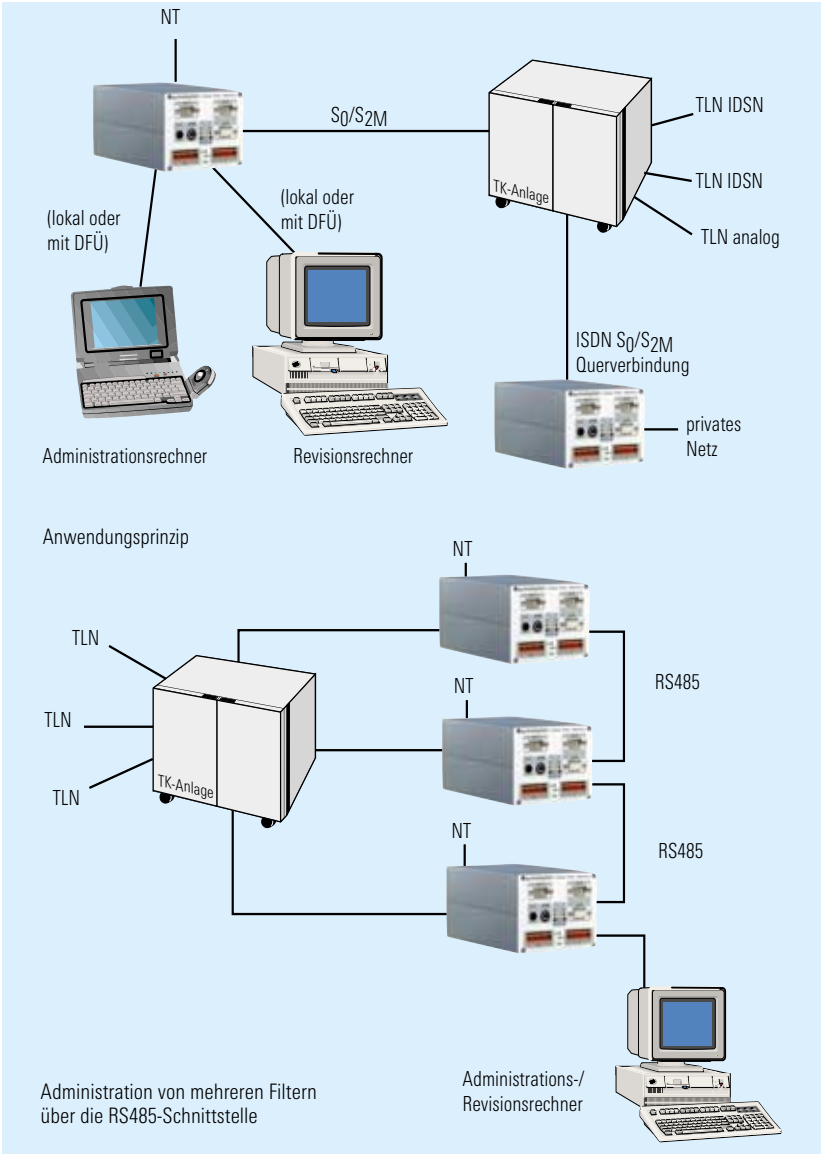
Hinzu kommt, dass die Anwender digitaler TK-Anlagen oft ihr System nicht selbst konfigurieren und administrieren. Damit ist es ihnen nicht möglich, sich einen exakten Überblick über die aktuelle Konfiguration der Anlage zu verschaffen.

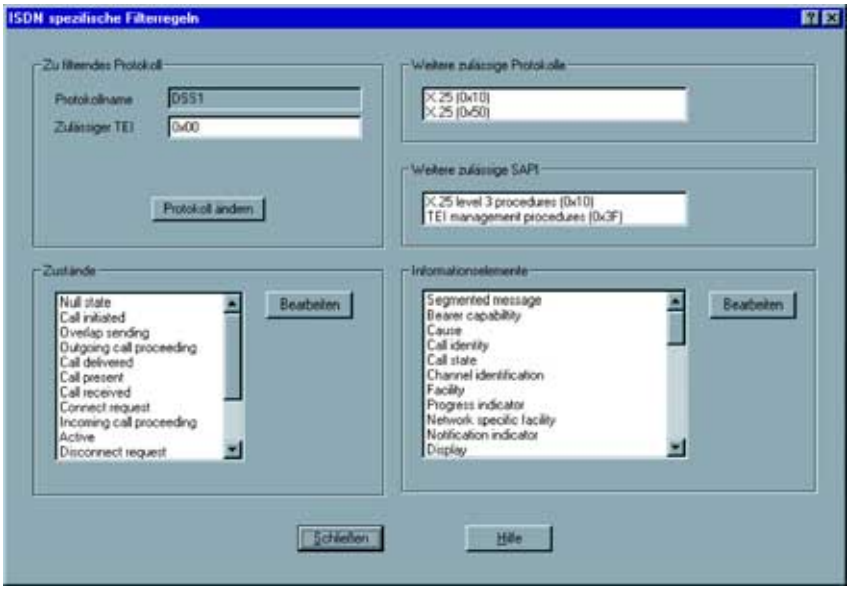
Die folgenden Beispiele zeigen, wie sich der Missbrauch solcher Möglichkeiten auswirken kann.

- Die Freisprecheinrichtung kann vom Apparat – unter Umständen auch aus dem öffentlichen Netz – heraus aktiviert werden und ermöglicht das Abhören des Raumes.
- Fernwartung wird zunehmend über spezielle Rufnummern realisiert. Zugehörige Passworte werden in der Praxis nur sehr selten gewechselt. So gelangt man leicht auf die Administratorebene und kann die Anlage umkonfigurieren.
- Durchwahl vom Amt ins Amt ermöglicht es, von einem externen Apparat auf Kosten des Eigentümers der TK-Anlage auch weltweit zu telefonieren.
- Verdeckte Informationsübertragung im D-Kanal ermöglicht das Aktivieren zuvor in die TK-Anlage eingeschleuster Programme (trojanische Pferde) mit dem Ziel, die Kontrolle an den Angreifer zu übergeben.

Ein wesentlicher Angriffspunkt ist dabei die „Offenheit" der Vermittlungstechnik über den D-Kanal des ISDN. Unter Voraussetzung von entsprechendem Know-how und geeigneter Technik können Elemente des Steuerprotokolls ausgenutzt werden, um Schäden in TK-Anlagen anzurichten (Aktivierung von Programmen in der TK-Anlage, Manipulation der internen Ablaufsteuerung der TK-Anlage, Zugang zur Administrationsebene).

Beispiele für Einbindung und Administration des D-Kanal-Filters

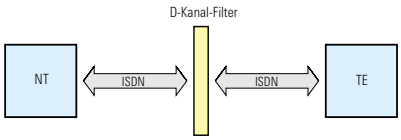




Dialogbox ISDN-spezifische Filterregeln

Lösung

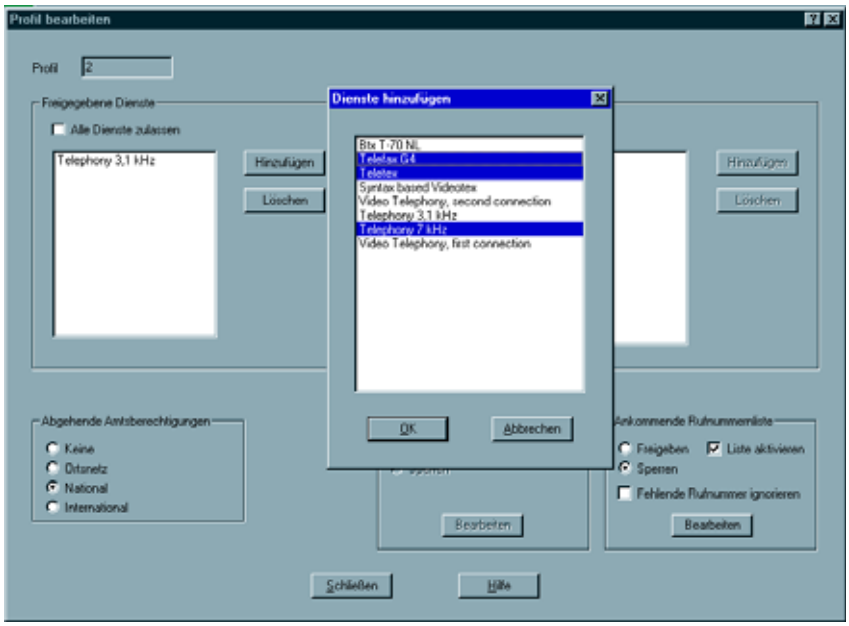
Ein Filter für den D-Kanal kann unerwünschte Steuerinformationen herausfiltern und damit verbundene Bedrohungen durch geeignete Reaktionen – so z.B. Abbruch der Verbindung – beseitigen.



Die Rohde & Schwarz SIT GmbH entwickelte im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik ein solches „D-Kanal-Filter zur Absicherung von digitalen TK-Anlagen" (ISDNwall) zur Abwehr von Manipulationsmöglichkeiten aus dem öffentlichen Netz.

ISDNwall schränkt Dienstmerkmale und Dienste für Rufnummern ankommender und ausgehender Verbindungen so ein, dass es normalerweise nicht zum Missbrauch von Diensten und Dienstmerkmalen oder zu Gefährdungen kommen kann. Verhindert werden soll das unberechtigte Nutzen von Diensten und Dienstmerkmalen sowie die gezielte Sabotage von außen. ISDNwall ist gegenüber dem ISDN-Netz eine Nachbildung der zu schützenden TK-Anlage. Die Nachbildung bezieht sich auf Rufnummern (Teilnehmer), Dienste (Sprache, Datenübertragung, Fax, Voice-Mail) und Dienstmerkmale sowie auf die Zuordnung von Diensten und Dienstmerkmalen zu den Rufnummern.

Das D-Kanal-Filter ISDNwall wird zwischen Amtsanschluss und TK-Anlage geschaltet. Bezüglich der Signalisierung im ISDN verhält sich das Filter zur Amtsleitung wie eine TK-Anlage (TE) und zur TK-Anlage wie ein Amtsanschluss (NT).



Dialogbox zur Einstellung von Teilnehmerprofilen

Durch den Funktionsumfang sind sowohl ISDN-Basisanschlüsse (S_0) als auch ISDN-Primärmultiplexanschlüsse (S_{2M}) für das Protokoll DSS1 abgedeckt. An weitere Protokolle kann ISDNwall optional angepasst werden.

Die B-Kanäle mit der Nutzinformation werden transparent durchgeschleift, es besteht jedoch zwischen NT- und TE-Seite des D-Kanal-Filters keine direkte physikalische Verbindung. Bei unbekannten, unvollständigen oder nicht erwarteten Protokollelementen oder -sequenzen reagiert ISDNwall konform zum DSS1-Protokoll. Versucht jemand unberechtigt Dienstmerkmale und Dienste zu nutzen, unterbindet ISDNwall dies durch einen Verbindungsabbau.
Das gleiche Verhalten gilt bei Verletzung ISDN-spezifischer Filterregeln. Solche Ereignisse werden bei ihrem Auftreten in einem internen Protokoll erfasst.

Sicherheitsverstöße lösen neben der Protokollierung einen optischen Alarm und einen akustischen Intervall-Alarm aus. Das optische Signal bleibt, bis es explizit vom Administrator zurückgesetzt wird.

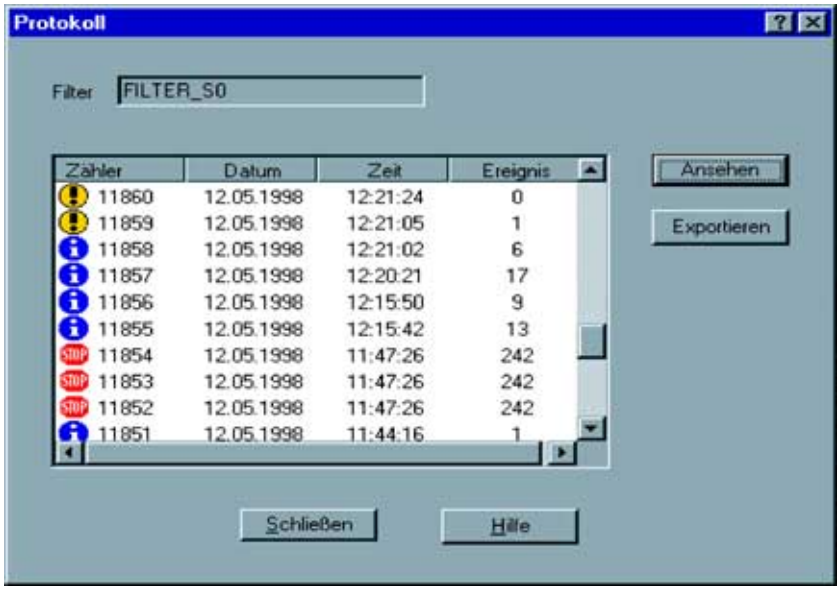
ISDNwall ist mit zwei seriellen Schnittstellen (RS-232-C, RS485) ausgestattet, die wahlweise zur lokalen Administration und Revision benutzt werden können. Ein zentrales Management zur Fernadministration, Fernrevision und Fernalarmierung ist als Option integrierbar. Sowohl Administration als auch Revision erfolgen über eine gesicherte und verschlüsselte Verbindung. Das dabei eingesetzte Protokoll erfüllt die Anforderungen an die Mechanismenstärke „hoch" (ITSEC).

Das D-Kanal-Filter ist in folgenden Varianten verfügbar:

- mit einer S_0-Schnittstelle für den Mehrgeräteanschluss
- mit einer S_0-Schnittstelle für den Anlagenanschluss
- mit 3 S_0-Schnittstellen für den Anlagenanschluss
- mit S_{2M}-Schnittstelle für den Anlagenanschluss (Primärmultiplexanschluss)

ISDNwall wird als externes Gerät geliefert. Zum Lieferumfang gehören Administrations- und Protokollierungs-Software, eine Basiskonfiguration des Filters (auf Wunsch auch kundenspezifisch) sowie Handbücher zu Installation und Betrieb.

Certified Quality System
ISO 9001
REG. NO CERT-01 100 025007



Protokollierte Ereignisse

Technische Daten

Rechnerteil	CPU 80486
ISDN-Eingänge/-Ausgänge	S_0-Geräte: 1 oder 3 Basisanschlüsse S_0 S_{2M}-Gerät: 1 Primärmultiplexanschluss S_{2M}
Serielle Schnittstellen	RS-232-C, RS485
ISDN-Protokolle	DSS1, Anpassung an weitere Protokolle möglich
Zulassungen	CE0681X
Sicherheitskriterien	Nach Maßgabe „E3/hoch" der ITSEC entwickelt und zur Zertifizierung eingereicht
Teilnehmerzahl	Filterparameter können für bis zu 9999 Teilnehmer (optional mehr) einer TK-Anlage in bis zu 256 Anwenderprofilen eingerichtet werden

Allgemeine Daten

Betriebstemperaturbereich	+5°C...+45°C
Stromversorgung	
Netzspannung	220 V...240 V + −10%, 47 Hz...53 Hz (12 VA)
Gleichspannung	5 V, 2 A
Potenzialfreier Ausgang	für Anschluss Alarmleitung
Abmessungen (B x H x T)	
S_0 und S_{2M}	105 mm x 85 mm x 205 mm
3x S_0	105 mm x 115 mm x 205 mm
Gewicht	
S_0 und S_{2M}	1,5 kg
3x S_0	2,0 kg

Bestellangaben

Bezeichnung	Bestellnummer
ISDNwall S_0	3534.3558
ISDNwall 3x S_0	3534.3858
ISDNwall S_{2M}	3534.3612
ISDNwall für Mehrgeräteanschluss	3534.3206

Lieferumfang

Filtereinheit
Netzteil mit Anschlusskabel, Kabel zum Anschluss an die RS-232-C-Schnittstelle
CD-ROM mit Administrations- und Revisionssoftware in deutsch und englisch,
Anwenderhandbuch, Installationsanleitung

Einsatzhinweis

Für Administration und Revision ist ein PC/Laptop mit Windows9x oder NT erforderlich.
Es wird der Anschluss des Filters an eine USV empfohlen.

ROHDE&SCHWARZ
ROHDE & SCHWARZ SIT GmbH · Agastr. 3 · 12489 Berlin
Tel. (030) 65884-223· Fax (030) 65884-184 · E-Mail: contact@sit.rohde-schwarz.com · www.sit.rohde-schwarz.com

Printed in Germany 0201/0902 (Bi bb)